

ISO 20022

Card Payments Exchanges - Terminal Management - ISO - Latest version

Message Definition Report - Part 2

Approved by the Cards and Related Retail Financial Services SEG
on 4 February 2020

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

27 February 2020

Table of Contents

1	Message Set Overview	4
1.1	List of MessageDefinitions	4
2	catm.001.001.09 StatusReportV09	5
2.1	MessageDefinition Functionality	5
2.2	Structure	6
2.3	Constraints	7
2.4	Message Building Blocks	7
3	catm.002.001.08 ManagementPlanReplacementV08	22
3.1	MessageDefinition Functionality	22
3.2	Structure	23
3.3	Message Building Blocks	24
4	catm.003.001.09 AcceptorConfigurationUpdateV09	44
4.1	MessageDefinition Functionality	44
4.2	Structure	45
4.3	Message Building Blocks	46
5	catm.004.001.05 TerminalManagementRejectionV05	61
5.1	MessageDefinition Functionality	61
5.2	Structure	61
5.3	Message Building Blocks	61
6	catm.005.001.06 MaintenanceDelegationRequestV06	66
6.1	MessageDefinition Functionality	66
6.2	Structure	67
6.3	Message Building Blocks	68
7	catm.006.001.04 MaintenanceDelegationResponseV04	91
7.1	MessageDefinition Functionality	91
7.2	Structure	92
7.3	Message Building Blocks	92
8	catm.007.001.03 CertificateManagementRequestV03	100
8.1	MessageDefinition Functionality	100
8.2	Structure	101
8.3	Message Building Blocks	102
9	catm.008.001.03 CertificateManagementResponseV03	113
9.1	MessageDefinition Functionality	113
9.2	Structure	114
9.3	Message Building Blocks	114

10	Message Items Types	121
10.1	MessageComponents	121
10.2	Message Datatypes	265

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
catm.001.001.09 StatusReportV09	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.
catm.002.001.08 ManagementPlanReplacementV08	The ManagementPlanReplacement message is sent by a terminal manager to a POI to set maintenance actions to be performed.
catm.003.001.09 AcceptorConfigurationUpdateV09	The AcceptorConfigurationUpdate message is sent by a TM to a POI to update configurations.
catm.004.001.05 TerminalManagementRejectionV05	The TerminalManagementRejection message is sent by the terminal manager to reject a message request sent by an acceptor, to indicate that the received message could not be processed.
catm.005.001.06 MaintenanceDelegationRequestV06	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.
catm.006.001.04 MaintenanceDelegationResponseV04	The MaintenanceDelegationResponse message is sent by the master terminal manager to a terminal manager to provide the outcome of a maintenance delegation request.
catm.007.001.03 CertificateManagementRequestV03	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.
catm.008.001.03 CertificateManagementResponseV03	The CertificateManagementResponse is sent by a terminal manager in response to a CertificateManagementRequest to provide the outcome of the requested service.

2 catm.001.001.09 StatusReportV09

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 StatusReportV09 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]			7
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		7
	FormatVersion <FrmtVrsn>	[1..1]	Text		8
	ExchangeIdentification <XchgId>	[1..1]	Quantity		8
	CreationDateTime <CreDtTm>	[1..1]	DateTime		8
	InitiatingParty <InitgPty>	[1..1]	±		8
	RecipientParty <RcptPty>	[0..1]	±		8
	Traceability <Tracblt>	[0..*]	±		9
	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]	±		13
	SequenceCounter <SeqCntr>	[0..1]	Text		14
	Content <Cntt>	[1..1]			14
	POICapabilities <POICpblties>	[0..1]	±		14
	POIComponent <POICmpnt>	[0..*]	±		15
	AttendanceContext <AtndncCntxt>	[0..1]	CodeSet		17
	POIDateTime <POIDtTm>	[1..1]	DateTime		18
	DataSetRequired <DataSetReqrd>	[0..*]			18
	Identification <Id>	[1..1]	±		18
	POIChallenge <POIChllng>	[0..1]	Binary		18
	TMChallenge <TMChllng>	[0..1]	Binary		18
	SessionKey <SsnKey>	[0..1]	±		19

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	DelegationProof <DlgnProof>	[0..1]	Binary		19
	ProtectedDelegationProof <PrctdDlgnProof>	[0..1]	±		19
	Event <Evt>	[0..*]	±		20
	Errors <Errs>	[0..*]	Text		20
	SecurityTrailer <SctyTrlr>	[0..1]	±		20

2.3 Constraints

C1 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		8
	ExchangeIdentification <XchgId>	[1..1]	Quantity		8
	CreationDateTime <CreDtTm>	[1..1]	DateTime		8
	InitiatingParty <InitgPty>	[1..1]	±		8
	RecipientParty <RcptPty>	[0..1]	±		8
	Traceability <Tracblt>	[0..*]	±		9

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 295):

- *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 297

2.4.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 295

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 294

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwr>	[1..1]	Text		174

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 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

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 **StatusReport9** 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]	±		13
	SequenceCounter <SeqCntr>	[0..1]	Text		14
	Content <Cntt>	[1..1]			14
	POICapabilities <POICpblties>	[0..1]	±		14
	POIComponent <POICmpnt>	[0..*]	±		15
	AttendanceContext <AttdncCntxt>	[0..1]	CodeSet		17
	POIDateTime <POIDtTm>	[1..1]	DateTime		18
	DataSetRequired <DataSetReqrd>	[0..*]			18
	Identification <Id>	[1..1]	±		18
	POIChallenge <POIChllng>	[0..1]	Binary		18
	TMChallenge <TMChllng>	[0..1]	Binary		18
	SessionKey <SsnKey>	[0..1]	±		19
	DelegationProof <DlgtNProof>	[0..1]	Binary		19
	ProtectedDelegationProof <PrtctdDlgtNProof>	[0..1]	±		19
	Event <Evt>	[0..*]	±		20
	Errors <Errs>	[0..*]	Text		20

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 287

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 296

2.4.2.2.3 TriggerType <TrggrTp>

Presence: [1..1]

Definition: Identification of the type of the call.

Datatype: "ExchangePolicy2Code" on page 282

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 297

2.4.2.3 TerminalManagerIdentification <TermnIMgrId>

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 **StatusReportDataSetRequest1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	±		13
	SequenceCounter <SeqCntr>	[0..1]	Text		14
	Content <Cntt>	[1..1]			14
	POICapabilities <POICpbilities>	[0..1]	±		14
	POIComponent <POICmpnt>	[0..*]	±		15
	AttendanceContext <AttndhcCntxt>	[0..1]	CodeSet		17
	POIDateTime <POIDtTm>	[1..1]	DateTime		18
	DataSetRequired <DataSetReqrd>	[0..*]			18
	Identification <Id>	[1..1]	±		18
	POIChallenge <POIChllng>	[0..1]	Binary		18
	TMChallenge <TMChllng>	[0..1]	Binary		18
	SessionKey <SsnKey>	[0..1]	±		19
	DelegationProof <DlgtProof>	[0..1]	Binary		19
	ProtectedDelegationProof <PrtctdDlgtProof>	[0..1]	±		19
	Event <Evt>	[0..*]	±		20
	Errors <Errs>	[0..*]	Text		20

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 "DataSetIdentification8" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

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 297

2.4.2.4.3 Content <Cntt>

Presence: [1..1]

Definition: Content of the status report.

Content <Cntt> contains the following **StatusReportContent9** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	POICapabilities <POICpblties>	[0..1]	±		14
	POIComponent <POICmpnt>	[0..*]	±		15
	AttendanceContext <AttdncCntxt>	[0..1]	CodeSet		17
	POIDateTime <POIDtTm>	[1..1]	DateTime		18
	DataSetRequired <DataSetReqrd>	[0..*]			18
	Identification <Id>	[1..1]	±		18
	POIChallenge <POIChllng>	[0..1]	Binary		18
	TMChallenge <TMChllng>	[0..1]	Binary		18
	SessionKey <SsnKey>	[0..1]	±		19
	DelegationProof <DlgtProof>	[0..1]	Binary		19
	ProtectedDelegationProof <PrctcdDlgtProof>	[0..1]	±		19
	Event <Evt>	[0..*]	±		20
	Errors <Errs>	[0..*]	Text		20

2.4.2.4.3.1 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 190 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	CardReadingCapabilities <CardRdngCpblties>	[0..*]	CodeSet		190
	CardholderVerificationCapabilities <CrdhldrVrfctnCpblties>	[0..*]	CodeSet		191
	PINLengthCapabilities <PINLnghCpblties>	[0..1]	Quantity		191
	ApprovalCodeLength <ApprvlCdLngh>	[0..1]	Quantity		192
	MaxScriptLength <MxScrptLngh>	[0..1]	Quantity		192
	CardCaptureCapable <CardCaptrCpbl>	[0..1]	Indicator		192
	OnLineCapabilities <OnLineCpblties>	[0..1]	CodeSet		192
	MessageCapabilities <MsgCpblties>	[0..*]			192
	Destination <Dstn>	[1..*]	CodeSet		193
	AvailableFormat <AvlblFrmt>	[0..*]	CodeSet		193
	NumberOfLines <NbOfLines>	[0..1]	Quantity		193
	LineWidth <LineWidth>	[0..1]	Quantity		193
	AvailableLanguage <AvlblLang>	[0..*]	CodeSet	C1	194

2.4.2.4.3.2 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 "PointOfInteractionComponent10" on page 194 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Type <Tp>	[1..1]	CodeSet		196
	SubTypeInfoInformation <SubTpInf>	[0..1]	Text		197
	Identification <Id>	[1..1]			198
	ItemNumber <ItmNb>	[0..1]	Text		198
	ProviderIdentification <PrvdrlId>	[0..1]	Text		198
	Identification <Id>	[0..1]	Text		198
	SerialNumber <SrlNb>	[0..1]	Text		198
	Status <Sts>	[0..1]			198
	VersionNumber <VrsnNb>	[0..1]	Text		199
	Status <Sts>	[0..1]	CodeSet		199
	ExpiryDate <XpryDt>	[0..1]	Date		199
	StandardCompliance <StdCmplc>	[0..*]			199
	Identification <Id>	[1..1]	Text		199
	Version <Vrsn>	[1..1]	Text		200
	Issuer <Issr>	[1..1]	Text		200
	Characteristics <Chrtcs>	[0..1]			200
	Memory <Mmry>	[0..*]			201
	Identification <Id>	[1..1]	Text		202
	TotalSize <TtlSz>	[1..1]	Quantity		202
	FreeSize <FreeSz>	[1..1]	Quantity		202
	Unit <Unit>	[1..1]	CodeSet		202
	Communication <Com>	[0..*]			202
	CommunicationType <ComTp>	[1..1]	CodeSet		203
	RemoteParty <RmotPty>	[1..*]	CodeSet		204
	Active <Actv>	[1..1]	Indicator		204
	Parameters <Params>	[0..1]	±		204
	PhysicalInterface <PhysIntrfc>	[0..1]			205
	InterfaceName <IntrfcNm>	[1..1]	Text		205
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		205
	UserName <UsrNm>	[0..1]	Text		206

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	AccessCode <AccsCd>	[0..1]	Binary		206
	SecurityProfile <SctyPrfl>	[0..1]	Text		206
	AdditionalParameters <AddtlParams>	[0..1]	Binary		206
	SecurityAccessModules <SctyAccsMdl>	[0..1]	Quantity		207
	SubscriberIdentityModules <SbcbrldntyMdl>	[0..1]	Quantity		207
	SecurityElement <SctyElmt>	[0..*]	±		207
	Assessment <Assmnt>	[0..*]			207
	Type <Tp>	[1..1]	CodeSet		208
	Assigner <Assgnr>	[1..*]	Text		208
	DeliveryDate <DlrvyDt>	[0..1]	DateTime		208
	ExpirationDate <XprtnDt>	[0..1]	DateTime		208
	Number <Nb>	[1..1]	Text		208
	Package <Packg>	[0..*]			209
	PackageIdentification <PackgId>	[0..1]	±		209
	PackageLength <PackgLngh>	[0..1]	Quantity		209
	OffsetStart <OffsetStart>	[0..1]	Quantity		209
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		210
	PackageBlock <PackgBlck>	[0..*]			210
	Identification <Id>	[1..1]	Text		210
	Value <Val>	[0..1]	Binary		210
	ProtectedValue <PrctcdVal>	[0..1]	±		210
	Type <Tp>	[0..1]	Text		211

2.4.2.4.3.3 AttendanceContext <AttndncCntxt>

Presence: [0..1]

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

Datatype: "AttendanceContext1Code" on page 274

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.

