ISO 20022

Card Payments Exchanges - Terminal Management - DRAFT -

Message Definition Report - Part 2

For review by the Cards and Related Financial Services SEG

This document provides details of the Message Definitions for Card Payments Exchanges - Terminal Management - DRAFT -.

December 2021

Table of Contents

1 Message Set Overview

Introduction

Set of messages that support card-related, terminal management services between a Terminal Management System (TMS) and a Point of Interaction (POI) system.

1.1 List of MessageDefinitions

The following table lists all MessageDefinitions described in this book.

MessageDefinition	Definition
DRAFT1catm.001.001.11 StatusReportV11	The StatusReport message is sent by a POI to inform the master terminal manager (MTM) or the terminal manager (TM) about the status of the acceptor system including the identification of the POI, its components and their installed versions.
DRAFT1catm.002.001.10 ManagementPlanReplacementV10	The ManagementPlanReplacement message is sent by a terminal manager to a POI to set maintenance actions to be performed.
DRAFT1catm.003.001.11 AcceptorConfigurationUpdateV11	The AcceptorConfigurationUpdate message is sent by a TM to a POI to update configurations.
DRAFT1catm.005.001.08 MaintenanceDelegationRequestV08	The MaintenanceDelegationRequest message is sent by a terminal manager to the master terminal manager to request delegation of maintenance functions or maintenance operation on the terminal estate managed by the master terminal manager.
DRAFT1catm.006.001.06 MaintenanceDelegationResponseV06	The MaintenanceDelegationResponse message is sent by the master terminal manager to a terminal manager to provide the outcome of a maintenance delegation request.
DRAFT1catm.007.001.05 CertificateManagementRequestV05	The CertificateManagementRequest message is sent by a POI terminal or any intermediary entity either to a terminal manager acting as a certificate authority for managing X.509 certificate of a public key owned by the initiating party, or for requesting the inclusion or the removal of the POI to a white list of the terminal manager.
DRAFT1catm.008.001.05 CertificateManagementResponseV05	The CertificateManagementResponse is sent by a terminal manager in response to a CertificateManagementRequest to provide the outcome of the requested service.

2 DRAFT1catm.001.001.11 StatusReportV11

2.1 MessageDefinition Functionality

The StatusReport message is sent by a POI to inform the master terminal manager (MTM) or the terminal manager (TM) about the status of the acceptor system including the identification of the POI, its components and their installed versions.

Outline

The StatusReportV11 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Set of characteristics related to the transfer of the status report.

B. StatusReport

   Status of the point of interaction (POI), its components and their installed versions.

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

2.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <Document> <StsRpt>	[1..1]			
	Header <*Hdr*>	[1..1]			6
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		7
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		7
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		7
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		7
	InitiatingParty <*InitgPty*>	[1..1]	±		7
	RecipientParty <*RcptPty*>	[0..1]	±		8
	Traceability <*Tracblt*>	[0..*]	±		8
	StatusReport <*StsRpt*>	[1..1]			9
	POIIdentification <*POIId*>	[1..1]	±		10
	InitiatingTrigger <*InitgTrggr*>	[0..1]			11
	TriggerSource <*TrggrSrc*>	[1..1]	CodeSet		11
	SourceIdentification <*SrcId*>	[1..1]	Text		12
	TriggerType <*TrggrTp*>	[1..1]	CodeSet		12
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		12
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		12
	DataSet <*DataSet*>	[1..1]			13
	Identification <*Id*>	[1..1]	±		14
	SequenceCounter <*SeqCntr*>	[0..1]	Text		14
	LastSequence <*LastSeq*>	[0..1]	Indicator		14
	Content <*Cntt*>	[1..1]			14
	POICapabilities <*POICpblties*>	[0..1]	±		15
	POIComponent <*POICmpnt*>	[0..*]	±		16
	POIGroupIdentification <*POIGrpId*>	[0..*]	Text		18
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		18
	POIDateTime <*POIDtTm*>	[1..1]	DateTime		19
	DataSetRequired <*DataSetReqrd*>	[0..*]			19
	Identification <*Id*>	[1..1]	±		19
	POIChallenge <*POIChllng*>	[0..1]	Binary		19

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TMChallenge <*TMChllng*>	[0..1]	Binary		20
	SessionKey <*SsnKey*>	[0..1]	±		20
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		20
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		20
	Event <*Evt*>	[0..*]	±		21
	Errors <*Errs*>	[0..*]	Text		21
	SecurityTrailer <*SctyTrlr*>	[0..1]	±		21

2.3 Constraints

C1 ActiveCurrency

The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217 Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

C2 AnyBIC

Only a valid Business identifier code is allowed. Business identifier codes for financial or non-financial institutions are registered and published by the ISO 9362 Registration Authority in the ISO directory of BICs, and consists of eight (8) or eleven (11) contiguous characters.

C3 Country

The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

C4 IBAN

A valid IBAN consists of all three of the following components: Country Code, check digits and BBAN.

C5 SupplementaryDataRule

This component may not be used without the explicit approval of a SEG and submission to the RA of ISO 20022 compliant structure(s) to be used in the Envelope element.

C6 ValidationByTable

Must be a valid terrestrial language.

2.4 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

2.4.1 Header <Hdr>

Presence: [1..1]

Definition: Set of characteristics related to the transfer of the status report.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		7
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		7
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		7
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		7
	InitiatingParty <*InitgPty*>	[1..1]	±		7
	RecipientParty <*RcptPty*>	[0..1]	±		8
	Traceability <*Tracblt*>	[0..*]	±		8

2.4.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

2.4.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

2.4.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

2.4.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

2.4.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

2.4.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

2.4.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <TracBlt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

2.4.2 StatusReport <StsRpt>

Presence: [1..1]

Definition: Status of the point of interaction (POI), its components and their installed versions.

StatusReport <StsRpt> contains the following **StatusReport11** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIIdentification <*POIId*>	[1..1]	±		10
	InitiatingTrigger <*InitgTrggr*>	[0..1]			11
	TriggerSource <*TrggrSrc*>	[1..1]	CodeSet		11
	SourceIdentification <*SrcId*>	[1..1]	Text		12
	TriggerType <*TrggrTp*>	[1..1]	CodeSet		12
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		12
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		12
	DataSet <*DataSet*>	[1..1]			13
	Identification <*Id*>	[1..1]	±		14
	SequenceCounter <*SeqCntr*>	[0..1]	Text		14
	LastSequence <*LastSeq*>	[0..1]	Indicator		14
	Content <*Cntt*>	[1..1]			14
	POICapabilities <*POICpblties*>	[0..1]	±		15
	POIComponent <*POICmpnt*>	[0..*]	±		16
	POIGroupIdentification <*POIGrpId*>	[0..*]	Text		18
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		18
	POIDateTime <*POIDtTm*>	[1..1]	DateTime		19
	DataSetRequired <*DataSetReqrd*>	[0..*]			19
	Identification <*Id*>	[1..1]	±		19
	POIChallenge <*POIChllng*>	[0..1]	Binary		19
	TMChallenge <*TMChllng*>	[0..1]	Binary		20
	SessionKey <*SsnKey*>	[0..1]	±		20
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		20
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		20
	Event <*Evt*>	[0..*]	±		21
	Errors <*Errs*>	[0..*]	Text		21

2.4.2.1 POIIdentification <POIId>

Presence: [1..1]

Definition: Identification of the point of interaction for terminal management.

POIIdentification <POIId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

2.4.2.2 InitiatingTrigger <InitgTrggr>

Presence: [0..1]

Definition: Identification of the requestor.

InitiatingTrigger <InitgTrggr> contains the following **TriggerInformation2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TriggerSource <*TrggrSrc*>	[1..1]	CodeSet		11
	SourceIdentification <*SrcId*>	[1..1]	Text		12
	TriggerType <*TrggrTp*>	[1..1]	CodeSet		12
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		12

2.4.2.2.1 TriggerSource <TrggrSrc>

Presence: [1..1]

Definition: Actor who trigger the request.

Datatype: "PartyType5Code" on page 495

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACQR	Acquirer	Entity acquiring card transactions.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

2.4.2.2.2 SourceIdentification <SrcId>

Presence: [1..1]

Definition: Identification of the trigger source.

Datatype: "Max35Text" on page 519

2.4.2.2.3 TriggerType <TrggrTp>

Presence: [1..1]

Definition: Identification of the type of the call.

Datatype: "ExchangePolicy2Code" on page 485

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

2.4.2.2.4 AdditionalInformation <AddtlInf>

Presence: [0..1]

Definition: Additional information related to request.

Datatype: "Max70Text" on page 520

2.4.2.3 TerminalManagerIdentification <TermnlMgrId>

Presence: [1..1]

Definition: Identification of the terminal management system (TMS) to contact for the maintenance.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

2.4.2.4 DataSet <DataSet>

Presence: [1..1]

Definition: Data related to a status report of a point of interaction (POI).

DataSet <DataSet> contains the following **StatusReportDataSetRequest3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		14
	SequenceCounter <*SeqCntr*>	[0..1]	Text		14
	LastSequence <*LastSeq*>	[0..1]	Indicator		14
	Content <*Cntt*>	[1..1]			14
	POICapabilities <*POICpblties*>	[0..1]	±		15
	POIComponent <*POICmpnt*>	[0..*]	±		16
	POIGroupIdentification <*POIGrpId*>	[0..*]	Text		18
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		18
	POIDateTime <*POIDtTm*>	[1..1]	DateTime		19
	DataSetRequired <*DataSetReqrd*>	[0..*]			19
	Identification <*Id*>	[1..1]	±		19
	POIChallenge <*POIChllng*>	[0..1]	Binary		19
	TMChallenge <*TMChllng*>	[0..1]	Binary		20
	SessionKey <*SsnKey*>	[0..1]	±		20
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		20
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		20
	Event <*Evt*>	[0..*]	±		21
	Errors <*Errs*>	[0..*]	Text		21

2.4.2.4.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the data set containing the status report.

Identification <Id> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

2.4.2.4.2 SequenceCounter <SeqCntr>

Presence: [0..1]

Definition: Counter to identify a single data set within the whole transfer.

Datatype: "Max9NumericText" on page 521

2.4.2.4.3 LastSequence <LastSeq>

Presence: [0..1]

Definition: Indication of the last sequence in case of split messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

2.4.2.4.4 Content <Cntt>

Presence: [1..1]

Definition: Content of the status report.

Content <Cntt> contains the following **StatusReportContent11** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POICapabilities <*POICpblties*>	[0..1]	±		15
	POIComponent <*POICmpnt*>	[0..*]	±		16
	POIGroupIdentification <*POIGrpId*>	[0..*]	Text		18
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		18
	POIDateTime <*POIDtTm*>	[1..1]	DateTime		19
	DataSetRequired <*DataSetReqrd*>	[0..*]			19
	Identification <*Id*>	[1..1]	±		19
	POIChallenge <*POIChllng*>	[0..1]	Binary		19
	TMChallenge <*TMChllng*>	[0..1]	Binary		20
	SessionKey <*SsnKey*>	[0..1]	±		20
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		20
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		20
	Event <*Evt*>	[0..*]	±		21
	Errors <*Errs*>	[0..*]	Text		21

2.4.2.4.4.1 POICapabilities <POICpblties>

Presence: [0..1]

Definition: Capabilities of the POI (Point Of Interaction) performing the status report.

POICapabilities <POICpblties> contains the following elements (see "PointOfInteractionCapabilities9" on page 377 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardReadingCapabilities <*CardRdngCpblties*>	[0..*]	CodeSet		378
	CardholderVerificationCapabilities <*CrdhldrVrfctnCpblties*>	[0..*]	CodeSet		379
	PINLengthCapabilities <*PINLngthCpblties*>	[0..1]	Quantity		379
	ApprovalCodeLength <*ApprvlCdLngth*>	[0..1]	Quantity		379
	MaxScriptLength <*MxScrptLngth*>	[0..1]	Quantity		380
	CardCaptureCapable <*CardCaptrCpbl*>	[0..1]	Indicator		380
	OnLineCapabilities <*OnLineCpblties*>	[0..1]	CodeSet		380
	MessageCapabilities <*MsgCpblties*>	[0..*]			380
	Destination <*Dstn*>	[1..*]	CodeSet		380
	AvailableFormat <*AvlblFrmt*>	[0..*]	CodeSet		381
	NumberOfLines <*NbOfLines*>	[0..1]	Quantity		381
	LineWidth <*LineWidth*>	[0..1]	Quantity		381
	AvailableLanguage <*AvlblLang*>	[0..*]	CodeSet	C6	381

2.4.2.4.4.2 POIComponent <POICmpnt>

Presence: [0..*]

Definition: Data related to a component of the POI (Point Of Interaction) performing the status report.

POIComponent <POICmpnt> contains the following elements (see "PointOfInteractionComponent12" on page 256 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		258
	SubTypeInformation <*SubTpInf*>	[0..1]	Text		259
	Identification <*Id*>	[1..1]			260
	ItemNumber <*ItmNb*>	[0..1]	Text		260
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		260
	Identification <*Id*>	[0..1]	Text		260
	SerialNumber <*SrlNb*>	[0..1]	Text		260
	Status <*Sts*>	[0..1]			260
	VersionNumber <*VrsnNb*>	[0..1]	Text		261
	Status <*Sts*>	[0..1]	CodeSet		261
	ExpiryDate <*XpryDt*>	[0..1]	Date		261
	StandardCompliance <*StdCmplc*>	[0..*]			261
	Identification <*Id*>	[1..1]	Text		261
	Version <*Vrsn*>	[1..1]	Text		262
	Issuer <*Issr*>	[1..1]	Text		262
	Characteristics <*Chrtcs*>	[0..1]			262
	Memory <*Mmry*>	[0..*]			263
	Identification <*Id*>	[1..1]	Text		264
	TotalSize <*TtlSz*>	[1..1]	Quantity		264
	FreeSize <*FreeSz*>	[1..1]	Quantity		264
	Unit <*Unit*>	[1..1]	CodeSet		264
	Communication <*Com*>	[0..*]			264
	CommunicationType <*ComTp*>	[1..1]	CodeSet		265
	RemoteParty <*RmotPty*>	[1..*]	CodeSet		266
	Active <*Actv*>	[1..1]	Indicator		266
	Parameters <*Params*>	[0..1]	±		266
	PhysicalInterface <*PhysIntrfc*>	[0..1]			267
	InterfaceName <*IntrfcNm*>	[1..1]	Text		267
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		267
	UserName <*UsrNm*>	[0..1]	Text		268

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AccessCode <*AccsCd*>	[0..1]	Binary		268
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		268
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		268
	SecurityAccessModules <*SctyAccsMdls*>	[0..1]	Quantity		269
	SubscriberIdentityModules <*SbcbrIdntyMdls*>	[0..1]	Quantity		269
	SecurityElement <*SctyElmt*>	[0..*]	±		269
	Assessment <*Assmnt*>	[0..*]			269
	Type <*Tp*>	[1..1]	CodeSet		270
	Assigner <*Assgnr*>	[1..*]	Text		270
	DeliveryDate <*DlvryDt*>	[0..1]	DateTime		270
	ExpirationDate <*XprtnDt*>	[0..1]	DateTime		270
	Number <*Nb*>	[1..1]	Text		270
	Package <*Packg*>	[0..*]			271
	PackageIdentification <*PackgId*>	[0..1]	±		271
	PackageLength <*PackgLngth*>	[0..1]	Quantity		271
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		271
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		272
	PackageBlock <*PackgBlck*>	[0..*]			272
	Identification <*Id*>	[1..1]	Text		272
	Value <*Val*>	[0..1]	Binary		272
	ProtectedValue <*PrtctdVal*>	[0..1]	±		272
	Type <*Tp*>	[0..1]	Text		273

2.4.2.4.4.3 POIGroupIdentification <POIGrpId>

Presence: [0..*]

Definition: Identifier assigned to a set of POI terminals performing some categories of transactions.

Datatype: "Max35Text" on page 519

2.4.2.4.4.4 AttendanceContext <AttndncCntxt>

Presence: [0..1]

Definition: Human attendance at the POI (Point Of Interaction) location during transactions.

Datatype: "AttendanceContext1Code" on page 471

CodeName	Name	Definition
ATTD	Attended	Attended payment, with an attendant.

CodeName	Name	Definition
SATT	SemiAttended	Semi-attended, including self checkout. An attendant supervises several payment, and could be called to help the cardholder.
UATT	Unattended	Unattended payment, no attendant present.

2.4.2.4.4.5 POIDateTime <POIDtTm>

Presence: [1..1]

Definition: System date time of the point of interaction (POI) sending the status report.

Datatype: "ISODateTime" on page 513

2.4.2.4.4.6 DataSetRequired <DataSetReqrd>

Presence: [0..*]

Definition: Request the terminal management system to answer with the identified data set.

DataSetRequired <DataSetReqrd> contains the following **DataSetRequest3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		19
	POIChallenge <*POIChllng*>	[0..1]	Binary		19
	TMChallenge <*TMChllng*>	[0..1]	Binary		20
	SessionKey <*SsnKey*>	[0..1]	±		20
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		20
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		20

2.4.2.4.4.6.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the required data set.

Identification <Id> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

2.4.2.4.4.6.2 POIChallenge <POIChllng>

Presence: [0..1]

Definition: Point of interaction challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

2.4.2.4.4.6.3 TMChallenge <TMChlIng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

2.4.2.4.4.6.4 SessionKey <SsnKey>

Presence: [0..1]

Definition: Temporary encryption key that the host will use for protecting keys to download.

SessionKey <SsnKey> contains the following elements (see "CryptographicKey16" on page 419 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		419
	AdditionalIdentification <*AddtlId*>	[0..1]	Binary		419
	Name <*Nm*>	[0..1]	Text		420
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		420
	ItemNumber <*ItmNb*>	[0..1]	Text		420
	Version <*Vrsn*>	[1..1]	Text		420
	Type <*Tp*>	[0..1]	CodeSet		420
	Function <*Fctn*>	[0..*]	CodeSet		421
	ActivationDate <*ActvtnDt*>	[0..1]	DateTime		421
	DeactivationDate <*DeactvtnDt*>	[0..1]	DateTime		422
	KeyValue <*KeyVal*>	[0..1]	±		422
	KeyCheckValue <*KeyChckVal*>	[0..1]	Binary		422
	AdditionalManagementInformation <*AddtlMgmtInf*>	[0..*]			422
	Name <*Nm*>	[1..1]	Text		422
	Value <*Val*>	[0..1]	Text		423

2.4.2.4.4.6.5 DelegationProof <DlgtnProof>

Presence: [0..1]

Definition: Proof of delegation to be validated by the terminal manager receiving a status report from a new POI.

Datatype: "Max5000Binary" on page 462

2.4.2.4.4.6.6 ProtectedDelegationProof <PrtctdDlgtnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtnProof> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

2.4.2.4.4.7 Event <Evt>

Presence: [0..*]

Definition: Result of an individual terminal management action by the point of interaction.

Event <Evt> contains the following elements (see "TMSEvent9" on page 391 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TimeStamp <*TmStmp*>	[1..1]	DateTime		391
	Result <*Rslt*>	[1..1]	CodeSet		391
	ActionIdentification <*ActnId*>	[1..1]			392
	ActionType <*ActnTp*>	[1..1]	CodeSet		393
	DataSetIdentification <*DataSetId*>	[0..1]	±		393
	AdditionalErrorInformation <*AddtlErrInf*>	[0..1]	Text		394
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	Text		394
	DeviceResponse <*DvcRspn*>	[0..1]	±		394

2.4.2.4.4.8 Errors <Errs>

Presence: [0..*]

Definition: Error log of the point of interaction since the last status report.

Datatype: "Max140Text" on page 517

2.4.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

3 DRAFT1catm.002.001.10 ManagementPlanReplacementV10

3.1 MessageDefinition Functionality

The ManagementPlanReplacement message is sent by a terminal manager to a POI to set maintenance actions to be performed.

Outline

The ManagementPlanReplacementV10 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Set of characteristics related to the transfer of the management plan.

B. ManagementPlan

   Sequence of terminal maintenance actions to be performed by a point of interaction (POI).

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

3.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <Document> <MgmtPlanRplcmnt>	[1..1]			
	Header <*Hdr*>	[1..1]			26
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		26
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		26
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		27
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		27
	InitiatingParty <*InitgPty*>	[1..1]	±		27
	RecipientParty <*RcptPty*>	[0..1]	±		27
	Traceability <*Tracblt*>	[0..*]	±		28
	ManagementPlan <*MgmtPlan*>	[1..1]			28
	POIIdentification <*POIId*>	[0..1]	±		30
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		30
	DataSet <*DataSet*>	[1..1]			31
	Identification <*Id*>	[1..1]	±		33
	SequenceCounter <*SeqCntr*>	[0..1]	Text		33
	LastSequence <*LastSeq*>	[0..1]	Indicator		33
	Content <*Cntt*>	[0..1]			33
	TMChallenge <*TMChllng*>	[0..1]	Binary		35
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		35
	Action <*Actn*>	[1..*]			35
	Type <*Tp*>	[1..1]	CodeSet		36
	RemoteAccess <*RmotAccs*>	[0..1]	±		37
	Key <*Key*>	[0..*]			38
	KeyIdentification <*KeyId*>	[1..1]	Text		38
	KeyVersion <*KeyVrsn*>	[1..1]	Text		38
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		38
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		38
	Type <*Tp*>	[0..1]	CodeSet		38
	Function <*Fctn*>	[0..*]	CodeSet		39
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		40

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		40
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		40
	DataSetIdentification <*DataSetId*>	[0..1]	±		40
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		41
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		42
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		42
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		42
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		42
	Trigger <*Trggr*>	[1..1]	CodeSet		43
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		43
	ReTry <*ReTry*>	[0..1]	±		43
	TimeCondition <*TmCond*>	[0..1]	±		44
	TMChallenge <*TMChllng*>	[0..1]	Binary		44
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		44
	ErrorAction <*ErrActn*>	[0..*]	±		44
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		45
	MessageItem <*MsgItm*>	[0..*]	±		45
	DeviceRequest <*DvcReq*>	[0..1]	±		45
	SecurityTrailer <*SctyTrlr*>	[0..1]	±		48

3.3 Constraints

C1 ActiveCurrency

The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217 Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

C2 AnyBIC

Only a valid Business identifier code is allowed. Business identifier codes for financial or non-financial institutions are registered and published by the ISO 9362 Registration Authority in the ISO directory of BICs, and consists of eight (8) or eleven (11) contiguous characters.

C3 Country

The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

C4 IBAN

A valid IBAN consists of all three of the following components: Country Code, check digits and BBAN.

C5 SupplementaryDataRule

This component may not be used without the explicit approval of a SEG and submission to the RA of ISO 20022 compliant structure(s) to be used in the Envelope element.

C6 ValidationByTable

Must be a valid terrestrial language.

3.4 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

3.4.1 Header <Hdr>

Presence: [1..1]

Definition: Set of characteristics related to the transfer of the management plan.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		26
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		26
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		27
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		27
	InitiatingParty <*InitgPty*>	[1..1]	±		27
	RecipientParty <*RcptPty*>	[0..1]	±		27
	Traceability <*Tracblt*>	[0..*]	±		28

3.4.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

3.4.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

3.4.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

3.4.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

3.4.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

3.4.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

3.4.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <Tracblt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

3.4.2 ManagementPlan <MgmtPlan>

Presence: [1..1]

Definition: Sequence of terminal maintenance actions to be performed by a point of interaction (POI).

ManagementPlan <MgmtPlan> contains the following **ManagementPlan10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIIdentification <*POIId*>	[0..1]	±		30
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		30
	DataSet <*DataSet*>	[1..1]			31
	Identification <*Id*>	[1..1]	±		33
	SequenceCounter <*SeqCntr*>	[0..1]	Text		33
	LastSequence <*LastSeq*>	[0..1]	Indicator		33
	Content <*Cntt*>	[0..1]			33
	TMChallenge <*TMChllng*>	[0..1]	Binary		35
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		35
	Action <*Actn*>	[1..*]			35
	Type <*Tp*>	[1..1]	CodeSet		36
	RemoteAccess <*RmotAccs*>	[0..1]	±		37
	Key <*Key*>	[0..*]			38
	KeyIdentification <*KeyId*>	[1..1]	Text		38
	KeyVersion <*KeyVrsn*>	[1..1]	Text		38
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		38
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		38
	Type <*Tp*>	[0..1]	CodeSet		38
	Function <*Fctn*>	[0..*]	CodeSet		39
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		40
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		40
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		40
	DataSetIdentification <*DataSetId*>	[0..1]	±		40
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		41
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		42
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		42
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		42
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		42
	Trigger <*Trggr*>	[1..1]	CodeSet		43
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		43
	ReTry <*ReTry*>	[0..1]	±		43

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TimeCondition <*TmCond*>	[0..1]	±		44
	TMChallenge <*TMChllng*>	[0..1]	Binary		44
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		44
	ErrorAction <*ErrActn*>	[0..*]	±		44
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		45
	MessageItem <*MsgItm*>	[0..*]	±		45
	DeviceRequest <*DvcReq*>	[0..1]	±		45

3.4.2.1 POIIdentification <POIId>

Presence: [0..1]

Definition: Identification of the point of interaction (POI) for terminal management.

POIIdentification <POIId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

3.4.2.2 TerminalManagerIdentification <TermnlMgrId>

Presence: [1..1]

Definition: Identification of the terminal management system (TMS) sending the management plan.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

3.4.2.3 DataSet <DataSet>

Presence: [1..1]

Definition: Data set related to the sequence of actions to be performed by a point of interaction (POI).

DataSet <DataSet> contains the following **TerminalManagementDataSet31** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		33
	SequenceCounter <*SeqCntr*>	[0..1]	Text		33
	LastSequence <*LastSeq*>	[0..1]	Indicator		33
	Content <*Cntt*>	[0..1]			33
	TMChallenge <*TMChllng*>	[0..1]	Binary		35
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		35
	Action <*Actn*>	[1..*]			35
	Type <*Tp*>	[1..1]	CodeSet		36
	RemoteAccess <*RmotAccs*>	[0..1]	±		37
	Key <*Key*>	[0..*]			38
	KeyIdentification <*KeyId*>	[1..1]	Text		38
	KeyVersion <*KeyVrsn*>	[1..1]	Text		38
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		38
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		38
	Type <*Tp*>	[0..1]	CodeSet		38
	Function <*Fctn*>	[0..*]	CodeSet		39
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		40
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		40
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		40
	DataSetIdentification <*DataSetId*>	[0..1]	±		40
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		41
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		42
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		42
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		42
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		42
	Trigger <*Trggr*>	[1..1]	CodeSet		43
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		43
	ReTry <*ReTry*>	[0..1]	±		43
	TimeCondition <*TmCond*>	[0..1]	±		44
	TMChallenge <*TMChllng*>	[0..1]	Binary		44
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		44

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ErrorAction <*ErrActn*>	[0..*]	±		44
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		45
	MessageItem <*MsgItm*>	[0..*]	±		45
	DeviceRequest <*DvcReq*>	[0..1]	±		45

3.4.2.3.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the data set containing the management plan.

Identification <Id> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

3.4.2.3.2 SequenceCounter <SeqCntr>

Presence: [0..1]

Definition: Counter to identify a single data set within the whole transfer.

Datatype: "Max9NumericText" on page 521

3.4.2.3.3 LastSequence <LastSeq>

Presence: [0..1]

Definition: Indication of the last sequence in case of split messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

3.4.2.3.4 Content <Cntt>

Presence: [0..1]

Definition: Content of the management plan.

Content <Cntt> contains the following **ManagementPlanContent10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TMChallenge <*TMChllng*>	[0..1]	Binary		35
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		35
	Action <*Actn*>	[1..*]			35
	Type <*Tp*>	[1..1]	CodeSet		36
	RemoteAccess <*RmotAccs*>	[0..1]	±		37
	Key <*Key*>	[0..*]			38
	KeyIdentification <*KeyId*>	[1..1]	Text		38
	KeyVersion <*KeyVrsn*>	[1..1]	Text		38
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		38
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		38
	Type <*Tp*>	[0..1]	CodeSet		38
	Function <*Fctn*>	[0..*]	CodeSet		39
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		40
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		40
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		40
	DataSetIdentification <*DataSetId*>	[0..1]	±		40
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		41
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		42
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		42
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		42
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		42
	Trigger <*Trggr*>	[1..1]	CodeSet		43
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		43
	ReTry <*ReTry*>	[0..1]	±		43
	TimeCondition <*TmCond*>	[0..1]	±		44
	TMChallenge <*TMChllng*>	[0..1]	Binary		44
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		44
	ErrorAction <*ErrActn*>	[0..*]	±		44
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		45
	MessageItem <*MsgItm*>	[0..*]	±		45
	DeviceRequest <*DvcReq*>	[0..1]	±		45

3.4.2.3.4.1 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

3.4.2.3.4.2 KeyEnciphermentCertificate <KeyNcphrmntCert>

Presence: [0..*]

Definition: Certificate chain of an asymmetric encryption keys for the encryption of temporary transport key of the key to inject.

Datatype: "Max10KBinary" on page 461

3.4.2.3.4.3 Action <Actn>

Presence: [1..*]

Definition: Terminal management action to be performed by the point of interaction (POI).

Action <Actn> contains the following **TMSAction10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		36
	RemoteAccess <*RmotAccs*>	[0..1]	±		37
	Key <*Key*>	[0..*]			38
	KeyIdentification <*KeyId*>	[1..1]	Text		38
	KeyVersion <*KeyVrsn*>	[1..1]	Text		38
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		38
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		38
	Type <*Tp*>	[0..1]	CodeSet		38
	Function <*Fctn*>	[0..*]	CodeSet		39
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		40
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		40
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		40
	DataSetIdentification <*DataSetId*>	[0..1]	±		40
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		41
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		42
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		42
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		42
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		42
	Trigger <*Trggr*>	[1..1]	CodeSet		43
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		43
	ReTry <*ReTry*>	[0..1]	±		43
	TimeCondition <*TmCond*>	[0..1]	±		44
	TMChallenge <*TMChllng*>	[0..1]	Binary		44
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		44
	ErrorAction <*ErrActn*>	[0..*]	±		44
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		45
	MessageItem <*MsgItm*>	[0..*]	±		45
	DeviceRequest <*DvcReq*>	[0..1]	±		45

3.4.2.3.4.3.1 Type <Tp>

Presence: [1..1]

Definition: Types of action to be performed by a point of interaction (POI).

Datatype: "TerminalManagementAction5Code" on page 507

CodeName	Name	Definition
DCTV	Deactivate	Request to deactivate the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
DWNL	Download	Request to download the element identified inside the message exchange.
INST	Install	Request to install the element identified inside the message exchange.
RSTR	Restart	Request to restart the element identified inside the message exchange.
UPLD	Upload	Request to upload the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.
BIND	Bind	Request sent to a POI to bind with a server.
RBND	Rebind	Request sent to a POI to rebind with a server.
UBND	Unbind	Request sent to a POI to unbind with a server.
ACTV	Activate	Request to activate the element identified inside the message exchange.
DEVR	DeviceRequest	Request to execute a device request.

3.4.2.3.4.3.2 RemoteAccess <RmotAccs>

Presence: [0..1]

Definition: Host access information.

RemoteAccess <RmotAccs> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

3.4.2.3.4.3.3 Key <Key>

Presence: [0..*]

Definition: Cryptographic key used to communicate with the host.

Key <Key> contains the following **KEKIdentifier5** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		38
	KeyVersion <*KeyVrsn*>	[1..1]	Text		38
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		38
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		38
	Type <*Tp*>	[0..1]	CodeSet		38
	Function <*Fctn*>	[0..*]	CodeSet		39

3.4.2.3.4.3.3.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 517

3.4.2.3.4.3.3.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 517

3.4.2.3.4.3.3.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 515

3.4.2.3.4.3.3.4 DerivationIdentification <DerivtnId>

Presence: [0..1]

Definition: Identification used for derivation of a unique key from a master key provided for the data protection.

Datatype: "Min5Max16Binary" on page 463

3.4.2.3.4.3.3.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 481

CodeName	Name	Definition
AES2	AES128	AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by

CodeName	Name	Definition
		the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE3	DES112	Data encryption standard key of 112 bits (without the parity bits).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.
AES9	AES192	AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
AES5	AES256	AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

3.4.2.3.4.3.3.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 488

CodeName	Name	Definition
ENCR	Encryption	Key may encrypt.
DCPT	Decryption	Key may decrypt.
DENC	DataEncryption	Key may encrypt data.
DDEC	DataDecryption	Key may decrypt data.
TRNI	TranslateInput	Key may encrypt information before translation.
TRNX	TranslateOutput	Key may encrypt information after translation.
MACG	MessageAuthenticationCodeGeneration	Key may generate message authentication codes (MAC).
MACV	MessageAuthenticationCodeVerification	Key may verify message authentication codes (MAC).
SIGG	SignatureGeneration	Key may generate digital signatures.
SUGV	SignatureVerification	Key may verify digital signatures.
PINE	PINEncryption	Key may encrypt personal identification numbers (PIN).
PIND	PINDecryption	Key may decrypt personal identification numbers (PIN).

CodeName	Name	Definition
PINV	PINVerification	Key may verify personal identification numbers (PIN).
KEYG	KeyGeneration	Key may generate keys.
KEYI	KeyImport	Key may import keys.
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

3.4.2.3.4.3.4 TerminalManagerIdentification <TermnlMgrId>

Presence: [0..1]

Definition: Identification of the master terminal manager or the terminal manager with which the POI has to perform the action.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

3.4.2.3.4.3.5 TMSProtocol <TMSPrtcol>

Presence: [0..1]

Definition: TMS protocol to use for performing the maintenance action.

Datatype: "Max35Text" on page 519

3.4.2.3.4.3.6 TMSProtocolVersion <TMSPrtcolVrsn>

Presence: [0..1]

Definition: Version of the TMS protocol to use to perform the maintenance action.

Datatype: "Max35Text" on page 519

3.4.2.3.4.3.7 DataSetIdentification <DataSetId>

Presence: [0..1]

Definition: Data set on which the action has to be performed.

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

3.4.2.3.4.3.8 ComponentType <CmpntTp>

Presence: [0..*]

Definition: Type of POI components to send in a status report.

Datatype: "DataSetCategory17Code" on page 483

CodeName	Name	Definition
AQPR	AcquirerParameters	Acquirer specific configuration parameters for the point of interaction (POI) system.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
TXCP	BatchCapture	Batch upload of transaction data (data capture of a group of transactions).
AKCP	CaptureResponse	Batch download response for the batch capture of transactions.
DLGT	DelegationData	Data needed to create a terminal management sub-domain.
MGTP	ManagementPlan	Configuration of management plan in the point of interaction.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
SCPR	SecurityParameters	Point of interaction parameters related to the security of software application and application protocol.
SWPK	SoftwareModule	Software module.
STRP	StatusReport	Report of software configuration and parameter status.
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
VDPR	VendorParameters	Point of interaction parameters defined by the manufacturer for instance the PIN verification capabilities.
PARA	Parameters	Any combination of configuration parameters for the point of interaction (POI).

CodeName	Name	Definition
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
LOGF	LogFile	Any repository used for recording log traces.
CMRQ	CertificateManagementRequest	Trigger for CertificateManagementRequest.
MDFL	MediaFile	Media file managed by an application of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

3.4.2.3.4.3.9 DelegationScopeIdentification <DlgtnScpId>

Presence: [0..1]

Definition: Identification of the delegation scope assigned by the MTM.

Datatype: "Max35Text" on page 519

3.4.2.3.4.3.10 DelegationScopeDefinition <DlgtnScpDef>

Presence: [0..1]

Definition: This element contains all information relevant to the DelegationScopeIdentification. The format of this element is out of scope of this definition.

Datatype: "Max3000Binary" on page 462

3.4.2.3.4.3.11 DelegationProof <DlgtnProof>

Presence: [0..1]

Definition: This element contains the necessary information to secure the management of the Delegation. The format of this element is out of scope of this definition.

Datatype: "Max5000Binary" on page 462

3.4.2.3.4.3.12 ProtectedDelegationProof <PrtctdDlgtnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtnProof> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

3.4.2.3.4.3.13 Trigger <Trggr>

Presence: [1..1]

Definition: Event on which the action has to be activated by the point of interaction (POI).

Datatype: "TerminalManagementActionTrigger1Code" on page 509

CodeName	Name	Definition
DATE	DateTime	Date and time trigger the terminal management action.
HOST	HostEvent	Acquirer triggers the terminal management action.
MANU	Manual	Acceptor triggers the terminal management action.
SALE	SaleEvent	Sale system triggers the terminal management action.

3.4.2.3.4.3.14 AdditionalProcess <AddtlPrc>

Presence: [0..*]

Definition: Additional process to perform before starting or after completing the action by the point of interaction (POI).

Datatype: "TerminalManagementAdditionalProcess1Code" on page 509

CodeName	Name	Definition
MANC	ManualConfirmation	Manual confirmation of the merchant before the terminal management action.
RCNC	Reconciliation	Acquirer reconciliation to be performed before the terminal management action.
RSRT	RestartSystem	Restart the system after performing the terminal management action.

3.4.2.3.4.3.15 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of the action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

3.4.2.3.4.3.16 TimeCondition <TmCond>

Presence: [0..1]

Definition: Date and time the action has to be performed.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming5" on page 456 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	WaitingTime <*WtgTm*>	[0..1]	Text		456
	StartTime <*StartTm*>	[0..1]	DateTime		456
	EndTime <*EndTm*>	[0..1]	DateTime		456
	Period <*Prd*>	[0..1]	Text		457
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		457
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		457

3.4.2.3.4.3.17 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

3.4.2.3.4.3.18 KeyEnciphermentCertificate <KeyNcphrmntCert>

Presence: [0..*]

Definition: Certificate chain for the encryption of temporary transport key of the key to inject.

Datatype: "Max10KBinary" on page 461

3.4.2.3.4.3.19 ErrorAction <ErrActn>

Presence: [0..*]

Definition: Action to perform in case of error on the related action in progress.

ErrorAction <ErrActn> contains the following elements (see "ErrorAction5" on page 390 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionResult <*ActnRslt*>	[1..*]	CodeSet		390
	ActionToProcess <*ActnToPrc*>	[1..1]	CodeSet		391

3.4.2.3.4.3.20 AdditionalInformation <AddtlInf>

Presence: [0..*]

Definition: Additional information about the maintenance action.

Datatype: "Max3000Binary" on page 462

3.4.2.3.4.3.21 MessageItem <MsgItm>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <MsgItm> contains the following elements (see "MessageItemCondition1" on page 376 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemIdentification <*ItmId*>	[1..1]	Text		377
	Condition <*Cond*>	[1..1]	CodeSet		377
	Value <*Val*>	[0..*]	Text		377

3.4.2.3.4.3.22 DeviceRequest <DvcReq>

Presence: [0..1]

Definition: Information related to a device request of the POI.

DeviceRequest <DvcReq> contains the following elements (see "DeviceRequest5" on page 130 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Environment <*Envt*>	[0..1]	±		133
	Context <*Cntxt*>	[0..1]	±		139
	ServiceContent <*SvcCntt*>	[1..1]	CodeSet		142
	DisplayRequest <*DispReq*>	[0..1]			142
	DisplayOutput <*DispOutpt*>	[1..*]	±		142
	InputRequest <*InptReq*>	[0..1]			143
	DisplayOutput <*DispOutpt*>	[0..1]	±		144
	InputData <*InptData*>	[1..1]			145
	DeviceType <*DvcTp*>	[1..1]	CodeSet		146
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		146
	InputCommand <*InptCmd*>	[1..1]	CodeSet		147
	NotifyCardInputFlag <*NtfyCardInptFlg*>	[1..1]	Indicator		148
	MaximumInputTime <*MaxInptTm*>	[0..1]	Quantity		148
	InputText <*InptTxt*>	[0..1]	±		148
	ImmediateResponseFlag <*ImdtRspnFlg*>	[0..1]	Indicator		149
	WaitUserValidationFlag <*WaitUsrVldtnFlg*>	[0..1]	Indicator		149
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		149
	GlobalCorrectionFlag <*GblCrrctnFlg*>	[0..1]	Indicator		150
	DisableCancelFlag <*DsblCclFlg*>	[0..1]	Indicator		150
	DisableCorrectFlag <*DsblCrrctFlg*>	[0..1]	Indicator		150
	DisableValidFlag <*DsblVldFlg*>	[0..1]	Indicator		150
	MenuBackFlag <*MenuBckFlg*>	[0..1]	Indicator		150
	PrintRequest <*PrtReq*>	[0..1]			151
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		151
	ResponseMode <*RspnMd*>	[1..1]	CodeSet		151
	IntegratedPrintFlag <*IntgrtdPrtFlg*>	[0..1]	Indicator		152
	RequiredSignatureFlag <*ReqrdSgntrFlg*>	[0..1]	Indicator		152
	OutputContent <*OutptCntt*>	[1..1]	±		152
	PlayResourceRequest <*PlayRsrcReq*>	[0..1]			153
	ResponseMode <*RspnMd*>	[0..1]	CodeSet		154

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ResourceAction <*RsrcActn*>	[1..1]	CodeSet		154
	SoundVolume <*SoundVol*>	[0..1]	Rate		154
	DisplayResolution <*DispRsltn*>	[0..1]	Text		154
	Resource <*Rsrc*>	[0..1]			154
	ResourceType <*RsrcTp*>	[1..1]	CodeSet		155
	ResourceFormat <*RsrcFrmt*>	[0..1]	CodeSet		155
	Language <*Lang*>	[0..1]	CodeSet	C6	155
	ResourceReference <*RsrcRef*>	[0..1]	Text		155
	TimingSlot <*TmgSlot*>	[0..1]	CodeSet		156
	SecureInputRequest <*ScrInptReq*>	[0..1]			156
	PINRequestType <*PINReqTp*>	[1..1]	CodeSet		156
	PINVerificationMethod <*PINVrfctnMtd*>	[0..1]	Text		157
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		157
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		157
	CardholderPIN <*CrdhldrPIN*>	[0..1]			157
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		157
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		158
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		158
	InitialisationCardReaderRequest <*InitlstnCardRdrReq*>	[0..1]			158
	WarmResetFlag <*WarmRstFlg*>	[0..1]	Indicator		159
	ForceEntryMode <*ForceNtryMd*>	[0..*]	CodeSet		159
	LeaveCardFlag <*LeavCardFlg*>	[0..1]	Indicator		160
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		160
	DisplayOutput <*DispOutpt*>	[0..1]	±		160
	CardReaderAPDURequest <*CardRdrAPDUReq*>	[0..1]			161
	Class <*Clss*>	[1..1]	Binary		161
	Instruction <*Instr*>	[1..1]	Binary		161
	Parameter1 <*Param1*>	[1..1]	Binary		161
	Parameter2 <*Param2*>	[1..1]	Binary		161
	Data <*Data*>	[0..1]	Binary		161
	ExpectedLength <*XpctdLngth*>	[0..1]	Binary		161

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PowerOffCardReaderRequest <*PwrOffCardRdrReq*>	[0..1]			162
	PowerOffMaximumWaitingTime <*PwrOffMaxWtgTm*>	[0..1]	Quantity		162
	DisplayOutput <*DispOutpt*>	[0..1]	±		162
	TransmissionRequest <*TrnsmssnReq*>	[0..1]			163
	DestinationAddress <*DstnAdr*>	[1..1]	±		163
	MaximumTransmissionTime <*MaxTrnsmssnTm*>	[1..1]	Quantity		164
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		164
	MessageToSend <*MsgToSnd*>	[1..1]	Binary		164
	InputNotification <*InptNtfctn*>	[0..1]			164
	ExchangeIdentification <*XchgId*>	[1..1]	Text		164
	OutputContent <*OutptCntt*>	[1..1]	±		165
	SupplementaryData <*SplmtryData*>	[0..*]	±	C5	165

3.4.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

4 DRAFT1catm.003.001.11 AcceptorConfigurationUpdateV11

4.1 MessageDefinition Functionality

The AcceptorConfigurationUpdate message is sent by a TM to a POI to update configurations.

Outline

The AcceptorConfigurationUpdateV11 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Set of characteristics related to the transfer of the acceptor parameters.

B. AcceptorConfiguration

   Acceptor configuration to be downloaded from the terminal management system.

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

4.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <Document> <AccptrCfgtnUpd>	[1..1]			
	Header <*Hdr*>	[1..1]			51
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		51
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		51
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		51
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		52
	InitiatingParty <*InitgPty*>	[1..1]	±		52
	RecipientParty <*RcptPty*>	[0..1]	±		52
	Traceability <*Tracblt*>	[0..*]	±		53
	AcceptorConfiguration <*AccptrCfgtn*>	[1..1]			53
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		54
	POIGroupIdentification <*POIGrpId*>	[0..*]	Text		55
	DataSet <*DataSet*>	[1..*]			55
	Identification <*Id*>	[1..1]	±		56
	SequenceCounter <*SeqCntr*>	[0..1]	Text		56
	LastSequence <*LastSeq*>	[0..1]	Indicator		57
	POIIdentification <*POIId*>	[0..*]	±		57
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		57
	Content <*Cntt*>	[1..1]			57
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		58
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		58
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		59
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		62
	MerchantParameters <*MrchntParams*>	[0..*]	±		62
	TerminalParameters <*TermnlParams*>	[0..*]	±		63
	ApplicationParameters <*ApplParams*>	[0..*]	±		64
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		65
	SecurityParameters <*SctyParams*>	[0..*]	±		66
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		67
	TerminalPackage <*TermnlPackg*>	[0..*]	±		67

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SecurityTrailer <*SctyTrlr*>	[0..1]	±		68

4.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

4.3.1 Header <Hdr>

Presence: [1..1]

Definition: Set of characteristics related to the transfer of the acceptor parameters.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		51
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		51
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		51
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		52
	InitiatingParty <*InitgPty*>	[1..1]	±		52
	RecipientParty <*RcptPty*>	[0..1]	±		52
	Traceability <*Tracblt*>	[0..*]	±		53

4.3.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

4.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

4.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

4.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

4.3.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

4.3.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

4.3.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <Tracblt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

4.3.2 AcceptorConfiguration <AccptrCfgtn>

Presence: [1..1]

Definition: Acceptor configuration to be downloaded from the terminal management system.

AcceptorConfiguration <AccptrCfgtn> contains the following **AcceptorConfiguration11** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		54
	POIGroupIdentification <*POIGrpId*>	[0..*]	Text		55
	DataSet <*DataSet*>	[1..*]			55
	Identification <*Id*>	[1..1]	±		56
	SequenceCounter <*SeqCntr*>	[0..1]	Text		56
	LastSequence <*LastSeq*>	[0..1]	Indicator		57
	POIIdentification <*POIId*>	[0..*]	±		57
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		57
	Content <*Cntt*>	[1..1]			57
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		58
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		58
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		59
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		62
	MerchantParameters <*MrchntParams*>	[0..*]	±		62
	TerminalParameters <*TermnlParams*>	[0..*]	±		63
	ApplicationParameters <*ApplParams*>	[0..*]	±		64
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		65
	SecurityParameters <*SctyParams*>	[0..*]	±		66
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		67
	TerminalPackage <*TermnlPackg*>	[0..*]	±		67

4.3.2.1 TerminalManagerIdentification <TermnlMgrId>

Presence: [1..1]

Definition: Identification of the terminal management system (TMS) sending the acceptor parameters.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

4.3.2.2 POIGroupIdentification <POIGrpId>

Presence: [0..*]

Definition: Identifier assigned to a set of POI terminals performing some categories of transactions.

Datatype: "Max35Text" on page 519

4.3.2.3 DataSet <DataSet>

Presence: [1..*]

Definition: Data set containing the acceptor parameters of a point of interaction (POI).

DataSet <DataSet> contains the following **AcceptorConfigurationDataSet3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		56
	SequenceCounter <*SeqCntr*>	[0..1]	Text		56
	LastSequence <*LastSeq*>	[0..1]	Indicator		57
	POIIdentification <*POIId*>	[0..*]	±		57
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		57
	Content <*Cntt*>	[1..1]			57
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		58
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		58
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		59
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		62
	MerchantParameters <*MrchntParams*>	[0..*]	±		62
	TerminalParameters <*TermnlParams*>	[0..*]	±		63
	ApplicationParameters <*ApplParams*>	[0..*]	±		64
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		65
	SecurityParameters <*SctyParams*>	[0..*]	±		66
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		67
	TerminalPackage <*TermnlPackg*>	[0..*]	±		67

4.3.2.3.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the data set transferred.

Identification <Id> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

4.3.2.3.2 SequenceCounter <SeqCntr>

Presence: [0..1]

Definition: Counter to identify a single data set within the whole transfer.

Datatype: "Max9NumericText" on page 521

4.3.2.3.3 LastSequence <LastSeq>

Presence: [0..1]

Definition: Indication of the last sequence in case of split messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

4.3.2.3.4 POIIdentification <POIId>

Presence: [0..*]

Definition: Identification of the point of interactions involved by the configuration data set.

POIIdentification <POIId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

4.3.2.3.5 ConfigurationScope <CfgtnScp>

Presence: [0..1]

Definition: Scope of the configuration contained in the data set.

Datatype: "PartyType15Code" on page 494

CodeName	Name	Definition
PGRP	POIGroup	Configuration to apply to a subset of the whole POI system.
PSYS	POISystem	Configuration to apply to the whole POI system.
PSNG	SinglePOI	Configuration to apply to a single POI terminal.

4.3.2.3.6 Content <Cntt>

Presence: [1..1]

Definition: Content of the acceptor parameters.

Content <Cntt> contains the following **AcceptorConfigurationContent11** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		58
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		58
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		59
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		62
	MerchantParameters <*MrchntParams*>	[0..*]	±		62
	TerminalParameters <*TermnlParams*>	[0..*]	±		63
	ApplicationParameters <*ApplParams*>	[0..*]	±		64
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		65
	SecurityParameters <*SctyParams*>	[0..*]	±		66
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		67
	TerminalPackage <*TermnlPackg*>	[0..*]	±		67

4.3.2.3.6.1 ReplaceConfiguration <RplcCfgtn>

Presence: [0..1]

Definition: True if the whole configuration related to the terminal manager has to be replaced by the configuration included in the message content.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

4.3.2.3.6.2 TMSProtocolParameters <TMSPrtcolParams>

Presence: [0..*]

Definition: Configuration parameters of the TMS protocol between a POI and a terminal manager.

TMSProtocolParameters <TMSPrtcolParams> contains the following elements (see "TMSProtocolParameters6" on page 203 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		204
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		204
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		205
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		205
	Version <*Vrsn*>	[1..1]	Text		206
	ApplicationIdentification <*ApplId*>	[0..*]	Text		206
	HostIdentification <*HstId*>	[1..1]	Text		206
	POIIdentification <*POIId*>	[0..1]	Text		206
	InitiatingPartyIdentification <*InitgPtyId*>	[0..1]	Text		206
	RecipientPartyIdentification <*RcptPtyId*>	[0..1]	Text		206
	FileTransfer <*FileTrf*>	[0..1]	Indicator		206
	MessageItem <*MsgItm*>	[0..*]	±		206
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		207

4.3.2.3.6.3 AcquirerProtocolParameters <AcqrrPrtcolParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to an acquirer protocol.

AcquirerProtocolParameters <AcqrrPrtcolParams> contains the following elements (see "AcquirerProtocolParameters15" on page 210 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		213
	AcquirerIdentification <*AcqrrId*>	[1..*]	±		213
	Version <*Vrsn*>	[1..1]	Text		213
	ApplicationIdentification <*ApplId*>	[0..*]	Text		213
	Host <*Hst*>	[0..*]			214
	HostIdentification <*HstId*>	[1..1]	Text		214
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		214
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		215
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		215
	OnLineTransaction <*OnLineTx*>	[0..1]			215
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		216
	BatchTransfer <*BtchTrf*>	[0..1]			216
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		217
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		217
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		218
	ReTry <*ReTry*>	[0..1]	±		218
	TimeCondition <*TmCond*>	[0..1]	±		218
	CompletionExchange <*CmpltnXchg*>	[0..1]			218
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		219
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		219
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		220
	ReTry <*ReTry*>	[0..1]	±		220
	TimeCondition <*TmCond*>	[0..1]	±		220
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		220
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		220
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		221
	OffLineTransaction <*OffLineTx*>	[0..1]			221
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		222
	BatchTransfer <*BtchTrf*>	[0..1]			222
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		223

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		223
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		224
	ReTry <*ReTry*>	[0..1]	±		224
	TimeCondition <*TmCond*>	[0..1]	±		224
	CompletionExchange <*CmpltnXchg*>	[0..1]			224
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		225
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		225
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		226
	ReTry <*ReTry*>	[0..1]	±		226
	TimeCondition <*TmCond*>	[0..1]	±		226
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		226
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		226
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		227
	ReconciliationExchange <*RcncltnXchg*>	[0..1]			227
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		227
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		228
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		228
	ReTry <*ReTry*>	[0..1]	±		228
	TimeCondition <*TmCond*>	[0..1]	±		228
	ReconciliationByAcquirer <*RcncltnByAcqrr*>	[0..1]	Indicator		229
	TotalsPerCurrency <*TtlsPerCcy*>	[0..1]	Indicator		229
	SplitTotals <*SpltTtls*>	[0..1]	Indicator		229
	SplitTotalCriteria <*SpltTtlCrit*>	[0..*]	CodeSet		229
	CompletionAdviceMandated <*CmpltnAdvcMndtd*>	[0..1]	Indicator		230
	AmountQualifierForReservation <*AmtQlfrForRsvatn*>	[0..*]	CodeSet		230
	ReconciliationError <*RcncltnErr*>	[0..1]	Indicator		230
	CardDataVerification <*CardDataVrfctn*>	[0..1]	Indicator		231
	NotifyOffLineCancellation <*NtfyOffLineCxl*>	[0..1]	Indicator		231
	BatchTransferContent <*BtchTrfCntt*>	[0..*]	CodeSet		231
	FileTransferBatch <*FileTrfBtch*>	[0..1]	Indicator		231
	BatchDigitalSignature <*BtchDgtlSgntr*>	[0..1]	Indicator		231

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageItem <*MsgItm*>	[0..*]	±		232
	ProtectCardData <*PrtctCardData*>	[1..1]	Indicator		232
	PrivateCardData <*PrvtCardData*>	[0..1]	Indicator		232
	MandatorySecurityTrailer <*MndtrySctyTrlr*>	[0..1]	Indicator		232

4.3.2.3.6.4 ServiceProviderParameters <SvcPrvdrParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to a service provider.

ServiceProviderParameters <SvcPrvdrParams> contains the following elements (see "ServiceProviderParameters2" on page 207 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		207
	ServiceProviderIdentification <*SvcPrvdrId*>	[1..*]	±		208
	Version <*Vrsn*>	[1..1]	Text		208
	ApplicationIdentification <*ApplId*>	[0..*]	Text		208
	Host <*Hst*>	[0..*]			208
	HostIdentification <*HstId*>	[1..1]	Text		208
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		209
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		209
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		209
	NonFinancialActionSupported <*NonFinActnSpprtd*>	[0..*]	CodeSet		210

4.3.2.3.6.5 MerchantParameters <MrchntParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to the merchant.

MerchantParameters <MrchntParams> contains the following elements (see "MerchantConfigurationParameters6" on page 244 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		245
	MerchantIdentification <*MrchntId*>	[0..1]	Text		245
	Version <*Vrsn*>	[0..1]	Text		245
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		245
	Proxy <*Prxy*>	[0..1]			246
	Type <*Tp*>	[1..1]	CodeSet		246
	Access <*Accs*>	[1..1]	±		246
	OtherParametersLength <*OthrParamsLngth*>	[0..1]	Quantity		246
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		247
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		247
	OtherParameters <*OthrParams*>	[0..1]	Binary		247

4.3.2.3.6.6 TerminalParameters <TermnlParams>

Presence: [0..*]

Definition: Manufacturer configuration parameters of the point of interaction.

TerminalParameters <TermnlParams> contains the following elements (see "PaymentTerminalParameters8" on page 240 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		241
	VendorIdentification <*VndrId*>	[0..1]	Text		241
	Version <*Vrsn*>	[0..1]	Text		242
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		242
	ClockSynchronisation <*ClckSynctn*>	[0..1]			242
	POITimeZone <*POITmZone*>	[1..1]	Text		242
	SynchronisationServer <*SynctnSvr*>	[0..*]	±		242
	Delay <*Dely*>	[0..1]	Time		243
	TimeZoneLine <*TmZoneLine*>	[0..*]	Text		243
	LocalDateTime <*LclDtTm*>	[0..*]			243
	FromDateTime <*FrDtTm*>	[0..1]	DateTime		243
	ToDateTime <*ToDtTm*>	[0..1]	DateTime		244
	UTCOffset <*UTCOffset*>	[1..1]	Quantity		244
	OtherParametersLength <*OthrParamsLngth*>	[0..1]	Quantity		244
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		244
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		244
	OtherParameters <*OthrParams*>	[0..1]	Binary		244

4.3.2.3.6.7 ApplicationParameters <ApplParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to a payment application of the point of interaction.

ApplicationParameters <ApplParams> contains the following elements (see "ApplicationParameters11" on page 232 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		233
	ApplicationIdentification <*ApplId*>	[1..1]	Text		233
	Version <*Vrsn*>	[0..1]	Text		233
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		233
	ParametersLength <*ParamsLngth*>	[0..1]	Quantity		234
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		234
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		234
	Parameters <*Params*>	[0..*]	Binary		234
	EncryptedParameters <*NcrptdParams*>	[0..1]	±		234

4.3.2.3.6.8 HostCommunicationParameters <HstComParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to the communication with an acquirer host or a terminal manager host.

HostCommunicationParameters <HstComParams> contains the following elements (see "HostCommunicationParameter6" on page 195 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		195
	HostIdentification <*HstId*>	[1..1]	Text		196
	Address <*Adr*>	[0..1]	±		196
	Key <*Key*>	[0..*]			196
	KeyIdentification <*KeyId*>	[1..1]	Text		197
	KeyVersion <*KeyVrsn*>	[1..1]	Text		197
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		197
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		197
	Type <*Tp*>	[0..1]	CodeSet		197
	Function <*Fctn*>	[0..*]	CodeSet		198
	NetworkServiceProvider <*NtwkSvcPrvdr*>	[0..1]	±		199
	PhysicalInterface <*PhysIntrfc*>	[0..1]			199
	InterfaceName <*IntrfcNm*>	[1..1]	Text		200
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		200
	UserName <*UsrNm*>	[0..1]	Text		200
	AccessCode <*AccsCd*>	[0..1]	Binary		200
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		201
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		201

4.3.2.3.6.9 SecurityParameters <SctyParams>

Presence: [0..*]

Definition: Point of interaction parameters related to the security of software application and application protocol.

SecurityParameters <SctyParams> contains the following elements (see "SecurityParameters14" on page 238 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		239
	Version <*Vrsn*>	[1..1]	Text		239
	POIChallenge <*POIChllng*>	[0..1]	Binary		239
	TMChallenge <*TMChllng*>	[0..1]	Binary		239
	SecurityElement <*SctyElmt*>	[0..*]	±		239

4.3.2.3.6.10 SaleToPOIParameters <SaleToPOIParams>

Presence: [0..*]

Definition: Parameters dedicated to protocols between a sale system and the POI.

SaleToPOIParameters <SaleToPOIParams> contains the following elements (see "SaleToPOIProtocolParameter2" on page 201 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		201
	MerchantIdentification <*MrchntId*>	[0..1]			202
	CommonName <*CmonNm*>	[1..1]	Text		202
	Address <*Adr*>	[0..1]	Text		202
	CountryCode <*CtryCd*>	[1..1]	CodeSet		202
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		202
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		202
	Version <*Vrsn*>	[1..1]	Text		203
	HostIdentification <*HstId*>	[1..1]	Text		203
	MerchantPOIIdentification <*MrchntPOIId*>	[0..1]	Text		203
	SaleIdentification <*SaleId*>	[0..1]	Text		203
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		203

4.3.2.3.6.11 TerminalPackage <TermnlPackg>

Presence: [0..*]

Definition: Group of software packages to transfer to a group of POIComponent of the POI System.

TerminalPackage <TermnlPackg> contains the following elements (see "TerminalPackageType3" on page 234 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIComponentIdentification <*POICmpntId*>	[0..*]			235
	ItemNumber <*ItmNb*>	[0..1]	Text		235
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		236
	Identification <*Id*>	[0..1]	Text		236
	SerialNumber <*SrlNb*>	[0..1]	Text		236
	Package <*Packg*>	[1..*]			236
	PackageIdentification <*PackgId*>	[0..1]	±		236
	PackageLength <*PackgLngth*>	[0..1]	Quantity		237
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		237
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		237
	PackageBlock <*PackgBlck*>	[0..*]			237
	Identification <*Id*>	[1..1]	Text		238
	Value <*Val*>	[0..1]	Binary		238
	ProtectedValue <*PrtctdVal*>	[0..1]	±		238
	Type <*Tp*>	[0..1]	Text		238

4.3.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

5 DRAFT1catm.005.001.08 MaintenanceDelegationRequestV08

5.1 MessageDefinition Functionality

The MaintenanceDelegationRequest message is sent by a terminal manager to the master terminal manager to request delegation of maintenance functions or maintenance operation on the terminal estate managed by the master terminal manager.

Outline

The MaintenanceDelegationRequestV08 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Information related to the protocol management.

B. MaintenanceDelegationRequest

   Information related to the request of maintenance delegations.

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

5.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <Document> <MntncDlgtnReq>	[1..1]			
	Header <*Hdr*>	[0..1]			72
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		72
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		72
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		72
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		73
	InitiatingParty <*InitgPty*>	[1..1]	±		73
	RecipientParty <*RcptPty*>	[0..1]	±		73
	Traceability <*Tracblt*>	[0..*]	±		74
	MaintenanceDelegationRequest <*MntncDlgtnReq*>	[1..1]			74
	TMIdentification <*TMId*>	[1..1]	±		76
	MasterTMIdentification <*MstrTMId*>	[0..1]	±		76
	RequestedDelegation <*ReqdDlgtn*>	[1..*]			77
	DelegationType <*DlgtnTp*>	[1..1]	CodeSet		79
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		79
	PartialDelegation <*PrtlDlgtn*>	[0..1]	Indicator		80
	POISubset <*POISubset*>	[0..*]	Text		80
	DelegatedAction <*DlgtdActn*>	[0..1]	±		80
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		82
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		82
	Certificate <*Cert*>	[0..*]	Binary		82
	POIIdentificationAssociation <*POIIdAssoctn*>	[0..*]	±		82
	SymmetricKey <*SmmtrcKey*>	[0..*]			82
	KeyIdentification <*KeyId*>	[1..1]	Text		83
	KeyVersion <*KeyVrsn*>	[1..1]	Text		83
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		83
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		83
	Type <*Tp*>	[0..1]	CodeSet		83
	Function <*Fctn*>	[0..*]	CodeSet		84
	ParameterDataSet <*ParamDataSet*>	[0..1]			85

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		85
	SequenceCounter <*SeqCntr*>	[0..1]	Text		86
	LastSequence <*LastSeq*>	[0..1]	Indicator		86
	POIIdentification <*POIId*>	[0..*]	±		86
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		86
	Content <*Cntt*>	[1..1]			87
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		87
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		87
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		88
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		91
	MerchantParameters <*MrchntParams*>	[0..*]	±		91
	TerminalParameters <*TermnlParams*>	[0..*]	±		92
	ApplicationParameters <*ApplParams*>	[0..*]	±		93
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		94
	SecurityParameters <*SctyParams*>	[0..*]	±		95
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		96
	TerminalPackage <*TermnlPackg*>	[0..*]	±		96
	SecurityTrailer <*SctyTrlr*>	[1..1]	±		97

5.3 Constraints

C1 ActiveCurrency

The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217 Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

C2 AnyBIC

Only a valid Business identifier code is allowed. Business identifier codes for financial or non-financial institutions are registered and published by the ISO 9362 Registration Authority in the ISO directory of BICs, and consists of eight (8) or eleven (11) contiguous characters.

C3 Country

The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

C4 IBAN

A valid IBAN consists of all three of the following components: Country Code, check digits and BBAN.

C5 SupplementaryDataRule

This component may not be used without the explicit approval of a SEG and submission to the RA of ISO 20022 compliant structure(s) to be used in the Envelope element.

C6 ValidationByTable

Must be a valid terrestrial language.

5.4 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

5.4.1 Header <Hdr>

Presence: [0..1]

Definition: Information related to the protocol management.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		72
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		72
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		72
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		73
	InitiatingParty <*InitgPty*>	[1..1]	±		73
	RecipientParty <*RcptPty*>	[0..1]	±		73
	Traceability <*Tracblt*>	[0..*]	±		74

5.4.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

5.4.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

5.4.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

5.4.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

5.4.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

5.4.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

5.4.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <Tracblt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

5.4.2 MaintenanceDelegationRequest <MntncDlgtnReq>

Presence: [1..1]

Definition: Information related to the request of maintenance delegations.

MaintenanceDelegationRequest <MntncDlgtnReq> contains the following **MaintenanceDelegationRequest8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TMIdentification <*TMId*>	[1..1]	±		76
	MasterTMIdentification <*MstrTMId*>	[0..1]	±		76
	RequestedDelegation <*ReqdDlgtn*>	[1..*]			77
	DelegationType <*DlgtnTp*>	[1..1]	CodeSet		79
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		79
	PartialDelegation <*PrtlDlgtn*>	[0..1]	Indicator		80
	POISubset <*POISubset*>	[0..*]	Text		80
	DelegatedAction <*DlgtdActn*>	[0..1]	±		80
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		82
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		82
	Certificate <*Cert*>	[0..*]	Binary		82
	POIIdentificationAssociation <*POIIdAssoctn*>	[0..*]	±		82
	SymmetricKey <*SmmtrcKey*>	[0..*]			82
	KeyIdentification <*KeyId*>	[1..1]	Text		83
	KeyVersion <*KeyVrsn*>	[1..1]	Text		83
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		83
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		83
	Type <*Tp*>	[0..1]	CodeSet		83
	Function <*Fctn*>	[0..*]	CodeSet		84
	ParameterDataSet <*ParamDataSet*>	[0..1]			85
	Identification <*Id*>	[1..1]	±		85
	SequenceCounter <*SeqCntr*>	[0..1]	Text		86
	LastSequence <*LastSeq*>	[0..1]	Indicator		86
	POIIdentification <*POIId*>	[0..*]	±		86
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		86
	Content <*Cntt*>	[1..1]			87
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		87
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		87
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		88
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		91

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MerchantParameters <*MrchntParams*>	[0..*]	±		91
	TerminalParameters <*TermnlParams*>	[0..*]	±		92
	ApplicationParameters <*ApplParams*>	[0..*]	±		93
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		94
	SecurityParameters <*SctyParams*>	[0..*]	±		95
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		96
	TerminalPackage <*TermnlPackg*>	[0..*]	±		96

5.4.2.1 TMIdentification <TMId>

Presence: [1..1]

Definition: Terminal manager identification.

TMIdentification <TMId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

5.4.2.2 MasterTMIdentification <MstrTMId>

Presence: [0..1]

Definition: Master terminal manager identification.

MasterTMIdentification <MstrTMId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

5.4.2.3 RequestedDelegation <ReqdDlgtn>

Presence: [1..*]

Definition: Information on the delegation of a maintenance action.

RequestedDelegation <ReqdDlgtn> contains the following **MaintenanceDelegation13** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DelegationType <*DlgtnTp*>	[1..1]	CodeSet		79
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		79
	PartialDelegation <*PrtlDlgtn*>	[0..1]	Indicator		80
	POISubset <*POISubset*>	[0..*]	Text		80
	DelegatedAction <*DlgtdActn*>	[0..1]	±		80
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		82
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		82
	Certificate <*Cert*>	[0..*]	Binary		82
	POIIdentificationAssociation <*POIIdAssoctn*>	[0..*]	±		82
	SymmetricKey <*SmmtrcKey*>	[0..*]			82
	KeyIdentification <*KeyId*>	[1..1]	Text		83
	KeyVersion <*KeyVrsn*>	[1..1]	Text		83
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		83
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		83
	Type <*Tp*>	[0..1]	CodeSet		83
	Function <*Fctn*>	[0..*]	CodeSet		84
	ParameterDataSet <*ParamDataSet*>	[0..1]			85
	Identification <*Id*>	[1..1]	±		85
	SequenceCounter <*SeqCntr*>	[0..1]	Text		86
	LastSequence <*LastSeq*>	[0..1]	Indicator		86
	POIIdentification <*POIId*>	[0..*]	±		86
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		86
	Content <*Cntt*>	[1..1]			87
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		87
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		87
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		88
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		91
	MerchantParameters <*MrchntParams*>	[0..*]	±		91
	TerminalParameters <*TermnlParams*>	[0..*]	±		92
	ApplicationParameters <*ApplParams*>	[0..*]	±		93
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		94

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SecurityParameters <*SctyParams*>	[0..*]	±		95
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		96
	TerminalPackage <*TermnlPackg*>	[0..*]	±		96

5.4.2.3.1 DelegationType <DlgtnTp>

Presence: [1..1]

Definition: Type of delegation action.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

5.4.2.3.2 MaintenanceService <MntncSvc>

Presence: [1..*]

Definition: Maintenance service to be delegated.

Datatype: "DataSetCategory16Code" on page 482

CodeName	Name	Definition
ACQP	AcquirerProtocolParameters	Configuration parameters of the payment acquirer protocol.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
APSB	ApplicationParametersSubsetCreation	Creation of a subset of the configuration parameters of an application.
KDWL	KeyDownload	Download of cryptographic keys with the related information.
KMGT	KeyManagement	Activate, deactivate or revoke loaded cryptographic keys.
RPRT	Reporting	Reporting on activity, status and error of a point of interaction.
SWPK	SoftwareModule	Software module.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).

CodeName	Name	Definition
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
SACP	SaleComponent	Component of the Sale system.
SAPR	SaleToPOIProtocolParameters	Parameters related to the Sale to POI protocol.
LOGF	LogFile	Any repository used for recording log traces.
RPFL	ReportFile	Report file generated by the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
SPRP	ServiceProviderParameters	Service Provider specific parameters for the point of interaction (POI) system.

5.4.2.3.3 PartialDelegation <PrtlDlgtn>

Presence: [0..1]

Definition: Flag to indicate that the delegated maintenance must be performed on a subset of the terminal estate.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

5.4.2.3.4 POISubset <POISubset>

Presence: [0..*]

Definition: Subset of the terminal estate for the delegated actions, for instance for pilot or key deactivation). The subset may be expressed as a list of POI or terminal estate subset identifier.

Datatype: "Max35Text" on page 519

5.4.2.3.5 DelegatedAction <DlgtdActn>

Presence: [0..1]

Definition: Information for the MTM to build or include delegated actions in the management plan of the POI.

DelegatedAction <DlgtdActn> contains the following elements (see "MaintenanceDelegateAction7" on page 338 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PeriodicAction <*PrdcActn*>	[0..1]	Indicator		340
	TMRemoteAccess <*TMRmotAccs*>	[0..1]	±		340
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		340
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		341
	DataSetIdentification <*DataSetId*>	[0..1]	±		341
	ReTry <*ReTry*>	[0..1]	±		341
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		341
	Action <*Actn*>	[0..*]			341
	Type <*Tp*>	[1..1]	CodeSet		342
	RemoteAccess <*RmotAccs*>	[0..1]	±		343
	Key <*Key*>	[0..*]			344
	KeyIdentification <*KeyId*>	[1..1]	Text		344
	KeyVersion <*KeyVrsn*>	[1..1]	Text		344
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		344
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		344
	Type <*Tp*>	[0..1]	CodeSet		344
	Function <*Fctn*>	[0..*]	CodeSet		345
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		346
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		346
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		346
	DataSetIdentification <*DataSetId*>	[0..1]	±		346
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		347
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		348
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		348
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		348
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		348
	Trigger <*Trggr*>	[1..1]	CodeSet		349
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		349
	ReTry <*ReTry*>	[0..1]	±		349
	TimeCondition <*TmCond*>	[0..1]	±		350

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TMChallenge <*TMChllng*>	[0..1]	Binary		350
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		350
	ErrorAction <*ErrActn*>	[0..*]	±		350
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		351
	MessageItem <*MsgItm*>	[0..*]	±		351
	DeviceRequest <*DvcReq*>	[0..1]	±		351

5.4.2.3.6 DelegationScopeIdentification <DlgtnScpId>

Presence: [0..1]

Definition: Identification of the delegation scope assigned by the MTM.

Datatype: "Max35Text" on page 519

5.4.2.3.7 DelegationScopeDefinition <DlgtnScpDef>

Presence: [0..1]

Definition: This element contains all information relevant to the DelegationScopeIdentification. The format of this element is out of scope of this definition.

Datatype: "Max3000Binary" on page 462

5.4.2.3.8 Certificate <Cert>

Presence: [0..*]

Definition: Certificate path of the terminal manager.

Datatype: "Max10KBinary" on page 461

5.4.2.3.9 POIIdentificationAssociation <POIIdAssoctn>

Presence: [0..*]

Definition: Association of the TM identifier and the MTM identifier of a POI.

POIIdentificationAssociation <POIIdAssoctn> contains the following elements (see "MaintenanceIdentificationAssociation1" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MasterTMIdentification <*MstrTMId*>	[1..1]	Text		388
	TMIdentification <*TMId*>	[1..1]	Text		388

5.4.2.3.10 SymmetricKey <SmmtrcKey>

Presence: [0..*]

Definition: Identification of the key to manage or to download.

SymmetricKey <SmmtrcKey> contains the following **KEKIdentifier5** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		83
	KeyVersion <*KeyVrsn*>	[1..1]	Text		83
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		83
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		83
	Type <*Tp*>	[0..1]	CodeSet		83
	Function <*Fctn*>	[0..*]	CodeSet		84

5.4.2.3.10.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 517

5.4.2.3.10.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 517

5.4.2.3.10.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 515

5.4.2.3.10.4 DerivationIdentification <DerivtnId>

Presence: [0..1]

Definition: Identification used for derivation of a unique key from a master key provided for the data protection.