2.4.2.4.3.4 POIDateTime <POIDtTm>

Presence: [1..1]

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

Datatype: "ISODateTime" on page 294

2.4.2.4.3.5 DataSetRequired <DataSetReqrd>

Presence: [0..*]

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

DataSetRequired <DataSetReqrd> contains the following **DataSetRequest1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	±		18
	POIChallenge <POIChllng>	[0..1]	Binary		18
	TMChallenge <TMChllng>	[0..1]	Binary		18
	SessionKey <SsnKey>	[0..1]	±		19
	DelegationProof <DlgtProof>	[0..1]	Binary		19
	ProtectedDelegationProof <PrctcdDlgtProof>	[0..1]	±		19

2.4.2.4.3.5.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the required data set.

Identification <Id> contains the following elements (see "DataSetIdentification8" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

2.4.2.4.3.5.2 POIChallenge <POIChllng>

Presence: [0..1]

Definition: Point of interaction challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 266

2.4.2.4.3.5.3 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 266

2.4.2.4.3.5.4 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 "[CryptographicKey14](#)" on page 221 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		221
	AdditionalIdentification <AddtlId>	[0..1]	Binary		222
	Name <Nm>	[0..1]	Text		222
	SecurityProfile <SctyPrfl>	[0..1]	Text		222
	ItemNumber <ItmNb>	[0..1]	Text		222
	Version <Vrsn>	[1..1]	Text		222
	Type <Tp>	[0..1]	CodeSet		222
	Function <Fctn>	[0..*]	CodeSet		223
	ActivationDate <ActvtnDt>	[0..1]	DateTime		224
	DeactivationDate <DeactvtnDt>	[0..1]	DateTime		224
	KeyValue <KeyVal>	[0..1]	±		224
	KeyCheckValue <KeyChckVal>	[0..1]	Binary		224
	AdditionalManagementInformation <AddtlMgmtInf>	[0..*]			224
	Name <Nm>	[1..1]	Text		225
	Value <Val>	[0..1]	Text		225

2.4.2.4.3.5.5 DelegationProof <DlgnProof>

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 266

2.4.2.4.3.5.6 ProtectedDelegationProof <PrctcdDlgnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtNProof> contains the following elements (see "ContentInformationType23" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

2.4.2.4.3.6 Event <Evt>

Presence: [0..*]

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

Event <Evt> contains the following elements (see "TMSEvent7" on page 214 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TimeStamp <TmStmp>	[1..1]	DateTime		214
	Result <Rslt>	[1..1]	CodeSet		214
	ActionIdentification <ActnId>	[1..1]			215
	ActionType <ActnTp>	[1..1]	CodeSet		215
	DataSetIdentification <DataSetId>	[0..1]	±		216
	AdditionalErrorInformation <AddtlErrInf>	[0..1]	Text		216
	TerminalManagerIdentification <TermnlMgrld>	[0..1]	Text		216

2.4.2.4.3.7 Errors <Errs>

Presence: [0..*]

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

Datatype: "Max140Text" on page 296

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 "[ContentInformationType21](#)" on page 244 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

3 catm.002.001.08 ManagementPlanReplacementV08

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 ManagementPlanReplacementV08 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]			24
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		25
	FormatVersion <FrmtVrsn>	[1..1]	Text		25
	ExchangeIdentification <XchgId>	[1..1]	Quantity		25
	CreationDateTime <CreDtTm>	[1..1]	DateTime		25
	InitiatingParty <InitgPty>	[1..1]	±		25
	RecipientParty <RcptPty>	[0..1]	±		26
	Traceability <Tracblt>	[0..*]	±		26
	ManagementPlan <MgmtPlan>	[1..1]			27
	POIdentification <POId>	[0..1]	±		29
	TerminalManagerIdentification <TermnlMgrld>	[1..1]	±		29
	DataSet <DataSet>	[1..1]			29
	Identification <Id>	[1..1]	±		31
	SequenceCounter <SeqCntr>	[0..1]	Text		31
	Content <Cnnt>	[0..1]			31
	TMChallenge <TMChllng>	[0..1]	Binary		33
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		33
	Action <Actn>	[1..*]			33
	Type <Tp>	[1..1]	CodeSet		34
	RemoteAccess <RmotAccs>	[0..1]	±		35
	Key <Key>	[0..*]			36
	KeyIdentification <KeyId>	[1..1]	Text		36
	KeyVersion <KeyVrsn>	[1..1]	Text		36
	SequenceNumber <SeqNb>	[0..1]	Quantity		36
	DerivationIdentification <DerivtnId>	[0..1]	Binary		36
	Type <Tp>	[0..1]	CodeSet		36
	Function <Fctn>	[0..*]	CodeSet		37
	TerminalManagerIdentification <TermnlMgrld>	[0..1]	±		38
	TMSProtocol <TMSPrtcol>	[0..1]	Text		38

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		38
	DataSetIdentification <DataSetId>	[0..1]	±		38
	ComponentType <CmpntTp>	[0..*]	CodeSet		39
	DelegationScopelIdentification <DlgtScpld>	[0..1]	Text		40
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		40
	DelegationProof <DlgtProof>	[0..1]	Binary		40
	ProtectedDelegationProof <PrtctdDlgtProof>	[0..1]	±		40
	Trigger <Trggr>	[1..1]	CodeSet		41
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		41
	ReTry <ReTry>	[0..1]	±		41
	TimeCondition <TmCond>	[0..1]	±		42
	TMChallenge <TMChllng>	[0..1]	Binary		42
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		42
	ErrorAction <ErrActn>	[0..*]	±		42
	AdditionalInformation <AddtlInf>	[0..*]	Binary		42
	MessageItem <Msgltn>	[0..*]	±		43
	SecurityTrailer <SctyTrlr>	[0..1]	±		43

3.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

3.3.1 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		25
	FormatVersion <FrmtVrsn>	[1..1]	Text		25
	ExchangeIdentification <XchgId>	[1..1]	Quantity		25
	CreationDateTime <CreDtTm>	[1..1]	DateTime		25
	InitiatingParty <InitgPty>	[1..1]	±		25
	RecipientParty <RcptPty>	[0..1]	±		26
	Traceability <Tracblt>	[0..*]	±		26

3.3.1.1 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 295](#)):

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

3.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: ["Max6Text" on page 297](#)

3.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: ["Number" on page 295](#)

3.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

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

Datatype: ["ISODateTime" on page 294](#)

3.3.1.5 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

3.3.1.6 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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

3.3.1.7 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 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

3.3.2 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 **ManagementPlan8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	POIIdentification <POIId>	[0..1]	±		29
	TerminalManagerIdentification <TermnlMgrld>	[1..1]	±		29
	DataSet <DataSet>	[1..1]			29
	Identification <Id>	[1..1]	±		31
	SequenceCounter <SeqCntr>	[0..1]	Text		31
	Content <Cntt>	[0..1]			31
	TMChallenge <TMChllng>	[0..1]	Binary		33
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		33
	Action <Actn>	[1..*]			33
	Type <Tp>	[1..1]	CodeSet		34
	RemoteAccess <RmotAccs>	[0..1]	±		35
	Key <Key>	[0..*]			36
	KeyIdIdentification <KeyId>	[1..1]	Text		36
	KeyVersion <KeyVrsn>	[1..1]	Text		36
	SequenceNumber <SeqNb>	[0..1]	Quantity		36
	DerivationIdentification <DerivtnId>	[0..1]	Binary		36
	Type <Tp>	[0..1]	CodeSet		36
	Function <Fctn>	[0..*]	CodeSet		37
	TerminalManagerIdentification <TermnlMgrld>	[0..1]	±		38
	TMSProtocol <TMSPrtcol>	[0..1]	Text		38
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		38
	DataSetIdentification <DataSetId>	[0..1]	±		38
	ComponentType <CmpntTp>	[0..*]	CodeSet		39
	DelegationScopeIdentification <DlgtnScpld>	[0..1]	Text		40
	DelegationScopeDefinition <DlgtnScpDef>	[0..1]	Binary		40
	DelegationProof <DlgtnProof>	[0..1]	Binary		40
	ProtectedDelegationProof <PrtctdDlgtnProof>	[0..1]	±		40
	Trigger <Trggr>	[1..1]	CodeSet		41
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		41
	ReTry <ReTry>	[0..1]	±		41
	TimeCondition <TmCond>	[0..1]	±		42

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TMChallenge <TMChllng>	[0..1]	Binary		42
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		42
	ErrorAction <ErrActn>	[0..*]	±		42
	AdditionalInformation <AddtlInf>	[0..*]	Binary		42
	MessageItem <Msgltn>	[0..*]	±		43

3.3.2.1 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

3.3.2.2 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

3.3.2.3 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 **TerminalManagementDataSet29** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	±		31
	SequenceCounter <SeqCntr>	[0..1]	Text		31
	Content <Cntt>	[0..1]			31
	TMChallenge <TMChllng>	[0..1]	Binary		33
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		33
	Action <Actn>	[1..*]			33
	Type <Tp>	[1..1]	CodeSet		34
	RemoteAccess <RmotAccs>	[0..1]	±		35
	Key <Key>	[0..*]			36
	KeyIdentification <KeyId>	[1..1]	Text		36
	KeyVersion <KeyVrsn>	[1..1]	Text		36
	SequenceNumber <SeqNb>	[0..1]	Quantity		36
	DerivationIdentification <DerivtnId>	[0..1]	Binary		36
	Type <Tp>	[0..1]	CodeSet		36
	Function <Fctn>	[0..*]	CodeSet		37
	TerminalManagerIdentification <TermnlMgrId>	[0..1]	±		38
	TMSProtocol <TMSPrtcol>	[0..1]	Text		38
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		38
	DataSetIdentification <DataSetId>	[0..1]	±		38
	ComponentType <CmpntTp>	[0..*]	CodeSet		39
	DelegationScopeIdentification <DlgtNScpld>	[0..1]	Text		40
	DelegationScopeDefinition <DlgtNScpDef>	[0..1]	Binary		40
	DelegationProof <DlgtNProof>	[0..1]	Binary		40
	ProtectedDelegationProof <PrctcdDlgtNProof>	[0..1]	±		40
	Trigger <Trggr>	[1..1]	CodeSet		41
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		41
	ReTry <ReTry>	[0..1]	±		41
	TimeCondition <TmCond>	[0..1]	±		42
	TMChallenge <TMChllng>	[0..1]	Binary		42
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		42
	ErrorAction <ErrActn>	[0..*]	±		42

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	AdditionalInformation <AddtlInf>	[0..*]	Binary		42
	MessageItem <Msgltn>	[0..*]	±		43

3.3.2.3.1 Identification <Id>

Presence: [1..1]

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

Identification <Id> contains the following elements (see "[DataSetIdentification8](#)" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

3.3.2.3.2 SequenceCounter <SeqCntr>

Presence: [0..1]

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

Datatype: "[Max9NumericText](#)" on page 297

3.3.2.3.3 Content <Cntt>

Presence: [0..1]

Definition: Content of the management plan.