Datatype: "Min5Max16Binary" on page 463

5.4.2.3.10.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 481

CodeName	Name	Definition
AES2	AES128	AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

CodeName	Name	Definition
EDE3	DES112	Data encryption standard key of 112 bits (without the parity bits).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.
AES9	AES192	AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
AES5	AES256	AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

5.4.2.3.10.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 488

CodeName	Name	Definition
ENCR	Encryption	Key may encrypt.
DCPT	Decryption	Key may decrypt.
DENC	DataEncryption	Key may encrypt data.
DDEC	DataDecryption	Key may decrypt data.
TRNI	TranslateInput	Key may encrypt information before translation.
TRNX	TranslateOutput	Key may encrypt information after translation.
MACG	MessageAuthenticationCodeGeneration	Key may generate message authentication codes (MAC).
MACV	MessageAuthenticationCodeVerification	Key may verify message authentication codes (MAC).
SIGG	SignatureGeneration	Key may generate digital signatures.
SUGV	SignatureVerification	Key may verify digital signatures.
PINE	PINEncryption	Key may encrypt personal identification numbers (PIN).
PIND	PINDecryption	Key may decrypt personal identification numbers (PIN).
PINV	PINVerification	Key may verify personal identification numbers (PIN).

CodeName	Name	Definition
KEYG	KeyGeneration	Key may generate keys.
KEYI	KeyImport	Key may import keys.
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

5.4.2.3.11 ParameterDataSet <ParamDataSet>

Presence: [0..1]

Definition: Configuration parameters of the terminal manager to be sent by the MTM.

ParameterDataSet <ParamDataSet> contains the following **AcceptorConfigurationDataSet3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		85
	SequenceCounter <*SeqCntr*>	[0..1]	Text		86
	LastSequence <*LastSeq*>	[0..1]	Indicator		86
	POIIdentification <*POIId*>	[0..*]	±		86
	ConfigurationScope <*CfgtnScp*>	[0..1]	CodeSet		86
	Content <*Cntt*>	[1..1]			87
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		87
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		87
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		88
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		91
	MerchantParameters <*MrchntParams*>	[0..*]	±		91
	TerminalParameters <*TermnlParams*>	[0..*]	±		92
	ApplicationParameters <*ApplParams*>	[0..*]	±		93
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		94
	SecurityParameters <*SctyParams*>	[0..*]	±		95
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		96
	TerminalPackage <*TermnlPackg*>	[0..*]	±		96

5.4.2.3.11.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the data set transferred.

Identification <Id> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

5.4.2.3.11.2 SequenceCounter <SeqCntr>

Presence: [0..1]

Definition: Counter to identify a single data set within the whole transfer.

Datatype: "Max9NumericText" on page 521

5.4.2.3.11.3 LastSequence <LastSeq>

Presence: [0..1]

Definition: Indication of the last sequence in case of split messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

5.4.2.3.11.4 POIIdentification <POIId>

Presence: [0..*]

Definition: Identification of the point of interactions involved by the configuration data set.

POIIdentification <POIId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

5.4.2.3.11.5 ConfigurationScope <CfgtnScp>

Presence: [0..1]

Definition: Scope of the configuration contained in the data set.

Datatype: "PartyType15Code" on page 494

CodeName	Name	Definition
PGRP	POIGroup	Configuration to apply to a subset of the whole POI system.
PSYS	POISystem	Configuration to apply to the whole POI system.
PSNG	SinglePOI	Configuration to apply to a single POI terminal.

5.4.2.3.11.6 Content <Cntt>

Presence: [1..1]

Definition: Content of the acceptor parameters.

Content <Cntt> contains the following **AcceptorConfigurationContent11** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ReplaceConfiguration <*RplcCfgtn*>	[0..1]	Indicator		87
	TMSProtocolParameters <*TMSPrtcolParams*>	[0..*]	±		87
	AcquirerProtocolParameters <*AcqrrPrtcolParams*>	[0..*]	±		88
	ServiceProviderParameters <*SvcPrvdrParams*>	[0..*]	±		91
	MerchantParameters <*MrchntParams*>	[0..*]	±		91
	TerminalParameters <*TermnlParams*>	[0..*]	±		92
	ApplicationParameters <*ApplParams*>	[0..*]	±		93
	HostCommunicationParameters <*HstComParams*>	[0..*]	±		94
	SecurityParameters <*SctyParams*>	[0..*]	±		95
	SaleToPOIParameters <*SaleToPOIParams*>	[0..*]	±		96
	TerminalPackage <*TermnlPackg*>	[0..*]	±		96

5.4.2.3.11.6.1 ReplaceConfiguration <RplcCfgtn>

Presence: [0..1]

Definition: True if the whole configuration related to the terminal manager has to be replaced by the configuration included in the message content.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

5.4.2.3.11.6.2 TMSProtocolParameters <TMSPrtcolParams>

Presence: [0..*]

Definition: Configuration parameters of the TMS protocol between a POI and a terminal manager.

TMSProtocolParameters <TMSPrtcolParams> contains the following elements (see "TMSProtocolParameters6" on page 203 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		204
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		204
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		205
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		205
	Version <*Vrsn*>	[1..1]	Text		206
	ApplicationIdentification <*ApplId*>	[0..*]	Text		206
	HostIdentification <*HstId*>	[1..1]	Text		206
	POIIdentification <*POIId*>	[0..1]	Text		206
	InitiatingPartyIdentification <*InitgPtyId*>	[0..1]	Text		206
	RecipientPartyIdentification <*RcptPtyId*>	[0..1]	Text		206
	FileTransfer <*FileTrf*>	[0..1]	Indicator		206
	MessageItem <*MsgItm*>	[0..*]	±		206
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		207

5.4.2.3.11.6.3 AcquirerProtocolParameters <AcqrrPrtcolParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to an acquirer protocol.

AcquirerProtocolParameters <AcqrrPrtcolParams> contains the following elements (see "AcquirerProtocolParameters15" on page 210 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		213
	AcquirerIdentification <*AcqrrId*>	[1..*]	±		213
	Version <*Vrsn*>	[1..1]	Text		213
	ApplicationIdentification <*ApplId*>	[0..*]	Text		213
	Host <*Hst*>	[0..*]			214
	HostIdentification <*HstId*>	[1..1]	Text		214
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		214
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		215
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		215
	OnLineTransaction <*OnLineTx*>	[0..1]			215
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		216
	BatchTransfer <*BtchTrf*>	[0..1]			216
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		217
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		217
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		218
	ReTry <*ReTry*>	[0..1]	±		218
	TimeCondition <*TmCond*>	[0..1]	±		218
	CompletionExchange <*CmpltnXchg*>	[0..1]			218
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		219
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		219
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		220
	ReTry <*ReTry*>	[0..1]	±		220
	TimeCondition <*TmCond*>	[0..1]	±		220
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		220
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		220
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		221
	OffLineTransaction <*OffLineTx*>	[0..1]			221
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		222
	BatchTransfer <*BtchTrf*>	[0..1]			222
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		223

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		223
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		224
	ReTry <*ReTry*>	[0..1]	±		224
	TimeCondition <*TmCond*>	[0..1]	±		224
	CompletionExchange <*CmpltnXchg*>	[0..1]			224
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		225
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		225
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		226
	ReTry <*ReTry*>	[0..1]	±		226
	TimeCondition <*TmCond*>	[0..1]	±		226
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		226
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		226
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		227
	ReconciliationExchange <*RcncltnXchg*>	[0..1]			227
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		227
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		228
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		228
	ReTry <*ReTry*>	[0..1]	±		228
	TimeCondition <*TmCond*>	[0..1]	±		228
	ReconciliationByAcquirer <*RcncltnByAcqrr*>	[0..1]	Indicator		229
	TotalsPerCurrency <*TtlsPerCcy*>	[0..1]	Indicator		229
	SplitTotals <*SpltTtls*>	[0..1]	Indicator		229
	SplitTotalCriteria <*SpltTtlCrit*>	[0..*]	CodeSet		229
	CompletionAdviceMandated <*CmpltnAdvcMndtd*>	[0..1]	Indicator		230
	AmountQualifierForReservation <*AmtQlfrForRsvatn*>	[0..*]	CodeSet		230
	ReconciliationError <*RcncltnErr*>	[0..1]	Indicator		230
	CardDataVerification <*CardDataVrfctn*>	[0..1]	Indicator		231
	NotifyOffLineCancellation <*NtfyOffLineCxl*>	[0..1]	Indicator		231
	BatchTransferContent <*BtchTrfCntt*>	[0..*]	CodeSet		231
	FileTransferBatch <*FileTrfBtch*>	[0..1]	Indicator		231
	BatchDigitalSignature <*BtchDgtlSgntr*>	[0..1]	Indicator		231

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageItem <*MsgItm*>	[0..*]	±		232
	ProtectCardData <*PrtctCardData*>	[1..1]	Indicator		232
	PrivateCardData <*PrvtCardData*>	[0..1]	Indicator		232
	MandatorySecurityTrailer <*MndtrySctyTrlr*>	[0..1]	Indicator		232

5.4.2.3.11.6.4 ServiceProviderParameters <SvcPrvdrParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to a service provider.

ServiceProviderParameters <SvcPrvdrParams> contains the following elements (see "ServiceProviderParameters2" on page 207 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		207
	ServiceProviderIdentification <*SvcPrvdrId*>	[1..*]	±		208
	Version <*Vrsn*>	[1..1]	Text		208
	ApplicationIdentification <*ApplId*>	[0..*]	Text		208
	Host <*Hst*>	[0..*]			208
	HostIdentification <*HstId*>	[1..1]	Text		208
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		209
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		209
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		209
	NonFinancialActionSupported <*NonFinActnSpprtd*>	[0..*]	CodeSet		210

5.4.2.3.11.6.5 MerchantParameters <MrchntParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to the merchant.

MerchantParameters <MrchntParams> contains the following elements (see "MerchantConfigurationParameters6" on page 244 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		245
	MerchantIdentification <*MrchntId*>	[0..1]	Text		245
	Version <*Vrsn*>	[0..1]	Text		245
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		245
	Proxy <*Prxy*>	[0..1]			246
	Type <*Tp*>	[1..1]	CodeSet		246
	Access <*Accs*>	[1..1]	±		246
	OtherParametersLength <*OthrParamsLngth*>	[0..1]	Quantity		246
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		247
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		247
	OtherParameters <*OthrParams*>	[0..1]	Binary		247

5.4.2.3.11.6.6 TerminalParameters <TermnlParams>

Presence: [0..*]

Definition: Manufacturer configuration parameters of the point of interaction.

TerminalParameters <TermnlParams> contains the following elements (see "PaymentTerminalParameters8" on page 240 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		241
	VendorIdentification <*VndrId*>	[0..1]	Text		241
	Version <*Vrsn*>	[0..1]	Text		242
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		242
	ClockSynchronisation <*ClckSynctn*>	[0..1]			242
	POITimeZone <*POITmZone*>	[1..1]	Text		242
	SynchronisationServer <*SynctnSvr*>	[0..*]	±		242
	Delay <*Dely*>	[0..1]	Time		243
	TimeZoneLine <*TmZoneLine*>	[0..*]	Text		243
	LocalDateTime <*LclDtTm*>	[0..*]			243
	FromDateTime <*FrDtTm*>	[0..1]	DateTime		243
	ToDateTime <*ToDtTm*>	[0..1]	DateTime		244
	UTCOffset <*UTCOffset*>	[1..1]	Quantity		244
	OtherParametersLength <*OthrParamsLngth*>	[0..1]	Quantity		244
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		244
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		244
	OtherParameters <*OthrParams*>	[0..1]	Binary		244

5.4.2.3.11.6.7 ApplicationParameters <ApplParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to a payment application of the point of interaction.

ApplicationParameters <ApplParams> contains the following elements (see "ApplicationParameters11" on page 232 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		233
	ApplicationIdentification <*ApplId*>	[1..1]	Text		233
	Version <*Vrsn*>	[0..1]	Text		233
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		233
	ParametersLength <*ParamsLngth*>	[0..1]	Quantity		234
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		234
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		234
	Parameters <*Params*>	[0..*]	Binary		234
	EncryptedParameters <*NcrptdParams*>	[0..1]	±		234

5.4.2.3.11.6.8 HostCommunicationParameters <HstComParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to the communication with an acquirer host or a terminal manager host.

HostCommunicationParameters <HstComParams> contains the following elements (see "HostCommunicationParameter6" on page 195 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		195
	HostIdentification <*HstId*>	[1..1]	Text		196
	Address <*Adr*>	[0..1]	±		196
	Key <*Key*>	[0..*]			196
	KeyIdentification <*KeyId*>	[1..1]	Text		197
	KeyVersion <*KeyVrsn*>	[1..1]	Text		197
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		197
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		197
	Type <*Tp*>	[0..1]	CodeSet		197
	Function <*Fctn*>	[0..*]	CodeSet		198
	NetworkServiceProvider <*NtwkSvcPrvdr*>	[0..1]	±		199
	PhysicalInterface <*PhysIntrfc*>	[0..1]			199
	InterfaceName <*IntrfcNm*>	[1..1]	Text		200
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		200
	UserName <*UsrNm*>	[0..1]	Text		200
	AccessCode <*AccsCd*>	[0..1]	Binary		200
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		201
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		201

5.4.2.3.11.6.9 SecurityParameters <SctyParams>

Presence: [0..*]

Definition: Point of interaction parameters related to the security of software application and application protocol.

SecurityParameters <SctyParams> contains the following elements (see "SecurityParameters14" on page 238 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		239
	Version <*Vrsn*>	[1..1]	Text		239
	POIChallenge <*POIChllng*>	[0..1]	Binary		239
	TMChallenge <*TMChllng*>	[0..1]	Binary		239
	SecurityElement <*SctyElmt*>	[0..*]	±		239

5.4.2.3.11.6.10 SaleToPOIParameters <SaleToPOIParams>

Presence: [0..*]

Definition: Parameters dedicated to protocols between a sale system and the POI.

SaleToPOIParameters <SaleToPOIParams> contains the following elements (see "SaleToPOIProtocolParameter2" on page 201 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		201
	MerchantIdentification <*MrchntId*>	[0..1]			202
	CommonName <*CmonNm*>	[1..1]	Text		202
	Address <*Adr*>	[0..1]	Text		202
	CountryCode <*CtryCd*>	[1..1]	CodeSet		202
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		202
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		202
	Version <*Vrsn*>	[1..1]	Text		203
	HostIdentification <*HstId*>	[1..1]	Text		203
	MerchantPOIIdentification <*MrchntPOIId*>	[0..1]	Text		203
	SaleIdentification <*SaleId*>	[0..1]	Text		203
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		203

5.4.2.3.11.6.11 TerminalPackage <TermnlPackg>

Presence: [0..*]

Definition: Group of software packages to transfer to a group of POIComponent of the POI System.

TerminalPackage <TermnlPackg> contains the following elements (see "TerminalPackageType3" on page 234 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIComponentIdentification <*POICmpntId*>	[0..*]			235
	ItemNumber <*ItmNb*>	[0..1]	Text		235
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		236
	Identification <*Id*>	[0..1]	Text		236
	SerialNumber <*SrlNb*>	[0..1]	Text		236
	Package <*Packg*>	[1..*]			236
	PackageIdentification <*PackgId*>	[0..1]	±		236
	PackageLength <*PackgLngth*>	[0..1]	Quantity		237
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		237
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		237
	PackageBlock <*PackgBlck*>	[0..*]			237
	Identification <*Id*>	[1..1]	Text		238
	Value <*Val*>	[0..1]	Binary		238
	ProtectedValue <*PrtctdVal*>	[0..1]	±		238
	Type <*Tp*>	[0..1]	Text		238

5.4.3 SecurityTrailer <SctyTrlr>

Presence: [1..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

6 DRAFT1catm.006.001.06 MaintenanceDelegationResponseV06

6.1 MessageDefinition Functionality

The MaintenanceDelegationResponse message is sent by the master terminal manager to a terminal manager to provide the outcome of a maintenance delegation request.

Outline

The MaintenanceDelegationResponseV06 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Maintenance delegation response message management information.

B. MaintenanceDelegationResponse

   Information related to the request of maintenance delegations.

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

6.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <Document> <MntncDlgtnRspn>	[1..1]			
	Header <*Hdr*>	[1..1]			99
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		100
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		100
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		100
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		100
	InitiatingParty <*InitgPty*>	[1..1]	±		100
	RecipientParty <*RcptPty*>	[0..1]	±		101
	Traceability <*Tracblt*>	[0..*]	±		101
	MaintenanceDelegationResponse <*MntncDlgtnRspn*>	[1..1]			102
	TMIdentification <*TMId*>	[1..1]	±		102
	MasterTMIdentification <*MstrTMId*>	[0..1]	±		103
	DelegationResponse <*DlgtnRspn*>	[1..*]			103
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		104
	Response <*Rspn*>	[1..1]	CodeSet		105
	ResponseReason <*RspnRsn*>	[0..1]	Text		105
	DelegationType <*DlgtnTp*>	[1..1]	CodeSet		105
	POISubset <*POISubset*>	[0..*]	Text		105
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		106
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		106
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		106
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		106
	POIIdentificationAssociation <*POIIdAssoctn*>	[0..*]	±		106
	SecurityTrailer <*SctyTrlr*>	[0..1]	±		107

6.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

6.3.1 Header <Hdr>

Presence: [1..1]

Definition: Maintenance delegation response message management information.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		100
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		100
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		100
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		100
	InitiatingParty <*InitgPty*>	[1..1]	±		100
	RecipientParty <*RcptPty*>	[0..1]	±		101
	Traceability <*Tracblt*>	[0..*]	±		101

6.3.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

6.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

6.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

6.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

6.3.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

6.3.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

6.3.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <TracbIt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

6.3.2 MaintenanceDelegationResponse <MntncDlgtnRspn>

Presence: [1..1]

Definition: Information related to the request of maintenance delegations.

MaintenanceDelegationResponse <MntncDlgtnRspn> contains the following **MaintenanceDelegationResponse6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TMIdentification <*TMId*>	[1..1]	±		102
	MasterTMIdentification <*MstrTMId*>	[0..1]	±		103
	DelegationResponse <*DlgtnRspn*>	[1..*]			103
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		104
	Response <*Rspn*>	[1..1]	CodeSet		105
	ResponseReason <*RspnRsn*>	[0..1]	Text		105
	DelegationType <*DlgtnTp*>	[1..1]	CodeSet		105
	POISubset <*POISubset*>	[0..*]	Text		105
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		106
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		106
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		106
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		106
	POIIdentificationAssociation <*POIIdAssoctn*>	[0..*]	±		106

6.3.2.1 TMIdentification <TMId>

Presence: [1..1]

Definition: Terminal manager identification.

TMIdentification <TMId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

6.3.2.2 MasterTMIdentification <MstrTMId>

Presence: [0..1]

Definition: Master terminal manager identification.

MasterTMIdentification <MstrTMId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

6.3.2.3 DelegationResponse <DlgtnRspn>

Presence: [1..*]

Definition: Information on the delegation of a maintenance action.

DelegationResponse <DlgtnRspn> contains the following **MaintenanceDelegation14** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		104
	Response <*Rspn*>	[1..1]	CodeSet		105
	ResponseReason <*RspnRsn*>	[0..1]	Text		105
	DelegationType <*DlgtnTp*>	[1..1]	CodeSet		105
	POISubset <*POISubset*>	[0..*]	Text		105
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		106
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		106
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		106
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		106
	POIIdentificationAssociation <*POIIdAssoctn*>	[0..*]	±		106

6.3.2.3.1 MaintenanceService <MntncSvc>

Presence: [1..*]

Definition: Maintenance service to be delegated.

Datatype: "DataSetCategory16Code" on page 482

CodeName	Name	Definition
ACQP	AcquirerProtocolParameters	Configuration parameters of the payment acquirer protocol.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
APSB	ApplicationParametersSubsetCreation	Creation of a subset of the configuration parameters of an application.
KDWL	KeyDownload	Download of cryptographic keys with the related information.
KMGT	KeyManagement	Activate, deactivate or revoke loaded cryptographic keys.
RPRT	Reporting	Reporting on activity, status and error of a point of interaction.
SWPK	SoftwareModule	Software module.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
CRTF	CertificateParameters	Certificate provided by a terminal manager.

CodeName	Name	Definition
SACP	SaleComponent	Component of the Sale system.
SAPR	SaleToPOIProtocolParameters	Parameters related to the Sale to POI protocol.
LOGF	LogFile	Any repository used for recording log traces.
RPFL	ReportFile	Report file generated by the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
SPRP	ServiceProviderParameters	Service Provider specific parameters for the point of interaction (POI) system.

6.3.2.3.2 Response <Rspn>

Presence: [1..1]

Definition: Response of the MTM to the delegation of the maintenance service.

Datatype: "Response2Code" on page 501

CodeName	Name	Definition
APPR	Approved	Service has been successfuly provided.
DECL	Declined	Service is declined.

6.3.2.3.3 ResponseReason <RspnRsn>

Presence: [0..1]

Definition: Reason of the response of the MTM.

Datatype: "Max35Text" on page 519

6.3.2.3.4 DelegationType <DlgtnTp>

Presence: [1..1]

Definition: Type of delegation action.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

6.3.2.3.5 POISubset <POISubset>

Presence: [0..*]

Definition: Subset of the terminal estate for the delegated actions, for instance for pilot or key deactivation). The subset may be expressed as a list of POI or terminal estate subset identifier.

Datatype: "Max35Text" on page 519

6.3.2.3.6 DelegationScopeIdentification <DlgtnScpId>

Presence: [0..1]

Definition: Identification of the parameters subset assigned by the MTM.

Datatype: "Max35Text" on page 519

6.3.2.3.7 DelegationScopeDefinition <DlgtnScpDef>

Presence: [0..1]

Definition: This element contains all information relevant to the DelegationScopeIdentification. The format of this element is out of scope of this definition.

Datatype: "Max3000Binary" on page 462

6.3.2.3.8 DelegationProof <DlgtnProof>

Presence: [0..1]

Definition: This element contains the necessary information to secure the management of the Delegation. The format of this element is out of scope of this definition.

Datatype: "Max5000Binary" on page 462

6.3.2.3.9 ProtectedDelegationProof <PrtctdDlgtnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtnProof> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

6.3.2.3.10 POIIdentificationAssociation <POIIdAssoctn>

Presence: [0..*]

Definition: Association of the TM identifier and the MTM identifier of a POI.

POIIdentificationAssociation <POIIdAssoctn> contains the following elements (see "MaintenanceIdentificationAssociation1" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MasterTMIdentification <*MstrTMId*>	[1..1]	Text		388
	TMIdentification <*TMId*>	[1..1]	Text		388

6.3.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

7 DRAFT1catm.007.001.05 CertificateManagementRequestV05

7.1 MessageDefinition Functionality

The CertificateManagementRequest message is sent by a POI terminal or any intermediary entity either to a terminal manager acting as a certificate authority for managing X.509 certificate of a public key owned by the initiating party, or for requesting the inclusion or the removal of the POI to a white list of the terminal manager.

Outline

The CertificateManagementRequestV05 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Information related to the protocol management.

B. CertificateManagementRequest

   Information related to the request of certificate management.

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

7.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <Document> <CertMgmtReq>	[1..1]			
	Header <*Hdr*>	[1..1]			110
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		110
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		111
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		111
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		111
	InitiatingParty <*InitgPty*>	[1..1]	±		111
	RecipientParty <*RcptPty*>	[0..1]	±		111
	Traceability <*Tracblt*>	[0..*]	±		112
	CertificateManagementRequest <*CertMgmtReq*>	[1..1]			112
	POIIdentification <*POIId*>	[1..1]	±		113
	TMIdentification <*TMId*>	[0..1]	±		114
	CertificateService <*CertSvc*>	[1..1]	CodeSet		114
	SecurityDomain <*SctyDomn*>	[0..1]	Text		115
	BinaryCertificationRequest <*BinryCertfctnReq*>	[0..1]	Text		115
	CertificationRequest <*CertfctnReq*>	[0..1]			115
	CertificateRequestInformation <*CertReqInf*>	[1..1]			116
	Version <*Vrsn*>	[0..1]	Quantity		116
	SubjectName <*SbjtNm*>	[0..1]			116
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			116
	AttributeType <*AttrTp*>	[1..1]	CodeSet		117
	AttributeValue <*AttrVal*>	[1..1]	Text		117
	SubjectPublicKeyInformation <*SbjtPblcKeyInf*>	[1..1]			117
	Algorithm <*Algo*>	[0..1]	CodeSet		118
	PublicKeyValue <*PblcKeyVal*>	[1..1]			118
	Modulus <*Mdlus*>	[1..1]	Binary		118
	Exponent <*Expnt*>	[1..1]	Binary		118
	Attribute <*Attr*>	[1..*]			118
	AttributeType <*AttrTp*>	[1..1]	CodeSet		119
	AttributeValue <*AttrVal*>	[1..1]	Text		119

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[0..1]	Text		119
	KeyVersion <*KeyVrsn*>	[0..1]	Text		119
	ClientCertificate <*ClntCert*>	[0..1]	Binary		119
	WhiteListIdentification <*WhtListId*>	[0..1]			119
	ManufacturerIdentifier <*ManfctrIdr*>	[1..1]	Text		120
	Model <*Mdl*>	[1..1]	Text		120
	SerialNumber <*SrlNb*>	[1..1]	Text		120
	SecurityTrailer <*SctyTrlr*>	[0..1]	±		120

7.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

7.3.1 Header <Hdr>

Presence: [1..1]

Definition: Information related to the protocol management.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		110
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		111
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		111
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		111
	InitiatingParty <*InitgPty*>	[1..1]	±		111
	RecipientParty <*RcptPty*>	[0..1]	±		111
	Traceability <*Tracblt*>	[0..*]	±		112

7.3.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

7.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

7.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

7.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

7.3.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

7.3.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

7.3.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <Tracblt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

7.3.2 CertificateManagementRequest <CertMgmtReq>

Presence: [1..1]

Definition: Information related to the request of certificate management.

CertificateManagementRequest <CertMgmtReq> contains the following **CertificateManagementRequest2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIIdentification <*POIId*>	[1..1]	±		113
	TMIdentification <*TMId*>	[0..1]	±		114
	CertificateService <*CertSvc*>	[1..1]	CodeSet		114
	SecurityDomain <*SctyDomn*>	[0..1]	Text		115
	BinaryCertificationRequest <*BinryCertfctnReq*>	[0..1]	Text		115
	CertificationRequest <*CertfctnReq*>	[0..1]			115
	CertificateRequestInformation <*CertReqInf*>	[1..1]			116
	Version <*Vrsn*>	[0..1]	Quantity		116
	SubjectName <*SbjtNm*>	[0..1]			116
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			116
	AttributeType <*AttrTp*>	[1..1]	CodeSet		117
	AttributeValue <*AttrVal*>	[1..1]	Text		117
	SubjectPublicKeyInformation <*SbjtPblcKeyInf*>	[1..1]			117
	Algorithm <*Algo*>	[0..1]	CodeSet		118
	PublicKeyValue <*PblcKeyVal*>	[1..1]			118
	Modulus <*Mdlus*>	[1..1]	Binary		118
	Exponent <*Expnt*>	[1..1]	Binary		118
	Attribute <*Attr*>	[1..*]			118
	AttributeType <*AttrTp*>	[1..1]	CodeSet		119
	AttributeValue <*AttrVal*>	[1..1]	Text		119
	KeyIdentification <*KeyId*>	[0..1]	Text		119
	KeyVersion <*KeyVrsn*>	[0..1]	Text		119
	ClientCertificate <*ClntCert*>	[0..1]	Binary		119
	WhiteListIdentification <*WhtListId*>	[0..1]			119
	ManufacturerIdentifier <*ManfctrIdr*>	[1..1]	Text		120
	Model <*Mdl*>	[1..1]	Text		120
	SerialNumber <*SrlNb*>	[1..1]	Text		120

7.3.2.1 POIIdentification <POIId>

Presence: [1..1]

Definition: Identification of the terminal or system using the certificate management service.

POIIdentification <POIId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

7.3.2.2 TMIdentification <TMId>

Presence: [0..1]

Definition: Identification of the TM or the MTM providing the Certificate Authority service.

TMIdentification <TMId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

7.3.2.3 CertificateService <CertSvc>

Presence: [1..1]

Definition: Requested certificate management service.

Datatype: "CardPaymentServiceType10Code" on page 479

CodeName	Name	Definition
CRTC	CreateCertificate	Creation of an X.509 certificate with the public key and the information of the owner of the asymmetric key provided by the requestor.
CRTR	RenewCerificate	Renewal of an X.509 certificate, protected by the certificate to renew.
CRTK	RevokeCertificate	Revocation of an active X.509 certificate.
WLSR	RemoveWhiteList	Remove a POI from the white list of the terminal manager.
WLSA	AddWhiteList	Add a POI in the white list of the terminal manager.

7.3.2.4 SecurityDomain <SctyDomn>

Presence: [0..1]

Definition: Identification of the client and server public key infrastructures containing the certificate. In addition, it may identify specific requirements of the customer.

Datatype: "Max70Text" on page 520

7.3.2.5 BinaryCertificationRequest <BinryCertfctnReq>

Presence: [0..1]

Definition: PKCS#10 (Public Key Certificate Standard 10) certification request coded in base64 ASN.1/DER (Abstract Syntax Notation 1, Distinguished Encoding Rules) or PEM (Privacy Enhanced Message) format.

Datatype: "Max20000Text" on page 517

7.3.2.6 CertificationRequest <CertfctnReq>

Presence: [0..1]

Definition: Certification request PKCS#10 (Public Key Certificate Standard 10) for creation or renewal of an X.509 certificate.

CertificationRequest <CertfctnReq> contains the following **CertificationRequest1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CertificateRequestInformation <*CertReqInf*>	[1..1]			116
	Version <*Vrsn*>	[0..1]	Quantity		116
	SubjectName <*SbjtNm*>	[0..1]			116
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			116
	AttributeType <*AttrTp*>	[1..1]	CodeSet		117
	AttributeValue <*AttrVal*>	[1..1]	Text		117
	SubjectPublicKeyInformation <*SbjtPblcKeyInf*>	[1..1]			117
	Algorithm <*Algo*>	[0..1]	CodeSet		118
	PublicKeyValue <*PblcKeyVal*>	[1..1]			118
	Modulus <*Mdlus*>	[1..1]	Binary		118
	Exponent <*Expnt*>	[1..1]	Binary		118
	Attribute <*Attr*>	[1..*]			118
	AttributeType <*AttrTp*>	[1..1]	CodeSet		119
	AttributeValue <*AttrVal*>	[1..1]	Text		119
	KeyIdentification <*KeyId*>	[0..1]	Text		119
	KeyVersion <*KeyVrsn*>	[0..1]	Text		119

7.3.2.6.1 CertificateRequestInformation <CertReqInf>

Presence: [1..1]

Definition: Information of the certificate to create.

CertificateRequestInformation <CertReqInf> contains the following **CertificationRequest2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		116
	SubjectName <*SbjtNm*>	[0..1]			116
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			116
	AttributeType <*AttrTp*>	[1..1]	CodeSet		117
	AttributeValue <*AttrVal*>	[1..1]	Text		117
	SubjectPublicKeyInformation <*SbjtPblcKeyInf*>	[1..1]			117
	Algorithm <*Algo*>	[0..1]	CodeSet		118
	PublicKeyValue <*PblcKeyVal*>	[1..1]			118
	Modulus <*Mdlus*>	[1..1]	Binary		118
	Exponent <*Expnt*>	[1..1]	Binary		118
	Attribute <*Attr*>	[1..*]			118
	AttributeType <*AttrTp*>	[1..1]	CodeSet		119
	AttributeValue <*AttrVal*>	[1..1]	Text		119

7.3.2.6.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the certificate request information data structure.

Datatype: "Number" on page 515

7.3.2.6.1.2 SubjectName <SbjtNm>

Presence: [0..1]

Definition: Distinguished name of the certificate subject, the entity whose public key is to be certified.

SubjectName <SbjtNm> contains the following **CertificateIssuer1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			116
	AttributeType <*AttrTp*>	[1..1]	CodeSet		117
	AttributeValue <*AttrVal*>	[1..1]	Text		117

7.3.2.6.1.2.1 RelativeDistinguishedName <RltvDstngshdNm>

Presence: [1..*]

Definition: Relative distinguished name inside a X.509 certificate.

RelativeDistinguishedName <RltvDstngshdNm> contains the following **RelativeDistinguishedName1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AttributeType <*AttrTp*>	[1..1]	CodeSet		117
	AttributeValue <*AttrVal*>	[1..1]	Text		117

7.3.2.6.1.2.1.1 AttributeType <AttrTp>

Presence: [1..1]

Definition: Type of attribute of a distinguished name (see X.500).

Datatype: "AttributeType1Code" on page 472

CodeName	Name	Definition
CNAT	CommonName	Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).
LATT	Locality	Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).
OATT	OrganisationName	Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).
OUAT	OrganisationUnitName	Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).
CATT	CountryName	Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).

7.3.2.6.1.2.1.2 AttributeValue <AttrVal>

Presence: [1..1]

Definition: Value of the attribute of a distinguished name (see X.500).

Datatype: "Max140Text" on page 517

7.3.2.6.1.3 SubjectPublicKeyInformation <SbjtPblcKeyInf>

Presence: [1..1]

Definition: Information about the public key being certified.

SubjectPublicKeyInformation <SbjtPblcKeyInf> contains the following **PublicRSAKey2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[0..1]	CodeSet		118
	PublicKeyValue <*PblcKeyVal*>	[1..1]			118
	Modulus <*Mdlus*>	[1..1]	Binary		118
	Exponent <*Expnt*>	[1..1]	Binary		118

7.3.2.6.1.3.1 Algorithm <Algo>

Presence: [0..1]

Definition: Asymmetric cryptographic algorithm.

Datatype: "Algorithm7Code" on page 471

CodeName	Name	Definition
ERSA	RSAEncryption	RSA encryption algorithm - (ASN.1 Object Identifier: rsaEncryption).
RSAO	RSAES-OAEP	RSA encryption scheme based on Optimal Asymmetric Encryption scheme (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-RSAES-OAEP).

7.3.2.6.1.3.2 PublicKeyValue <PblcKeyVal>

Presence: [1..1]

Definition: Public key value.

PublicKeyValue <PblcKeyVal> contains the following **PublicRSAKey1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Modulus <*Mdlus*>	[1..1]	Binary		118
	Exponent <*Expnt*>	[1..1]	Binary		118

7.3.2.6.1.3.2.1 Modulus <Mdlus>

Presence: [1..1]

Definition: Modulus of the RSA key.

Datatype: "Max5000Binary" on page 462

7.3.2.6.1.3.2.2 Exponent <Expnt>

Presence: [1..1]

Definition: Public exponent of the RSA key.

Datatype: "Max5000Binary" on page 462

7.3.2.6.1.4 Attribute <Attr>

Presence: [1..*]

Definition: Attribute of the certificate service to be put in the certificate extensions, or to be used for the request.

Attribute <Attr> contains the following **RelativeDistinguishedName2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AttributeType <*AttrTp*>	[1..1]	CodeSet		119
	AttributeValue <*AttrVal*>	[1..1]	Text		119

7.3.2.6.1.4.1 AttributeType <AttrTp>

Presence: [1..1]

Definition: Type of attribute of a distinguished name (see X.500).

Datatype: "AttributeType2Code" on page 472

CodeName	Name	Definition
EMAL	EmailAddress	Email address of the certificate subject.
CHLG	ChallengePassword	Password by which an entity may request certificate revocation.

7.3.2.6.1.4.2 AttributeValue <AttrVal>

Presence: [1..1]

Definition: Value of the attribute of a distinguished name (see X.500).

Datatype: "Max140Text" on page 517

7.3.2.6.2 KeyIdentification <KeyId>

Presence: [0..1]

Definition: Identification of the key.

Datatype: "Max140Text" on page 517

7.3.2.6.3 KeyVersion <KeyVrsn>

Presence: [0..1]

Definition: Version of the key.

Datatype: "Max140Text" on page 517

7.3.2.7 ClientCertificate <ClntCert>

Presence: [0..1]

Definition: Created certificate. The certificate is ASN.1/DER encoded, for renewal or revocation of certificate.

Datatype: "Max10KBinary" on page 461

7.3.2.8 WhiteListIdentification <WhtListId>

Presence: [0..1]

Definition: Identification of the white list element, for white list addition or removal.

WhiteListIdentification <WhtListId> contains the following **PointOfInteraction6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ManufacturerIdentifier <*ManfctrIdr*>	[1..1]	Text		120
	Model <*Mdl*>	[1..1]	Text		120
	SerialNumber <*SrlNb*>	[1..1]	Text		120

7.3.2.8.1 ManufacturerIdentifier <ManfctrIdr>

Presence: [1..1]

Definition: Identifier of the terminal manufacturer.

Datatype: "Max35Text" on page 519

7.3.2.8.2 Model <Mdl>

Presence: [1..1]

Definition: Identifier of the terminal model.

Datatype: "Max35Text" on page 519

7.3.2.8.3 SerialNumber <SrlNb>

Presence: [1..1]

Definition: Serial number of the terminal manufacturer.

Datatype: "Max35Text" on page 519

7.3.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

8 DRAFT1catm.008.001.05 CertificateManagementResponseV05

8.1 MessageDefinition Functionality

The CertificateManagementResponse is sent by a terminal manager in response to a CertificateManagementRequest to provide the outcome of the requested service.

Outline

The CertificateManagementResponseV05 MessageDefinition is composed of 3 MessageBuildingBlocks:

A. Header

   Information related to the protocol management.

B. CertificateManagementResponse

   Information related to the result of the certificate management request.

C. SecurityTrailer

   Trailer of the message containing a MAC or a digital signature.

8.2 Structure

Or	MessageElement/BuildingBlock<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Message root <*Document*> <*CertMgmtRspn*>	[1..1]			
	Header <*Hdr*>	[1..1]			122
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		123
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		123
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		123
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		123
	InitiatingParty <*InitgPty*>	[1..1]	±		123
	RecipientParty <*RcptPty*>	[0..1]	±		124
	Traceability <*Tracblt*>	[0..*]	±		124
	CertificateManagementResponse <*CertMgmtRspn*>	[1..1]			125
	POIIdentification <*POIId*>	[1..1]	±		125
	TMIdentification <*TMId*>	[0..1]	±		126
	CertificateService <*CertSvc*>	[1..1]	CodeSet		126
	Result <*Rslt*>	[1..1]			127
	Response <*Rspn*>	[1..1]	CodeSet		127
	ResponseDetail <*RspnDtl*>	[0..1]	CodeSet		127
	AdditionalResponse <*AddtlRspn*>	[0..1]	Text		127
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		127
	ClientCertificate <*ClntCert*>	[0..1]	Binary		127
	ClientCertificatePath <*ClntCertPth*>	[0..*]	Binary		128
	ServerCertificatePath <*SvrCertPth*>	[0..*]	Binary		128
	SecurityTrailer <*SctyTrlr*>	[0..1]	±		128

8.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

8.3.1 Header <Hdr>

Presence: [1..1]

Definition: Information related to the protocol management.

Header <Hdr> contains the following **TMSHeader1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <*DwnldTrf*>	[1..1]	Indicator		123
	FormatVersion <*FrmtVrsn*>	[1..1]	Text		123
	ExchangeIdentification <*XchgId*>	[1..1]	Quantity		123
	CreationDateTime <*CreDtTm*>	[1..1]	DateTime		123
	InitiatingParty <*InitgPty*>	[1..1]	±		123
	RecipientParty <*RcptPty*>	[0..1]	±		124
	Traceability <*Tracblt*>	[0..*]	±		124

8.3.1.1 DownloadTransfer <DwnldTrf>

Presence: [1..1]

Definition: Indicates if the file transfer is a download or an upload.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

8.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: "Max6Text" on page 520

8.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 515

8.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

Definition: Date and time at which the file or message was created.

Datatype: "ISODateTime" on page 513

8.3.1.5 InitiatingParty <InitgPty>

Presence: [1..1]

Definition: Unique identification of the partner that has initiated the exchange.

InitiatingParty <InitgPty> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

8.3.1.6 RecipientParty <RcptPty>

Presence: [0..1]

Definition: Unique identification of the partner that is the recipient of the exchange.

RecipientParty <RcptPty> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

8.3.1.7 Traceability <Tracblt>

Presence: [0..*]

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Traceability <TracbIt> contains the following elements (see "Traceability8" on page 388 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

8.3.2 CertificateManagementResponse <CertMgmtRspn>

Presence: [1..1]

Definition: Information related to the result of the certificate management request.

CertificateManagementResponse <CertMgmtRspn> contains the following **CertificateManagementResponse2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIIdentification <*POIId*>	[1..1]	±		125
	TMIdentification <*TMId*>	[0..1]	±		126
	CertificateService <*CertSvc*>	[1..1]	CodeSet		126
	Result <*Rslt*>	[1..1]			127
	Response <*Rspn*>	[1..1]	CodeSet		127
	ResponseDetail <*RspnDtl*>	[0..1]	CodeSet		127
	AdditionalResponse <*AddtlRspn*>	[0..1]	Text		127
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		127
	ClientCertificate <*ClntCert*>	[0..1]	Binary		127
	ClientCertificatePath <*ClntCertPth*>	[0..*]	Binary		128
	ServerCertificatePath <*SvrCertPth*>	[0..*]	Binary		128

8.3.2.1 POIIdentification <POIId>

Presence: [1..1]

Definition: Identification of the terminal or system using the certificate management service.

POIIdentification <POIId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

8.3.2.2 TMIdentification <TMId>

Presence: [0..1]

Definition: Identification of the TM or the MTM providing the Certificate Authority service.

TMIdentification <TMId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

8.3.2.3 CertificateService <CertSvc>

Presence: [1..1]

Definition: Requested certificate management service.

Datatype: "CardPaymentServiceType10Code" on page 479

CodeName	Name	Definition
CRTC	CreateCertificate	Creation of an X.509 certificate with the public key and the information of the owner of the asymmetric key provided by the requestor.
CRTR	RenewCerificate	Renewal of an X.509 certificate, protected by the certificate to renew.
CRTK	RevokeCertificate	Revocation of an active X.509 certificate.
WLSR	RemoveWhiteList	Remove a POI from the white list of the terminal manager.
WLSA	AddWhiteList	Add a POI in the white list of the terminal manager.

8.3.2.4 Result <Rslt>

Presence: [1..1]

Definition: Outcome of the certificate service processing.

Result <Rslt> contains the following **ResponseType6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Response <*Rspn*>	[1..1]	CodeSet		127
	ResponseDetail <*RspnDtl*>	[0..1]	CodeSet		127
	AdditionalResponse <*AddtlRspn*>	[0..1]	Text		127

8.3.2.4.1 Response <Rspn>

Presence: [1..1]

Definition: Response of the terminal manager.

Datatype: "Response2Code" on page 501

CodeName	Name	Definition
APPR	Approved	Service has been successfuly provided.
DECL	Declined	Service is declined.

8.3.2.4.2 ResponseDetail <RspnDtl>

Presence: [0..1]

Definition: Detail of the response.

Datatype: "ResultDetail3Code" on page 502

CodeName	Name	Definition
CRTU	UnknownCertificate	The certificate is unknown.
SVSU	UnsupportedService	Requested service not supported.

8.3.2.4.3 AdditionalResponse <AddtlRspn>

Presence: [0..1]

Definition: Additional information on the response for further examination.

Datatype: "Max140Text" on page 517

8.3.2.5 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the security profile, for creation, renewal or revocation of certificate.

Datatype: "Max35Text" on page 519

8.3.2.6 ClientCertificate <ClntCert>

Presence: [0..1]

Definition: Created or renewed certificate. The certificate is ASN.1/DER encoded.

Datatype: "Max3000Binary" on page 462

8.3.2.7 ClientCertificatePath <ClntCertPth>

Presence: [0..*]

Definition: Certificate of the client certificate path, from the CA (Certificate Authority) certificate, to the root certificate, for renewal or revocation of certificate.

Datatype: "Max10KBinary" on page 461

8.3.2.8 ServerCertificatePath <SvrCertPth>

Presence: [0..*]

Definition: Certificate of the server certificate path, from the CA (Certificate Authority) certificate, to the root certificate, for renewal or revocation of certificate.

Datatype: "Max10KBinary" on page 461

8.3.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

Definition: Trailer of the message containing a MAC or a digital signature.

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

9 Message Items Types

9.1 MessageComponents

9.1.1 Acquirer

9.1.1.1 Acquirer10

Definition: Acquirer involved in the card payment.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]	±		129
	ParametersVersion <*ParamsVrsn*>	[0..1]	Text		129

9.1.1.1.1 Identification <Id>

Presence: [0..1]

Definition: Identification of the acquirer (for example the bank identification number BIN).

Identification <Id> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

9.1.1.1.2 ParametersVersion <ParamsVrsn>

Presence: [0..1]

Definition: Version of the payment acquirer parameters of the POI.

Datatype: "Max256Text" on page 518

9.1.2 Action

9.1.2.1 DeviceRequest5

Definition: This component define the environment, the context and the services to be used with this message.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Environment <*Envt*>	[0..1]	±		133
	Context <*Cntxt*>	[0..1]	±		139
	ServiceContent <*SvcCntt*>	[1..1]	CodeSet		142
	DisplayRequest <*DispReq*>	[0..1]			142
	DisplayOutput <*DispOutpt*>	[1..*]	±		142
	InputRequest <*InptReq*>	[0..1]			143
	DisplayOutput <*DispOutpt*>	[0..1]	±		144
	InputData <*InptData*>	[1..1]			145
	DeviceType <*DvcTp*>	[1..1]	CodeSet		146
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		146
	InputCommand <*InptCmd*>	[1..1]	CodeSet		147
	NotifyCardInputFlag <*NtfyCardInptFlg*>	[1..1]	Indicator		148
	MaximumInputTime <*MaxInptTm*>	[0..1]	Quantity		148
	InputText <*InptTxt*>	[0..1]	±		148
	ImmediateResponseFlag <*ImdtRspnFlg*>	[0..1]	Indicator		149
	WaitUserValidationFlag <*WaitUsrVldtnFlg*>	[0..1]	Indicator		149
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		149
	GlobalCorrectionFlag <*GblCrrctnFlg*>	[0..1]	Indicator		150
	DisableCancelFlag <*DsblCclFlg*>	[0..1]	Indicator		150
	DisableCorrectFlag <*DsblCrrctFlg*>	[0..1]	Indicator		150
	DisableValidFlag <*DsblVldFlg*>	[0..1]	Indicator		150
	MenuBackFlag <*MenuBckFlg*>	[0..1]	Indicator		150
	PrintRequest <*PrtReq*>	[0..1]			151
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		151
	ResponseMode <*RspnMd*>	[1..1]	CodeSet		151
	IntegratedPrintFlag <*IntgrtdPrtFlg*>	[0..1]	Indicator		152
	RequiredSignatureFlag <*ReqrdSgntrFlg*>	[0..1]	Indicator		152
	OutputContent <*OutptCntt*>	[1..1]	±		152
	PlayResourceRequest <*PlayRsrcReq*>	[0..1]			153
	ResponseMode <*RspnMd*>	[0..1]	CodeSet		154
	ResourceAction <*RsrcActn*>	[1..1]	CodeSet		154

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SoundVolume <*SoundVol*>	[0..1]	Rate		154
	DisplayResolution <*DispRsltn*>	[0..1]	Text		154
	Resource <*Rsrc*>	[0..1]			154
	ResourceType <*RsrcTp*>	[1..1]	CodeSet		155
	ResourceFormat <*RsrcFrmt*>	[0..1]	CodeSet		155
	Language <*Lang*>	[0..1]	CodeSet	C6	155
	ResourceReference <*RsrcRef*>	[0..1]	Text		155
	TimingSlot <*TmgSlot*>	[0..1]	CodeSet		156
	SecureInputRequest <*ScrInptReq*>	[0..1]			156
	PINRequestType <*PINReqTp*>	[1..1]	CodeSet		156
	PINVerificationMethod <*PINVrfctnMtd*>	[0..1]	Text		157
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		157
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		157
	CardholderPIN <*CrdhldrPIN*>	[0..1]			157
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		157
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		158
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		158
	InitialisationCardReaderRequest <*InitlstnCardRdrReq*>	[0..1]			158
	WarmResetFlag <*WarmRstFlg*>	[0..1]	Indicator		159
	ForceEntryMode <*ForceNtryMd*>	[0..*]	CodeSet		159
	LeaveCardFlag <*LeavCardFlg*>	[0..1]	Indicator		160
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		160
	DisplayOutput <*DispOutpt*>	[0..1]	±		160
	CardReaderAPDURequest <*CardRdrAPDUReq*>	[0..1]			161
	Class <*Clss*>	[1..1]	Binary		161
	Instruction <*Instr*>	[1..1]	Binary		161
	Parameter1 <*Param1*>	[1..1]	Binary		161
	Parameter2 <*Param2*>	[1..1]	Binary		161
	Data <*Data*>	[0..1]	Binary		161
	ExpectedLength <*XpctdLngth*>	[0..1]	Binary		161
	PowerOffCardReaderRequest <*PwrOffCardRdrReq*>	[0..1]			162

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PowerOffMaximumWaitingTime <*PwrOffMaxWtgTm*>	[0..1]	Quantity		162
	DisplayOutput <*DispOutpt*>	[0..1]	±		162
	TransmissionRequest <*TrnsmssnReq*>	[0..1]			163
	DestinationAddress <*DstnAdr*>	[1..1]	±		163
	MaximumTransmissionTime <*MaxTrnsmssnTm*>	[1..1]	Quantity		164
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		164
	MessageToSend <*MsgToSnd*>	[1..1]	Binary		164
	InputNotification <*InptNtfctn*>	[0..1]			164
	ExchangeIdentification <*XchgId*>	[1..1]	Text		164
	OutputContent <*OutptCntt*>	[1..1]	±		165
	SupplementaryData <*SplmtryData*>	[0..*]	±	C5	165

9.1.2.1.1 Environment <Envt>

Presence: [0..1]

Definition: Environment of the transaction.

Environment <Envt> contains the following elements (see "CardPaymentEnvironment78" on page 280 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Acquirer <*Acqrr*>	[0..1]	±		286
	Merchant <*Mrchnt*>	[0..1]			286
	Identification <*Id*>	[0..1]	±		286
	CommonName <*CmonNm*>	[0..1]	Text		287
	LocationCategory <*LctnCtgy*>	[0..1]	CodeSet		287
	LocationAndContact <*LctnAndCtct*>	[0..1]	±		287
	SchemeData <*SchmeData*>	[0..1]	Text		288
	POI <*POI*>	[0..1]			288
	Identification <*Id*>	[1..1]	±		288
	SystemName <*SysNm*>	[0..1]	Text		289
	GroupIdentification <*GrpId*>	[0..1]	Text		289
	Capabilities <*Cpblties*>	[0..1]	±		289
	TimeZone <*TmZone*>	[0..1]	Text		290
	TerminalIntegration <*TermnlIntgtn*>	[0..1]	CodeSet		290
	Component <*Cmpnt*>	[0..*]	±		291
	Card <*Card*>	[0..1]			293
	ProtectedCardData <*PrtctdCardData*>	[0..1]	±		294
	PrivateCardData <*PrvtCardData*>	[0..1]	Binary		294
	PlainCardData <*PlainCardData*>	[0..1]	±		294
	PaymentAccountReference <*PmtAcctRef*>	[0..1]	Text		295
	MaskedPAN <*MskdPAN*>	[0..1]	Text		295
	IssuerBIN <*IssrBIN*>	[0..1]	Text		295
	CardCountryCode <*CardCtryCd*>	[0..1]	Text		295
	CardCurrencyCode <*CardCcyCd*>	[0..1]	Text		295
	CardProductProfile <*CardPdctPrfl*>	[0..1]	Text		296
	CardBrand <*CardBrnd*>	[0..1]	Text		296
	CardProductType <*CardPdctTp*>	[0..1]	CodeSet		296
	CardProductSubType <*CardPdctSubTp*>	[0..1]	Text		296
	InternationalCard <*IntrnlCard*>	[0..1]	Indicator		296
	AllowedProduct <*AllwdPdct*>	[0..*]	Text		296

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ServiceOption <*SvcOptn*>	[0..1]	Text		297
	AdditionalCardData <*AddtlCardData*>	[0..1]	Text		297
	Check <*Chck*>	[0..1]			297
	BankIdentification <*BkId*>	[0..1]	Text		297
	AccountNumber <*AcctNb*>	[0..1]	Text		297
	CheckNumber <*ChckNb*>	[0..1]	Text		297
	CheckCardNumber <*ChckCardNb*>	[0..1]	Text		298
	CheckTrackData2 <*ChckTrckData2*>	[0..1]			298
	TrackNumber <*TrckNb*>	[0..1]	Quantity		298
	TrackFormat <*TrckFrmt*>	[0..1]	CodeSet		298
	TrackValue <*TrckVal*>	[1..1]	Text		299
	CheckType <*ChckTp*>	[0..1]	CodeSet		299
	Country <*Ctry*>	[0..1]	Text		299
	StoredValueAccount <*StordValAcct*>	[0..*]			299
	AccountType <*AcctTp*>	[0..1]	CodeSet		300
	IdentificationType <*IdTp*>	[0..1]	CodeSet		301
	Identification <*Id*>	[0..1]	Text		301
	Brand <*Brnd*>	[0..1]	Text		301
	Provider <*Prvdr*>	[0..1]	Text		301
	OwnerName <*OwnrNm*>	[0..1]	Text		301
	ExpiryDate <*XpryDt*>	[0..1]	Text		302
	EntryMode <*NtryMd*>	[0..1]	CodeSet		302
	Currency <*Ccy*>	[0..1]	CodeSet	C1	302
	Balance <*Bal*>	[0..1]	Amount		303
	LoyaltyAccount <*LltyAcct*>	[0..*]	±		303
	CustomerDevice <*CstmrDvc*>	[0..1]	±		303
	Wallet <*Wllt*>	[0..1]	±		303
	PaymentToken <*PmtTkn*>	[0..1]	±		304
	MerchantToken <*MrchntTkn*>	[0..1]	±		304
	Cardholder <*Crdhldr*>	[0..1]			305
	Identification <*Id*>	[0..1]			309

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		309
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		309
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		310
	DriverIdentification <*DrvrId*>	[0..1]	Text		310
	CustomerNumber <*CstmrNb*>	[0..1]	Text		310
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		310
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		310
	PassportNumber <*PsptNb*>	[0..1]	Text		310
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		310
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		310
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		311
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		311
	JobNumber <*JobNb*>	[0..1]	Text		311
	Department <*Dept*>	[0..1]	Text		311
	EmailAddress <*EmailAdr*>	[0..1]	Text		311
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			311
	BirthDate <*BirthDt*>	[1..1]	Date		311
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		312
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		312
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	312
	Other <*Othr*>	[0..*]	±		312
	Name <*Nm*>	[0..1]	Text		312
	Language <*Lang*>	[0..1]	CodeSet	C6	312
	BillingAddress <*BllgAdr*>	[0..1]	±		313
	ShippingAddress <*ShppgAdr*>	[0..1]	±		313
	TripNumber <*TripNb*>	[0..1]	Text		314
	Vehicle <*Vhcl*>	[0..1]	±		314
	Authentication <*Authntcn*>	[0..*]			315
	AuthenticationMethod <*AuthntcnMtd*>	[0..1]	CodeSet		317
	AuthenticationExemption <*AuthntcnXmptn*>	[0..1]	CodeSet		318
	AuthenticationValue <*AuthntcnVal*>	[0..1]	Binary		319

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ProtectedAuthenticationValue <*PrtctdAuthntcnVal*>	[0..1]	±		319
	CardholderOnLinePIN <*CrdhldrOnLinePIN*>	[0..1]			319
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		319
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		320
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		320
	CardholderIdentification <*CrdhldrId*>	[0..1]			320
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		321
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		321
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		321
	DriverIdentification <*DrvrId*>	[0..1]	Text		322
	CustomerNumber <*CstmrNb*>	[0..1]	Text		322
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		322
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		322
	PassportNumber <*PsptNb*>	[0..1]	Text		322
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		322
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		322
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		322
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		323
	JobNumber <*JobNb*>	[0..1]	Text		323
	Department <*Dept*>	[0..1]	Text		323
	EmailAddress <*EmailAdr*>	[0..1]	Text		323
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			323
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324
	Other <*Othr*>	[0..*]	±		324
	AddressVerification <*AdrVrfctn*>	[0..1]			324
	AddressDigits <*AdrDgts*>	[0..1]	Text		324
	PostalCodeDigits <*PstlCdDgts*>	[0..1]	Text		325
	AuthenticationType <*AuthntcnTp*>	[0..1]	Text		325

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AuthenticationLevel <*AuthntcnLvl*>	[0..1]	Text		325
	AuthenticationResult <*AuthntcnRslt*>	[0..1]	CodeSet		325
	AuthenticationAdditionalInformation <*AuthntcnAddtlInf*>	[0..1]			325
	Identification <*Id*>	[1..1]	Text		326
	Value <*Val*>	[0..1]	Binary		326
	ProtectedValue <*PrtctdVal*>	[0..1]	±		326
	Type <*Tp*>	[0..1]	Text		326
	TransactionVerificationResult <*TxVrfctnRslt*>	[0..*]			326
	Method <*Mtd*>	[1..1]	CodeSet		327
	VerificationEntity <*VrfctnNtty*>	[0..1]	CodeSet		328
	Result <*Rslt*>	[0..1]	CodeSet		328
	AdditionalResult <*AddtlRslt*>	[0..1]	Text		328
	PersonalData <*PrsnlData*>	[0..1]	Text		329
	MobileData <*MobData*>	[0..*]			329
	MobileCountryCode <*MobCtryCd*>	[0..1]	Text		329
	MobileNetworkCode <*MobNtwkCd*>	[0..1]	Text		329
	MobileMaskedMSISDN <*MobMskdMSISDN*>	[0..1]	Text		330
	Geolocation <*Glctn*>	[0..1]			330
	GeographicCoordinates <*GeogcCordints*>	[0..1]			330
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330
	UTMCoordinates <*UTMCordints*>	[0..1]			331
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331
	SensitiveMobileData <*SnstvMobData*>	[0..1]			331
	MSISDN <*MSISDN*>	[1..1]	Text		332
	IMSI <*IMSI*>	[0..1]	Text		332
	IMEI <*IMEI*>	[0..1]	Text		332
	ProtectedMobileData <*PrtctdMobData*>	[0..1]	±		332
	ProtectedCardholderData <*PrtctdCrdhldrData*>	[0..1]	±		332

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SaleEnvironment <*SaleEnvt*>	[0..1]			333
	SaleCapabilities <*SaleCpblties*>	[0..*]	CodeSet		333
	Currency <*Ccy*>	[0..1]	CodeSet	C1	334
	MinimumAmountToDeliver <*MinAmtToDlvr*>	[0..1]	Amount		334
	MaximumCashBackAmount <*MaxCshBckAmt*>	[0..1]	Amount		334
	MinimumSplitAmount <*MinSpltAmt*>	[0..1]	Amount		335
	DebitPreferredFlag <*DbtPrefrdFlg*>	[0..1]	Indicator		335
	LoyaltyHandling <*LltyHdlg*>	[0..1]	CodeSet		335

9.1.2.1.2 Context <Cntxt>

Presence: [0..1]

Definition: Context in which the transaction is performed (payment and sale).

Context <Cntxt> contains the following elements (see "CardPaymentContext29" on page 354 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PaymentContext <*PmtCntxt*>	[0..1]			357
	CardPresent <*CardPres*>	[0..1]	Indicator		357
	CardholderPresent <*CrdhldrPres*>	[0..1]	Indicator		357
	OnLineContext <*OnLineCntxt*>	[0..1]	Indicator		358
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		358
	TransactionEnvironment <*TxEnvt*>	[0..1]	CodeSet		358
	TransactionChannel <*TxChanl*>	[0..1]	CodeSet		358
	BusinessArea <*BizArea*>	[0..1]	CodeSet		359
	AttendantMessageCapable <*AttndntMsgCpbl*>	[0..1]	Indicator		359
	AttendantLanguage <*AttndntLang*>	[0..1]	CodeSet	C6	359
	CardDataEntryMode <*CardDataNtryMd*>	[0..1]	CodeSet		360
	FallbackIndicator <*FllbckInd*>	[0..1]	CodeSet		360
	SupportedOption <*SpprtdOptn*>	[0..*]	CodeSet		361
	SaleContext <*SaleCntxt*>	[0..1]			361
	SaleIdentification <*SaleId*>	[0..1]	Text		362
	SaleReferenceNumber <*SaleRefNb*>	[0..1]	Text		362
	SaleReconciliationIdentification <*SaleRcncltnId*>	[0..1]	Text		363
	CashierIdentification <*CshrId*>	[0..1]	Text		363
	CashierLanguage <*CshrLang*>	[0..*]	CodeSet	C6	363
	ShiftNumber <*ShftNb*>	[0..1]	Text		363
	CustomerOrderRequestFlag <*CstmrOrdrReqFlg*>	[0..1]	Indicator		363
	PurchaseOrderNumber <*PurchsOrdrNb*>	[0..1]	Text		363
	InvoiceNumber <*InvcNb*>	[0..1]	Text		363
	DeliveryNoteNumber <*DlvryNoteNb*>	[0..1]	Text		364
	SponsoredMerchant <*SpnsrdMrchnt*>	[0..*]			364
	CommonName <*CmonNm*>	[1..1]	Text		364
	Address <*Adr*>	[0..1]	Text		364
	CountryCode <*CtryCd*>	[1..1]	CodeSet		364
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		364
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		364

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SplitPayment <*SpltPmt*>	[0..1]	Indicator		365
	RemainingAmount <*RmngAmt*>	[0..1]	Amount		365
	ForceOnlineFlag <*ForceOnlnFlg*>	[0..1]	Indicator		365
	ReuseCardDataFlag <*ReuseCardDataFlg*>	[0..1]	Indicator		365
	AllowedEntryMode <*AllwdNtryMd*>	[0..*]	CodeSet		365
	SaleTokenScope <*SaleTknScp*>	[0..1]	CodeSet		366
	AdditionalSaleData <*AddtlSaleData*>	[0..1]	Text		366
	DirectDebitContext <*DrctDbtCntxt*>	[0..1]			366
	DebtorIdentification <*DbtrId*>	[0..1]			367
	Debtor <*Dbtr*>	[0..1]			368
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	368
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		369
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			369
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369
	AccountIdentification <*AcctId*>	[0..1]			370
{Or	IBAN <*IBAN*>	[1..1]	IdentifierSet	C4	370
Or	BBAN <*BBAN*>	[1..1]	IdentifierSet		370
Or	UPIC <*UPIC*>	[1..1]	IdentifierSet		371
Or}	DomesticAccount <*DmstAcct*>	[1..1]			371
	Identification <*Id*>	[1..1]	Text		371
	CreditorIdentification <*CdtrId*>	[1..1]			371
	Creditor <*Cdtr*>	[1..1]			372
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	372
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		372
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			372
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373
	RegistrationIdentification <*RegnId*>	[0..1]	Text		373
	MandateRelatedInformation <*MndtRltdInf*>	[1..1]			373
	MandateIdentification <*MndtId*>	[1..1]	Text		374

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DateOfSignature <*DtOfSgntr*>	[0..1]	Date		374
	MandateImage <*MndtImg*>	[0..1]	Binary		374

9.1.2.1.3 ServiceContent <SvcCntt>

Presence: [1..1]

Definition: Define the type of service requested.

Datatype: "RetailerService8Code" on page 503

CodeName	Name	Definition
DDYQ	DeviceDisplayRequest	One System requests the other to display a message for cashier or customer.
DINQ	DeviceInputRequest	One system requests to the other System to get data input.
DPRQ	DevicePrintRequest	One system requests to the other System to print data.
DSOQ	DevicePlaySoundRequest	One system requests to the Other System to play a sound.
DSIQ	DeviceSecureInputRequest	One system requests to the Other System to securely get data input (e.g. for PIN).
DCIQ	DeviceInitialisationCardReaderRequest	Service to send parameters to use when card reader initializes a new communication with the card.
DCAQ	DeviceSendApplicationProtocolDataUnitCardReaderRequest	A service to send commands to a card.
DCPQ	DevicePowerOffCardReaderRequest	The Sale system requests to the POI System to power off the card reader.
DCOQ	DeviceTransmissionMessageRequest	The Sale system requests to the POI System to transmit a message (for instance to a mobile server).
DINO	DeviceInputNotification	One system sends a notification to the POI System to update a input request.

9.1.2.1.4 DisplayRequest <DispReq>

Presence: [0..1]

Definition: Content of the Display Request message.

DisplayRequest <DispReq> contains the following **DeviceDisplayRequest4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DisplayOutput <*DispOutpt*>	[1..*]	±		142

9.1.2.1.4.1 DisplayOutput <DispOutpt>

Presence: [1..*]

Definition: Message to be displayed.

DisplayOutput <DispOutpt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.5 InputRequest <InptReq>

Presence: [0..1]

Definition: Content of the Input Request message.

InputRequest <InptReq> contains the following **DeviceInputRequest4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DisplayOutput <*DispOutpt*>	[0..1]	±		144
	InputData <*InptData*>	[1..1]			145
	DeviceType <*DvcTp*>	[1..1]	CodeSet		146
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		146
	InputCommand <*InptCmd*>	[1..1]	CodeSet		147
	NotifyCardInputFlag <*NtfyCardInptFlg*>	[1..1]	Indicator		148
	MaximumInputTime <*MaxInptTm*>	[0..1]	Quantity		148
	InputText <*InptTxt*>	[0..1]	±		148
	ImmediateResponseFlag <*ImdtRspnFlg*>	[0..1]	Indicator		149
	WaitUserValidationFlag <*WaitUsrVldtnFlg*>	[0..1]	Indicator		149
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		149
	GlobalCorrectionFlag <*GblCrrctnFlg*>	[0..1]	Indicator		150
	DisableCancelFlag <*DsblCclFlg*>	[0..1]	Indicator		150
	DisableCorrectFlag <*DsblCrrctFlg*>	[0..1]	Indicator		150
	DisableValidFlag <*DsblVldFlg*>	[0..1]	Indicator		150
	MenuBackFlag <*MenuBckFlg*>	[0..1]	Indicator		150

9.1.2.1.5.1 DisplayOutput <DispOutpt>

Presence: [0..1]

Definition: Information to display before input.

DisplayOutput <DispOutpt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.5.2 InputData <InptData>

Presence: [1..1]

Definition: Information related to an Input request.

InputData <InptData> contains the following **InputData4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DeviceType <*DvcTp*>	[1..1]	CodeSet		146
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		146
	InputCommand <*InptCmd*>	[1..1]	CodeSet		147
	NotifyCardInputFlag <*NtfyCardInptFlg*>	[1..1]	Indicator		148
	MaximumInputTime <*MaxInptTm*>	[0..1]	Quantity		148
	InputText <*InptTxt*>	[0..1]	±		148
	ImmediateResponseFlag <*ImdtRspnFlg*>	[0..1]	Indicator		149
	WaitUserValidationFlag <*WaitUsrVldtnFlg*>	[0..1]	Indicator		149
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		149
	GlobalCorrectionFlag <*GblCrrctnFlg*>	[0..1]	Indicator		150
	DisableCancelFlag <*DsblCclFlg*>	[0..1]	Indicator		150
	DisableCorrectFlag <*DsblCrrctFlg*>	[0..1]	Indicator		150
	DisableValidFlag <*DsblVldFlg*>	[0..1]	Indicator		150
	MenuBackFlag <*MenuBckFlg*>	[0..1]	Indicator		150

9.1.2.1.5.2.1 DeviceType <DvcTp>

Presence: [1..1]

Definition: Type of logical device located on a Sale Terminal or a POI Terminal.

Datatype: "SaleCapabilities2Code" on page 505

CodeName	Name	Definition
CHIN	CashierInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element). The output device attached to this input device is the CashierDisplay device.
CUIN	CustomerInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element).

9.1.2.1.5.2.2 InformationQualifier <InfQlfr>

Presence: [1..1]

Definition: Qualification of the information to output to the logical device.

Datatype: "InformationQualify1Code" on page 487

CodeName	Name	Definition
CUSA	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
DISP	Display	Standard display interface.
DOCT	Document	When the POI System wants to print specific document (check, dynamic currency conversion ...). Used by the Sale System when the printer is not located on the Sale System.
ERRO	Error	The information is related to an error situation occurring on the message sender.
INPT	Input	Answer to a question or information to be entered by the Cashier or the Customer, at the request of the POI Terminal or the Sale Terminal.
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
RCPT	Receipt	Where you print the Payment receipt that could be located on the Sale System or in some cases a restricted Sale ticket on the POI Terminal.
SOND	Sound	Standard sound interface.
STAT	Status	The information is a new state on which the message sender is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
VCHR	Voucher	Coupons, voucher or special ticket generated by the POI or the Sale System and to be printed.

9.1.2.1.5.2.3 InputCommand <InptCmd>

Presence: [1..1]

Definition: Type of requested input.

Datatype: "InputCommand1Code" on page 487

CodeName	Name	Definition
DCSG	DecimalString	Wait for a string of digit characters with a decimal point, the length range could be specified.
DGSG	DigitString	Wait for a string of digit characters.
GAKY	GetAnyKey	Wait for a key pressed on the Terminal, to be able to read the message displayed on the Terminal.
GCNF	GetConfirmation	Wait for a confirmation Yes (Y) or No (N) on the Sale System. Wait for a confirmation (Valid or Cancel button) on

CodeName	Name	Definition
		the POI Terminal. The result of the command is a Boolean: True or False.
GFKY	GetFunctionKey	Wait for a function key pressed on the Terminal: From POI, Valid, Clear, Correct, Generic Function key number. From Sale, Generic Function key.
GMNE	GetMenuEntry	To choose an entry among a list of entries (all of them are not necessary selectable). The OutputFormat has to be MenuEntry.
PSWD	Password	Request to enter a password with masked characters while typing the password.
SITE	SiteManager	Wait for a confirmation Yes (Y) or No (N) of the Site Manager on the Sale System.
TXSG	TextString	Wait for a string of alphanumeric characters.
HTML	XHTMLText	Wait for a XHTML data.
SIGN	Signature	Request to wait for signature.

9.1.2.1.5.2.4 NotifyCardInputFlag <NtfyCardInptFlg>

Presence: [1..1]

Definition: Flag of notification of card to be entered in the POI card reader.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.5 MaximumInputTime <MaxInptTm>

Presence: [0..1]

Definition: Maximum input time in seconds.

Datatype: "Number" on page 515

9.1.2.1.5.2.6 InputText <InptTxt>

Presence: [0..1]

Definition: Text value set for an input command.

InputText <InptTxt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.5.2.7 ImmediateResponseFlag <ImdtRspnFlg>

Presence: [0..1]

Definition: Flag to request Immediate response without waiting for the completion of the command.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.8 WaitUserValidationFlag <WaitUsrVldtnFlg>

Presence: [0..1]

Definition: Flag to confirm by the user the entered characters, when the maximum allowed length is reached.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.9 BeepKeyFlag <BeepKeyFlg>

Presence: [0..1]

Definition: Flag to indicate that when the user press a key, a beep has to be generated.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.10 GlobalCorrectionFlag <GblCrrctnFlg>

Presence: [0..1]

Definition: Flag to correct all characters (True) or just the last one (False).

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.11 DisableCancelFlag <DsblCclFlg>

Presence: [0..1]

Definition: Flag to deactivate the "Cancel" function key.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.12 DisableCorrectFlag <DsblCrrctFlg>

Presence: [0..1]

Definition: Flag to deactivate the "Correct" function key.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.13 DisableValidFlag <DsblVldFlg>

Presence: [0..1]

Definition: Flag to disable the "Valid" function key.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.5.2.14 MenuBackFlag <MenuBckFlg>

Presence: [0..1]

Definition: Flag to enable the "Back" function key to go the upper level.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.6 PrintRequest <PrtReq>

Presence: [0..1]

Definition: Content of the Print Request message.

PrintRequest <PrtReq> contains the following **DevicePrintRequest4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		151
	ResponseMode <*RspnMd*>	[1..1]	CodeSet		151
	IntegratedPrintFlag <*IntgrtdPrtFlg*>	[0..1]	Indicator		152
	RequiredSignatureFlag <*ReqrdSgntrFlg*>	[0..1]	Indicator		152
	OutputContent <*OutptCntt*>	[1..1]	±		152

9.1.2.1.6.1 DocumentQualifier <DocQlfr>

Presence: [1..1]

Definition: Qualifies the type of document.

Datatype: "DocumentType7Code" on page 484

CodeName	Name	Definition
JNRL	Journal	When the POI or the Sale System wants to store a message on the journal printer or electronic journal of the Sale Terminal (it is sometimes a Sale Logging/Journal Printer).
CRCP	CustomerReceipt	When the Sale System requires the POI system to print the Customer receipt.
HRCP	CashierReceipt	When the Sale system print the Cashier copy of the Payment receipt.
SRCP	SaleReceipt	When the Sale System requires the POI system to print the Sale receipt.
RPIN	RelatedPaymentInstruction	Document is a linked payment instruction to which the current payment instruction is related, for example, in a cover scenario.
VCHR	Voucher	Document is an electronic payment document.

9.1.2.1.6.2 ResponseMode <RspnMd>

Presence: [1..1]

Definition: Type of awaited response (none, immediate, after printing, after sound).

Datatype: "ResponseMode2Code" on page 502

CodeName	Name	Definition
SEND	EndOfPlay	The Response is required at the end of play.

CodeName	Name	Definition
IMMD	Immediate	The Message Response is immediate, after taking into account the request.
NREQ	NotRequired	The Message Response is not required, except in case of error.
PEND	PrintEnd	The Print Response is required at the end of print.

9.1.2.1.6.3 IntegratedPrintFlag <IntgrtdPrtFlg>

Presence: [0..1]

Definition: Flag that the print is integrated to other prints.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.6.4 RequiredSignatureFlag <ReqrdSgntrFlg>

Presence: [0..1]

Definition: Flag to require a physical signature by the Customer.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.6.5 OutputContent <OutptCntt>

Presence: [1..1]

Definition: Content of the message to print.

OutputContent <OutptCntt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.7 PlayResourceRequest <PlayRsrcReq>

Presence: [0..1]

Definition: Content of the Resource Request message.

PlayResourceRequest <PlayRsrcReq> contains the following **DevicePlayResourceRequest1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ResponseMode <*RspnMd*>	[0..1]	CodeSet		154
	ResourceAction <*RsrcActn*>	[1..1]	CodeSet		154
	SoundVolume <*SoundVol*>	[0..1]	Rate		154
	DisplayResolution <*DispRsltn*>	[0..1]	Text		154
	Resource <*Rsrc*>	[0..1]			154
	ResourceType <*RsrcTp*>	[1..1]	CodeSet		155
	ResourceFormat <*RsrcFrmt*>	[0..1]	CodeSet		155
	Language <*Lang*>	[0..1]	CodeSet	C6	155
	ResourceReference <*RsrcRef*>	[0..1]	Text		155
	TimingSlot <*TmgSlot*>	[0..1]	CodeSet		156

9.1.2.1.7.1 ResponseMode <RspnMd>

Presence: [0..1]

Definition: Message response awaited by the initiator of the Request.