Content <Cntt> contains the following **ManagementPlanContent8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TMChallenge <TMChllng>	[0..1]	Binary		33
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		33
	Action <Actn>	[1..*]			33
	Type <Tp>	[1..1]	CodeSet		34
	RemoteAccess <RmotAccs>	[0..1]	±		35
	Key <Key>	[0..*]			36
	KeyIdentification <KeyId>	[1..1]	Text		36
	KeyVersion <KeyVrsn>	[1..1]	Text		36
	SequenceNumber <SeqNb>	[0..1]	Quantity		36
	DerivationIdentification <DerivtnId>	[0..1]	Binary		36
	Type <Tp>	[0..1]	CodeSet		36
	Function <Fctn>	[0..*]	CodeSet		37
	TerminalManagerIdentification <TermnlMgrId>	[0..1]	±		38
	TMSProtocol <TMSPrtcol>	[0..1]	Text		38
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		38
	DataSetIdentification <DataSetId>	[0..1]	±		38
	ComponentType <CmpntTp>	[0..*]	CodeSet		39
	DelegationScopeIdentification <DlgtNScpld>	[0..1]	Text		40
	DelegationScopeDefinition <DlgtNScpDef>	[0..1]	Binary		40
	DelegationProof <DlgtNProof>	[0..1]	Binary		40
	ProtectedDelegationProof <PrtctdDlgtNProof>	[0..1]	±		40
	Trigger <Trggr>	[1..1]	CodeSet		41
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		41
	ReTry <ReTry>	[0..1]	±		41
	TimeCondition <TmCond>	[0..1]	±		42
	TMChallenge <TMChllng>	[0..1]	Binary		42
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		42
	ErrorAction <ErrActn>	[0..*]	±		42
	AdditionalInformation <AddtlInf>	[0..*]	Binary		42
	MessageItem <Msgltn>	[0..*]	±		43

3.3.2.3.3.1 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 266

3.3.2.3.3.2 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 265

3.3.2.3.3.3 Action <Actn>

Presence: [1..*]

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

Action <Actn> contains the following **TMSAction8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Type <Tp>	[1..1]	CodeSet		34
	RemoteAccess <RmotAccs>	[0..1]	±		35
	Key <Key>	[0..*]			36
	KeyIdentification <KeyId>	[1..1]	Text		36
	KeyVersion <KeyVrsn>	[1..1]	Text		36
	SequenceNumber <SeqNb>	[0..1]	Quantity		36
	DerivationIdentification <DerivtnId>	[0..1]	Binary		36
	Type <Tp>	[0..1]	CodeSet		36
	Function <Fctn>	[0..*]	CodeSet		37
	TerminalManagerIdentification <TermnlMgrld>	[0..1]	±		38
	TMSProtocol <TMSPrtcol>	[0..1]	Text		38
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		38
	DataSetIdentification <DataSetId>	[0..1]	±		38
	ComponentType <CmpntTp>	[0..*]	CodeSet		39
	DelegationScopeIdentification <DlgtScpld>	[0..1]	Text		40
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		40
	DelegationProof <DlgtProof>	[0..1]	Binary		40
	ProtectedDelegationProof <PrctcdDlgtProof>	[0..1]	±		40
	Trigger <Trgg>	[1..1]	CodeSet		41
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		41
	ReTry <ReTry>	[0..1]	±		41
	TimeCondition <TmCond>	[0..1]	±		42
	TMChallenge <TMChllng>	[0..1]	Binary		42
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		42
	ErrorAction <ErrActn>	[0..*]	±		42
	AdditionalInformation <AddtlInf>	[0..*]	Binary		42
	MessageItem <Msgltn>	[0..*]	±		43

3.3.2.3.3.1 Type <Tp>

Presence: [1..1]

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

Datatype: "TerminalManagementAction4Code" on page 291

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.

3.3.2.3.3.2 RemoteAccess <RmotAccs>

Presence: [0..1]

Definition: Host access information.

RemoteAccess <RmotAccs> contains the following elements (see "[NetworkParameters7](#)" on page 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

3.3.2.3.3.3.3 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		36
	KeyVersion <KeyVrsn>	[1..1]	Text		36
	SequenceNumber <SeqNb>	[0..1]	Quantity		36
	DerivationIdentification <DerivtnId>	[0..1]	Binary		36
	Type <Tp>	[0..1]	CodeSet		36
	Function <Fctn>	[0..*]	CodeSet		37

3.3.2.3.3.3.3.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 296

3.3.2.3.3.3.3.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 296

3.3.2.3.3.3.3.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 295

3.3.2.3.3.3.3.4 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 267

3.3.2.3.3.3.3.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 278

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).

3.3.2.3.3.3.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 283

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	TranslatelInput	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.

3.3.2.3.3.3.4 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

3.3.2.3.3.3.5 TMSProtocol <TMSPrtcol>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

3.3.2.3.3.3.6 TMSProtocolVersion <TMSPrtcolVrsn>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

3.3.2.3.3.3.7 DataSetIdentification <DataSetId>

Presence: [0..1]

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

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification8" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

3.3.2.3.3.3.8 ComponentType <CmpntTp>

Presence: [0..*]

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

Datatype: "DataSetCategory14Code" on page 280

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.
SOFT	SoftwareApplication	Software Application or module of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

3.3.2.3.3.3.9 DelegationScopelIdentification <DlgnScpld>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

3.3.2.3.3.3.10 DelegationScopeDefinition <DlgnScpDef>

Presence: [0..1]

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

Datatype: "Max3000Binary" on page 266

3.3.2.3.3.3.11 DelegationProof <DlgnProof>

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 266

3.3.2.3.3.3.12 ProtectedDelegationProof <PrctcdDlgnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtProof> contains the following elements (see "ContentInformationType23" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

3.3.2.3.3.13 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 293

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.

3.3.2.3.3.14 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 293

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.

3.3.2.3.3.15 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

3.3.2.3.3.16 TimeCondition <TmCond>

Presence: [0..1]

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

TimeCondition <TmCond> contains the following elements (see "ProcessTiming3" on page 264 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	WaitingTime <WtgTm>	[0..1]	Text		264
	StartTime <StartTm>	[0..1]	DateTime		264
	EndTime <EndTm>	[0..1]	DateTime		264
	Period <Prd>	[0..1]	Text		264
	MaximumNumber <MaxNb>	[0..1]	Quantity		264

3.3.2.3.3.17 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 266

3.3.2.3.3.18 KeyEnciphermentCertificate <KeyNcphrmntCert>

Presence: [0..*]

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

Datatype: "Max10KBinary" on page 265

3.3.2.3.3.19 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 "ErrorAction4" on page 216 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionResult <ActnRslt>	[1..*]	CodeSet		217
	ActionToProcess <ActnToPrc>	[1..1]	CodeSet		218

3.3.2.3.3.20 AdditionalInformation <AddtlInf>

Presence: [0..*]

Definition: Additional information about the maintenance action.

Datatype: "Max3000Binary" on page 266

3.3.2.3.3.21 MessageItem <Msgltn>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <Msgltn> contains the following elements (see "MessageItemCondition1" on page 174 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemIdentification <ItmId>	[1..1]	Text		174
	Condition <Cond>	[1..1]	CodeSet		175
	Value <Val>	[0..*]	Text		175

3.3.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

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

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType21" on page 244 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

4 catm.003.001.09 AcceptorConfigurationUpdateV09

4.1 MessageDefinition Functionality

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

Outline

The AcceptorConfigurationUpdateV09 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> <AccptrCfgrnUpd>	[1..1]			
	Header <Hdr>	[1..1]			46
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		46
	FormatVersion <FrmtVrsn>	[1..1]	Text		46
	ExchangeIdentification <XchgId>	[1..1]	Quantity		46
	CreationDateTime <CreDtTm>	[1..1]	DateTime		46
	InitiatingParty <InitgPty>	[1..1]	±		47
	RecipientParty <RcptPty>	[0..1]	±		47
	Traceability <Tracblt>	[0..*]	±		48
	AcceptorConfiguration <AccptrCfgrn>	[1..1]			48
	TerminalManagerIdentification <TermnlMgrId>	[1..1]	±		49
	DataSet <DataSet>	[1..*]			49
	Identification <Id>	[1..1]	±		50
	SequenceCounter <SeqCntr>	[0..1]	Text		50
	POIIdentification <POIID>	[0..*]	±		51
	ConfigurationScope <CfgrnScp>	[0..1]	CodeSet		51
	Content <Cntt>	[1..1]			51
	ReplaceConfiguration <RplcCfgrn>	[0..1]	Indicator		52
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		52
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		53
	MerchantParameters <MrchntParams>	[0..*]	±		56
	TerminalParameters <TermnlParams>	[0..*]	±		56
	ApplicationParameters <ApplParams>	[0..*]	±		57
	HostCommunicationParameters <HstComParams>	[0..*]	±		57
	SecurityParameters <SctyParams>	[0..*]	±		58
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		59
	TerminalPackage <TermnlPackg>	[0..*]	±		59
	SecurityTrailer <SctyTrlr>	[0..1]	±		60

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		46
	FormatVersion <FrmtVrsn>	[1..1]	Text		46
	ExchangeIdentification <XchgId>	[1..1]	Quantity		46
	CreationDateTime <CreDtTm>	[1..1]	DateTime		46
	InitiatingParty <InitgPty>	[1..1]	±		47
	RecipientParty <RcptPty>	[0..1]	±		47
	Traceability <Tracblt>	[0..*]	±		48

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 295):

- *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 297

4.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: ["Number"](#) on page 295

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 294

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

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 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

4.3.2 AcceptorConfiguration <AccptrCfgtn>

Presence: [1..1]

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

AcceptorConfiguration <AcptrCfgtn> contains the following **AcceptorConfiguration9** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TerminalManagerIdentification <TermnlMgrld>	[1..1]	±		49
	DataSet <DataSet>	[1..*]			49
	Identification <Id>	[1..1]	±		50
	SequenceCounter <SeqCntr>	[0..1]	Text		50
	POIIdentification <POIID>	[0..*]	±		51
	ConfigurationScope <CfgtnScp>	[0..1]	CodeSet		51
	Content <Cntt>	[1..1]			51
	ReplaceConfiguration <RplcCfgtn>	[0..1]	Indicator		52
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		52
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		53
	MerchantParameters <MrchntParams>	[0..*]	±		56
	TerminalParameters <TermnlParams>	[0..*]	±		56
	ApplicationParameters <ApplParams>	[0..*]	±		57
	HostCommunicationParameters <HstComParams>	[0..*]	±		57
	SecurityParameters <SctyParams>	[0..*]	±		58
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		59
	TerminalPackage <TermnlPackg>	[0..*]	±		59

4.3.2.1 TerminalManagerIdentification <TermnlMgrld>

Presence: [1..1]

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

TerminalManagerIdentification <TermnlMgrld> contains the following elements (see "GenericIdentification176" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

4.3.2.2 DataSet <DataSet>

Presence: [1..*]

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

DataSet <DataSet> contains the following **AcceptorConfigurationDataSet1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	±		50
	SequenceCounter <SeqCntr>	[0..1]	Text		50
	POIIdentification <POIID>	[0..*]	±		51
	ConfigurationScope <CfgtnScp>	[0..1]	CodeSet		51
	Content <Cntt>	[1..1]			51
	ReplaceConfiguration <RplcCfgtn>	[0..1]	Indicator		52
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		52
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		53
	MerchantParameters <MrchntParams>	[0..*]	±		56
	TerminalParameters <TermnlParams>	[0..*]	±		56
	ApplicationParameters <ApplParams>	[0..*]	±		57
	HostCommunicationParameters <HstComParams>	[0..*]	±		57
	SecurityParameters <SctyParams>	[0..*]	±		58
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		59
	TerminalPackage <TermnlPackg>	[0..*]	±		59

4.3.2.2.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the data set transferred.