Datatype: "ResponseMode2Code" on page 502

CodeName	Name	Definition
SEND	EndOfPlay	The Response is required at the end of play.
IMMD	Immediate	The Message Response is immediate, after taking into account the request.
NREQ	NotRequired	The Message Response is not required, except in case of error.
PEND	PrintEnd	The Print Response is required at the end of print.

9.1.2.1.7.2 ResourceAction <RsrcActn>

Presence: [1..1]

Definition: Requested Action: Start to play a media resource, Stop to play a media resource, Set the default volume.

Datatype: "ResourceAction1Code" on page 500

CodeName	Name	Definition
PAUS	Pause	Pause the media resource in progress as specified in the message.
STAS	Play	Start the media resource as specified in the message.
LOOP	PlayInLoop	Play in a loop the media resource as specified in the message.
RESU	Resume	Resume the progress of the media resource as specified in the message.
DVOL	SetDefaultVolume	Set the default volume of sounds.
STOS	Stop	Stop the media resource in progress.

9.1.2.1.7.3 SoundVolume <SoundVol>

Presence: [0..1]

Definition: Volume of a sound, either in a percentage of the maximum volume, or 0 to mute.

Datatype: "PercentageRate" on page 515

9.1.2.1.7.4 DisplayResolution <DispRsltn>

Presence: [0..1]

Definition: Resolution to use.

Datatype: "Max35Text" on page 519

9.1.2.1.7.5 Resource <Rsrc>

Presence: [0..1]

Definition: Identification of the resource to use.

Resource <Rsrc> contains the following **ResourceContent1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ResourceType <*RsrcTp*>	[1..1]	CodeSet		155
	ResourceFormat <*RsrcFrmt*>	[0..1]	CodeSet		155
	Language <*Lang*>	[0..1]	CodeSet	C6	155
	ResourceReference <*RsrcRef*>	[0..1]	Text		155

9.1.2.1.7.5.1 ResourceType <RsrcTp>

Presence: [1..1]

Definition: Type of media resource.

Datatype: "ResourceType1Code" on page 501

CodeName	Name	Definition
TEXT	TextToSpeech	Voice synthesis.
URLI	UniformResourceIdentifier	String of characters that unambiguously identifies a particular resource.

9.1.2.1.7.5.2 ResourceFormat <RsrcFrmt>

Presence: [0..1]

Definition: Format of the media resource;

Datatype: "SoundFormat1Code" on page 506

CodeName	Name	Definition
MSGR	MessageRef	Reference of a preloaded text to play.
SNDR	SoundRef	Preloaded sound File.
TEXT	Text	Text to play.

9.1.2.1.7.5.3 Language <Lang>

Presence: [0..1]

Definition: Language of the media resource.

Impacted by: C6 "ValidationByTable"

Datatype: "LanguageCode" on page 489

Constraints

- **ValidationByTable**

  Must be a valid terrestrial language.

9.1.2.1.7.5.4 ResourceReference <RsrcRef>

Presence: [0..1]

Definition: Reference of a media resource.

Datatype: "Max1025Text" on page 516

9.1.2.1.7.6 TimingSlot <TmgSlot>

Presence: [0..1]

Definition: Identification of the moment to manage the media resource.

Datatype: "ProcessingPosition2Code" on page 499

CodeName	Name	Definition
AFTE	After	Specifies that the transaction/instruction is to be executed after the linked transaction/instruction.
WITH	With	Specifies that the transaction/instruction is to be executed with the linked transaction/instruction.
BEFO	Before	Specifies that the transaction/instruction is to be executed before the linked transaction/instruction.
INFO	Information	Specifies that the transactions/ instructions are linked for information purposes only.

9.1.2.1.8 SecureInputRequest <ScrInptReq>

Presence: [0..1]

Definition: Request a secure input for a PIN.

SecureInputRequest <ScrInptReq> contains the following **DeviceSecureInputRequest4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PINRequestType <*PINReqTp*>	[1..1]	CodeSet		156
	PINVerificationMethod <*PINVrfctnMtd*>	[0..1]	Text		157
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		157
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		157
	CardholderPIN <*CrdhldrPIN*>	[0..1]			157
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		157
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		158
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		158

9.1.2.1.8.1 PINRequestType <PINReqTp>

Presence: [1..1]

Definition: Type of PIN Service.

Datatype: "PINRequestType1Code" on page 497

CodeName	Name	Definition
PIAE	PINAcquisitionEncryption	The cardholder enters the PIN, the POI enciphers the PIN Block and provides it as a result to the Sale System.
PIAV	PINAcquisitionVerification	The Cardholder enters the PIN and the POI verifies it.
PIVO	PINVerifyOnly	The Sale System send a previous keyed PIN and the POI verifies it.

9.1.2.1.8.2 PINVerificationMethod <PINVrfctnMtd>

Presence: [0..1]

Definition: Identify the PIN verification method and keys.

Datatype: "Max35Text" on page 519

9.1.2.1.8.3 MaximumWaitingTime <MaxWtgTm>

Presence: [0..1]

Definition: Maximum time to wait for the request processing in seconds.

Datatype: "Number" on page 515

9.1.2.1.8.4 BeepKeyFlag <BeepKeyFlg>

Presence: [0..1]

Definition: Indicates, when the user press a key, if a beep has to be generated.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.8.5 CardholderPIN <CrdhldrPIN>

Presence: [0..1]

Definition: Enciphered PIN and related information.

CardholderPIN <CrdhldrPIN> contains the following **OnLinePIN9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		157
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		158
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		158

9.1.2.1.8.5.1 EncryptedPINBlock <NcrptdPINBlck>

Presence: [1..1]

Definition: Encrypted PIN (Personal Identification Number).

EncryptedPINBlock <NcrptdPINBlck> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.2.1.8.5.2 PINFormat <PINFrmt>

Presence: [1..1]

Definition: PIN (Personal Identification Number) format before encryption.

Datatype: "PINFormat3Code" on page 496

CodeName	Name	Definition
ISO0	ISO0	PIN diversified with the card account number, conforming to the standard ISO 9564-2.
ISO1	ISO1	PIN completed with random padding characters, conforming to the standard ISO 9564-2.
ISO2	ISO2	PIN without diversification characters, conforming to the standard ISO 9564-2.
ISO3	ISO3	PIN diversified with the card account number and random characters, conforming to the standard ISO 9564-2.
ISO4	ISO4	PIN format used with AES encryption, conforming to the new ISO SC2 format.
ISO5	ISO5	Alternative PIN format used with AES encryption, conforming to the new ISO SC2 format.

9.1.2.1.8.5.3 AdditionalInput <AddtlInpt>

Presence: [0..1]

Definition: Additional information required to verify the PIN (Personal Identification Number).

Datatype: "Max35Text" on page 519

9.1.2.1.9 InitialisationCardReaderRequest <InitlstnCardRdrReq>

Presence: [0..1]

Definition: A service to send parameters to Card Reader to initialize a new communication with a card.

InitialisationCardReaderRequest <InitIstnCardRdrReq> contains the following **DeviceInitialisationCardReaderRequest4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	WarmResetFlag <*WarmRstFlg*>	[0..1]	Indicator		159
	ForceEntryMode <*ForceNtryMd*>	[0..*]	CodeSet		159
	LeaveCardFlag <*LeavCardFlg*>	[0..1]	Indicator		160
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		160
	DisplayOutput <*DispOutpt*>	[0..1]	±		160

9.1.2.1.9.1 WarmResetFlag <WarmRstFlg>

Presence: [0..1]

Definition: Flag to request a warm reset on a chip.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.9.2 ForceEntryMode <ForceNtryMd>

Presence: [0..*]

Definition: Payment instrument entry mode requested by the Sale System.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.
UNKW	Unknown	Unknown card reading capability.

CodeName	Name	Definition
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.2.1.9.3 LeaveCardFlag <LeavCardFlg>

Presence: [0..1]

Definition: Flag to indicate the POI System to keep the card in the reader for a smart card.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.1.9.4 MaximumWaitingTime <MaxWtgTm>

Presence: [0..1]

Definition: Maximum time in seconds that the POI has to wait for a card response.

Datatype: "Number" on page 515

9.1.2.1.9.5 DisplayOutput <DispOutpt>

Presence: [0..1]

Definition: Information to display.

DisplayOutput <DispOutpt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.10 CardReaderAPDURequest <CardRdrAPDUReq>

Presence: [0..1]

Definition: Content of the APDU (Application Protocol Data Unit) to send to the Card.

CardReaderAPDURequest <CardRdrAPDUReq> contains the following **DeviceSendApplicationProtocolDataUnitCardReaderRequest1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Class <*Clss*>	[1..1]	Binary		161
	Instruction <*Instr*>	[1..1]	Binary		161
	Parameter1 <*Param1*>	[1..1]	Binary		161
	Parameter2 <*Param2*>	[1..1]	Binary		161
	Data <*Data*>	[0..1]	Binary		161
	ExpectedLength <*XpctdLngth*>	[0..1]	Binary		161

9.1.2.1.10.1 Class <Clss>

Presence: [1..1]

Definition: Class field of the Application Protocol Data Unit command (CLA).

Datatype: "Min1Max256Binary" on page 463

9.1.2.1.10.2 Instruction <Instr>

Presence: [1..1]

Definition: Instruction field of the Application Protocol Data Unit command (INS).

Datatype: "Min1Max256Binary" on page 463

9.1.2.1.10.3 Parameter1 <Param1>

Presence: [1..1]

Definition: Parameter 1 field of the Application Protocol Data Unit command

Datatype: "Min1Max256Binary" on page 463

9.1.2.1.10.4 Parameter2 <Param2>

Presence: [1..1]

Definition: Parameter 2 field of the Application Protocol Data Unit command

Datatype: "Min1Max256Binary" on page 463

9.1.2.1.10.5 Data <Data>

Presence: [0..1]

Definition: Data field of the Application Protocol Data Unit command to send including the length.

Datatype: "Min1Max256Binary" on page 463

9.1.2.1.10.6 ExpectedLength <XpctdLngth>

Presence: [0..1]

Definition: Expected length of the data field of the Application Protocol Data Unit response to the command.

Datatype: "Min1Max256Binary" on page 463

9.1.2.1.11 PowerOffCardReaderRequest <PwrOffCardRdrReq>

Presence: [0..1]

Definition: Content of the Power Off Card Reader Request message.

PowerOffCardReaderRequest <PwrOffCardRdrReq> contains the following **DevicePoweroffCardReaderRequest4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PowerOffMaximumWaitingTime <*PwrOffMaxWtgTm*>	[0..1]	Quantity		162
	DisplayOutput <*DispOutpt*>	[0..1]	±		162

9.1.2.1.11.1 PowerOffMaximumWaitingTime <PwrOffMaxWtgTm>

Presence: [0..1]

Definition: Maximum time to wait for the request processing in seconds.

Datatype: "Number" on page 515

9.1.2.1.11.2 DisplayOutput <DispOutpt>

Presence: [0..1]

Definition: Optional message before Power-Off.

DisplayOutput <DispOutpt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.12 TransmissionRequest <TrnsmssnReq>

Presence: [0..1]

Definition: Content of the Request message to transmit.

TransmissionRequest <TrnsmssnReq> contains the following **DeviceTransmitMessageRequest2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DestinationAddress <*DstnAdr*>	[1..1]	±		163
	MaximumTransmissionTime <*MaxTrnsmssnTm*>	[1..1]	Quantity		164
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		164
	MessageToSend <*MsgToSnd*>	[1..1]	Binary		164

9.1.2.1.12.1 DestinationAddress <DstnAdr>

Presence: [1..1]

Definition: Transport address.

DestinationAddress <DstnAdr> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.2.1.12.2 MaximumTransmissionTime <MaxTrnsmssnTm>

Presence: [1..1]

Definition: Maximum time in seconds of transmission.

Datatype: "Number" on page 515

9.1.2.1.12.3 MaximumWaitingTime <MaxWtgTm>

Presence: [0..1]

Definition: Defines the timeout to receive an answer.

Datatype: "Number" on page 515

9.1.2.1.12.4 MessageToSend <MsgToSnd>

Presence: [1..1]

Definition: Content of the message to be transmitted.

Datatype: "Max100KBinary" on page 461

9.1.2.1.13 InputNotification <InptNtfctn>

Presence: [0..1]

Definition: Content of the Input notification message.

InputNotification <InptNtfctn> contains the following **DeviceInputNotification4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ExchangeIdentification <*XchgId*>	[1..1]	Text		164
	OutputContent <*OutptCntt*>	[1..1]	±		165

9.1.2.1.13.1 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Message main identifier.

Datatype: "Max35Text" on page 519

9.1.2.1.13.2 OutputContent <OutptCntt>

Presence: [1..1]

Definition: Updated content of the message to display before input.

OutputContent <OutptCntt> contains the following elements (see "ActionMessage9" on page 273 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.2.1.14 SupplementaryData <SplmtryData>

Presence: [0..*]

Definition: Additional information incorporated as an extension to the message.

Impacted by: C5 "SupplementaryDataRule"

SupplementaryData <SplmtryData> contains the following elements (see "SupplementaryData1" on page 256 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PlaceAndName <*PlcAndNm*>	[0..1]	Text		256
	Envelope <*Envlp*>	[1..1]	(External Schema)		256

Constraints

- **SupplementaryDataRule**

  This component may not be used without the explicit approval of a SEG and submission to the RA of ISO 20022 compliant structure(s) to be used in the Envelope element.

9.1.2.2 DeviceResponse5

Definition: This component define the type of Device service to be used with this message.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Environment <*Envt*>	[0..1]	±		168
	Context <*Cntxt*>	[0..1]	±		174
	ServiceContent <*SvcCntt*>	[1..1]	CodeSet		177
	DisplayResponse <*DispRspn*>	[0..1]			177
	OutputResult <*OutptRslt*>	[1..*]			178
	DeviceType <*DvcTp*>	[1..1]	CodeSet		178
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		178
	Response <*Rspn*>	[1..1]	±		179
	InputResponse <*InptRspn*>	[0..1]			179
	OutputResult <*OutptRslt*>	[0..1]			180
	DeviceType <*DvcTp*>	[1..1]	CodeSet		180
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		181
	Response <*Rspn*>	[1..1]	±		182
	InputResult <*InptRslt*>	[1..1]			182
	DeviceType <*DvcTp*>	[1..1]	CodeSet		182
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		183
	InputResultData <*InptRsltData*>	[1..1]			183
	InputCommand <*InptCmd*>	[1..1]	CodeSet		184
	ConfirmedFlag <*ConfdFlg*>	[0..1]	Indicator		185
	FunctionKey <*FctnKey*>	[0..1]	Quantity		185
	InputMessage <*InptMsg*>	[0..1]	Text		185
	Password <*Pwd*>	[0..1]	±		185
	ImageCapturedSignature <*ImgCaptrdSgntr*>	[0..1]			186
	ImageFormat <*ImgFrmt*>	[1..1]	Text		186
	ImageData <*ImgData*>	[0..1]	Binary		186
	ImageReference <*ImgRef*>	[0..1]	Text		186
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		186
	PrintResponse <*PrtRspn*>	[0..1]			186
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		186
	SecureInputResponse <*ScrInptRspn*>	[0..1]			187
	CardholderPIN <*CrdhldrPIN*>	[0..1]			187

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		188
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		188
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		188
	InitialisationCardReaderResponse <*InitlstnCardRdrRspn*>	[0..1]			188
	CardEntryMode <*CardNtryMd*>	[0..1]	CodeSet		189
	ICCResetData <*ICCRstData*>	[0..1]			189
	ATRValue <*ATRVal*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[0..1]	Binary		190
	AdditionalInformation <*AddtlInf*>	[0..1]	Binary		190
	CardReaderApplicationProtocolDataUnitResponse <*CardRdrApplPrtcolDataUnitRspn*>	[0..1]			190
	Data <*Data*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[1..1]	Binary		190
	TransmissionResponse <*TrnsmssnRspn*>	[0..1]			191
	ReceivedMessage <*RcvdMsg*>	[0..1]	Binary		191
	Response <*Rspn*>	[1..1]	±		191
	SupplementaryData <*SplmtryData*>	[0..*]	±	C5	191

9.1.2.2.1 Environment <Envt>

Presence: [0..1]

Definition: Environment of the transaction.

Environment <Envt> contains the following elements (see "CardPaymentEnvironment78" on page 280 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Acquirer <*Acqrr*>	[0..1]	±		286
	Merchant <*Mrchnt*>	[0..1]			286
	Identification <*Id*>	[0..1]	±		286
	CommonName <*CmonNm*>	[0..1]	Text		287
	LocationCategory <*LctnCtgy*>	[0..1]	CodeSet		287
	LocationAndContact <*LctnAndCtct*>	[0..1]	±		287
	SchemeData <*SchmeData*>	[0..1]	Text		288
	POI <*POI*>	[0..1]			288
	Identification <*Id*>	[1..1]	±		288
	SystemName <*SysNm*>	[0..1]	Text		289
	GroupIdentification <*GrpId*>	[0..1]	Text		289
	Capabilities <*Cpblties*>	[0..1]	±		289
	TimeZone <*TmZone*>	[0..1]	Text		290
	TerminalIntegration <*TermnlIntgtn*>	[0..1]	CodeSet		290
	Component <*Cmpnt*>	[0..*]	±		291
	Card <*Card*>	[0..1]			293
	ProtectedCardData <*PrtctdCardData*>	[0..1]	±		294
	PrivateCardData <*PrvtCardData*>	[0..1]	Binary		294
	PlainCardData <*PlainCardData*>	[0..1]	±		294
	PaymentAccountReference <*PmtAcctRef*>	[0..1]	Text		295
	MaskedPAN <*MskdPAN*>	[0..1]	Text		295
	IssuerBIN <*IssrBIN*>	[0..1]	Text		295
	CardCountryCode <*CardCtryCd*>	[0..1]	Text		295
	CardCurrencyCode <*CardCcyCd*>	[0..1]	Text		295
	CardProductProfile <*CardPdctPrfl*>	[0..1]	Text		296
	CardBrand <*CardBrnd*>	[0..1]	Text		296
	CardProductType <*CardPdctTp*>	[0..1]	CodeSet		296
	CardProductSubType <*CardPdctSubTp*>	[0..1]	Text		296
	InternationalCard <*IntrnlCard*>	[0..1]	Indicator		296
	AllowedProduct <*AllwdPdct*>	[0..*]	Text		296

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ServiceOption <*SvcOptn*>	[0..1]	Text		297
	AdditionalCardData <*AddtlCardData*>	[0..1]	Text		297
	Check <*Chck*>	[0..1]			297
	BankIdentification <*BkId*>	[0..1]	Text		297
	AccountNumber <*AcctNb*>	[0..1]	Text		297
	CheckNumber <*ChckNb*>	[0..1]	Text		297
	CheckCardNumber <*ChckCardNb*>	[0..1]	Text		298
	CheckTrackData2 <*ChckTrckData2*>	[0..1]			298
	TrackNumber <*TrckNb*>	[0..1]	Quantity		298
	TrackFormat <*TrckFrmt*>	[0..1]	CodeSet		298
	TrackValue <*TrckVal*>	[1..1]	Text		299
	CheckType <*ChckTp*>	[0..1]	CodeSet		299
	Country <*Ctry*>	[0..1]	Text		299
	StoredValueAccount <*StordValAcct*>	[0..*]			299
	AccountType <*AcctTp*>	[0..1]	CodeSet		300
	IdentificationType <*IdTp*>	[0..1]	CodeSet		301
	Identification <*Id*>	[0..1]	Text		301
	Brand <*Brnd*>	[0..1]	Text		301
	Provider <*Prvdr*>	[0..1]	Text		301
	OwnerName <*OwnrNm*>	[0..1]	Text		301
	ExpiryDate <*XpryDt*>	[0..1]	Text		302
	EntryMode <*NtryMd*>	[0..1]	CodeSet		302
	Currency <*Ccy*>	[0..1]	CodeSet	C1	302
	Balance <*Bal*>	[0..1]	Amount		303
	LoyaltyAccount <*LltyAcct*>	[0..*]	±		303
	CustomerDevice <*CstmrDvc*>	[0..1]	±		303
	Wallet <*Wllt*>	[0..1]	±		303
	PaymentToken <*PmtTkn*>	[0..1]	±		304
	MerchantToken <*MrchntTkn*>	[0..1]	±		304
	Cardholder <*Crdhldr*>	[0..1]			305
	Identification <*Id*>	[0..1]			309

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		309
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		309
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		310
	DriverIdentification <*DrvrId*>	[0..1]	Text		310
	CustomerNumber <*CstmrNb*>	[0..1]	Text		310
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		310
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		310
	PassportNumber <*PsptNb*>	[0..1]	Text		310
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		310
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		310
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		311
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		311
	JobNumber <*JobNb*>	[0..1]	Text		311
	Department <*Dept*>	[0..1]	Text		311
	EmailAddress <*EmailAdr*>	[0..1]	Text		311
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			311
	BirthDate <*BirthDt*>	[1..1]	Date		311
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		312
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		312
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	312
	Other <*Othr*>	[0..*]	±		312
	Name <*Nm*>	[0..1]	Text		312
	Language <*Lang*>	[0..1]	CodeSet	C6	312
	BillingAddress <*BllgAdr*>	[0..1]	±		313
	ShippingAddress <*ShppgAdr*>	[0..1]	±		313
	TripNumber <*TripNb*>	[0..1]	Text		314
	Vehicle <*Vhcl*>	[0..1]	±		314
	Authentication <*Authntcn*>	[0..*]			315
	AuthenticationMethod <*AuthntcnMtd*>	[0..1]	CodeSet		317
	AuthenticationExemption <*AuthntcnXmptn*>	[0..1]	CodeSet		318
	AuthenticationValue <*AuthntcnVal*>	[0..1]	Binary		319

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ProtectedAuthenticationValue <*PrtctdAuthntcnVal*>	[0..1]	±		319
	CardholderOnLinePIN <*CrdhldrOnLinePIN*>	[0..1]			319
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		319
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		320
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		320
	CardholderIdentification <*CrdhldrId*>	[0..1]			320
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		321
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		321
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		321
	DriverIdentification <*DrvrId*>	[0..1]	Text		322
	CustomerNumber <*CstmrNb*>	[0..1]	Text		322
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		322
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		322
	PassportNumber <*PsptNb*>	[0..1]	Text		322
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		322
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		322
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		322
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		323
	JobNumber <*JobNb*>	[0..1]	Text		323
	Department <*Dept*>	[0..1]	Text		323
	EmailAddress <*EmailAdr*>	[0..1]	Text		323
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			323
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324
	Other <*Othr*>	[0..*]	±		324
	AddressVerification <*AdrVrfctn*>	[0..1]			324
	AddressDigits <*AdrDgts*>	[0..1]	Text		324
	PostalCodeDigits <*PstlCdDgts*>	[0..1]	Text		325
	AuthenticationType <*AuthntcnTp*>	[0..1]	Text		325

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AuthenticationLevel <*AuthntcnLvl*>	[0..1]	Text		325
	AuthenticationResult <*AuthntcnRslt*>	[0..1]	CodeSet		325
	AuthenticationAdditionalInformation <*AuthntcnAddtlInf*>	[0..1]			325
	Identification <*Id*>	[1..1]	Text		326
	Value <*Val*>	[0..1]	Binary		326
	ProtectedValue <*PrtctdVal*>	[0..1]	±		326
	Type <*Tp*>	[0..1]	Text		326
	TransactionVerificationResult <*TxVrfctnRslt*>	[0..*]			326
	Method <*Mtd*>	[1..1]	CodeSet		327
	VerificationEntity <*VrfctnNtty*>	[0..1]	CodeSet		328
	Result <*Rslt*>	[0..1]	CodeSet		328
	AdditionalResult <*AddtlRslt*>	[0..1]	Text		328
	PersonalData <*PrsnlData*>	[0..1]	Text		329
	MobileData <*MobData*>	[0..*]			329
	MobileCountryCode <*MobCtryCd*>	[0..1]	Text		329
	MobileNetworkCode <*MobNtwkCd*>	[0..1]	Text		329
	MobileMaskedMSISDN <*MobMskdMSISDN*>	[0..1]	Text		330
	Geolocation <*Glctn*>	[0..1]			330
	GeographicCoordinates <*GeogcCordints*>	[0..1]			330
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330
	UTMCoordinates <*UTMCordints*>	[0..1]			331
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331
	SensitiveMobileData <*SnstvMobData*>	[0..1]			331
	MSISDN <*MSISDN*>	[1..1]	Text		332
	IMSI <*IMSI*>	[0..1]	Text		332
	IMEI <*IMEI*>	[0..1]	Text		332
	ProtectedMobileData <*PrtctdMobData*>	[0..1]	±		332
	ProtectedCardholderData <*PrtctdCrdhldrData*>	[0..1]	±		332

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SaleEnvironment <*SaleEnvt*>	[0..1]			333
	SaleCapabilities <*SaleCpblties*>	[0..*]	CodeSet		333
	Currency <*Ccy*>	[0..1]	CodeSet	C1	334
	MinimumAmountToDeliver <*MinAmtToDlvr*>	[0..1]	Amount		334
	MaximumCashBackAmount <*MaxCshBckAmt*>	[0..1]	Amount		334
	MinimumSplitAmount <*MinSpltAmt*>	[0..1]	Amount		335
	DebitPreferredFlag <*DbtPrefrdFlg*>	[0..1]	Indicator		335
	LoyaltyHandling <*LltyHdlg*>	[0..1]	CodeSet		335

9.1.2.2.2 Context <Cntxt>

Presence: [0..1]

Definition: Context in which the transaction is performed (payment and sale).

Context <Cntxt> contains the following elements (see "CardPaymentContext29" on page 354 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PaymentContext <*PmtCntxt*>	[0..1]			357
	CardPresent <*CardPres*>	[0..1]	Indicator		357
	CardholderPresent <*CrdhldrPres*>	[0..1]	Indicator		357
	OnLineContext <*OnLineCntxt*>	[0..1]	Indicator		358
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		358
	TransactionEnvironment <*TxEnvt*>	[0..1]	CodeSet		358
	TransactionChannel <*TxChanl*>	[0..1]	CodeSet		358
	BusinessArea <*BizArea*>	[0..1]	CodeSet		359
	AttendantMessageCapable <*AttndntMsgCpbl*>	[0..1]	Indicator		359
	AttendantLanguage <*AttndntLang*>	[0..1]	CodeSet	C6	359
	CardDataEntryMode <*CardDataNtryMd*>	[0..1]	CodeSet		360
	FallbackIndicator <*FllbckInd*>	[0..1]	CodeSet		360
	SupportedOption <*SpprtdOptn*>	[0..*]	CodeSet		361
	SaleContext <*SaleCntxt*>	[0..1]			361
	SaleIdentification <*SaleId*>	[0..1]	Text		362
	SaleReferenceNumber <*SaleRefNb*>	[0..1]	Text		362
	SaleReconciliationIdentification <*SaleRcncltnId*>	[0..1]	Text		363
	CashierIdentification <*CshrId*>	[0..1]	Text		363
	CashierLanguage <*CshrLang*>	[0..*]	CodeSet	C6	363
	ShiftNumber <*ShftNb*>	[0..1]	Text		363
	CustomerOrderRequestFlag <*CstmrOrdrReqFlg*>	[0..1]	Indicator		363
	PurchaseOrderNumber <*PurchsOrdrNb*>	[0..1]	Text		363
	InvoiceNumber <*InvcNb*>	[0..1]	Text		363
	DeliveryNoteNumber <*DlvryNoteNb*>	[0..1]	Text		364
	SponsoredMerchant <*SpnsrdMrchnt*>	[0..*]			364
	CommonName <*CmonNm*>	[1..1]	Text		364
	Address <*Adr*>	[0..1]	Text		364
	CountryCode <*CtryCd*>	[1..1]	CodeSet		364
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		364
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		364

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SplitPayment <*SpltPmt*>	[0..1]	Indicator		365
	RemainingAmount <*RmngAmt*>	[0..1]	Amount		365
	ForceOnlineFlag <*ForceOnlnFlg*>	[0..1]	Indicator		365
	ReuseCardDataFlag <*ReuseCardDataFlg*>	[0..1]	Indicator		365
	AllowedEntryMode <*AllwdNtryMd*>	[0..*]	CodeSet		365
	SaleTokenScope <*SaleTknScp*>	[0..1]	CodeSet		366
	AdditionalSaleData <*AddtlSaleData*>	[0..1]	Text		366
	DirectDebitContext <*DrctDbtCntxt*>	[0..1]			366
	DebtorIdentification <*DbtrId*>	[0..1]			367
	Debtor <*Dbtr*>	[0..1]			368
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	368
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		369
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			369
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369
	AccountIdentification <*AcctId*>	[0..1]			370
{Or	IBAN <*IBAN*>	[1..1]	IdentifierSet	C4	370
Or	BBAN <*BBAN*>	[1..1]	IdentifierSet		370
Or	UPIC <*UPIC*>	[1..1]	IdentifierSet		371
Or}	DomesticAccount <*DmstAcct*>	[1..1]			371
	Identification <*Id*>	[1..1]	Text		371
	CreditorIdentification <*CdtrId*>	[1..1]			371
	Creditor <*Cdtr*>	[1..1]			372
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	372
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		372
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			372
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373
	RegistrationIdentification <*RegnId*>	[0..1]	Text		373
	MandateRelatedInformation <*MndtRltdInf*>	[1..1]			373
	MandateIdentification <*MndtId*>	[1..1]	Text		374

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DateOfSignature <*DtOfSgntr*>	[0..1]	Date		374
	MandateImage <*MndtImg*>	[0..1]	Binary		374

9.1.2.2.3 ServiceContent <SvcCntt>

Presence: [1..1]

Definition: Define the type of service answered.

Datatype: "RetailerService9Code" on page 504

CodeName	Name	Definition
DDYP	DeviceDisplayResponse	One system responds to the other system for a display request.
DINP	DeviceInputResponse	One system responds to the other System for a input request.
DPRP	DevicePrintResponse	One system responds to the other System for a print request.
DSOP	DevicePlaySoundResponse	One system responds to the other System for a play sound request.
DSIP	DeviceSecureInputResponse	One system responds to the other System for secure data input.
DCIP	DeviceInitialisationCardReaderResponse	The POI system responds to the Sale System for a card reader initialisation.
DCAP	DeviceSendApplicationProtocolDataUnitCardReaderResponse	The POI system responds to the Sale System for a card reader Application Protocol Data Unit sending.
DCPP	DevicePowerOffCardRequestResponse	The POI system responds to the Sale System for a card reader power off.
DCOP	DeviceTransmissionMessageResponse	The POI system responds to the Sale System after a message transmission.

9.1.2.2.4 DisplayResponse <DispRspn>

Presence: [0..1]

Definition: Content of the Display Response message.

DisplayResponse <DispRspn> contains the following **DeviceDisplayResponse2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	OutputResult <*OutptRslt*>	[1..*]			178
	DeviceType <*DvcTp*>	[1..1]	CodeSet		178
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		178
	Response <*Rspn*>	[1..1]	±		179

9.1.2.2.4.1 OutputResult <OutptRslt>

Presence: [1..*]

Definition: Give result for display request.

OutputResult <OutptRslt> contains the following **OutputResult2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DeviceType <*DvcTp*>	[1..1]	CodeSet		178
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		178
	Response <*Rspn*>	[1..1]	±		179

9.1.2.2.4.1.1 DeviceType <DvcTp>

Presence: [1..1]

Definition: Logical device located on a Sale Terminal or a POI Terminal, in term of class of information to output.

Datatype: "UserInterface4Code" on page 512

CodeName	Name	Definition
CDSP	CardholderDisplay	Cardholder display or interface.
CRCP	CardholderReceipt	Cardholder receipt.
MDSP	MerchantDisplay	Merchant display or interface.
MRCP	MerchantReceipt	Merchant receipt.
CRDO	OtherCardholderInterface	Other interface of the cardholder, for instance e-mail or smartphone message.

9.1.2.2.4.1.2 InformationQualifier <InfQlfr>

Presence: [1..1]

Definition: Qualification of the information to sent to an output logical device.

Datatype: "InformationQualify1Code" on page 487

CodeName	Name	Definition
CUSA	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
DISP	Display	Standard display interface.
DOCT	Document	When the POI System wants to print specific document (check, dynamic currency conversion ...). Used by the Sale System when the printer is not located on the Sale System.
ERRO	Error	The information is related to an error situation occurring on the message sender.
INPT	Input	Answer to a question or information to be entered by the Cashier or the

CodeName	Name	Definition
		Customer, at the request of the POI Terminal or the Sale Terminal.
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
RCPT	Receipt	Where you print the Payment receipt that could be located on the Sale System or in some cases a restricted Sale ticket on the POI Terminal.
SOND	Sound	Standard sound interface.
STAT	Status	The information is a new state on which the message sender is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
VCHR	Voucher	Coupons, voucher or special ticket generated by the POI or the Sale System and to be printed.

9.1.2.2.4.1.3 Response <Rspn>

Presence: [1..1]

Definition: Gives response for each peripheral.

Response <Rspn> contains the following elements (see "ResponseType11" on page 374 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Response <*Rspn*>	[1..1]	CodeSet		374
	ResponseReason <*RspnRsn*>	[0..1]	CodeSet		374
	AdditionalResponseInformation <*AddtlRspnInf*>	[0..1]	Text		376

9.1.2.2.5 InputResponse <InptRspn>

Presence: [0..1]

Definition: Content of the Input Response message.

InputResponse <InptRspn> contains the following **DeviceInputResponse4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	OutputResult <*OutptRslt*>	[0..1]			180
	DeviceType <*DvcTp*>	[1..1]	CodeSet		180
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		181
	Response <*Rspn*>	[1..1]	±		182
	InputResult <*InptRslt*>	[1..1]			182
	DeviceType <*DvcTp*>	[1..1]	CodeSet		182
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		183
	InputResultData <*InptRsltData*>	[1..1]			183
	InputCommand <*InptCmd*>	[1..1]	CodeSet		184
	ConfirmedFlag <*ConfdFlg*>	[0..1]	Indicator		185
	FunctionKey <*FctnKey*>	[0..1]	Quantity		185
	InputMessage <*InptMsg*>	[0..1]	Text		185
	Password <*Pwd*>	[0..1]	±		185
	ImageCapturedSignature <*ImgCaptrdSgntr*>	[0..1]			186
	ImageFormat <*ImgFrmt*>	[1..1]	Text		186
	ImageData <*ImgData*>	[0..1]	Binary		186
	ImageReference <*ImgRef*>	[0..1]	Text		186
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		186

9.1.2.2.5.1 OutputResult <OutptRslt>

Presence: [0..1]

Definition: Result of display request.

OutputResult <OutptRslt> contains the following **OutputResult2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DeviceType <*DvcTp*>	[1..1]	CodeSet		180
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		181
	Response <*Rspn*>	[1..1]	±		182

9.1.2.2.5.1.1 DeviceType <DvcTp>

Presence: [1..1]

Definition: Logical device located on a Sale Terminal or a POI Terminal, in term of class of information to output.

Datatype: "UserInterface4Code" on page 512

CodeName	Name	Definition
CDSP	CardholderDisplay	Cardholder display or interface.
CRCP	CardholderReceipt	Cardholder receipt.
MDSP	MerchantDisplay	Merchant display or interface.
MRCP	MerchantReceipt	Merchant receipt.
CRDO	OtherCardholderInterface	Other interface of the cardholder, for instance e-mail or smartphone message.

9.1.2.2.5.1.2 InformationQualifier <InfQlfr>

Presence: [1..1]

Definition: Qualification of the information to sent to an output logical device.

Datatype: "InformationQualify1Code" on page 487

CodeName	Name	Definition
CUSA	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
DISP	Display	Standard display interface.
DOCT	Document	When the POI System wants to print specific document (check, dynamic currency conversion ...). Used by the Sale System when the printer is not located on the Sale System.
ERRO	Error	The information is related to an error situation occurring on the message sender.
INPT	Input	Answer to a question or information to be entered by the Cashier or the Customer, at the request of the POI Terminal or the Sale Terminal.
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
RCPT	Receipt	Where you print the Payment receipt that could be located on the Sale System or in some cases a restricted Sale ticket on the POI Terminal.
SOND	Sound	Standard sound interface.
STAT	Status	The information is a new state on which the message sender is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
VCHR	Voucher	Coupons, voucher or special ticket generated by the POI or the Sale System and to be printed.

9.1.2.2.5.1.3 Response <Rspn>

Presence: [1..1]

Definition: Gives response for each peripheral.

Response <Rspn> contains the following elements (see "ResponseType11" on page 374 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Response <*Rspn*>	[1..1]	CodeSet		374
	ResponseReason <*RspnRsn*>	[0..1]	CodeSet		374
	AdditionalResponseInformation <*AddtlRspnInf*>	[0..1]	Text		376

9.1.2.2.5.2 InputResult <InptRslt>

Presence: [1..1]

Definition: Result of input request.

InputResult <InptRslt> contains the following **InputResult4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DeviceType <*DvcTp*>	[1..1]	CodeSet		182
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		183
	InputResultData <*InptRsltData*>	[1..1]			183
	InputCommand <*InptCmd*>	[1..1]	CodeSet		184
	ConfirmedFlag <*ConfdFlg*>	[0..1]	Indicator		185
	FunctionKey <*FctnKey*>	[0..1]	Quantity		185
	InputMessage <*InptMsg*>	[0..1]	Text		185
	Password <*Pwd*>	[0..1]	±		185
	ImageCapturedSignature <*ImgCaptrdSgntr*>	[0..1]			186
	ImageFormat <*ImgFrmt*>	[1..1]	Text		186
	ImageData <*ImgData*>	[0..1]	Binary		186
	ImageReference <*ImgRef*>	[0..1]	Text		186
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		186

9.1.2.2.5.2.1 DeviceType <DvcTp>

Presence: [1..1]

Definition: Type of Input device.

Datatype: "SaleCapabilities2Code" on page 505

CodeName	Name	Definition
CHIN	CashierInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI

CodeName	Name	Definition
		System (InputCommand data element). The output device attached to this input device is the CashierDisplay device.
CUIN	CustomerInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element).

9.1.2.2.5.2.2 InformationQualifier <InfQlfr>

Presence: [1..1]

Definition: Qualifies the type of given information.

Datatype: "InformationQualify1Code" on page 487

CodeName	Name	Definition
CUSA	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
DISP	Display	Standard display interface.
DOCT	Document	When the POI System wants to print specific document (check, dynamic currency conversion ...). Used by the Sale System when the printer is not located on the Sale System.
ERRO	Error	The information is related to an error situation occurring on the message sender.
INPT	Input	Answer to a question or information to be entered by the Cashier or the Customer, at the request of the POI Terminal or the Sale Terminal.
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
RCPT	Receipt	Where you print the Payment receipt that could be located on the Sale System or in some cases a restricted Sale ticket on the POI Terminal.
SOND	Sound	Standard sound interface.
STAT	Status	The information is a new state on which the message sender is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
VCHR	Voucher	Coupons, voucher or special ticket generated by the POI or the Sale System and to be printed.

9.1.2.2.5.2.3 InputResultData <InptRsltData>

Presence: [1..1]

Definition: Data resulting of input after POI or Sale processing.

InputResultData <InptRsltData> contains the following **InputResultData4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	InputCommand <*InptCmd*>	[1..1]	CodeSet		184
	ConfirmedFlag <*ConfdFlg*>	[0..1]	Indicator		185
	FunctionKey <*FctnKey*>	[0..1]	Quantity		185
	InputMessage <*InptMsg*>	[0..1]	Text		185
	Password <*Pwd*>	[0..1]	±		185
	ImageCapturedSignature <*ImgCaptrdSgntr*>	[0..1]			186
	ImageFormat <*ImgFrmt*>	[1..1]	Text		186
	ImageData <*ImgData*>	[0..1]	Binary		186
	ImageReference <*ImgRef*>	[0..1]	Text		186
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		186

9.1.2.2.5.2.3.1 InputCommand <InptCmd>

Presence: [1..1]

Definition: Type of processed input.

Datatype: "InputCommand1Code" on page 487

CodeName	Name	Definition
DCSG	DecimalString	Wait for a string of digit characters with a decimal point, the length range could be specified.
DGSG	DigitString	Wait for a string of digit characters.
GAKY	GetAnyKey	Wait for a key pressed on the Terminal, to be able to read the message displayed on the Terminal.
GCNF	GetConfirmation	Wait for a confirmation Yes (Y) or No (N) on the Sale System. Wait for a confirmation (Valid or Cancel button) on the POI Terminal. The result of the command is a Boolean: True or False.
GFKY	GetFunctionKey	Wait for a function key pressed on the Terminal: From POI, Valid, Clear, Correct, Generic Function key number. From Sale, Generic Function key.
GMNE	GetMenuEntry	To choose an entry among a list of entries (all of them are not necessary selectable). The OutputFormat has to be MenuEntry.
PSWD	Password	Request to enter a password with masked characters while typing the password.

CodeName	Name	Definition
SITE	SiteManager	Wait for a confirmation Yes (Y) or No (N) of the Site Manager on the Sale System.
TXSG	TextString	Wait for a string of alphanumeric characters.
HTML	XHTMLText	Wait for a XHTML data.
SIGN	Signature	Request to wait for signature.

9.1.2.2.5.2.3.2 ConfirmedFlag <ConfdFlg>

Presence: [0..1]

Definition: Flag of notification of card to be entered in the POI card reader.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.2.2.5.2.3.3 FunctionKey <FctnKey>

Presence: [0..1]

Definition: The number of the function key which is typed by the Customer on the POI system or the Cashier on the Sale System.

Datatype: "Number" on page 515

9.1.2.2.5.2.3.4 InputMessage <InptMsg>

Presence: [0..1]

Definition: The input text and data given by the POI or the Sale System.

Datatype: "Max20000Text" on page 517

9.1.2.2.5.2.3.5 Password <Pwd>

Presence: [0..1]

Definition: An enciphered password typed by the Customer on the POI system or the Cashier on the Sale system.

Password <Pwd> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.2.2.5.2.3.6 ImageCapturedSignature <ImgCaptrdSgntr>

Presence: [0..1]

Definition: Numeric value of a handwritten signature.

ImageCapturedSignature <ImgCaptrdSgntr> contains the following **CapturedSignature1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ImageFormat <*ImgFrmt*>	[1..1]	Text		186
	ImageData <*ImgData*>	[0..1]	Binary		186
	ImageReference <*ImgRef*>	[0..1]	Text		186
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		186

9.1.2.2.5.2.3.6.1 ImageFormat <ImgFrmt>

Presence: [1..1]

Definition: Format of the image.

Datatype: "Max35Text" on page 519

9.1.2.2.5.2.3.6.2 ImageData <ImgData>

Presence: [0..1]

Definition: Data of the image.

Datatype: "Max2MBBinary" on page 462

9.1.2.2.5.2.3.6.3 ImageReference <ImgRef>

Presence: [0..1]

Definition: URL or name of the image.

Datatype: "Max500Text" on page 519

9.1.2.2.5.2.3.6.4 AdditionalInformation <AddtlInf>

Presence: [0..1]

Definition: Additional information for the image.

Datatype: "Max140Text" on page 517

9.1.2.2.6 PrintResponse <PrtRspn>

Presence: [0..1]

Definition: Content of the Print Response message.

PrintResponse <PrtRspn> contains the following **DevicePrintResponse1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		186

9.1.2.2.6.1 DocumentQualifier <DocQlfr>

Presence: [1..1]

Definition: Qualification of the document printed to the Cashier or the Customer.

Datatype: "DocumentType7Code" on page 484

CodeName	Name	Definition
JNRL	Journal	When the POI or the Sale System wants to store a message on the journal printer or electronic journal of the Sale Terminal (it is sometimes a Sale Logging/Journal Printer).
CRCP	CustomerReceipt	When the Sale System requires the POI system to print the Customer receipt.
HRCP	CashierReceipt	When the Sale system print the Cashier copy of the Payment receipt.
SRCP	SaleReceipt	When the Sale System requires the POI system to print the Sale receipt.
RPIN	RelatedPaymentInstruction	Document is a linked payment instruction to which the current payment instruction is related, for example, in a cover scenario.
VCHR	Voucher	Document is an electronic payment document.

9.1.2.2.7 SecureInputResponse <ScrInptRspn>

Presence: [0..1]

Definition: Response to a secure input request.

SecureInputResponse <ScrInptRspn> contains the following **DeviceSecureInputResponse4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardholderPIN <*CrdhldrPIN*>	[0..1]			187
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		188
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		188
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		188

9.1.2.2.7.1 CardholderPIN <CrdhldrPIN>

Presence: [0..1]

Definition: Cardholder PIN data when needed.

CardholderPIN <CrdhldrPIN> contains the following **OnLinePIN9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		188
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		188
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		188

9.1.2.2.7.1.1 EncryptedPINBlock <NcrptdPINBlck>

Presence: [1..1]

Definition: Encrypted PIN (Personal Identification Number).

EncryptedPINBlock <NcrptdPINBlck> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.2.2.7.1.2 PINFormat <PINFrmt>

Presence: [1..1]

Definition: PIN (Personal Identification Number) format before encryption.

Datatype: "PINFormat3Code" on page 496

CodeName	Name	Definition
ISO0	ISO0	PIN diversified with the card account number, conforming to the standard ISO 9564-2.
ISO1	ISO1	PIN completed with random padding characters, conforming to the standard ISO 9564-2.
ISO2	ISO2	PIN without diversification characters, conforming to the standard ISO 9564-2.
ISO3	ISO3	PIN diversified with the card account number and random characters, conforming to the standard ISO 9564-2.
ISO4	ISO4	PIN format used with AES encryption, conforming to the new ISO SC2 format.
ISO5	ISO5	Alternative PIN format used with AES encryption, conforming to the new ISO SC2 format.

9.1.2.2.7.1.3 AdditionalInput <AddtlInpt>

Presence: [0..1]

Definition: Additional information required to verify the PIN (Personal Identification Number).

Datatype: "Max35Text" on page 519

9.1.2.2.8 InitialisationCardReaderResponse <InitlstnCardRdrRspn>

Presence: [0..1]

Definition: Content received after a card initialisation.

InitialisationCardReaderResponse <InitlstnCardRdrRspn> contains the following **DeviceInitialisationCardReaderResponse2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardEntryMode <*CardNtryMd*>	[0..1]	CodeSet		189
	ICCResetData <*ICCRstData*>	[0..1]			189
	ATRValue <*ATRVal*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[0..1]	Binary		190
	AdditionalInformation <*AddtlInf*>	[0..1]	Binary		190

9.1.2.2.8.1 CardEntryMode <CardNtryMd>

Presence: [0..1]

Definition: Payment instrument entry mode requested by the Sale System.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.2.2.8.2 ICCResetData <ICCRstData>

Presence: [0..1]

Definition: Data of a Chip Card related to the reset of the chip.

ICCResetData <ICCRstData> contains the following **ICCResetData1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ATRValue <*ATRVal*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[0..1]	Binary		190

9.1.2.2.8.2.1 ATRValue <ATRVal>

Presence: [0..1]

Definition: Value of the Answer To Reset of a chip card.

Datatype: "Max140Binary" on page 461

9.1.2.2.8.2.2 CardStatus <CardSts>

Presence: [0..1]

Definition: Status of a smartcard response to a command (SW1-SW2).

Datatype: "Max35Binary" on page 462

9.1.2.2.8.3 AdditionalInformation <AddtlInf>

Presence: [0..1]

Definition: Additional information about the Device Initialisation Card Reader Response.

Datatype: "Max10000Binary" on page 461

9.1.2.2.9 CardReaderApplicationProtocolDataUnitResponse <CardRdrApplPrtcolDataUnitRspn>

Presence: [0..1]

Definition: Content of the Card Reader APDU (Application Protocol Data Unit) response message.

CardReaderApplicationProtocolDataUnitResponse <CardRdrApplPrtcolDataUnitRspn> contains the following **DeviceSendApplicationProtocolDataUnitCardReaderResponse1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Data <*Data*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[1..1]	Binary		190

9.1.2.2.9.1 Data <Data>

Presence: [0..1]

Definition: Class field of the Application Protocol Data Unit command (CLA).

Datatype: "Min1Max256Binary" on page 463

9.1.2.2.9.2 CardStatus <CardSts>

Presence: [1..1]

Definition: Status of a smartcard response to a command (SW1-SW2). Reference: ISO 7816-4.

Datatype: "Min1Max256Binary" on page 463

9.1.2.2.10 TransmissionResponse <TrnsmssnRspn>

Presence: [0..1]

Definition: Content of the Transmit Response message.

TransmissionResponse <TrnsmssnRspn> contains the following **DeviceTransmitMessageResponse1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ReceivedMessage <*RcvdMsg*>	[0..1]	Binary		191

9.1.2.2.10.1 ReceivedMessage <RcvdMsg>

Presence: [0..1]

Definition: Content of a transmitted message.

Datatype: "Max100KBinary" on page 461

9.1.2.2.11 Response <Rspn>

Presence: [1..1]

Definition: Result of the processing of the request.

Response <Rspn> contains the following elements (see "ResponseType11" on page 374 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Response <*Rspn*>	[1..1]	CodeSet		374
	ResponseReason <*RspnRsn*>	[0..1]	CodeSet		374
	AdditionalResponseInformation <*AddtlRspnInf*>	[0..1]	Text		376

9.1.2.2.12 SupplementaryData <SplmtryData>

Presence: [0..*]

Definition: Additional information incorporated as an extension to the message.

Impacted by: C5 "SupplementaryDataRule"

SupplementaryData <SplmtryData> contains the following elements (see "SupplementaryData1" on page 256 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PlaceAndName <*PlcAndNm*>	[0..1]	Text		256
	Envelope <*Envlp*>	[1..1]	(External Schema)		256

Constraints

- **SupplementaryDataRule**

  This component may not be used without the explicit approval of a SEG and submission to the RA of ISO 20022 compliant structure(s) to be used in the Envelope element.

9.1.3 Address

9.1.3.1 CommunicationAddress9

Definition: Communication information.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PostalAddress <*PstlAdr*>	[0..1]	±		192
	Email <*Email*>	[0..1]	Text		192
	URLAddress <*URLAdr*>	[0..1]	Text		193
	Phone <*Phne*>	[0..1]	Text		193
	CustomerService <*CstmrSvc*>	[0..1]	Text		193
	AdditionalContactInformation <*AddtlCtctInf*>	[0..1]	Text		193

9.1.3.1.1 PostalAddress <PstlAdr>

Presence: [0..1]

Definition: Postal address of the entity.

PostalAddress <PstlAdr> contains the following elements (see "PostalAddress22" on page 398 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AddressType <*AdrTp*>	[0..1]	CodeSet		399
	Department <*Dept*>	[0..1]	Text		399
	SubDepartment <*SubDept*>	[0..1]	Text		399
	AddressLine <*AdrLine*>	[0..2]	Text		399
	StreetName <*StrtNm*>	[0..1]	Text		400
	BuildingNumber <*BldgNb*>	[0..1]	Text		400
	PostCode <*PstCd*>	[0..1]	Text		400
	TownName <*TwnNm*>	[0..1]	Text		400
	CountrySubDivision <*CtrySubDvsn*>	[0..2]	Text		400
	CountryCode <*CtryCd*>	[0..1]	Text		400

9.1.3.1.2 Email <Email>

Presence: [0..1]

Definition: Address for electronic mail (e-mail).

Datatype: "Max256Text" on page 518

9.1.3.1.3 URLAddress <URLAdr>

Presence: [0..1]

Definition: Address for the Universal Resource Locator (URL), for example used over the www (HTTP) service.

Datatype: "Max256Text" on page 518

9.1.3.1.4 Phone <Phne>

Presence: [0..1]

Definition: Collection of information that identifies a phone number, as defined by telecom services.

Datatype: "PhoneNumber" on page 522

9.1.3.1.5 CustomerService <CstmrSvc>

Presence: [0..1]

Definition: Phone number of the customer service.

Datatype: "PhoneNumber" on page 522

9.1.3.1.6 AdditionalContactInformation <AddtlCtctInf>

Presence: [0..1]

Definition: Additional information used to facilitate contact with the card acceptor, for instance sales agent name, dispute manager name.

Datatype: "Max256Text" on page 518

9.1.4 Card

9.1.4.1 PlainCardData15

Definition: Sensible data associated with the payment card performing the transaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PAN <*PAN*>	[1..1]	Text		194
	CardSequenceNumber <*CardSeqNb*>	[0..1]	Text		194
	EffectiveDate <*FctvDt*>	[0..1]	Text		194
	ExpiryDate <*XpryDt*>	[1..1]	Text		194
	ServiceCode <*SvcCd*>	[0..1]	Text		194
	Track1 <*Trck1*>	[0..1]	Text		194
	Track2 <*Trck2*>	[0..1]	Text		194
	Track3 <*Trck3*>	[0..1]	Text		194
	CardholderName <*CrdhldrNm*>	[0..1]	Text		195

9.1.4.1.1 PAN <PAN>

Presence: [1..1]

Definition: Primary Account Number (PAN) of the card, or surrogate of the PAN by a payment token.

Datatype: "Min8Max28NumericText" on page 522

9.1.4.1.2 CardSequenceNumber <CardSeqNb>

Presence: [0..1]

Definition: Identify a card or a payment token inside a set of cards with the same PAN or token.

Datatype: "Min2Max3NumericText" on page 521

9.1.4.1.3 EffectiveDate <FctvDt>

Presence: [0..1]

Definition: Date from which the card can be used, expressed either in the YYYY-MM format, or in the YYYY-MM-DD format.

Datatype: "Max10Text" on page 516

9.1.4.1.4 ExpiryDate <XpryDt>

Presence: [1..1]

Definition: Expiry date of the card or the payment token expressed either in the YYYY-MM format, or in the YYYY-MM-DD format.

Datatype: "Max10Text" on page 516

9.1.4.1.5 ServiceCode <SvcCd>

Presence: [0..1]

Definition: Services attached to the card, as defined in ISO 7813.

Datatype: "Exact3NumericText" on page 516

9.1.4.1.6 Track1 <Trck1>

Presence: [0..1]

Definition: ISO track 1 issued from the magnetic stripe card or from the ICC if the magnetic stripe was not read. The format is conform to ISO 7813, removing beginning and ending sentinels and longitudinal redundancy check characters.

Datatype: "Max76Text" on page 520

9.1.4.1.7 Track2 <Trck2>

Presence: [0..1]

Definition: ISO track 2 issued from the magnetic stripe card or from the ICC if the magnetic stripe was not read. The content is conform to ISO 7813, removing beginning and ending sentinels and longitudinal redundancy check characters.

Datatype: "Max37Text" on page 519

9.1.4.1.8 Track3 <Trck3>

Presence: [0..1]

Definition: ISO track 3 issued from the magnetic stripe card or from the ICC if the magnetic stripe was not read. The content is conform to ISO 4909, removing beginning and ending sentinels and longitudinal redundancy check characters.

Datatype: "Max104Text" on page 516

9.1.4.1.9 CardholderName <CrdhldrNm>

Presence: [0..1]

Definition: Name of the cardholder stored on the card.

Datatype: "Max45Text" on page 519

9.1.5 Configuration

9.1.5.1 HostCommunicationParameter6

Definition: Configuration parameters to communicate with a host.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		195
	HostIdentification <*HstId*>	[1..1]	Text		196
	Address <*Adr*>	[0..1]	±		196
	Key <*Key*>	[0..*]			196
	KeyIdentification <*KeyId*>	[1..1]	Text		197
	KeyVersion <*KeyVrsn*>	[1..1]	Text		197
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		197
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		197
	Type <*Tp*>	[0..1]	CodeSet		197
	Function <*Fctn*>	[0..*]	CodeSet		198
	NetworkServiceProvider <*NtwkSvcPrvdr*>	[0..1]	±		199
	PhysicalInterface <*PhysIntrfc*>	[0..1]			199
	InterfaceName <*IntrfcNm*>	[1..1]	Text		200
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		200
	UserName <*UsrNm*>	[0..1]	Text		200
	AccessCode <*AccsCd*>	[0..1]	Binary		200
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		201
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		201

9.1.5.1.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.1.2 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification of the host.

Datatype: "Max35Text" on page 519

9.1.5.1.3 Address <Adr>

Presence: [0..1]

Definition: Network parameters of the host.

Address <Adr> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.5.1.4 Key <Key>

Presence: [0..*]

Definition: Cryptographic key used to communicate with the host.

Key <Key> contains the following **KEKIdentifier5** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		197
	KeyVersion <*KeyVrsn*>	[1..1]	Text		197
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		197
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		197
	Type <*Tp*>	[0..1]	CodeSet		197
	Function <*Fctn*>	[0..*]	CodeSet		198

9.1.5.1.4.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 517

9.1.5.1.4.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 517

9.1.5.1.4.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 515

9.1.5.1.4.4 DerivationIdentification <DerivtnId>

Presence: [0..1]

Definition: Identification used for derivation of a unique key from a master key provided for the data protection.

Datatype: "Min5Max16Binary" on page 463

9.1.5.1.4.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 481

CodeName	Name	Definition
AES2	AES128	AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

CodeName	Name	Definition
EDE3	DES112	Data encryption standard key of 112 bits (without the parity bits).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.
AES9	AES192	AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
AES5	AES256	AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

9.1.5.1.4.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 488

CodeName	Name	Definition
ENCR	Encryption	Key may encrypt.
DCPT	Decryption	Key may decrypt.
DENC	DataEncryption	Key may encrypt data.
DDEC	DataDecryption	Key may decrypt data.
TRNI	TranslateInput	Key may encrypt information before translation.
TRNX	TranslateOutput	Key may encrypt information after translation.
MACG	MessageAuthenticationCodeGeneration	Key may generate message authentication codes (MAC).
MACV	MessageAuthenticationCodeVerification	Key may verify message authentication codes (MAC).
SIGG	SignatureGeneration	Key may generate digital signatures.
SUGV	SignatureVerification	Key may verify digital signatures.
PINE	PINEncryption	Key may encrypt personal identification numbers (PIN).
PIND	PINDecryption	Key may decrypt personal identification numbers (PIN).
PINV	PINVerification	Key may verify personal identification numbers (PIN).

CodeName	Name	Definition
KEYG	KeyGeneration	Key may generate keys.
KEYI	KeyImport	Key may import keys.
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

9.1.5.1.5 NetworkServiceProvider <NtwkSvcPrvdr>

Presence: [0..1]

Definition: Access information to reach an intermediate network service provider.

NetworkServiceProvider <NtwkSvcPrvdr> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.5.1.6 PhysicalInterface <PhysIntrfc>

Presence: [0..1]

Definition: Physical Interface where the host is connected.

PhysicalInterface <PhysIntrfc> contains the following **PhysicalInterfaceParameter1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	InterfaceName <*IntrfcNm*>	[1..1]	Text		200
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		200
	UserName <*UsrNm*>	[0..1]	Text		200
	AccessCode <*AccsCd*>	[0..1]	Binary		200
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		201
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		201

9.1.5.1.6.1 InterfaceName <IntrfcNm>

Presence: [1..1]

Definition: Identification of the interface.

Datatype: "Max35Text" on page 519

9.1.5.1.6.2 InterfaceType <IntrfcTp>

Presence: [0..1]

Definition: Identification of the physical link layer.

Datatype: "POICommunicationType2Code" on page 497

CodeName	Name	Definition
BLTH	Bluetooth	Communication with a host using Bluetooth.
ETHR	Ethernet	Ethernet port to communicate.
GPRS	GPRS	Communication with a host using GPRS.
GSMF	GSM	Communication with a host using GSM.
PSTN	PSTN	Communication with a host using Public Switching Telephone Network.
RS23	RS232	Serial port to communicate.
USBD	USBDevice	Communication with a USB stick or any USB device.
USBH	USBHost	Communication with a host from an USB port.
WIFI	Wifi	Wifi communication with another component.
WT2G	WirelessTechnology2G	Includes all communication technologies which can be qualified as being part of the 2G technology (e.g EDGE or PDC).
WT3G	WirelessTechnology3G	Includes all communication technologies which can be qualified as being part of the 3G technology.
WT4G	WirelessTechnology4G	Includes all communication technologies which can be qualified as being part of the 4G technology.
WT5G	WirelessTechnology5G	Includes all communication technologies which can be qualified as being part of the 5G technology.

9.1.5.1.6.3 UserName <UsrNm>

Presence: [0..1]

Definition: Optional user name to provide to use this interface.

Datatype: "Max35Text" on page 519

9.1.5.1.6.4 AccessCode <AccsCd>

Presence: [0..1]

Definition: Optional access code to provide to use this interface.

Datatype: "Max35Binary" on page 462

9.1.5.1.6.5 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the optional security profile to use with this interface.

Datatype: "Max35Text" on page 519

9.1.5.1.6.6 AdditionalParameters <AddtlParams>

Presence: [0..1]

Definition: Any other parameters relevant for this interface.

Datatype: "Max2KBinary" on page 462

9.1.5.2 SaleToPOIProtocolParameter2

Definition: Configuration parameters to communicate with a sale system.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		201
	MerchantIdentification <*MrchntId*>	[0..1]			202
	CommonName <*CmonNm*>	[1..1]	Text		202
	Address <*Adr*>	[0..1]	Text		202
	CountryCode <*CtryCd*>	[1..1]	CodeSet		202
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		202
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		202
	Version <*Vrsn*>	[1..1]	Text		203
	HostIdentification <*HstId*>	[1..1]	Text		203
	MerchantPOIIdentification <*MrchntPOIId*>	[0..1]	Text		203
	SaleIdentification <*SaleId*>	[0..1]	Text		203
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		203

9.1.5.2.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.

CodeName	Name	Definition
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.2.2 MerchantIdentification <MrchntId>

Presence: [0..1]

Definition: Identification of the merchant.

MerchantIdentification <MrchntId> contains the following **Organisation26** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CommonName <*CmonNm*>	[1..1]	Text		202
	Address <*Adr*>	[0..1]	Text		202
	CountryCode <*CtryCd*>	[1..1]	CodeSet		202
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		202
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		202

9.1.5.2.2.1 CommonName <CmonNm>

Presence: [1..1]

Definition: Name of the merchant.

Datatype: "Max70Text" on page 520

9.1.5.2.2.2 Address <Adr>

Presence: [0..1]

Definition: Location of the merchant.

Datatype: "Max140Text" on page 517

9.1.5.2.2.3 CountryCode <CtryCd>

Presence: [1..1]

Definition: Country of the merchant.

Datatype: "ISO3NumericCountryCode" on page 488

9.1.5.2.2.4 MerchantCategoryCode <MrchntCtgyCd>

Presence: [1..1]

Definition: Category code conform to ISO 18245, related to the type of services or goods the merchant provides for the transaction.

Datatype: "Min3Max4Text" on page 521

9.1.5.2.2.5 RegisteredIdentifier <RegdIdr>

Presence: [1..1]

Definition: Identifier of the sponsored merchant assigned by the payment facilitator of their acquirer.

Datatype: "Max35Text" on page 519

9.1.5.2.3 Version <Vrsn>

Presence: [1..1]

Definition: Version of the parameters.

Datatype: "Max256Text" on page 518

9.1.5.2.4 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification used to retrieve HostCommunicationParameters.

Datatype: "Max35Text" on page 519

9.1.5.2.5 MerchantPOIIdentification <MrchntPOIId>

Presence: [0..1]

Definition: Identification of the POI during communication with sale system.

Datatype: "Max35Text" on page 519

9.1.5.2.6 SaleIdentification <SaleId>

Presence: [0..1]

Definition: Identification of the SaleSystem connected to the POI.

Datatype: "Max35Text" on page 519

9.1.5.2.7 ExternallyTypeSupported <XtrnlyTpSpprtd>

Presence: [0..*]

Definition: List of types that the receiver supports and that the sender could use as type of an ExternallyDefinedData message component.

Datatype: "Max1025Text" on page 516

9.1.5.3 TMSProtocolParameters6

Definition: Configuration parameters of the TMS protocol between a POI and a terminal manager.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		204
	TerminalManagerIdentification <*TermnlMgrId*>	[1..1]	±		204
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		205
	MaintenanceService <*MntncSvc*>	[1..*]	CodeSet		205
	Version <*Vrsn*>	[1..1]	Text		206
	ApplicationIdentification <*ApplId*>	[0..*]	Text		206
	HostIdentification <*HstId*>	[1..1]	Text		206
	POIIdentification <*POIId*>	[0..1]	Text		206
	InitiatingPartyIdentification <*InitgPtyId*>	[0..1]	Text		206
	RecipientPartyIdentification <*RcptPtyId*>	[0..1]	Text		206
	FileTransfer <*FileTrf*>	[0..1]	Indicator		206
	MessageItem <*MsgItm*>	[0..*]	±		206
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		207

9.1.5.3.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.3.2 TerminalManagerIdentification <TermnlMgrId>

Presence: [1..1]

Definition: Identification of the master terminal manager or the terminal manager.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.5.3.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Protocol version to use when using these parameters.

Datatype: "Max8Text" on page 521

9.1.5.3.4 MaintenanceService <MntncSvc>

Presence: [1..*]

Definition: Maintenance services provided by the terminal manager.

Datatype: "DataSetCategory10Code" on page 482

CodeName	Name	Definition
AQPR	AcquirerParameters	Acquirer specific configuration parameters for the point of interaction (POI) system.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
MTMG	MasterTerminalManager	The terminal manager is the master.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
MTOR	Monitoring	Monitoring of the terminal estate.
SCPR	SecurityParameters	Point of interaction parameters related to the security of software application and application protocol.
SWPK	SoftwareModule	Software module.
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.

9.1.5.3.5 Version <Vrsn>

Presence: [1..1]

Definition: Version of the TMS protocol parameters.

Datatype: "Max256Text" on page 518

9.1.5.3.6 ApplicationIdentification <ApplId>

Presence: [0..*]

Definition: Identification of applications which may be managed by the TM, partially or globally.

Datatype: "Max35Text" on page 519

9.1.5.3.7 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification of the terminal manager host.

Datatype: "Max35Text" on page 519

9.1.5.3.8 POIIdentification <POIId>

Presence: [0..1]

Definition: New identification of the POI for the terminal manager.

Datatype: "Max35Text" on page 519

9.1.5.3.9 InitiatingPartyIdentification <InitgPtyId>

Presence: [0..1]

Definition: New identification of the initiating party to set in TMS messages with this terminal manager.

Datatype: "Max35Text" on page 519

9.1.5.3.10 RecipientPartyIdentification <RcptPtyId>

Presence: [0..1]

Definition: New identification of the recipient party to set in TMS messages with this terminal manager.

Datatype: "Max35Text" on page 519

9.1.5.3.11 FileTransfer <FileTrf>

Presence: [0..1]

Definition: Configuration parameters are exchanged per file transfer protocol rather than per message.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.3.12 MessageItem <MsgItm>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <MsgItm> contains the following elements (see "MessageItemCondition1" on page 376 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemIdentification <*ItmId*>	[1..1]	Text		377
	Condition <*Cond*>	[1..1]	CodeSet		377
	Value <*Val*>	[0..*]	Text		377

9.1.5.3.13 ExternallyTypeSupported <XtrnlyTpSpprtd>

Presence: [0..*]

Definition: List of types that the receiver supports and that the sender could use as type of an ExternallyDefinedData message component.

Datatype: "Max1025Text" on page 516

9.1.5.4 ServiceProviderParameters2

Definition: Service provider parameters of the point of interaction (POI).

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		207
	ServiceProviderIdentification <*SvcPrvdrId*>	[1..*]	±		208
	Version <*Vrsn*>	[1..1]	Text		208
	ApplicationIdentification <*ApplId*>	[0..*]	Text		208
	Host <*Hst*>	[0..*]			208
	HostIdentification <*HstId*>	[1..1]	Text		208
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		209
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		209
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		209
	NonFinancialActionSupported <*NonFinActnSpprtd*>	[0..*]	CodeSet		210

9.1.5.4.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.

CodeName	Name	Definition
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.4.2 ServiceProviderIdentification <SvcPrvdrId>

Presence: [1..*]

Definition: Identification of the service provider.

ServiceProviderIdentification <SvcPrvdrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.5.4.3 Version <Vrsn>

Presence: [1..1]

Definition: Version of the service provider parameters.

Datatype: "Max256Text" on page 518

9.1.5.4.4 ApplicationIdentification <ApplId>

Presence: [0..*]

Definition: Identification of payment application relevant for this service provider.

Datatype: "Max35Text" on page 519

9.1.5.4.5 Host <Hst>

Presence: [0..*]

Definition: Service provider host configuration.

Host <Hst> contains the following **AcquirerHostConfiguration9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	HostIdentification <*HstId*>	[1..1]	Text		208
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		209
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		209
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		209

9.1.5.4.5.1 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification of a host.

Datatype: "Max35Text" on page 519

9.1.5.4.5.2 MessageToSend <MsgToSnd>

Presence: [0..*]

Definition: Types of message to sent to this host.

Datatype: "MessageFunction43Code" on page 491

CodeName	Name	Definition
FAUQ	FinancialAuthorisationRequest	Request for authorisation with financial capture.
CCAQ	CancellationRequest	Request for cancellation.
CMPV	CompletionAdvice	Advice for completion without financial capture.
DGNP	DiagnosticRequest	Request for diagnostic.
RCLQ	ReconciliationRequest	Request for reconciliation.
CCAV	CancellationAdvice	Advice for cancellation.
BTCH	BatchTransfer	Transfer the financial data as a collection of transction.
FRVA	FinancialReversalAdvice	Advice for reversal with financial capture.
AUTQ	AuthorisationRequest	The initiator requests an authorisation without financial impact to complete the transaction.
FCMV	FinancialCompletionAdvice	Advice for completion with financial capture.
DCCQ	CurrencyConversionRequest	Request for dynamic currency conversion.
RVRA	ReversalAdvice	Advice for reversal without financial capture.
DCAV	CurrencyConversionAdvice	Advice for dynamic currency conversion.
TRNA	TransactionAdvice	Advise of the transaction's processing.
NFRQ	NonFinancialRequest	Initiator of the message requests additional information to the receiver.
TRPQ	TransactionReportRequest	Request to receive of a report of transaction from the issuer to the receiver.

9.1.5.4.5.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Protocol version to use when using these parameters.

Datatype: "Max8Text" on page 521

9.1.5.4.5.4 ExternallyTypeSupported <XtrnlyTpSpprtd>

Presence: [0..*]

Definition: List of types that the receiver supports and that the sender could use as type of an ExternallyDefinedData message component.

Datatype: "Max1025Text" on page 516

9.1.5.4.6 NonFinancialActionSupported <NonFinActnSpprtd>

Presence: [0..*]

Definition: Identification of non financial action supported by the Service Provider.

Datatype: "NonFinancialRequestType1Code" on page 492

CodeName	Name	Definition
ACQR	AcquirerSelection	According to several parameters of a transaction, an Intermediary Agent helps an Acceptor to identify the more relevant Acquirer to process the transaction.
PARQ	ParRequest	The Intermediary Agent or Acquirer provides the PaymentAccountReference to use to process the transaction.
RISK	RiskManagement	The Intermediary Agent or Acquirer helps the Acceptor to assess the risk management of the transaction.
TOKN	TokenRequest	The Intermediary Agent or Acquirer provides the token to use to process the transaction.

9.1.5.5 AcquirerProtocolParameters15

Definition: Acceptor parameters dedicated to the acquirer protocol.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		213
	AcquirerIdentification <*AcqrrId*>	[1..*]	±		213
	Version <*Vrsn*>	[1..1]	Text		213
	ApplicationIdentification <*ApplId*>	[0..*]	Text		213
	Host <*Hst*>	[0..*]			214
	HostIdentification <*HstId*>	[1..1]	Text		214
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		214
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		215
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		215
	OnLineTransaction <*OnLineTx*>	[0..1]			215
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		216
	BatchTransfer <*BtchTrf*>	[0..1]			216
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		217
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		217
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		218
	ReTry <*ReTry*>	[0..1]	±		218
	TimeCondition <*TmCond*>	[0..1]	±		218
	CompletionExchange <*CmpltnXchg*>	[0..1]			218
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		219
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		219
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		220
	ReTry <*ReTry*>	[0..1]	±		220
	TimeCondition <*TmCond*>	[0..1]	±		220
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		220
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		220
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		221
	OffLineTransaction <*OffLineTx*>	[0..1]			221
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		222
	BatchTransfer <*BtchTrf*>	[0..1]			222
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		223
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		223

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		224
	ReTry <*ReTry*>	[0..1]	±		224
	TimeCondition <*TmCond*>	[0..1]	±		224
	CompletionExchange <*CmpltnXchg*>	[0..1]			224
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		225
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		225
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		226
	ReTry <*ReTry*>	[0..1]	±		226
	TimeCondition <*TmCond*>	[0..1]	±		226
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		226
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		226
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		227
	ReconciliationExchange <*RcncltnXchg*>	[0..1]			227
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		227
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		228
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		228
	ReTry <*ReTry*>	[0..1]	±		228
	TimeCondition <*TmCond*>	[0..1]	±		228
	ReconciliationByAcquirer <*RcncltnByAcqrr*>	[0..1]	Indicator		229
	TotalsPerCurrency <*TtlsPerCcy*>	[0..1]	Indicator		229
	SplitTotals <*SpltTtls*>	[0..1]	Indicator		229
	SplitTotalCriteria <*SpltTtlCrit*>	[0..*]	CodeSet		229
	CompletionAdviceMandated <*CmpltnAdvcMndtd*>	[0..1]	Indicator		230
	AmountQualifierForReservation <*AmtQlfrForRsvatn*>	[0..*]	CodeSet		230
	ReconciliationError <*RcncltnErr*>	[0..1]	Indicator		230
	CardDataVerification <*CardDataVrfctn*>	[0..1]	Indicator		231
	NotifyOffLineCancellation <*NtfyOffLineCxl*>	[0..1]	Indicator		231
	BatchTransferContent <*BtchTrfCntt*>	[0..*]	CodeSet		231
	FileTransferBatch <*FileTrfBtch*>	[0..1]	Indicator		231
	BatchDigitalSignature <*BtchDgtlSgntr*>	[0..1]	Indicator		231
	MessageItem <*MsgItm*>	[0..*]	±		232

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ProtectCardData <*PrtctCardData*>	[1..1]	Indicator		232
	PrivateCardData <*PrvtCardData*>	[0..1]	Indicator		232
	MandatorySecurityTrailer <*MndtrySctyTrlr*>	[0..1]	Indicator		232

9.1.5.5.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.5.2 AcquirerIdentification <AcqrrId>

Presence: [1..*]

Definition: Identification of the acquirer using this protocol.