Identification <Id> contains the following elements (see ["DataSetIdentification8"](#) on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

4.3.2.2.2 SequenceCounter <SeqCntr>

Presence: [0..1]

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

Datatype: ["Max9NumericText"](#) on page 297

4.3.2.2.3 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

4.3.2.2.4 ConfigurationScope <CfgtnScp>

Presence: [0..1]

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

Datatype: "PartyType15Code" on page 286

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.

4.3.2.2.5 Content <Cntt>

Presence: [1..1]

Definition: Content of the acceptor parameters.

Content <Cntt> contains the following **AcceptorConfigurationContent9** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ReplaceConfiguration <RplcCfgrn>	[0..1]	Indicator		52
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		52
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		53
	MerchantParameters <MrchntParams>	[0..*]	±		56
	TerminalParameters <TermnlParams>	[0..*]	±		56
	ApplicationParameters <ApplParams>	[0..*]	±		57
	HostCommunicationParameters <HstComParams>	[0..*]	±		57
	SecurityParameters <SctyParams>	[0..*]	±		58
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		59
	TerminalPackage <TermnlPackg>	[0..*]	±		59

4.3.2.2.5.1 ReplaceConfiguration <RplcCfgrn>

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 295):

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

4.3.2.2.5.2 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 "TMSProtocolParameters5" on page 121 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		122
	TerminalManagerIdentification <TermnlMgrld>	[1..1]	±		122
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		123
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		123
	Version <Vrsn>	[1..1]	Text		124
	ApplicationIdentification <ApplId>	[0..*]	Text		124
	HostIdentification <Hstld>	[1..1]	Text		124
	POIIdentification <POIId>	[0..1]	Text		124
	InitiatingPartyIdentification <InitgPtyld>	[0..1]	Text		124
	RecipientPartyIdentification <RcptPtyld>	[0..1]	Text		124
	FileTransfer <FileTrf>	[0..1]	Indicator		124
	MessageItem <Msgltn>	[0..*]	±		124

4.3.2.2.5.3 AcquirerProtocolParameters <AcqrrPrtcolParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to an acquirer protocol.

AcquirerProtocolParameters <AcqrrPrtcolParams> contains the following elements (see "AcquirerProtocolParameters13" on page 145 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		148
	AcquirerIdentification <Acqrrld>	[1..*]	±		148
	Version <Vrsn>	[1..1]	Text		149
	ApplicationIdentification <Applld>	[0..*]	Text		149
	Host <Hst>	[0..*]			149
	HostIdentification <Hstld>	[1..1]	Text		149
	MessageToSend <MsgToSnd>	[0..*]	CodeSet		149
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		150
	OnLineTransaction <OnLineTx>	[0..1]			150
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		151
	BatchTransfer <BtchTrf>	[0..1]			152
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		152
	MaximumNumber <MaxNb>	[0..1]	Quantity		153
	MaximumAmount <MaxAmt>	[0..1]	Amount		153
	ReTry <ReTry>	[0..1]	±		153
	TimeCondition <TmCond>	[0..1]			153
	StartTime <StartTm>	[0..1]	DateTime		153
	EndTime <EndTm>	[0..1]	DateTime		154
	Period <Prd>	[0..1]	Text		154
	CompletionExchange <CmpltnXchg>	[0..1]			154
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		154
	MaximumNumber <MaxNb>	[0..1]	Quantity		155
	MaximumAmount <MaxAmt>	[0..1]	Amount		155
	ReTry <ReTry>	[0..1]	±		155
	TimeCondition <TmCond>	[0..1]			155
	StartTime <StartTm>	[0..1]	DateTime		156
	EndTime <EndTm>	[0..1]	DateTime		156
	Period <Prd>	[0..1]	Text		156
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		156
	OffLineTransaction <OffLineTx>	[0..1]			156

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		157
	BatchTransfer <BtchTrf>	[0..1]			158
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		158
	MaximumNumber <MaxNb>	[0..1]	Quantity		159
	MaximumAmount <MaxAmt>	[0..1]	Amount		159
	ReTry <ReTry>	[0..1]	±		159
	TimeCondition <TmCond>	[0..1]			159
	StartTime <StartTm>	[0..1]	DateTime		159
	EndTime <EndTm>	[0..1]	DateTime		160
	Period <Prd>	[0..1]	Text		160
	CompletionExchange <CmpltnXchg>	[0..1]			160
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		160
	MaximumNumber <MaxNb>	[0..1]	Quantity		161
	MaximumAmount <MaxAmt>	[0..1]	Amount		161
	ReTry <ReTry>	[0..1]	±		161
	TimeCondition <TmCond>	[0..1]			161
	StartTime <StartTm>	[0..1]	DateTime		162
	EndTime <EndTm>	[0..1]	DateTime		162
	Period <Prd>	[0..1]	Text		162
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		162
	ReconciliationExchange <RcncltnXchg>	[0..1]			162
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		163
	MaximumNumber <MaxNb>	[0..1]	Quantity		164
	MaximumAmount <MaxAmt>	[0..1]	Amount		164
	ReTry <ReTry>	[0..1]	±		164
	TimeCondition <TmCond>	[0..1]			164
	StartTime <StartTm>	[0..1]	DateTime		164
	EndTime <EndTm>	[0..1]	DateTime		164
	Period <Prd>	[0..1]	Text		164
	ReconciliationByAcquirer <RcncltnByAcqrr>	[0..1]	Indicator		165
	TotalsPerCurrency <TtlsPerCcy>	[0..1]	Indicator		165

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	SplitTotals <SplTtIs>	[0..1]	Indicator		165
	ReconciliationError <RcncltnErr>	[0..1]	Indicator		165
	CardDataVerification <CardDataVrfctn>	[0..1]	Indicator		165
	NotifyOffLineCancellation <NtfyOffLineCxl>	[0..1]	Indicator		166
	BatchTransferContent <BtchTrfCntt>	[0..*]	CodeSet		166
	FileTransferBatch <FileTrfBtch>	[0..1]	Indicator		166
	BatchDigitalSignature <BtchDgtlSgntr>	[0..1]	Indicator		166
	MessageItem <Msgltn>	[0..*]	±		166
	ProtectCardData <PrctCardData>	[1..1]	Indicator		167
	PrivateCardData <PrvtCardData>	[0..1]	Indicator		167
	MandatorySecurityTrailer <MndtrySctyTrlr>	[0..1]	Indicator		167

4.3.2.2.5.4 MerchantParameters <MrchntParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to the merchant.

MerchantParameters <MrchntParams> contains the following elements (see "MerchantConfigurationParameters5" on page 143 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		143
	MerchantIdentification <MrchntId>	[0..1]	Text		144
	Version <Vrsn>	[0..1]	Text		144
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		144
	Proxy <Prxy>	[0..1]			144
	Type <Tp>	[1..1]	CodeSet		144
	Access <Accs>	[1..1]	±		145
	OtherParameters <OthrParams>	[0..1]	Binary		145

4.3.2.2.5.5 TerminalParameters <TermnlParams>

Presence: [0..*]

Definition: Manufacturer configuration parameters of the point of interaction.

TerminalParameters <TermnlParams> contains the following elements (see
"PaymentTerminalParameters7" on page 140 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		140
	VendorIdentification <Vndrld>	[0..1]	Text		141
	Version <Vrsn>	[0..1]	Text		141
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		141
	ClockSynchronisation <ClckSynctn>	[0..1]			141
	POITimeZone <POITmZone>	[1..1]	Text		141
	SynchronisationServer <SynctnSvr>	[0..*]	±		142
	Delay <Dely>	[0..1]	Time		142
	TimeZoneLine <TmZoneLine>	[0..*]	Text		142
	LocalDateTime <LclDtTm>	[0..*]			142
	FromDateTime <FrDtTm>	[0..1]	DateTime		143
	ToDateTime <ToDtTm>	[0..1]	DateTime		143
	UTCOffset <UTCOffset>	[1..1]	Quantity		143
	OtherParameters <OthrParams>	[0..1]	Binary		143

4.3.2.2.5.6 ApplicationParameters <ApplParams>

Presence: [0..*]

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

ApplicationParameters <ApplParams> contains the following elements (see
"ApplicationParameters9" on page 139 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		139
	ApplicationIdentification <Applld>	[1..1]	Text		139
	Version <Vrsn>	[0..1]	Text		139
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		139
	Parameters <Params>	[0..*]	Binary		140
	EncryptedParameters <NcrptdParams>	[0..1]	±		140

4.3.2.2.5.7 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 132 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		133
	HostIdentification <HstId>	[1..1]	Text		133
	Address <Adr>	[0..1]	±		134
	Key <Key>	[0..*]			134
	KeyIdentification <KeyId>	[1..1]	Text		134
	KeyVersion <KeyVrsn>	[1..1]	Text		134
	SequenceNumber <SeqNb>	[0..1]	Quantity		135
	DerivationIdentification <DerivtnId>	[0..1]	Binary		135
	Type <Tp>	[0..1]	CodeSet		135
	Function <Fctn>	[0..*]	CodeSet		135
	NetworkServiceProvider <NtwkSvcPrvdr>	[0..1]	±		136
	PhysicalInterface <PhysIntrfc>	[0..1]			137
	InterfaceName <IntrfcNm>	[1..1]	Text		137
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		137
	UserName <UsrNm>	[0..1]	Text		138
	AccessCode <AccsCd>	[0..1]	Binary		138
	SecurityProfile <SctyPrfl>	[0..1]	Text		138
	AdditionalParameters <AddtlParams>	[0..1]	Binary		138

4.3.2.2.5.8 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 "SecurityParameters12" on page 131 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		131
	Version <Vrsn>	[1..1]	Text		131
	POIChallenge <POIChllng>	[0..1]	Binary		132
	TMChallenge <TMChllng>	[0..1]	Binary		132
	SecurityElement <SctyElmt>	[0..*]	±		132

4.3.2.2.5.9 SaleToPOIParameters <SaleToPOIParams>

Presence: [0..*]

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

SaleToPOIParameters <SaleToPOIParams> contains the following elements (see "SaleToPOIProtocolParameter1" on page 129 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		129
	MerchantIdentification <MrchntId>	[0..1]			129
	CommonName <CmonNm>	[1..1]	Text		130
	Address <Adr>	[0..1]	Text		130
	CountryCode <CtryCd>	[1..1]	CodeSet		130
	MerchantCategoryCode <MrchntCtgyCd>	[1..1]	Text		130
	RegisteredIdentifier <RegIdr>	[1..1]	Text		130
	Version <Vrsn>	[1..1]	Text		130
	HostIdentification <HstId>	[1..1]	Text		131
	MerchantPOIIdentification <MrchntPOId>	[0..1]	Text		131
	SaleIdentification <SaleId>	[0..1]	Text		131

4.3.2.2.5.10 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 "TerminalPackageType1" on page 125 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	POIComponentIdentification <POICmpntId>	[0..*]			125
	ItemNumber <itmNb>	[0..1]	Text		126
	ProviderIdentification <PrvdrId>	[0..1]	Text		126
	Identification <Id>	[0..1]	Text		126
	SerialNumber <SrlNb>	[0..1]	Text		126
	Package <Packg>	[1..*]			126
	PackageIdentification <PackgId>	[0..1]	±		127
	PackageLength <PackgLngh>	[0..1]	Quantity		127
	OffsetStart <OffsetStart>	[0..1]	Quantity		127
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		127
	PackageBlock <PackgBlck>	[0..*]			128
	Identification <Id>	[1..1]	Text		128
	Value <Val>	[0..1]	Binary		128
	ProtectedValue <PrtctdVal>	[0..1]	±		128
	Type <Tp>	[0..1]	Text		129

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 "ContentInformationType21" on page 244 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

5 catm.004.001.05 TerminalManagementRejectionV05

5.1 MessageDefinition Functionality

The TerminalManagementRejection message is sent by the terminal manager to reject a message request sent by an acceptor, to indicate that the received message could not be processed.