AcquirerIdentification <AcqrrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.5.5.3 Version <Vrsn>

Presence: [1..1]

Definition: Version of the acquirer protocol parameters.

Datatype: "Max256Text" on page 518

9.1.5.5.4 ApplicationIdentification <ApplId>

Presence: [0..*]

Definition: Identification of the payment application, user of the acquirer protocol.

Datatype: "Max35Text" on page 519

9.1.5.5.5 Host <Hst>

Presence: [0..*]

Definition: Acquirer host configuration.

Host <Hst> contains the following **AcquirerHostConfiguration9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	HostIdentification <*HstId*>	[1..1]	Text		214
	MessageToSend <*MsgToSnd*>	[0..*]	CodeSet		214
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		215
	ExternallyTypeSupported <*XtrnlyTpSpprtd*>	[0..*]	Text		215

9.1.5.5.5.1 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification of a host.

Datatype: "Max35Text" on page 519

9.1.5.5.5.2 MessageToSend <MsgToSnd>

Presence: [0..*]

Definition: Types of message to sent to this host.

Datatype: "MessageFunction43Code" on page 491

CodeName	Name	Definition
FAUQ	FinancialAuthorisationRequest	Request for authorisation with financial capture.
CCAQ	CancellationRequest	Request for cancellation.
CMPV	CompletionAdvice	Advice for completion without financial capture.
DGNP	DiagnosticRequest	Request for diagnostic.
RCLQ	ReconciliationRequest	Request for reconciliation.
CCAV	CancellationAdvice	Advice for cancellation.
BTCH	BatchTransfer	Transfer the financial data as a collection of transction.
FRVA	FinancialReversalAdvice	Advice for reversal with financial capture.
AUTQ	AuthorisationRequest	The initiator requests an authorisation without financial impact to complete the transaction.
FCMV	FinancialCompletionAdvice	Advice for completion with financial capture.
DCCQ	CurrencyConversionRequest	Request for dynamic currency conversion.
RVRA	ReversalAdvice	Advice for reversal without financial capture.

CodeName	Name	Definition
DCAV	CurrencyConversionAdvice	Advice for dynamic currency conversion.
TRNA	TransactionAdvice	Advise of the transaction's processing.
NFRQ	NonFinancialRequest	Initiator of the message requests additional information to the receiver.
TRPQ	TransactionReportRequest	Request to receive of a report of transaction from the issuer to the receiver.

9.1.5.5.5.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Protocol version to use when using these parameters.

Datatype: "Max8Text" on page 521

9.1.5.5.5.4 ExternallyTypeSupported <XtrnlyTpSpprtd>

Presence: [0..*]

Definition: List of types that the receiver supports and that the sender could use as type of an ExternallyDefinedData message component.

Datatype: "Max1025Text" on page 516

9.1.5.5.6 OnLineTransaction <OnLineTx>

Presence: [0..1]

Definition: Acquirer protocol parameters of transactions performing an online authorisation.

OnLineTransaction <OnLineTx> contains the following **AcquirerProtocolExchangeBehavior2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		216
	BatchTransfer <*BtchTrf*>	[0..1]			216
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		217
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		217
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		218
	ReTry <*ReTry*>	[0..1]	±		218
	TimeCondition <*TmCond*>	[0..1]	±		218
	CompletionExchange <*CmpltnXchg*>	[0..1]			218
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		219
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		219
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		220
	ReTry <*ReTry*>	[0..1]	±		220
	TimeCondition <*TmCond*>	[0..1]	±		220
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		220
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		220
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		221

9.1.5.5.6.1 FinancialCapture <FinCaptr>

Presence: [1..1]

Definition: Mode for the financial capture of the transaction by the acquirer.

Datatype: "FinancialCapture1Code" on page 486

CodeName	Name	Definition
AUTH	Authorisation	Financial capture of the transaction is performed by the acquirer during the authorisation exchange.
COMP	Completion	Financial capture of the transaction is performed by the acquirer during the completion exchange.
BTCH	Batch	Financial capture of the transaction is performed by the acquirer at the reception of a batch transfer.

9.1.5.5.6.2 BatchTransfer <BtchTrf>

Presence: [0..1]

Definition: Configuration of the batch transfers.

BatchTransfer <BtchTrf> contains the following **ExchangeConfiguration9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		217
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		217
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		218
	ReTry <*ReTry*>	[0..1]	±		218
	TimeCondition <*TmCond*>	[0..1]	±		218

9.1.5.5.6.2.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 485

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

9.1.5.5.6.2.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 515

9.1.5.5.6.2.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.5.5.6.2.4 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of an action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.5.5.6.2.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming6" on page 455 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StartTime <*StartTm*>	[0..1]	DateTime		455
	EndTime <*EndTm*>	[0..1]	DateTime		455
	Period <*Prd*>	[0..1]	Text		455
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		456

9.1.5.5.6.3 CompletionExchange <CmpltnXchg>

Presence: [0..1]

Definition: Configuration parameters of completion exchanges.

CompletionExchange <CmpltnXchg> contains the following **ExchangeConfiguration10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		219
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		219
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		220
	ReTry <*ReTry*>	[0..1]	±		220
	TimeCondition <*TmCond*>	[0..1]	±		220
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		220
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		220

9.1.5.5.6.3.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 485

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

9.1.5.5.6.3.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 515

9.1.5.5.6.3.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.5.5.6.3.4 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of an action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.5.5.6.3.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming6" on page 455 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StartTime <*StartTm*>	[0..1]	DateTime		455
	EndTime <*EndTm*>	[0..1]	DateTime		455
	Period <*Prd*>	[0..1]	Text		455
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		456

9.1.5.5.6.3.6 ExchangeFailed <XchgFaild>

Presence: [0..1]

Definition: Failed transaction must be exchanged.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.6.3.7 ExchangeDeclined <XchgDclnd>

Presence: [0..1]

Definition: Indicates that declined transaction must be exchanged.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.6.4 CancellationExchange <CxlXchg>

Presence: [0..1]

Definition: Configuration of the cancellation exchanges.

Datatype: "CancellationProcess2Code" on page 477

CodeName	Name	Definition
ADVC	Advice	Card payment transaction may be cancelled by an advice only before closure of the reconciliation period or before the capture by batch.
NALW	NotAllowed	Card payment transaction cannot be cancelled by the acquirer.
REQU	Request	Card payment transaction may also be cancelled after the closure of the reconciliation period or after the capture by batch. In this case a cancellation request exchange is required.
APPL	ApplicationLevel	Cancellation of the Card payment transaction is defined by the payment application.

9.1.5.5.7 OffLineTransaction <OffLineTx>

Presence: [0..1]

Definition: Acquirer protocol parameters of transactions performing an offline authorisation.

OffLineTransaction <OffLineTx> contains the following **AcquirerProtocolExchangeBehavior2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	FinancialCapture <*FinCaptr*>	[1..1]	CodeSet		222
	BatchTransfer <*BtchTrf*>	[0..1]			222
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		223
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		223
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		224
	ReTry <*ReTry*>	[0..1]	±		224
	TimeCondition <*TmCond*>	[0..1]	±		224
	CompletionExchange <*CmpltnXchg*>	[0..1]			224
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		225
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		225
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		226
	ReTry <*ReTry*>	[0..1]	±		226
	TimeCondition <*TmCond*>	[0..1]	±		226
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		226
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		226
	CancellationExchange <*CxlXchg*>	[0..1]	CodeSet		227

9.1.5.5.7.1 FinancialCapture <FinCaptr>

Presence: [1..1]

Definition: Mode for the financial capture of the transaction by the acquirer.

Datatype: "FinancialCapture1Code" on page 486

CodeName	Name	Definition
AUTH	Authorisation	Financial capture of the transaction is performed by the acquirer during the authorisation exchange.
COMP	Completion	Financial capture of the transaction is performed by the acquirer during the completion exchange.
BTCH	Batch	Financial capture of the transaction is performed by the acquirer at the reception of a batch transfer.

9.1.5.5.7.2 BatchTransfer <BtchTrf>

Presence: [0..1]

Definition: Configuration of the batch transfers.

BatchTransfer <BtchTrf> contains the following **ExchangeConfiguration9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		223
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		223
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		224
	ReTry <*ReTry*>	[0..1]	±		224
	TimeCondition <*TmCond*>	[0..1]	±		224

9.1.5.5.7.2.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 485

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

9.1.5.5.7.2.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 515

9.1.5.5.7.2.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.5.5.7.2.4 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of an action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.5.5.7.2.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming6" on page 455 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StartTime <*StartTm*>	[0..1]	DateTime		455
	EndTime <*EndTm*>	[0..1]	DateTime		455
	Period <*Prd*>	[0..1]	Text		455
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		456

9.1.5.5.7.3 CompletionExchange <CmpltnXchg>

Presence: [0..1]

Definition: Configuration parameters of completion exchanges.

CompletionExchange <CmpltnXchg> contains the following **ExchangeConfiguration10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		225
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		225
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		226
	ReTry <*ReTry*>	[0..1]	±		226
	TimeCondition <*TmCond*>	[0..1]	±		226
	ExchangeFailed <*XchgFaild*>	[0..1]	Indicator		226
	ExchangeDeclined <*XchgDclnd*>	[0..1]	Indicator		226

9.1.5.5.7.3.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 485

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

9.1.5.5.7.3.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 515

9.1.5.5.7.3.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.5.5.7.3.4 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of an action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.5.5.7.3.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming6" on page 455 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StartTime <*StartTm*>	[0..1]	DateTime		455
	EndTime <*EndTm*>	[0..1]	DateTime		455
	Period <*Prd*>	[0..1]	Text		455
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		456

9.1.5.5.7.3.6 ExchangeFailed <XchgFaild>

Presence: [0..1]

Definition: Failed transaction must be exchanged.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.7.3.7 ExchangeDeclined <XchgDclnd>

Presence: [0..1]

Definition: Indicates that declined transaction must be exchanged.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.7.4 CancellationExchange <CxlXchg>

Presence: [0..1]

Definition: Configuration of the cancellation exchanges.

Datatype: "CancellationProcess2Code" on page 477

CodeName	Name	Definition
ADVC	Advice	Card payment transaction may be cancelled by an advice only before closure of the reconciliation period or before the capture by batch.
NALW	NotAllowed	Card payment transaction cannot be cancelled by the acquirer.
REQU	Request	Card payment transaction may also be cancelled after the closure of the reconciliation period or after the capture by batch. In this case a cancellation request exchange is required.
APPL	ApplicationLevel	Cancellation of the Card payment transaction is defined by the payment application.

9.1.5.5.8 ReconciliationExchange <RcncltnXchg>

Presence: [0..1]

Definition: Configuration parameters of reconciliation exchanges.

ReconciliationExchange <RcncltnXchg> contains the following **ExchangeConfiguration9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <*XchgPlcy*>	[1..*]	CodeSet		227
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		228
	MaximumAmount <*MaxAmt*>	[0..1]	Amount		228
	ReTry <*ReTry*>	[0..1]	±		228
	TimeCondition <*TmCond*>	[0..1]	±		228

9.1.5.5.8.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 485

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.

CodeName	Name	Definition
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

9.1.5.5.8.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 515

9.1.5.5.8.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.5.5.8.4 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of an action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.5.5.8.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming6" on page 455 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StartTime <*StartTm*>	[0..1]	DateTime		455
	EndTime <*EndTm*>	[0..1]	DateTime		455
	Period <*Prd*>	[0..1]	Text		455
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		456

9.1.5.5.9 ReconciliationByAcquirer <RcncltnByAcqrr>

Presence: [0..1]

Definition: Indicates the reconciliation period is assigned by the acquirer instead of the acceptor.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.10 TotalsPerCurrency <TtlsPerCcy>

Presence: [0..1]

Definition: Indicates the reconciliation total amounts are computed per currency.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.11 SplitTotals <SpltTtls>

Presence: [0..1]

Definition: Indicates that totals in reconciliation or batch must be split.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.12 SplitTotalCriteria <SpltTtlCrit>

Presence: [0..*]

Definition: List of criterion to use when totals in reconciliation or batch must be split.

Datatype: "ReconciliationCriteria1Code" on page 500

CodeName	Name	Definition
BRND	CardBrand	The set is defined by transactions made with cards belonging to the same brand.

CodeName	Name	Definition
PROF	CardProductProfile	The set is defined by transactions made with cards sharing the same CardProductProfile.
GRUP	PoiGroup	The set is defined by transactions processed by POIs identified with the same POIGroup.

9.1.5.5.13 CompletionAdviceMandated <CmpltnAdvcMndtd>

Presence: [0..1]

Definition: To notify that the acquirer expect to receive a completion advice after each update of reservation.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.14 AmountQualifierForReservation <AmtQlfrForRsvatn>

Presence: [0..*]

Definition: Identification of available amount qualifier for a reservation.

Datatype: "TypeOfAmount8Code" on page 511

CodeName	Name	Definition
ACTL	Actual	Actual amount.
ESTM	Estimated	Estimated amount (the final amount could be above or below).
MAXI	Maximum	Maximum amount (the final amount must be less or equal).
DFLT	Default	Default amount.
RPLT	Replacement	Replacement amount.
INCR	Incremental	Incremental amount for reservation.
DECR	Decremental	Decremental amount for reservation.
RESD	Reserved	Reserved or updated reserved amount for reservation.

9.1.5.5.15 ReconciliationError <RcncltnErr>

Presence: [0..1]

Definition: After an error in a totals of the Reconciliation, the POI sends transactions in error in the BatchTransfer messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.16 CardDataVerification <CardDataVrfctn>

Presence: [0..1]

Definition: Indicates whether the POI must send card data (protected or plain card data) in the AcceptorCompletionAdvice message following an authorisation exchange.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.17 NotifyOffLineCancellation <NtfyOffLineCxl>

Presence: [0..1]

Definition: Send a cancellation advice for offline transactions not yet captured.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.18 BatchTransferContent <BtchTrfCntt>

Presence: [0..*]

Definition: Types of transaction to include in the batch.

Datatype: "BatchTransactionType1Code" on page 476

CodeName	Name	Definition
DTCT	DebitCredit	Debit and credit transactions.
CNCL	Cancellation	Cancellation of a previous transaction.
FAIL	Failed	Failed transactions.
DCLN	Declined	Declined transactions.

9.1.5.5.19 FileTransferBatch <FileTrfBtch>

Presence: [0..1]

Definition: BatchTransfer are exchanged per file transfer protocol rather than per message.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.20 BatchDigitalSignature <BtchDgtlSgntr>

Presence: [0..1]

Definition: BatchTransfer are authenticated by digital signature rather than a MAC (Message Authentication Code).

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.21 MessageItem <MsgItm>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <MsgItm> contains the following elements (see "MessageItemCondition1" on page 376 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemIdentification <*ItmId*>	[1..1]	Text		377
	Condition <*Cond*>	[1..1]	CodeSet		377
	Value <*Val*>	[0..*]	Text		377

9.1.5.5.22 ProtectCardData <PrtctCardData>

Presence: [1..1]

Definition: Indicator to require protection of sensitive card data in messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.23 PrivateCardData <PrvtCardData>

Presence: [0..1]

Definition: Indicator to require a private protection of sensitive card data in messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.5.24 MandatorySecurityTrailer <MndtrySctyTrlr>

Presence: [0..1]

Definition: A security trailer is mandatory in the messages.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.5.6 ApplicationParameters11

Definition: Acceptor parameters dedicated to a payment application of the point of interaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		233
	ApplicationIdentification <*ApplId*>	[1..1]	Text		233
	Version <*Vrsn*>	[0..1]	Text		233
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		233
	ParametersLength <*ParamsLngth*>	[0..1]	Quantity		234
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		234
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		234
	Parameters <*Params*>	[0..*]	Binary		234
	EncryptedParameters <*NcrptdParams*>	[0..1]	±		234

9.1.5.6.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.6.2 ApplicationIdentification <ApplId>

Presence: [1..1]

Definition: Identification of the payment application.

Datatype: "Max35Text" on page 519

9.1.5.6.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the payment application configuration parameters.

Datatype: "Max256Text" on page 518

9.1.5.6.4 ParameterFormatIdentifier <ParamFrmtIdr>

Presence: [0..1]

Definition: Version of the parameters' format.

Datatype: "Max8Text" on page 521

9.1.5.6.5 ParametersLength <ParamsLngth>

Presence: [0..1]

Definition: Full length of parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.6.6 OffsetStart <OffsetStart>

Presence: [0..1]

Definition: Place of this Block, beginning with 0, in the full parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.6.7 OffsetEnd <OffsetEnd>

Presence: [0..1]

Definition: Following place of this Block in the full parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.6.8 Parameters <Params>

Presence: [0..*]

Definition: Configuration parameters used by the related payment application.

Datatype: "Max100KBinary" on page 461

9.1.5.6.9 EncryptedParameters <NcrptdParams>

Presence: [0..1]

Definition: Sensitive parameters (sequence of parameters including the envelope) encrypted with a cryptographic key.

EncryptedParameters <NcrptdParams> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.5.7 TerminalPackageType3

Definition: Group of software packages related to a group of POIComponent of the POI System.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POIComponentIdentification <*POICmpntId*>	[0..*]			235
	ItemNumber <*ItmNb*>	[0..1]	Text		235
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		236
	Identification <*Id*>	[0..1]	Text		236
	SerialNumber <*SrlNb*>	[0..1]	Text		236
	Package <*Packg*>	[1..*]			236
	PackageIdentification <*PackgId*>	[0..1]	±		236
	PackageLength <*PackgLngth*>	[0..1]	Quantity		237
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		237
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		237
	PackageBlock <*PackgBlck*>	[0..*]			237
	Identification <*Id*>	[1..1]	Text		238
	Value <*Val*>	[0..1]	Binary		238
	ProtectedValue <*PrtctdVal*>	[0..1]	±		238
	Type <*Tp*>	[0..1]	Text		238

9.1.5.7.1 POIComponentIdentification <POICmpntId>

Presence: [0..*]

Definition: Identification of the POI (Point Of Interaction) component.

POIComponentIdentification <POICmpntId> contains the following **PointOfInteractionComponentIdentification2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemNumber <*ItmNb*>	[0..1]	Text		235
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		236
	Identification <*Id*>	[0..1]	Text		236
	SerialNumber <*SrlNb*>	[0..1]	Text		236

9.1.5.7.1.1 ItemNumber <ItmNb>

Presence: [0..1]

Definition: Hierarchical identification of a hardware component inside all the hardware component of the POI. It is composed of all item numbers of the upper level components, separated by the '.' character, ended by the item number of the current component.

Datatype: "Max35Text" on page 519

9.1.5.7.1.2 ProviderIdentification <PrvdrId>

Presence: [0..1]

Definition: Identifies the provider of the software, hardware or parameters of the POI component.

Datatype: "Max35Text" on page 519

9.1.5.7.1.3 Identification <Id>

Presence: [0..1]

Definition: Identification of the POI component assigned by its provider.

Datatype: "Max256Text" on page 518

9.1.5.7.1.4 SerialNumber <SrlNb>

Presence: [0..1]

Definition: Serial number identifying an occurrence of an hardware component.

Datatype: "Max256Text" on page 518

9.1.5.7.2 Package <Packg>

Presence: [1..*]

Definition: Chunk of a software package.

Package <Packg> contains the following **PackageType3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PackageIdentification <*PackgId*>	[0..1]	±		236
	PackageLength <*PackgLngth*>	[0..1]	Quantity		237
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		237
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		237
	PackageBlock <*PackgBlck*>	[0..*]			237
	Identification <*Id*>	[1..1]	Text		238
	Value <*Val*>	[0..1]	Binary		238
	ProtectedValue <*PrtctdVal*>	[0..1]	±		238
	Type <*Tp*>	[0..1]	Text		238

9.1.5.7.2.1 PackageIdentification <PackgId>

Presence: [0..1]

Definition: Identification of the software packages of which the chunk belongs.

PackageIdentification <PackgId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.5.7.2.2 PackageLength <PackgLngth>

Presence: [0..1]

Definition: Full length of software package identified through PackageIdentification.

Datatype: "PositiveNumber" on page 515

9.1.5.7.2.3 OffsetStart <OffsetStart>

Presence: [0..1]

Definition: Place of the first following PackageBlock, beginning with 0, in the full software package identified through PackageIdentification.

Datatype: "PositiveNumber" on page 515

9.1.5.7.2.4 OffsetEnd <OffsetEnd>

Presence: [0..1]

Definition: Following place of the last following PackageBlock in the full software package identified through PackageIdentification.

Datatype: "PositiveNumber" on page 515

9.1.5.7.2.5 PackageBlock <PackgBlck>

Presence: [0..*]

Definition: Consecutive slices of the full software package identified through PackageIdentification starting with first slice at the place identified with OffsetStart and ending with the last slice at the previous place identified with OffsetEnd.

PackageBlock <PackgBlck> contains the following **ExternallyDefinedData3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		238
	Value <*Val*>	[0..1]	Binary		238
	ProtectedValue <*PrtctdVal*>	[0..1]	±		238
	Type <*Tp*>	[0..1]	Text		238

9.1.5.7.2.5.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the set of data to exchange.

Datatype: "Max1025Text" on page 516

9.1.5.7.2.5.2 Value <Val>

Presence: [0..1]

Definition: Data to exchange according to an external standard.

Datatype: "Max100KBinary" on page 461

9.1.5.7.2.5.3 ProtectedValue <PrtctdVal>

Presence: [0..1]

Definition: Protection of the values to exchange.

ProtectedValue <PrtctdVal> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.5.7.2.5.4 Type <Tp>

Presence: [0..1]

Definition: Identification of the standard used to encode the values to exchange.

Datatype: "Max1025Text" on page 516

9.1.5.8 SecurityParameters14

Definition: Parameters related to the security of software application and application protocol.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		239
	Version <*Vrsn*>	[1..1]	Text		239
	POIChallenge <*POIChllng*>	[0..1]	Binary		239
	TMChallenge <*TMChllng*>	[0..1]	Binary		239
	SecurityElement <*SctyElmt*>	[0..*]	±		239

9.1.5.8.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.8.2 Version <Vrsn>

Presence: [1..1]

Definition: Version of the security parameters.

Datatype: "Max256Text" on page 518

9.1.5.8.3 POIChallenge <POIChllng>

Presence: [0..1]

Definition: Point of interaction challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

9.1.5.8.4 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

9.1.5.8.5 SecurityElement <SctyElmt>

Presence: [0..*]

Definition: Key to inject in the point of interaction, protected by the temporary key previously sent.

SecurityElement <SctyElmt> contains the following elements (see "CryptographicKey16" on page 419 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		419
	AdditionalIdentification <*AddtlId*>	[0..1]	Binary		419
	Name <*Nm*>	[0..1]	Text		420
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		420
	ItemNumber <*ItmNb*>	[0..1]	Text		420
	Version <*Vrsn*>	[1..1]	Text		420
	Type <*Tp*>	[0..1]	CodeSet		420
	Function <*Fctn*>	[0..*]	CodeSet		421
	ActivationDate <*ActvtnDt*>	[0..1]	DateTime		421
	DeactivationDate <*DeactvtnDt*>	[0..1]	DateTime		422
	KeyValue <*KeyVal*>	[0..1]	±		422
	KeyCheckValue <*KeyChckVal*>	[0..1]	Binary		422
	AdditionalManagementInformation <*AddtlMgmtInf*>	[0..*]			422
	Name <*Nm*>	[1..1]	Text		422
	Value <*Val*>	[0..1]	Text		423

9.1.5.9 PaymentTerminalParameters8

Definition: Manufacturer configuration parameters of the point of interaction (POI).

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		241
	VendorIdentification <*VndrId*>	[0..1]	Text		241
	Version <*Vrsn*>	[0..1]	Text		242
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		242
	ClockSynchronisation <*ClckSynctn*>	[0..1]			242
	POITimeZone <*POITmZone*>	[1..1]	Text		242
	SynchronisationServer <*SynctnSvr*>	[0..*]	±		242
	Delay <*Dely*>	[0..1]	Time		243
	TimeZoneLine <*TmZoneLine*>	[0..*]	Text		243
	LocalDateTime <*LclDtTm*>	[0..*]			243
	FromDateTime <*FrDtTm*>	[0..1]	DateTime		243
	ToDateTime <*ToDtTm*>	[0..1]	DateTime		244
	UTCOffset <*UTCOffset*>	[1..1]	Quantity		244
	OtherParametersLength <*OthrParamsLngth*>	[0..1]	Quantity		244
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		244
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		244
	OtherParameters <*OthrParams*>	[0..1]	Binary		244

9.1.5.9.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.9.2 VendorIdentification <VndrId>

Presence: [0..1]

Definition: Identification of the vendor for the MTM, if the POI manages various subsets of terminal parameters.

Datatype: "Max35Text" on page 519

9.1.5.9.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the terminal parameters.

Datatype: "Max256Text" on page 518

9.1.5.9.4 ParameterFormatIdentifier <ParamFrmtIdr>

Presence: [0..1]

Definition: Version of the parameters' format.

Datatype: "Max8Text" on page 521

9.1.5.9.5 ClockSynchronisation <ClckSynctn>

Presence: [0..1]

Definition: Parameters to synchronise the real time clock of the POI (Point Of Interaction).

ClockSynchronisation <ClckSynctn> contains the following **ClockSynchronisation3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	POITimeZone <*POITmZone*>	[1..1]	Text		242
	SynchronisationServer <*SynctnSvr*>	[0..*]	±		242
	Delay <*Dely*>	[0..1]	Time		243

9.1.5.9.5.1 POITimeZone <POITmZone>

Presence: [1..1]

Definition: Name of the time zone where is located the POI (Point Of Interaction), as definined by the IANA (Internet Assigned Number Authority) time zone data base.

Datatype: "Max70Text" on page 520

9.1.5.9.5.2 SynchronisationServer <SynctnSvr>

Presence: [0..*]

Definition: Parameters to contact a time server.

SynchronisationServer <SynctnSvr> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.5.9.5.3 Delay <Dely>

Presence: [0..1]

Definition: Delay between two contacts of the server.

Datatype: "ISOTime" on page 522

9.1.5.9.6 TimeZoneLine <TmZoneLine>

Presence: [0..*]

Definition: Time zone line to update in the time zone data base subset stored in the POI (Point Of Interaction). The format of the line is conform to the IANA (Internet Assigned Number Authority) time zone data base.

Datatype: "Max70Text" on page 520

9.1.5.9.7 LocalDateTime <LclDtTm>

Presence: [0..*]

Definition: Local time offset to UTC (Coordinated Universal Time).

LocalDateTime <LclDtTm> contains the following **LocalDateTime1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	FromDateTime <*FrDtTm*>	[0..1]	DateTime		243
	ToDateTime <*ToDtTm*>	[0..1]	DateTime		244
	UTCOffset <*UTCOffset*>	[1..1]	Quantity		244

9.1.5.9.7.1 FromDateTime <FrDtTm>

Presence: [0..1]

Definition: Date time of the beginning of the period (inclusive).

Datatype: "ISODateTime" on page 513

9.1.5.9.7.2 ToDateTime <ToDtTm>

Presence: [0..1]

Definition: Date time of the end of the period (exclusive).

Datatype: "ISODateTime" on page 513

9.1.5.9.7.3 UTCOffset <UTCOffset>

Presence: [1..1]

Definition: UTC offset in minutes, of the local time during the period. For instance, 120 for Central European Time, -720 for Central Standard Time (North America).

Datatype: "Number" on page 515

9.1.5.9.8 OtherParametersLength <OthrParamsLngth>

Presence: [0..1]

Definition: Full length of other parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.9.9 OffsetStart <OffsetStart>

Presence: [0..1]

Definition: Place of this Block, beginning with 0, in the full other parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.9.10 OffsetEnd <OffsetEnd>

Presence: [0..1]

Definition: Following place of this Block in the full other parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.9.11 OtherParameters <OthrParams>

Presence: [0..1]

Definition: Others manufacturer configuration parameters of the point of interaction.

Datatype: "Max10000Binary" on page 461

9.1.5.10 MerchantConfigurationParameters6

Definition: Acceptor parameters dedicated to the merchant.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		245
	MerchantIdentification <*MrchntId*>	[0..1]	Text		245
	Version <*Vrsn*>	[0..1]	Text		245
	ParameterFormatIdentifier <*ParamFrmtIdr*>	[0..1]	Text		245
	Proxy <*Prxy*>	[0..1]			246
	Type <*Tp*>	[1..1]	CodeSet		246
	Access <*Accs*>	[1..1]	±		246
	OtherParametersLength <*OthrParamsLngth*>	[0..1]	Quantity		246
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		247
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		247
	OtherParameters <*OthrParams*>	[0..1]	Binary		247

9.1.5.10.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 507

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.1.5.10.2 MerchantIdentification <MrchntId>

Presence: [0..1]

Definition: Identification of the merchant for the MTM, if the POI manages several merchants.

Datatype: "Max35Text" on page 519

9.1.5.10.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the merchant parameters.

Datatype: "Max256Text" on page 518

9.1.5.10.4 ParameterFormatIdentifier <ParamFrmtIdr>

Presence: [0..1]

Definition: Version of the parameters' format.

Datatype: "Max8Text" on page 521

9.1.5.10.5 Proxy <Prxy>

Presence: [0..1]

Definition: Local proxy configuration.

Proxy <Prxy> contains the following **NetworkParameters8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		246
	Access <*Accs*>	[1..1]	±		246

9.1.5.10.5.1 Type <Tp>

Presence: [1..1]

Definition: Type of proxy.

Datatype: "NetworkType2Code" on page 492

CodeName	Name	Definition
SCK5	Sock5	Sock5 proxy.
SCK4	Sock4	Sock4 proxy.
HTTP	HTTP	HTTP proxy.

9.1.5.10.5.2 Access <Accs>

Presence: [1..1]

Definition: Access information to the proxy.

Access <Accs> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.5.10.6 OtherParametersLength <OthrParamsLngth>

Presence: [0..1]

Definition: Full length of other parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.10.7 OffsetStart <OffsetStart>

Presence: [0..1]

Definition: Place of this Block, beginning with 0, in the full other parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.10.8 OffsetEnd <OffsetEnd>

Presence: [0..1]

Definition: Following place of this Block in the full other parameters.

Datatype: "PositiveNumber" on page 515

9.1.5.10.9 OtherParameters <OthrParams>

Presence: [0..1]

Definition: Other merchant parameters.

Datatype: "Max10000Binary" on page 461

9.1.6 Identification Information

9.1.6.1 GenericIdentification32

Definition: Identification of an entity.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		247
	Type <*Tp*>	[0..1]	CodeSet		247
	Issuer <*Issr*>	[0..1]	CodeSet		248
	ShortName <*ShrtNm*>	[0..1]	Text		248

9.1.6.1.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the entity.

Datatype: "Max35Text" on page 519

9.1.6.1.2 Type <Tp>

Presence: [0..1]

Definition: Type of identified entity.

Datatype: "PartyType3Code" on page 495

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.

9.1.6.1.3 Issuer <Issr>

Presence: [0..1]

Definition: Entity assigning the identification (for example merchant, acceptor, acquirer, or tax authority).

Datatype: "PartyType4Code" on page 495

CodeName	Name	Definition
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
TAXH	TaxAuthority	Tax authority.

9.1.6.1.4 ShortName <ShrtNm>

Presence: [0..1]

Definition: Name of the entity.

Datatype: "Max35Text" on page 519

9.1.6.2 GenericIdentification177

Definition: Identification of an entity.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

9.1.6.2.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the entity.

Datatype: "Max35Text" on page 519

9.1.6.2.2 Type <Tp>

Presence: [0..1]

Definition: Type of identified entity.

Datatype: "PartyType33Code" on page 494

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.

CodeName	Name	Definition
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TAXH	TaxAuthority	Tax authority.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

9.1.6.2.3 Issuer <Issr>

Presence: [0..1]

Definition: Entity assigning the identification (for example merchant, acceptor, acquirer, or tax authority).

Datatype: "PartyType33Code" on page 494

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TAXH	TaxAuthority	Tax authority.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

9.1.6.2.4 Country <Ctry>

Presence: [0..1]

Definition: Country of the entity (ISO 3166-1 alpha-2 or alpha-3).

Datatype: "Min2Max3AlphaText" on page 521

9.1.6.2.5 ShortName <ShrtNm>

Presence: [0..1]

Definition: Name of the entity.

Datatype: "Max35Text" on page 519

9.1.6.2.6 RemoteAccess <RmotAccs>

Presence: [0..1]

Definition: Access information to reach the target host.

RemoteAccess <RmotAccs> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.6.2.7 Geolocation <Glctn>

Presence: [0..1]

Definition: Location of the entity.

Geolocation <Glctn> contains the following **Geolocation1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

9.1.6.2.7.1 GeographicCoordinates <GeogcCordints>

Presence: [0..1]

Definition: Geographic location specified by geographic coordinates.

GeographicCoordinates <GeogcCordints> contains the following **GeolocationGeographicCoordinates1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252

9.1.6.2.7.1.1 Latitude <Lat>

Presence: [1..1]

Definition: Angular distance of a location on the earth south or north of the equator.

The latitude is measured in degrees, minutes and seconds, following by "N" for the north and "S" for the south of the equator. For example: 48°51'29" N the Eiffel Tower latitude.

Datatype: "Max35Text" on page 519

9.1.6.2.7.1.2 Longitude <Long>

Presence: [1..1]

Definition: Angular measurement of the distance of a location on the earth east or west of the Greenwich observatory.

The longitude is measured in degrees, minutes and seconds, following by "E" for the east and "W" for the west. For example: 23°27'30" E.

Datatype: "Max35Text" on page 519

9.1.6.2.7.2 UTMCoordinates <UTMCordints>

Presence: [0..1]

Definition: Geographic location specified by UTM coordinates.

UTMCoordinates <UTMCordints> contains the following **GeolocationUTMCoordinates1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

9.1.6.2.7.2.1 UTMZone <UTMZone>

Presence: [1..1]

Definition: UTM grid zone combination of the longitude zone (1 to 60) and the latitude band (C to X, excluding I and O).

Datatype: "Max35Text" on page 519

9.1.6.2.7.2.2 UTMEastward <UTMEstwrd>

Presence: [1..1]

Definition: X-coordinate of the Universal Transverse Mercator

coordinate system.

Datatype: "Max35Text" on page 519

9.1.6.2.7.2.3 UTMNorthward <UTMNrthwrd>

Presence: [1..1]

Definition: Y-coordinate of the Universal Transverse Mercator

coordinate system.

Datatype: "Max35Text" on page 519

9.1.6.3 GenericIdentification176

Definition: Identification of an entity.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.6.3.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the entity.

Datatype: "Max35Text" on page 519

9.1.6.3.2 Type <Tp>

Presence: [0..1]

Definition: Type of identified entity.

Datatype: "PartyType33Code" on page 494

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.

CodeName	Name	Definition
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TAXH	TaxAuthority	Tax authority.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

9.1.6.3.3 Issuer <Issr>

Presence: [0..1]

Definition: Entity assigning the identification (for example merchant, acceptor, acquirer, or tax authority).

Datatype: "PartyType33Code" on page 494

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TAXH	TaxAuthority	Tax authority.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

9.1.6.3.4 Country <Ctry>

Presence: [0..1]

Definition: Country of the entity (ISO 3166-1 alpha-2 or alpha-3).

Datatype: "Min2Max3AlphaText" on page 521

9.1.6.3.5 ShortName <ShrtNm>

Presence: [0..1]

Definition: Name of the entity.

Datatype: "Max35Text" on page 519

9.1.6.4 GenericIdentification36

Definition: Identification using a proprietary scheme.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		255
	Issuer <*Issr*>	[1..1]	Text		255
	SchemeName <*SchmeNm*>	[0..1]	Text		255

9.1.6.4.1 Identification <Id>

Presence: [1..1]

Definition: Proprietary information, often a code, issued by the data source scheme issuer.

Datatype: "Max35Text" on page 519

9.1.6.4.2 Issuer <Issr>

Presence: [1..1]

Definition: Entity that assigns the identification.

Datatype: "Max35Text" on page 519

9.1.6.4.3 SchemeName <SchmeNm>

Presence: [0..1]

Definition: Short textual description of the scheme.

Datatype: "Max35Text" on page 519

9.1.6.5 GenericIdentification4

Definition: Information related to an identification, eg, party identification or account identification.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		255
	IdentificationType <*IdTp*>	[1..1]	Text		255

9.1.6.5.1 Identification <Id>

Presence: [1..1]

Definition: Identifier issued to a person for which no specific identifier has been defined.

Datatype: "Max35Text" on page 519

9.1.6.5.2 IdentificationType <IdTp>

Presence: [1..1]

Definition: Specifies the nature of the identifier.

Usage: IdentificationType is used to specify what kind of identifier is used. It should be used in case the identifier is different from the identifiers listed in the pre-defined identifier list.

Datatype: "Max35Text" on page 519

9.1.7 Miscellaneous

9.1.7.1 SupplementaryData1

Definition: Additional information that can not be captured in the structured fields and/or any other specific block.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PlaceAndName <*PlcAndNm*>	[0..1]	Text		256
	Envelope <*Envlp*>	[1..1]	(External Schema)		256

Constraints

- **SupplementaryDataRule**

  This component may not be used without the explicit approval of a SEG and submission to the RA of ISO 20022 compliant structure(s) to be used in the Envelope element.

9.1.7.1.1 PlaceAndName <PlcAndNm>

Presence: [0..1]

Definition: Unambiguous reference to the location where the supplementary data must be inserted in the message instance.

In the case of XML, this is expressed by a valid XPath.

Datatype: "Max350Text" on page 518

9.1.7.1.2 Envelope <Envlp>

Presence: [1..1]

Definition: Technical element wrapping the supplementary data.

Type: (External Schema)

Technical component that contains the validated supplementary data information. This technical envelope allows to segregate the supplementary data information from any other information.

9.1.7.2 PointOfInteractionComponent12

Definition: Data related to a component of the POI (Point Of Interaction) performing the transaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		258
	SubTypeInformation <*SubTpInf*>	[0..1]	Text		259
	Identification <*Id*>	[1..1]			260
	ItemNumber <*ItmNb*>	[0..1]	Text		260
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		260
	Identification <*Id*>	[0..1]	Text		260
	SerialNumber <*SrlNb*>	[0..1]	Text		260
	Status <*Sts*>	[0..1]			260
	VersionNumber <*VrsnNb*>	[0..1]	Text		261
	Status <*Sts*>	[0..1]	CodeSet		261
	ExpiryDate <*XpryDt*>	[0..1]	Date		261
	StandardCompliance <*StdCmplc*>	[0..*]			261
	Identification <*Id*>	[1..1]	Text		261
	Version <*Vrsn*>	[1..1]	Text		262
	Issuer <*Issr*>	[1..1]	Text		262
	Characteristics <*Chrtcs*>	[0..1]			262
	Memory <*Mmry*>	[0..*]			263
	Identification <*Id*>	[1..1]	Text		264
	TotalSize <*TtlSz*>	[1..1]	Quantity		264
	FreeSize <*FreeSz*>	[1..1]	Quantity		264
	Unit <*Unit*>	[1..1]	CodeSet		264
	Communication <*Com*>	[0..*]			264
	CommunicationType <*ComTp*>	[1..1]	CodeSet		265
	RemoteParty <*RmotPty*>	[1..*]	CodeSet		266
	Active <*Actv*>	[1..1]	Indicator		266
	Parameters <*Params*>	[0..1]	±		266
	PhysicalInterface <*PhysIntrfc*>	[0..1]			267
	InterfaceName <*IntrfcNm*>	[1..1]	Text		267
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		267
	UserName <*UsrNm*>	[0..1]	Text		268
	AccessCode <*AccsCd*>	[0..1]	Binary		268

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		268
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		268
	SecurityAccessModules <*SctyAccsMdls*>	[0..1]	Quantity		269
	SubscriberIdentityModules <*SbcbrIdntyMdls*>	[0..1]	Quantity		269
	SecurityElement <*SctyElmt*>	[0..*]	±		269
	Assessment <*Assmnt*>	[0..*]			269
	Type <*Tp*>	[1..1]	CodeSet		270
	Assigner <*Assgnr*>	[1..*]	Text		270
	DeliveryDate <*DlvryDt*>	[0..1]	DateTime		270
	ExpirationDate <*XprtnDt*>	[0..1]	DateTime		270
	Number <*Nb*>	[1..1]	Text		270
	Package <*Packg*>	[0..*]			271
	PackageIdentification <*PackgId*>	[0..1]	±		271
	PackageLength <*PackgLngth*>	[0..1]	Quantity		271
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		271
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		272
	PackageBlock <*PackgBlck*>	[0..*]			272
	Identification <*Id*>	[1..1]	Text		272
	Value <*Val*>	[0..1]	Binary		272
	ProtectedValue <*PrtctdVal*>	[0..1]	±		272
	Type <*Tp*>	[0..1]	Text		273

9.1.7.2.1 Type <Tp>

Presence: [1..1]

Definition: Type of component belonging to a POI (Point Of Interaction) Terminal.

Datatype: "POIComponentType6Code" on page 498

CodeName	Name	Definition
AQPP	AcquirerProtocolParameters	Parameters for acquirer interface of the point of interaction, including acquirer host configuration parameters.
APPR	ApplicationParameters	Parameters of a payment application running on the point of interaction.
TLPR	TerminalParameters	Manufacturer configuration parameters of the point of interaction.

CodeName	Name	Definition
SCPR	SecurityParameters	Security parameters of the point of interaction.
SERV	Server	Payment server of a point of interaction system.
TERM	Terminal	Payment terminal point of interaction.
DVCE	Device	Device sub-component of a component of the point of interaction.
SECM	SecureModule	Security module.
APLI	PaymentApplication	Payment application software.
EMVK	EMVKernel	EMV application kernel (EMV is the chip card specifications initially defined by Eurocard, Mastercard and Visa).
EMVO	EMVLevel1	EMV physical interface (EMV is the chip card specifications initially defined by Eurocard, Mastercard and Visa).
MDWR	Middleware	Software module of the point of interaction.
DRVR	Driver	Driver module of the point of interaction.
OPST	OperatingSystem	Software that manages hardware to provide common services to the applications.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
CRTF	CertificateParameters	Certificate provided by a terminal manager.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
SACP	SaleComponent	Component of the Sale system.
SAPR	SaleToPOIProtocolParameters	Parameters related to the Sale to POI protocol.
LOGF	LogFile	Any repository used for recording log traces.
MDFL	MediaFile	Media file managed by an application of the POI.
SOFT	Soft	Payment or other software application.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

9.1.7.2.2 SubTypeInformation <SubTpInf>

Presence: [0..1]

Definition: Additional information regarding the type of the component.

Datatype: "Max70Text" on page 520

9.1.7.2.3 Identification <Id>

Presence: [1..1]

Definition: Identification of the POI (Point Of Interaction) component.

Identification <Id> contains the following **PointOfInteractionComponentIdentification2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemNumber <*ItmNb*>	[0..1]	Text		260
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		260
	Identification <*Id*>	[0..1]	Text		260
	SerialNumber <*SrlNb*>	[0..1]	Text		260

9.1.7.2.3.1 ItemNumber <ItmNb>

Presence: [0..1]

Definition: Hierarchical identification of a hardware component inside all the hardware component of the POI. It is composed of all item numbers of the upper level components, separated by the '.' character, ended by the item number of the current component.

Datatype: "Max35Text" on page 519

9.1.7.2.3.2 ProviderIdentification <PrvdrId>

Presence: [0..1]

Definition: Identifies the provider of the software, hardware or parameters of the POI component.

Datatype: "Max35Text" on page 519

9.1.7.2.3.3 Identification <Id>

Presence: [0..1]

Definition: Identification of the POI component assigned by its provider.

Datatype: "Max256Text" on page 518

9.1.7.2.3.4 SerialNumber <SrlNb>

Presence: [0..1]

Definition: Serial number identifying an occurrence of an hardware component.

Datatype: "Max256Text" on page 518

9.1.7.2.4 Status <Sts>

Presence: [0..1]

Definition: Status of the POI (Point Of Interaction) component.

Status <Sts> contains the following **PointOfInteractionComponentStatus3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	VersionNumber <*VrsnNb*>	[0..1]	Text		261
	Status <*Sts*>	[0..1]	CodeSet		261
	ExpiryDate <*XpryDt*>	[0..1]	Date		261

9.1.7.2.4.1 VersionNumber <VrsnNb>

Presence: [0..1]

Definition: Current version of the component that might include the release number.

Datatype: "Max256Text" on page 518

9.1.7.2.4.2 Status <Sts>

Presence: [0..1]

Definition: Current status of the component.

Datatype: "POIComponentStatus1Code" on page 498

CodeName	Name	Definition
WAIT	WaitingActivation	Component not yet activated.
OUTD	OutOfOrder	Component not working properly.
OPER	InOperation	Component activated and in operation.
DACT	Deactivated	Component has been deactivated.

9.1.7.2.4.3 ExpiryDate <XpryDt>

Presence: [0..1]

Definition: Expiration date of the component.

Datatype: "ISODate" on page 512

9.1.7.2.5 StandardCompliance <StdCmplc>

Presence: [0..*]

Definition: Identification of the standard for which the component complies with.

StandardCompliance <StdCmplc> contains the following **GenericIdentification48** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		261
	Version <*Vrsn*>	[1..1]	Text		262
	Issuer <*Issr*>	[1..1]	Text		262

9.1.7.2.5.1 Identification <Id>

Presence: [1..1]

Definition: Proprietary information, often a code, issued by the data source scheme issuer.

Datatype: "Max35Text" on page 519

9.1.7.2.5.2 Version <Vrsn>

Presence: [1..1]

Definition: Version of the identification.

Datatype: "Max35Text" on page 519

9.1.7.2.5.3 Issuer <Issr>

Presence: [1..1]

Definition: Entity that assigns the identification.

Datatype: "Max35Text" on page 519

9.1.7.2.6 Characteristics <Chrtcs>

Presence: [0..1]

Definition: Characteristics of a POI (Point Of Interaction) component.

Characteristics <Chrtcs> contains the following **PointOfInteractionComponentCharacteristics8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Memory <*Mmry*>	[0..*]			263
	Identification <*Id*>	[1..1]	Text		264
	TotalSize <*TtlSz*>	[1..1]	Quantity		264
	FreeSize <*FreeSz*>	[1..1]	Quantity		264
	Unit <*Unit*>	[1..1]	CodeSet		264
	Communication <*Com*>	[0..*]			264
	CommunicationType <*ComTp*>	[1..1]	CodeSet		265
	RemoteParty <*RmotPty*>	[1..*]	CodeSet		266
	Active <*Actv*>	[1..1]	Indicator		266
	Parameters <*Params*>	[0..1]	±		266
	PhysicalInterface <*PhysIntrfc*>	[0..1]			267
	InterfaceName <*IntrfcNm*>	[1..1]	Text		267
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		267
	UserName <*UsrNm*>	[0..1]	Text		268
	AccessCode <*AccsCd*>	[0..1]	Binary		268
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		268
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		268
	SecurityAccessModules <*SctyAccsMdls*>	[0..1]	Quantity		269
	SubscriberIdentityModules <*SbcbrIdntyMdls*>	[0..1]	Quantity		269
	SecurityElement <*SctyElmt*>	[0..*]	±		269

9.1.7.2.6.1 Memory <Mmry>

Presence: [0..*]

Definition: Memory characteristics of the component.

Memory <Mmry> contains the following **MemoryCharacteristics1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		264
	TotalSize <*TtlSz*>	[1..1]	Quantity		264
	FreeSize <*FreeSz*>	[1..1]	Quantity		264
	Unit <*Unit*>	[1..1]	CodeSet		264

9.1.7.2.6.1.1 Identification <Id>

Presence: [1..1]

Definition: Identification or name of the memory.

Datatype: "Max35Text" on page 519

9.1.7.2.6.1.2 TotalSize <TtlSz>

Presence: [1..1]

Definition: Total size of the memory unit.

Datatype: "DecimalNumber" on page 514

9.1.7.2.6.1.3 FreeSize <FreeSz>

Presence: [1..1]

Definition: Total size of the available memory.

Datatype: "DecimalNumber" on page 514

9.1.7.2.6.1.4 Unit <Unit>

Presence: [1..1]

Definition: Memory unit of the sizes.

Datatype: "MemoryUnit1Code" on page 490

CodeName	Name	Definition
BYTE	Byte	Byte.
EXAB	ExaByte	Exa byte.
GIGA	GigaByte	Giga byte.
KILO	KiloByte	Kilo byte.
MEGA	MegaByte	Mega byte.
PETA	PetaByte	Peta byte.
TERA	TeraByte	Tera byte.

9.1.7.2.6.2 Communication <Com>

Presence: [0..*]

Definition: Low level communication of the hardware or software component toward another component or an external entity.

Communication <Com> contains the following **CommunicationCharacteristics5** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CommunicationType <*ComTp*>	[1..1]	CodeSet		265
	RemoteParty <*RmotPty*>	[1..*]	CodeSet		266
	Active <*Actv*>	[1..1]	Indicator		266
	Parameters <*Params*>	[0..1]	±		266
	PhysicalInterface <*PhysIntrfc*>	[0..1]			267
	InterfaceName <*IntrfcNm*>	[1..1]	Text		267
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		267
	UserName <*UsrNm*>	[0..1]	Text		268
	AccessCode <*AccsCd*>	[0..1]	Binary		268
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		268
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		268

9.1.7.2.6.2.1 CommunicationType <ComTp>

Presence: [1..1]

Definition: Type of low level communication.

Datatype: "POICommunicationType2Code" on page 497

CodeName	Name	Definition
BLTH	Bluetooth	Communication with a host using Bluetooth.
ETHR	Ethernet	Ethernet port to communicate.
GPRS	GPRS	Communication with a host using GPRS.
GSMF	GSM	Communication with a host using GSM.
PSTN	PSTN	Communication with a host using Public Switching Telephone Network.
RS23	RS232	Serial port to communicate.
USBD	USBDevice	Communication with a USB stick or any USB device.
USBH	USBHost	Communication with a host from an USB port.
WIFI	Wifi	Wifi communication with another component.
WT2G	WirelessTechnology2G	Includes all communication technologies which can be qualified as being part of the 2G technology (e.g EDGE or PDC).
WT3G	WirelessTechnology3G	Includes all communication technologies which can be qualified as being part of the 3G technology.

CodeName	Name	Definition
WT4G	WirelessTechnology4G	Includes all communication technologies which can be qualified as being part of the 4G technology.
WT5G	WirelessTechnology5G	Includes all communication technologies which can be qualified as being part of the 5G technology.

9.1.7.2.6.2.2 RemoteParty <RmotPty>

Presence: [1..*]

Definition: Entity that communicate with the current component, using this communication device.

Datatype: "PartyType7Code" on page 496

CodeName	Name	Definition
ACQR	Acquirer	Entity acquiring card transactions.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
PCPT	POIComponent	Party component of a POI system or POI terminal (Point of Interaction).
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.
SALE	SaleSystem	Party selling goods and services.

9.1.7.2.6.2.3 Active <Actv>

Presence: [1..1]

Definition: Communication hardware is activated.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.2.6.2.4 Parameters <Params>

Presence: [0..1]

Definition: Network parameters of the communication link.

Parameters <Params> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.7.2.6.2.5 PhysicalInterface <PhysIntrfc>

Presence: [0..1]

Definition: Physical Interface used by the communication link.

PhysicalInterface <PhysIntrfc> contains the following **PhysicalInterfaceParameter1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	InterfaceName <*IntrfcNm*>	[1..1]	Text		267
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		267
	UserName <*UsrNm*>	[0..1]	Text		268
	AccessCode <*AccsCd*>	[0..1]	Binary		268
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		268
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		268

9.1.7.2.6.2.5.1 InterfaceName <IntrfcNm>

Presence: [1..1]

Definition: Identification of the interface.

Datatype: "Max35Text" on page 519

9.1.7.2.6.2.5.2 InterfaceType <IntrfcTp>

Presence: [0..1]

Definition: Identification of the physical link layer.

Datatype: "POICommunicationType2Code" on page 497

CodeName	Name	Definition
BLTH	Bluetooth	Communication with a host using Bluetooth.
ETHR	Ethernet	Ethernet port to communicate.
GPRS	GPRS	Communication with a host using GPRS.
GSMF	GSM	Communication with a host using GSM.
PSTN	PSTN	Communication with a host using Public Switching Telephone Network.
RS23	RS232	Serial port to communicate.
USBD	USBDevice	Communication with a USB stick or any USB device.
USBH	USBHost	Communication with a host from an USB port.
WIFI	Wifi	Wifi communication with another component.
WT2G	WirelessTechnology2G	Includes all communication technologies which can be qualified as being part of the 2G technology (e.g EDGE or PDC).
WT3G	WirelessTechnology3G	Includes all communication technologies which can be qualified as being part of the 3G technology.
WT4G	WirelessTechnology4G	Includes all communication technologies which can be qualified as being part of the 4G technology.
WT5G	WirelessTechnology5G	Includes all communication technologies which can be qualified as being part of the 5G technology.

9.1.7.2.6.2.5.3 UserName <UsrNm>

Presence: [0..1]

Definition: Optional user name to provide to use this interface.

Datatype: "Max35Text" on page 519

9.1.7.2.6.2.5.4 AccessCode <AccsCd>

Presence: [0..1]

Definition: Optional access code to provide to use this interface.

Datatype: "Max35Binary" on page 462

9.1.7.2.6.2.5.5 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the optional security profile to use with this interface.

Datatype: "Max35Text" on page 519

9.1.7.2.6.2.5.6 AdditionalParameters <AddtlParams>

Presence: [0..1]

Definition: Any other parameters relevant for this interface.

Datatype: "Max2KBinary" on page 462

9.1.7.2.6.3 SecurityAccessModules <SctyAccsMdls>

Presence: [0..1]

Definition: Number of security access modules (SAM).

Datatype: "Number" on page 515

9.1.7.2.6.4 SubscriberIdentityModules <SbcbrIdntyMdls>

Presence: [0..1]

Definition: Number of subscriber identity modules (SIM).

Datatype: "Number" on page 515

9.1.7.2.6.5 SecurityElement <SctyElmt>

Presence: [0..*]

Definition: Security characteristics of the component.

SecurityElement <SctyElmt> contains the following elements (see "CryptographicKey16" on page 419 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		419
	AdditionalIdentification <*AddtlId*>	[0..1]	Binary		419
	Name <*Nm*>	[0..1]	Text		420
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		420
	ItemNumber <*ItmNb*>	[0..1]	Text		420
	Version <*Vrsn*>	[1..1]	Text		420
	Type <*Tp*>	[0..1]	CodeSet		420
	Function <*Fctn*>	[0..*]	CodeSet		421
	ActivationDate <*ActvtnDt*>	[0..1]	DateTime		421
	DeactivationDate <*DeactvtnDt*>	[0..1]	DateTime		422
	KeyValue <*KeyVal*>	[0..1]	±		422
	KeyCheckValue <*KeyChckVal*>	[0..1]	Binary		422
	AdditionalManagementInformation <*AddtlMgmtInf*>	[0..*]			422
	Name <*Nm*>	[1..1]	Text		422
	Value <*Val*>	[0..1]	Text		423

9.1.7.2.7 Assessment <Assmnt>

Presence: [0..*]

Definition: Assessments for the component of the point of interaction.

Assessment <Assmnt> contains the following **PointOfInteractionComponentAssessment1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		270
	Assigner <*Assgnr*>	[1..*]	Text		270
	DeliveryDate <*DlvryDt*>	[0..1]	DateTime		270
	ExpirationDate <*XprtnDt*>	[0..1]	DateTime		270
	Number <*Nb*>	[1..1]	Text		270

9.1.7.2.7.1 Type <Tp>

Presence: [1..1]

Definition: Type of assessment of the component.

Datatype: "POIComponentAssessment1Code" on page 498

CodeName	Name	Definition
APPL	Approval	Approval number delivered by an approval centre.
CERT	Certification	Certification number delivered by a certification body.
EVAL	Evaluation	Evaluation by a lab or a tool.

9.1.7.2.7.2 Assigner <Assgnr>

Presence: [1..*]

Definition: Body which has delivered the assessment.

Datatype: "Max35Text" on page 519

9.1.7.2.7.3 DeliveryDate <DlvryDt>

Presence: [0..1]

Definition: Date when the assessment has been delivered.

Datatype: "ISODateTime" on page 513

9.1.7.2.7.4 ExpirationDate <XprtnDt>

Presence: [0..1]

Definition: Date when the assessment will expire.

Datatype: "ISODateTime" on page 513

9.1.7.2.7.5 Number <Nb>

Presence: [1..1]

Definition: Unique assessment number for the component.

Datatype: "Max35Text" on page 519

9.1.7.2.8 Package <Packg>

Presence: [0..*]

Definition: Chunk of a software package.

Package <Packg> contains the following **PackageType3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PackageIdentification <*PackgId*>	[0..1]	±		271
	PackageLength <*PackgLngth*>	[0..1]	Quantity		271
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		271
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		272
	PackageBlock <*PackgBlck*>	[0..*]			272
	Identification <*Id*>	[1..1]	Text		272
	Value <*Val*>	[0..1]	Binary		272
	ProtectedValue <*PrtctdVal*>	[0..1]	±		272
	Type <*Tp*>	[0..1]	Text		273

9.1.7.2.8.1 PackageIdentification <PackgId>

Presence: [0..1]

Definition: Identification of the software packages of which the chunk belongs.

PackageIdentification <PackgId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.7.2.8.2 PackageLength <PackgLngth>

Presence: [0..1]

Definition: Full length of software package identified through PackageIdentification.

Datatype: "PositiveNumber" on page 515

9.1.7.2.8.3 OffsetStart <OffsetStart>

Presence: [0..1]

Definition: Place of the first following PackageBlock, beginning with 0, in the full software package identified through PackageIdentification.

Datatype: "PositiveNumber" on page 515

9.1.7.2.8.4 OffsetEnd <OffsetEnd>

Presence: [0..1]

Definition: Following place of the last following PackageBlock in the full software package identified through PackageIdentification.

Datatype: "PositiveNumber" on page 515

9.1.7.2.8.5 PackageBlock <PackgBlck>

Presence: [0..*]

Definition: Consecutive slices of the full software package identified through PackageIdentification starting with first slice at the place identified with OffsetStart and ending with the last slice at the previous place identified with OffsetEnd.

PackageBlock <PackgBlck> contains the following **ExternallyDefinedData3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		272
	Value <*Val*>	[0..1]	Binary		272
	ProtectedValue <*PrtctdVal*>	[0..1]	±		272
	Type <*Tp*>	[0..1]	Text		273

9.1.7.2.8.5.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the set of data to exchange.

Datatype: "Max1025Text" on page 516

9.1.7.2.8.5.2 Value <Val>

Presence: [0..1]

Definition: Data to exchange according to an external standard.

Datatype: "Max100KBinary" on page 461

9.1.7.2.8.5.3 ProtectedValue <PrtctdVal>

Presence: [0..1]

Definition: Protection of the values to exchange.

ProtectedValue <PrtctdVal> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.7.2.8.5.4 Type <Tp>

Presence: [0..1]

Definition: Identification of the standard used to encode the values to exchange.

Datatype: "Max1025Text" on page 516

9.1.7.3 ActionMessage9

Definition: Information to display, print or store.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MessageDestination <*MsgDstn*>	[1..1]	CodeSet		273
	InformationQualifier <*InfQlfr*>	[0..1]	CodeSet		274
	Format <*Frmt*>	[0..1]	CodeSet		275
	MessageContent <*MsgCntt*>	[0..1]	Text		275
	MessageContentSignature <*MsgCnttSgntr*>	[0..1]	±		275
	OutputBarcode <*OutptBrcd*>	[0..1]			275
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277
	ResponseRequiredFlag <*RspnReqrdFlg*>	[0..1]	Indicator		277
	MinimumDisplayTime <*MinDispTm*>	[0..1]	Quantity		277

9.1.7.3.1 MessageDestination <MsgDstn>

Presence: [1..1]

Definition: Destination of the message.

Datatype: "UserInterface4Code" on page 512

CodeName	Name	Definition
CDSP	CardholderDisplay	Cardholder display or interface.
CRCP	CardholderReceipt	Cardholder receipt.
MDSP	MerchantDisplay	Merchant display or interface.
MRCP	MerchantReceipt	Merchant receipt.
CRDO	OtherCardholderInterface	Other interface of the cardholder, for instance e-mail or smartphone message.

9.1.7.3.2 InformationQualifier <InfQlfr>

Presence: [0..1]

Definition: Qualification of the information to sent to an output logical device.

Datatype: "InformationQualify1Code" on page 487

CodeName	Name	Definition
CUSA	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
DISP	Display	Standard display interface.
DOCT	Document	When the POI System wants to print specific document (check, dynamic currency conversion ...). Used by the Sale System when the printer is not located on the Sale System.
ERRO	Error	The information is related to an error situation occurring on the message sender.
INPT	Input	Answer to a question or information to be entered by the Cashier or the Customer, at the request of the POI Terminal or the Sale Terminal.
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
RCPT	Receipt	Where you print the Payment receipt that could be located on the Sale System or in some cases a restricted Sale ticket on the POI Terminal.
SOND	Sound	Standard sound interface.
STAT	Status	The information is a new state on which the message sender is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
VCHR	Voucher	Coupons, voucher or special ticket generated by the POI or the Sale System and to be printed.

9.1.7.3.3 Format <Frmt>

Presence: [0..1]

Definition: Message format.

Datatype: "OutputFormat3Code" on page 493

CodeName	Name	Definition
BARC	Barcode	Barcode to output in several possible format.
MENT	MenuEntry	A text to display as a menu before requesting an input.
MREF	MessageReference	Predefined configured messages, identified by a reference.
SREF	ScreenReference	Screen to display identified by a reference.
TEXT	SimpleText	Text without format attributes.
HTML	XHTML	XHTML document which includes a subset of the XHTML output tag.

9.1.7.3.4 MessageContent <MsgCntt>

Presence: [0..1]

Definition: Content or reference of the message.

Datatype: "Max20000Text" on page 517

9.1.7.3.5 MessageContentSignature <MsgCnttSgntr>

Presence: [0..1]

Definition: Digital signature of the message.

MessageContentSignature <MsgCnttSgntr> contains the following elements (see "ContentInformationType29" on page 427 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

9.1.7.3.6 OutputBarcode <OutptBrcd>

Presence: [0..1]

Definition: Content of message displayed or printed as Barcode.

OutputBarcode <OutptBrcd> contains the following **OutputBarcode1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	BarcodeType <*BrcdTp*>	[1..1]	CodeSet		276
	BarcodeValue <*BrcdVal*>	[0..1]	Text		276
	QRCodeBinaryValue <*QRCdBinryVal*>	[0..1]	Binary		276
	QRCodeVersion <*QRCdVrsn*>	[0..1]	Text		277
	QRCodeEncodingMode <*QRCdNcodgMd*>	[1..1]	CodeSet		277
	QRCodeErrorCorrection <*QRCdErrCrrctn*>	[0..1]	CodeSet		277

9.1.7.3.6.1 BarcodeType <BrcdTp>

Presence: [1..1]

Definition: Type of Barcode coding.

Datatype: "BarcodeType1Code" on page 475

CodeName	Name	Definition
COQR	BarcodeEncodedAs2DQRCode	Barcode encoded according to the 2Dimensions Quick Response Code Standard.
C128	BarcodeEncodedAsCode128	Barcode encoded according to the Code 128 standard.
C025	BarcodeEncodedAsCode25	Barcode encoded according to the Code 25 standard.
C039	BarcodeEncodedAsCode39	Barcode encoded according to the Code 39 standard.
EA13	BarcodeEncodedAsEA13	Barcode encoded according to the EAN13 standard.
EAN8	BarcodeEncodedAsEAN8	Barcode encoded according to the EAN8 standard.
P417	BarcodeEncodedAsPDF417	Barcode encoded according to the PDF417 standard.
UPCA	BarcodeEncodedAsUPCA	Barcode encoded according to the UPCA standard.

9.1.7.3.6.2 BarcodeValue <BrcdVal>

Presence: [0..1]

Definition: Value with a Barcode coding.

Datatype: "Max8000Text" on page 520

9.1.7.3.6.3 QRCodeBinaryValue <QRCdBinryVal>

Presence: [0..1]

Definition: Use for binary and Kanji Quick Respone Code.

Datatype: "Max3000Binary" on page 462

9.1.7.3.6.4 QRCodeVersion <QRCdVrsn>

Presence: [0..1]

Definition: Version of the Quick Response Code.

Datatype: "Max16Text" on page 517

9.1.7.3.6.5 QRCodeEncodingMode <QRCdNcodgMd>

Presence: [1..1]

Definition: Encoding Mode of Quick Response Code.

Datatype: "QRCodeEncodingMode1Code" on page 500

CodeName	Name	Definition
ALFA	Alphanumeric	Alphanumeric value provided in Barcode field.
BINA	Binary	Binary value provided in Quick Response Code Binary Value.
KANJ	Kanji	Kanji value provided in Quick Response Code Binary Value.
NUME	Numeric	Numeric value provided in Barcode field.

9.1.7.3.6.6 QRCodeErrorCorrection <QRCdErrCrrctn>

Presence: [0..1]

Definition: Error Correction mode of Quick Response Code.

Datatype: "QRCodeErrorCorrection1Code" on page 500

CodeName	Name	Definition
M015	ErrorCorrection15Percent	Reed-Solomon error correction 15%
Q025	ErrorCorrection25Percent	Reed-Solomon error correction 25%
H030	ErrorCorrection30Percent	Reed-Solomon error correction 30%
L007	ErrorCorrection7Percent	Reed-Solomon error correction 7%

9.1.7.3.7 ResponseRequiredFlag <RspnReqrdFlg>

Presence: [0..1]

Definition: Flag to request a message response.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.3.8 MinimumDisplayTime <MinDispTm>

Presence: [0..1]

Definition: Number of seconds the message has to be displayed.

Datatype: "Number" on page 515

9.1.7.4 KEKIdentifier7

Definition: Identification of a key encryption key (KEK), using previously distributed symmetric key.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.7.4.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 517

9.1.7.4.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 517

9.1.7.4.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 515

9.1.7.4.4 DerivationIdentification <DerivtnId>

Presence: [0..1]

Definition: Identification used for derivation of a unique key from a master key provided for the data protection.

Datatype: "Max500Binary" on page 463

9.1.7.5 DataSetIdentification9

Definition: Identification of a data set.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

9.1.7.5.1 Name <Nm>

Presence: [0..1]

Definition: Name of the data set.

Datatype: "Max256Text" on page 518

9.1.7.5.2 Type <Tp>

Presence: [1..1]

Definition: Category of data set.

Datatype: "DataSetCategory17Code" on page 483

CodeName	Name	Definition
AQPR	AcquirerParameters	Acquirer specific configuration parameters for the point of interaction (POI) system.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
TXCP	BatchCapture	Batch upload of transaction data (data capture of a group of transactions).
AKCP	CaptureResponse	Batch download response for the batch capture of transactions.
DLGT	DelegationData	Data needed to create a terminal management sub-domain.
MGTP	ManagementPlan	Configuration of management plan in the point of interaction.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
SCPR	SecurityParameters	Point of interaction parameters related to the security of software application and application protocol.
SWPK	SoftwareModule	Software module.
STRP	StatusReport	Report of software configuration and parameter status.
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
VDPR	VendorParameters	Point of interaction parameters defined by the manufacturer for instance the PIN verification capabilities.
PARA	Parameters	Any combination of configuration parameters for the point of interaction (POI).
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
LOGF	LogFile	Any repository used for recording log traces.

CodeName	Name	Definition
CMRQ	CertificateManagementRequest	Trigger for CertificateManagementRequest.
MDFL	MediaFile	Media file managed by an application of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

9.1.7.5.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data set.

Datatype: "Max256Text" on page 518

9.1.7.5.4 CreationDateTime <CreDtTm>

Presence: [0..1]

Definition: Date and time of creation of the data set.

Datatype: "ISODateTime" on page 513

9.1.7.6 CardPaymentEnvironment78

Definition: Environment of the transaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Acquirer <*Acqrr*>	[0..1]	±		286
	Merchant <*Mrchnt*>	[0..1]			286
	Identification <*Id*>	[0..1]	±		286
	CommonName <*CmonNm*>	[0..1]	Text		287
	LocationCategory <*LctnCtgy*>	[0..1]	CodeSet		287
	LocationAndContact <*LctnAndCtct*>	[0..1]	±		287
	SchemeData <*SchmeData*>	[0..1]	Text		288
	POI <*POI*>	[0..1]			288
	Identification <*Id*>	[1..1]	±		288
	SystemName <*SysNm*>	[0..1]	Text		289
	GroupIdentification <*GrpId*>	[0..1]	Text		289
	Capabilities <*Cpblties*>	[0..1]	±		289
	TimeZone <*TmZone*>	[0..1]	Text		290
	TerminalIntegration <*TermnlIntgtn*>	[0..1]	CodeSet		290
	Component <*Cmpnt*>	[0..*]	±		291
	Card <*Card*>	[0..1]			293
	ProtectedCardData <*PrtctdCardData*>	[0..1]	±		294
	PrivateCardData <*PrvtCardData*>	[0..1]	Binary		294
	PlainCardData <*PlainCardData*>	[0..1]	±		294
	PaymentAccountReference <*PmtAcctRef*>	[0..1]	Text		295
	MaskedPAN <*MskdPAN*>	[0..1]	Text		295
	IssuerBIN <*IssrBIN*>	[0..1]	Text		295
	CardCountryCode <*CardCtryCd*>	[0..1]	Text		295
	CardCurrencyCode <*CardCcyCd*>	[0..1]	Text		295
	CardProductProfile <*CardPdctPrfl*>	[0..1]	Text		296
	CardBrand <*CardBrnd*>	[0..1]	Text		296
	CardProductType <*CardPdctTp*>	[0..1]	CodeSet		296
	CardProductSubType <*CardPdctSubTp*>	[0..1]	Text		296
	InternationalCard <*IntrnlCard*>	[0..1]	Indicator		296
	AllowedProduct <*AllwdPdct*>	[0..*]	Text		296
	ServiceOption <*SvcOptn*>	[0..1]	Text		297

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AdditionalCardData <*AddtlCardData*>	[0..1]	Text		297
	Check <*Chck*>	[0..1]			297
	BankIdentification <*BkId*>	[0..1]	Text		297
	AccountNumber <*AcctNb*>	[0..1]	Text		297
	CheckNumber <*ChckNb*>	[0..1]	Text		297
	CheckCardNumber <*ChckCardNb*>	[0..1]	Text		298
	CheckTrackData2 <*ChckTrckData2*>	[0..1]			298
	TrackNumber <*TrckNb*>	[0..1]	Quantity		298
	TrackFormat <*TrckFrmt*>	[0..1]	CodeSet		298
	TrackValue <*TrckVal*>	[1..1]	Text		299
	CheckType <*ChckTp*>	[0..1]	CodeSet		299
	Country <*Ctry*>	[0..1]	Text		299
	StoredValueAccount <*StordValAcct*>	[0..*]			299
	AccountType <*AcctTp*>	[0..1]	CodeSet		300
	IdentificationType <*IdTp*>	[0..1]	CodeSet		301
	Identification <*Id*>	[0..1]	Text		301
	Brand <*Brnd*>	[0..1]	Text		301
	Provider <*Prvdr*>	[0..1]	Text		301
	OwnerName <*OwnrNm*>	[0..1]	Text		301
	ExpiryDate <*XpryDt*>	[0..1]	Text		302
	EntryMode <*NtryMd*>	[0..1]	CodeSet		302
	Currency <*Ccy*>	[0..1]	CodeSet	C1	302
	Balance <*Bal*>	[0..1]	Amount		303
	LoyaltyAccount <*LltyAcct*>	[0..*]	±		303
	CustomerDevice <*CstmrDvc*>	[0..1]	±		303
	Wallet <*Wllt*>	[0..1]	±		303
	PaymentToken <*PmtTkn*>	[0..1]	±		304
	MerchantToken <*MrchntTkn*>	[0..1]	±		304
	Cardholder <*Crdhldr*>	[0..1]			305
	Identification <*Id*>	[0..1]			309
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		309

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		309
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		310
	DriverIdentification <*DrvrId*>	[0..1]	Text		310
	CustomerNumber <*CstmrNb*>	[0..1]	Text		310
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		310
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		310
	PassportNumber <*PsptNb*>	[0..1]	Text		310
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		310
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		310
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		311
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		311
	JobNumber <*JobNb*>	[0..1]	Text		311
	Department <*Dept*>	[0..1]	Text		311
	EmailAddress <*EmailAdr*>	[0..1]	Text		311
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			311
	BirthDate <*BirthDt*>	[1..1]	Date		311
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		312
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		312
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	312
	Other <*Othr*>	[0..*]	±		312
	Name <*Nm*>	[0..1]	Text		312
	Language <*Lang*>	[0..1]	CodeSet	C6	312
	BillingAddress <*BllgAdr*>	[0..1]	±		313
	ShippingAddress <*ShppgAdr*>	[0..1]	±		313
	TripNumber <*TripNb*>	[0..1]	Text		314
	Vehicle <*Vhcl*>	[0..1]	±		314
	Authentication <*Authntcn*>	[0..*]			315
	AuthenticationMethod <*AuthntcnMtd*>	[0..1]	CodeSet		317
	AuthenticationExemption <*AuthntcnXmptn*>	[0..1]	CodeSet		318
	AuthenticationValue <*AuthntcnVal*>	[0..1]	Binary		319
	ProtectedAuthenticationValue <*PrtctdAuthntcnVal*>	[0..1]	±		319

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardholderOnLinePIN <*CrdhldrOnLinePIN*>	[0..1]			319
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		319
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		320
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		320
	CardholderIdentification <*CrdhldrId*>	[0..1]			320
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		321
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		321
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		321
	DriverIdentification <*DrvrId*>	[0..1]	Text		322
	CustomerNumber <*CstmrNb*>	[0..1]	Text		322
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		322
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		322
	PassportNumber <*PsptNb*>	[0..1]	Text		322
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		322
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		322
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		322
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		323
	JobNumber <*JobNb*>	[0..1]	Text		323
	Department <*Dept*>	[0..1]	Text		323
	EmailAddress <*EmailAdr*>	[0..1]	Text		323
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			323
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324
	Other <*Othr*>	[0..*]	±		324
	AddressVerification <*AdrVrfctn*>	[0..1]			324
	AddressDigits <*AdrDgts*>	[0..1]	Text		324
	PostalCodeDigits <*PstlCdDgts*>	[0..1]	Text		325
	AuthenticationType <*AuthntcnTp*>	[0..1]	Text		325
	AuthenticationLevel <*AuthntcnLvl*>	[0..1]	Text		325

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AuthenticationResult <*AuthntcnRslt*>	[0..1]	CodeSet		325
	AuthenticationAdditionalInformation <*AuthntcnAddtlInf*>	[0..1]			325
	Identification <*Id*>	[1..1]	Text		326
	Value <*Val*>	[0..1]	Binary		326
	ProtectedValue <*PrtctdVal*>	[0..1]	±		326
	Type <*Tp*>	[0..1]	Text		326
	TransactionVerificationResult <*TxVrfctnRslt*>	[0..*]			326
	Method <*Mtd*>	[1..1]	CodeSet		327
	VerificationEntity <*VrfctnNtty*>	[0..1]	CodeSet		328
	Result <*Rslt*>	[0..1]	CodeSet		328
	AdditionalResult <*AddtlRslt*>	[0..1]	Text		328
	PersonalData <*PrsnlData*>	[0..1]	Text		329
	MobileData <*MobData*>	[0..*]			329
	MobileCountryCode <*MobCtryCd*>	[0..1]	Text		329
	MobileNetworkCode <*MobNtwkCd*>	[0..1]	Text		329
	MobileMaskedMSISDN <*MobMskdMSISDN*>	[0..1]	Text		330
	Geolocation <*Glctn*>	[0..1]			330
	GeographicCoordinates <*GeogcCordints*>	[0..1]			330
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330
	UTMCoordinates <*UTMCordints*>	[0..1]			331
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331
	SensitiveMobileData <*SnstvMobData*>	[0..1]			331
	MSISDN <*MSISDN*>	[1..1]	Text		332
	IMSI <*IMSI*>	[0..1]	Text		332
	IMEI <*IMEI*>	[0..1]	Text		332
	ProtectedMobileData <*PrtctdMobData*>	[0..1]	±		332
	ProtectedCardholderData <*PrtctdCrdhldrData*>	[0..1]	±		332
	SaleEnvironment <*SaleEnvt*>	[0..1]			333

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SaleCapabilities <*SaleCpblties*>	[0..*]	CodeSet		333
	Currency <*Ccy*>	[0..1]	CodeSet	C1	334
	MinimumAmountToDeliver <*MinAmtToDlvr*>	[0..1]	Amount		334
	MaximumCashBackAmount <*MaxCshBckAmt*>	[0..1]	Amount		334
	MinimumSplitAmount <*MinSpltAmt*>	[0..1]	Amount		335
	DebitPreferredFlag <*DbtPrefrdFlg*>	[0..1]	Indicator		335
	LoyaltyHandling <*LltyHdlg*>	[0..1]	CodeSet		335

9.1.7.6.1 Acquirer <Acqrr>

Presence: [0..1]

Definition: Acquirer involved in the card payment.