Outline

The TerminalManagementRejectionV05 MessageDefinition is composed of 2 MessageBuildingBlocks:

- A. Header
Rejection message management information.
- B. Reject
Information related to the reject.

5.2 Structure

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	<i>Message root</i> <Document> <TermnlMgmtRjctn>	[1..1]			
	Header <Hdr>	[1..1]			62
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		62
	FormatVersion <FrmtVrsn>	[1..1]	Text		62
	ExchangeIdentification <XchgId>	[1..1]	Quantity		62
	CreationDateTime <CreDtTm>	[1..1]	DateTime		62
	InitiatingParty <InitgPty>	[1..1]	±		62
	RecipientParty <RcptPty>	[0..1]	±		63
	Traceability <Tracblt>	[0..*]	±		63
	Reject <Rjct>	[1..1]			64
	RejectReason <RjctRsn>	[1..1]	CodeSet		64
	AdditionalInformation <AddtlInf>	[0..1]	Text		65
	MessageInError <MsgInErr>	[0..1]	Binary		65

5.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

5.3.1 Header <Hdr>

Presence: [1..1]

Definition: Rejection message management information.

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

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		62
	FormatVersion <FrmtVrsn>	[1..1]	Text		62
	Exchangeldentification <Xchgld>	[1..1]	Quantity		62
	CreationDateTime <CreDtTm>	[1..1]	DateTime		62
	InitiatingParty <InitgPty>	[1..1]	±		62
	RecipientParty <RcptPty>	[0..1]	±		63
	Traceability <Tracblt>	[0..*]	±		63

5.3.1.1 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 295):

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

5.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: ["Max6Text"](#) on page 297

5.3.1.3 Exchangeldentification <Xchgld>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: ["Number"](#) on page 295

5.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

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

Datatype: ["ISODatetime"](#) on page 294

5.3.1.5 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

5.3.1.6 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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwr>	[1..1]	Text		174

5.3.1.7 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 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

5.3.2 Reject <Rjct>

Presence: [1..1]

Definition: Information related to the reject.

Reject <Rjct> contains the following **AcceptorRejection3** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RejectReason <RjctRsn>	[1..1]	CodeSet		64
	AdditionalInformation <AddtlInf>	[0..1]	Text		65
	MessageInError <MsgInErr>	[0..1]	Binary		65

5.3.2.1 RejectReason <RjctRsn>

Presence: [1..1]

Definition: Reject reason of the request or the advice.

Datatype: "RejectReason2Code" on page 290

CodeName	Name	Definition
UNPR	UnableToProcess	Not possible to process the message, for instance the security module is unavailable, the hardware is unavailable, or there is a problem of resource.
IMSG	InvalidMessage	Invalid envelope of the message.
PARS	ParsingError	Invalid message: At least one of the data element or data structure is not present, the format, or the content of one data element or one data structure is not correct.
SECU	Security	Security error (for example an invalid key or an incorrect MAC value).
INTP	InitiatingParty	Invalid identification data for the sender.
RCPD	RecipientParty	Invalid identification data for the the receiver.
VERS	ProtocolVersion	Version of the protocol couldn't be supported by the recipient.

CodeName	Name	Definition
MSGT	MessageType	Type of message the recipient receives is unknow or unsupported.

5.3.2.2 AdditionalInformation <AddtlInf>

Presence: [0..1]

Definition: Additional information related to the reject of the exchange.

Datatype: "Max500Text" on page 297

5.3.2.3 MessageInError <MsgInErr>

Presence: [0..1]

Definition: Original request that caused the recipient party to reject it.

Datatype: "Max100KBinary" on page 265

6 catm.005.001.06 MaintenanceDelegationRequestV06

6.1 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 MaintenanceDelegationRequestV06 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.

6.2 Structure

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	Message root <Document> <MntncDlgtReq>	[1..1]			
	Header <Hdr>	[0..1]			68
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		69
	FormatVersion <FrmtVrsn>	[1..1]	Text		69
	ExchangeIdentification <XchgId>	[1..1]	Quantity		69
	CreationDateTime <CreDtTm>	[1..1]	DateTime		69
	InitiatingParty <InitgPty>	[1..1]	±		69
	RecipientParty <RcptPty>	[0..1]	±		69
	Traceability <Tracblt>	[0..*]	±		70
	MaintenanceDelegationRequest <MntncDlgtReq>	[1..1]			70
	TMIdentification <TMId>	[1..1]	±		72
	MasterTMIdentification <MstrTMId>	[0..1]	±		72
	RequestedDelegation <ReqdDlgt>	[1..*]			72
	DelegationType <DlgtTp>	[1..1]	CodeSet		74
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		74
	PartialDelegation <PrtlDlgt>	[0..1]	Indicator		75
	POISubset <POISubset>	[0..*]	Text		75
	DelegatedAction <DlgtActn>	[0..1]	±		75
	DelegationScopeIdentification <DlgtScpld>	[0..1]	Text		77
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		77
	Certificate <Cert>	[0..*]	Binary		77
	POIIdentificationAssociation <POIIdAssoctn>	[0..*]	±		77
	SymmetricKey <SmmtrcKey>	[0..*]			77
	KeyIdentification <KeyId>	[1..1]	Text		78
	KeyVersion <KeyVrsn>	[1..1]	Text		78
	SequenceNumber <SeqNb>	[0..1]	Quantity		78
	DerivationIdentification <DerivtnId>	[0..1]	Binary		78
	Type <Tp>	[0..1]	CodeSet		78
	Function <Fctn>	[0..*]	CodeSet		79
	ParameterDataSet <ParamDataSet>	[0..1]			80

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	±		80
	SequenceCounter <SeqCntr>	[0..1]	Text		81
	POIIdentification <POIID>	[0..*]	±		81
	ConfigurationScope <CfgrnScp>	[0..1]	CodeSet		81
	Content <Cntt>	[1..1]			81
	ReplaceConfiguration <RplcCfgrn>	[0..1]	Indicator		82
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		82
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		83
	MerchantParameters <MrchntParams>	[0..*]	±		86
	TerminalParameters <TermnlParams>	[0..*]	±		86
	ApplicationParameters <ApplParams>	[0..*]	±		87
	HostCommunicationParameters <HstComParams>	[0..*]	±		87
	SecurityParameters <SctyParams>	[0..*]	±		88
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		89
	TerminalPackage <TermnlPackg>	[0..*]	±		89
	SecurityTrailer <SctyTrlr>	[1..1]	±		90

6.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

6.3.1 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		69
	FormatVersion <FrmtVrsn>	[1..1]	Text		69
	ExchangeIdentification <Xchgld>	[1..1]	Quantity		69
	CreationDateTime <CreDtTm>	[1..1]	DateTime		69
	InitiatingParty <InitgPty>	[1..1]	±		69
	RecipientParty <RcptPty>	[0..1]	±		69
	Traceability <Tracblt>	[0..*]	±		70

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 295](#)):

- *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 297](#)

6.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: ["Number" on page 295](#)

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 294](#)

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 167](#) for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwr>	[1..1]	Text		174

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 <Tracblt> contains the following elements (see "[Traceability8](#)" on page 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

6.3.2 MaintenanceDelegationRequest <MntncDlgtReq>

Presence: [1..1]

Definition: Information related to the request of maintenance delegations.

MaintenanceDelegationRequest <MntncDlgtReq> contains the following
MaintenanceDelegationRequest6 elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TMIdentification <TMId>	[1..1]	±		72
	MasterTMIdentification <MstrTMId>	[0..1]	±		72
	RequestedDelegation <ReqdDlgt>	[1..*]			72
	DelegationType <DlgtTp>	[1..1]	CodeSet		74
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		74
	PartialDelegation <PrtlDlgt>	[0..1]	Indicator		75
	POISubset <POISubset>	[0..*]	Text		75
	DelegatedAction <DlgtActn>	[0..1]	±		75
	DelegationScopeIdentification <DlgtScpld>	[0..1]	Text		77
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		77
	Certificate <Cert>	[0..*]	Binary		77
	POIIdentificationAssociation <POIIdAssoctn>	[0..*]	±		77
	SymmetricKey <SmmtrcKey>	[0..*]			77
	KeyIdentification <KeyId>	[1..1]	Text		78
	KeyVersion <KeyVrsn>	[1..1]	Text		78
	SequenceNumber <SeqNb>	[0..1]	Quantity		78
	DerivationIdentification <DerivtnId>	[0..1]	Binary		78
	Type <Tp>	[0..1]	CodeSet		78
	Function <Fctn>	[0..*]	CodeSet		79
	ParameterDataSet <ParamDataSet>	[0..1]			80
	Identification <Id>	[1..1]	±		80
	SequenceCounter <SeqCntr>	[0..1]	Text		81
	POIIdentification <POIId>	[0..*]	±		81
	ConfigurationScope <CfgtnScp>	[0..1]	CodeSet		81
	Content <Cntt>	[1..1]			81
	ReplaceConfiguration <RplcCfgtn>	[0..1]	Indicator		82
	TMSProtocolParameters <TMSPrtolParams>	[0..*]	±		82
	AcquirerProtocolParameters <AcqrrPrtolParams>	[0..*]	±		83
	MerchantParameters <MrchntParams>	[0..*]	±		86
	TerminalParameters <TermnlParams>	[0..*]	±		86

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ApplicationParameters <ApplParams>	[0..*]	±		87
	HostCommunicationParameters <HstComParams>	[0..*]	±		87
	SecurityParameters <SctyParams>	[0..*]	±		88
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		89
	TerminalPackage <TermnlPackg>	[0..*]	±		89

6.3.2.1 TMIdentification <TMId>

Presence: [1..1]

Definition: Terminal manager identification.

TMIdentification <TMId> contains the following elements (see "[GenericIdentification176](#)" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

6.3.2.2 MasterTMIdentification <MstrTMId>

Presence: [0..1]

Definition: Master terminal manager identification.

MasterTMIdentification <MstrTMId> contains the following elements (see "[GenericIdentification176](#)" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

6.3.2.3 RequestedDelegation <ReqdDlgn>

Presence: [1..*]

Definition: Information on the delegation of a maintenance action.

RequestedDelegation <ReqdDlgn> contains the following **MaintenanceDelegation10** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	DelegationType <DlgnTp>	[1..1]	CodeSet		74
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		74
	PartialDelegation <PrtlDlgn>	[0..1]	Indicator		75
	POISubset <POISubset>	[0..*]	Text		75
	DelegatedAction <DlgtActn>	[0..1]	±		75
	DelegationScopeIdentification <DlgnScpld>	[0..1]	Text		77
	DelegationScopeDefinition <DlgnScpDef>	[0..1]	Binary		77
	Certificate <Cert>	[0..*]	Binary		77
	POIIdentificationAssociation <POIIdAssocn>	[0..*]	±		77
	SymmetricKey <SmmtrcKey>	[0..*]			77
	KeyIdentification <KeyId>	[1..1]	Text		78
	KeyVersion <KeyVrsn>	[1..1]	Text		78
	SequenceNumber <SeqNb>	[0..1]	Quantity		78
	DerivationIdentification <DerivtnId>	[0..1]	Binary		78
	Type <Tp>	[0..1]	CodeSet		78
	Function <Fctn>	[0..*]	CodeSet		79
	ParameterDataSet <ParamDataSet>	[0..1]			80
	Identification <Id>	[1..1]	±		80
	SequenceCounter <SeqCntr>	[0..1]	Text		81
	POIIdentification <POIId>	[0..*]	±		81
	ConfigurationScope <CfgrtnScp>	[0..1]	CodeSet		81
	Content <Cntt>	[1..1]			81
	ReplaceConfiguration <RplcCfgrtn>	[0..1]	Indicator		82
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		82
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		83
	MerchantParameters <MrchntParams>	[0..*]	±		86
	TerminalParameters <TermnlParams>	[0..*]	±		86
	ApplicationParameters <ApplParams>	[0..*]	±		87
	HostCommunicationParameters <HstComParams>	[0..*]	±		87
	SecurityParameters <SctyParams>	[0..*]	±		88
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		89

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TerminalPackage <TermnlPackg>	[0..*]	±		89

6.3.2.3.1 DelegationType <DlgtTp>

Presence: [1..1]

Definition: Type of delegation action.