Acquirer <Acqrr> contains the following elements (see "Acquirer10" on page 129 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]	±		129
	ParametersVersion <*ParamsVrsn*>	[0..1]	Text		129

9.1.7.6.2 Merchant <Mrchnt>

Presence: [0..1]

Definition: Merchant performing the card payment transaction.

Usage: In some cases, merchant and acceptor may be regarded as the same entity.

Merchant <Mrchnt> contains the following **Organisation41** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]	±		286
	CommonName <*CmonNm*>	[0..1]	Text		287
	LocationCategory <*LctnCtgy*>	[0..1]	CodeSet		287
	LocationAndContact <*LctnAndCtct*>	[0..1]	±		287
	SchemeData <*SchmeData*>	[0..1]	Text		288

9.1.7.6.2.1 Identification <Id>

Presence: [0..1]

Definition: Identification of the merchant.

Identification <Id> contains the following elements (see "GenericIdentification32" on page 247 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		247
	Type <*Tp*>	[0..1]	CodeSet		247
	Issuer <*Issr*>	[0..1]	CodeSet		248
	ShortName <*ShrtNm*>	[0..1]	Text		248

9.1.7.6.2.2 CommonName <CmonNm>

Presence: [0..1]

Definition: Name of the merchant as appearing on the receipt.

Datatype: "Max70Text" on page 520

9.1.7.6.2.3 LocationCategory <LctnCtgy>

Presence: [0..1]

Definition: Location category of the place where the merchant actually performed the transaction.

Datatype: "LocationCategory4Code" on page 490

CodeName	Name	Definition
ABRD	Aboard	Aboard is used when the sale is done in a vehicle (e.g a bus, train, ship, airplane, taxi, etc).
NMDC	Nomadic	Nomadic is used when the merchant is traveling to different locations (e.g fair or sport events, home delivery, food truck).
FIXD	PhysicalShop	Fixed location, for example in a shop.
VIRT	VirtualShop	Virtual Shop is used for any ecommerce solution.

9.1.7.6.2.4 LocationAndContact <LctnAndCtct>

Presence: [0..1]

Definition: Location and contact information of the merchant performing the transaction.

LocationAndContact <LctnAndCtct> contains the following elements (see "CommunicationAddress9" on page 192 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PostalAddress <*PstlAdr*>	[0..1]	±		192
	Email <*Email*>	[0..1]	Text		192
	URLAddress <*URLAdr*>	[0..1]	Text		193
	Phone <*Phne*>	[0..1]	Text		193
	CustomerService <*CstmrSvc*>	[0..1]	Text		193
	AdditionalContactInformation <*AddtlCtctInf*>	[0..1]	Text		193

9.1.7.6.2.5 SchemeData <SchmeData>

Presence: [0..1]

Definition: Additional merchant data required by a card scheme.

Datatype: "Max140Text" on page 517

9.1.7.6.3 POI <POI>

Presence: [0..1]

Definition: Point of interaction (POI) performing the transaction.

POI <POI> contains the following **PointOfInteraction12** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	±		288
	SystemName <*SysNm*>	[0..1]	Text		289
	GroupIdentification <*GrpId*>	[0..1]	Text		289
	Capabilities <*Cpblties*>	[0..1]	±		289
	TimeZone <*TmZone*>	[0..1]	Text		290
	TerminalIntegration <*TermnlIntgtn*>	[0..1]	CodeSet		290
	Component <*Cmpnt*>	[0..*]	±		291

9.1.7.6.3.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the POI (Point Of Interaction) for the acquirer or its agent.

Identification <Id> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

9.1.7.6.3.2 SystemName <SysNm>

Presence: [0..1]

Definition: Common name assigned by the acquirer to the POI (Point Of Interaction) system.

Datatype: "Max70Text" on page 520

9.1.7.6.3.3 GroupIdentification <GrpId>

Presence: [0..1]

Definition: Identifier assigned by the merchant identifying a set of POI (Point Of Interaction) terminals performing some categories of transactions.

Datatype: "Max35Text" on page 519

9.1.7.6.3.4 Capabilities <Cpblties>

Presence: [0..1]

Definition: Capabilities of the POI (Point Of Interaction) performing the transaction.

Capabilities <Cpblties> contains the following elements (see "PointOfInteractionCapabilities9" on page 377 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardReadingCapabilities <*CardRdngCpblties*>	[0..*]	CodeSet		378
	CardholderVerificationCapabilities <*CrdhldrVrfctnCpblties*>	[0..*]	CodeSet		379
	PINLengthCapabilities <*PINLngthCpblties*>	[0..1]	Quantity		379
	ApprovalCodeLength <*ApprvlCdLngth*>	[0..1]	Quantity		379
	MaxScriptLength <*MxScrptLngth*>	[0..1]	Quantity		380
	CardCaptureCapable <*CardCaptrCpbl*>	[0..1]	Indicator		380
	OnLineCapabilities <*OnLineCpblties*>	[0..1]	CodeSet		380
	MessageCapabilities <*MsgCpblties*>	[0..*]			380
	Destination <*Dstn*>	[1..*]	CodeSet		380
	AvailableFormat <*AvlblFrmt*>	[0..*]	CodeSet		381
	NumberOfLines <*NbOfLines*>	[0..1]	Quantity		381
	LineWidth <*LineWidth*>	[0..1]	Quantity		381
	AvailableLanguage <*AvlblLang*>	[0..*]	CodeSet	C6	381

9.1.7.6.3.5 TimeZone <TmZone>

Presence: [0..1]

Definition: Time zone name as defined by IANA (Internet Assigned Numbers Authority) in the time zone data base. America/Chicago or Europe/Paris are examples of time zone names.

Datatype: "Max70Text" on page 520

9.1.7.6.3.6 TerminalIntegration <TermnlIntgtn>

Presence: [0..1]

Definition: Indicates the type of integration of the POI terminal in the sale environment.

Datatype: "LocationCategory3Code" on page 489

CodeName	Name	Definition
INDR	Indoor	Indoor terminal.
IPMP	InsidePump	Terminal incorporated in the pump dispensing petrol.
MPOI	MultiplePOITerminal	Multiple terminals linked to a unique sale terminal.
MPMP	MultiplePump	Outdoor terminal serving several petrol pumps.
MSLE	MultipleSaleTerminal	Terminal serving multiple sale terminals.
SSLE	SingleSaleTerminal	Terminal linked to a unique sale terminal.

CodeName	Name	Definition
VNDG	VendingMachine	Terminal integrated in a vending machine.

9.1.7.6.3.7 Component <Cmpnt>

Presence: [0..*]

Definition: Data related to a component of the POI (Point Of Interaction) performing the transaction.

Component <Cmpnt> contains the following elements (see "PointOfInteractionComponent12" on page 256 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		258
	SubTypeInformation <*SubTpInf*>	[0..1]	Text		259
	Identification <*Id*>	[1..1]			260
	ItemNumber <*ItmNb*>	[0..1]	Text		260
	ProviderIdentification <*PrvdrId*>	[0..1]	Text		260
	Identification <*Id*>	[0..1]	Text		260
	SerialNumber <*SrlNb*>	[0..1]	Text		260
	Status <*Sts*>	[0..1]			260
	VersionNumber <*VrsnNb*>	[0..1]	Text		261
	Status <*Sts*>	[0..1]	CodeSet		261
	ExpiryDate <*XpryDt*>	[0..1]	Date		261
	StandardCompliance <*StdCmplc*>	[0..*]			261
	Identification <*Id*>	[1..1]	Text		261
	Version <*Vrsn*>	[1..1]	Text		262
	Issuer <*Issr*>	[1..1]	Text		262
	Characteristics <*Chrtcs*>	[0..1]			262
	Memory <*Mmry*>	[0..*]			263
	Identification <*Id*>	[1..1]	Text		264
	TotalSize <*TtlSz*>	[1..1]	Quantity		264
	FreeSize <*FreeSz*>	[1..1]	Quantity		264
	Unit <*Unit*>	[1..1]	CodeSet		264
	Communication <*Com*>	[0..*]			264
	CommunicationType <*ComTp*>	[1..1]	CodeSet		265
	RemoteParty <*RmotPty*>	[1..*]	CodeSet		266
	Active <*Actv*>	[1..1]	Indicator		266
	Parameters <*Params*>	[0..1]	±		266
	PhysicalInterface <*PhysIntrfc*>	[0..1]			267
	InterfaceName <*IntrfcNm*>	[1..1]	Text		267
	InterfaceType <*IntrfcTp*>	[0..1]	CodeSet		267
	UserName <*UsrNm*>	[0..1]	Text		268

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AccessCode <*AccsCd*>	[0..1]	Binary		268
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		268
	AdditionalParameters <*AddtlParams*>	[0..1]	Binary		268
	SecurityAccessModules <*SctyAccsMdls*>	[0..1]	Quantity		269
	SubscriberIdentityModules <*SbcbrIdntyMdls*>	[0..1]	Quantity		269
	SecurityElement <*SctyElmt*>	[0..*]	±		269
	Assessment <*Assmnt*>	[0..*]			269
	Type <*Tp*>	[1..1]	CodeSet		270
	Assigner <*Assgnr*>	[1..*]	Text		270
	DeliveryDate <*DlvryDt*>	[0..1]	DateTime		270
	ExpirationDate <*XprtnDt*>	[0..1]	DateTime		270
	Number <*Nb*>	[1..1]	Text		270
	Package <*Packg*>	[0..*]			271
	PackageIdentification <*PackgId*>	[0..1]	±		271
	PackageLength <*PackgLngth*>	[0..1]	Quantity		271
	OffsetStart <*OffsetStart*>	[0..1]	Quantity		271
	OffsetEnd <*OffsetEnd*>	[0..1]	Quantity		272
	PackageBlock <*PackgBlck*>	[0..*]			272
	Identification <*Id*>	[1..1]	Text		272
	Value <*Val*>	[0..1]	Binary		272
	ProtectedValue <*PrtctdVal*>	[0..1]	±		272
	Type <*Tp*>	[0..1]	Text		273

9.1.7.6.4 Card <Card>

Presence: [0..1]

Definition: Payment card performing the transaction.

Card <Card> contains the following **PaymentCard32** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ProtectedCardData <*PrtctdCardData*>	[0..1]	±		294
	PrivateCardData <*PrvtCardData*>	[0..1]	Binary		294
	PlainCardData <*PlainCardData*>	[0..1]	±		294
	PaymentAccountReference <*PmtAcctRef*>	[0..1]	Text		295
	MaskedPAN <*MskdPAN*>	[0..1]	Text		295
	IssuerBIN <*IssrBIN*>	[0..1]	Text		295
	CardCountryCode <*CardCtryCd*>	[0..1]	Text		295
	CardCurrencyCode <*CardCcyCd*>	[0..1]	Text		295
	CardProductProfile <*CardPdctPrfl*>	[0..1]	Text		296
	CardBrand <*CardBrnd*>	[0..1]	Text		296
	CardProductType <*CardPdctTp*>	[0..1]	CodeSet		296
	CardProductSubType <*CardPdctSubTp*>	[0..1]	Text		296
	InternationalCard <*IntrnlCard*>	[0..1]	Indicator		296
	AllowedProduct <*AllwdPdct*>	[0..*]	Text		296
	ServiceOption <*SvcOptn*>	[0..1]	Text		297
	AdditionalCardData <*AddtlCardData*>	[0..1]	Text		297

9.1.7.6.4.1 ProtectedCardData <PrtctdCardData>

Presence: [0..1]

Definition: Replacement of the message element PlainCardData by a digital envelope using a cryptographic key.

ProtectedCardData <PrtctdCardData> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.7.6.4.2 PrivateCardData <PrvtCardData>

Presence: [0..1]

Definition: Replacement of the message element PlainCardData by a private envelope.

Datatype: "Max100KBinary" on page 461

9.1.7.6.4.3 PlainCardData <PlainCardData>

Presence: [0..1]

Definition: Sensitive data associated with the card performing the transaction.

PlainCardData <PlainCardData> contains the following elements (see "PlainCardData15" on page 193 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PAN <*PAN*>	[1..1]	Text		194
	CardSequenceNumber <*CardSeqNb*>	[0..1]	Text		194
	EffectiveDate <*FctvDt*>	[0..1]	Text		194
	ExpiryDate <*XpryDt*>	[1..1]	Text		194
	ServiceCode <*SvcCd*>	[0..1]	Text		194
	Track1 <*Trck1*>	[0..1]	Text		194
	Track2 <*Trck2*>	[0..1]	Text		194
	Track3 <*Trck3*>	[0..1]	Text		194
	CardholderName <*CrdhldrNm*>	[0..1]	Text		195

9.1.7.6.4.4 PaymentAccountReference <PmtAcctRef>

Presence: [0..1]

Definition: Unique reference to the card, used by both merchants and acquirers to link tokenized and non-tokenized transactions associated to the same underlying card.

Datatype: "Max70Text" on page 520

9.1.7.6.4.5 MaskedPAN <MskdPAN>

Presence: [0..1]

Definition: Masked PAN to be printed on payment receipts or displayed to the cardholder. Masked digits may be absent or replaced by another character as '*'.

Datatype: "Max30Text" on page 518

9.1.7.6.4.6 IssuerBIN <IssrBIN>

Presence: [0..1]

Definition: Bank identifier number of the issuer for routing purpose.

Datatype: "Max15NumericText" on page 517

9.1.7.6.4.7 CardCountryCode <CardCtryCd>

Presence: [0..1]

Definition: Country code assigned to the card by the card issuer.

Datatype: "Max3Text" on page 519

9.1.7.6.4.8 CardCurrencyCode <CardCcyCd>

Presence: [0..1]

Definition: Currency code of the card issuer (ISO 4217 numeric code).

Datatype: "Exact3AlphaNumericText" on page 515

9.1.7.6.4.9 CardProductProfile <CardPdctPrfl>

Presence: [0..1]

Definition: Defines a category of cards related to the acceptance processing rules defined by the acquirer.

Datatype: "Max35Text" on page 519

9.1.7.6.4.10 CardBrand <CardBrnd>

Presence: [0..1]

Definition: Brand name of the card.

Datatype: "Max35Text" on page 519

9.1.7.6.4.11 CardProductType <CardPdctTp>

Presence: [0..1]

Definition: Type of card product.

Datatype: "CardProductType1Code" on page 480

CodeName	Name	Definition
COMM	CommercialCard	Cards issued as a means of business expenditure, for instance business card or corporate card. The user could be a company, an individual for business expenses or a self employed for business purposes.
CONS	ConsumerCard	Cards issued as a means of personal expenditure. The user is always an individual.

9.1.7.6.4.12 CardProductSubType <CardPdctSubTp>

Presence: [0..1]

Definition: Additional information to identify CardProduct.

Datatype: "Max35Text" on page 519

9.1.7.6.4.13 InternationalCard <IntrnlCard>

Presence: [0..1]

Definition: True if the card may be used abroad.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.6.4.14 AllowedProduct <AllwdPdct>

Presence: [0..*]

Definition: Product that can be purchased with the card.

Datatype: "Max70Text" on page 520

9.1.7.6.4.15 ServiceOption <SvcOptn>

Presence: [0..1]

Definition: Options to the service provided by the card.

Datatype: "Max35Text" on page 519

9.1.7.6.4.16 AdditionalCardData <AddtlCardData>

Presence: [0..1]

Definition: Additional card issuer specific data.

Datatype: "Max70Text" on page 520

9.1.7.6.5 Check <Chck>

Presence: [0..1]

Definition: Check Payment instrument.

Check <Chck> contains the following **Check1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	BankIdentification <*BkId*>	[0..1]	Text		297
	AccountNumber <*AcctNb*>	[0..1]	Text		297
	CheckNumber <*ChckNb*>	[0..1]	Text		297
	CheckCardNumber <*ChckCardNb*>	[0..1]	Text		298
	CheckTrackData2 <*ChckTrckData2*>	[0..1]			298
	TrackNumber <*TrckNb*>	[0..1]	Quantity		298
	TrackFormat <*TrckFrmt*>	[0..1]	CodeSet		298
	TrackValue <*TrckVal*>	[1..1]	Text		299
	CheckType <*ChckTp*>	[0..1]	CodeSet		299
	Country <*Ctry*>	[0..1]	Text		299

9.1.7.6.5.1 BankIdentification <BkId>

Presence: [0..1]

Definition: Identification of the institution (bank) issuing the check.

Datatype: "Max35Text" on page 519

9.1.7.6.5.2 AccountNumber <AcctNb>

Presence: [0..1]

Definition: Identification of the account linked to the check.

Datatype: "Max35Text" on page 519

9.1.7.6.5.3 CheckNumber <ChckNb>

Presence: [0..1]

Definition: Identification of the check.

Datatype: "Max35Text" on page 519

9.1.7.6.5.4 CheckCardNumber <ChckCardNb>

Presence: [0..1]

Definition: Check guarantee card number.

The human readable number from the Check Guarantee Card that is presented during the check tendering process.

Datatype: "Max35Text" on page 519

9.1.7.6.5.5 CheckTrackData2 <ChckTrckData2>

Presence: [0..1]

Definition: Track Data of the check to digitally identify the data.

CheckTrackData2 <ChckTrckData2> contains the following **TrackData2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TrackNumber <*TrckNb*>	[0..1]	Quantity		298
	TrackFormat <*TrckFrmt*>	[0..1]	CodeSet		298
	TrackValue <*TrckVal*>	[1..1]	Text		299

9.1.7.6.5.5.1 TrackNumber <TrckNb>

Presence: [0..1]

Definition: Track number of the card.

Datatype: "Number" on page 515

9.1.7.6.5.5.2 TrackFormat <TrckFrmt>

Presence: [0..1]

Definition: Card or check track format.

Datatype: "TrackFormat1Code" on page 510

CodeName	Name	Definition
AAMV	AAMVAFormat	American driver license.
CMC7	CMC7CheckFormat	Magnetic Ink Character Recognition, using the CMC-7 font - ISO 1004 Line at the bottom of a check containing the bank account and the check number.
E13B	E13BCheckFormat	Magnetic Ink Character Recognition, using the E-13B font) Line at the bottom of a check containing the bank account and the check number.
ISOF	ISOFormat	ISO card track format - ISO 7813 - ISO 4909.
JIS1	JISIFormat	Japanese track format I.

CodeName	Name	Definition
JIS2	JISIIFormat	Japanese track format II.

9.1.7.6.5.5.3 TrackValue <TrckVal>

Presence: [1..1]

Definition: Card track content or equivalent.

Datatype: "Max140Text" on page 517

9.1.7.6.5.6 CheckType <ChckTp>

Presence: [0..1]

Definition: Type of the check (personal or professional).

Datatype: "CheckType1Code" on page 480

CodeName	Name	Definition
BANK	BankCheck	The check is guaranteed by a bank.
BUSI	BusinessCheck	The check belongs to a Company or a professional entity.
GOVC	GovernmentCheck	Check issued by Government.
PAYR	PayrollCheck	Check issued by a company for the employees.
PERS	PersonalCheck	The check belongs to an individual.

9.1.7.6.5.7 Country <Ctry>

Presence: [0..1]

Definition: Country of the check.

Datatype: "Max3Text" on page 519

9.1.7.6.6 StoredValueAccount <StordValAcct>

Presence: [0..*]

Definition: Store value account payment instrument.

StoredValueAccount <StordValAcct> contains the following **StoredValueAccount2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AccountType <*AcctTp*>	[0..1]	CodeSet		300
	IdentificationType <*IdTp*>	[0..1]	CodeSet		301
	Identification <*Id*>	[0..1]	Text		301
	Brand <*Brnd*>	[0..1]	Text		301
	Provider <*Prvdr*>	[0..1]	Text		301
	OwnerName <*OwnrNm*>	[0..1]	Text		301
	ExpiryDate <*XpryDt*>	[0..1]	Text		302
	EntryMode <*NtryMd*>	[0..1]	CodeSet		302
	Currency <*Ccy*>	[0..1]	CodeSet	C1	302
	Balance <*Bal*>	[0..1]	Amount		303

9.1.7.6.6.1 AccountType <AcctTp>

Presence: [0..1]

Definition: Type of stored value account.

Datatype: "StoredValueAccountType1Code" on page 506

CodeName	Name	Definition
BNKA	BankPrepaidAccount	Prepaid account managed by a financial institution for low income customers.
CWVC	CarwashVoucher	Car wash specific account.
CPYA	CompanyPrepaidAccount	Specific prepaid account for companies or professionals expenses.
ELMY	ElectronicMoneyAccount	Account supporting e-money issued by an electronic money issuer.
GIFT	GiftCard	Payment mean issued by retailers or banks as a substitute to a non-monetary gift. Usually, this Stored Value item is used only once.
GCER	GiftCertificate	Certificate to be given to a customer. Usually one shot voucher.
MLVC	MealVoucher	Meal and check voucher for restaurants.
OLVC	OnlineVoucher	Voucher that can be used online once or in several times.
MERC	MerchantAccount	Prepaid account open with a merchant or big retailers.
OTHR	OtherPrepaidAccount	Other non listed stored value instrument.
PHON	PhoneCard	Stored value instrument used to pay telephone services (e.g. card or identifier).

CodeName	Name	Definition
CARD	SmartCardTag	Stored value account hold on the chip of a smart card.
TRVL	Travel	Travel prepaid account.

9.1.7.6.6.2 IdentificationType <IdTp>

Presence: [0..1]

Definition: Type of identification for this Stored Value Account.

Datatype: "CardIdentificationType1Code" on page 479

CodeName	Name	Definition
ACCT	AccountNumber	Account identification.
BARC	BarCode	Bar-code with a specific form of identification.
ISO2	ISOTrack2	ISO Track 2 including identification.
PHON	PhoneNumber	A phone number identifies the account on which the phone card is assigned.
CPAN	PrimaryAccountNumber	Standard card identification (card number).
PRIV	PrivativeNumbering	An identification set by a privative application.
UUID	UniversalUniqueIdentification	A Universal Unique Identification code is set for identification.

9.1.7.6.6.3 Identification <Id>

Presence: [0..1]

Definition: Identification of Stored Value Account.

Datatype: "Max35Text" on page 519

9.1.7.6.6.4 Brand <Brnd>

Presence: [0..1]

Definition: Brand to which belong the account.

Datatype: "Max35Text" on page 519

9.1.7.6.6.5 Provider <Prvdr>

Presence: [0..1]

Definition: Provider of the Stored Value Account.

Datatype: "Max35Text" on page 519

9.1.7.6.6.6 OwnerName <OwnrNm>

Presence: [0..1]

Definition: Owner name of an account.

Datatype: "Max45Text" on page 519

9.1.7.6.6.7 ExpiryDate <XpryDt>

Presence: [0..1]

Definition: Expiry date of the account of card.

Datatype: "Max10Text" on page 516

9.1.7.6.6.8 EntryMode <NtryMd>

Presence: [0..1]

Definition: Standard or last entry mode to access the Stored Value account or card.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.7.6.6.9 Currency <Ccy>

Presence: [0..1]

Definition: Currency of the Stored Value account.

Impacted by: C1 "ActiveCurrency"

Datatype: "ActiveCurrencyCode" on page 463

Constraints

- **ActiveCurrency**

  The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217

Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

9.1.7.6.6.10 Balance <Bal>

Presence: [0..1]

Definition: Current balance of the Stored Value account.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.7.6.7 LoyaltyAccount <LltyAcct>

Presence: [0..*]

Definition: Store value account associated to the payment.

LoyaltyAccount <LltyAcct> contains the following elements (see "LoyaltyAccount3" on page 335 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	LoyaltyIdentification <*LltyId*>	[1..1]	Text		336
	EntryMode <*NtryMd*>	[0..1]	CodeSet		336
	IdentificationType <*IdTp*>	[0..1]	CodeSet		337
	Brand <*Brnd*>	[0..1]	Text		337
	Provider <*Prvdr*>	[0..1]	Text		337
	OwnerName <*OwnrNm*>	[0..1]	Text		337
	Unit <*Unit*>	[0..1]	CodeSet		337
	Currency <*Ccy*>	[0..1]	CodeSet	C1	338
	Balance <*Bal*>	[0..1]	Amount		338

9.1.7.6.8 CustomerDevice <CstmrDvc>

Presence: [0..1]

Definition: Device used by the customer to perform the payment transaction.

CustomerDevice <CstmrDvc> contains the following elements (see "CustomerDevice3" on page 376 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]	Text		376
	Type <*Tp*>	[0..1]	Text		376
	Provider <*Prvdr*>	[0..1]	Text		376

9.1.7.6.9 Wallet <Wllt>

Presence: [0..1]

Definition: Container for tenders used by the customer to perform the payment transaction.

Wallet <Wllt> contains the following elements (see "CustomerDevice3" on page 376 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]	Text		376
	Type <*Tp*>	[0..1]	Text		376
	Provider <*Prvdr*>	[0..1]	Text		376

9.1.7.6.10 PaymentToken <PmtTkn>

Presence: [0..1]

Definition: Payment token information.

PaymentToken <PmtTkn> contains the following elements (see "Token1" on page 457 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PaymentToken <*PmtTkn*>	[0..1]	Text		458
	TokenExpiryDate <*TknXpryDt*>	[0..1]	Text		458
	TokenRequestorIdentification <*TknRqstrId*>	[0..1]	Text		458
	TokenAssuranceData <*TknAssrncData*>	[0..1]	Text		458
	TokenAssuranceMethod <*TknAssrncMtd*>	[0..1]	Text		458
	TokenInitiatedIndicator <*TknInittdInd*>	[0..1]	Indicator		458

9.1.7.6.11 MerchantToken <MrchntTkn>

Presence: [0..1]

Definition: Merchant token information.

MerchantToken <MrchntTkn> contains the following elements (see "MerchantToken2" on page 458 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Token <*Tkn*>	[0..1]	Text		459
	TokenExpiryDate <*TknXpryDt*>	[0..1]	Text		459
	TokenCharacteristic <*TknChrtc*>	[0..*]	Text		459
	TokenRequestor <*TknRqstr*>	[0..1]			459
	ProviderIdentification <*PrvdrId*>	[1..1]	Text		459
	RequestorIdentification <*RqstrId*>	[1..1]	Text		460
	TokenAssuranceLevel <*TknAssrncLvl*>	[0..1]	Quantity		460
	TokenAssuranceData <*TknAssrncData*>	[0..1]	Binary		460
	TokenAssuranceMethod <*TknAssrncMtd*>	[0..1]	Text		460
	TokenInitiatedIndicator <*TknInittdInd*>	[0..1]	Indicator		460

9.1.7.6.12 Cardholder <Crdhldr>

Presence: [0..1]

Definition: Cardholder involved in the card payment.

Cardholder <CrdhIdr> contains the following **Cardholder18** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]			309
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		309
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		309
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		310
	DriverIdentification <*DrvrId*>	[0..1]	Text		310
	CustomerNumber <*CstmrNb*>	[0..1]	Text		310
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		310
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		310
	PassportNumber <*PsptNb*>	[0..1]	Text		310
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		310
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		310
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		311
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		311
	JobNumber <*JobNb*>	[0..1]	Text		311
	Department <*Dept*>	[0..1]	Text		311
	EmailAddress <*EmailAdr*>	[0..1]	Text		311
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			311
	BirthDate <*BirthDt*>	[1..1]	Date		311
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		312
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		312
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	312
	Other <*Othr*>	[0..*]	±		312
	Name <*Nm*>	[0..1]	Text		312
	Language <*Lang*>	[0..1]	CodeSet	C6	312
	BillingAddress <*BllgAdr*>	[0..1]	±		313
	ShippingAddress <*ShppgAdr*>	[0..1]	±		313
	TripNumber <*TripNb*>	[0..1]	Text		314
	Vehicle <*Vhcl*>	[0..1]	±		314
	Authentication <*Authntcn*>	[0..*]			315
	AuthenticationMethod <*AuthntcnMtd*>	[0..1]	CodeSet		317
	AuthenticationExemption <*AuthntcnXmptn*>	[0..1]	CodeSet		318

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AuthenticationValue <*AuthntcnVal*>	[0..1]	Binary		319
	ProtectedAuthenticationValue <*PrtctdAuthntcnVal*>	[0..1]	±		319
	CardholderOnLinePIN <*CrdhldrOnLinePIN*>	[0..1]			319
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		319
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		320
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		320
	CardholderIdentification <*CrdhldrId*>	[0..1]			320
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		321
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		321
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		321
	DriverIdentification <*DrvrId*>	[0..1]	Text		322
	CustomerNumber <*CstmrNb*>	[0..1]	Text		322
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		322
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		322
	PassportNumber <*PsptNb*>	[0..1]	Text		322
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		322
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		322
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		322
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		323
	JobNumber <*JobNb*>	[0..1]	Text		323
	Department <*Dept*>	[0..1]	Text		323
	EmailAddress <*EmailAdr*>	[0..1]	Text		323
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			323
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324
	Other <*Othr*>	[0..*]	±		324
	AddressVerification <*AdrVrfctn*>	[0..1]			324
	AddressDigits <*AdrDgts*>	[0..1]	Text		324
	PostalCodeDigits <*PstlCdDgts*>	[0..1]	Text		325

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AuthenticationType <*AuthntcnTp*>	[0..1]	Text		325
	AuthenticationLevel <*AuthntcnLvl*>	[0..1]	Text		325
	AuthenticationResult <*AuthntcnRslt*>	[0..1]	CodeSet		325
	AuthenticationAdditionalInformation <*AuthntcnAddtlInf*>	[0..1]			325
	Identification <*Id*>	[1..1]	Text		326
	Value <*Val*>	[0..1]	Binary		326
	ProtectedValue <*PrtctdVal*>	[0..1]	±		326
	Type <*Tp*>	[0..1]	Text		326
	TransactionVerificationResult <*TxVrfctnRslt*>	[0..*]			326
	Method <*Mtd*>	[1..1]	CodeSet		327
	VerificationEntity <*VrfctnNtty*>	[0..1]	CodeSet		328
	Result <*Rslt*>	[0..1]	CodeSet		328
	AdditionalResult <*AddtlRslt*>	[0..1]	Text		328
	PersonalData <*PrsnlData*>	[0..1]	Text		329
	MobileData <*MobData*>	[0..*]			329
	MobileCountryCode <*MobCtryCd*>	[0..1]	Text		329
	MobileNetworkCode <*MobNtwkCd*>	[0..1]	Text		329
	MobileMaskedMSISDN <*MobMskdMSISDN*>	[0..1]	Text		330
	Geolocation <*Glctn*>	[0..1]			330
	GeographicCoordinates <*GeogcCordints*>	[0..1]			330
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330
	UTMCoordinates <*UTMCordints*>	[0..1]			331
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331
	SensitiveMobileData <*SnstvMobData*>	[0..1]			331
	MSISDN <*MSISDN*>	[1..1]	Text		332
	IMSI <*IMSI*>	[0..1]	Text		332
	IMEI <*IMEI*>	[0..1]	Text		332
	ProtectedMobileData <*PrtctdMobData*>	[0..1]	±		332

9.1.7.6.12.1 Identification <Id>

Presence: [0..1]

Definition: Identification of the cardholder involved in a transaction.

Identification <Id> contains the following **PersonIdentification15** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		309
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		309
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		310
	DriverIdentification <*DrvrId*>	[0..1]	Text		310
	CustomerNumber <*CstmrNb*>	[0..1]	Text		310
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		310
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		310
	PassportNumber <*PsptNb*>	[0..1]	Text		310
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		310
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		310
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		311
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		311
	JobNumber <*JobNb*>	[0..1]	Text		311
	Department <*Dept*>	[0..1]	Text		311
	EmailAddress <*EmailAdr*>	[0..1]	Text		311
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			311
	BirthDate <*BirthDt*>	[1..1]	Date		311
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		312
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		312
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	312
	Other <*Othr*>	[0..*]	±		312

9.1.7.6.12.1.1 DriverLicenseNumber <DrvrLicNb>

Presence: [0..1]

Definition: Number assigned by a license authority to a driver's license.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.2 DriverLicenseLocation <DrvrLicLctn>

Presence: [0..1]

Definition: Country, state or province, issuer of the driver license.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.3 DriverLicenseName <DrvrLicNm>

Presence: [0..1]

Definition: Name or title of the driver license.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.4 DriverIdentification <DrvrId>

Presence: [0..1]

Definition: Identification of the driver in the fleet of vehicle.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.5 CustomerNumber <CstmrNb>

Presence: [0..1]

Definition: Number assigned by an agent to identify its customer.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.6 SocialSecurityNumber <SclSctyNb>

Presence: [0..1]

Definition: Number assigned by a social security agency.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.7 AlienRegistrationNumber <AlnRegnNb>

Presence: [0..1]

Definition: Number assigned by a government agency to identify foreign nationals.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.8 PassportNumber <PsptNb>

Presence: [0..1]

Definition: Number assigned by a passport authority to a passport.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.9 TaxIdentificationNumber <TaxIdNb>

Presence: [0..1]

Definition: Number assigned by a tax authority to an entity.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.10 IdentityCardNumber <IdntyCardNb>

Presence: [0..1]

Definition: Number assigned by a national authority to an identity card.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.11 EmployerIdentificationNumber <MplyrIdNb>

Presence: [0..1]

Definition: Number assigned to an employer by a registration authority.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.12 EmployeeIdentificationNumber <MplyeeIdNb>

Presence: [0..1]

Definition: Number assigned to an employee by a employer.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.13 JobNumber <JobNb>

Presence: [0..1]

Definition: Identification of the job.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.14 Department <Dept>

Presence: [0..1]

Definition: Identification of the department.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.15 EmailAddress <EmailAdr>

Presence: [0..1]

Definition: Address for electronic mail (e-mail).

Datatype: "Max256Text" on page 518

9.1.7.6.12.1.16 DateAndPlaceOfBirth <DtAndPlcOfBirth>

Presence: [0..1]

Definition: Date and place of birth of a person.

DateAndPlaceOfBirth <DtAndPlcOfBirth> contains the following **DateAndPlaceOfBirth1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	BirthDate <*BirthDt*>	[1..1]	Date		311
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		312
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		312
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	312

9.1.7.6.12.1.16.1 BirthDate <BirthDt>

Presence: [1..1]

Definition: Date on which a person is born.

Datatype: "ISODate" on page 512

9.1.7.6.12.1.16.2 ProvinceOfBirth <PrvcOfBirth>

Presence: [0..1]

Definition: Province where a person was born.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.16.3 CityOfBirth <CityOfBirth>

Presence: [1..1]

Definition: City where a person was born.

Datatype: "Max35Text" on page 519

9.1.7.6.12.1.16.4 CountryOfBirth <CtryOfBirth>

Presence: [1..1]

Definition: Country where a person was born.

Impacted by: C3 "Country"

Datatype: "CountryCode" on page 481

Constraints

- **Country**

  The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

9.1.7.6.12.1.17 Other <Othr>

Presence: [0..*]

Definition: Unique identification of a person, as assigned by an institution, using an identification scheme.

Other <Othr> contains the following elements (see "GenericIdentification4" on page 255 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		255
	IdentificationType <*IdTp*>	[1..1]	Text		255

9.1.7.6.12.2 Name <Nm>

Presence: [0..1]

Definition: Cardholder name associated with the card.

Datatype: "Max45Text" on page 519

9.1.7.6.12.3 Language <Lang>

Presence: [0..1]

Definition: Language selected for the cardholder interface during the transaction.

Reference ISO 639-1 (alpha-2) et ISO 639-2 (alpha-3).

Impacted by: C6 "ValidationByTable"

Datatype: "LanguageCode" on page 489

Constraints

- **ValidationByTable**

  Must be a valid terrestrial language.

9.1.7.6.12.4 BillingAddress <BllgAdr>

Presence: [0..1]

Definition: Postal address of the owner of the payment card.

BillingAddress <BllgAdr> contains the following elements (see "PostalAddress22" on page 398 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AddressType <*AdrTp*>	[0..1]	CodeSet		399
	Department <*Dept*>	[0..1]	Text		399
	SubDepartment <*SubDept*>	[0..1]	Text		399
	AddressLine <*AdrLine*>	[0..2]	Text		399
	StreetName <*StrtNm*>	[0..1]	Text		400
	BuildingNumber <*BldgNb*>	[0..1]	Text		400
	PostCode <*PstCd*>	[0..1]	Text		400
	TownName <*TwnNm*>	[0..1]	Text		400
	CountrySubDivision <*CtrySubDvsn*>	[0..2]	Text		400
	CountryCode <*CtryCd*>	[0..1]	Text		400

9.1.7.6.12.5 ShippingAddress <ShppgAdr>

Presence: [0..1]

Definition: Postal address for delivery of goods or services.

ShippingAddress <ShppgAdr> contains the following elements (see "PostalAddress22" on page 398 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AddressType <*AdrTp*>	[0..1]	CodeSet		399
	Department <*Dept*>	[0..1]	Text		399
	SubDepartment <*SubDept*>	[0..1]	Text		399
	AddressLine <*AdrLine*>	[0..2]	Text		399
	StreetName <*StrtNm*>	[0..1]	Text		400
	BuildingNumber <*BldgNb*>	[0..1]	Text		400
	PostCode <*PstCd*>	[0..1]	Text		400
	TownName <*TwnNm*>	[0..1]	Text		400
	CountrySubDivision <*CtrySubDvsn*>	[0..2]	Text		400
	CountryCode <*CtryCd*>	[0..1]	Text		400

9.1.7.6.12.6 TripNumber <TripNb>

Presence: [0..1]

Definition: Identification of the trip.

Datatype: "Max35Text" on page 519

9.1.7.6.12.7 Vehicle <Vhcl>

Presence: [0..1]

Definition: Information related to the vehicle used for the transaction.

Vehicle <Vhcl> contains the following elements (see "Vehicle1" on page 382 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	VehicleNumber <*VhclNb*>	[0..1]	Text		382
	TrailerNumber <*TrlrNb*>	[0..1]	Text		383
	VehicleTag <*VhclTag*>	[0..1]	Text		383
	VehicleTagEntryMode <*VhclTagNtryMd*>	[0..1]	CodeSet		383
	UnitNumber <*UnitNb*>	[0..1]	Text		383
	ReplacementCar <*RplcmntCar*>	[0..1]	Indicator		383
	Odometer <*Odmtr*>	[0..1]	Quantity		384
	Hubometer <*Hbmtr*>	[0..1]	Quantity		384
	TrailerHours <*TrlrHrs*>	[0..1]	Text		384
	ReferHours <*RefrHrs*>	[0..1]	Text		384
	MaintenanceIdentification <*MntncId*>	[0..1]	Text		384
	DriverOrVehicleCard <*DrvrOrVhclCard*>	[0..1]			384
	PAN <*PAN*>	[0..1]	Text		385
	Track1 <*Trck1*>	[0..1]	Text		385
	Track2 <*Trck2*>	[0..1]	Text		385
	Track3 <*Trck3*>	[0..1]	Text		385
	AdditionalCardData <*AddtlCardData*>	[0..*]	Text		385
	EntryMode <*NtryMd*>	[0..1]	CodeSet		385
	AdditionalVehicleData <*AddtlVhclData*>	[0..*]			386
	Type <*Tp*>	[0..1]	Text		386
	EntryMode <*NtryMd*>	[0..1]	CodeSet		386
	Data <*Data*>	[1..1]	Text		387

9.1.7.6.12.8 Authentication <Authntcn>

Presence: [0..*]

Definition: Method and data intended to be used for this transaction to authenticate the cardholder and its card.

Authentication <Authntcn> contains the following **CardholderAuthentication15** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AuthenticationMethod <*AuthntcnMtd*>	[0..1]	CodeSet		317
	AuthenticationExemption <*AuthntcnXmptn*>	[0..1]	CodeSet		318
	AuthenticationValue <*AuthntcnVal*>	[0..1]	Binary		319
	ProtectedAuthenticationValue <*PrtctdAuthntcnVal*>	[0..1]	±		319
	CardholderOnLinePIN <*CrdhldrOnLinePIN*>	[0..1]			319
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		319
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		320
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		320
	CardholderIdentification <*CrdhldrId*>	[0..1]			320
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		321
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		321
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		321
	DriverIdentification <*DrvrId*>	[0..1]	Text		322
	CustomerNumber <*CstmrNb*>	[0..1]	Text		322
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		322
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		322
	PassportNumber <*PsptNb*>	[0..1]	Text		322
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		322
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		322
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		322
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		323
	JobNumber <*JobNb*>	[0..1]	Text		323
	Department <*Dept*>	[0..1]	Text		323
	EmailAddress <*EmailAdr*>	[0..1]	Text		323
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			323
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324
	Other <*Othr*>	[0..*]	±		324
	AddressVerification <*AdrVrfctn*>	[0..1]			324

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AddressDigits <*AdrDgts*>	[0..1]	Text		324
	PostalCodeDigits <*PstlCdDgts*>	[0..1]	Text		325
	AuthenticationType <*AuthntcnTp*>	[0..1]	Text		325
	AuthenticationLevel <*AuthntcnLvl*>	[0..1]	Text		325
	AuthenticationResult <*AuthntcnRslt*>	[0..1]	CodeSet		325
	AuthenticationAdditionalInformation <*AuthntcnAddtlInf*>	[0..1]			325
	Identification <*Id*>	[1..1]	Text		326
	Value <*Val*>	[0..1]	Binary		326
	ProtectedValue <*PrtctdVal*>	[0..1]	±		326
	Type <*Tp*>	[0..1]	Text		326

9.1.7.6.12.8.1 AuthenticationMethod <AuthntcnMtd>

Presence: [0..1]

Definition: Method and data intended to be used for this transaction to authenticate the cardholder or its card.

Datatype: "AuthenticationMethod8Code" on page 473

CodeName	Name	Definition
TOKA	AuthenticationToken	A token is used to verify an already performed authentication.
ADDB	BillingAddressVerification	Cardholder billing address verification.
BYPS	Bypass	Authentication bypassed by the merchant.
BIOM	Biometry	Biometric authentication of the cardholder.
CDHI	CardholderIdentificationData	Cardholder data provided for verification, for instance social security number, driver license number, passport number.
CRYP	CryptogramVerification	Verification of a cryptogram generated by a chip card or another device, for instance ARQC (Authorisation Request Cryptogram).
CSCV	CSCVerification	Verification of Card Security Code.
MANU	ManualVerification	Manual verification, for example passport or drivers license.
MERC	MerchantAuthentication	Merchant-related authentication.
MOBL	Mobile	Customer mobile device.
FPIN	OfflinePIN	Off-line PIN authentication (Personal Identification Number).
NPIN	OnLinePIN	On-line PIN authentication (Personal Identification Number).

CodeName	Name	Definition
OTHR	Other	Other customer authentication.
PPSG	PaperSignature	Handwritten paper signature.
PSVE	PassiveAuthentication	Authentication based on statistical cardholder behaviour.
PSWD	Password	Authentication by a password.
TOKP	PaymentToken	Verification or authentication related to the use of a payment token, for instance the validation of the authorised use of a token.
SCRT	SecureCertificate	Electronic commerce transaction secured with the X.509 certificate of a customer.
SCNL	SecuredChannel	Channel-encrypted transaction.
CSEC	SecureElectronicCommerce	Authentication performed during a secure electronic commerce transaction.
SNCT	SecureNoCertificate	Secure electronic transaction without cardholder certificate.
ADDS	ShippingAddressVerification	Cardholder shipping address verification.
CPSG	SignatureCapture	Electronic signature capture (handwritten signature).
TOKN	TokenAuthentication	Cryptogram generated by the token requestor or a customer device to validate the authorised use of a token.
UKNW	UnknownMethod	Authentication method is performed unknown.

9.1.7.6.12.8.2 AuthenticationExemption <AuthntcnXmptn>

Presence: [0..1]

Definition: If Strong Customer Authentication is not mandated to process the transaction, this message element must identify the reason of exemption.

Datatype: "Exemption1Code" on page 486

CodeName	Name	Definition
LOWA	LowAmountExemption	Transaction's amount is low and could be processed without strong customer authentication.
MINT	MerchantInitiatedTransaction	Transaction is initiated by the Card Acceptor.
RECP	RecurringPayment	Transaction is one of a series of recurring payment.
SCPE	SecureCorporatePaymentExemption	Transaction is a secure corporate payment.
SCAD	StrongCustomerAuthenticationDelegation	Card Acceptor is a strong customer authentication delegate.

CodeName	Name	Definition
TRAE	TransactionRiskAnalysisExemption	According to the transaction risk analysis the strong customer authentication is not mandated.
PKGE	TransportFareOrParkingFeeUnattendedPaymentExemption	Payment is processed in a environment where strong customer authentication is inappropriate.
TMBE	TrustedMerchantBeneficiaryExemption	Cardholder has enrolled the Card Acceptor in the exemption list of strong customer authentication.

9.1.7.6.12.8.3 AuthenticationValue <AuthntcnVal>

Presence: [0..1]

Definition: Value used to authenticate the cardholder.

Datatype: "Max5000Binary" on page 462

9.1.7.6.12.8.4 ProtectedAuthenticationValue <PrtctdAuthntcnVal>

Presence: [0..1]

Definition: Protection of the authentication value.

ProtectedAuthenticationValue <PrtctdAuthntcnVal> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.7.6.12.8.5 CardholderOnLinePIN <CrdhldrOnLinePIN>

Presence: [0..1]

Definition: Encrypted personal identification number (PIN) and related information.

CardholderOnLinePIN <CrdhldrOnLinePIN> contains the following **OnLinePIN9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		319
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		320
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		320

9.1.7.6.12.8.5.1 EncryptedPINBlock <NcrptdPINBlck>

Presence: [1..1]

Definition: Encrypted PIN (Personal Identification Number).

EncryptedPINBlock <NcrptdPINBlck> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.7.6.12.8.5.2 PINFormat <PINFrmt>

Presence: [1..1]

Definition: PIN (Personal Identification Number) format before encryption.

Datatype: "PINFormat3Code" on page 496

CodeName	Name	Definition
ISO0	ISO0	PIN diversified with the card account number, conforming to the standard ISO 9564-2.
ISO1	ISO1	PIN completed with random padding characters, conforming to the standard ISO 9564-2.
ISO2	ISO2	PIN without diversification characters, conforming to the standard ISO 9564-2.
ISO3	ISO3	PIN diversified with the card account number and random characters, conforming to the standard ISO 9564-2.
ISO4	ISO4	PIN format used with AES encryption, conforming to the new ISO SC2 format.
ISO5	ISO5	Alternative PIN format used with AES encryption, conforming to the new ISO SC2 format.

9.1.7.6.12.8.5.3 AdditionalInput <AddtlInpt>

Presence: [0..1]

Definition: Additional information required to verify the PIN (Personal Identification Number).

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6 CardholderIdentification <CrdhldrId>

Presence: [0..1]

Definition: Identification of the cardholder to verify.

CardholderIdentification <CrdhldrId> contains the following **PersonIdentification15** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DriverLicenseNumber <*DrvrLicNb*>	[0..1]	Text		321
	DriverLicenseLocation <*DrvrLicLctn*>	[0..1]	Text		321
	DriverLicenseName <*DrvrLicNm*>	[0..1]	Text		321
	DriverIdentification <*DrvrId*>	[0..1]	Text		322
	CustomerNumber <*CstmrNb*>	[0..1]	Text		322
	SocialSecurityNumber <*SclSctyNb*>	[0..1]	Text		322
	AlienRegistrationNumber <*AlnRegnNb*>	[0..1]	Text		322
	PassportNumber <*PsptNb*>	[0..1]	Text		322
	TaxIdentificationNumber <*TaxIdNb*>	[0..1]	Text		322
	IdentityCardNumber <*IdntyCardNb*>	[0..1]	Text		322
	EmployerIdentificationNumber <*MplyrIdNb*>	[0..1]	Text		322
	EmployeeIdentificationNumber <*MplyeeIdNb*>	[0..1]	Text		323
	JobNumber <*JobNb*>	[0..1]	Text		323
	Department <*Dept*>	[0..1]	Text		323
	EmailAddress <*EmailAdr*>	[0..1]	Text		323
	DateAndPlaceOfBirth <*DtAndPlcOfBirth*>	[0..1]			323
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324
	Other <*Othr*>	[0..*]	±		324

9.1.7.6.12.8.6.1 DriverLicenseNumber <DrvrLicNb>

Presence: [0..1]

Definition: Number assigned by a license authority to a driver's license.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.2 DriverLicenseLocation <DrvrLicLctn>

Presence: [0..1]

Definition: Country, state or province, issuer of the driver license.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.3 DriverLicenseName <DrvrLicNm>

Presence: [0..1]

Definition: Name or title of the driver license.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.4 DriverIdentification <DrvrId>

Presence: [0..1]

Definition: Identification of the driver in the fleet of vehicle.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.5 CustomerNumber <CstmrNb>

Presence: [0..1]

Definition: Number assigned by an agent to identify its customer.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.6 SocialSecurityNumber <SclSctyNb>

Presence: [0..1]

Definition: Number assigned by a social security agency.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.7 AlienRegistrationNumber <AlnRegnNb>

Presence: [0..1]

Definition: Number assigned by a government agency to identify foreign nationals.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.8 PassportNumber <PsptNb>

Presence: [0..1]

Definition: Number assigned by a passport authority to a passport.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.9 TaxIdentificationNumber <TaxIdNb>

Presence: [0..1]

Definition: Number assigned by a tax authority to an entity.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.10 IdentityCardNumber <IdntyCardNb>

Presence: [0..1]

Definition: Number assigned by a national authority to an identity card.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.11 EmployerIdentificationNumber <MplyrIdNb>

Presence: [0..1]

Definition: Number assigned to an employer by a registration authority.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.12 EmployeeIdentificationNumber <MplyeeIdNb>

Presence: [0..1]

Definition: Number assigned to an employee by a employer.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.13 JobNumber <JobNb>

Presence: [0..1]

Definition: Identification of the job.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.14 Department <Dept>

Presence: [0..1]

Definition: Identification of the department.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.15 EmailAddress <EmailAdr>

Presence: [0..1]

Definition: Address for electronic mail (e-mail).

Datatype: "Max256Text" on page 518

9.1.7.6.12.8.6.16 DateAndPlaceOfBirth <DtAndPlcOfBirth>

Presence: [0..1]

Definition: Date and place of birth of a person.

DateAndPlaceOfBirth <DtAndPlcOfBirth> contains the following **DateAndPlaceOfBirth1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	BirthDate <*BirthDt*>	[1..1]	Date		323
	ProvinceOfBirth <*PrvcOfBirth*>	[0..1]	Text		323
	CityOfBirth <*CityOfBirth*>	[1..1]	Text		324
	CountryOfBirth <*CtryOfBirth*>	[1..1]	CodeSet	C3	324

9.1.7.6.12.8.6.16.1 BirthDate <BirthDt>

Presence: [1..1]

Definition: Date on which a person is born.

Datatype: "ISODate" on page 512

9.1.7.6.12.8.6.16.2 ProvinceOfBirth <PrvcOfBirth>

Presence: [0..1]

Definition: Province where a person was born.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.16.3 CityOfBirth <CityOfBirth>

Presence: [1..1]

Definition: City where a person was born.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.6.16.4 CountryOfBirth <CtryOfBirth>

Presence: [1..1]

Definition: Country where a person was born.

Impacted by: C3 "Country"

Datatype: "CountryCode" on page 481

Constraints

- **Country**

  The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

9.1.7.6.12.8.6.17 Other <Othr>

Presence: [0..*]

Definition: Unique identification of a person, as assigned by an institution, using an identification scheme.

Other <Othr> contains the following elements (see "GenericIdentification4" on page 255 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		255
	IdentificationType <*IdTp*>	[1..1]	Text		255

9.1.7.6.12.8.7 AddressVerification <AdrVrfctn>

Presence: [0..1]

Definition: Numeric characters of the cardholder's billing or shipping address for verification.

AddressVerification <AdrVrfctn> contains the following **AddressVerification1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AddressDigits <*AdrDgts*>	[0..1]	Text		324
	PostalCodeDigits <*PstlCdDgts*>	[0..1]	Text		325

9.1.7.6.12.8.7.1 AddressDigits <AdrDgts>

Presence: [0..1]

Definition: Numeric characters from the cardholder's address excluding the postal code (that is street number).

Datatype: "Max5NumericText" on page 520

9.1.7.6.12.8.7.2 PostalCodeDigits <PstlCdDgts>

Presence: [0..1]

Definition: Numeric characters from the cardholder's postal code.

Datatype: "Max5NumericText" on page 520

9.1.7.6.12.8.8 AuthenticationType <AuthntcnTp>

Presence: [0..1]

Definition: Type of authentication for a given method - e.g. three-domain authentication, scheme-proprietary authentication, etc.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.9 AuthenticationLevel <AuthntcnLvl>

Presence: [0..1]

Definition: Level of authentication for a given type - e.g. value assigned by scheme rules or by bilateral agreements.

Datatype: "Max35Text" on page 519

9.1.7.6.12.8.10 AuthenticationResult <AuthntcnRslt>

Presence: [0..1]

Definition: Result of authentication.

Datatype: "AuthenticationResult1Code" on page 475

CodeName	Name	Definition
DENY	Denial	The authentication didn't succeed.
MRCH	MerchantNotEnroled	Merchant not enrolled in the authentication programme.
CARD	NonParticipation	The card does not participate in the authentication programme.
AUTH	UnableToAuthenticate	The authentication couldn't be carried out.
CRPT	WithCryptogram	Authentication succeeded with a cryptogram.
UCRP	WithoutCryptogram	Authentication succeeded without a cryptogram.

9.1.7.6.12.8.11 AuthenticationAdditionalInformation <AuthntcnAddtlInf>

Presence: [0..1]

Definition: Additional information related to the result of the authentication.

AuthenticationAdditionalInformation <AuthntcnAddtlInf> contains the following **ExternallyDefinedData3** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		326
	Value <*Val*>	[0..1]	Binary		326
	ProtectedValue <*PrtctdVal*>	[0..1]	±		326
	Type <*Tp*>	[0..1]	Text		326

9.1.7.6.12.8.11.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the set of data to exchange.

Datatype: "Max1025Text" on page 516

9.1.7.6.12.8.11.2 Value <Val>

Presence: [0..1]

Definition: Data to exchange according to an external standard.

Datatype: "Max100KBinary" on page 461

9.1.7.6.12.8.11.3 ProtectedValue <PrtctdVal>

Presence: [0..1]

Definition: Protection of the values to exchange.

ProtectedValue <PrtctdVal> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.7.6.12.8.11.4 Type <Tp>

Presence: [0..1]

Definition: Identification of the standard used to encode the values to exchange.

Datatype: "Max1025Text" on page 516

9.1.7.6.12.9 TransactionVerificationResult <TxVrfctnRslt>

Presence: [0..*]

Definition: Result of performed verifications for the transaction.

TransactionVerificationResult <TxVrfctnRslt> contains the following **TransactionVerificationResult4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Method <*Mtd*>	[1..1]	CodeSet		327
	VerificationEntity <*VrfctnNtty*>	[0..1]	CodeSet		328
	Result <*Rslt*>	[0..1]	CodeSet		328
	AdditionalResult <*AddtlRslt*>	[0..1]	Text		328

9.1.7.6.12.9.1 Method <Mtd>

Presence: [1..1]

Definition: Method of verification that has been performed.

Datatype: "AuthenticationMethod6Code" on page 473

CodeName	Name	Definition
NPIN	OnLinePIN	On-line PIN authentication (Personal Identification Number).
PPSG	PaperSignature	Handwritten paper signature.
PSWD	Password	Authentication by a password.
SCRT	SecureCertificate	Electronic commerce transaction secured with the X.509 certificate of a customer.
SCNL	SecuredChannel	Channel-encrypted transaction.
SNCT	SecureNoCertificate	Secure electronic transaction without cardholder certificate.
CPSG	SignatureCapture	Electronic signature capture (handwritten signature).
ADDB	BillingAddressVerification	Cardholder billing address verification.
BIOM	Biometry	Biometric authentication of the cardholder.
CDHI	CardholderIdentificationData	Cardholder data provided for verification, for instance social security number, driver license number, passport number.
CRYP	CryptogramVerification	Verification of a cryptogram generated by a chip card or another device, for instance ARQC (Authorisation Request Cryptogram).
CSCV	CSCVerification	Verification of Card Security Code.
PSVE	PassiveAuthentication	Authentication based on statistical cardholder behaviour.
CSEC	SecureElectronicCommerce	Authentication performed during a secure electronic commerce transaction.
ADDS	ShippingAddressVerification	Cardholder shipping address verification.
MANU	ManualVerification	Manual verification, for example passport or drivers license.

CodeName	Name	Definition
FPIN	OfflinePIN	Off-line PIN authentication (Personal Identification Number).
TOKP	PaymentToken	Verification or authentication related to the use of a payment token, for instance the validation of the authorised use of a token.

9.1.7.6.12.9.2 VerificationEntity <VrfctnNtty>

Presence: [0..1]

Definition: Entity or device that has performed the verification.

Datatype: "AuthenticationEntity2Code" on page 472

CodeName	Name	Definition
ICCD	ICC	Application in the chip card (Integrated Circuit Card), for instance an offline PIN verification.
AGNT	AuthorisedAgent	Authorisation agent of the issuer.
MERC	Merchant	Merchant (for example signature verification by the attendant).
ACQR	Acquirer	Acquirer of the transaction.
ISSR	Issuer	Card issuer.
TRML	Terminal	Secure application in the terminal.

9.1.7.6.12.9.3 Result <Rslt>

Presence: [0..1]

Definition: Result of the verification.

Datatype: "Verification1Code" on page 512

CodeName	Name	Definition
FAIL	Failed	Verification failed.
MISS	Missing	Information required to perform the verification was missing.
NOVF	NotPerformed	Verification has not been performed.
PART	PartialMatch	Verification was partially successful.
SUCC	Successful	Verification was successful.
ERRR	TechnicalError	Device or entity to perform the verification was unavailable.

9.1.7.6.12.9.4 AdditionalResult <AddtlRslt>

Presence: [0..1]

Definition: Additional result of the verification.

Datatype: "Max500Text" on page 519

9.1.7.6.12.10 PersonalData <PrsnlData>

Presence: [0..1]

Definition: Identifies personal data related to the cardholder.

Datatype: "Max70Text" on page 520

9.1.7.6.12.11 MobileData <MobData>

Presence: [0..*]

Definition: Data related to the mobile of stakeholder.

MobileData <MobData> contains the following **MobileData4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MobileCountryCode <*MobCtryCd*>	[0..1]	Text		329
	MobileNetworkCode <*MobNtwkCd*>	[0..1]	Text		329
	MobileMaskedMSISDN <*MobMskdMSISDN*>	[0..1]	Text		330
	Geolocation <*Glctn*>	[0..1]			330
	GeographicCoordinates <*GeogcCordints*>	[0..1]			330
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330
	UTMCoordinates <*UTMCordints*>	[0..1]			331
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331
	SensitiveMobileData <*SnstvMobData*>	[0..1]			331
	MSISDN <*MSISDN*>	[1..1]	Text		332
	IMSI <*IMSI*>	[0..1]	Text		332
	IMEI <*IMEI*>	[0..1]	Text		332
	ProtectedMobileData <*PrtctdMobData*>	[0..1]	±		332

9.1.7.6.12.11.1 MobileCountryCode <MobCtryCd>

Presence: [0..1]

Definition: Identifies the country of a mobile phone operator.

Datatype: "Min2Max3AlphaText" on page 521

9.1.7.6.12.11.2 MobileNetworkCode <MobNtwkCd>

Presence: [0..1]

Definition: Identifies the mobile phone operator inside a country.

Datatype: "Min2Max3NumericText" on page 521

9.1.7.6.12.11.3 MobileMaskedMSISDN <MobMskdMSISDN>

Presence: [0..1]

Definition: Masked Mobile Subscriber Integrated Service Digital Network.

Datatype: "Max35Text" on page 519

9.1.7.6.12.11.4 Geolocation <Glctn>

Presence: [0..1]

Definition: Geographic location specified by geographic or UTM coordinates.

Geolocation <Glctn> contains the following **Geolocation1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	GeographicCoordinates <*GeogcCordints*>	[0..1]			330
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330
	UTMCoordinates <*UTMCordints*>	[0..1]			331
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331

9.1.7.6.12.11.4.1 GeographicCoordinates <GeogcCordints>

Presence: [0..1]

Definition: Geographic location specified by geographic coordinates.

GeographicCoordinates <GeogcCordints> contains the following **GeolocationGeographicCoordinates1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Latitude <*Lat*>	[1..1]	Text		330
	Longitude <*Long*>	[1..1]	Text		330

9.1.7.6.12.11.4.1.1 Latitude <Lat>

Presence: [1..1]

Definition: Angular distance of a location on the earth south or north of the equator.

The latitude is measured in degrees, minutes and seconds, following by "N" for the north and "S" for the south of the equator. For example: 48°51'29" N the Eiffel Tower latitude.

Datatype: "Max35Text" on page 519

9.1.7.6.12.11.4.1.2 Longitude <Long>

Presence: [1..1]

Definition: Angular measurement of the distance of a location on the earth east or west of the Greenwich observatory.

The longitude is measured in degrees, minutes and seconds, following by "E" for the east and "W" for the west. For example: 23°27'30" E.

Datatype: "Max35Text" on page 519

9.1.7.6.12.11.4.2 UTMCoordinates <UTMCordints>

Presence: [0..1]

Definition: Geographic location specified by UTM coordinates.

UTMCoordinates <UTMCordints> contains the following **GeolocationUTMCoordinates1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	UTMZone <*UTMZone*>	[1..1]	Text		331
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		331
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		331

9.1.7.6.12.11.4.2.1 UTMZone <UTMZone>

Presence: [1..1]

Definition: UTM grid zone combination of the longitude zone (1 to 60) and the latitude band (C to X, excluding I and O).

Datatype: "Max35Text" on page 519

9.1.7.6.12.11.4.2.2 UTMEastward <UTMEstwrd>

Presence: [1..1]

Definition: X-coordinate of the Universal Transverse Mercator

coordinate system.

Datatype: "Max35Text" on page 519

9.1.7.6.12.11.4.2.3 UTMNorthward <UTMNrthwrd>

Presence: [1..1]

Definition: Y-coordinate of the Universal Transverse Mercator

coordinate system.

Datatype: "Max35Text" on page 519

9.1.7.6.12.11.5 SensitiveMobileData <SnstvMobData>

Presence: [0..1]

Definition: Sensitive information related to the mobile phone.

SensitiveMobileData <SnstvMobData> contains the following **SensitiveMobileData1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MSISDN <*MSISDN*>	[1..1]	Text		332
	IMSI <*IMSI*>	[0..1]	Text		332
	IMEI <*IMEI*>	[0..1]	Text		332

9.1.7.6.12.11.5.1 MSISDN <MSISDN>

Presence: [1..1]

Definition: identifies the mobile - Mobile Subscriber Integrated Service Digital Network (The SIM identifier).

Datatype: "Max35NumericText" on page 518

9.1.7.6.12.11.5.2 IMSI <IMSI>

Presence: [0..1]

Definition: International Mobile Subscriber Identity is a unique number associated with the mobile phone user, containing the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Identification Number (MSIN).

Datatype: "Max35NumericText" on page 518

9.1.7.6.12.11.5.3 IMEI <IMEI>

Presence: [0..1]

Definition: International Mobile Equipment Identity is a number usually unique to identify a mobile phone.

Datatype: "Max35NumericText" on page 518

9.1.7.6.12.11.6 ProtectedMobileData <PrtctdMobData>

Presence: [0..1]

Definition: Sensitive information related to the mobile phone, protected by CMS.

ProtectedMobileData <PrtctdMobData> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.7.6.13 ProtectedCardholderData <PrtctdCrdhldrData>

Presence: [0..1]

Definition: Replacement of the message element Cardholder by a digital envelope using a cryptographic key.

ProtectedCardholderData <PrtctdCrdhldrData> contains the following elements (see "ContentInformationType32" on page 407 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.7.6.14 SaleEnvironment <SaleEnvt>

Presence: [0..1]

Definition: Sale Retailer Environment for this message.

SaleEnvironment <SaleEnvt> contains the following **RetailerSaleEnvironment2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SaleCapabilities <*SaleCpblties*>	[0..*]	CodeSet		333
	Currency <*Ccy*>	[0..1]	CodeSet	C1	334
	MinimumAmountToDeliver <*MinAmtToDlvr*>	[0..1]	Amount		334
	MaximumCashBackAmount <*MaxCshBckAmt*>	[0..1]	Amount		334
	MinimumSplitAmount <*MinSpltAmt*>	[0..1]	Amount		335
	DebitPreferredFlag <*DbtPrefrdFlg*>	[0..1]	Indicator		335
	LoyaltyHandling <*LltyHdlg*>	[0..1]	CodeSet		335

9.1.7.6.14.1 SaleCapabilities <SaleCpblties>

Presence: [0..*]

Definition: Capabilities of the Sale system.

Datatype: "SaleCapabilities1Code" on page 504

CodeName	Name	Definition
CHDI	CashierDisplay	Standard Cashier display interface (to ask question, or to show information).
CHER	CashierError	To display to the Cashier information related to an error situation occurring on the POI.
CHIN	CashierInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element). The output device attached to this input device is the CashierDisplay device.
CHST	CashierStatus	To display to the Cashier a new state on which the POI is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.

CodeName	Name	Definition
CUDI	CustomerDisplay	Standard Customer display interface used by the POI System to ask question, or to show information to the Customer inside a Service dialogue.
CUAS	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
CUER	CustomerError	To display to the Customer information is related to an error situation occurring on the Sale Terminal during a Sale transaction.
CUIN	CustomerInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element).
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
PRDC	PrinterDocument	When the POI System wants to print specific document (check, dynamic currency conversion ...).
PRRP	PrinterReceipt	Printer for the Payment receipt.
PRVC	PrinterVoucher	Coupons, voucher or special ticket generated by the POI and to be printed.

9.1.7.6.14.2 Currency <Ccy>

Presence: [0..1]

Definition: Default currency associated with the sale system.

Impacted by: C1 "ActiveCurrency"

Datatype: "ActiveCurrencyCode" on page 463

Constraints

- **ActiveCurrency**

  The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217 Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

9.1.7.6.14.3 MinimumAmountToDeliver <MinAmtToDlvr>

Presence: [0..1]

Definition: Minimum amount the Sale System is allowed to deliver for this payment.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.7.6.14.4 MaximumCashBackAmount <MaxCshBckAmt>

Presence: [0..1]

Definition: Maximum amount which could be requested for cash-back.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.7.6.14.5 MinimumSplitAmount <MinSpltAmt>

Presence: [0..1]

Definition: Minimum amount to split a sale transaction.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.7.6.14.6 DebitPreferredFlag <DbtPrefrdFlg>

Presence: [0..1]

Definition: Flag if preferred type of payment is a debit transaction.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.6.14.7 LoyaltyHandling <LltyHdlg>

Presence: [0..1]

Definition: Way of Loyalty handling.

Datatype: "LoyaltyHandling1Code" on page 490

CodeName	Name	Definition
ALLO	Allowed	The loyalty is accepted, but the POI has not to require or ask a loyalty card. The loyalty is involved by the payment card (e.g. an hybrid or linked card).
DENY	Forbidden	No loyalty card to read and loyalty transaction to process. Any attempt to enter a pure loyalty card is rejected.
PRCS	Processed	The loyalty transaction is already processed, no loyalty card or loyalty transaction to process.
PROP	Proposed	The loyalty is accepted, and the POI has to ask a loyalty card. If the Customer does not enter a loyalty card, no loyalty transaction is realised.
REQU	Required	The loyalty is required, and the POI refuses the processing of the message request if the cardholder does not enter a loyalty card.

9.1.7.7 LoyaltyAccount3

Definition: Loyalty Account description.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	LoyaltyIdentification <*LltyId*>	[1..1]	Text		336
	EntryMode <*NtryMd*>	[0..1]	CodeSet		336
	IdentificationType <*IdTp*>	[0..1]	CodeSet		337
	Brand <*Brnd*>	[0..1]	Text		337
	Provider <*Prvdr*>	[0..1]	Text		337
	OwnerName <*OwnrNm*>	[0..1]	Text		337
	Unit <*Unit*>	[0..1]	CodeSet		337
	Currency <*Ccy*>	[0..1]	CodeSet	C1	338
	Balance <*Bal*>	[0..1]	Amount		338

9.1.7.7.1 LoyaltyIdentification <LltyId>

Presence: [1..1]

Definition: Identification of Loyalty Account.

Datatype: "Max35Text" on page 519

9.1.7.7.2 EntryMode <NtryMd>

Presence: [0..1]

Definition: Standard or last entry mode to access the Loyalty account or card.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.

CodeName	Name	Definition
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.7.7.3 IdentificationType <IdTp>

Presence: [0..1]

Definition: Type of identification for this Loyalty Account.

Datatype: "CardIdentificationType1Code" on page 479

CodeName	Name	Definition
ACCT	AccountNumber	Account identification.
BARC	BarCode	Bar-code with a specific form of identification.
ISO2	ISOTrack2	ISO Track 2 including identification.
PHON	PhoneNumber	A phone number identifies the account on which the phone card is assigned.
CPAN	PrimaryAccountNumber	Standard card identification (card number).
PRIV	PrivativeNumbering	An identification set by a privative application.
UUID	UniversalUniqueIdentification	A Universal Unique Identification code is set for identification.

9.1.7.7.4 Brand <Brnd>

Presence: [0..1]

Definition: Brand to which belong the account.

Datatype: "Max35Text" on page 519

9.1.7.7.5 Provider <Prvdr>

Presence: [0..1]

Definition: Provider of the Loyalty Account.

Datatype: "Max35Text" on page 519

9.1.7.7.6 OwnerName <OwnrNm>

Presence: [0..1]

Definition: Owner name of an account.

Datatype: "Max45Text" on page 519

9.1.7.7.7 Unit <Unit>

Presence: [0..1]

Definition: Unit of a Loyalty Account (Point or Currency).

Datatype: "AmountUnit1Code" on page 471

CodeName	Name	Definition
MONE	Monetary	The amount is expressed in a monetary value in a currency.
POIN	Point	The amount is expressed in point.

9.1.7.7.8 Currency <Ccy>

Presence: [0..1]

Definition: Currency of a Loyalty Account if any.

Impacted by: C1 "ActiveCurrency"

Datatype: "ActiveCurrencyCode" on page 463

Constraints

- **ActiveCurrency**

  The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217 Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

9.1.7.7.9 Balance <Bal>

Presence: [0..1]

Definition: Balance of a Loyalty Account.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.7.8 MaintenanceDelegateAction7

Definition: Information for the MTM to build or include delegated actions in the management plan of the POI.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PeriodicAction <*PrdcActn*>	[0..1]	Indicator		340
	TMRemoteAccess <*TMRmotAccs*>	[0..1]	±		340
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		340
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		341
	DataSetIdentification <*DataSetId*>	[0..1]	±		341
	ReTry <*ReTry*>	[0..1]	±		341
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		341
	Action <*Actn*>	[0..*]			341
	Type <*Tp*>	[1..1]	CodeSet		342
	RemoteAccess <*RmotAccs*>	[0..1]	±		343
	Key <*Key*>	[0..*]			344
	KeyIdentification <*KeyId*>	[1..1]	Text		344
	KeyVersion <*KeyVrsn*>	[1..1]	Text		344
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		344
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		344
	Type <*Tp*>	[0..1]	CodeSet		344
	Function <*Fctn*>	[0..*]	CodeSet		345
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		346
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		346
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		346
	DataSetIdentification <*DataSetId*>	[0..1]	±		346
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		347
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		348
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		348
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		348
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		348
	Trigger <*Trggr*>	[1..1]	CodeSet		349
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		349
	ReTry <*ReTry*>	[0..1]	±		349
	TimeCondition <*TmCond*>	[0..1]	±		350
	TMChallenge <*TMChllng*>	[0..1]	Binary		350

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		350
	ErrorAction <*ErrActn*>	[0..*]	±		350
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		351
	MessageItem <*MsgItm*>	[0..*]	±		351
	DeviceRequest <*DvcReq*>	[0..1]	±		351

9.1.7.8.1 PeriodicAction <PrdcActn>

Presence: [0..1]

Definition: Flag to indicate that the delegated actions have to be included in a periodic sequence of actions.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.8.2 TMRemoteAccess <TMRmotAccs>

Presence: [0..1]

Definition: Network address and parameters of the terminal manager host which will performs the delegated actions.

TMRemoteAccess <TMRmotAccs> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.7.8.3 TMSProtocol <TMSPrtcol>

Presence: [0..1]

Definition: TMS protocol to use to perform the maintenance action.

Datatype: "Max35Text" on page 519

9.1.7.8.4 TMSProtocolVersion <TMSPrtcolVrsn>

Presence: [0..1]

Definition: Version of the TMS protocol to use to perform the maintenance action.

Datatype: "Max35Text" on page 519

9.1.7.8.5 DataSetIdentification <DataSetId>

Presence: [0..1]

Definition: Data set on which the delegated action has to be performed.

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

9.1.7.8.6 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process when activation of the action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.7.8.7 AdditionalInformation <AddtlInf>

Presence: [0..*]

Definition: Additional information to include in the maintenance action.

Datatype: "Max3000Binary" on page 462

9.1.7.8.8 Action <Actn>

Presence: [0..*]

Definition: Sequence of action to include in the next MTM management plan.

Action <Actn> contains the following **TMSAction10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[1..1]	CodeSet		342
	RemoteAccess <*RmotAccs*>	[0..1]	±		343
	Key <*Key*>	[0..*]			344
	KeyIdentification <*KeyId*>	[1..1]	Text		344
	KeyVersion <*KeyVrsn*>	[1..1]	Text		344
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		344
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		344
	Type <*Tp*>	[0..1]	CodeSet		344
	Function <*Fctn*>	[0..*]	CodeSet		345
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	±		346
	TMSProtocol <*TMSPrtcol*>	[0..1]	Text		346
	TMSProtocolVersion <*TMSPrtcolVrsn*>	[0..1]	Text		346
	DataSetIdentification <*DataSetId*>	[0..1]	±		346
	ComponentType <*CmpntTp*>	[0..*]	CodeSet		347
	DelegationScopeIdentification <*DlgtnScpId*>	[0..1]	Text		348
	DelegationScopeDefinition <*DlgtnScpDef*>	[0..1]	Binary		348
	DelegationProof <*DlgtnProof*>	[0..1]	Binary		348
	ProtectedDelegationProof <*PrtctdDlgtnProof*>	[0..1]	±		348
	Trigger <*Trggr*>	[1..1]	CodeSet		349
	AdditionalProcess <*AddtlPrc*>	[0..*]	CodeSet		349
	ReTry <*ReTry*>	[0..1]	±		349
	TimeCondition <*TmCond*>	[0..1]	±		350
	TMChallenge <*TMChllng*>	[0..1]	Binary		350
	KeyEnciphermentCertificate <*KeyNcphrmntCert*>	[0..*]	Binary		350
	ErrorAction <*ErrActn*>	[0..*]	±		350
	AdditionalInformation <*AddtlInf*>	[0..*]	Binary		351
	MessageItem <*MsgItm*>	[0..*]	±		351
	DeviceRequest <*DvcReq*>	[0..1]	±		351

9.1.7.8.8.1 Type <Tp>

Presence: [1..1]

Definition: Types of action to be performed by a point of interaction (POI).

Datatype: "TerminalManagementAction5Code" on page 507

CodeName	Name	Definition
DCTV	Deactivate	Request to deactivate the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
DWNL	Download	Request to download the element identified inside the message exchange.
INST	Install	Request to install the element identified inside the message exchange.
RSTR	Restart	Request to restart the element identified inside the message exchange.
UPLD	Upload	Request to upload the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.
BIND	Bind	Request sent to a POI to bind with a server.
RBND	Rebind	Request sent to a POI to rebind with a server.
UBND	Unbind	Request sent to a POI to unbind with a server.
ACTV	Activate	Request to activate the element identified inside the message exchange.
DEVR	DeviceRequest	Request to execute a device request.

9.1.7.8.8.2 RemoteAccess <RmotAccs>

Presence: [0..1]

Definition: Host access information.

RemoteAccess <RmotAccs> contains the following elements (see "NetworkParameters7" on page 396 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.7.8.8.3 Key <Key>

Presence: [0..*]

Definition: Cryptographic key used to communicate with the host.

Key <Key> contains the following **KEKIdentifier5** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		344
	KeyVersion <*KeyVrsn*>	[1..1]	Text		344
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		344
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		344
	Type <*Tp*>	[0..1]	CodeSet		344
	Function <*Fctn*>	[0..*]	CodeSet		345

9.1.7.8.8.3.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 517

9.1.7.8.8.3.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 517

9.1.7.8.8.3.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 515

9.1.7.8.8.3.4 DerivationIdentification <DerivtnId>

Presence: [0..1]

Definition: Identification used for derivation of a unique key from a master key provided for the data protection.

Datatype: "Min5Max16Binary" on page 463

9.1.7.8.8.3.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 481

CodeName	Name	Definition
AES2	AES128	AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by

CodeName	Name	Definition
		the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE3	DES112	Data encryption standard key of 112 bits (without the parity bits).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.
AES9	AES192	AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
AES5	AES256	AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

9.1.7.8.8.3.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 488

CodeName	Name	Definition
ENCR	Encryption	Key may encrypt.
DCPT	Decryption	Key may decrypt.
DENC	DataEncryption	Key may encrypt data.
DDEC	DataDecryption	Key may decrypt data.
TRNI	TranslateInput	Key may encrypt information before translation.
TRNX	TranslateOutput	Key may encrypt information after translation.
MACG	MessageAuthenticationCodeGeneration	Key may generate message authentication codes (MAC).
MACV	MessageAuthenticationCodeVerification	Key may verify message authentication codes (MAC).
SIGG	SignatureGeneration	Key may generate digital signatures.
SUGV	SignatureVerification	Key may verify digital signatures.
PINE	PINEncryption	Key may encrypt personal identification numbers (PIN).
PIND	PINDecryption	Key may decrypt personal identification numbers (PIN).

CodeName	Name	Definition
PINV	PINVerification	Key may verify personal identification numbers (PIN).
KEYG	KeyGeneration	Key may generate keys.
KEYI	KeyImport	Key may import keys.
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

9.1.7.8.8.4 TerminalManagerIdentification <TermnlMgrId>

Presence: [0..1]

Definition: Identification of the master terminal manager or the terminal manager with which the POI has to perform the action.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see "GenericIdentification176" on page 253 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		253
	Type <*Tp*>	[0..1]	CodeSet		253
	Issuer <*Issr*>	[0..1]	CodeSet		254
	Country <*Ctry*>	[0..1]	Text		254
	ShortName <*ShrtNm*>	[0..1]	Text		254

9.1.7.8.8.5 TMSProtocol <TMSPrtcol>

Presence: [0..1]

Definition: TMS protocol to use for performing the maintenance action.

Datatype: "Max35Text" on page 519

9.1.7.8.8.6 TMSProtocolVersion <TMSPrtcolVrsn>

Presence: [0..1]

Definition: Version of the TMS protocol to use to perform the maintenance action.

Datatype: "Max35Text" on page 519

9.1.7.8.8.7 DataSetIdentification <DataSetId>

Presence: [0..1]

Definition: Data set on which the action has to be performed.

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

9.1.7.8.8.8 ComponentType <CmpntTp>

Presence: [0..*]

Definition: Type of POI components to send in a status report.

Datatype: "DataSetCategory17Code" on page 483

CodeName	Name	Definition
AQPR	AcquirerParameters	Acquirer specific configuration parameters for the point of interaction (POI) system.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
TXCP	BatchCapture	Batch upload of transaction data (data capture of a group of transactions).
AKCP	CaptureResponse	Batch download response for the batch capture of transactions.
DLGT	DelegationData	Data needed to create a terminal management sub-domain.
MGTP	ManagementPlan	Configuration of management plan in the point of interaction.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
SCPR	SecurityParameters	Point of interaction parameters related to the security of software application and application protocol.
SWPK	SoftwareModule	Software module.
STRP	StatusReport	Report of software configuration and parameter status.
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
VDPR	VendorParameters	Point of interaction parameters defined by the manufacturer for instance the PIN verification capabilities.
PARA	Parameters	Any combination of configuration parameters for the point of interaction (POI).

CodeName	Name	Definition
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
LOGF	LogFile	Any repository used for recording log traces.
CMRQ	CertificateManagementRequest	Trigger for CertificateManagementRequest.
MDFL	MediaFile	Media file managed by an application of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

9.1.7.8.8.9 DelegationScopeIdentification <DlgtnScpId>

Presence: [0..1]

Definition: Identification of the delegation scope assigned by the MTM.

Datatype: "Max35Text" on page 519

9.1.7.8.8.10 DelegationScopeDefinition <DlgtnScpDef>

Presence: [0..1]

Definition: This element contains all information relevant to the DelegationScopeIdentification. The format of this element is out of scope of this definition.

Datatype: "Max3000Binary" on page 462

9.1.7.8.8.11 DelegationProof <DlgtnProof>

Presence: [0..1]

Definition: This element contains the necessary information to secure the management of the Delegation. The format of this element is out of scope of this definition.

Datatype: "Max5000Binary" on page 462

9.1.7.8.8.12 ProtectedDelegationProof <PrtctdDlgtnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtnProof> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.7.8.8.13 Trigger <Trggr>

Presence: [1..1]

Definition: Event on which the action has to be activated by the point of interaction (POI).

Datatype: "TerminalManagementActionTrigger1Code" on page 509

CodeName	Name	Definition
DATE	DateTime	Date and time trigger the terminal management action.
HOST	HostEvent	Acquirer triggers the terminal management action.
MANU	Manual	Acceptor triggers the terminal management action.
SALE	SaleEvent	Sale system triggers the terminal management action.

9.1.7.8.8.14 AdditionalProcess <AddtlPrc>

Presence: [0..*]

Definition: Additional process to perform before starting or after completing the action by the point of interaction (POI).

Datatype: "TerminalManagementAdditionalProcess1Code" on page 509

CodeName	Name	Definition
MANC	ManualConfirmation	Manual confirmation of the merchant before the terminal management action.
RCNC	Reconciliation	Acquirer reconciliation to be performed before the terminal management action.
RSRT	RestartSystem	Restart the system after performing the terminal management action.

9.1.7.8.8.15 ReTry <ReTry>

Presence: [0..1]

Definition: Definition of retry process if activation of the action fails.

ReTry <ReTry> contains the following elements (see "ProcessRetry3" on page 454 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.7.8.8.16 TimeCondition <TmCond>

Presence: [0..1]

Definition: Date and time the action has to be performed.

TimeCondition <TmCond> contains the following elements (see "ProcessTiming5" on page 456 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	WaitingTime <*WtgTm*>	[0..1]	Text		456
	StartTime <*StartTm*>	[0..1]	DateTime		456
	EndTime <*EndTm*>	[0..1]	DateTime		456
	Period <*Prd*>	[0..1]	Text		457
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		457
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		457

9.1.7.8.8.17 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 461

9.1.7.8.8.18 KeyEnciphermentCertificate <KeyNcphrmntCert>

Presence: [0..*]

Definition: Certificate chain for the encryption of temporary transport key of the key to inject.

Datatype: "Max10KBinary" on page 461

9.1.7.8.8.19 ErrorAction <ErrActn>

Presence: [0..*]

Definition: Action to perform in case of error on the related action in progress.

ErrorAction <ErrActn> contains the following elements (see "ErrorAction5" on page 390 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionResult <*ActnRslt*>	[1..*]	CodeSet		390
	ActionToProcess <*ActnToPrc*>	[1..1]	CodeSet		391

9.1.7.8.8.20 AdditionalInformation <AddtlInf>

Presence: [0..*]

Definition: Additional information about the maintenance action.

Datatype: "Max3000Binary" on page 462

9.1.7.8.8.21 MessageItem <MsgItm>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <MsgItm> contains the following elements (see "MessageItemCondition1" on page 376 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemIdentification <*ItmId*>	[1..1]	Text		377
	Condition <*Cond*>	[1..1]	CodeSet		377
	Value <*Val*>	[0..*]	Text		377

9.1.7.8.8.22 DeviceRequest <DvcReq>

Presence: [0..1]

Definition: Information related to a device request of the POI.

DeviceRequest <DvcReq> contains the following elements (see "DeviceRequest5" on page 130 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Environment <*Envt*>	[0..1]	±		133
	Context <*Cntxt*>	[0..1]	±		139
	ServiceContent <*SvcCntt*>	[1..1]	CodeSet		142
	DisplayRequest <*DispReq*>	[0..1]			142
	DisplayOutput <*DispOutpt*>	[1..*]	±		142
	InputRequest <*InptReq*>	[0..1]			143
	DisplayOutput <*DispOutpt*>	[0..1]	±		144
	InputData <*InptData*>	[1..1]			145
	DeviceType <*DvcTp*>	[1..1]	CodeSet		146
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		146
	InputCommand <*InptCmd*>	[1..1]	CodeSet		147
	NotifyCardInputFlag <*NtfyCardInptFlg*>	[1..1]	Indicator		148
	MaximumInputTime <*MaxInptTm*>	[0..1]	Quantity		148
	InputText <*InptTxt*>	[0..1]	±		148
	ImmediateResponseFlag <*ImdtRspnFlg*>	[0..1]	Indicator		149
	WaitUserValidationFlag <*WaitUsrVldtnFlg*>	[0..1]	Indicator		149
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		149
	GlobalCorrectionFlag <*GblCrrctnFlg*>	[0..1]	Indicator		150
	DisableCancelFlag <*DsblCclFlg*>	[0..1]	Indicator		150
	DisableCorrectFlag <*DsblCrrctFlg*>	[0..1]	Indicator		150
	DisableValidFlag <*DsblVldFlg*>	[0..1]	Indicator		150
	MenuBackFlag <*MenuBckFlg*>	[0..1]	Indicator		150
	PrintRequest <*PrtReq*>	[0..1]			151
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		151
	ResponseMode <*RspnMd*>	[1..1]	CodeSet		151
	IntegratedPrintFlag <*IntgrtdPrtFlg*>	[0..1]	Indicator		152
	RequiredSignatureFlag <*ReqrdSgntrFlg*>	[0..1]	Indicator		152
	OutputContent <*OutptCntt*>	[1..1]	±		152
	PlayResourceRequest <*PlayRsrcReq*>	[0..1]			153
	ResponseMode <*RspnMd*>	[0..1]	CodeSet		154

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ResourceAction <*RsrcActn*>	[1..1]	CodeSet		154
	SoundVolume <*SoundVol*>	[0..1]	Rate		154
	DisplayResolution <*DispRsltn*>	[0..1]	Text		154
	Resource <*Rsrc*>	[0..1]			154
	ResourceType <*RsrcTp*>	[1..1]	CodeSet		155
	ResourceFormat <*RsrcFrmt*>	[0..1]	CodeSet		155
	Language <*Lang*>	[0..1]	CodeSet	C6	155
	ResourceReference <*RsrcRef*>	[0..1]	Text		155
	TimingSlot <*TmgSlot*>	[0..1]	CodeSet		156
	SecureInputRequest <*ScrInptReq*>	[0..1]			156
	PINRequestType <*PINReqTp*>	[1..1]	CodeSet		156
	PINVerificationMethod <*PINVrfctnMtd*>	[0..1]	Text		157
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		157
	BeepKeyFlag <*BeepKeyFlg*>	[0..1]	Indicator		157
	CardholderPIN <*CrdhldrPIN*>	[0..1]			157
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		157
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		158
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		158
	InitialisationCardReaderRequest <*InitlstnCardRdrReq*>	[0..1]			158
	WarmResetFlag <*WarmRstFlg*>	[0..1]	Indicator		159
	ForceEntryMode <*ForceNtryMd*>	[0..*]	CodeSet		159
	LeaveCardFlag <*LeavCardFlg*>	[0..1]	Indicator		160
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		160
	DisplayOutput <*DispOutpt*>	[0..1]	±		160
	CardReaderAPDURequest <*CardRdrAPDUReq*>	[0..1]			161
	Class <*Clss*>	[1..1]	Binary		161
	Instruction <*Instr*>	[1..1]	Binary		161
	Parameter1 <*Param1*>	[1..1]	Binary		161
	Parameter2 <*Param2*>	[1..1]	Binary		161
	Data <*Data*>	[0..1]	Binary		161
	ExpectedLength <*XpctdLngth*>	[0..1]	Binary		161

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PowerOffCardReaderRequest <*PwrOffCardRdrReq*>	[0..1]			162
	PowerOffMaximumWaitingTime <*PwrOffMaxWtgTm*>	[0..1]	Quantity		162
	DisplayOutput <*DispOutpt*>	[0..1]	±		162
	TransmissionRequest <*TrnsmssnReq*>	[0..1]			163
	DestinationAddress <*DstnAdr*>	[1..1]	±		163
	MaximumTransmissionTime <*MaxTrnsmssnTm*>	[1..1]	Quantity		164
	MaximumWaitingTime <*MaxWtgTm*>	[0..1]	Quantity		164
	MessageToSend <*MsgToSnd*>	[1..1]	Binary		164
	InputNotification <*InptNtfctn*>	[0..1]			164
	ExchangeIdentification <*XchgId*>	[1..1]	Text		164
	OutputContent <*OutptCntt*>	[1..1]	±		165
	SupplementaryData <*SplmtryData*>	[0..*]	±	C5	165

9.1.7.9 CardPaymentContext29

Definition: Context in which the transaction is performed (payment and sale).

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PaymentContext <*PmtCntxt*>	[0..1]			357
	CardPresent <*CardPres*>	[0..1]	Indicator		357
	CardholderPresent <*CrdhldrPres*>	[0..1]	Indicator		357
	OnLineContext <*OnLineCntxt*>	[0..1]	Indicator		358
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		358
	TransactionEnvironment <*TxEnvt*>	[0..1]	CodeSet		358
	TransactionChannel <*TxChanl*>	[0..1]	CodeSet		358
	BusinessArea <*BizArea*>	[0..1]	CodeSet		359
	AttendantMessageCapable <*AttndntMsgCpbl*>	[0..1]	Indicator		359
	AttendantLanguage <*AttndntLang*>	[0..1]	CodeSet	C6	359
	CardDataEntryMode <*CardDataNtryMd*>	[0..1]	CodeSet		360
	FallbackIndicator <*FllbckInd*>	[0..1]	CodeSet		360
	SupportedOption <*SpprtdOptn*>	[0..*]	CodeSet		361
	SaleContext <*SaleCntxt*>	[0..1]			361
	SaleIdentification <*SaleId*>	[0..1]	Text		362
	SaleReferenceNumber <*SaleRefNb*>	[0..1]	Text		362
	SaleReconciliationIdentification <*SaleRcncltnId*>	[0..1]	Text		363
	CashierIdentification <*CshrId*>	[0..1]	Text		363
	CashierLanguage <*CshrLang*>	[0..*]	CodeSet	C6	363
	ShiftNumber <*ShftNb*>	[0..1]	Text		363
	CustomerOrderRequestFlag <*CstmrOrdrReqFlg*>	[0..1]	Indicator		363
	PurchaseOrderNumber <*PurchsOrdrNb*>	[0..1]	Text		363
	InvoiceNumber <*InvcNb*>	[0..1]	Text		363
	DeliveryNoteNumber <*DlvryNoteNb*>	[0..1]	Text		364
	SponsoredMerchant <*SpnsrdMrchnt*>	[0..*]			364
	CommonName <*CmonNm*>	[1..1]	Text		364
	Address <*Adr*>	[0..1]	Text		364
	CountryCode <*CtryCd*>	[1..1]	CodeSet		364
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		364
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		364
	SplitPayment <*SpltPmt*>	[0..1]	Indicator		365

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RemainingAmount <*RmngAmt*>	[0..1]	Amount		365
	ForceOnlineFlag <*ForceOnlnFlg*>	[0..1]	Indicator		365
	ReuseCardDataFlag <*ReuseCardDataFlg*>	[0..1]	Indicator		365
	AllowedEntryMode <*AllwdNtryMd*>	[0..*]	CodeSet		365
	SaleTokenScope <*SaleTknScp*>	[0..1]	CodeSet		366
	AdditionalSaleData <*AddtlSaleData*>	[0..1]	Text		366
	DirectDebitContext <*DrctDbtCntxt*>	[0..1]			366
	DebtorIdentification <*DbtrId*>	[0..1]			367
	Debtor <*Dbtr*>	[0..1]			368
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	368
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		369
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			369
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369
	AccountIdentification <*AcctId*>	[0..1]			370
{Or	IBAN <*IBAN*>	[1..1]	IdentifierSet	C4	370
Or	BBAN <*BBAN*>	[1..1]	IdentifierSet		370
Or	UPIC <*UPIC*>	[1..1]	IdentifierSet		371
Or}	DomesticAccount <*DmstAcct*>	[1..1]			371
	Identification <*Id*>	[1..1]	Text		371
	CreditorIdentification <*CdtrId*>	[1..1]			371
	Creditor <*Cdtr*>	[1..1]			372
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	372
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		372
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			372
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373
	RegistrationIdentification <*RegnId*>	[0..1]	Text		373
	MandateRelatedInformation <*MndtRltdInf*>	[1..1]			373
	MandateIdentification <*MndtId*>	[1..1]	Text		374
	DateOfSignature <*DtOfSgntr*>	[0..1]	Date		374

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MandateImage <*MndtImg*>	[0..1]	Binary		374

9.1.7.9.1 PaymentContext <PmtCntxt>

Presence: [0..1]

Definition: Context of the card payment transaction.

PaymentContext <PmtCntxt> contains the following **PaymentContext28** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardPresent <*CardPres*>	[0..1]	Indicator		357
	CardholderPresent <*CrdhldrPres*>	[0..1]	Indicator		357
	OnLineContext <*OnLineCntxt*>	[0..1]	Indicator		358
	AttendanceContext <*AttndncCntxt*>	[0..1]	CodeSet		358
	TransactionEnvironment <*TxEnvt*>	[0..1]	CodeSet		358
	TransactionChannel <*TxChanl*>	[0..1]	CodeSet		358
	BusinessArea <*BizArea*>	[0..1]	CodeSet		359
	AttendantMessageCapable <*AttndntMsgCpbl*>	[0..1]	Indicator		359
	AttendantLanguage <*AttndntLang*>	[0..1]	CodeSet	C6	359
	CardDataEntryMode <*CardDataNtryMd*>	[0..1]	CodeSet		360
	FallbackIndicator <*FllbckInd*>	[0..1]	CodeSet		360
	SupportedOption <*SpprtdOptn*>	[0..*]	CodeSet		361

9.1.7.9.1.1 CardPresent <CardPres>

Presence: [0..1]

Definition: Indicates whether the transaction has been initiated by a card physically present or not.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.1.2 CardholderPresent <CrdhldrPres>

Presence: [0..1]

Definition: Indicates whether the transaction has been initiated in presence of the cardholder or not.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.1.3 OnLineContext <OnLineCntxt>

Presence: [0..1]

Definition: On-line or off-line context of the transaction.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.1.4 AttendanceContext <AttndncCntxt>

Presence: [0..1]

Definition: Human attendance at the POI (Point Of Interaction) location during the transaction.

Datatype: "AttendanceContext1Code" on page 471

CodeName	Name	Definition
ATTD	Attended	Attended payment, with an attendant.
SATT	SemiAttended	Semi-attended, including self checkout. An attendant supervises several payment, and could be called to help the cardholder.
UATT	Unattended	Unattended payment, no attendant present.

9.1.7.9.1.5 TransactionEnvironment <TxEnvt>

Presence: [0..1]

Definition: Indicates the environment of the transaction.

Datatype: "TransactionEnvironment1Code" on page 511

CodeName	Name	Definition
MERC	Merchant	Merchant environment.
PRIV	Private	Private environment.
PUBL	Public	Public environment.

9.1.7.9.1.6 TransactionChannel <TxChanl>

Presence: [0..1]

Definition: Identifies the type of the communication channels used by the cardholder to the acceptor system.

Datatype: "TransactionChannel5Code" on page 511

CodeName	Name	Definition
MAIL	MailOrder	Mail order.
TLPH	TelephoneOrder	Telephone order.
ECOM	ElectronicCommerce	Electronic commerce.
TVPY	TelevisionPayment	Payment on television.

CodeName	Name	Definition
SECM	SecuredElectronicCommerce	Electronic commerce with cardholder authentication.
MOBL	MobilePayment	Payment performed through a cardholder mobile device.
MPOS	MobilePOS	Payment performed through a merchant mobile device.

9.1.7.9.1.7 BusinessArea <BizArea>

Presence: [0..1]

Definition: Defines the business context of this transaction that could imply specific scheme rules.

Datatype: "BusinessArea1Code" on page 476

CodeName	Name	Definition
AIBD	ArtificialIntelligenceBasedDecision	The payment is initiated by an artificial intelligence based decision.
OPMT	Openpayment	The card is used in a Transit business case where the fare amount is not known when the transaction is initiated.
PPAY	PlainPayment	The card is used to perform a plain payment.
TKNF	TransitKnownFare	The card is used in a Transit business case where the fare amount is known when the transaction is initiated.

9.1.7.9.1.8 AttendantMessageCapable <AttndntMsgCpbl>

Presence: [0..1]

Definition: Indicates whether a message can be sent or not on an attendant display (attendant display present or not).

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.1.9 AttendantLanguage <AttndntLang>

Presence: [0..1]

Definition: Language used to display messages to the attendant.

Reference ISO 639-1 (alpha-2) et ISO 639-2 (alpha-3).

Impacted by: C6 "ValidationByTable"

Datatype: "LanguageCode" on page 489

Constraints

- **ValidationByTable**

  Must be a valid terrestrial language.

9.1.7.9.1.10 CardDataEntryMode <CardDataNtryMd>

Presence: [0..1]

Definition: Entry mode of the card data.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.7.9.1.11 FallbackIndicator <FllbckInd>

Presence: [0..1]

Definition: Indicator of a card entry mode fallback.

Datatype: "CardFallback1Code" on page 478

CodeName	Name	Definition
FFLB	FallbackAfterFailure	Card fall-back occurred during the transaction in progress. The previous transaction on the terminal failed.
SFLB	FallbackAfterSuccess	Card fall-back occurred during the transaction in progress. The previous transaction on the terminal was successful.

CodeName	Name	Definition
NFLB	NoFallback	No card fall-back during the transaction in progress.

9.1.7.9.1.12 SupportedOption <SpprtdOptn>

Presence: [0..*]

Definition: Payment options the card acceptor can support.

Datatype: "SupportedPaymentOption2Code" on page 507

CodeName	Name	Definition
PART	PartialApproval	The entity supports a partial approval of the payment transaction.
MSRV	PaymentApprovalOnly	The entity supports the approval of the payment service along with the decline of additional requested services (as cash-back).
INSI	IssuerInstalment	The sender support IssuerInstalment proposals to the Cardholder.
PINQ	PINRequest	The sender is able to support Single Tap transaction.

9.1.7.9.2 SaleContext <SaleCntxt>

Presence: [0..1]

Definition: Context of the sale involving the card payment transaction.

SaleContext <SaleCntxt> contains the following **SaleContext4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	SaleIdentification <*SaleId*>	[0..1]	Text		362
	SaleReferenceNumber <*SaleRefNb*>	[0..1]	Text		362
	SaleReconciliationIdentification <*SaleRcncltnId*>	[0..1]	Text		363
	CashierIdentification <*CshrId*>	[0..1]	Text		363
	CashierLanguage <*CshrLang*>	[0..*]	CodeSet	C6	363
	ShiftNumber <*ShftNb*>	[0..1]	Text		363
	CustomerOrderRequestFlag <*CstmrOrdrReqFlg*>	[0..1]	Indicator		363
	PurchaseOrderNumber <*PurchsOrdrNb*>	[0..1]	Text		363
	InvoiceNumber <*InvcNb*>	[0..1]	Text		363
	DeliveryNoteNumber <*DlvryNoteNb*>	[0..1]	Text		364
	SponsoredMerchant <*SpnsrdMrchnt*>	[0..*]			364
	CommonName <*CmonNm*>	[1..1]	Text		364
	Address <*Adr*>	[0..1]	Text		364
	CountryCode <*CtryCd*>	[1..1]	CodeSet		364
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		364
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		364
	SplitPayment <*SpltPmt*>	[0..1]	Indicator		365
	RemainingAmount <*RmngAmt*>	[0..1]	Amount		365
	ForceOnlineFlag <*ForceOnlnFlg*>	[0..1]	Indicator		365
	ReuseCardDataFlag <*ReuseCardDataFlg*>	[0..1]	Indicator		365
	AllowedEntryMode <*AllwdNtryMd*>	[0..*]	CodeSet		365
	SaleTokenScope <*SaleTknScp*>	[0..1]	CodeSet		366
	AdditionalSaleData <*AddtlSaleData*>	[0..1]	Text		366

9.1.7.9.2.1 SaleIdentification <SaleId>

Presence: [0..1]

Definition: Identification of the sale terminal (electronic cash register or point of sale terminal) or the sale system.

Datatype: "Max35Text" on page 519

9.1.7.9.2.2 SaleReferenceNumber <SaleRefNb>

Presence: [0..1]

Definition: Identify a sale transaction assigned by the sale system.

Datatype: "Max35Text" on page 519

9.1.7.9.2.3 SaleReconciliationIdentification <SaleRcncltnId>

Presence: [0..1]

Definition: Identifier of the reconciliation between the Sale system and the POI system.

Datatype: "Max35Text" on page 519

9.1.7.9.2.4 CashierIdentification <CshrId>

Presence: [0..1]

Definition: Identification of the cashier who carried out the transaction.

Datatype: "Max35Text" on page 519

9.1.7.9.2.5 CashierLanguage <CshrLang>

Presence: [0..*]

Definition: Languages used by the cashier.

Impacted by: C6 "ValidationByTable"

Datatype: "LanguageCode" on page 489

Constraints

- **ValidationByTable**

  Must be a valid terrestrial language.

9.1.7.9.2.6 ShiftNumber <ShftNb>

Presence: [0..1]

Definition: Identifies the shift of the cashier.

Datatype: "Max2NumericText" on page 518

9.1.7.9.2.7 CustomerOrderRequestFlag <CstmrOrdrReqFlg>

Presence: [0..1]

Definition: Flag indicating that list of CustomerOrders should be returned in response.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.2.8 PurchaseOrderNumber <PurchsOrdrNb>

Presence: [0..1]

Definition: Identification of the purchase order.

Datatype: "Max35Text" on page 519

9.1.7.9.2.9 InvoiceNumber <InvcNb>

Presence: [0..1]

Definition: Identification of the invoice.

Datatype: "Max35Text" on page 519

9.1.7.9.2.10 DeliveryNoteNumber <DlvryNoteNb>

Presence: [0..1]

Definition: Identification allocated by the sale system and given to the customer.

Datatype: "Max35Text" on page 519

9.1.7.9.2.11 SponsoredMerchant <SpnsrdMrchnt>

Presence: [0..*]

Definition: Merchant using the payment services of a payment facilitator, acting as a card acceptor.

SponsoredMerchant <SpnsrdMrchnt> contains the following **Organisation26** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CommonName <*CmonNm*>	[1..1]	Text		364
	Address <*Adr*>	[0..1]	Text		364
	CountryCode <*CtryCd*>	[1..1]	CodeSet		364
	MerchantCategoryCode <*MrchntCtgyCd*>	[1..1]	Text		364
	RegisteredIdentifier <*RegdIdr*>	[1..1]	Text		364

9.1.7.9.2.11.1 CommonName <CmonNm>

Presence: [1..1]

Definition: Name of the merchant.

Datatype: "Max70Text" on page 520

9.1.7.9.2.11.2 Address <Adr>

Presence: [0..1]

Definition: Location of the merchant.

Datatype: "Max140Text" on page 517

9.1.7.9.2.11.3 CountryCode <CtryCd>

Presence: [1..1]

Definition: Country of the merchant.

Datatype: "ISO3NumericCountryCode" on page 488

9.1.7.9.2.11.4 MerchantCategoryCode <MrchntCtgyCd>

Presence: [1..1]

Definition: Category code conform to ISO 18245, related to the type of services or goods the merchant provides for the transaction.

Datatype: "Min3Max4Text" on page 521

9.1.7.9.2.11.5 RegisteredIdentifier <RegdIdr>

Presence: [1..1]

Definition: Identifier of the sponsored merchant assigned by the payment facilitator of their acquirer.

Datatype: "Max35Text" on page 519

9.1.7.9.2.12 SplitPayment <SpltPmt>

Presence: [0..1]

Definition: True if the payment transaction is a partial payment of the sale transaction.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.2.13 RemainingAmount <RmngAmt>

Presence: [0..1]

Definition: Remaining amount to complete the sale transaction, if a partial payment has been completed for the sale transaction.

Datatype: "ImpliedCurrencyAndAmount" on page 460

9.1.7.9.2.14 ForceOnlineFlag <ForceOnlnFlg>

Presence: [0..1]

Definition: Indicates if the Cashier requires POI forces online access to the Acquirer.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.2.15 ReuseCardDataFlag <ReuseCardDataFlg>

Presence: [0..1]

Definition: Indicates if the card data has to be taken from a previous transaction.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.9.2.16 AllowedEntryMode <AllwdNtryMd>

Presence: [0..*]

Definition: Type of card data reading.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.

CodeName	Name	Definition
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.7.9.2.17 SaleTokenScope <SaleTknScp>

Presence: [0..1]

Definition: Scope of the token that identifies the payment mean of the customer.

Datatype: "SaleTokenScope1Code" on page 506

CodeName	Name	Definition
MULT	MultipleUse	The token is generated to recognise a customer for a longer period.
SNGL	SingleUse	The token is generated to recognise a customer during the lifetime of a transaction.

9.1.7.9.2.18 AdditionalSaleData <AddtlSaleData>

Presence: [0..1]

Definition: Additional information associated with the sale transaction.

Datatype: "Max70Text" on page 520

9.1.7.9.3 DirectDebitContext <DrctDbtCntxt>

Presence: [0..1]

Definition: Context of the direct debit transaction.

DirectDebitContext <DrctDbtCntxt> contains the following **CardDirectDebit2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DebtorIdentification <*DbtrId*>	[0..1]			367
	Debtor <*Dbtr*>	[0..1]			368
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	368
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		369
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			369
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369
	AccountIdentification <*AcctId*>	[0..1]			370
{Or	IBAN <*IBAN*>	[1..1]	IdentifierSet	C4	370
Or	BBAN <*BBAN*>	[1..1]	IdentifierSet		370
Or	UPIC <*UPIC*>	[1..1]	IdentifierSet		371
Or}	DomesticAccount <*DmstAcct*>	[1..1]			371
	Identification <*Id*>	[1..1]	Text		371
	CreditorIdentification <*CdtrId*>	[1..1]			371
	Creditor <*Cdtr*>	[1..1]			372
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	372
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		372
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			372
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373
	RegistrationIdentification <*RegnId*>	[0..1]	Text		373
	MandateRelatedInformation <*MndtRltdInf*>	[1..1]			373
	MandateIdentification <*MndtId*>	[1..1]	Text		374
	DateOfSignature <*DtOfSgntr*>	[0..1]	Date		374
	MandateImage <*MndtImg*>	[0..1]	Binary		374

9.1.7.9.3.1 DebtorIdentification <DbtrId>

Presence: [0..1]

Definition: Information related to the debtor.

DebtorIdentification <DbtrId> contains the following **Debtor4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Debtor <*Dbtr*>	[0..1]			368
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	368
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		369
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			369
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369
	AccountIdentification <*AcctId*>	[0..1]			370
{Or	IBAN <*IBAN*>	[1..1]	IdentifierSet	C4	370
Or	BBAN <*BBAN*>	[1..1]	IdentifierSet		370
Or	UPIC <*UPIC*>	[1..1]	IdentifierSet		371
Or}	DomesticAccount <*DmstAcct*>	[1..1]			371
	Identification <*Id*>	[1..1]	Text		371

9.1.7.9.3.1.1 Debtor <Dbtr>

Presence: [0..1]

Definition: Party that owes an amount of money to the (ultimate) creditor. In the context of the payment model, the debtor is also the debit account owner.

Debtor <Dbtr> contains one of the following **PartyIdentification178Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	368
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		369
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			369
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369

9.1.7.9.3.1.1.1 AnyBIC <AnyBIC>

Presence: [1..1]

Definition: Unique and unambiguous identifier for an organisation that is allocated by an institution, for example, Dun & Bradstreet Identification.

Impacted by: C2 "AnyBIC"

Datatype: "AnyBICDec2014Identifier" on page 513

Constraints

- **AnyBIC**

  Only a valid Business identifier code is allowed. Business identifier codes for financial or non-financial institutions are registered and published by the ISO 9362 Registration Authority in the ISO directory of BICs, and consists of eight (8) or eleven (11) contiguous characters.

9.1.7.9.3.1.1.2 ProprietaryIdentification <PrtryId>

Presence: [1..1]

Definition: Unique and unambiguous identifier, as assigned to a financial institution using a proprietary identification scheme.

ProprietaryIdentification <PrtryId> contains the following elements (see "GenericIdentification36" on page 255 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		255
	Issuer <*Issr*>	[1..1]	Text		255
	SchemeName <*SchmeNm*>	[0..1]	Text		255

9.1.7.9.3.1.1.3 NameAndAddress <NmAndAdr>

Presence: [1..1]

Definition: Name by which a party is known and which is usually used to identify that party.

NameAndAddress <NmAndAdr> contains the following **NameAndAddress6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[1..1]	Text		369
	Address <*Adr*>	[1..1]	±		369

9.1.7.9.3.1.1.3.1 Name <Nm>

Presence: [1..1]

Definition: Name by which a party is known and which is usually used to identify that party.

Datatype: "Max70Text" on page 520

9.1.7.9.3.1.1.3.2 Address <Adr>

Presence: [1..1]

Definition: Information that locates and identifies a specific address, as defined by postal services.

Address <Adr> contains the following elements (see "PostalAddress2" on page 453 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StreetName <*StrtNm*>	[0..1]	Text		453
	PostCodeIdentification <*PstCdId*>	[1..1]	Text		453
	TownName <*TwnNm*>	[1..1]	Text		454
	CountrySubDivision <*CtrySubDvsn*>	[0..1]	Text		454
	Country <*Ctry*>	[1..1]	CodeSet	C3	454

9.1.7.9.3.1.2 AccountIdentification <AcctId>

Presence: [0..1]

Definition: Unique and unambiguous identification for the account between the account owner and the account servicer.

AccountIdentification <AcctId> contains one of the following **CashAccountIdentification7Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	IBAN <*IBAN*>	[1..1]	IdentifierSet	C4	370
Or	BBAN <*BBAN*>	[1..1]	IdentifierSet		370
Or	UPIC <*UPIC*>	[1..1]	IdentifierSet		371
Or}	DomesticAccount <*DmstAcct*>	[1..1]			371
	Identification <*Id*>	[1..1]	Text		371

9.1.7.9.3.1.2.1 IBAN <IBAN>

Presence: [1..1]

Definition: International Bank Account Number (IBAN) - identifier used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.

Impacted by: C4 "IBAN"

Datatype: "IBAN2007Identifier" on page 514

Constraints

- **IBAN**

  A valid IBAN consists of all three of the following components: Country Code, check digits and BBAN.

9.1.7.9.3.1.2.2 BBAN <BBAN>

Presence: [1..1]

Definition: Basic Bank Account Number (BBAN) - identifier used nationally by financial institutions, ie, in individual countries, generally as part of a National Account Numbering Scheme(s), to uniquely identify the account of a customer.

Datatype: "BBANIdentifier" on page 513

9.1.7.9.3.1.2.3 UPIC <UPIC>

Presence: [1..1]

Definition: Universal Payment Identification Code (UPIC) - identifier used by the New York Clearing House to mask confidential data, such as bank accounts and bank routing numbers. UPIC numbers remain with business customers, regardless of banking relationship changes.

Datatype: "UPICIdentifier" on page 514

9.1.7.9.3.1.2.4 DomesticAccount <DmstAcct>

Presence: [1..1]

Definition: Account number used by financial institutions in individual countries to identify an account of a customer, but not necessarily the bank and branch of the financial institution in which the account is held.

DomesticAccount <DmstAcct> contains the following **SimpleIdentificationInformation4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		371

9.1.7.9.3.1.2.4.1 Identification <Id>

Presence: [1..1]

Definition: Name or number assigned by an entity to enable recognition of that entity, for example, account identifier.

Datatype: "Max35Text" on page 519

9.1.7.9.3.2 CreditorIdentification <CdtrId>

Presence: [1..1]

Definition: Information related to the creditor.

CreditorIdentification <CdtrId> contains the following **Creditor4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Creditor <*Cdtr*>	[1..1]			372
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	372
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		372
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			372
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373
	RegistrationIdentification <*RegnId*>	[0..1]	Text		373

9.1.7.9.3.2.1 Creditor <Cdtr>

Presence: [1..1]

Definition: Party that receives an amount of money from the debtor. In the context of the payment model, the creditor is also the credit account owner.

Creditor <Cdtr> contains one of the following **PartyIdentification178Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	AnyBIC <*AnyBIC*>	[1..1]	IdentifierSet	C2	372
Or	ProprietaryIdentification <*PrtryId*>	[1..1]	±		372
Or}	NameAndAddress <*NmAndAdr*>	[1..1]			372
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373

9.1.7.9.3.2.1.1 AnyBIC <AnyBIC>

Presence: [1..1]

Definition: Unique and unambiguous identifier for an organisation that is allocated by an institution, for example, Dun & Bradstreet Identification.

Impacted by: C2 "AnyBIC"

Datatype: "AnyBICDec2014Identifier" on page 513

Constraints

- **AnyBIC**

  Only a valid Business identifier code is allowed. Business identifier codes for financial or non-financial institutions are registered and published by the ISO 9362 Registration Authority in the ISO directory of BICs, and consists of eight (8) or eleven (11) contiguous characters.

9.1.7.9.3.2.1.2 ProprietaryIdentification <PrtryId>

Presence: [1..1]

Definition: Unique and unambiguous identifier, as assigned to a financial institution using a proprietary identification scheme.

ProprietaryIdentification <PrtryId> contains the following elements (see "GenericIdentification36" on page 255 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		255
	Issuer <*Issr*>	[1..1]	Text		255
	SchemeName <*SchmeNm*>	[0..1]	Text		255

9.1.7.9.3.2.1.3 NameAndAddress <NmAndAdr>

Presence: [1..1]

Definition: Name by which a party is known and which is usually used to identify that party.

NameAndAddress <NmAndAdr> contains the following **NameAndAddress6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[1..1]	Text		373
	Address <*Adr*>	[1..1]	±		373

9.1.7.9.3.2.1.3.1 Name <Nm>

Presence: [1..1]

Definition: Name by which a party is known and which is usually used to identify that party.

Datatype: "Max70Text" on page 520

9.1.7.9.3.2.1.3.2 Address <Adr>

Presence: [1..1]

Definition: Information that locates and identifies a specific address, as defined by postal services.

Address <Adr> contains the following elements (see "PostalAddress2" on page 453 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StreetName <*StrtNm*>	[0..1]	Text		453
	PostCodeIdentification <*PstCdId*>	[1..1]	Text		453
	TownName <*TwnNm*>	[1..1]	Text		454
	CountrySubDivision <*CtrySubDvsn*>	[0..1]	Text		454
	Country <*Ctry*>	[1..1]	CodeSet	C3	454

9.1.7.9.3.2.2 RegistrationIdentification <RegnId>

Presence: [0..1]

Definition: Reference assigned to a creditor by its financial institution, or relevant authority, authorising the creditor to take part in a direct debit scheme.

Datatype: "Max35Text" on page 519

9.1.7.9.3.3 MandateRelatedInformation <MndtRltdInf>

Presence: [1..1]

Definition: Provides further details of the mandate signed between the creditor and the debtor.

MandateRelatedInformation <MndtRltdInf> contains the following **MandateRelatedInformation13** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MandateIdentification <*MndtId*>	[1..1]	Text		374
	DateOfSignature <*DtOfSgntr*>	[0..1]	Date		374
	MandateImage <*MndtImg*>	[0..1]	Binary		374

9.1.7.9.3.3.1 MandateIdentification <MndtId>

Presence: [1..1]

Definition: Unique identification, as assigned by the creditor, to unambiguously identify the mandate.

Datatype: "Max35Text" on page 519

9.1.7.9.3.3.2 DateOfSignature <DtOfSgntr>

Presence: [0..1]

Definition: Date on which the direct debit mandate has been signed by the debtor.

Datatype: "ISODate" on page 512

9.1.7.9.3.3.3 MandateImage <MndtImg>

Presence: [0..1]

Definition: Image of scanned signed mandate.

Datatype: "Max2MBBinary" on page 462

9.1.7.10 ResponseType11

Definition: Response of a requested service.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Response <*Rspn*>	[1..1]	CodeSet		374
	ResponseReason <*RspnRsn*>	[0..1]	CodeSet		374
	AdditionalResponseInformation <*AddtlRspnInf*>	[0..1]	Text		376

9.1.7.10.1 Response <Rspn>

Presence: [1..1]

Definition: Result of the requested transaction.

Datatype: "Response11Code" on page 501

CodeName	Name	Definition
WARN	Warning	An additional Response Code, mainly a functional one, should be considered to identify the outcome of the request.
FAIL	Failure	Processing of the request fails for various reasons. Some further processing according to the type of requested service, the context of the process, and some additional precision about the failure notified in the ErrorCondition data element.
SUCC	Success	Processing OK. Information related to the result of the processing is contained in other parts of the response message.

9.1.7.10.2 ResponseReason <RspnRsn>

Presence: [0..1]

Definition: Detail of the response.

Datatype: "RetailerResultDetail1Code" on page 502

CodeName	Name	Definition
ABRT	Aborted	The Initiator of the request has sent an Abort message request, which was accepted and processed.
BUSY	Busy	The system is busy, try later.
CANC	Cancel	The user has aborted the transaction on the PED keyboard, for instance during PIN entering.
DEVO	DeviceOut	Device out of order.
WPIN	WrongPIN	The user has entered the PIN on the PED keyboard and the verification fails.
NHOS	UnreachableHost	Acquirer or any host is unreachable or has not answered to an online request, so is considered as temporary unavailable. Depending on the Sale context, the request could be repeated (to be compared with "Refusal").
UNVS	UnavailableService	The service is not available (not implemented, not configured, protocol version too old...).
UNVD	UnavailableDevice	The hardware is not available (absent, not configured...).
REFU	Refusal	The transaction is refused by the host or by the local rules associated to the card or the POI.
PAYR	PaymentRestriction	Some sale items are not payable by the card proposed by the Customer.
TNFD	NotFound	The transaction is not found (e.g. for a reversal or a repeat).
NALW	NotAllowed	A service request is sent during a Service dialogue. A combination of services not possible to provide. During the DeviceInitialisationCardReader message processing, the user has entered a card which has to be protected by the POI, and cannot be processed with this device request from the external, and then the Sale System.
LOUT	LoggedOut	Not logged in.
IVCA	InvalidCard	The card entered by the Customer cannot be processed by the POI because this card is not configured in the system.
ICAR	InsertedCard	If the Input Device request a NotifyCardInputFlag and the Customer enters a card in the card reader without answers to the Input command, the POI abort the Input command processing, and answer a dedicated ErrorCondition value in the Input response message.

CodeName	Name	Definition
WIPG	InProgress	The transaction is still in progress and then the command cannot be processed.

9.1.7.10.3 AdditionalResponseInformation <AddtlRspnInf>

Presence: [0..1]

Definition: Additional information to be logged for further examination.

Datatype: "Max140Text" on page 517

9.1.7.11 CustomerDevice3

Definition: Device used by the customer to perform the payment.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[0..1]	Text		376
	Type <*Tp*>	[0..1]	Text		376
	Provider <*Prvdr*>	[0..1]	Text		376

9.1.7.11.1 Identification <Id>

Presence: [0..1]

Definition: Identifier of the component.

Datatype: "Max35Text" on page 519

9.1.7.11.2 Type <Tp>

Presence: [0..1]

Definition: Type of component.

Datatype: "Max70Text" on page 520

9.1.7.11.3 Provider <Prvdr>

Presence: [0..1]

Definition: Provider of the component.

Datatype: "Max35Text" on page 519

9.1.7.12 MessageItemCondition1

Definition: Presence condition of a message item.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ItemIdentification <*ItmId*>	[1..1]	Text		377
	Condition <*Cond*>	[1..1]	CodeSet		377
	Value <*Val*>	[0..*]	Text		377

9.1.7.12.1 ItemIdentification <ItmId>

Presence: [1..1]

Definition: Unique identification of the message and the message item.

Datatype: "Max140Text" on page 517

9.1.7.12.2 Condition <Cond>

Presence: [1..1]

Definition: Condition of presence of the message item.

Datatype: "MessageItemCondition1Code" on page 492

CodeName	Name	Definition
MNDT	Mandatory	Message item must be present.
CFVL	ConfiguredValue	Message item must be present with the configured value.
DFLT	DefaultValue	Message item has the configured value if the item is absent.
ALWV	AllowedValues	Message item must have one of the configured values.
IFAV	IfAvailable	Message item has to be present if available.
COPY	Copy	Message item is present if it was present in a previous related message with the same value.
UNSP	NotSupported	Message item is not supported and has to be absent.

9.1.7.12.3 Value <Val>

Presence: [0..*]

Definition: Value to be used for the message item.

Datatype: "Max140Text" on page 517

9.1.7.13 PointOfInteractionCapabilities9

Definition: Capabilities of the POI (Point Of Interaction) performing the transaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardReadingCapabilities <*CardRdngCpblties*>	[0..*]	CodeSet		378
	CardholderVerificationCapabilities <*CrdhldrVrfctnCpblties*>	[0..*]	CodeSet		379
	PINLengthCapabilities <*PINLngthCpblties*>	[0..1]	Quantity		379
	ApprovalCodeLength <*ApprvlCdLngth*>	[0..1]	Quantity		379
	MaxScriptLength <*MxScrptLngth*>	[0..1]	Quantity		380
	CardCaptureCapable <*CardCaptrCpbl*>	[0..1]	Indicator		380
	OnLineCapabilities <*OnLineCpblties*>	[0..1]	CodeSet		380
	MessageCapabilities <*MsgCpblties*>	[0..*]			380
	Destination <*Dstn*>	[1..*]	CodeSet		380
	AvailableFormat <*AvlblFrmt*>	[0..*]	CodeSet		381
	NumberOfLines <*NbOfLines*>	[0..1]	Quantity		381
	LineWidth <*LineWidth*>	[0..1]	Quantity		381
	AvailableLanguage <*AvlblLang*>	[0..*]	CodeSet	C6	381

9.1.7.13.1 CardReadingCapabilities <CardRdngCpblties>

Presence: [0..*]

Definition: Card reading capabilities of the POI (Point Of Interaction) performing the transaction.

Datatype: "CardDataReading8Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.

CodeName	Name	Definition
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.1.7.13.2 CardholderVerificationCapabilities <CrdhldrVrfctnCpblties>

Presence: [0..*]

Definition: Cardholder verification capabilities of the POI (Point Of Interaction) performing the transaction.

Datatype: "CardholderVerificationCapability4Code" on page 478

CodeName	Name	Definition
APKI	AccountDigitalSignature	Account based digital signature.
CHDT	CardholderData	Cardholder authentication data.
MNSG	ManualSignature	Manual signature verification.
MNVR	ManualVerification	Other manual verification, for example passport or drivers license.
FBIG	OfflineBiographics	Offline biographics.
FBIO	OfflineBiometrics	Offline biometrics.
FDSG	OfflineDigitalSignature	Offline digital signature analysis.
FCPN	OfflinePINClear	Offline PIN in clear (Personal Identification Number).
FEPN	OfflinePINEncrypted	Offline PIN encrypted (Personal Identification Number).
NPIN	OnLinePIN	Online PIN (Personal Identification Number).
PKIS	PKISignature	PKI (Public Key Infrastructure) based digital signature.
SCEC	SecureElectronicCommerce	Three domain secure (three domain secure authentication of the cardholder).
NBIO	OnLineBiometrics	Online biometrics.
NOVF	NoCapabilities	No cardholder verification capability.
OTHR	Other	Other cardholder verification capabilities.

9.1.7.13.3 PINLengthCapabilities <PINLngthCpblties>

Presence: [0..1]

Definition: Maximum number of digits the POI is able to accept when the cardholder enters its PIN.

Datatype: "PositiveNumber" on page 515

9.1.7.13.4 ApprovalCodeLength <ApprvlCdLngth>

Presence: [0..1]

Definition: Maximum number of characters of the approval code the POI is able to manage.

Datatype: "PositiveNumber" on page 515

9.1.7.13.5 MaxScriptLength <MxScrptLngth>

Presence: [0..1]

Definition: Maximum data length in bytes that a card issuer can return to the ICC at the terminal.

Datatype: "PositiveNumber" on page 515

9.1.7.13.6 CardCaptureCapable <CardCaptrCpbl>

Presence: [0..1]

Definition: True if the POI is able to capture card.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.13.7 OnLineCapabilities <OnLineCpblties>

Presence: [0..1]

Definition: On-line and off-line capabilities of the POI (Point Of Interaction).

Datatype: "OnLineCapability1Code" on page 493

CodeName	Name	Definition
OFLN	OffLine	Off-line only capable.
ONLN	OnLine	On-line only capable.
SMON	SemiOffLine	Off-line capable with possible on-line requests to the acquirer.

9.1.7.13.8 MessageCapabilities <MsgCpblties>

Presence: [0..*]

Definition: Capabilities of the terminal to display or print message to the cardholder and the merchant.

MessageCapabilities <MsgCpblties> contains the following **DisplayCapabilities4** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Destination <*Dstn*>	[1..*]	CodeSet		380
	AvailableFormat <*AvlblFrmt*>	[0..*]	CodeSet		381
	NumberOfLines <*NbOfLines*>	[0..1]	Quantity		381
	LineWidth <*LineWidth*>	[0..1]	Quantity		381
	AvailableLanguage <*AvlblLang*>	[0..*]	CodeSet	C6	381

9.1.7.13.8.1 Destination <Dstn>

Presence: [1..*]

Definition: Destination of the message to present.

Datatype: "UserInterface4Code" on page 512

CodeName	Name	Definition
CDSP	CardholderDisplay	Cardholder display or interface.
CRCP	CardholderReceipt	Cardholder receipt.
MDSP	MerchantDisplay	Merchant display or interface.
MRCP	MerchantReceipt	Merchant receipt.
CRDO	OtherCardholderInterface	Other interface of the cardholder, for instance e-mail or smartphone message.

9.1.7.13.8.2 AvailableFormat <AvlblFrmt>

Presence: [0..*]

Definition: Available message format.

Datatype: "OutputFormat1Code" on page 493

CodeName	Name	Definition
MREF	MessageReference	Predefined configured messages, identified by a reference.
TEXT	SimpleText	Text without format attributes.
HTML	XHTML	XHTML document which includes a subset of the XHTML output tag.

9.1.7.13.8.3 NumberOfLines <NbOfLines>

Presence: [0..1]

Definition: Number of lines of the display.

Datatype: "Number" on page 515

9.1.7.13.8.4 LineWidth <LineWidth>

Presence: [0..1]

Definition: Number of columns of the display or printer.

Datatype: "Number" on page 515

9.1.7.13.8.5 AvailableLanguage <AvlblLang>

Presence: [0..*]

Definition: Available language for the message. Reference ISO 639-1 (alpha-2) et ISO 639-2 (alpha-3).

Impacted by: C6 "ValidationByTable"

Datatype: "LanguageCode" on page 489

Constraints

- **ValidationByTable**

  Must be a valid terrestrial language.

9.1.7.14 Vehicle1

Definition: Information related to a vehicle used during a transaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	VehicleNumber <*VhclNb*>	[0..1]	Text		382
	TrailerNumber <*TrlrNb*>	[0..1]	Text		383
	VehicleTag <*VhclTag*>	[0..1]	Text		383
	VehicleTagEntryMode <*VhclTagNtryMd*>	[0..1]	CodeSet		383
	UnitNumber <*UnitNb*>	[0..1]	Text		383
	ReplacementCar <*RplcmntCar*>	[0..1]	Indicator		383
	Odometer <*Odmtr*>	[0..1]	Quantity		384
	Hubometer <*Hbmtr*>	[0..1]	Quantity		384
	TrailerHours <*TrlrHrs*>	[0..1]	Text		384
	ReferHours <*RefrHrs*>	[0..1]	Text		384
	MaintenanceIdentification <*MntncId*>	[0..1]	Text		384
	DriverOrVehicleCard <*DrvrOrVhclCard*>	[0..1]			384
	PAN <*PAN*>	[0..1]	Text		385
	Track1 <*Trck1*>	[0..1]	Text		385
	Track2 <*Trck2*>	[0..1]	Text		385
	Track3 <*Trck3*>	[0..1]	Text		385
	AdditionalCardData <*AddtlCardData*>	[0..*]	Text		385
	EntryMode <*NtryMd*>	[0..1]	CodeSet		385
	AdditionalVehicleData <*AddtlVhclData*>	[0..*]			386
	Type <*Tp*>	[0..1]	Text		386
	EntryMode <*NtryMd*>	[0..1]	CodeSet		386
	Data <*Data*>	[1..1]	Text		387

9.1.7.14.1 VehicleNumber <VhclNb>

Presence: [0..1]

Definition: Number assigned to the vehicle for identification.

Datatype: "Max35NumericText" on page 518

9.1.7.14.2 TrailerNumber <TrlrNb>

Presence: [0..1]

Definition: Number assigned to the vehicle trailer for identification.

Datatype: "Max35NumericText" on page 518

9.1.7.14.3 VehicleTag <VhclTag>

Presence: [0..1]

Definition: Registration tag of the vehicle.

Datatype: "Max35Text" on page 519

9.1.7.14.4 VehicleTagEntryMode <VhclTagNtryMd>

Presence: [0..1]

Definition: Entry mode of the registration tag.

Datatype: "CardDataReading5Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.

9.1.7.14.5 UnitNumber <UnitNb>

Presence: [0..1]

Definition: Identification of the vehicle in the fleet.

Datatype: "Max35NumericText" on page 518

9.1.7.14.6 ReplacementCar <RplcmntCar>

Presence: [0..1]

Definition: True if the car is a replacement car.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.7.14.7 Odometer <Odmtr>

Presence: [0..1]

Definition: Odometer reading value indicating the distance travelled by the vehicle.

Datatype: "DecimalNumber" on page 514

9.1.7.14.8 Hubometer <Hbmtr>

Presence: [0..1]

Definition: Hubometer reading value indicating the distance travelled by the trailer.

Datatype: "DecimalNumber" on page 514

9.1.7.14.9 TrailerHours <TrlrHrs>

Presence: [0..1]

Definition: Number of hours the trailer has been in operation.

Datatype: "Max35Text" on page 519

9.1.7.14.10 ReferHours <RefrHrs>

Presence: [0..1]

Definition: Number of hours the refer unit has been in operation.

Datatype: "Max35Text" on page 519

9.1.7.14.11 MaintenanceIdentification <MntncId>

Presence: [0..1]

Definition: Identification assigned to the vehicle related to maintenance.

Datatype: "Max35Text" on page 519

9.1.7.14.12 DriverOrVehicleCard <DrvrOrVhclCard>

Presence: [0..1]

Definition: Second card presented for the payment transaction.

DriverOrVehicleCard <DrvrOrVhclCard> contains the following **PlainCardData17** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PAN <*PAN*>	[0..1]	Text		385
	Track1 <*Trck1*>	[0..1]	Text		385
	Track2 <*Trck2*>	[0..1]	Text		385
	Track3 <*Trck3*>	[0..1]	Text		385
	AdditionalCardData <*AddtlCardData*>	[0..*]	Text		385
	EntryMode <*NtryMd*>	[0..1]	CodeSet		385

9.1.7.14.12.1 PAN <PAN>

Presence: [0..1]

Definition: Primary Account Number (PAN) of the card.

Datatype: "Min8Max28NumericText" on page 522

9.1.7.14.12.2 Track1 <Trck1>

Presence: [0..1]

Definition: ISO track 1 issued from the magnetic stripe card or from the ICC if the magnetic stripe was not read. The format is conform to ISO 7813, removing beginning and ending sentinels and longitudinal redundancy check characters.

Datatype: "Max76Text" on page 520

9.1.7.14.12.3 Track2 <Trck2>

Presence: [0..1]

Definition: ISO track 2 issued from the magnetic stripe card or from the ICC if the magnetic stripe was not read. The content is conform to ISO 7813, removing beginning and ending sentinels and longitudinal redundancy check characters.

Datatype: "Max37Text" on page 519

9.1.7.14.12.4 Track3 <Trck3>

Presence: [0..1]

Definition: ISO track 3 issued from the magnetic stripe card or from the ICC if the magnetic stripe was not read. The content is conform to ISO 4909, removing beginning and ending sentinels and longitudinal redundancy check characters.

Datatype: "Max104Text" on page 516

9.1.7.14.12.5 AdditionalCardData <AddtlCardData>

Presence: [0..*]

Definition: Additional card issuer specific data.

Datatype: "Max35Text" on page 519

9.1.7.14.12.6 EntryMode <NtryMd>

Presence: [0..1]

Definition: Entry mode of the card.

Datatype: "CardDataReading5Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.

CodeName	Name	Definition
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.

9.1.7.14.13 AdditionalVehicleData <AddtlVhclData>

Presence: [0..*]

Definition: Additional information related to the vehicle.

AdditionalVehicleData <AddtlVhclData> contains the following **Vehicle2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Type <*Tp*>	[0..1]	Text		386
	EntryMode <*NtryMd*>	[0..1]	CodeSet		386
	Data <*Data*>	[1..1]	Text		387

9.1.7.14.13.1 Type <Tp>

Presence: [0..1]

Definition: Type of information related to the vehicle.

Datatype: "Max35Text" on page 519

9.1.7.14.13.2 EntryMode <NtryMd>

Presence: [0..1]

Definition: Entry mode of the information.

Datatype: "CardDataReading5Code" on page 477

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.

CodeName	Name	Definition
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.

9.1.7.14.13.3 Data <Data>

Presence: [1..1]

Definition: Information related to the vehicle.

Datatype: "Max35Text" on page 519

9.1.7.15 EncapsulatedContent3

Definition: Data to authenticate.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		387
	Content <*Cntt*>	[0..1]	Binary		387

9.1.7.15.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data which have been authenticated.

Datatype: "ContentType2Code" on page 480

CodeName	Name	Definition
DATA	PlainData	Generic, non cryptographic, or unqualified data content - (ASN.1 Object Identifier: id-data).
SIGN	SignedData	Digital signature - (ASN.1 Object Identifier: id-signedData).
EVLP	EnvelopedData	Encrypted data, with encryption key - (ASN.1 Object Identifier: id-envelopedData).
DGST	DigestedData	Message digest - (ASN.1 Object Identifier: id-digestedData).
AUTH	AuthenticatedData	MAC (Message Authentication Code), with encryption key - (ASN.1 Object Identifier: id-ct-authData).

9.1.7.15.2 Content <Cntt>

Presence: [0..1]

Definition: Actual data to authenticate.

Datatype: "Max100KBinary" on page 461

9.1.7.16 MaintenanceIdentificationAssociation1

Definition: Association of the TM identifier and the MTM identifier of an entity.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	MasterTMIdentification <*MstrTMId*>	[1..1]	Text		388
	TMIdentification <*TMId*>	[1..1]	Text		388

9.1.7.16.1 MasterTMIdentification <MstrTMId>

Presence: [1..1]

Definition: Identifier for the master terminal manager.

Datatype: "Max35Text" on page 519

9.1.7.16.2 TMIdentification <TMId>

Presence: [1..1]

Definition: Identifier for the terminal manager requesting the delegation.

Datatype: "Max35Text" on page 519

9.1.8 Monitoring

9.1.8.1 Traceability8

Definition: Identification of partners involved in exchange from the merchant to the issuer, with the relative timestamp of their exchanges.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelayIdentification <*RlayId*>	[1..1]	±		388
	ProtocolName <*PrtcolNm*>	[0..1]	Text		389
	ProtocolVersion <*PrtcolVrsn*>	[0..1]	Text		389
	TraceDateTimeIn <*TracDtTmIn*>	[1..1]	DateTime		389
	TraceDateTimeOut <*TracDtTmOut*>	[1..1]	DateTime		389

9.1.8.1.1 RelayIdentification <RlayId>

Presence: [1..1]

Definition: Identification of a partner of a message exchange.

RelayIdentification <RlayId> contains the following elements (see "GenericIdentification177" on page 248 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		249
	Type <*Tp*>	[0..1]	CodeSet		249
	Issuer <*Issr*>	[0..1]	CodeSet		250
	Country <*Ctry*>	[0..1]	Text		250
	ShortName <*ShrtNm*>	[0..1]	Text		250
	RemoteAccess <*RmotAccs*>	[0..1]	±		251
	Geolocation <*Glctn*>	[0..1]			251
	GeographicCoordinates <*GeogcCordints*>	[0..1]			251
	Latitude <*Lat*>	[1..1]	Text		252
	Longitude <*Long*>	[1..1]	Text		252
	UTMCoordinates <*UTMCordints*>	[0..1]			252
	UTMZone <*UTMZone*>	[1..1]	Text		252
	UTMEastward <*UTMEstwrd*>	[1..1]	Text		252
	UTMNorthward <*UTMNrthwrd*>	[1..1]	Text		253

9.1.8.1.2 ProtocolName <PrtcolNm>

Presence: [0..1]

Definition: Name of the outgoing protocol used by the node.

Datatype: "Max35Text" on page 519

9.1.8.1.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Version of the protocol.

Datatype: "Max6Text" on page 520

9.1.8.1.4 TraceDateTimeIn <TracDtTmIn>

Presence: [1..1]

Definition: Date and time of incoming data exchange for relaying or processing.

Datatype: "ISODateTime" on page 513

9.1.8.1.5 TraceDateTimeOut <TracDtTmOut>

Presence: [1..1]

Definition: Date and time of the outgoing exchange for relaying or processing.

Datatype: "ISODateTime" on page 513

9.1.8.2 ErrorAction5

Definition: Action to perform in case of error on the related action in progress.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionResult <*ActnRslt*>	[1..*]	CodeSet		390
	ActionToProcess <*ActnToPrc*>	[1..1]	CodeSet		391

9.1.8.2.1 ActionResult <ActnRslt>

Presence: [1..*]

Definition: List of error action result codes.

Datatype: "TerminalManagementActionResult5Code" on page 508

CodeName	Name	Definition
ACCD	AccessDenied	Access is denied while performing the action.
CNTE	ConnectionError	Problem to connect while performing the action.
FMTE	FormatError	Data transferred has a wrong format.
INVC	InvalidContent	Content of the data is invalid.
LENE	LengthError	Data transferred has a wrong length.
OVER	MemoryOverflow	Memory to store the date exceeded.
MISS	MissingFile	Data set to be maintained is missing.
NSUP	NotSupported	Action is not supported.
SIGE	SignatureError	Data transferred has a wrong digital signature.
WARN	SuccessWithWarning	Action was performed but some warnings arose.
SYNE	SyntaxError	Data transferred has a wrong syntax.
TIMO	Timeout	Timeout expired during the data transfer.
UKDT	UnknownData	Data set identification invalid.
UKRF	UnknownKeyReference	Cryptographic key reference used for the data signature is not valid.
INDP	InvalidDelegationProof	Delegation Proof transmitted by the delegated TMS is not the one expected.
IDMP	InvalidDelegationInManagementPlan	One action of the AcceptorManagementPlan refers to an update unauthorized by the delegation.
DPRU	DelegationParametersReceivedUnauthorized	The content analysis of the AcceptorConfigurationUpdate reveals unexpected parameters.
AERR	AnyError	This code value means all TerminalManagementActionResultCode except "Any Error" and "Unlisted Error".

CodeName	Name	Definition
CMER	CommunicationError	Error in communication once the connection has been established.
ULER	UnlistedError	Any error that is not defined by a code value inside the TerminalManagementActionResultCode.
SUCC	Success	Action was successfully performed.

9.1.8.2.2 ActionToProcess <ActnToPrc>

Presence: [1..1]

Definition: Action to be processed for the related errors.

Datatype: "TerminalManagementErrorAction2Code" on page 510

CodeName	Name	Definition
SDSR	SendStatusReport	Send a status report immediately.
STOP	StopSequence	Stop the current sequence of terminal management actions without any action, and do not notice the error with a status report.

9.1.8.3 TMSEvent9

Definition: Result of an individual terminal management action performed by the point of interaction.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	TimeStamp <*TmStmp*>	[1..1]	DateTime		391
	Result <*Rslt*>	[1..1]	CodeSet		391
	ActionIdentification <*ActnId*>	[1..1]			392
	ActionType <*ActnTp*>	[1..1]	CodeSet		393
	DataSetIdentification <*DataSetId*>	[0..1]	±		393
	AdditionalErrorInformation <*AddtlErrInf*>	[0..1]	Text		394
	TerminalManagerIdentification <*TermnlMgrId*>	[0..1]	Text		394
	DeviceResponse <*DvcRspn*>	[0..1]	±		394

9.1.8.3.1 TimeStamp <TmStmp>

Presence: [1..1]

Definition: Date time of the terminal management action performed by the point of interaction.

Datatype: "ISODateTime" on page 513

9.1.8.3.2 Result <Rslt>

Presence: [1..1]

Definition: Final result of the processed terminal management action.

Datatype: "TerminalManagementActionResult5Code" on page 508

CodeName	Name	Definition
ACCD	AccessDenied	Access is denied while performing the action.
CNTE	ConnectionError	Problem to connect while performing the action.
FMTE	FormatError	Data transferred has a wrong format.
INVC	InvalidContent	Content of the data is invalid.
LENE	LengthError	Data transferred has a wrong length.
OVER	MemoryOverflow	Memory to store the date exceeded.
MISS	MissingFile	Data set to be maintained is missing.
NSUP	NotSupported	Action is not supported.
SIGE	SignatureError	Data transferred has a wrong digital signature.
WARN	SuccessWithWarning	Action was performed but some warnings arose.
SYNE	SyntaxError	Data transferred has a wrong syntax.
TIMO	Timeout	Timeout expired during the data transfer.
UKDT	UnknownData	Data set identification invalid.
UKRF	UnknownKeyReference	Cryptographic key reference used for the data signature is not valid.
INDP	InvalidDelegationProof	Delegation Proof transmitted by the delegated TMS is not the one expected.
IDMP	InvalidDelegationInManagementPlan	One action of the AcceptorManagementPlan refers to an update unauthorized by the delegation.
DPRU	DelegationParametersReceivedUnauthorized	The content analysis of the AcceptorConfigurationUpdate reveals unexpected parameters.
AERR	AnyError	This code value means all TerminalManagementActionResultCode except "Any Error" and "Unlisted Error".
CMER	CommunicationError	Error in communication once the connection has been established.
ULER	UnlistedError	Any error that is not defined by a code value inside the TerminalManagementActionResultCode.
SUCC	Success	Action was successfully performed.

9.1.8.3.3 ActionIdentification <ActnId>

Presence: [1..1]

Definition: Identification of the terminal management action performed by the point of interaction.

ActionIdentification <ActnId> contains the following **TMSActionIdentification8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ActionType <*ActnTp*>	[1..1]	CodeSet		393
	DataSetIdentification <*DataSetId*>	[0..1]	±		393

9.1.8.3.3.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Types of terminal management action performed by a point of interaction.

Datatype: "TerminalManagementAction5Code" on page 507

CodeName	Name	Definition
DCTV	Deactivate	Request to deactivate the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
DWNL	Download	Request to download the element identified inside the message exchange.
INST	Install	Request to install the element identified inside the message exchange.
RSTR	Restart	Request to restart the element identified inside the message exchange.
UPLD	Upload	Request to upload the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.
BIND	Bind	Request sent to a POI to bind with a server.
RBND	Rebind	Request sent to a POI to rebind with a server.
UBND	Unbind	Request sent to a POI to unbind with a server.
ACTV	Activate	Request to activate the element identified inside the message exchange.
DEVR	DeviceRequest	Request to execute a device request.

9.1.8.3.3.2 DataSetIdentification <DataSetId>

Presence: [0..1]

Definition: Data set on which the action has been performed.

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification9" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[0..1]	Text		279
	Type <*Tp*>	[1..1]	CodeSet		279
	Version <*Vrsn*>	[0..1]	Text		280
	CreationDateTime <*CreDtTm*>	[0..1]	DateTime		280

9.1.8.3.4 AdditionalErrorInformation <AddtlErrInf>

Presence: [0..1]

Definition: Additional information related to a failure.

Datatype: "Max70Text" on page 520

9.1.8.3.5 TerminalManagerIdentification <TermnlMgrId>

Presence: [0..1]

Definition: Identification of the terminal management system (TMS) used with the action.

Datatype: "Max35Text" on page 519

9.1.8.3.6 DeviceResponse <DvcRspn>

Presence: [0..1]

Definition: Response of a device request done previously.