Datatype: "TerminalManagementAction3Code" on page 291

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.

6.3.2.3.2 MaintenanceService <MntncSvc>

Presence: [1..*]

Definition: Maintenance service to be delegated.

Datatype: "DataSetCategory15Code" on page 281

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.

6.3.2.3.3 PartialDelegation <PrtlDlgn>

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 295):

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

6.3.2.3.4 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 296

6.3.2.3.5 DelegatedAction <DlgtActn>

Presence: [0..1]

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

DelegatedAction <DlgtActn> contains the following elements (see "MaintenanceDelegationAction5" on page 175 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	PeriodicAction <PrdcActn>	[0..1]	Indicator		177
	TMRemoteAccess <TMRemoteAccs>	[0..1]	±		177
	TMSProtocol <TMSPrtcol>	[0..1]	Text		177
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		178
	DataSetIdentification <DataSetId>	[0..1]	±		178
	ReTry <ReTry>	[0..1]	±		178
	AdditionalInformation <AddtlInf>	[0..*]	Binary		178
	Action <Actn>	[0..*]			178
	Type <Tp>	[1..1]	CodeSet		179
	RemoteAccess <RmotAccs>	[0..1]	±		180
	Key <Key>	[0..*]			181
	KeyIdentification <KeyId>	[1..1]	Text		181
	KeyVersion <KeyVrsn>	[1..1]	Text		181
	SequenceNumber <SeqNb>	[0..1]	Quantity		181
	DerivationIdentification <DerivtnId>	[0..1]	Binary		181
	Type <Tp>	[0..1]	CodeSet		181
	Function <Fctn>	[0..*]	CodeSet		182
	TerminalManagerIdentification <TermnlMgrId>	[0..1]	±		183
	TMSProtocol <TMSPrtcol>	[0..1]	Text		183
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		183
	DataSetIdentification <DataSetId>	[0..1]	±		183
	ComponentType <CmpntTp>	[0..*]	CodeSet		184
	DelegationScopeIdentification <DlgtScpld>	[0..1]	Text		185
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		185
	DelegationProof <DlgtProof>	[0..1]	Binary		185
	ProtectedDelegationProof <PrctdDlgtProof>	[0..1]	±		185
	Trigger <Trgr>	[1..1]	CodeSet		186
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		186
	ReTry <ReTry>	[0..1]	±		186
	TimeCondition <TmCond>	[0..1]	±		187

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TMChallenge <TMChllng>	[0..1]	Binary		187
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		187
	ErrorAction <ErrActn>	[0..*]	±		187
	AdditionalInformation <AddtlInf>	[0..*]	Binary		187
	MessageItem <Msgltn>	[0..*]	±		188

6.3.2.3.6 DelegationScopelIdentification <DlgnScpld>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

6.3.2.3.7 DelegationScopeDefinition <DlgnScpDef>

Presence: [0..1]

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

Datatype: "Max3000Binary" on page 266

6.3.2.3.8 Certificate <Cert>

Presence: [0..*]

Definition: Certificate path of the terminal manager.

Datatype: "Max10KBinary" on page 265

6.3.2.3.9 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 174 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	MasterTMIdentification <MstrTMId>	[1..1]	Text		174
	TMIdentification <TMId>	[1..1]	Text		174

6.3.2.3.10 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		78
	KeyVersion <KeyVrsn>	[1..1]	Text		78
	SequenceNumber <SeqNb>	[0..1]	Quantity		78
	DerivationIdentification <DerivtnId>	[0..1]	Binary		78
	Type <Tp>	[0..1]	CodeSet		78
	Function <Fctn>	[0..*]	CodeSet		79

6.3.2.3.10.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 296

6.3.2.3.10.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 296

6.3.2.3.10.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 295

6.3.2.3.10.4 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 267

6.3.2.3.10.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 278

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).

6.3.2.3.10.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 283

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.

6.3.2.3.11 ParameterDataSet <ParamDataSet>

Presence: [0..1]

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

ParameterDataSet <ParamDataSet> contains the following **AcceptorConfigurationDataSet1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	±		80
	SequenceCounter <SeqCntr>	[0..1]	Text		81
	POIIdentification <POIID>	[0..*]	±		81
	ConfigurationScope <CfgtnScp>	[0..1]	CodeSet		81
	Content <Cntt>	[1..1]			81
	ReplaceConfiguration <RplcCfgtn>	[0..1]	Indicator		82
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		82
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		83
	MerchantParameters <MrchntParams>	[0..*]	±		86
	TerminalParameters <TermnlParams>	[0..*]	±		86
	ApplicationParameters <ApplParams>	[0..*]	±		87
	HostCommunicationParameters <HstComParams>	[0..*]	±		87
	SecurityParameters <SctyParams>	[0..*]	±		88
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		89
	TerminalPackage <TermnlPackg>	[0..*]	±		89

6.3.2.3.11.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the data set transferred.

Identification <Id> contains the following elements (see "DataSetIdentification8" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

6.3.2.3.11.2 SequenceCounter <SeqCntr>

Presence: [0..1]

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

Datatype: "Max9NumericText" on page 297

6.3.2.3.11.3 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

6.3.2.3.11.4 ConfigurationScope <CfgtnScp>

Presence: [0..1]

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

Datatype: "PartyType15Code" on page 286

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.

6.3.2.3.11.5 Content <Cntt>

Presence: [1..1]

Definition: Content of the acceptor parameters.

Content <Cntt> contains the following **AcceptorConfigurationContent9** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ReplaceConfiguration <RplcCfgr>	[0..1]	Indicator		82
	TMSProtocolParameters <TMSPrtcolParams>	[0..*]	±		82
	AcquirerProtocolParameters <AcqrrPrtcolParams>	[0..*]	±		83
	MerchantParameters <MrchntParams>	[0..*]	±		86
	TerminalParameters <TermnlParams>	[0..*]	±		86
	ApplicationParameters <ApplParams>	[0..*]	±		87
	HostCommunicationParameters <HstComParams>	[0..*]	±		87
	SecurityParameters <SctyParams>	[0..*]	±		88
	SaleToPOIParameters <SaleToPOIParams>	[0..*]	±		89
	TerminalPackage <TermnlPackg>	[0..*]	±		89

6.3.2.3.11.5.1 ReplaceConfiguration <RplcCfgr>

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 295):

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

6.3.2.3.11.5.2 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 "TMSProtocolParameters5" on page 121 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		122
	TerminalManagerIdentification <TermnlMgrld>	[1..1]	±		122
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		123
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		123
	Version <Vrsn>	[1..1]	Text		124
	ApplicationIdentification <ApplId>	[0..*]	Text		124
	HostIdentification <Hstld>	[1..1]	Text		124
	POIIdentification <POIID>	[0..1]	Text		124
	InitiatingPartyIdentification <InitgPtyld>	[0..1]	Text		124
	RecipientPartyIdentification <RcptPtyld>	[0..1]	Text		124
	FileTransfer <FileTrf>	[0..1]	Indicator		124
	MessageItem <Msgltn>	[0..*]	±		124

6.3.2.3.11.5.3 AcquirerProtocolParameters <AcqrrPrtcolParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to an acquirer protocol.

AcquirerProtocolParameters <AcqrrPrtcolParams> contains the following elements (see "AcquirerProtocolParameters13" on page 145 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		148
	AcquirerIdentification <Acqrrld>	[1..*]	±		148
	Version <Vrsn>	[1..1]	Text		149
	ApplicationIdentification <Applld>	[0..*]	Text		149
	Host <Hst>	[0..*]			149
	HostIdentification <Hstld>	[1..1]	Text		149
	MessageToSend <MsgToSnd>	[0..*]	CodeSet		149
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		150
	OnLineTransaction <OnLineTx>	[0..1]			150
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		151
	BatchTransfer <BtchTrf>	[0..1]			152
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		152
	MaximumNumber <MaxNb>	[0..1]	Quantity		153
	MaximumAmount <MaxAmt>	[0..1]	Amount		153
	ReTry <ReTry>	[0..1]	±		153
	TimeCondition <TmCond>	[0..1]			153
	StartTime <StartTm>	[0..1]	DateTime		153
	EndTime <EndTm>	[0..1]	DateTime		154
	Period <Prd>	[0..1]	Text		154
	CompletionExchange <CmpltnXchg>	[0..1]			154
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		154
	MaximumNumber <MaxNb>	[0..1]	Quantity		155
	MaximumAmount <MaxAmt>	[0..1]	Amount		155
	ReTry <ReTry>	[0..1]	±		155
	TimeCondition <TmCond>	[0..1]			155
	StartTime <StartTm>	[0..1]	DateTime		156
	EndTime <EndTm>	[0..1]	DateTime		156
	Period <Prd>	[0..1]	Text		156
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		156
	OffLineTransaction <OffLineTx>	[0..1]			156

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		157
	BatchTransfer <BtchTrf>	[0..1]			158
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		158
	MaximumNumber <MaxNb>	[0..1]	Quantity		159
	MaximumAmount <MaxAmt>	[0..1]	Amount		159
	ReTry <ReTry>	[0..1]	±		159
	TimeCondition <TmCond>	[0..1]			159
	StartTime <StartTm>	[0..1]	DateTime		159
	EndTime <EndTm>	[0..1]	DateTime		160
	Period <Prd>	[0..1]	Text		160
	CompletionExchange <CmpltnXchg>	[0..1]			160
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		160
	MaximumNumber <MaxNb>	[0..1]	Quantity		161
	MaximumAmount <MaxAmt>	[0..1]	Amount		161
	ReTry <ReTry>	[0..1]	±		161
	TimeCondition <TmCond>	[0..1]			161
	StartTime <StartTm>	[0..1]	DateTime		162
	EndTime <EndTm>	[0..1]	DateTime		162
	Period <Prd>	[0..1]	Text		162
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		162
	ReconciliationExchange <RcncltnXchg>	[0..1]			162
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		163
	MaximumNumber <MaxNb>	[0..1]	Quantity		164
	MaximumAmount <MaxAmt>	[0..1]	Amount		164
	ReTry <ReTry>	[0..1]	±		164
	TimeCondition <TmCond>	[0..1]			164
	StartTime <StartTm>	[0..1]	DateTime		164
	EndTime <EndTm>	[0..1]	DateTime		164
	Period <Prd>	[0..1]	Text		164
	ReconciliationByAcquirer <RcncltnByAcqrr>	[0..1]	Indicator		165
	TotalsPerCurrency <TtlsPerCcy>	[0..1]	Indicator		165

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	SplitTotals <SplTtIs>	[0..1]	Indicator		165
	ReconciliationError <RcncltnErr>	[0..1]	Indicator		165
	CardDataVerification <CardDataVrfctn>	[0..1]	Indicator		165
	NotifyOffLineCancellation <NtfyOffLineCxl>	[0..1]	Indicator		166
	BatchTransferContent <BtchTrfCntt>	[0..*]	CodeSet		166
	FileTransferBatch <FileTrfBtch>	[0..1]	Indicator		166
	BatchDigitalSignature <BtchDgtlSgntr>	[0..1]	Indicator		166
	MessageItem <Msgltn>	[0..*]	±		166
	ProtectCardData <PrctCardData>	[1..1]	Indicator		167
	PrivateCardData <PrvtCardData>	[0..1]	Indicator		167
	MandatorySecurityTrailer <MndtrySctyTrlr>	[0..1]	Indicator		167

6.3.2.3.11.5.4 MerchantParameters <MrchntParams>

Presence: [0..*]

Definition: Acceptor parameters dedicated to the merchant.