DeviceResponse <DvcRspn> contains the following elements (see "DeviceResponse5" on page 166 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Environment <*Envt*>	[0..1]	±		168
	Context <*Cntxt*>	[0..1]	±		174
	ServiceContent <*SvcCntt*>	[1..1]	CodeSet		177
	DisplayResponse <*DispRspn*>	[0..1]			177
	OutputResult <*OutptRslt*>	[1..*]			178
	DeviceType <*DvcTp*>	[1..1]	CodeSet		178
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		178
	Response <*Rspn*>	[1..1]	±		179
	InputResponse <*InptRspn*>	[0..1]			179
	OutputResult <*OutptRslt*>	[0..1]			180
	DeviceType <*DvcTp*>	[1..1]	CodeSet		180
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		181
	Response <*Rspn*>	[1..1]	±		182
	InputResult <*InptRslt*>	[1..1]			182
	DeviceType <*DvcTp*>	[1..1]	CodeSet		182
	InformationQualifier <*InfQlfr*>	[1..1]	CodeSet		183
	InputResultData <*InptRsltData*>	[1..1]			183
	InputCommand <*InptCmd*>	[1..1]	CodeSet		184
	ConfirmedFlag <*ConfdFlg*>	[0..1]	Indicator		185
	FunctionKey <*FctnKey*>	[0..1]	Quantity		185
	InputMessage <*InptMsg*>	[0..1]	Text		185
	Password <*Pwd*>	[0..1]	±		185
	ImageCapturedSignature <*ImgCaptrdSgntr*>	[0..1]			186
	ImageFormat <*ImgFrmt*>	[1..1]	Text		186
	ImageData <*ImgData*>	[0..1]	Binary		186
	ImageReference <*ImgRef*>	[0..1]	Text		186
	AdditionalInformation <*AddtlInf*>	[0..1]	Text		186
	PrintResponse <*PrtRspn*>	[0..1]			186
	DocumentQualifier <*DocQlfr*>	[1..1]	CodeSet		186
	SecureInputResponse <*ScrInptRspn*>	[0..1]			187

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	CardholderPIN <*CrdhldrPIN*>	[0..1]			187
	EncryptedPINBlock <*NcrptdPINBlck*>	[1..1]	±		188
	PINFormat <*PINFrmt*>	[1..1]	CodeSet		188
	AdditionalInput <*AddtlInpt*>	[0..1]	Text		188
	InitialisationCardReaderResponse <*InitlstnCardRdrRspn*>	[0..1]			188
	CardEntryMode <*CardNtryMd*>	[0..1]	CodeSet		189
	ICCResetData <*ICCRstData*>	[0..1]			189
	ATRValue <*ATRVal*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[0..1]	Binary		190
	AdditionalInformation <*AddtlInf*>	[0..1]	Binary		190
	CardReaderApplicationProtocolDataUnitResponse <*CardRdrApplPrtcolDataUnitRspn*>	[0..1]			190
	Data <*Data*>	[0..1]	Binary		190
	CardStatus <*CardSts*>	[1..1]	Binary		190
	TransmissionResponse <*TrnsmssnRspn*>	[0..1]			191
	ReceivedMessage <*RcvdMsg*>	[0..1]	Binary		191
	Response <*Rspn*>	[1..1]	±		191
	SupplementaryData <*SplmtryData*>	[0..*]	±	C5	191

9.1.9 Network Access

9.1.9.1 NetworkParameters7

Definition: Parameters to communicate with a host.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Address <*Adr*>	[1..*]			397
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397
	UserName <*UsrNm*>	[0..1]	Text		397
	AccessCode <*AccsCd*>	[0..1]	Binary		398
	ServerCertificate <*SvrCert*>	[0..*]	Binary		398
	ServerCertificateIdentifier <*SvrCertIdr*>	[0..*]	Binary		398
	ClientCertificate <*ClntCert*>	[0..*]	Binary		398
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		398

9.1.9.1.1 Address <Adr>

Presence: [1..*]

Definition: Network addresses of the host.

Address <Adr> contains the following **NetworkParameters9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	NetworkType <*NtwkTp*>	[1..1]	CodeSet		397
	AddressValue <*AdrVal*>	[1..1]	Text		397

9.1.9.1.1.1 NetworkType <NtwkTp>

Presence: [1..1]

Definition: Type of communication network.

Datatype: "NetworkType1Code" on page 492

CodeName	Name	Definition
IPNW	InternetProtocol	Protocol of an IP network.
PSTN	PublicTelephone	Protocol of a Public Switched Telephone Network (PSTN).

9.1.9.1.1.2 AddressValue <AdrVal>

Presence: [1..1]

Definition: Value of the address. The value of an internet protocol address contains the IP address or the DNS (Domain Name Server) address, followed by the character ': ' and the port number if the default port is not used. The value of a public telephone address contains the phone number with possible prefix and extensions.

Datatype: "Max500Text" on page 519

9.1.9.1.2 UserName <UsrNm>

Presence: [0..1]

Definition: User name identifying the client.

Datatype: "Max35Text" on page 519

9.1.9.1.3 AccessCode <AccsCd>

Presence: [0..1]

Definition: Password authenticating the client.

Datatype: "Max35Binary" on page 462

9.1.9.1.4 ServerCertificate <SvrCert>

Presence: [0..*]

Definition: X.509 Certificate required to authenticate the server.

Datatype: "Max10KBinary" on page 461

9.1.9.1.5 ServerCertificateIdentifier <SvrCertIdr>

Presence: [0..*]

Definition: Identification of the X.509 Certificates required to authenticate the server, for instance a digest of the certificate.

Datatype: "Max140Binary" on page 461

9.1.9.1.6 ClientCertificate <ClntCert>

Presence: [0..*]

Definition: X.509 Certificate required to authenticate the client.

Datatype: "Max10KBinary" on page 461

9.1.9.1.7 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the set of security elements to access the host.

Datatype: "Max35Text" on page 519

9.1.10 Postal Address

9.1.10.1 PostalAddress22

Definition: Information that locates and identifies a specific address, as defined by postal services.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AddressType <*AdrTp*>	[0..1]	CodeSet		399
	Department <*Dept*>	[0..1]	Text		399
	SubDepartment <*SubDept*>	[0..1]	Text		399
	AddressLine <*AdrLine*>	[0..2]	Text		399
	StreetName <*StrtNm*>	[0..1]	Text		400
	BuildingNumber <*BldgNb*>	[0..1]	Text		400
	PostCode <*PstCd*>	[0..1]	Text		400
	TownName <*TwnNm*>	[0..1]	Text		400
	CountrySubDivision <*CtrySubDvsn*>	[0..2]	Text		400
	CountryCode <*CtryCd*>	[0..1]	Text		400

9.1.10.1.1 AddressType <AdrTp>

Presence: [0..1]

Definition: Identifies the nature of the postal address.

Datatype: "AddressType2Code" on page 464

CodeName	Name	Definition
ADDR	Postal	Address is the complete postal address.
PBOX	POBox	Address is a postal office (PO) box.
HOME	Residential	Address is the home address.
BIZZ	Business	Address is the business address.
MLTO	MailTo	Address is the address to which mail is sent.
DLVY	DeliveryTo	Address is the address to which delivery is to take place.

9.1.10.1.2 Department <Dept>

Presence: [0..1]

Definition: Identification of a division of a large organisation or building.

Datatype: "Max70Text" on page 520

9.1.10.1.3 SubDepartment <SubDept>

Presence: [0..1]

Definition: Identification of a sub-division of a large organisation or building.

Datatype: "Max70Text" on page 520

9.1.10.1.4 AddressLine <AdrLine>

Presence: [0..2]

Definition: Information that locates and identifies a specific address, as defined by postal services, presented in free format text.

Datatype: "Max70Text" on page 520

9.1.10.1.5 StreetName <StrtNm>

Presence: [0..1]

Definition: Name of a street or thoroughfare.

Datatype: "Max70Text" on page 520

9.1.10.1.6 BuildingNumber <BldgNb>

Presence: [0..1]

Definition: Number that identifies the position of a building on a street.

Datatype: "Max16Text" on page 517

9.1.10.1.7 PostCode <PstCd>

Presence: [0..1]

Definition: Identifier consisting of a group of letters and/or numbers that is added to a postal address to assist the sorting of mail.

Datatype: "Max16Text" on page 517

9.1.10.1.8 TownName <TwnNm>

Presence: [0..1]

Definition: Name of a built-up area, with defined boundaries, and a local government.

Datatype: "Max70Text" on page 520

9.1.10.1.9 CountrySubDivision <CtrySubDvsn>

Presence: [0..2]

Definition: Identifies a subdivision of a country such as state, region, county.

Datatype: "Max35Text" on page 519

9.1.10.1.10 CountryCode <CtryCd>

Presence: [0..1]

Definition: Nation with its own government.

Datatype: "Min2Max3AlphaText" on page 521

9.1.11 Secure Element

9.1.11.1 DigestedData5

Definition: Digest computed on the identified data.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		401
	DigestAlgorithm <*DgstAlgo*>	[1..1]	±		401
	EncapsulatedContent <*NcpsltdCntt*>	[1..1]	±		401
	Digest <*Dgst*>	[1..1]	Binary		401

9.1.11.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.1.2 DigestAlgorithm <DgstAlgo>

Presence: [1..1]

Definition: Identification of the digest algorithm.

DigestAlgorithm <DgstAlgo> contains the following elements (see "AlgorithmIdentification21" on page 449 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		449

9.1.11.1.3 EncapsulatedContent <NcpsltdCntt>

Presence: [1..1]

Definition: Data on which the digest is computed.

EncapsulatedContent <NcpsltdCntt> contains the following elements (see "EncapsulatedContent3" on page 387 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		387
	Content <*Cntt*>	[0..1]	Binary		387

9.1.11.1.4 Digest <Dgst>

Presence: [1..1]

Definition: Result of data-digesting process.

Datatype: "Max140Binary" on page 461

9.1.11.2 SignedData7

Definition: Digital signatures of data from one or several signers.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		402
	DigestAlgorithm <*DgstAlgo*>	[0..*]	±		402
	EncapsulatedContent <*NcpsltdCntt*>	[0..1]	±		403
	Certificate <*Cert*>	[0..*]	Binary		403
	Signer <*Sgnr*>	[0..*]			403
	Version <*Vrsn*>	[0..1]	Quantity		404
	SignerIdentification <*SgnrId*>	[0..1]			404
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			404
	Issuer <*Issr*>	[1..1]			404
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405
	SerialNumber <*SrlNb*>	[1..1]	Binary		405
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		406
	DigestAlgorithm <*DgstAlgo*>	[1..1]	±		406
	SignedAttributes <*SgndAttrbts*>	[0..*]			406
	Name <*Nm*>	[1..1]	Text		406
	Value <*Val*>	[0..1]	Text		406
	SignatureAlgorithm <*SgntrAlgo*>	[1..1]	±		407
	Signature <*Sgntr*>	[1..1]	Binary		407

9.1.11.2.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.2.2 DigestAlgorithm <DgstAlgo>

Presence: [0..*]

Definition: Identification of digest algorithm applied before signature.

DigestAlgorithm <DgstAlgo> contains the following elements (see "AlgorithmIdentification21" on page 449 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		449

9.1.11.2.3 EncapsulatedContent <NcpsltdCntt>

Presence: [0..1]

Definition: Data to sign.

EncapsulatedContent <NcpsltdCntt> contains the following elements (see "EncapsulatedContent3" on page 387 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		387
	Content <*Cntt*>	[0..1]	Binary		387

9.1.11.2.4 Certificate <Cert>

Presence: [0..*]

Definition: Chain of X.509 certificates.

Datatype: "Max5000Binary" on page 462

9.1.11.2.5 Signer <Sgnr>

Presence: [0..*]

Definition: Digital signature and identification of a signer.

Signer <Sgnr> contains the following **Signer6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		404
	SignerIdentification <*SgnrId*>	[0..1]			404
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			404
	Issuer <*Issr*>	[1..1]			404
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405
	SerialNumber <*SrlNb*>	[1..1]	Binary		405
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		406
	DigestAlgorithm <*DgstAlgo*>	[1..1]	±		406
	SignedAttributes <*SgndAttrbts*>	[0..*]			406
	Name <*Nm*>	[1..1]	Text		406
	Value <*Val*>	[0..1]	Text		406
	SignatureAlgorithm <*SgntrAlgo*>	[1..1]	±		407
	Signature <*Sgntr*>	[1..1]	Binary		407

9.1.11.2.5.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the Cryptographic Message Syntax (CMS) data structure.

Datatype: "Number" on page 515

9.1.11.2.5.2 SignerIdentification <SgnrId>

Presence: [0..1]

Definition: Identification of the entity who has signed the data.

SignerIdentification <SgnrId> contains one of the following **Recipient12Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			404
	Issuer <*Issr*>	[1..1]			404
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405
	SerialNumber <*SrlNb*>	[1..1]	Binary		405
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		406

9.1.11.2.5.2.1 IssuerAndSerialNumber <IssrAndSrlNb>

Presence: [1..1]

Definition: Certificate issuer name and serial number (see ITU X.509).

IssuerAndSerialNumber <IssrAndSrlNb> contains the following **IssuerAndSerialNumber2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Issuer <*Issr*>	[1..1]			404
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405
	SerialNumber <*SrlNb*>	[1..1]	Binary		405

9.1.11.2.5.2.1.1 Issuer <Issr>

Presence: [1..1]

Definition: Certificate issuer name (see X.509).

Issuer <Issr> contains the following **CertificateIssuer1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405

9.1.11.2.5.2.1.1.1 RelativeDistinguishedName <RltvDstngshdNm>

Presence: [1..*]

Definition: Relative distinguished name inside a X.509 certificate.

RelativeDistinguishedName <RltvDstngshdNm> contains the following **RelativeDistinguishedName1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405

9.1.11.2.5.2.1.1.1.1 AttributeType <AttrTp>

Presence: [1..1]

Definition: Type of attribute of a distinguished name (see X.500).

Datatype: "AttributeType1Code" on page 472

CodeName	Name	Definition
CNAT	CommonName	Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).
LATT	Locality	Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).
OATT	OrganisationName	Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).
OUAT	OrganisationUnitName	Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).
CATT	CountryName	Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).

9.1.11.2.5.2.1.1.1.2 AttributeValue <AttrVal>

Presence: [1..1]

Definition: Value of the attribute of a distinguished name (see X.500).

Datatype: "Max140Text" on page 517

9.1.11.2.5.2.1.2 SerialNumber <SrlNb>

Presence: [1..1]

Definition: Certificate serial number (see X.509).

Datatype: "Max500Binary" on page 463

9.1.11.2.5.2.2 KeyIdentifier <KeyIdr>

Presence: [1..1]

Definition: Identifier of a cryptographic asymmetric key, previously exchanged between initiator and recipient.

KeyIdentifier <KeyIdr> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.2.5.3 DigestAlgorithm <DgstAlgo>

Presence: [1..1]

Definition: Identification of a digest algorithm to apply before signature.

DigestAlgorithm <DgstAlgo> contains the following elements (see "AlgorithmIdentification21" on page 449 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		449

9.1.11.2.5.4 SignedAttributes <SgndAttrbts>

Presence: [0..*]

Definition: Collection of attributes that are signed.

SignedAttributes <SgndAttrbts> contains the following **GenericInformation1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[1..1]	Text		406
	Value <*Val*>	[0..1]	Text		406

9.1.11.2.5.4.1 Name <Nm>

Presence: [1..1]

Definition: Name of the generic information to exchange.

Datatype: "Max70Text" on page 520

9.1.11.2.5.4.2 Value <Val>

Presence: [0..1]

Definition: Value of the generic information to exchange.

Datatype: "Max140Text" on page 517

9.1.11.2.5.5 SignatureAlgorithm <SgntrAlgo>

Presence: [1..1]

Definition: Cryptographic digital signature algorithm.

SignatureAlgorithm <SgntrAlgo> contains the following elements (see "AlgorithmIdentification30" on page 437 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		438
	Parameter <*Param*>	[0..1]			439
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		440
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]			440
	Algorithm <*Algo*>	[1..1]	CodeSet		441
	Parameter <*Param*>	[0..1]			441
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		441
	SaltLength <*SaltLngth*>	[0..1]	Quantity		441
	TrailerField <*TrlrFld*>	[0..1]	Quantity		441
	OIDCurveName <*OIDCrvNm*>	[0..1]	Text		442

9.1.11.2.5.6 Signature <Sgntr>

Presence: [1..1]

Definition: Digital signature.

Datatype: "Max3000Binary" on page 462

9.1.11.3 ContentInformationType32

Definition: General cryptographic message syntax (CMS) containing encrypted data.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		407
	EnvelopedData <*EnvlpdData*>	[1..1]	±		408

9.1.11.3.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data protection.

Datatype: "ContentType2Code" on page 480

CodeName	Name	Definition
DATA	PlainData	Generic, non cryptographic, or unqualified data content - (ASN.1 Object Identifier: id-data).

CodeName	Name	Definition
SIGN	SignedData	Digital signature - (ASN.1 Object Identifier: id-signedData).
EVLP	EnvelopedData	Encrypted data, with encryption key - (ASN.1 Object Identifier: id-envelopedData).
DGST	DigestedData	Message digest - (ASN.1 Object Identifier: id-digestedData).
AUTH	AuthenticatedData	MAC (Message Authentication Code), with encryption key - (ASN.1 Object Identifier: id-ct-authData).

9.1.11.3.2 EnvelopedData <EnvlpdData>

Presence: [1..1]

Definition: Data protection by encryption or by a digital envelope, with an encryption key.

EnvelopedData <EnvlpdData> contains the following elements (see "EnvelopedData9" on page 409 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		410
	OriginatorInformation <*OrgtrInf*>	[0..1]			411
	Certificate <*Cert*>	[0..*]	Binary		411
	Recipient <*Rcpt*>	[1..*]			411
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			412
	Version <*Vrsn*>	[0..1]	Quantity		413
	RecipientIdentification <*RcptId*>	[1..1]			413
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			413
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		415
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		415
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		416
Or	KEK <*KEK*>	[1..1]			416
	Version <*Vrsn*>	[0..1]	Quantity		416
	KEKIdentification <*KEKId*>	[1..1]	±		416
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		417
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		417
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		417
	EncryptedContent <*NcrptdCntt*>	[0..1]			418
	ContentType <*CnttTp*>	[1..1]	CodeSet		418
	ContentEncryptionAlgorithm <*CnttNcrptnAlgo*>	[0..1]	±		418
	EncryptedData <*NcrptdData*>	[1..1]	Binary		419

9.1.11.4 EnvelopedData9

Definition: Encrypted data with encryption key.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		410
	OriginatorInformation <*OrgtrInf*>	[0..1]			411
	Certificate <*Cert*>	[0..*]	Binary		411
	Recipient <*Rcpt*>	[1..*]			411
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			412
	Version <*Vrsn*>	[0..1]	Quantity		413
	RecipientIdentification <*RcptId*>	[1..1]			413
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			413
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		415
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		415
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		416
Or	KEK <*KEK*>	[1..1]			416
	Version <*Vrsn*>	[0..1]	Quantity		416
	KEKIdentification <*KEKId*>	[1..1]	±		416
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		417
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		417
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		417
	EncryptedContent <*NcrptdCntt*>	[0..1]			418
	ContentType <*CnttTp*>	[1..1]	CodeSet		418
	ContentEncryptionAlgorithm <*CnttNcrptnAlgo*>	[0..1]	±		418
	EncryptedData <*NcrptdData*>	[1..1]	Binary		419

9.1.11.4.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.4.2 OriginatorInformation <OrgtrInf>

Presence: [0..1]

Definition: Provides certificates of the originator.

OriginatorInformation <OrgtrInf> contains the following **OriginatorInformation1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Certificate <*Cert*>	[0..*]	Binary		411

9.1.11.4.2.1 Certificate <Cert>

Presence: [0..*]

Definition: It may contain originator certificates associated with several different key management algorithms.

Datatype: "Max5000Binary" on page 462

9.1.11.4.3 Recipient <Rcpt>

Presence: [1..*]

Definition: Session key or identification of the protection key used by the recipient.

Recipient <Rcpt> contains one of the following **Recipient11Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			412
	Version <*Vrsn*>	[0..1]	Quantity		413
	RecipientIdentification <*RcptId*>	[1..1]			413
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			413
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		415
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		415
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		416
Or	KEK <*KEK*>	[1..1]			416
	Version <*Vrsn*>	[0..1]	Quantity		416
	KEKIdentification <*KEKId*>	[1..1]	±		416
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		417
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		417
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		417

9.1.11.4.3.1 KeyTransport <KeyTrnsprt>

Presence: [1..1]

Definition: Encryption key using previously distributed asymmetric public key.

KeyTransport <KeyTrnsprt> contains the following **KeyTransport8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		413
	RecipientIdentification <*RcptId*>	[1..1]			413
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			413
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		415
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		415
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		416

9.1.11.4.3.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.4.3.1.2 RecipientIdentification <RcptId>

Presence: [1..1]

Definition: Identification of a cryptographic asymmetric key for the recipient.

RecipientIdentification <RcptId> contains one of the following **Recipient12Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			413
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		415

9.1.11.4.3.1.2.1 IssuerAndSerialNumber <IssrAndSrlNb>

Presence: [1..1]

Definition: Certificate issuer name and serial number (see ITU X.509).

IssuerAndSerialNumber <IssrAndSrlNb> contains the following **IssuerAndSerialNumber2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415

9.1.11.4.3.1.2.1.1 Issuer <Issr>

Presence: [1..1]

Definition: Certificate issuer name (see X.509).

Issuer <Issr> contains the following **CertificateIssuer1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415

9.1.11.4.3.1.2.1.1.1 RelativeDistinguishedName <RltvDstngshdNm>

Presence: [1..*]

Definition: Relative distinguished name inside a X.509 certificate.

RelativeDistinguishedName <RltvDstngshdNm> contains the following **RelativeDistinguishedName1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415

9.1.11.4.3.1.2.1.1.1.1 AttributeType <AttrTp>

Presence: [1..1]

Definition: Type of attribute of a distinguished name (see X.500).

Datatype: "AttributeType1Code" on page 472

CodeName	Name	Definition
CNAT	CommonName	Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).
LATT	Locality	Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).

CodeName	Name	Definition
OATT	OrganisationName	Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).
OUAT	OrganisationUnitName	Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).
CATT	CountryName	Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).

9.1.11.4.3.1.2.1.1.1.2 AttributeValue <AttrVal>

Presence: [1..1]

Definition: Value of the attribute of a distinguished name (see X.500).

Datatype: "Max140Text" on page 517

9.1.11.4.3.1.2.1.2 SerialNumber <SrlNb>

Presence: [1..1]

Definition: Certificate serial number (see X.509).

Datatype: "Max500Binary" on page 463

9.1.11.4.3.1.2.2 KeyIdentifier <KeyIdr>

Presence: [1..1]

Definition: Identifier of a cryptographic asymmetric key, previously exchanged between initiator and recipient.

KeyIdentifier <KeyIdr> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.4.3.1.3 KeyEncryptionAlgorithm <KeyNcrptnAlgo>

Presence: [1..1]

Definition: Algorithm to encrypt the key encryption key (KEK).

KeyEncryptionAlgorithm <KeyNcrptnAlgo> contains the following elements (see "AlgorithmIdentification19" on page 449 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		450
	Parameter <*Param*>	[0..1]			450
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		450
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		451
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]	±		451

9.1.11.4.3.1.4 EncryptedKey <NcrptdKey>

Presence: [1..1]

Definition: Encrypted key encryption key (KEK).

Datatype: "Max5000Binary" on page 462

9.1.11.4.3.2 KEK <KEK>

Presence: [1..1]

Definition: Key encryption key using previously distributed symmetric key.

KEK <KEK> contains the following **KEK8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		416
	KEKIdentification <*KEKId*>	[1..1]	±		416
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		417
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		417

9.1.11.4.3.2.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.4.3.2.2 KEKIdentification <KEKId>

Presence: [1..1]

Definition: Identification of the key encryption key (KEK).

KEKIdentification <KEKId> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.4.3.2.3 KeyEncryptionAlgorithm <KeyNcrptnAlgo>

Presence: [1..1]

Definition: Algorithm to encrypt the key encryption key (KEK).

KeyEncryptionAlgorithm <KeyNcrptnAlgo> contains the following elements (see "AlgorithmIdentification29" on page 442 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		442
	Parameter <*Param*>	[0..1]			444
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		444
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		445
	BytePadding <*BPddg*>	[0..1]	CodeSet		445

9.1.11.4.3.2.4 EncryptedKey <NcrptdKey>

Presence: [0..1]

Definition: Encrypted key encryption key (KEK).

Datatype: "Max500Binary" on page 463

9.1.11.4.3.3 KeyIdentifier <KeyIdr>

Presence: [1..1]

Definition: Identification of a protection key without a session key, shared and previously exchanged between the initiator and the recipient.

KeyIdentifier <KeyIdr> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.4.4 EncryptedContent <NcrptdCntt>

Presence: [0..1]

Definition: Data protection by encryption (digital envelope), with an encryption key.

EncryptedContent <NcrptdCntt> contains the following **EncryptedContent6** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		418
	ContentEncryptionAlgorithm <*CnttNcrptnAlgo*>	[0..1]	±		418
	EncryptedData <*NcrptdData*>	[1..1]	Binary		419

9.1.11.4.4.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data which have been encrypted.

Datatype: "ContentType2Code" on page 480

CodeName	Name	Definition
DATA	PlainData	Generic, non cryptographic, or unqualified data content - (ASN.1 Object Identifier: id-data).
SIGN	SignedData	Digital signature - (ASN.1 Object Identifier: id-signedData).
EVLP	EnvelopedData	Encrypted data, with encryption key - (ASN.1 Object Identifier: id-envelopedData).
DGST	DigestedData	Message digest - (ASN.1 Object Identifier: id-digestedData).
AUTH	AuthenticatedData	MAC (Message Authentication Code), with encryption key - (ASN.1 Object Identifier: id-ct-authData).

9.1.11.4.4.2 ContentEncryptionAlgorithm <CnttNcrptnAlgo>

Presence: [0..1]

Definition: Algorithm used to encrypt the data.

ContentEncryptionAlgorithm <CnttNcrptnAlgo> contains the following elements (see "AlgorithmIdentification29" on page 442 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		442
	Parameter <*Param*>	[0..1]			444
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		444
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		445
	BytePadding <*BPddg*>	[0..1]	CodeSet		445

9.1.11.4.4.3 EncryptedData <NcrptdData>

Presence: [1..1]

Definition: Encrypted data, result of the content encryption.

Datatype: "Max100KBinary" on page 461

9.1.11.5 CryptographicKey16

Definition: Cryptographic Key.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Identification <*Id*>	[1..1]	Text		419
	AdditionalIdentification <*AddtlId*>	[0..1]	Binary		419
	Name <*Nm*>	[0..1]	Text		420
	SecurityProfile <*SctyPrfl*>	[0..1]	Text		420
	ItemNumber <*ItmNb*>	[0..1]	Text		420
	Version <*Vrsn*>	[1..1]	Text		420
	Type <*Tp*>	[0..1]	CodeSet		420
	Function <*Fctn*>	[0..*]	CodeSet		421
	ActivationDate <*ActvtnDt*>	[0..1]	DateTime		421
	DeactivationDate <*DeactvtnDt*>	[0..1]	DateTime		422
	KeyValue <*KeyVal*>	[0..1]	±		422
	KeyCheckValue <*KeyChckVal*>	[0..1]	Binary		422
	AdditionalManagementInformation <*AddtlMgmtInf*>	[0..*]			422
	Name <*Nm*>	[1..1]	Text		422
	Value <*Val*>	[0..1]	Text		423

9.1.11.5.1 Identification <Id>

Presence: [1..1]

Definition: Name of the cryptographic key.

Datatype: "Max350Text" on page 518

9.1.11.5.2 AdditionalIdentification <AddtlId>

Presence: [0..1]

Definition: Additional identification of the key.

Usage

For derived unique key per transaction (DUKPT) keys, the key serial number (KSN) with the 21 bits of the transaction counter set to zero.

Datatype: "Max35Binary" on page 462

9.1.11.5.3 Name <Nm>

Presence: [0..1]

Definition: Name of the Cryptographic Element.

Datatype: "Max256Text" on page 518

9.1.11.5.4 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the set of security elements to which this element belongs.

Datatype: "Max35Text" on page 519

9.1.11.5.5 ItemNumber <ItmNb>

Presence: [0..1]

Definition: Hierarchical identification of a key inside all the key system. It is composed of all item numbers of the upper level components, separated by the '.' character, ended by the item number of the current component.

Datatype: "Max35Text" on page 519

9.1.11.5.6 Version <Vrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max256Text" on page 518

9.1.11.5.7 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 481

CodeName	Name	Definition
AES2	AES128	AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE3	DES112	Data encryption standard key of 112 bits (without the parity bits).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.
AES9	AES192	AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
AES5	AES256	AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal

CodeName	Name	Definition
		Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

9.1.11.5.8 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 488

CodeName	Name	Definition
ENCR	Encryption	Key may encrypt.
DCPT	Decryption	Key may decrypt.
DENC	DataEncryption	Key may encrypt data.
DDEC	DataDecryption	Key may decrypt data.
TRNI	TranslateInput	Key may encrypt information before translation.
TRNX	TranslateOutput	Key may encrypt information after translation.
MACG	MessageAuthenticationCodeGeneration	Key may generate message authentication codes (MAC).
MACV	MessageAuthenticationCodeVerification	Key may verify message authentication codes (MAC).
SIGG	SignatureGeneration	Key may generate digital signatures.
SUGV	SignatureVerification	Key may verify digital signatures.
PINE	PINEncryption	Key may encrypt personal identification numbers (PIN).
PIND	PINDecryption	Key may decrypt personal identification numbers (PIN).
PINV	PINVerification	Key may verify personal identification numbers (PIN).
KEYG	KeyGeneration	Key may generate keys.
KEYI	KeyImport	Key may import keys.
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

9.1.11.5.9 ActivationDate <ActvtnDt>

Presence: [0..1]

Definition: Date and time on which the key must be activated.

Datatype: "ISODateTime" on page 513

9.1.11.5.10 DeactivationDate <DeactvtnDt>

Presence: [0..1]

Definition: Date and time on which the key must be deactivated.

Datatype: "ISODateTime" on page 513

9.1.11.5.11 KeyValue <KeyVal>

Presence: [0..1]

Definition: Encrypted cryptographic key.

KeyValue <KeyVal> contains the following elements (see "ContentInformationType30" on page 423 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.11.5.12 KeyCheckValue <KeyChckVal>

Presence: [0..1]

Definition: Value for checking a cryptographic key security parameter.

Datatype: "Max35Binary" on page 462

9.1.11.5.13 AdditionalManagementInformation <AddtlMgmtInf>

Presence: [0..*]

Definition: Additional Information needed by the receiver to securely process the management of the security element.

AdditionalManagementInformation <AddtlMgmtInf> contains the following **GenericInformation1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Name <*Nm*>	[1..1]	Text		422
	Value <*Val*>	[0..1]	Text		423

9.1.11.5.13.1 Name <Nm>

Presence: [1..1]

Definition: Name of the generic information to exchange.

Datatype: "Max70Text" on page 520

9.1.11.5.13.2 Value <Val>

Presence: [0..1]

Definition: Value of the generic information to exchange.

Datatype: "Max140Text" on page 517

9.1.11.6 ContentInformationType30

Definition: General cryptographic message syntax (CMS) containing protected data.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		423
	EnvelopedData <*EnvlpdData*>	[0..1]	±		423
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		424
	SignedData <*SgndData*>	[0..1]	±		425
	DigestedData <*DgstdData*>	[0..1]	±		426

9.1.11.6.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data protection.

Datatype: "ContentType2Code" on page 480

CodeName	Name	Definition
DATA	PlainData	Generic, non cryptographic, or unqualified data content - (ASN.1 Object Identifier: id-data).
SIGN	SignedData	Digital signature - (ASN.1 Object Identifier: id-signedData).
EVLP	EnvelopedData	Encrypted data, with encryption key - (ASN.1 Object Identifier: id-envelopedData).
DGST	DigestedData	Message digest - (ASN.1 Object Identifier: id-digestedData).
AUTH	AuthenticatedData	MAC (Message Authentication Code), with encryption key - (ASN.1 Object Identifier: id-ct-authData).

9.1.11.6.2 EnvelopedData <EnvlpdData>

Presence: [0..1]

Definition: Data protection by encryption, with a session key.

EnvelopedData <EnvlpdData> contains the following elements (see "EnvelopedData9" on page 409 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		410
	OriginatorInformation <*OrgtrInf*>	[0..1]			411
	Certificate <*Cert*>	[0..*]	Binary		411
	Recipient <*Rcpt*>	[1..*]			411
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			412
	Version <*Vrsn*>	[0..1]	Quantity		413
	RecipientIdentification <*RcptId*>	[1..1]			413
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			413
	Issuer <*Issr*>	[1..1]			414
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			414
	AttributeType <*AttrTp*>	[1..1]	CodeSet		414
	AttributeValue <*AttrVal*>	[1..1]	Text		415
	SerialNumber <*SrlNb*>	[1..1]	Binary		415
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		415
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		415
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		416
Or	KEK <*KEK*>	[1..1]			416
	Version <*Vrsn*>	[0..1]	Quantity		416
	KEKIdentification <*KEKId*>	[1..1]	±		416
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		417
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		417
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		417
	EncryptedContent <*NcrptdCntt*>	[0..1]			418
	ContentType <*CnttTp*>	[1..1]	CodeSet		418
	ContentEncryptionAlgorithm <*CnttNcrptnAlgo*>	[0..1]	±		418
	EncryptedData <*NcrptdData*>	[1..1]	Binary		419

9.1.11.6.3 AuthenticatedData <AuthntcdData>

Presence: [0..1]

Definition: Data protection by a message authentication code (MAC).

AuthenticatedData <AuthntcdData> contains the following elements (see "AuthenticatedData8" on page 429 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		430
	Recipient <*Rcpt*>	[1..*]			430
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			431
	Version <*Vrsn*>	[0..1]	Quantity		432
	RecipientIdentification <*RcptId*>	[1..1]			432
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			432
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		434
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		434
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		435
Or	KEK <*KEK*>	[1..1]			435
	Version <*Vrsn*>	[0..1]	Quantity		435
	KEKIdentification <*KEKId*>	[1..1]	±		435
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		436
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		436
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		436
	MACAlgorithm <*MACAlgo*>	[1..1]	±		437
	EncapsulatedContent <*NcpsltdCntt*>	[1..1]	±		437
	MAC <*MAC*>	[1..1]	Binary		437

9.1.11.6.4 SignedData <SgndData>

Presence: [0..1]

Definition: Data protected by a digital signatures.

SignedData <SgndData> contains the following elements (see "SignedData7" on page 401 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		402
	DigestAlgorithm <*DgstAlgo*>	[0..*]	±		402
	EncapsulatedContent <*NcpsltdCntt*>	[0..1]	±		403
	Certificate <*Cert*>	[0..*]	Binary		403
	Signer <*Sgnr*>	[0..*]			403
	Version <*Vrsn*>	[0..1]	Quantity		404
	SignerIdentification <*SgnrId*>	[0..1]			404
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			404
	Issuer <*Issr*>	[1..1]			404
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405
	SerialNumber <*SrlNb*>	[1..1]	Binary		405
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		406
	DigestAlgorithm <*DgstAlgo*>	[1..1]	±		406
	SignedAttributes <*SgndAttrbts*>	[0..*]			406
	Name <*Nm*>	[1..1]	Text		406
	Value <*Val*>	[0..1]	Text		406
	SignatureAlgorithm <*SgntrAlgo*>	[1..1]	±		407
	Signature <*Sgntr*>	[1..1]	Binary		407

9.1.11.6.5 DigestedData <DgstdData>

Presence: [0..1]

Definition: Data protected by a digest.

DigestedData <DgstdData> contains the following elements (see "DigestedData5" on page 400 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		401
	DigestAlgorithm <*DgstAlgo*>	[1..1]	±		401
	EncapsulatedContent <*NcpsltdCntt*>	[1..1]	±		401
	Digest <*Dgst*>	[1..1]	Binary		401

9.1.11.7 ContentInformationType29

Definition: General cryptographic message syntax (CMS) containing data. protected by a MAC or a digital signature.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		427
	AuthenticatedData <*AuthntcdData*>	[0..1]	±		427
	SignedData <*SgndData*>	[0..1]	±		428

9.1.11.7.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data protection.

Datatype: "ContentType2Code" on page 480

CodeName	Name	Definition
DATA	PlainData	Generic, non cryptographic, or unqualified data content - (ASN.1 Object Identifier: id-data).
SIGN	SignedData	Digital signature - (ASN.1 Object Identifier: id-signedData).
EVLP	EnvelopedData	Encrypted data, with encryption key - (ASN.1 Object Identifier: id-envelopedData).
DGST	DigestedData	Message digest - (ASN.1 Object Identifier: id-digestedData).
AUTH	AuthenticatedData	MAC (Message Authentication Code), with encryption key - (ASN.1 Object Identifier: id-ct-authData).

9.1.11.7.2 AuthenticatedData <AuthntcdData>

Presence: [0..1]

Definition: Data protection by a message authentication code (MAC).

AuthenticatedData <AuthntcdData> contains the following elements (see "AuthenticatedData8" on page 429 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		430
	Recipient <*Rcpt*>	[1..*]			430
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			431
	Version <*Vrsn*>	[0..1]	Quantity		432
	RecipientIdentification <*RcptId*>	[1..1]			432
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			432
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		434
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		434
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		435
Or	KEK <*KEK*>	[1..1]			435
	Version <*Vrsn*>	[0..1]	Quantity		435
	KEKIdentification <*KEKId*>	[1..1]	±		435
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		436
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		436
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		436
	MACAlgorithm <*MACAlgo*>	[1..1]	±		437
	EncapsulatedContent <*NcpsltdCntt*>	[1..1]	±		437
	MAC <*MAC*>	[1..1]	Binary		437

9.1.11.7.3 SignedData <SgndData>

Presence: [0..1]

Definition: Data protected by a digital signatures.

SignedData <SgndData> contains the following elements (see "SignedData7" on page 401 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		402
	DigestAlgorithm <*DgstAlgo*>	[0..*]	±		402
	EncapsulatedContent <*NcpsltdCntt*>	[0..1]	±		403
	Certificate <*Cert*>	[0..*]	Binary		403
	Signer <*Sgnr*>	[0..*]			403
	Version <*Vrsn*>	[0..1]	Quantity		404
	SignerIdentification <*SgnrId*>	[0..1]			404
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			404
	Issuer <*Issr*>	[1..1]			404
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			405
	AttributeType <*AttrTp*>	[1..1]	CodeSet		405
	AttributeValue <*AttrVal*>	[1..1]	Text		405
	SerialNumber <*SrlNb*>	[1..1]	Binary		405
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		406
	DigestAlgorithm <*DgstAlgo*>	[1..1]	±		406
	SignedAttributes <*SgndAttrbts*>	[0..*]			406
	Name <*Nm*>	[1..1]	Text		406
	Value <*Val*>	[0..1]	Text		406
	SignatureAlgorithm <*SgntrAlgo*>	[1..1]	±		407
	Signature <*Sgntr*>	[1..1]	Binary		407

9.1.11.8 AuthenticatedData8

Definition: Message authentication code (MAC), computed on the data to protect with an encryption key.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		430
	Recipient <*Rcpt*>	[1..*]			430
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			431
	Version <*Vrsn*>	[0..1]	Quantity		432
	RecipientIdentification <*RcptId*>	[1..1]			432
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			432
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		434
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		434
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		435
Or	KEK <*KEK*>	[1..1]			435
	Version <*Vrsn*>	[0..1]	Quantity		435
	KEKIdentification <*KEKId*>	[1..1]	±		435
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		436
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		436
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		436
	MACAlgorithm <*MACAlgo*>	[1..1]	±		437
	EncapsulatedContent <*NcpsltdCntt*>	[1..1]	±		437
	MAC <*MAC*>	[1..1]	Binary		437

9.1.11.8.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.8.2 Recipient <Rcpt>

Presence: [1..*]

Definition: Session key or protection key identification used by the recipient.

Recipient <Rcpt> contains one of the following **Recipient11Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	KeyTransport <*KeyTrnsprt*>	[1..1]			431
	Version <*Vrsn*>	[0..1]	Quantity		432
	RecipientIdentification <*RcptId*>	[1..1]			432
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			432
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		434
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		434
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		435
Or	KEK <*KEK*>	[1..1]			435
	Version <*Vrsn*>	[0..1]	Quantity		435
	KEKIdentification <*KEKId*>	[1..1]	±		435
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		436
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		436
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		436

9.1.11.8.2.1 KeyTransport <KeyTrnsprt>

Presence: [1..1]

Definition: Encryption key using previously distributed asymmetric public key.

KeyTransport <KeyTrnsprt> contains the following **KeyTransport8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		432
	RecipientIdentification <*RcptId*>	[1..1]			432
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			432
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		434
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		434
	EncryptedKey <*NcrptdKey*>	[1..1]	Binary		435

9.1.11.8.2.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.8.2.1.2 RecipientIdentification <RcptId>

Presence: [1..1]

Definition: Identification of a cryptographic asymmetric key for the recipient.

RecipientIdentification <RcptId> contains one of the following **Recipient12Choice** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
{Or	IssuerAndSerialNumber <*IssrAndSrlNb*>	[1..1]			432
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434
Or}	KeyIdentifier <*KeyIdr*>	[1..1]	±		434

9.1.11.8.2.1.2.1 IssuerAndSerialNumber <IssrAndSrlNb>

Presence: [1..1]

Definition: Certificate issuer name and serial number (see ITU X.509).

IssuerAndSerialNumber <IssrAndSrlNb> contains the following **IssuerAndSerialNumber2** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Issuer <*Issr*>	[1..1]			433
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434
	SerialNumber <*SrlNb*>	[1..1]	Binary		434

9.1.11.8.2.1.2.1.1 Issuer <Issr>

Presence: [1..1]

Definition: Certificate issuer name (see X.509).

Issuer <Issr> contains the following **CertificateIssuer1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	RelativeDistinguishedName <*RltvDstngshdNm*>	[1..*]			433
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434

9.1.11.8.2.1.2.1.1.1 RelativeDistinguishedName <RltvDstngshdNm>

Presence: [1..*]

Definition: Relative distinguished name inside a X.509 certificate.

RelativeDistinguishedName <RltvDstngshdNm> contains the following **RelativeDistinguishedName1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	AttributeType <*AttrTp*>	[1..1]	CodeSet		433
	AttributeValue <*AttrVal*>	[1..1]	Text		434

9.1.11.8.2.1.2.1.1.1.1 AttributeType <AttrTp>

Presence: [1..1]

Definition: Type of attribute of a distinguished name (see X.500).

Datatype: "AttributeType1Code" on page 472

CodeName	Name	Definition
CNAT	CommonName	Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).
LATT	Locality	Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).

CodeName	Name	Definition
OATT	OrganisationName	Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).
OUAT	OrganisationUnitName	Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).
CATT	CountryName	Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).

9.1.11.8.2.1.2.1.1.1.2 AttributeValue <AttrVal>

Presence: [1..1]

Definition: Value of the attribute of a distinguished name (see X.500).

Datatype: "Max140Text" on page 517

9.1.11.8.2.1.2.1.2 SerialNumber <SrlNb>

Presence: [1..1]

Definition: Certificate serial number (see X.509).

Datatype: "Max500Binary" on page 463

9.1.11.8.2.1.2.2 KeyIdentifier <KeyIdr>

Presence: [1..1]

Definition: Identifier of a cryptographic asymmetric key, previously exchanged between initiator and recipient.

KeyIdentifier <KeyIdr> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.8.2.1.3 KeyEncryptionAlgorithm <KeyNcrptnAlgo>

Presence: [1..1]

Definition: Algorithm to encrypt the key encryption key (KEK).

KeyEncryptionAlgorithm <KeyNcrptnAlgo> contains the following elements (see "AlgorithmIdentification19" on page 449 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		450
	Parameter <*Param*>	[0..1]			450
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		450
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		451
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]	±		451

9.1.11.8.2.1.4 EncryptedKey <NcrptdKey>

Presence: [1..1]

Definition: Encrypted key encryption key (KEK).

Datatype: "Max5000Binary" on page 462

9.1.11.8.2.2 KEK <KEK>

Presence: [1..1]

Definition: Key encryption key using previously distributed symmetric key.

KEK <KEK> contains the following **KEK8** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Version <*Vrsn*>	[0..1]	Quantity		435
	KEKIdentification <*KEKId*>	[1..1]	±		435
	KeyEncryptionAlgorithm <*KeyNcrptnAlgo*>	[1..1]	±		436
	EncryptedKey <*NcrptdKey*>	[0..1]	Binary		436

9.1.11.8.2.2.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 515

9.1.11.8.2.2.2 KEKIdentification <KEKId>

Presence: [1..1]

Definition: Identification of the key encryption key (KEK).

KEKIdentification <KEKId> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.8.2.2.3 KeyEncryptionAlgorithm <KeyNcrptnAlgo>

Presence: [1..1]

Definition: Algorithm to encrypt the key encryption key (KEK).

KeyEncryptionAlgorithm <KeyNcrptnAlgo> contains the following elements (see "AlgorithmIdentification29" on page 442 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		442
	Parameter <*Param*>	[0..1]			444
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		444
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		445
	BytePadding <*BPddg*>	[0..1]	CodeSet		445

9.1.11.8.2.2.4 EncryptedKey <NcrptdKey>

Presence: [0..1]

Definition: Encrypted key encryption key (KEK).

Datatype: "Max500Binary" on page 463

9.1.11.8.2.3 KeyIdentifier <KeyIdr>

Presence: [1..1]

Definition: Identification of a protection key without a session key, shared and previously exchanged between the initiator and the recipient.

KeyIdentifier <KeyIdr> contains the following elements (see "KEKIdentifier7" on page 278 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	KeyIdentification <*KeyId*>	[1..1]	Text		278
	KeyVersion <*KeyVrsn*>	[1..1]	Text		278
	SequenceNumber <*SeqNb*>	[0..1]	Quantity		278
	DerivationIdentification <*DerivtnId*>	[0..1]	Binary		278

9.1.11.8.3 MACAlgorithm <MACAlgo>

Presence: [1..1]

Definition: Algorithm to compute message authentication code (MAC).

MACAlgorithm <MACAlgo> contains the following elements (see "AlgorithmIdentification22" on page 445 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		445
	Parameter <*Param*>	[0..1]			448
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		448
	BytePadding <*BPddg*>	[0..1]	CodeSet		448

9.1.11.8.4 EncapsulatedContent <NcpsltdCntt>

Presence: [1..1]

Definition: Data to authenticate.

EncapsulatedContent <NcpsltdCntt> contains the following elements (see "EncapsulatedContent3" on page 387 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ContentType <*CnttTp*>	[1..1]	CodeSet		387
	Content <*Cntt*>	[0..1]	Binary		387

9.1.11.8.5 MAC <MAC>

Presence: [1..1]

Definition: Message authentication code value.

Datatype: "Max140Binary" on page 461

9.1.11.9 AlgorithmIdentification30

Definition: Identification of a cryptographic algorithm and parameters for digital signatures.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		438
	Parameter <*Param*>	[0..1]			439
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		440
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]			440
	Algorithm <*Algo*>	[1..1]	CodeSet		441
	Parameter <*Param*>	[0..1]			441
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		441
	SaltLength <*SaltLngth*>	[0..1]	Quantity		441
	TrailerField <*TrlrFld*>	[0..1]	Quantity		441
	OIDCurveName <*OIDCrvNm*>	[0..1]	Text		442

9.1.11.9.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the algorithm.

Datatype: "Algorithm25Code" on page 469

CodeName	Name	Definition
ERS2	SHA256WithRSA	Signature algorithms with RSA, using SHA-256 digest algorithm - (ASN.1 Object Identifier: sha256WithRSAEncryption).
ERS1	SHA1WithRSA	The DEPRECATED Signature algorithms with RSA (PKCS #1 version 2.1), using SHA-1 digest algorithm - (ASN.1 Object Identifier: sha1WithRSAEncryption).
RPSS	RSASSA-PSS	Signature algorithm with Appendix, Probabilistic Signature Scheme (PKCS #1 version 2.1), - (ASN.1 Object Identifier: id-RSASSA-PSS).
ERS3	SHA3-256WithRSA	Signature algorithms with RSA, using SHA3-256 digest algorithm. (ASN.1 Object Identifier: id-rsassa-pkcs1-v1-5-with-sha3-256).
ED32	EcdsaSha3-256	Elliptic Curve Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.
ED33	EcdsaSha3-384	Elliptic Curve Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.
ED35	EcdsaSha3-512	Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.

CodeName	Name	Definition
ED23	EcdsaSha384	Elliptic Curve Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.
ED25	EcdsaSha512	Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.
ES22	EcsdsaSha256	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.
ES32	EcsdaSha3-256	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.
ES33	EcsdsaSha3-384	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.
ES35	EcsdsaSha3-512	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.
ES23	EcsdsaSha384	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.
ES25	EcsdsaSha512	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.
ED22	EcdsaSha256	Elliptic Curve Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.

9.1.11.9.2 Parameter <Param>

Presence: [0..1]

Definition: Parameters of the RSASSA-PSS digital signature algorithm (RSA signature algorithm with appendix: Probabilistic Signature Scheme).

Parameter <Param> contains the following **Parameter15** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		440
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]			440
	Algorithm <*Algo*>	[1..1]	CodeSet		441
	Parameter <*Param*>	[0..1]			441
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		441
	SaltLength <*SaltLngth*>	[0..1]	Quantity		441
	TrailerField <*TrlrFld*>	[0..1]	Quantity		441
	OIDCurveName <*OIDCrvNm*>	[0..1]	Text		442

9.1.11.9.2.1 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Identification of the digest algorithm.

Datatype: "Algorithm16Code" on page 464

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).
SH31	SHA3-224	Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).
SH32	SHA3-256	Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).
SH33	SHA3-384	Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).
SH35	SHA3-512	Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).
SHK1	SHAKE128	Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).
SHK2	SHAKE256	Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).

9.1.11.9.2.2 MaskGeneratorAlgorithm <MskGnrtrAlgo>

Presence: [0..1]

Definition: Mask generator function cryptographic algorithm and parameters.

MaskGeneratorAlgorithm <MskGnrtrAlgo> contains the following **AlgorithmIdentification12** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		441
	Parameter <*Param*>	[0..1]			441
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		441

9.1.11.9.2.2.1 Algorithm <Algo>

Presence: [1..1]

Definition: Mask generator function cryptographic algorithm.

Datatype: "Algorithm8Code" on page 471

CodeName	Name	Definition
MGF1	MGF1	Generator Function, used for RSA encryption and RSA igital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).

9.1.11.9.2.2.2 Parameter <Param>

Presence: [0..1]

Definition: Parameters associated to the mask generator function cryptographic algorithm.

Parameter <Param> contains the following **Parameter5** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		441

9.1.11.9.2.2.2.1 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Digest algorithm used in the mask generator function.

Datatype: "Algorithm11Code" on page 464

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).

9.1.11.9.2.3 SaltLength <SaltLngth>

Presence: [0..1]

Definition: Length of the salt to include in the signature.

Datatype: "Number" on page 515

9.1.11.9.2.4 TrailerField <TrlrFld>

Presence: [0..1]

Definition: Trailer field number.

Datatype: "Number" on page 515

9.1.11.9.2.5 OIDCurveName <OIDCrvNm>

Presence: [0..1]

Definition: Name of the Elliptic Curve according to the OID notation.

Datatype: "Max140Text" on page 517

9.1.11.10 AlgorithmIdentification29

Definition: Cryptographic algorithm and parameters for the protection of the transported key.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		442
	Parameter <*Param*>	[0..1]			444
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		444
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		445
	BytePadding <*BPddg*>	[0..1]	CodeSet		445

9.1.11.10.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the algorithm.

Datatype: "Algorithm24Code" on page 467

CodeName	Name	Definition
EA2C	AES128CBC	AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
E3DC	DES112CBC	Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with double length key (112 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) algorithm, as specified in ANSI X9.24-2009 Annex A.
UKPT	UKPT	UKPT (Unique Key Per Transaction) or Master Session Key key encryption - (ASN.1 Object Identifier: id-ukpt-wrap).
UKA2	UKPTwithAES192	UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 -

CodeName	Name	Definition
		November 6, 2001 - Advanced Encryption Standard).
EA9C	AES192CBC	AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA5C	AES256CBC	AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
DA12	AESDUKPT128ECB	AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A, With key length of 128 bits.
DA19	AESDUKPT192ECB	AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 192 bits.
DA25	AESDUKPT256ECB	AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 256 bits.
N108	Nist800-108KeyDerivation	Key Derivation according to the Special Publication from the NIST entitled 800-108.
EA5R	AES256CTR	AES (Advanced Encryption Standard) CTR (Counter) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA9R	AES192CTR	AES (Advanced Encryption Standard) CTR (Counter) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA2R	AES128CTR	AES (Advanced Encryption Standard) CTR (Counter) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
E3DR	DES112CTR	Triple DES (Data Encryption Standard) CTR (Counter) encryption with double length key (112 Bit) as defined in FIPS SP 800-38a.
E36C	DES168CBC	Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with triple length key (168 Bit) as defined

CodeName	Name	Definition
		in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).
E36R	DES168CTR	Triple DES (Data Encryption Standard) CTR (Counter) encryption with triple length key (168 Bit) as defined in FIPS SP 800-38a.
SD5C	SDE056CBC	The DEPRECATED Simple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with simple length key (56 Bit) as defined in FIPS PUB 81 - (ASN.1 Object Identifier: des-cbc).
UKA1	UKPTwithAES128	UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
UKA3	UKPTwithAES256	UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

9.1.11.10.2 Parameter <Param>

Presence: [0..1]

Definition: Parameters associated to the encryption algorithm.

Parameter <Param> contains the following **Parameter12** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		444
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		445
	BytePadding <*BPddg*>	[0..1]	CodeSet		445

9.1.11.10.2.1 EncryptionFormat <NcrptnFrmt>

Presence: [0..1]

Definition: Format of data before encryption, if the format is not plaintext or implicit.

Datatype: "EncryptionFormat2Code" on page 485

CodeName	Name	Definition
TR31	TR31	Format of a cryptographic key specified by the ANSI X9 TR-31 standard.
TR34	TR34	Format of a cryptographic key specified by the ANSI X9 TR-34 standard.

CodeName	Name	Definition
I238	ISO20038KeyWrap	Format of a cryptographic key specified by the ISO20038 standard.

9.1.11.10.2.2 InitialisationVector <InitlstnVctr>

Presence: [0..1]

Definition: Initialisation vector of a cipher block chaining (CBC) mode encryption.

Datatype: "Max500Binary" on page 463

9.1.11.10.2.3 BytePadding <BPddg>

Presence: [0..1]

Definition: Byte padding for a cypher block chaining mode encryption, if the padding is not implicit.

Datatype: "BytePadding1Code" on page 476

CodeName	Name	Definition
LNGT	LengthPadding	Message to encrypt is completed by a byte value containing the total number of added bytes.
NUL8	Null80Padding	Message to encrypt is completed by one bit of value 1, followed by null bits until the encryption block length is reached.
NULG	NullLengthPadding	Message to encrypt is completed by null byte values, the last byte containing the total number of added bytes.
NULL	NullPadding	Message to encrypt is completed by null bytes.
RAND	RandomPadding	Message to encrypt is completed by random value, the last byte containing the total number of added bytes.

9.1.11.11 AlgorithmIdentification22

Definition: Identification of a cryptographic algorithm and parameters for the MAC computation.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		445
	Parameter <*Param*>	[0..1]			448
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		448
	BytePadding <*BPddg*>	[0..1]	CodeSet		448

9.1.11.11.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the MAC algorithm.

Datatype: "Algorithm17Code" on page 465

CodeName	Name	Definition
MACC	RetailCBCMAC	Retail CBC (Chaining Block Cypher) MAC (Message Authentication Code) (cf. ISO 9807, ANSI X9.19) - (ASN.1 Object Identifier: id-retail-cbc-mac).
MCCS	RetailSHA256MAC	Retail-CBC-MAC with SHA-256 (Secure HAsh standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-256).
CMA1	SHA256CMACwithAES128	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.
MCC1	RetailSHA1MAC	The DEPRECATED Retail-CBC-MAC with SHA-1 (Secure Hash standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-1).
CMA9	SHA384CMACwithAES192	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-384 digest of the message.
CMA5	SHA512CMACwithAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-512 digest of the message.
CMA2	SHA256CMACWithAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.

CodeName	Name	Definition
CM31	SHA3-256CMACWithAES128	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-256 digest of the message.
CM32	SHA3-384CMACWithAES192	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-384 digest of the message.
CM33	SHA3-512CMACWithAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-512 digest of the message.
MCS3	SHA3-256-3DESMAC	3DES CBC-MAC with SHA3-256 (SecureHAsh standard) and ISO/ IEC9797-1 method 2 padding.
CCA1	CMACAES128	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
CCA2	CMACAES192	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

CodeName	Name	Definition
CCA3	CMACAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

9.1.11.11.2 Parameter <Param>

Presence: [0..1]

Definition: Parameters associated to the MAC algorithm.

Parameter <Param> contains the following **Parameter7** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	InitialisationVector <*InitlstnVctr*>	[0..1]	Binary		448
	BytePadding <*BPddg*>	[0..1]	CodeSet		448

9.1.11.11.2.1 InitialisationVector <InitlstnVctr>

Presence: [0..1]

Definition: Initialisation vector of a cipher block chaining (CBC) mode encryption.

Datatype: "Max500Binary" on page 463

9.1.11.11.2.2 BytePadding <BPddg>

Presence: [0..1]

Definition: Byte padding for a cypher block chaining mode encryption, if the padding is not implicit.

Datatype: "BytePadding1Code" on page 476

CodeName	Name	Definition
LNGT	LengthPadding	Message to encrypt is completed by a byte value containing the total number of added bytes.
NUL8	Null80Padding	Message to encrypt is completed by one bit of value 1, followed by null bits until the encryption block length is reached.
NULG	NullLengthPadding	Message to encrypt is completed by null byte values, the last byte containing the total number of added bytes.
NULL	NullPadding	Message to encrypt is completed by null bytes.
RAND	RandomPadding	Message to encrypt is completed by random value, the last byte containing the total number of added bytes.

9.1.11.12 AlgorithmIdentification21

Definition: Cryptographic algorithm and parameters of digests.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		449

9.1.11.12.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the digest algorithm.

Datatype: "Algorithm16Code" on page 464

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).
SH31	SHA3-224	Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).
SH32	SHA3-256	Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).
SH33	SHA3-384	Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).
SH35	SHA3-512	Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).
SHK1	SHAKE128	Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).
SHK2	SHAKE256	Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).

9.1.11.13 AlgorithmIdentification19

Definition: Cryptographic algorithms and parameters for the protection of transported keys by an asymmetric key.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		450
	Parameter <*Param*>	[0..1]			450
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		450
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		451
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]	±		451

9.1.11.13.1 Algorithm <Algo>

Presence: [1..1]

Definition: Asymmetric encryption algorithm of a transport key.

Datatype: "Algorithm7Code" on page 471

CodeName	Name	Definition
ERSA	RSAEncryption	RSA encryption algorithm - (ASN.1 Object Identifier: rsaEncryption).
RSAO	RSAES-OAEP	RSA encryption scheme based on Optimal Asymmetric Encryption scheme (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-RSAES-OAEP).

9.1.11.13.2 Parameter <Param>

Presence: [0..1]

Definition: Parameters of the encryption algorithm.

Parameter <Param> contains the following **Parameter10** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	EncryptionFormat <*NcrptnFrmt*>	[0..1]	CodeSet		450
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		451
	MaskGeneratorAlgorithm <*MskGnrtrAlgo*>	[0..1]	±		451

9.1.11.13.2.1 EncryptionFormat <NcrptnFrmt>

Presence: [0..1]

Definition: Format of data before encryption, if the format is not plaintext or implicit.

Datatype: "EncryptionFormat2Code" on page 485

CodeName	Name	Definition
TR31	TR31	Format of a cryptographic key specified by the ANSI X9 TR-31 standard.
TR34	TR34	Format of a cryptographic key specified by the ANSI X9 TR-34 standard.
I238	ISO20038KeyWrap	Format of a cryptographic key specified by the ISO20038 standard.

9.1.11.13.2.2 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Identification of the digest algorithm.

Datatype: "Algorithm16Code" on page 464

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).
SH31	SHA3-224	Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).
SH32	SHA3-256	Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).
SH33	SHA3-384	Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).
SH35	SHA3-512	Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).
SHK1	SHAKE128	Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).
SHK2	SHAKE256	Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).

9.1.11.13.2.3 MaskGeneratorAlgorithm <MskGnrtrAlgo>

Presence: [0..1]

Definition: Mask generator function cryptographic algorithm and parameters.

MaskGeneratorAlgorithm <MskGnrtrAlgo> contains the following elements (see "AlgorithmIdentification18" on page 452 for details)

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		452
	Parameter <*Param*>	[0..1]			452
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		452

9.1.11.14 AlgorithmIdentification18

Definition: Mask generator function cryptographic algorithm and parameters.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Algorithm <*Algo*>	[1..1]	CodeSet		452
	Parameter <*Param*>	[0..1]			452
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		452

9.1.11.14.1 Algorithm <Algo>

Presence: [1..1]

Definition: Mask generator function cryptographic algorithm.

Datatype: "Algorithm8Code" on page 471

CodeName	Name	Definition
MGF1	MGF1	Generator Function, used for RSA encryption and RSA igital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).

9.1.11.14.2 Parameter <Param>

Presence: [0..1]

Definition: Parameters associated to the mask generator function cryptographic algorithm.

Parameter <Param> contains the following **Parameter9** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	DigestAlgorithm <*DgstAlgo*>	[0..1]	CodeSet		452

9.1.11.14.2.1 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Digest algorithm used in the mask generator function.

Datatype: "Algorithm16Code" on page 464

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS

CodeName	Name	Definition
		180-1 - (ASN.1 Object Identifier: id-sha1).
SH31	SHA3-224	Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).
SH32	SHA3-256	Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).
SH33	SHA3-384	Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).
SH35	SHA3-512	Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).
SHK1	SHAKE128	Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).
SHK2	SHAKE256	Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).

9.1.12 Structured Postal Address

9.1.12.1 PostalAddress2

Definition: Address of a party expressed in a formal structure, usually according to the country's postal services specifications.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StreetName <*StrtNm*>	[0..1]	Text		453
	PostCodeIdentification <*PstCdId*>	[1..1]	Text		453
	TownName <*TwnNm*>	[1..1]	Text		454
	CountrySubDivision <*CtrySubDvsn*>	[0..1]	Text		454
	Country <*Ctry*>	[1..1]	CodeSet	C3	454

9.1.12.1.1 StreetName <StrtNm>

Presence: [0..1]

Definition: Name of a street or thoroughfare.

Datatype: "Max70Text" on page 520

9.1.12.1.2 PostCodeIdentification <PstCdId>

Presence: [1..1]

Definition: Identifier consisting of a group of letters and/or numbers that is added to a postal address to assist the sorting of mail.

Datatype: "Max16Text" on page 517

9.1.12.1.3 TownName <TwnNm>

Presence: [1..1]

Definition: Name of a built-up area, with defined boundaries, and a local government.

Datatype: "Max35Text" on page 519

9.1.12.1.4 CountrySubDivision <CtrySubDvsn>

Presence: [0..1]

Definition: Identifies a subdivision of a country for example, state, region, county.

Datatype: "Max35Text" on page 519

9.1.12.1.5 Country <Ctry>

Presence: [1..1]

Definition: Nation with its own government.

Impacted by: C3 "Country"

Datatype: "CountryCode" on page 481

Constraints

- **Country**

  The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

9.1.13 Synchronisation

9.1.13.1 ProcessRetry3

Definition: Definition of retry process if activation of an action fails.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Delay <*Dely*>	[1..1]	Text		454
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		454
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		455

9.1.13.1.1 Delay <Dely>

Presence: [1..1]

Definition: Time period to wait for a retry in months, days, hours and minutes, leading zeros could be omitted.

Datatype: "Max9NumericText" on page 521

9.1.13.1.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of retries.

Datatype: "Number" on page 515

9.1.13.1.3 UnitOfTime <UnitOfTm>

Presence: [0..1]

Definition: Identification of the minimum unit of time used by time configuration parameters.

Datatype: "TimeUnit1Code" on page 510

CodeName	Name	Definition
DAYC	CalendarDay	Time unit is calendar day.
HOUR	Hour	Time unit is hour.
MINU	Minute	Time unit is minute.
MNTH	Month	Time unit is month.
SECO	Second	Time unit is second.
WEEK	Week	Time unit is week.
YEAR	Year	Time unit is year.

9.1.13.2 ProcessTiming6

Definition: Parameters defining the timing conditions to process an action.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	StartTime <*StartTm*>	[0..1]	DateTime		455
	EndTime <*EndTm*>	[0..1]	DateTime		455
	Period <*Prd*>	[0..1]	Text		455
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		456

9.1.13.2.1 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODateTime" on page 513

9.1.13.2.2 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODateTime" on page 513

9.1.13.2.3 Period <Prd>

Presence: [0..1]

Definition: Period delay between cyclic action activation in months, days, hours and minutes, leading zeros could be omitted.

Datatype: "Max9NumericText" on page 521

9.1.13.2.4 UnitOfTime <UnitOfTm>

Presence: [0..1]

Definition: Identification of the minimum unit of time used by time configuration parameters.

Datatype: "TimeUnit1Code" on page 510

CodeName	Name	Definition
DAYC	CalendarDay	Time unit is calendar day.
HOUR	Hour	Time unit is hour.
MINU	Minute	Time unit is minute.
MNTH	Month	Time unit is month.
SECO	Second	Time unit is second.
WEEK	Week	Time unit is week.
YEAR	Year	Time unit is year.

9.1.13.3 ProcessTiming5

Definition: Parameters defining the timing conditions to process an action.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	WaitingTime <*WtgTm*>	[0..1]	Text		456
	StartTime <*StartTm*>	[0..1]	DateTime		456
	EndTime <*EndTm*>	[0..1]	DateTime		456
	Period <*Prd*>	[0..1]	Text		457
	MaximumNumber <*MaxNb*>	[0..1]	Quantity		457
	UnitOfTime <*UnitOfTm*>	[0..1]	CodeSet		457

9.1.13.3.1 WaitingTime <WtgTm>

Presence: [0..1]

Definition: Waiting time after the previous action in months, days, hours and minutes, leading zeros could be omitted.

Datatype: "Max9NumericText" on page 521

9.1.13.3.2 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODateTime" on page 513

9.1.13.3.3 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODateTime" on page 513

9.1.13.3.4 Period <Prd>

Presence: [0..1]

Definition: Period delay between cyclic action activation in months, days, hours and minutes, leading zeros could be omitted.

Datatype: "Max9NumericText" on page 521

9.1.13.3.5 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of cyclic calls.

Datatype: "Number" on page 515

9.1.13.3.6 UnitOfTime <UnitOfTm>

Presence: [0..1]

Definition: Identification of the minimum unit of time used by time configuration parameters.

Datatype: "TimeUnit1Code" on page 510

CodeName	Name	Definition
DAYC	CalendarDay	Time unit is calendar day.
HOUR	Hour	Time unit is hour.
MINU	Minute	Time unit is minute.
MNTH	Month	Time unit is month.
SECO	Second	Time unit is second.
WEEK	Week	Time unit is week.
YEAR	Year	Time unit is year.

9.1.14 Token

9.1.14.1 Token1

Definition: Unencrypted sensitive data of a token.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	PaymentToken <*PmtTkn*>	[0..1]	Text		458
	TokenExpiryDate <*TknXpryDt*>	[0..1]	Text		458
	TokenRequestorIdentification <*TknRqstrId*>	[0..1]	Text		458
	TokenAssuranceData <*TknAssrncData*>	[0..1]	Text		458
	TokenAssuranceMethod <*TknAssrncMtd*>	[0..1]	Text		458
	TokenInitiatedIndicator <*TknInittdInd*>	[0..1]	Indicator		458

9.1.14.1.1 PaymentToken <PmtTkn>

Presence: [0..1]

Definition: Surrogate value of the PAN.

Datatype: "Max19NumericText" on page 517

9.1.14.1.2 TokenExpiryDate <TknXpryDt>

Presence: [0..1]

Definition: Expiry date of the payment token.

ISO 8583 bit 14.

Datatype: "Exact4NumericText" on page 516

9.1.14.1.3 TokenRequestorIdentification <TknRqstrId>

Presence: [0..1]

Definition: Identification of a party requesting a token.

Datatype: "Max11NumericText" on page 517

9.1.14.1.4 TokenAssuranceData <TknAssrncData>

Presence: [0..1]

Definition: Supporting information for the Token Assurance Method.

Datatype: "Max140Text" on page 517

9.1.14.1.5 TokenAssuranceMethod <TknAssrncMtd>

Presence: [0..1]

Definition: Value that allows a Token Service Provider to indicate the identification and verification performed representing the binding of the payment token to the underlying PAN and cardholder.

Datatype: "Max2NumericText" on page 518

9.1.14.1.6 TokenInitiatedIndicator <TknInittdInd>

Presence: [0..1]

Definition: Original transaction was initiated by Token.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.1.14.2 MerchantToken2

Definition: Merchant token information.

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	Token <*Tkn*>	[0..1]	Text		459
	TokenExpiryDate <*TknXpryDt*>	[0..1]	Text		459
	TokenCharacteristic <*TknChrtc*>	[0..*]	Text		459
	TokenRequestor <*TknRqstr*>	[0..1]			459
	ProviderIdentification <*PrvdrId*>	[1..1]	Text		459
	RequestorIdentification <*RqstrId*>	[1..1]	Text		460
	TokenAssuranceLevel <*TknAssrncLvl*>	[0..1]	Quantity		460
	TokenAssuranceData <*TknAssrncData*>	[0..1]	Binary		460
	TokenAssuranceMethod <*TknAssrncMtd*>	[0..1]	Text		460
	TokenInitiatedIndicator <*TknInittdInd*>	[0..1]	Indicator		460

9.1.14.2.1 Token <Tkn>

Presence: [0..1]

Definition: Surrogate value of the PAN.

Datatype: "Max35Text" on page 519

9.1.14.2.2 TokenExpiryDate <TknXpryDt>

Presence: [0..1]

Definition: Expiration date of the payment token that is generated by and maintained in the token vault.

Datatype: "Max10Text" on page 516

9.1.14.2.3 TokenCharacteristic <TknChrtc>

Presence: [0..*]

Definition: Additional payment token information.

Datatype: "Max35Text" on page 519

9.1.14.2.4 TokenRequestor <TknRqstr>

Presence: [0..1]

Definition: Identifier of a token provider requestor.

TokenRequestor <TknRqstr> contains the following **PaymentTokenIdentifiers1** elements

Or	MessageElement<*XML Tag*>	Mult.	Type	Constr. No.	Page
	ProviderIdentification <*PrvdrId*>	[1..1]	Text		459
	RequestorIdentification <*RqstrId*>	[1..1]	Text		460

9.1.14.2.4.1 ProviderIdentification <PrvdrId>

Presence: [1..1]

Definition: Identifier of the token provider.

Datatype: "Max35Text" on page 519

9.1.14.2.4.2 RequestorIdentification <RqstrId>

Presence: [1..1]

Definition: Identifier of the token requestor.

Datatype: "Max35Text" on page 519

9.1.14.2.5 TokenAssuranceLevel <TknAssrncLvl>

Presence: [0..1]

Definition: Level of confidence resulting of the identification and authentication of the cardholder performed and the entity that performed it.

Datatype: "Number" on page 515

9.1.14.2.6 TokenAssuranceData <TknAssrncData>

Presence: [0..1]

Definition: Information about the identification and verification of the cardholder.

Datatype: "Max500Binary" on page 463

9.1.14.2.7 TokenAssuranceMethod <TknAssrncMtd>

Presence: [0..1]

Definition: Value that allows a Token Service Provider to indicate the identification and verification performed representing the binding of the payment token to the underlying PAN and cardholder.

Datatype: "Max2NumericText" on page 518

9.1.14.2.8 TokenInitiatedIndicator <TknInittdInd>

Presence: [0..1]

Definition: Original transaction was initiated by Token.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 514):

- *Meaning When True:* True
- *Meaning When False:* False

9.2 Message Datatypes

9.2.1 Amount

9.2.1.1 ImpliedCurrencyAndAmount

Definition: Number of monetary units specified in a currency where the unit of currency is implied by the context and compliant with ISO 4217. The decimal separator is a dot.

Note: a zero amount is considered a positive amount.

Type: Amount

Format

minInclusive	0
totalDigits	18
fractionDigits	5

9.2.2 Binary

9.2.2.1 Max10000Binary

Definition: Specifies a binary string with a maximum length of 10000 binary bytes.

Type: Binary

Format

minLength	1
maxLength	10000

9.2.2.2 Max100KBinary

Definition: Binary data of 100K maximum.

Type: Binary

Format

minLength	1
maxLength	102400

9.2.2.3 Max10KBinary

Definition: Binary data of 10K maximum.

Type: Binary

Format

minLength	1
maxLength	10240

9.2.2.4 Max140Binary

Definition: Specifies a binary string with a maximum length of 140 binary bytes.

Type: Binary

Format

minLength	1
maxLength	140

9.2.2.5 Max2KBinary

Definition: Binary data of 2K maximum.

Type: Binary

Format

minLength	1
maxLength	2048

9.2.2.6 Max2MBBinary

Definition: Binary data of 2MB maximum.

Type: Binary

Format

minLength	1
maxLength	2097152

9.2.2.7 Max3000Binary

Definition: Specifies a binary string with a maximum length of 3000 binary bytes.

Type: Binary

Format

minLength	1
maxLength	3000

9.2.2.8 Max35Binary

Definition: Specifies a binary string with a maximum length of 35 binary bytes.

Type: Binary

Format

minLength	1
maxLength	35

9.2.2.9 Max5000Binary

Definition: Specifies a binary string with a maximum length of 5000 binary bytes.

Type: Binary

Format

minLength	1
maxLength	5000

9.2.2.10 Max500Binary

Definition: Specifies a binary string with a maximum length of 500 binary bytes.

Type: Binary

Format

minLength	1
maxLength	500

9.2.2.11 Min1Max256Binary

Definition: Specifies a binary string with a minimum length of 1 byte, and a maximum length of 256 bytes.

Type: Binary

Format

minLength	1
maxLength	256

9.2.2.12 Min5Max16Binary

Definition: Specifies a binary string with a minimum length of 5 bytes, and a maximum length of 16 bytes.

Type: Binary

Format

minLength	5
maxLength	16

9.2.3 CodeSet

9.2.3.1 ActiveCurrencyCode

Definition: A code allocated to a currency by a Maintenance Agency under an international identification scheme as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".

Type: CodeSet

Format

pattern	[A-Z]{3,3}

Constraints

- **ActiveCurrency**

  The currency code must be a valid active currency code, not yet withdrawn on the day the message containing the currency is exchanged. Valid active currency codes are registered with the ISO 4217

Maintenance Agency, consist of three (3) contiguous letters, and are not yet withdrawn on the day the message containing the Currency is exchanged.

9.2.3.2 AddressType2Code

Definition: Specifies the type of address.

Type: CodeSet

CodeName	Name	Definition
ADDR	Postal	Address is the complete postal address.
PBOX	POBox	Address is a postal office (PO) box.
HOME	Residential	Address is the home address.
BIZZ	Business	Address is the business address.
MLTO	MailTo	Address is the address to which mail is sent.
DLVY	DeliveryTo	Address is the address to which delivery is to take place.

9.2.3.3 Algorithm11Code

Definition: Identification of a digest algorithm.

Type: CodeSet

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).

9.2.3.4 Algorithm16Code

Definition: Identification of a digest algorithm.

Type: CodeSet

CodeName	Name	Definition
HS25	SHA256	Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).
HS38	SHA384	Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).