MerchantParameters <MrchntParams> contains the following elements (see "MerchantConfigurationParameters5" on page 143 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		143
	MerchantIdentification <MrchntId>	[0..1]	Text		144
	Version <Vrsn>	[0..1]	Text		144
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		144
	Proxy <Prxy>	[0..1]			144
	Type <Tp>	[1..1]	CodeSet		144
	Access <Accs>	[1..1]	±		145
	OtherParameters <OthrParams>	[0..1]	Binary		145

6.3.2.3.11.5.5 TerminalParameters <TermnlParams>

Presence: [0..*]

Definition: Manufacturer configuration parameters of the point of interaction.

TerminalParameters <TermnlParams> contains the following elements (see
"PaymentTerminalParameters7" on page 140 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		140
	VendorIdentification <Vndrld>	[0..1]	Text		141
	Version <Vrsn>	[0..1]	Text		141
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		141
	ClockSynchronisation <ClckSynctn>	[0..1]			141
	POITimeZone <POITmZone>	[1..1]	Text		141
	SynchronisationServer <SynctnSvr>	[0..*]	±		142
	Delay <Dely>	[0..1]	Time		142
	TimeZoneLine <TmZoneLine>	[0..*]	Text		142
	LocalDateTime <LclDtTm>	[0..*]			142
	FromDateTime <FrDtTm>	[0..1]	DateTime		143
	ToDateTime <ToDtTm>	[0..1]	DateTime		143
	UTCOffset <UTCOffset>	[1..1]	Quantity		143
	OtherParameters <OthrParams>	[0..1]	Binary		143

6.3.2.3.11.5.6 ApplicationParameters <ApplParams>

Presence: [0..*]

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

ApplicationParameters <ApplParams> contains the following elements (see
"ApplicationParameters9" on page 139 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		139
	ApplicationIdentification <Applld>	[1..1]	Text		139
	Version <Vrsn>	[0..1]	Text		139
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		139
	Parameters <Params>	[0..*]	Binary		140
	EncryptedParameters <NcrptdParams>	[0..1]	±		140

6.3.2.3.11.5.7 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 132 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		133
	HostIdentification <HstId>	[1..1]	Text		133
	Address <Adr>	[0..1]	±		134
	Key <Key>	[0..*]			134
	KeyIdentification <KeyId>	[1..1]	Text		134
	KeyVersion <KeyVrsn>	[1..1]	Text		134
	SequenceNumber <SeqNb>	[0..1]	Quantity		135
	DerivationIdentification <DerivtnId>	[0..1]	Binary		135
	Type <Tp>	[0..1]	CodeSet		135
	Function <Fctn>	[0..*]	CodeSet		135
	NetworkServiceProvider <NtwkSvcPrvdr>	[0..1]	±		136
	PhysicalInterface <PhysIntrfc>	[0..1]			137
	InterfaceName <IntrfcNm>	[1..1]	Text		137
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		137
	UserName <UsrNm>	[0..1]	Text		138
	AccessCode <AccsCd>	[0..1]	Binary		138
	SecurityProfile <SctyPrfl>	[0..1]	Text		138
	AdditionalParameters <AddtlParams>	[0..1]	Binary		138

6.3.2.3.11.5.8 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 "SecurityParameters12" on page 131 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		131
	Version <Vrsn>	[1..1]	Text		131
	POIChallenge <POIChllng>	[0..1]	Binary		132
	TMChallenge <TMChllng>	[0..1]	Binary		132
	SecurityElement <SctyElmt>	[0..*]	±		132

6.3.2.3.11.5.9 SaleToPOIParameters <SaleToPOIParams>

Presence: [0..*]

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

SaleToPOIParameters <SaleToPOIParams> contains the following elements (see "SaleToPOIProtocolParameter1" on page 129 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		129
	MerchantIdentification <MrchntId>	[0..1]			129
	CommonName <CmonNm>	[1..1]	Text		130
	Address <Adr>	[0..1]	Text		130
	CountryCode <CtryCd>	[1..1]	CodeSet		130
	MerchantCategoryCode <MrchntCtgyCd>	[1..1]	Text		130
	RegisteredIdentifier <RegIdr>	[1..1]	Text		130
	Version <Vrsn>	[1..1]	Text		130
	HostIdentification <HstId>	[1..1]	Text		131
	MerchantPOIIdentification <MrchntPOIID>	[0..1]	Text		131
	SaleIdentification <SaleId>	[0..1]	Text		131

6.3.2.3.11.5.10 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 "TerminalPackageType1" on page 125 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	POIComponentIdentification <POICmpntId>	[0..*]			125
	ItemNumber <itmNb>	[0..1]	Text		126
	ProviderIdentification <PrvdrId>	[0..1]	Text		126
	Identification <Id>	[0..1]	Text		126
	SerialNumber <SrlNb>	[0..1]	Text		126
	Package <Packg>	[1..*]			126
	PackageIdentification <PackgId>	[0..1]	±		127
	PackageLength <PackgLngh>	[0..1]	Quantity		127
	OffsetStart <OffsetStart>	[0..1]	Quantity		127
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		127
	PackageBlock <PackgBlck>	[0..*]			128
	Identification <Id>	[1..1]	Text		128
	Value <Val>	[0..1]	Binary		128
	ProtectedValue <PrtctdVal>	[0..1]	±		128
	Type <Tp>	[0..1]	Text		129

6.3.3 SecurityTrailer <SctyTrlr>

Presence: [1..1]

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

SecurityTrailer <SctyTrlr> contains the following elements (see "ContentInformationType21" on page 244 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

7 catm.006.001.04 MaintenanceDelegationResponseV04

7.1 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 MaintenanceDelegationResponseV04 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.

7.2 Structure

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	Message root <Document> <MntncDlgtRspn>	[1..1]			
	Header <Hdr>	[1..1]			92
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		93
	FormatVersion <FrmtVrsn>	[1..1]	Text		93
	ExchangeIdentification <XchgId>	[1..1]	Quantity		93
	CreationDateTime <CreDtTm>	[1..1]	DateTime		93
	InitiatingParty <InitgPty>	[1..1]	±		93
	RecipientParty <RcptPty>	[0..1]	±		94
	Traceability <Tracblt>	[0..*]	±		94
	MaintenanceDelegationResponse <MntncDlgtRspn>	[1..1]			95
	TMIIdentification <TMId>	[1..1]	±		95
	MasterTMIIdentification <MstrTMId>	[0..1]	±		96
	DelegationResponse <DlgtRspn>	[1..*]			96
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		97
	Response <Rspn>	[1..1]	CodeSet		98
	ResponseReason <RspnRsn>	[0..1]	Text		98
	DelegationType <DlgtTp>	[1..1]	CodeSet		98
	POISubset <POISubset>	[0..*]	Text		98
	DelegationScopeIdentification <DlgtScpld>	[0..1]	Text		98
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		98
	DelegationProof <DlgtProof>	[0..1]	Binary		99
	ProtectedDelegationProof <PrctcdDlgtProof>	[0..1]	±		99
	POIIdentificationAssociation <POIIDAssocn>	[0..*]	±		99
	SecurityTrailer <SctyTrlr>	[0..1]	±		99

7.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

7.3.1 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		93
	FormatVersion <FrmtVrsn>	[1..1]	Text		93
	ExchangeIdentification <XchgId>	[1..1]	Quantity		93
	CreationDateTime <CreDtTm>	[1..1]	DateTime		93
	InitiatingParty <InitgPty>	[1..1]	±		93
	RecipientParty <RcptPty>	[0..1]	±		94
	Traceability <Tracblt>	[0..*]	±		94

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 295):

- *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 297

7.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: ["Number"](#) on page 295

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 294

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

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 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeln <TracDtTmln>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

7.3.2 MaintenanceDelegationResponse <MntncDlgtRspn>

Presence: [1..1]

Definition: Information related to the request of maintenance delegations.

MaintenanceDelegationResponse <MntncDlgtRspn> contains the following **MaintenanceDelegationResponse4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	TMIdentification <TMId>	[1..1]	±		95
	MasterTMIdentification <MstrTMId>	[0..1]	±		96
	DelegationResponse <DlgtRspn>	[1..*]			96
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		97
	Response <Rspn>	[1..1]	CodeSet		98
	ResponseReason <RspnRsn>	[0..1]	Text		98
	DelegationType <DlgtTp>	[1..1]	CodeSet		98
	POISubset <POISubset>	[0..*]	Text		98
	DelegationScopelIdentification <DlgtScpld>	[0..1]	Text		98
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		98
	DelegationProof <DlgtProof>	[0..1]	Binary		99
	ProtectedDelegationProof <PrctdDlgtProof>	[0..1]	±		99
	POIIdentificationAssociation <POIIdAssoctn>	[0..*]	±		99

7.3.2.1 TMIdentification <TMId>

Presence: [1..1]

Definition: Terminal manager identification.

TMIdentification <TMId> contains the following elements (see "[GenericIdentification176](#)" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

7.3.2.2 MasterTMIdentification <MstrTMId>

Presence: [0..1]

Definition: Master terminal manager identification.

MasterTMIdentification <MstrTMId> contains the following elements (see "[GenericIdentification176](#)" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

7.3.2.3 DelegationResponse <DlgnRspn>

Presence: [1..*]

Definition: Information on the delegation of a maintenance action.

DelegationResponse <DlgtnRspn> contains the following **MaintenanceDelegation9** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		97
	Response <Rspn>	[1..1]	CodeSet		98
	ResponseReason <RspnRsn>	[0..1]	Text		98
	DelegationType <DlgtnTp>	[1..1]	CodeSet		98
	POISubset <POISubset>	[0..*]	Text		98
	DelegationScopeIdentification <DlgtnScpld>	[0..1]	Text		98
	DelegationScopeDefinition <DlgtnScpDef>	[0..1]	Binary		98
	DelegationProof <DlgtnProof>	[0..1]	Binary		99
	ProtectedDelegationProof <PrctcdDlgtnProof>	[0..1]	±		99
	POIIdentificationAssociation <POIIdAssocn>	[0..*]	±		99

7.3.2.3.1 MaintenanceService <MntncSvc>

Presence: [1..*]

Definition: Maintenance service to be delegated.

Datatype: "DataSetCategory11Code" on page 279

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.

7.3.2.3.2 Response <Rspn>

Presence: [1..1]

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

Datatype: "Response2Code" on page 291

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

7.3.2.3.3 ResponseReason <RspnRsn>

Presence: [0..1]

Definition: Reason of the response of the MTM.

Datatype: "Max35Text" on page 296

7.3.2.3.4 DelegationType <DlgnTp>

Presence: [1..1]

Definition: Type of delegation action.

Datatype: "TerminalManagementAction3Code" on page 291

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.