CodeName	Name	Definition
HS51	SHA512	Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).
HS01	SHA1	The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).
SH31	SHA3-224	Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).
SH32	SHA3-256	Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).
SH33	SHA3-384	Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).
SH35	SHA3-512	Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).
SHK1	SHAKE128	Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).
SHK2	SHAKE256	Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).

9.2.3.5 Algorithm17Code

Definition: Cryptographic algorithms for the MAC (Message Authentication Code).

Type: CodeSet

CodeName	Name	Definition
MACC	RetailCBCMAC	Retail CBC (Chaining Block Cypher) MAC (Message Authentication Code) (cf. ISO 9807, ANSI X9.19) - (ASN.1 Object Identifier: id-retail-cbc-mac).
MCCS	RetailSHA256MAC	Retail-CBC-MAC with SHA-256 (Secure HAsh standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-256).
CMA1	SHA256CMACwithAES128	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.
MCC1	RetailSHA1MAC	The DEPRECATED Retail-CBC-MAC with SHA-1 (Secure Hash standard) -

CodeName	Name	Definition
		(ASN.1 Object Identifier: id-retail-cbc-mac-sha-1).
CMA9	SHA384CMACwithAES192	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-384 digest of the message.
CMA5	SHA512CMACwithAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-512 digest of the message.
CMA2	SHA256CMACWithAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.
CM31	SHA3-256CMACWithAES128	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-256 digest of the message.
CM32	SHA3-384CMACWithAES192	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

CodeName	Name	Definition
		The CMAC algorithm is computed on the SHA3-384 digest of the message.
CM33	SHA3-512CMACWithAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-512 digest of the message.
MCS3	SHA3-256-3DESMAC	3DES CBC-MAC with SHA3-256 (SecureHAsh standard) and ISO/ IEC9797-1 method 2 padding.
CCA1	CMACAES128	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
CCA2	CMACAES192	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
CCA3	CMACAES256	CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

9.2.3.6 Algorithm24Code

Definition: Cryptographic algorithms for the protection of transported keys.

Type: CodeSet

CodeName	Name	Definition
EA2C	AES128CBC	AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 128 bits cryptographic key as defined by the Federal Information

CodeName	Name	Definition
		Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
E3DC	DES112CBC	Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with double length key (112 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) algorithm, as specified in ANSI X9.24-2009 Annex A.
UKPT	UKPT	UKPT (Unique Key Per Transaction) or Master Session Key key encryption - (ASN.1 Object Identifier: id-ukpt-wrap).
UKA2	UKPTwithAES192	UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA9C	AES192CBC	AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA5C	AES256CBC	AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
DA12	AESDUKPT128ECB	AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A, With key length of 128 bits.
DA19	AESDUKPT192ECB	AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 192 bits.
DA25	AESDUKPT256ECB	AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 256 bits.
N108	Nist800-108KeyDerivation	Key Derivation according to the Special Publication from the NIST entitled 800-108.
EA5R	AES256CTR	AES (Advanced Encryption Standard) CTR (Counter) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing

CodeName	Name	Definition
		Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA9R	AES192CTR	AES (Advanced Encryption Standard) CTR (Counter) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EA2R	AES128CTR	AES (Advanced Encryption Standard) CTR (Counter) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
E3DR	DES112CTR	Triple DES (Data Encryption Standard) CTR (Counter) encryption with double length key (112 Bit) as defined in FIPS SP 800-38a.
E36C	DES168CBC	Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with triple length key (168 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).
E36R	DES168CTR	Triple DES (Data Encryption Standard) CTR (Counter) encryption with triple length key (168 Bit) as defined in FIPS SP 800-38a.
SD5C	SDE056CBC	The DEPRECATED Simple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with simple length key (56 Bit) as defined in FIPS PUB 81 - (ASN.1 Object Identifier: des-cbc).
UKA1	UKPTwithAES128	UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
UKA3	UKPTwithAES256	UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).

9.2.3.7 Algorithm25Code

Definition: Cryptographic algorithms for digital signatures.

Type: CodeSet

CodeName	Name	Definition
ERS2	SHA256WithRSA	Signature algorithms with RSA, using SHA-256 digest algorithm - (ASN.1 Object Identifier: sha256WithRSAEncryption).
ERS1	SHA1WithRSA	The DEPRECATED Signature algorithms with RSA (PKCS #1 version 2.1), using SHA-1 digest algorithm - (ASN.1 Object Identifier: sha1WithRSAEncryption).
RPSS	RSASSA-PSS	Signature algorithm with Appendix, Probabilistic Signature Scheme (PKCS #1 version 2.1), - (ASN.1 Object Identifier: id-RSASSA-PSS).
ERS3	SHA3-256WithRSA	Signature algorithms with RSA, using SHA3-256 digest algorithm. (ASN.1 Object Identifier: id-rsassa-pkcs1-v1-5-with-sha3-256).
ED32	EcdsaSha3-256	Elliptic Curve Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.
ED33	EcdsaSha3-384	Elliptic Curve Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.
ED35	EcdsaSha3-512	Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.
ED23	EcdsaSha384	Elliptic Curve Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.
ED25	EcdsaSha512	Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.
ES22	EcsdsaSha256	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.
ES32	EcsdaSha3-256	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.
ES33	EcsdsaSha3-384	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.
ES35	EcsdsaSha3-512	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.
ES23	EcsdsaSha384	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.
ES25	EcsdsaSha512	Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.

CodeName	Name	Definition
ED22	EcdsaSha256	Elliptic Curve Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.

9.2.3.8 Algorithm7Code

Definition: Asymmetric encryption algorithm of a transport key.

Type: CodeSet

CodeName	Name	Definition
ERSA	RSAEncryption	RSA encryption algorithm - (ASN.1 Object Identifier: rsaEncryption).
RSAO	RSAES-OAEP	RSA encryption scheme based on Optimal Asymmetric Encryption scheme (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-RSAES-OAEP).

9.2.3.9 Algorithm8Code

Definition: Mask generator functions of the RSAES-OAEP encryption algorithm (RSA Encryption Scheme: Optimal Asymmetric Encryption Padding).

Type: CodeSet

CodeName	Name	Definition
MGF1	MGF1	Generator Function, used for RSA encryption and RSA igital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).

9.2.3.10 AmountUnit1Code

Definition: Unit of a amount (for loyalty or account).

Type: CodeSet

CodeName	Name	Definition
MONE	Monetary	The amount is expressed in a monetary value in a currency.
POIN	Point	The amount is expressed in point.

9.2.3.11 AttendanceContext1Code

Definition: Human attendance at the POI location during the transaction.

Type: CodeSet

CodeName	Name	Definition
ATTD	Attended	Attended payment, with an attendant.
SATT	SemiAttended	Semi-attended, including self checkout. An attendant supervises several payment, and could be called to help the cardholder.

CodeName	Name	Definition
UATT	Unattended	Unattended payment, no attendant present.

9.2.3.12 AttributeType1Code

Definition: Type of attribute of a distinguished name (DN).

Type: CodeSet

CodeName	Name	Definition
CNAT	CommonName	Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).
LATT	Locality	Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).
OATT	OrganisationName	Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).
OUAT	OrganisationUnitName	Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).
CATT	CountryName	Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).

9.2.3.13 AttributeType2Code

Definition: Attributes of certificate extensions.

Type: CodeSet

CodeName	Name	Definition
EMAL	EmailAddress	Email address of the certificate subject.
CHLG	ChallengePassword	Password by which an entity may request certificate revocation.

9.2.3.14 AuthenticationEntity2Code

Definition: Entity or device that has performed the verification.

Type: CodeSet

CodeName	Name	Definition
ICCD	ICC	Application in the chip card (Integrated Circuit Card), for instance an offline PIN verification.
AGNT	AuthorisedAgent	Authorisation agent of the issuer.
MERC	Merchant	Merchant (for example signature verification by the attendant).
ACQR	Acquirer	Acquirer of the transaction.
ISSR	Issuer	Card issuer.
TRML	Terminal	Secure application in the terminal.

9.2.3.15 AuthenticationMethod6Code

Definition: Methods used to authenticate a person or a card.

Type: CodeSet

CodeName	Name	Definition
NPIN	OnLinePIN	On-line PIN authentication (Personal Identification Number).
PPSG	PaperSignature	Handwritten paper signature.
PSWD	Password	Authentication by a password.
SCRT	SecureCertificate	Electronic commerce transaction secured with the X.509 certificate of a customer.
SCNL	SecuredChannel	Channel-encrypted transaction.
SNCT	SecureNoCertificate	Secure electronic transaction without cardholder certificate.
CPSG	SignatureCapture	Electronic signature capture (handwritten signature).
ADDB	BillingAddressVerification	Cardholder billing address verification.
BIOM	Biometry	Biometric authentication of the cardholder.
CDHI	CardholderIdentificationData	Cardholder data provided for verification, for instance social security number, driver license number, passport number.
CRYP	CryptogramVerification	Verification of a cryptogram generated by a chip card or another device, for instance ARQC (Authorisation Request Cryptogram).
CSCV	CSCVerification	Verification of Card Security Code.
PSVE	PassiveAuthentication	Authentication based on statistical cardholder behaviour.
CSEC	SecureElectronicCommerce	Authentication performed during a secure electronic commerce transaction.
ADDS	ShippingAddressVerification	Cardholder shipping address verification.
MANU	ManualVerification	Manual verification, for example passport or drivers license.
FPIN	OfflinePIN	Off-line PIN authentication (Personal Identification Number).
TOKP	PaymentToken	Verification or authentication related to the use of a payment token, for instance the validation of the authorised use of a token.

9.2.3.16 AuthenticationMethod8Code

Definition: Method to authenticate the customer or its card.

Type: CodeSet

CodeName	Name	Definition
TOKA	AuthenticationToken	A token is used to verify an already performed authentication.
ADDB	BillingAddressVerification	Cardholder billing address verification.
BYPS	Bypass	Authentication bypassed by the merchant.
BIOM	Biometry	Biometric authentication of the cardholder.
CDHI	CardholderIdentificationData	Cardholder data provided for verification, for instance social security number, driver license number, passport number.
CRYP	CryptogramVerification	Verification of a cryptogram generated by a chip card or another device, for instance ARQC (Authorisation Request Cryptogram).
CSCV	CSCVerification	Verification of Card Security Code.
MANU	ManualVerification	Manual verification, for example passport or drivers license.
MERC	MerchantAuthentication	Merchant-related authentication.
MOBL	Mobile	Customer mobile device.
FPIN	OfflinePIN	Off-line PIN authentication (Personal Identification Number).
NPIN	OnLinePIN	On-line PIN authentication (Personal Identification Number).
OTHR	Other	Other customer authentication.
PPSG	PaperSignature	Handwritten paper signature.
PSVE	PassiveAuthentication	Authentication based on statistical cardholder behaviour.
PSWD	Password	Authentication by a password.
TOKP	PaymentToken	Verification or authentication related to the use of a payment token, for instance the validation of the authorised use of a token.
SCRT	SecureCertificate	Electronic commerce transaction secured with the X.509 certificate of a customer.
SCNL	SecuredChannel	Channel-encrypted transaction.
CSEC	SecureElectronicCommerce	Authentication performed during a secure electronic commerce transaction.
SNCT	SecureNoCertificate	Secure electronic transaction without cardholder certificate.
ADDS	ShippingAddressVerification	Cardholder shipping address verification.
CPSG	SignatureCapture	Electronic signature capture (handwritten signature).

CodeName	Name	Definition
TOKN	TokenAuthentication	Cryptogram generated by the token requestor or a customer device to validate the authorised use of a token.
UKNW	UnknownMethod	Authentication method is performed unknown.

9.2.3.17 AuthenticationResult1Code

Definition: Specifies the result of authentication done.

Type: CodeSet

CodeName	Name	Definition
DENY	Denial	The authentication didn't succeed.
MRCH	MerchantNotEnroled	Merchant not enrolled in the authentication programme.
CARD	NonParticipation	The card does not participate in the authentication programme.
AUTH	UnableToAuthenticate	The authentication couldn't be carried out.
CRPT	WithCryptogram	Authentication succeeded with a cryptogram.
UCRP	WithoutCryptogram	Authentication succeeded without a cryptogram.

9.2.3.18 BarcodeType1Code

Definition: Type of BarCode coding.

Type: CodeSet

CodeName	Name	Definition
COQR	BarcodeEncodedAs2DQRCode	Barcode encoded according to the 2Dimensions Quick Response Code Standard.
C128	BarcodeEncodedAsCode128	Barcode encoded according to the Code 128 standard.
C025	BarcodeEncodedAsCode25	Barcode encoded according to the Code 25 standard.
C039	BarcodeEncodedAsCode39	Barcode encoded according to the Code 39 standard.
EA13	BarcodeEncodedAsEA13	Barcode encoded according to the EAN13 standard.
EAN8	BarcodeEncodedAsEAN8	Barcode encoded according to the EAN8 standard.
P417	BarcodeEncodedAsPDF417	Barcode encoded according to the PDF417 standard.
UPCA	BarcodeEncodedAsUPCA	Barcode encoded according to the UPCA standard.

9.2.3.19 BatchTransactionType1Code

Definition: Type of transactions to include in a batch transfer.

Type: CodeSet

CodeName	Name	Definition
DTCT	DebitCredit	Debit and credit transactions.
CNCL	Cancellation	Cancellation of a previous transaction.
FAIL	Failed	Failed transactions.
DCLN	Declined	Declined transactions.

9.2.3.20 BusinessArea1Code

Definition: Specifies the business context of the transaction

Type: CodeSet

CodeName	Name	Definition
AIBD	ArtificialIntelligenceBasedDecision	The payment is initiated by an artificial intelligence based decision.
OPMT	Openpayment	The card is used in a Transit business case where the fare amount is not known when the transaction is initiated.
PPAY	PlainPayment	The card is used to perform a plain payment.
TKNF	TransitKnownFare	The card is used in a Transit business case where the fare amount is known when the transaction is initiated.

9.2.3.21 BytePadding1Code

Definition: Byte padding for a cypher block chaining mode encryption, if the padding is not implicit.

Type: CodeSet

CodeName	Name	Definition
LNGT	LengthPadding	Message to encrypt is completed by a byte value containing the total number of added bytes.
NUL8	Null80Padding	Message to encrypt is completed by one bit of value 1, followed by null bits until the encryption block length is reached.
NULG	NullLengthPadding	Message to encrypt is completed by null byte values, the last byte containing the total number of added bytes.
NULL	NullPadding	Message to encrypt is completed by null bytes.
RAND	RandomPadding	Message to encrypt is completed by random value, the last byte containing the total number of added bytes.

9.2.3.22 CancellationProcess2Code

Definition: Configuration of the exchanges to perform the cancellation of a payment transaction.

Type: CodeSet

CodeName	Name	Definition
ADVC	Advice	Card payment transaction may be cancelled by an advice only before closure of the reconciliation period or before the capture by batch.
NALW	NotAllowed	Card payment transaction cannot be cancelled by the acquirer.
REQU	Request	Card payment transaction may also be cancelled after the closure of the reconciliation period or after the capture by batch. In this case a cancellation request exchange is required.
APPL	ApplicationLevel	Cancellation of the Card payment transaction is defined by the payment application.

9.2.3.23 CardDataReading5Code

Definition: Type of reading of the card data.

Type: CodeSet

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.

9.2.3.24 CardDataReading8Code

Definition: Type of reading of the card data.

Type: CodeSet

CodeName	Name	Definition
TAGC	Tag	Tag reading capabilities (RFID, etc.).
PHYS	Physical	Keyboard entry or OCR reading of embossing or printed data, either at time of transaction or after the event.
BRCD	BarCode	Bar code.
MGST	MagneticStripe	Magnetic stripe.
CICC	ICC	ICC (Integrated Circuit Card) with contact containing software applications conform to ISO 7816.
DFLE	AccountData	Account data on file.
CTLS	ProximityReader	Contactless proximity reader.
ECTL	EMVProximityReader	Contactless proximity reader, with application conform to the standard EMV (standard initiated by Europay, Mastercard and Visa).
CDFL	CardOnFile	Card information are stored on a file.
SICC	SynchronousIntegratedCircuitCard	Synchronous ICC - (Integrated Circuit Card) with contact.
UNKW	Unknown	Unknown card reading capability.
QRCD	QRCode	Quick response code.
OPTC	OpticalCode	Optical coded reading capabilities (e.g. barcode, QR code, etc.)

9.2.3.25 CardFallback1Code

Definition: Information about card entry mode fallback.

Type: CodeSet

CodeName	Name	Definition
FFLB	FallbackAfterFailure	Card fall-back occurred during the transaction in progress. The previous transaction on the terminal failed.
SFLB	FallbackAfterSuccess	Card fall-back occurred during the transaction in progress. The previous transaction on the terminal was successful.
NFLB	NoFallback	No card fall-back during the transaction in progress.

9.2.3.26 CardholderVerificationCapability4Code

Definition: Cardholder verification capabilities by the terminal.

Type: CodeSet

CodeName	Name	Definition
APKI	AccountDigitalSignature	Account based digital signature.

CodeName	Name	Definition
CHDT	CardholderData	Cardholder authentication data.
MNSG	ManualSignature	Manual signature verification.
MNVR	ManualVerification	Other manual verification, for example passport or drivers license.
FBIG	OfflineBiographics	Offline biographics.
FBIO	OfflineBiometrics	Offline biometrics.
FDSG	OfflineDigitalSignature	Offline digital signature analysis.
FCPN	OfflinePINClear	Offline PIN in clear (Personal Identification Number).
FEPN	OfflinePINEncrypted	Offline PIN encrypted (Personal Identification Number).
NPIN	OnLinePIN	Online PIN (Personal Identification Number).
PKIS	PKISignature	PKI (Public Key Infrastructure) based digital signature.
SCEC	SecureElectronicCommerce	Three domain secure (three domain secure authentication of the cardholder).
NBIO	OnLineBiometrics	Online biometrics.
NOVF	NoCapabilities	No cardholder verification capability.
OTHR	Other	Other cardholder verification capabilities.

9.2.3.27 CardIdentificationType1Code

Definition: Type of account identification.

Type: CodeSet

CodeName	Name	Definition
ACCT	AccountNumber	Account identification.
BARC	BarCode	Bar-code with a specific form of identification.
ISO2	ISOTrack2	ISO Track 2 including identification.
PHON	PhoneNumber	A phone number identifies the account on which the phone card is assigned.
CPAN	PrimaryAccountNumber	Standard card identification (card number).
PRIV	PrivativeNumbering	An identification set by a privative application.
UUID	UniversalUniqueIdentification	A Universal Unique Identification code is set for identification.

9.2.3.28 CardPaymentServiceType10Code

Definition: Requested certificate management service.

Type: CodeSet

CodeName	Name	Definition
CRTC	CreateCertificate	Creation of an X.509 certificate with the public key and the information of the owner of the asymmetric key provided by the requestor.
CRTR	RenewCerificate	Renewal of an X.509 certificate, protected by the certificate to renew.
CRTK	RevokeCertificate	Revocation of an active X.509 certificate.
WLSR	RemoveWhiteList	Remove a POI from the white list of the terminal manager.
WLSA	AddWhiteList	Add a POI in the white list of the terminal manager.

9.2.3.29 CardProductType1Code

Definition: Type of card product.

Type: CodeSet

CodeName	Name	Definition
COMM	CommercialCard	Cards issued as a means of business expenditure, for instance business card or corporate card. The user could be a company, an individual for business expenses or a self employed for business purposes.
CONS	ConsumerCard	Cards issued as a means of personal expenditure. The user is always an individual.

9.2.3.30 CheckType1Code

Definition: Type of bank check.

Type: CodeSet

CodeName	Name	Definition
BANK	BankCheck	The check is guaranteed by a bank.
BUSI	BusinessCheck	The check belongs to a Company or a professional entity.
GOVC	GovernmentCheck	Check issued by Government.
PAYR	PayrollCheck	Check issued by a company for the employees.
PERS	PersonalCheck	The check belongs to an individual.

9.2.3.31 ContentType2Code

Definition: Identification of the type of a Cryptographic Message Syntax (CMS) data structure.

Type: CodeSet

CodeName	Name	Definition
DATA	PlainData	Generic, non cryptographic, or unqualified data content - (ASN.1 Object Identifier: id-data).
SIGN	SignedData	Digital signature - (ASN.1 Object Identifier: id-signedData).
EVLP	EnvelopedData	Encrypted data, with encryption key - (ASN.1 Object Identifier: id-envelopedData).
DGST	DigestedData	Message digest - (ASN.1 Object Identifier: id-digestedData).
AUTH	AuthenticatedData	MAC (Message Authentication Code), with encryption key - (ASN.1 Object Identifier: id-ct-authData).

9.2.3.32 CountryCode

Definition: Code to identify a country, a dependency, or another area of particular geopolitical interest, on the basis of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

Type: CodeSet

Format

pattern	[A-Z]{2,2}

Constraints

- **Country**

  The code is checked against the list of country names obtained from the United Nations (ISO 3166, Alpha-2 code).

9.2.3.33 CryptographicKeyType3Code

Definition: Codes for qualifying the type of cryptographic keys.

Type: CodeSet

CodeName	Name	Definition
AES2	AES128	AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE3	DES112	Data encryption standard key of 112 bits (without the parity bits).
DKP9	DUKPT2009	DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.
AES9	AES192	AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS

CodeName	Name	Definition
		197 - November 6, 2001 - Advanced Encryption Standard).
AES5	AES256	AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

9.2.3.34 DataSetCategory10Code

Definition: Maintenance services provided by a terminal manager.

Type: CodeSet

CodeName	Name	Definition
AQPR	AcquirerParameters	Acquirer specific configuration parameters for the point of interaction (POI) system.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
MTMG	MasterTerminalManager	The terminal manager is the master.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
MTOR	Monitoring	Monitoring of the terminal estate.
SCPR	SecurityParameters	Point of interaction parameters related to the security of software application and application protocol.
SWPK	SoftwareModule	Software module.
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.

9.2.3.35 DataSetCategory16Code

Definition: Maintenance service to delegate.

Type: CodeSet

CodeName	Name	Definition
ACQP	AcquirerProtocolParameters	Configuration parameters of the payment acquirer protocol.

CodeName	Name	Definition
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
APSB	ApplicationParametersSubsetCreation	Creation of a subset of the configuration parameters of an application.
KDWL	KeyDownload	Download of cryptographic keys with the related information.
KMGT	KeyManagement	Activate, deactivate or revoke loaded cryptographic keys.
RPRT	Reporting	Reporting on activity, status and error of a point of interaction.
SWPK	SoftwareModule	Software module.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
SACP	SaleComponent	Component of the Sale system.
SAPR	SaleToPOIProtocolParameters	Parameters related to the Sale to POI protocol.
LOGF	LogFile	Any repository used for recording log traces.
RPFL	ReportFile	Report file generated by the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
SPRP	ServiceProviderParameters	Service Provider specific parameters for the point of interaction (POI) system.

9.2.3.36 DataSetCategory17Code

Definition: Category of data set.

Type: CodeSet

CodeName	Name	Definition
AQPR	AcquirerParameters	Acquirer specific configuration parameters for the point of interaction (POI) system.
APPR	ApplicationParameters	Payment application specific configuration parameters for the point of interaction (POI) system.
TXCP	BatchCapture	Batch upload of transaction data (data capture of a group of transactions).
AKCP	CaptureResponse	Batch download response for the batch capture of transactions.

CodeName	Name	Definition
DLGT	DelegationData	Data needed to create a terminal management sub-domain.
MGTP	ManagementPlan	Configuration of management plan in the point of interaction.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
SCPR	SecurityParameters	Point of interaction parameters related to the security of software application and application protocol.
SWPK	SoftwareModule	Software module.
STRP	StatusReport	Report of software configuration and parameter status.
TRPR	TerminalParameters	Point of interaction parameters attached to the terminal as serial number or physical capabilities.
VDPR	VendorParameters	Point of interaction parameters defined by the manufacturer for instance the PIN verification capabilities.
PARA	Parameters	Any combination of configuration parameters for the point of interaction (POI).
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
CRTF	CertificateParameters	Certificate provided by a terminal manager.
LOGF	LogFile	Any repository used for recording log traces.
CMRQ	CertificateManagementRequest	Trigger for CertificateManagementRequest.
MDFL	MediaFile	Media file managed by an application of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

9.2.3.37 DocumentType7Code

Definition: Specifies a type of financial or commercial document.

Type: CodeSet

CodeName	Name	Definition
JNRL	Journal	When the POI or the Sale System wants to store a message on the journal printer or electronic journal of the Sale Terminal (it is sometimes a Sale Logging/Journal Printer).
CRCP	CustomerReceipt	When the Sale System requires the POI system to print the Customer receipt.

CodeName	Name	Definition
HRCP	CashierReceipt	When the Sale system print the Cashier copy of the Payment receipt.
SRCP	SaleReceipt	When the Sale System requires the POI system to print the Sale receipt.
RPIN	RelatedPaymentInstruction	Document is a linked payment instruction to which the current payment instruction is related, for example, in a cover scenario.
VCHR	Voucher	Document is an electronic payment document.

9.2.3.38 EncryptionFormat2Code

Definition: Format of data before encryption, if the format is not plaintext or implicit.

Type: CodeSet

CodeName	Name	Definition
TR31	TR31	Format of a cryptographic key specified by the ANSI X9 TR-31 standard.
TR34	TR34	Format of a cryptographic key specified by the ANSI X9 TR-34 standard.
I238	ISO20038KeyWrap	Format of a cryptographic key specified by the ISO20038 standard.

9.2.3.39 ExchangePolicy2Code

Definition: Exchange policy between parties.

Type: CodeSet

CodeName	Name	Definition
ONDM	OnDemand	Exchange is performed if requested by the acquirer in a previous exchange, or at any time by the acceptor.
IMMD	Immediately	Exchange is performed just after the transaction completion.
ASAP	AsSoonAsPossible	As soon as the acquirer is contacted, for example with the next on-line transaction.
AGRP	AsGroup	Exchanges are performed after reaching a maximum number of transaction or time period.
NBLT	NumberLimit	Exchange is performed after reaching a number of transactions without exchanges with the acquirer.
TTLT	TotalLimit	Exchange is performed after reaching a cumulative amount of transactions without exchanges with the acquirer.
CYCL	Cyclic	Cyclic exchanges based on the related time conditions.

CodeName	Name	Definition
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

9.2.3.40 Exemption1Code

Definition: Strong customer authentication exemption.

Type: CodeSet

CodeName	Name	Definition
LOWA	LowAmountExemption	Transaction's amount is low and could be processed without strong customer authentication.
MINT	MerchantInitiatedTransaction	Transaction is initiated by the Card Acceptor.
RECP	RecurringPayment	Transaction is one of a series of recurring payment.
SCPE	SecureCorporatePaymentExemption	Transaction is a secure corporate payment.
SCAD	StrongCustomerAuthenticationDelegation	Card Acceptor is a strong customer authentication delegate.
TRAE	TransactionRiskAnalysisExemption	According to the transaction risk analysis the strong customer authentication is not mandated.
PKGE	TransportFareOrParkingFeeUnattendedPaymentExemption	Payment is processed in a environment where strong customer authentication is inappropriate.
TMBE	TrustedMerchantBeneficiaryExemption	Cardholder has enrolled the Card Acceptor in the exemption list of strong customer authentication.

9.2.3.41 FinancialCapture1Code

Definition: Mode for the financial capture of the transaction by the acquirer.

Type: CodeSet

CodeName	Name	Definition
AUTH	Authorisation	Financial capture of the transaction is performed by the acquirer during the authorisation exchange.
COMP	Completion	Financial capture of the transaction is performed by the acquirer during the completion exchange.
BTCH	Batch	Financial capture of the transaction is performed by the acquirer at the reception of a batch transfer.

9.2.3.42 InformationQualify1Code

Definition: Qualification of the information to sent to an output logical device, to display or print to the Cashier or the Customer.

Type: CodeSet

CodeName	Name	Definition
CUSA	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
DISP	Display	Standard display interface.
DOCT	Document	When the POI System wants to print specific document (check, dynamic currency conversion ...). Used by the Sale System when the printer is not located on the Sale System.
ERRO	Error	The information is related to an error situation occurring on the message sender.
INPT	Input	Answer to a question or information to be entered by the Cashier or the Customer, at the request of the POI Terminal or the Sale Terminal.
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
RCPT	Receipt	Where you print the Payment receipt that could be located on the Sale System or in some cases a restricted Sale ticket on the POI Terminal.
SOND	Sound	Standard sound interface.
STAT	Status	The information is a new state on which the message sender is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
VCHR	Voucher	Coupons, voucher or special ticket generated by the POI or the Sale System and to be printed.

9.2.3.43 InputCommand1Code

Definition: Type of requested input

Type: CodeSet

CodeName	Name	Definition
DCSG	DecimalString	Wait for a string of digit characters with a decimal point, the length range could be specified.
DGSG	DigitString	Wait for a string of digit characters.

CodeName	Name	Definition
GAKY	GetAnyKey	Wait for a key pressed on the Terminal, to be able to read the message displayed on the Terminal.
GCNF	GetConfirmation	Wait for a confirmation Yes (Y) or No (N) on the Sale System. Wait for a confirmation (Valid or Cancel button) on the POI Terminal. The result of the command is a Boolean: True or False.
GFKY	GetFunctionKey	Wait for a function key pressed on the Terminal: From POI, Valid, Clear, Correct, Generic Function key number. From Sale, Generic Function key.
GMNE	GetMenuEntry	To choose an entry among a list of entries (all of them are not necessary selectable). The OutputFormat has to be MenuEntry.
PSWD	Password	Request to enter a password with masked characters while typing the password.
SITE	SiteManager	Wait for a confirmation Yes (Y) or No (N) of the Site Manager on the Sale System.
TXSG	TextString	Wait for a string of alphanumeric characters.
HTML	XHTMLText	Wait for a XHTML data.
SIGN	Signature	Request to wait for signature.

9.2.3.44 ISO3NumericCountryCode

Definition: Code to identify a country, a dependency, or another area of particular geopolitical interest, on the basis of country names obtained from the United Nations (ISO 3166, Numeric-3 code). The code is checked against the list of country names coded with three digit characters, defined in the standard.

Type: CodeSet

Format

pattern	[0-9]{3,3}

9.2.3.45 KeyUsage1Code

Definition: Allowed usages of the key.

Type: CodeSet

CodeName	Name	Definition
ENCR	Encryption	Key may encrypt.
DCPT	Decryption	Key may decrypt.
DENC	DataEncryption	Key may encrypt data.
DDEC	DataDecryption	Key may decrypt data.
TRNI	TranslateInput	Key may encrypt information before translation.

CodeName	Name	Definition
TRNX	TranslateOutput	Key may encrypt information after translation.
MACG	MessageAuthenticationCodeGeneration	Key may generate message authentication codes (MAC).
MACV	MessageAuthenticationCodeVerification	Key may verify message authentication codes (MAC).
SIGG	SignatureGeneration	Key may generate digital signatures.
SUGV	SignatureVerification	Key may verify digital signatures.
PINE	PINEncryption	Key may encrypt personal identification numbers (PIN).
PIND	PINDecryption	Key may decrypt personal identification numbers (PIN).
PINV	PINVerification	Key may verify personal identification numbers (PIN).
KEYG	KeyGeneration	Key may generate keys.
KEYI	KeyImport	Key may import keys.
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

9.2.3.46 LanguageCode

Definition: Specifies a language.

Type: CodeSet

Constraints

- **ValidationByTable**

  Must be a valid terrestrial language.

9.2.3.47 LocationCategory3Code

Definition: Indicates the type of integration of the POI terminal in the sale environment.

Type: CodeSet

CodeName	Name	Definition
INDR	Indoor	Indoor terminal.
IPMP	InsidePump	Terminal incorporated in the pump dispensing petrol.
MPOI	MultiplePOITerminal	Multiple terminals linked to a unique sale terminal.
MPMP	MultiplePump	Outdoor terminal serving several petrol pumps.
MSLE	MultipleSaleTerminal	Terminal serving multiple sale terminals.
SSLE	SingleSaleTerminal	Terminal linked to a unique sale terminal.

CodeName	Name	Definition
VNDG	VendingMachine	Terminal integrated in a vending machine.

9.2.3.48 LocationCategory4Code

Definition: Indicates the type of integration of the POI terminal in the sale environment.

Type: CodeSet

CodeName	Name	Definition
ABRD	Aboard	Aboard is used when the sale is done in a vehicle (e.g a bus, train, ship, airplane, taxi, etc).
NMDC	Nomadic	Nomadic is used when the merchant is traveling to different locations (e.g fair or sport events, home delivery, food truck).
FIXD	PhysicalShop	Fixed location, for example in a shop.
VIRT	VirtualShop	Virtual Shop is used for any ecommerce solution.

9.2.3.49 LoyaltyHandling1Code

Definition: Possible types of Loyalty processing.

Type: CodeSet

CodeName	Name	Definition
ALLO	Allowed	The loyalty is accepted, but the POI has not to require or ask a loyalty card. The loyalty is involved by the payment card (e.g. an hybrid or linked card).
DENY	Forbidden	No loyalty card to read and loyalty transaction to process. Any attempt to enter a pure loyalty card is rejected.
PRCS	Processed	The loyalty transaction is already processed, no loyalty card or loyalty transaction to process.
PROP	Proposed	The loyalty is accepted, and the POI has to ask a loyalty card. If the Customer does not enter a loyalty card, no loyalty transaction is realised.
REQU	Required	The loyalty is required, and the POI refuses the processing of the message request if the cardholder does not enter a loyalty card.

9.2.3.50 MemoryUnit1Code

Definition: Unit of the memory size.

Type: CodeSet

CodeName	Name	Definition
BYTE	Byte	Byte.
EXAB	ExaByte	Exa byte.
GIGA	GigaByte	Giga byte.
KILO	KiloByte	Kilo byte.
MEGA	MegaByte	Mega byte.
PETA	PetaByte	Peta byte.
TERA	TeraByte	Tera byte.

9.2.3.51 MessageFunction43Code

Definition: Type of message supporting a service.

Type: CodeSet

CodeName	Name	Definition
FAUQ	FinancialAuthorisationRequest	Request for authorisation with financial capture.
CCAQ	CancellationRequest	Request for cancellation.
CMPV	CompletionAdvice	Advice for completion without financial capture.
DGNP	DiagnosticRequest	Request for diagnostic.
RCLQ	ReconciliationRequest	Request for reconciliation.
CCAV	CancellationAdvice	Advice for cancellation.
BTCH	BatchTransfer	Transfer the financial data as a collection of transction.
FRVA	FinancialReversalAdvice	Advice for reversal with financial capture.
AUTQ	AuthorisationRequest	The initiator requests an authorisation without financial impact to complete the transaction.
FCMV	FinancialCompletionAdvice	Advice for completion with financial capture.
DCCQ	CurrencyConversionRequest	Request for dynamic currency conversion.
RVRA	ReversalAdvice	Advice for reversal without financial capture.
DCAV	CurrencyConversionAdvice	Advice for dynamic currency conversion.
TRNA	TransactionAdvice	Advise of the transaction's processing.
NFRQ	NonFinancialRequest	Initiator of the message requests additional information to the receiver.
TRPQ	TransactionReportRequest	Request to receive of a report of transaction from the issuer to the receiver.

9.2.3.52 MessageItemCondition1Code

Definition: Rule to apply for the presence of a message item.

Type: CodeSet

CodeName	Name	Definition
MNDT	Mandatory	Message item must be present.
CFVL	ConfiguredValue	Message item must be present with the configured value.
DFLT	DefaultValue	Message item has the configured value if the item is absent.
ALWV	AllowedValues	Message item must have one of the configured values.
IFAV	IfAvailable	Message item has to be present if available.
COPY	Copy	Message item is present if it was present in a previous related message with the same value.
UNSP	NotSupported	Message item is not supported and has to be absent.

9.2.3.53 NetworkType1Code

Definition: Type of communication network.

Type: CodeSet

CodeName	Name	Definition
IPNW	InternetProtocol	Protocol of an IP network.
PSTN	PublicTelephone	Protocol of a Public Switched Telephone Network (PSTN).

9.2.3.54 NetworkType2Code

Definition: Type of proxy.

Type: CodeSet

CodeName	Name	Definition
SCK5	Sock5	Sock5 proxy.
SCK4	Sock4	Sock4 proxy.
HTTP	HTTP	HTTP proxy.

9.2.3.55 NonFinancialRequestType1Code

Definition: Type of non financial request that could be processed between an Acceptor and an Intermediary Agent or an Acquirer.

Type: CodeSet

CodeName	Name	Definition
ACQR	AcquirerSelection	According to several parameters of a transaction, an Intermediary Agent helps an Acceptor to identify the more relevant Acquirer to process the transaction.
PARQ	ParRequest	The Intermediary Agent or Acquirer provides the PaymentAccountReference to use to process the transaction.
RISK	RiskManagement	The Intermediary Agent or Acquirer helps the Acceptor to assess the risk management of the transaction.
TOKN	TokenRequest	The Intermediary Agent or Acquirer provides the token to use to process the transaction.

9.2.3.56 OnLineCapability1Code

Definition: On-line and off-line capabilities of the POI (Point Of Interaction).

Type: CodeSet

CodeName	Name	Definition
OFLN	OffLine	Off-line only capable.
ONLN	OnLine	On-line only capable.
SMON	SemiOffLine	Off-line capable with possible on-line requests to the acquirer.

9.2.3.57 OutputFormat1Code

Definition: Message format.

Type: CodeSet

CodeName	Name	Definition
MREF	MessageReference	Predefined configured messages, identified by a reference.
TEXT	SimpleText	Text without format attributes.
HTML	XHTML	XHTML document which includes a subset of the XHTML output tag.

9.2.3.58 OutputFormat3Code

Definition: Type of output format.

Type: CodeSet

CodeName	Name	Definition
BARC	Barcode	Barcode to output in several possible format.
MENT	MenuEntry	A text to display as a menu before requesting an input.
MREF	MessageReference	Predefined configured messages, identified by a reference.

CodeName	Name	Definition
SREF	ScreenReference	Screen to display identified by a reference.
TEXT	SimpleText	Text without format attributes.
HTML	XHTML	XHTML document which includes a subset of the XHTML output tag.

9.2.3.59 PartyType15Code

Definition: Party involved by the data set.

Type: CodeSet

CodeName	Name	Definition
PGRP	POIGroup	Configuration to apply to a subset of the whole POI system.
PSYS	POISystem	Configuration to apply to the whole POI system.
PSNG	SinglePOI	Configuration to apply to a single POI terminal.

9.2.3.60 PartyType33Code

Definition: Identification of the type of entity involved in a transaction.

Type: CodeSet

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TAXH	TaxAuthority	Tax authority.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

9.2.3.61 PartyType3Code

Definition: Identification of the type of entity involved in a transaction.

Type: CodeSet

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
DLIS	DelegateIssuer	Party to whom the card issuer delegates to authorise card payment transactions.

9.2.3.62 PartyType4Code

Definition: Entity assigning an identification (for example merchant, acceptor, acquirer, tax authority, etc.).

Type: CodeSet

CodeName	Name	Definition
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
ACQR	Acquirer	Entity acquiring card transactions.
CISS	CardIssuer	Party that issues cards.
TAXH	TaxAuthority	Tax authority.

9.2.3.63 PartyType5Code

Definition: Identification of the type of entity involved in a maintenance operation.

Type: CodeSet

CodeName	Name	Definition
OPOI	OriginatingPOI	Point Of Interaction initiating the card payment transaction.
ACCP	Acceptor	Card acceptor, party accepting the card and presenting transaction data to the acquirer.

CodeName	Name	Definition
MERC	Merchant	Merchant providing goods and service in the card payment transaction.
ACQR	Acquirer	Entity acquiring card transactions.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
MTMG	MasterTerminalManager	Responsible for the maintenance of a card payment acceptance terminal.
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.

9.2.3.64 PartyType7Code

Definition: Party that communicate with a POI component (Point of Interaction), using a communication device.

Type: CodeSet

CodeName	Name	Definition
ACQR	Acquirer	Entity acquiring card transactions.
ITAG	IntermediaryAgent	Party acting on behalf of other parties to process or forward data to other parties.
PCPT	POIComponent	Party component of a POI system or POI terminal (Point of Interaction).
TMGT	TerminalManager	Responsible for one or several maintenance functions of a card payment acceptance terminal.
SALE	SaleSystem	Party selling goods and services.

9.2.3.65 PINFormat3Code

Definition: PIN (Personal Identification Number) format used before encryption.

Type: CodeSet

CodeName	Name	Definition
ISO0	ISO0	PIN diversified with the card account number, conforming to the standard ISO 9564-2.
ISO1	ISO1	PIN completed with random padding characters, conforming to the standard ISO 9564-2.
ISO2	ISO2	PIN without diversification characters, conforming to the standard ISO 9564-2.
ISO3	ISO3	PIN diversified with the card account number and random characters, conforming to the standard ISO 9564-2.
ISO4	ISO4	PIN format used with AES encryption, conforming to the new ISO SC2 format.

CodeName	Name	Definition
ISO5	ISO5	Alternative PIN format used with AES encryption, conforming to the new ISO SC2 format.

9.2.3.66 PINRequestType1Code

Definition: Type of PIN Service.

Type: CodeSet

CodeName	Name	Definition
PIAE	PINAcquisitionEncryption	The cardholder enters the PIN, the POI enciphers the PIN Block and provides it as a result to the Sale System.
PIAV	PINAcquisitionVerification	The Cardholder enters the PIN and the POI verifies it.
PIVO	PINVerifyOnly	The Sale System send a previous keyed PIN and the POI verifies it.

9.2.3.67 POICommunicationType2Code

Definition: Low level communication of the hardware or software component toward another component or an external entity.

Type: CodeSet

CodeName	Name	Definition
BLTH	Bluetooth	Communication with a host using Bluetooth.
ETHR	Ethernet	Ethernet port to communicate.
GPRS	GPRS	Communication with a host using GPRS.
GSMF	GSM	Communication with a host using GSM.
PSTN	PSTN	Communication with a host using Public Switching Telephone Network.
RS23	RS232	Serial port to communicate.
USBD	USBDevice	Communication with a USB stick or any USB device.
USBH	USBHost	Communication with a host from an USB port.
WIFI	Wifi	Wifi communication with another component.
WT2G	WirelessTechnology2G	Includes all communication technologies which can be qualified as being part of the 2G technology (e.g EDGE or PDC).
WT3G	WirelessTechnology3G	Includes all communication technologies which can be qualified as being part of the 3G technology.
WT4G	WirelessTechnology4G	Includes all communication technologies which can be qualified as being part of the 4G technology.

CodeName	Name	Definition
WT5G	WirelessTechnology5G	Includes all communication technologies which can be qualified as being part of the 5G technology.

9.2.3.68 POIComponentAssessment1Code

Definition: Type of assessment of a POI component (Point of Interaction).

Type: CodeSet

CodeName	Name	Definition
APPL	Approval	Approval number delivered by an approval centre.
CERT	Certification	Certification number delivered by a certification body.
EVAL	Evaluation	Evaluation by a lab or a tool.

9.2.3.69 POIComponentStatus1Code

Definition: Status of a component belonging to a POI Terminal (Point of Interaction).

Type: CodeSet

CodeName	Name	Definition
WAIT	WaitingActivation	Component not yet activated.
OUTD	OutOfOrder	Component not working properly.
OPER	InOperation	Component activated and in operation.
DACT	Deactivated	Component has been deactivated.

9.2.3.70 POIComponentType6Code

Definition: Type of component belonging to a POI (Point of Interaction) Terminal.

Type: CodeSet

CodeName	Name	Definition
AQPP	AcquirerProtocolParameters	Parameters for acquirer interface of the point of interaction, including acquirer host configuration parameters.
APPR	ApplicationParameters	Parameters of a payment application running on the point of interaction.
TLPR	TerminalParameters	Manufacturer configuration parameters of the point of interaction.
SCPR	SecurityParameters	Security parameters of the point of interaction.
SERV	Server	Payment server of a point of interaction system.
TERM	Terminal	Payment terminal point of interaction.
DVCE	Device	Device sub-component of a component of the point of interaction.

CodeName	Name	Definition
SECM	SecureModule	Security module.
APLI	PaymentApplication	Payment application software.
EMVK	EMVKernel	EMV application kernel (EMV is the chip card specifications initially defined by Eurocard, Mastercard and Visa).
EMVO	EMVLevel1	EMV physical interface (EMV is the chip card specifications initially defined by Eurocard, Mastercard and Visa).
MDWR	Middleware	Software module of the point of interaction.
DRVR	Driver	Driver module of the point of interaction.
OPST	OperatingSystem	Software that manages hardware to provide common services to the applications.
MRPR	MerchantParameters	Merchant configuration parameters for the point of interaction (POI).
CRTF	CertificateParameters	Certificate provided by a terminal manager.
TMSP	TMSProtocolParameters	Configuration parameters for the TMS protocol.
SACP	SaleComponent	Component of the Sale system.
SAPR	SaleToPOIProtocolParameters	Parameters related to the Sale to POI protocol.
LOGF	LogFile	Any repository used for recording log traces.
MDFL	MediaFile	Media file managed by an application of the POI.
SOFT	Soft	Payment or other software application.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

9.2.3.71 ProcessingPosition2Code

Definition: Specifies the processing position.

Type: CodeSet

CodeName	Name	Definition
AFTE	After	Specifies that the transaction/instruction is to be executed after the linked transaction/instruction.
WITH	With	Specifies that the transaction/instruction is to be executed with the linked transaction/instruction.
BEFO	Before	Specifies that the transaction/instruction is to be executed before the linked transaction/instruction.

CodeName	Name	Definition
INFO	Information	Specifies that the transactions/ instructions are linked for information purposes only.

9.2.3.72 QRCodeEncodingMode1Code

Definition: Encoding Mode of Quick Response Code.

Type: CodeSet

CodeName	Name	Definition
ALFA	Alphanumeric	Alphanumeric value provided in Barcode field.
BINA	Binary	Binary value provided in Quick Response Code Binary Value.
KANJ	Kanji	Kanji value provided in Quick Response Code Binary Value.
NUME	Numeric	Numeric value provided in Barcode field.

9.2.3.73 QRCodeErrorCorrection1Code

Definition: Error Correction mode of Quick Response Code.

Type: CodeSet

CodeName	Name	Definition
M015	ErrorCorrection15Percent	Reed-Solomon error correction 15%
Q025	ErrorCorrection25Percent	Reed-Solomon error correction 25%
H030	ErrorCorrection30Percent	Reed-Solomon error correction 30%
L007	ErrorCorrection7Percent	Reed-Solomon error correction 7%

9.2.3.74 ReconciliationCriteria1Code

Definition: Available criterion to group transactions when a reconliation is made.

Type: CodeSet

CodeName	Name	Definition
BRND	CardBrand	The set is defined by transactions made with cards belonging to the same brand.
PROF	CardProductProfile	The set is defined by transactions made with cards sharing the same CardProductProfile.
GRUP	PoiGroup	The set is defined by transactions processed by POIs identified with the same POIGroup.

9.2.3.75 ResourceAction1Code

Definition: Type of action to perform on a media resource.

Type: CodeSet

CodeName	Name	Definition
PAUS	Pause	Pause the media resource in progress as specified in the message.
STAS	Play	Start the media resource as specified in the message.
LOOP	PlayInLoop	Play in a loop the media resource as specified in the message.
RESU	Resume	Resume the progress of the media resource as specified in the message.
DVOL	SetDefaultVolume	Set the default volume of sounds.
STOS	Stop	Stop the media resource in progress.

9.2.3.76 ResourceType1Code

Definition: Type of resource.

Type: CodeSet

CodeName	Name	Definition
TEXT	TextToSpeech	Voice synthesis.
URLI	UniformResourceIdentifier	String of characters that unambiguously identifies a particular resource.

9.2.3.77 Response11Code

Definition: Result of the processing of the message

Type: CodeSet

CodeName	Name	Definition
WARN	Warning	An additional Response Code, mainly a functional one, should be considered to identify the outcome of the request.
FAIL	Failure	Processing of the request fails for various reasons. Some further processing according to the type of requested service, the context of the process, and some additional precision about the failure notified in the ErrorCondition data element.
SUCC	Success	Processing OK. Information related to the result of the processing is contained in other parts of the response message.

9.2.3.78 Response2Code

Definition: Response to a request of service.

Type: CodeSet

CodeName	Name	Definition
APPR	Approved	Service has been successfuly provided.
DECL	Declined	Service is declined.

9.2.3.79 ResponseMode2Code

Definition: Message response awaited by the initiator of the Request.

Type: CodeSet

CodeName	Name	Definition
SEND	EndOfPlay	The Response is required at the end of play.
IMMD	Immediate	The Message Response is immediate, after taking into account the request.
NREQ	NotRequired	The Message Response is not required, except in case of error.
PEND	PrintEnd	The Print Response is required at the end of print.

9.2.3.80 ResultDetail3Code

Definition: Detail of the response.

Type: CodeSet

CodeName	Name	Definition
CRTU	UnknownCertificate	The certificate is unknown.
SVSU	UnsupportedService	Requested service not supported.

9.2.3.81 RetailerResultDetail1Code

Definition: Result of the processing of the message

Type: CodeSet

CodeName	Name	Definition
ABRT	Aborted	The Initiator of the request has sent an Abort message request, which was accepted and processed.
BUSY	Busy	The system is busy, try later.
CANC	Cancel	The user has aborted the transaction on the PED keyboard, for instance during PIN entering.
DEVO	DeviceOut	Device out of order.
WPIN	WrongPIN	The user has entered the PIN on the PED keyboard and the verification fails.
NHOS	UnreachableHost	Acquirer or any host is unreachable or has not answered to an online request, so is considered as temporary unavailable. Depending on the Sale context, the request could be repeated (to be compared with "Refusal").
UNVS	UnavailableService	The service is not available (not implemented, not configured, protocol version too old...).

CodeName	Name	Definition
UNVD	UnavailableDevice	The hardware is not available (absent, not configured...).
REFU	Refusal	The transaction is refused by the host or by the local rules associated to the card or the POI.
PAYR	PaymentRestriction	Some sale items are not payable by the card proposed by the Customer.
TNFD	NotFound	The transaction is not found (e.g. for a reversal or a repeat).
NALW	NotAllowed	A service request is sent during a Service dialogue. A combination of services not possible to provide. During the DeviceInitialisationCardReader message processing, the user has entered a card which has to be protected by the POI, and cannot be processed with this device request from the external, and then the Sale System.
LOUT	LoggedOut	Not logged in.
IVCA	InvalidCard	The card entered by the Customer cannot be processed by the POI because this card is not configured in the system.
ICAR	InsertedCard	If the Input Device request a NotifyCardInputFlag and the Customer enters a card in the card reader without answers to the Input command, the POI abort the Input command processing, and answer a dedicated ErrorCondition value in the Input response message.
WIPG	InProgress	The transaction is still in progress and then the command cannot be processed.

9.2.3.82 RetailerService8Code

Definition: List of specific services for DeviceRequest.

Type: CodeSet

CodeName	Name	Definition
DDYQ	DeviceDisplayRequest	One System requests the other to display a message for cashier or customer.
DINQ	DeviceInputRequest	One system requests to the other System to get data input.
DPRQ	DevicePrintRequest	One system requests to the other System to print data.
DSOQ	DevicePlaySoundRequest	One system requests to the Other System to play a sound.
DSIQ	DeviceSecureInputRequest	One system requests to the Other System to securely get data input (e.g. for PIN).

CodeName	Name	Definition
DCIQ	DeviceInitialisationCardReaderRequest	Service to send parameters to use when card reader initializes a new communication with the card.
DCAQ	DeviceSendApplicationProtocolDataUnitCardReaderRequest	A service to send commands to a card.
DCPQ	DevicePowerOffCardReaderRequest	The Sale system requests to the POI System to power off the card reader.
DCOQ	DeviceTransmissionMessageRequest	The Sale system requests to the POI System to transmit a message (for instance to a mobile server).
DINO	DeviceInputNotification	One system sends a notification to the POI System to update a input request.

9.2.3.83 RetailerService9Code

Definition: List of specific services for DeviceResponse.

Type: CodeSet

CodeName	Name	Definition
DDYP	DeviceDisplayResponse	One system responds to the other system for a display request.
DINP	DeviceInputResponse	One system responds to the other System for a input request.
DPRP	DevicePrintResponse	One system responds to the other System for a print request.
DSOP	DevicePlaySoundResponse	One system responds to the other System for a play sound request.
DSIP	DeviceSecureInputResponse	One system responds to the other System for secure data input.
DCIP	DeviceInitialisationCardReaderResponse	The POI system responds to the Sale System for a card reader initialisation.
DCAP	DeviceSendApplicationProtocolDataUnitCardReaderResponse	The POI system responds to the Sale System for a card reader Application Protocol Data Unit sending.
DCPP	DevicePowerOffCardRequestResponse	The POI system responds to the Sale System for a card reader power off.
DCOP	DeviceTransmissionMessageResponse	The POI system responds to the Sale System after a message transmission.

9.2.3.84 SaleCapabilities1Code

Definition: Hardware capabilities of the Sale Terminal.

Type: CodeSet

CodeName	Name	Definition
CHDI	CashierDisplay	Standard Cashier display interface (to ask question, or to show information).

CodeName	Name	Definition
CHER	CashierError	To display to the Cashier information related to an error situation occurring on the POI.
CHIN	CashierInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element). The output device attached to this input device is the CashierDisplay device.
CHST	CashierStatus	To display to the Cashier a new state on which the POI is entering. For instance, during a payment, the POI could display to the Cashier that POI request an authorisation to the host acquirer.
CUDI	CustomerDisplay	Standard Customer display interface used by the POI System to ask question, or to show information to the Customer inside a Service dialogue.
CUAS	CustomerAssistance	Input of the Cardholder POI interface which can be entered by the Cashier to assist the Customer.
CUER	CustomerError	To display to the Customer information is related to an error situation occurring on the Sale Terminal during a Sale transaction.
CUIN	CustomerInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element).
POIR	POIReplication	Information displayed on the Cardholder POI interface, replicated on the Cashier interface.
PRDC	PrinterDocument	When the POI System wants to print specific document (check, dynamic currency conversion ...).
PRRP	PrinterReceipt	Printer for the Payment receipt.
PRVC	PrinterVoucher	Coupons, voucher or special ticket generated by the POI and to be printed.

9.2.3.85 SaleCapabilities2Code

Definition: Type of the Logical device located on a Sale Terminal or a POI Terminal, in term of class of information to output (display, print or store), or input (keyboard) for the Cashier

or the Customer.

Type: CodeSet

CodeName	Name	Definition
CHIN	CashierInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element).

CodeName	Name	Definition
		The output device attached to this input device is the CashierDisplay device.
CUIN	CustomerInput	Any kind of keyboard allowing all or part of the commands of the Input message request from the Sale System to the POI System (InputCommand data element).

9.2.3.86 SaleTokenScope1Code

Definition: Scope of the token that identifies the payment mean of the customer.

Type: CodeSet

CodeName	Name	Definition
MULT	MultipleUse	The token is generated to recognise a customer for a longer period.
SNGL	SingleUse	The token is generated to recognise a customer during the lifetime of a transaction.

9.2.3.87 SoundFormat1Code

Definition: Type of sound to play.

Type: CodeSet

CodeName	Name	Definition
MSGR	MessageRef	Reference of a preloaded text to play.
SNDR	SoundRef	Preloaded sound File.
TEXT	Text	Text to play.

9.2.3.88 StoredValueAccountType1Code

Definition: Type of stored value account.

Type: CodeSet

CodeName	Name	Definition
BNKA	BankPrepaidAccount	Prepaid account managed by a financial institution for low income customers.
CWVC	CarwashVoucher	Car wash specific account.
CPYA	CompanyPrepaidAccount	Specific prepaid account for companies or professionals expenses.
ELMY	ElectronicMoneyAccount	Account supporting e-money issued by an electronic money issuer.
GIFT	GiftCard	Payment mean issued by retailers or banks as a substitute to a non-monetary gift. Usually, this Stored Value item is used only once.
GCER	GiftCertificate	Certificate to be given to a customer. Usually one shot voucher.

CodeName	Name	Definition
MLVC	MealVoucher	Meal and check voucher for restaurants.
OLVC	OnlineVoucher	Voucher that can be used online once or in several times.
MERC	MerchantAccount	Prepaid account open with a merchant or big retailers.
OTHR	OtherPrepaidAccount	Other non listed stored value instrument.
PHON	PhoneCard	Stored value instrument used to pay telephone services (e.g. card or identifier).
CARD	SmartCardTag	Stored value account hold on the chip of a smart card.
TRVL	Travel	Travel prepaid account.

9.2.3.89 SupportedPaymentOption2Code

Definition: Specifies the options supported for a payment transaction.

Type: CodeSet

CodeName	Name	Definition
PART	PartialApproval	The entity supports a partial approval of the payment transaction.
MSRV	PaymentApprovalOnly	The entity supports the approval of the payment service along with the decline of additional requested services (as cash-back).
INSI	IssuerInstalment	The sender support IssuerInstalment proposals to the Cardholder.
PINQ	PINRequest	The sender is able to support Single Tap transaction.

9.2.3.90 TerminalManagementAction3Code

Definition: Type of action to perform.

Type: CodeSet

CodeName	Name	Definition
CREA	Create	Request to create or add the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.

9.2.3.91 TerminalManagementAction5Code

Definition: Types of terminal management action to be performed by a point of interaction.

Type: CodeSet

CodeName	Name	Definition
DCTV	Deactivate	Request to deactivate the element identified inside the message exchange.
DELT	Delete	Request to delete the element identified inside the message exchange.
DWNL	Download	Request to download the element identified inside the message exchange.
INST	Install	Request to install the element identified inside the message exchange.
RSTR	Restart	Request to restart the element identified inside the message exchange.
UPLD	Upload	Request to upload the element identified inside the message exchange.
UPDT	Update	Request to update the element identified inside the message exchange.
BIND	Bind	Request sent to a POI to bind with a server.
RBND	Rebind	Request sent to a POI to rebind with a server.
UBND	Unbind	Request sent to a POI to unbind with a server.
ACTV	Activate	Request to activate the element identified inside the message exchange.
DEVR	DeviceRequest	Request to execute a device request.

9.2.3.92 TerminalManagementActionResult5Code

Definition: Final result of the processed terminal management action.

Type: CodeSet

CodeName	Name	Definition
ACCD	AccessDenied	Access is denied while performing the action.
CNTE	ConnectionError	Problem to connect while performing the action.
FMTE	FormatError	Data transferred has a wrong format.
INVC	InvalidContent	Content of the data is invalid.
LENE	LengthError	Data transferred has a wrong length.
OVER	MemoryOverflow	Memory to store the date exceeded.
MISS	MissingFile	Data set to be maintained is missing.
NSUP	NotSupported	Action is not supported.
SIGE	SignatureError	Data transferred has a wrong digital signature.
WARN	SuccessWithWarning	Action was performed but some warnings arose.

CodeName	Name	Definition
SYNE	SyntaxError	Data transferred has a wrong syntax.
TIMO	Timeout	Timeout expired during the data transfer.
UKDT	UnknownData	Data set identification invalid.
UKRF	UnknownKeyReference	Cryptographic key reference used for the data signature is not valid.
INDP	InvalidDelegationProof	Delegation Proof transmitted by the delegated TMS is not the one expected.
IDMP	InvalidDelegationInManagementPlan	One action of the AcceptorManagementPlan refers to an update unauthorized by the delegation.
DPRU	DelegationParametersReceivedUnauthorized	The content analysis of the AcceptorConfigurationUpdate reveals unexpected parameters.
AERR	AnyError	This code value means all TerminalManagementActionResultCode except "Any Error" and "Unlisted Error".
CMER	CommunicationError	Error in communication once the connection has been established.
ULER	UnlistedError	Any error that is not defined by a code value inside the TerminalManagementActionResultCode.
SUCC	Success	Action was successfully performed.

9.2.3.93 TerminalManagementActionTrigger1Code

Definition: Event to start a terminal management action by the point of interaction (POI).

Type: CodeSet

CodeName	Name	Definition
DATE	DateTime	Date and time trigger the terminal management action.
HOST	HostEvent	Acquirer triggers the terminal management action.
MANU	Manual	Acceptor triggers the terminal management action.
SALE	SaleEvent	Sale system triggers the terminal management action.

9.2.3.94 TerminalManagementAdditionalProcess1Code

Definition: Additional process to perform before starting or after a terminal management action by the point of interaction (POI).

Type: CodeSet

CodeName	Name	Definition
MANC	ManualConfirmation	Manual confirmation of the merchant before the terminal management action.

CodeName	Name	Definition
RCNC	Reconciliation	Acquirer reconciliation to be performed before the terminal management action.
RSRT	RestartSystem	Restart the system after performing the terminal management action.

9.2.3.95 TerminalManagementErrorAction2Code

Definition: Action to perform in case of error during the maintenance action in progress.

Type: CodeSet

CodeName	Name	Definition
SDSR	SendStatusReport	Send a status report immediately.
STOP	StopSequence	Stop the current sequence of terminal management actions without any action, and do not notice the error with a status report.

9.2.3.96 TimeUnit1Code

Definition: Unit of time associated with the contract.

Type: CodeSet

CodeName	Name	Definition
DAYC	CalendarDay	Time unit is calendar day.
HOUR	Hour	Time unit is hour.
MINU	Minute	Time unit is minute.
MNTH	Month	Time unit is month.
SECO	Second	Time unit is second.
WEEK	Week	Time unit is week.
YEAR	Year	Time unit is year.

9.2.3.97 TrackFormat1Code

Definition: Use to identify format of a track on a card or other documents like checks.

Type: CodeSet

CodeName	Name	Definition
AAMV	AAMVAFormat	American driver license.
CMC7	CMC7CheckFormat	Magnetic Ink Character Recognition, using the CMC-7 font - ISO 1004 Line at the bottom of a check containing the bank account and the check number.
E13B	E13BCheckFormat	Magnetic Ink Character Recognition, using the E-13B font) Line at the bottom of a check containing the bank account and the check number.

CodeName	Name	Definition
ISOF	ISOFormat	ISO card track format - ISO 7813 - ISO 4909.
JIS1	JISIFormat	Japanese track format I.
JIS2	JISIIFormat	Japanese track format II.

9.2.3.98 TransactionChannel5Code

Definition: Identifies the type of the communication channels used by the cardholder to the acceptor system.

Type: CodeSet

CodeName	Name	Definition
MAIL	MailOrder	Mail order.
TLPH	TelephoneOrder	Telephone order.
ECOM	ElectronicCommerce	Electronic commerce.
TVPY	TelevisionPayment	Payment on television.
SECM	SecuredElectronicCommerce	Electronic commerce with cardholder authentication.
MOBL	MobilePayment	Payment performed through a cardholder mobile device.
MPOS	MobilePOS	Payment performed through a merchant mobile device.

9.2.3.99 TransactionEnvironment1Code

Definition: Indicates the environment of the transaction.

Type: CodeSet

CodeName	Name	Definition
MERC	Merchant	Merchant environment.
PRIV	Private	Private environment.
PUBL	Public	Public environment.

9.2.3.100 TypeOfAmount8Code

Definition: Qualifies the amount associated with the transaction.

Type: CodeSet

CodeName	Name	Definition
ACTL	Actual	Actual amount.
ESTM	Estimated	Estimated amount (the final amount could be above or below).
MAXI	Maximum	Maximum amount (the final amount must be less or equal).
DFLT	Default	Default amount.

CodeName	Name	Definition
RPLT	Replacement	Replacement amount.
INCR	Incremental	Incremental amount for reservation.
DECR	Decremental	Decremental amount for reservation.
RESD	Reserved	Reserved or updated reserved amount for reservation.

9.2.3.101 UserInterface4Code

Definition: Destination of the message.

Type: CodeSet

CodeName	Name	Definition
CDSP	CardholderDisplay	Cardholder display or interface.
CRCP	CardholderReceipt	Cardholder receipt.
MDSP	MerchantDisplay	Merchant display or interface.
MRCP	MerchantReceipt	Merchant receipt.
CRDO	OtherCardholderInterface	Other interface of the cardholder, for instance e-mail or smartphone message.

9.2.3.102 Verification1Code

Definition: Result of the verification.

Type: CodeSet

CodeName	Name	Definition
FAIL	Failed	Verification failed.
MISS	Missing	Information required to perform the verification was missing.
NOVF	NotPerformed	Verification has not been performed.
PART	PartialMatch	Verification was partially successful.
SUCC	Successful	Verification was successful.
ERRR	TechnicalError	Device or entity to perform the verification was unavailable.

9.2.4 Date

9.2.4.1 ISODate

Definition: A particular point in the progression of time in a calendar year expressed in the YYYY-MM-DD format. This representation is defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" which is aligned with ISO 8601.

Type: Date

9.2.5 DateTime

9.2.5.1 ISODateTime

Definition: A particular point in the progression of time defined by a mandatory date and a mandatory time component, expressed in either UTC time format (YYYY-MM-DDThh:mm:ss.sssZ), local time with UTC offset format (YYYY-MM-DDThh:mm:ss.sss+/-hh:mm), or local time format (YYYY-MM-DDThh:mm:ss.sss). These representations are defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" which is aligned with ISO 8601.

Note on the time format:

1) beginning / end of calendar day

00:00:00 = the beginning of a calendar day

24:00:00 = the end of a calendar day

2) fractions of second in time format

Decimal fractions of seconds may be included. In this case, the involved parties shall agree on the maximum number of digits that are allowed.

Type: DateTime

9.2.6 IdentifierSet

9.2.6.1 AnyBICDec2014Identifier

Definition: Code allocated to a financial or non-financial institution by the ISO 9362 Registration Authority, as described in ISO 9362: 2014 - "Banking - Banking telecommunication messages - Business identifier code (BIC)".

Type: IdentifierSet

Identification scheme: SWIFT; AnyBICIdentifier

Format

pattern	[A-Z0-9]{4,4}[A-Z]{2,2}[A-Z0-9]{2,2}([A-Z0-9]{3,3}){0,1}

Constraints

- **AnyBIC**

  Only a valid Business identifier code is allowed. Business identifier codes for financial or non-financial institutions are registered and published by the ISO 9362 Registration Authority in the ISO directory of BICs, and consists of eight (8) or eleven (11) contiguous characters.

9.2.6.2 BBANIdentifier

Definition: Basic Bank Account Number (BBAN). Identifier used nationally by financial institutions, ie, in individual countries, generally as part of a National Account Numbering Scheme(s), which uniquely identifies the account of a customer.

Type: IdentifierSet

Identification scheme: National Banking Association; Basic Bank Account Number

Format

pattern	[a-zA-Z0-9]{1,30}

9.2.6.3 IBAN2007Identifier

Definition: The International Bank Account Number is a code used internationally by financial institutions to uniquely identify the account of a customer at a financial institution as described in the 2007 edition of the ISO 13616 standard "Banking and related financial services - International Bank Account Number (IBAN)" and replaced by the more recent edition of the standard.

Type: IdentifierSet

Identification scheme: National Banking Association; International Bank Account Number (ISO 13616)

Format

pattern	[A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}

Constraints

- **IBAN**

  A valid IBAN consists of all three of the following components: Country Code, check digits and BBAN.

9.2.6.4 UPICIdentifier

Definition: Universal Payment Identification Code (UPIC). Identifier used by the New York Clearing House to mask confidential data, such as bank accounts and bank routing numbers. UPIC numbers remain with business customers, regardless of banking relationship changes.

Type: IdentifierSet

Identification scheme: The Clearing House (formerly The New York Clearing House); Universal Payment Identification Code

Format

pattern	[0-9]{8,17}

9.2.7 Indicator

9.2.7.1 TrueFalseIndicator

Definition: A flag indicating a True or False value.

Type: Indicator

Meaning When True: True

Meaning When False: False

9.2.8 Quantity

9.2.8.1 DecimalNumber

Definition: Number of objects represented as a decimal number, for example 0.75 or 45.6.

Type: Quantity

Format

totalDigits	18
fractionDigits	17

9.2.8.2 Number

Definition: Number of objects represented as an integer.

Type: Quantity

Format

totalDigits	18
fractionDigits	0

9.2.8.3 PositiveNumber

Definition: Number of objects represented as a positive integer.

Type: Quantity

Format

minInclusive	1
totalDigits	18
fractionDigits	0

9.2.9 Rate

9.2.9.1 PercentageRate

Definition: Rate expressed as a percentage, that is, in hundredths, for example, 0.7 is 7/10 of a percent, and 7.0 is 7%.

Type: Rate

Format

totalDigits	11
fractionDigits	10
baseValue	100.0

9.2.10 Text

9.2.10.1 Exact3AlphaNumericText

Definition: Specifies an alphanumeric string with a length of exact 3 characters.

Type: Text

Format

pattern	[a-zA-Z0-9]{3}

9.2.10.2 Exact3NumericText

Definition: Specifies a numeric string with an exact length of 3 digits.

Type: Text

Format

pattern	[0-9]{3}

9.2.10.3 Exact4NumericText

Definition: Specifies a numeric string with an exact length of 4 digits.

Type: Text

Format

pattern	[0-9]{4}

9.2.10.4 Max1025Text

Definition: Specifies a character string with a maximum length of 1025 characters.

Type: Text

Format

minLength	1
maxLength	1025

9.2.10.5 Max104Text

Definition: Specifies a character string with a maximum length of 104 characters.

Type: Text

Format

minLength	1
maxLength	104

9.2.10.6 Max10Text

Definition: Specifies a character string with a maximum length of 10 characters.

Type: Text

Format

minLength	1
maxLength	10

9.2.10.7 Max11NumericText

Definition: Specifies a numeric string with a maximum length of 11 digits.

Type: Text

Format

pattern	[0-9]{1,11}

9.2.10.8 Max140Text

Definition: Specifies a character string with a maximum length of 140 characters.

Type: Text

Format

minLength	1
maxLength	140

9.2.10.9 Max15NumericText

Definition: Specifies a numeric string with a maximum length of 15 digits.

Type: Text

Format

pattern	[0-9]{1,15}

9.2.10.10 Max16Text

Definition: Specifies a character string with a maximum length of 16 characters.

Type: Text

Format

minLength	1
maxLength	16

9.2.10.11 Max19NumericText

Definition: Specifies a numeric string with a maximum length of 19 digits.

Type: Text

Format

pattern	[0-9]{1,19}

9.2.10.12 Max20000Text

Definition: Specifies a character string with a maximum length of 20, 000 characters.

Type: Text

Format

minLength	1
maxLength	20000

9.2.10.13 Max256Text

Definition: Specifies a character string with a maximum length of 256 characters.

Type: Text

Format

minLength	1
maxLength	256

9.2.10.14 Max2NumericText

Definition: Specifies a numeric string with a maximum length of 2 digits.

Type: Text

Format

pattern	[0-9]{1,2}

9.2.10.15 Max30Text

Definition: Specifies a character string with a maximum length of 30 characters.

Type: Text

Format

maxLength	30

9.2.10.16 Max350Text

Definition: Specifies a character string with a maximum length of 350 characters.

Type: Text

Format

minLength	1
maxLength	350

9.2.10.17 Max35NumericText

Definition: Specifies a numeric string with a maximum length of 35 digits.

Type: Text

Format

pattern	[0-9]{1,35}

9.2.10.18 Max35Text

Definition: Specifies a character string with a maximum length of 35 characters.

Type: Text

Format

minLength	1
maxLength	35

9.2.10.19 Max37Text

Definition: Specifies a character string with a maximum length of 37 characters.

Type: Text

Format

minLength	1
maxLength	37

9.2.10.20 Max3Text

Definition: Specifies a character string with a maximum length of 3 characters.

Type: Text

Format

minLength	1
maxLength	3

9.2.10.21 Max45Text

Definition: Specifies a character string with a maximum length of 45 characters.

Type: Text

Format

minLength	1
maxLength	45

9.2.10.22 Max500Text

Definition: Specifies a character string with a maximum length of 500 characters.

Type: Text

Format

minLength	1
maxLength	500

9.2.10.23 Max5NumericText

Definition: Specifies a numeric string with a maximum length of 5 digits.

Type: Text

Format

pattern	[0-9]{1,5}

9.2.10.24 Max6Text

Definition: Specifies a character string with a maximum length of 6 characters.

Type: Text

Format

minLength	1
maxLength	6

9.2.10.25 Max70Text

Definition: Specifies a character string with a maximum length of 70characters.

Type: Text

Format

minLength	1
maxLength	70

9.2.10.26 Max76Text

Definition: Specifies a character string with a maximum length of 76 characters.

Type: Text

Format

minLength	1
maxLength	76

9.2.10.27 Max8000Text

Definition: Specifies a character string with a maximum length of 8000 characters.

Type: Text

Format

minLength	1
maxLength	8000

9.2.10.28 Max8Text

Definition: Specifies a character string with a maximum length of 8 characters.

Type: Text

Format

minLength	1
maxLength	8

9.2.10.29 Max9NumericText

Definition: Specifies a numeric string with a maximum length of 9 digits.

Type: Text

Format

pattern	[0-9]{1,9}

9.2.10.30 Min2Max3AlphaText

Definition: Specifies an alpha string with a minimum length of 2 characters and a maximum length of 3 characters.

Type: Text

Format

pattern	[a-zA-Z]{2,3}

9.2.10.31 Min2Max3NumericText

Definition: Specifies a numeric string with a minimum length of 2 digits, and a maximum length of 3 digits.

Type: Text

Format

pattern	[0-9]{2,3}

9.2.10.32 Min3Max4Text

Definition: Specifies a character string with a minimum length of 3 characters, and a maximum length of 4 characters.

Type: Text

Format

minLength	3
maxLength	4

9.2.10.33 Min8Max28NumericText

Definition: Specifies a numeric string with a minimum length of 8 digits, and a maximum length of 28 digits.

Type: Text

Format

pattern	[0-9]{8,28}

9.2.10.34 PhoneNumber

Definition: The collection of information which identifies a specific phone or FAX number as defined by telecom services.

It consists of a "+" followed by the country code (from 1 to 3 characters) then a "-" and finally, any combination of numbers, "(", ")", "+" and "-" (up to 30 characters).

Type: Text

Format

pattern	\+[0-9]{1,3}-[0-9()+\-]{1,30}

9.2.11 Time

9.2.11.1 ISOTime

Definition: A particular point in the progression of time in a calendar day expressed in either UTC time format (hh:mm:ss.sssZ), local time with UTC offset format (hh:mm:ss.sss+/-hh:mm), or local time format (hh:mm:ss.sss). These representations are defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" which is aligned with ISO 8601.

Note on the time format:

1) beginning / end of calendar day

00:00:00 = the beginning of a calendar day

24:00:00 = the end of a calendar day

2) fractions of second in time format

Decimal fractions of seconds may be included. In this case, the involved parties shall agree on the maximum number of digits that are allowed.

Type: Time