7.3.2.3.5 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 296

7.3.2.3.6 DelegationScopelIdentification <DlgnScpld>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

7.3.2.3.7 DelegationScopeDefinition <DlgnScpDef>

Presence: [0..1]

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

Datatype: "Max3000Binary" on page 266

7.3.2.3.8 DelegationProof <DlgtProof>

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 266

7.3.2.3.9 ProtectedDelegationProof <PrtctdDlgtProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtProof> contains the following elements (see "ContentInformationType23" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

7.3.2.3.10 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 174 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	MasterTMIdentification <MstrTMId>	[1..1]	Text		174
	TMIdentification <TMId>	[1..1]	Text		174

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 "ContentInformationType21" on page 244 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

8 catm.007.001.03 CertificateManagementRequestV03

8.1 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 CertificateManagementRequestV03 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.

8.2 Structure

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	Message root <Document> <CertMgmtReq>	[1..1]			
	Header <Hdr>	[1..1]			102
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		102
	FormatVersion <FrmtVrsn>	[1..1]	Text		103
	ExchangeIdentification <XchgId>	[1..1]	Quantity		103
	CreationDateTime <CreDtTm>	[1..1]	DateTime		103
	InitiatingParty <InitgPty>	[1..1]	±		103
	RecipientParty <RcptPty>	[0..1]	±		103
	Traceability <Tracblt>	[0..*]	±		104
	CertificateManagementRequest <CertMgmtReq>	[1..1]			104
	POIdentification <POId>	[1..1]	±		105
	TMIIdentification <TMId>	[0..1]	±		106
	CertificateService <CertSvc>	[1..1]	CodeSet		106
	SecurityDomain <SctyDomn>	[0..1]	Text		107
	BinaryCertificationRequest <BinryCertfctnReq>	[0..1]	Text		107
	CertificationRequest <CertfctnReq>	[0..1]			107
	CertificateRequestInformation <CertReqInf>	[1..1]			108
	Version <Vrsn>	[0..1]	Quantity		108
	SubjectName <SbjtNm>	[0..1]			108
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			108
	AttributeType <AttrTp>	[1..1]	CodeSet		109
	AttributeValue <AttrVal>	[1..1]	Text		109
	SubjectPublicKeyInformation <SbjtPblyKeyInf>	[1..1]			109
	Algorithm <Algo>	[0..1]	CodeSet		110
	PublicKeyValue <PblyKeyVal>	[1..1]			110
	Modulus <Mdlus>	[1..1]	Binary		110
	Exponent <Expnt>	[1..1]	Binary		110
	Attribute <Attr>	[1..*]			110
	AttributeType <AttrTp>	[1..1]	CodeSet		111
	AttributeValue <AttrVal>	[1..1]	Text		111

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	KeyIdentification <KeyId>	[0..1]	Text		111
	KeyVersion <KeyVrsn>	[0..1]	Text		111
	ClientCertificate <ClntCert>	[0..1]	Binary		111
	WhiteListIdentification <WhtListId>	[0..1]			111
	ManufacturerIdentifier <Manfctrldr>	[1..1]	Text		112
	Model <Mdl>	[1..1]	Text		112
	SerialNumber <SrlNb>	[1..1]	Text		112
	SecurityTrailer <SctyTrlr>	[0..1]	±		112

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		102
	FormatVersion <FrmtVrsn>	[1..1]	Text		103
	ExchangeIdentification <XchgId>	[1..1]	Quantity		103
	CreationDateTime <CreDtTm>	[1..1]	DateTime		103
	InitiatingParty <InitgPty>	[1..1]	±		103
	RecipientParty <RcptPty>	[0..1]	±		103
	Traceability <Tracblt>	[0..*]	±		104

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 295):

- *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 297

8.3.1.3 Exchangeldentification <Xchgld>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: "Number" on page 295

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 294

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwr>	[1..1]	Text		174

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 <Tracblt> contains the following elements (see "[Traceability8](#)" on page 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

8.3.2 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]	±		105
	TMIdentification <TMId>	[0..1]	±		106
	CertificateService <CertSvc>	[1..1]	CodeSet		106
	SecurityDomain <SctyDomn>	[0..1]	Text		107
	BinaryCertificationRequest <BinryCertfctnReq>	[0..1]	Text		107
	CertificationRequest <CertfctnReq>	[0..1]			107
	CertificateRequestInformation <CertReqInf>	[1..1]			108
	Version <Vrsn>	[0..1]	Quantity		108
	SubjectName <SbjNm>	[0..1]			108
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			108
	AttributeType <AttrTp>	[1..1]	CodeSet		109
	AttributeValue <AttrVal>	[1..1]	Text		109
	SubjectPublicKeyInformation <SbjtpbkcKeyInf>	[1..1]			109
	Algorithm <Algo>	[0..1]	CodeSet		110
	PublicKeyValue <PbkcKeyVal>	[1..1]			110
	Modulus <Mdlus>	[1..1]	Binary		110
	Exponent <Expnt>	[1..1]	Binary		110
	Attribute <Attr>	[1..*]			110
	AttributeType <AttrTp>	[1..1]	CodeSet		111
	AttributeValue <AttrVal>	[1..1]	Text		111
	KeyIdentification <KeyId>	[0..1]	Text		111
	KeyVersion <KeyVrsn>	[0..1]	Text		111
	ClientCertificate <CIntCert>	[0..1]	Binary		111
	WhiteListIdentification <WhtListId>	[0..1]			111
	ManufacturerIdentifier <Manfctrldr>	[1..1]	Text		112
	Model <Mdl>	[1..1]	Text		112
	SerialNumber <SrlNb>	[1..1]	Text		112

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

8.3.2.3 CertificateService <CertSvc>

Presence: [1..1]

Definition: Requested certificate management service.

Datatype: "[CardPaymentServiceType10Code](#)" on page 277

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 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 297

8.3.2.5 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 296

8.3.2.6 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]			108
	Version <Vrsn>	[0..1]	Quantity		108
	SubjectName <SbjtNm>	[0..1]			108
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			108
	AttributeType <AttrTp>	[1..1]	CodeSet		109
	AttributeValue <AttrVal>	[1..1]	Text		109
	SubjectPublicKeyInformation <SbjtPblcKeyInf>	[1..1]			109
	Algorithm <Algo>	[0..1]	CodeSet		110
	PublicKeyValue <PblcKeyVal>	[1..1]			110
	Modulus <Mdlus>	[1..1]	Binary		110
	Exponent <Expnt>	[1..1]	Binary		110
	Attribute <Attr>	[1..*]			110
	AttributeType <AttrTp>	[1..1]	CodeSet		111
	AttributeValue <AttrVal>	[1..1]	Text		111
	KeyIdentification <KeyId>	[0..1]	Text		111
	KeyVersion <KeyVrsn>	[0..1]	Text		111

8.3.2.6.1 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		108
	SubjectName <SbjtNm>	[0..1]			108
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			108
	AttributeType <AttrTp>	[1..1]	CodeSet		109
	AttributeValue <AttrVal>	[1..1]	Text		109
	SubjectPublicKeyInformation <SbjtPbkcKeyInf>	[1..1]			109
	Algorithm <Algo>	[0..1]	CodeSet		110
	PublicKeyValue <PbkcKeyVal>	[1..1]			110
	Modulus <Mdlus>	[1..1]	Binary		110
	Exponent <Expnt>	[1..1]	Binary		110
	Attribute <Attr>	[1..*]			110
	AttributeType <AttrTp>	[1..1]	CodeSet		111
	AttributeValue <AttrVal>	[1..1]	Text		111

8.3.2.6.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the certificate request information data structure.

Datatype: "Number" on page 295

8.3.2.6.1.2 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..*]			108
	AttributeType <AttrTp>	[1..1]	CodeSet		109
	AttributeValue <AttrVal>	[1..1]	Text		109

8.3.2.6.1.2.1 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		109
	AttributeValue <AttrVal>	[1..1]	Text		109

8.3.2.6.1.2.1.1 AttributeType <AttrTp>

Presence: [1..1]

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

Datatype: "AttributeType1Code" on page 274

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).

8.3.2.6.1.2.1.2 AttributeValue <AttrVal>

Presence: [1..1]

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

Datatype: "Max140Text" on page 296

8.3.2.6.1.3 SubjectPublicKeyInformation <SbjtPblicKeyInf>

Presence: [1..1]

Definition: Information about the public key being certified.

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

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[0..1]	CodeSet		110
	PublicKeyValue <PblicKeyVal>	[1..1]			110
	Modulus <Mdlus>	[1..1]	Binary		110
	Exponent <Expnt>	[1..1]	Binary		110

8.3.2.6.1.4.1 AttributeType <AttrTp>

Presence: [1..1]

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

Datatype: "AttributeType2Code" on page 275

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

8.3.2.6.1.4.2 AttributeValue <AttrVal>

Presence: [1..1]

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

Datatype: "Max140Text" on page 296

8.3.2.6.2 KeyIdentification <KeyId>

Presence: [0..1]

Definition: Identification of the key.

Datatype: "Max140Text" on page 296

8.3.2.6.3 KeyVersion <KeyVrsn>

Presence: [0..1]

Definition: Version of the key.

Datatype: "Max140Text" on page 296

8.3.2.7 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 265

8.3.2.8 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 <ManfctrId>	[1..1]	Text		112
	Model <Mdl>	[1..1]	Text		112
	SerialNumber <SrINb>	[1..1]	Text		112

8.3.2.8.1 ManufacturerIdentifier <ManfctrIdr>

Presence: [1..1]

Definition: Identifier of the terminal manufacturer.

Datatype: "Max35Text" on page 296

8.3.2.8.2 Model <Mdl>

Presence: [1..1]

Definition: Identifier of the terminal model.

Datatype: "Max35Text" on page 296

8.3.2.8.3 SerialNumber <SrINb>

Presence: [1..1]

Definition: Serial number of the terminal manufacturer.

Datatype: "Max35Text" on page 296

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 "[ContentInformationType21](#)" on page 244 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

9 catm.008.001.03 CertificateManagementResponseV03

9.1 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 CertificateManagementResponseV03 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.

9.2 Structure

Or	MessageElement/BuildingBlock<XML Tag>	Mult.	Type	Constr. No.	Page
	Message root <Document> <CertMgmtRspn>	[1..1]			
	Header <Hdr>	[1..1]			114
	DownloadTransfer <DwnldTrf>	[1..1]	Indicator		115
	FormatVersion <FrmtVrsn>	[1..1]	Text		115
	ExchangeIdentification <XchgId>	[1..1]	Quantity		115
	CreationDateTime <CreDtTm>	[1..1]	DateTime		115
	InitiatingParty <InitgPty>	[1..1]	±		115
	RecipientParty <RcptPty>	[0..1]	±		116
	Traceability <Tracblt>	[0..*]	±		116
	CertificateManagementResponse <CertMgmtRspn>	[1..1]			117
	POIIdentification <POIID>	[1..1]	±		117
	TMIIdentification <TMId>	[0..1]	±		118
	CertificateService <CertSvc>	[1..1]	CodeSet		118
	Result <Rslt>	[1..1]			119
	Response <Rspn>	[1..1]	CodeSet		119
	ResponseDetail <RspnDtl>	[0..1]	CodeSet		119
	AdditionalResponse <AddtlRspn>	[0..1]	Text		119
	SecurityProfile <SctyPrfl>	[0..1]	Text		119
	ClientCertificate <CIntCert>	[0..1]	Binary		119
	ClientCertificatePath <CIntCertPth>	[0..*]	Binary		120
	ServerCertificatePath <SvrCertPth>	[0..*]	Binary		120
	SecurityTrailer <SctyTrlr>	[0..1]	±		120

9.3 Message Building Blocks

This chapter describes the MessageBuildingBlocks of this MessageDefinition.

9.3.1 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		115
	FormatVersion <FrmtVrsn>	[1..1]	Text		115
	ExchangeIdentification <XchgId>	[1..1]	Quantity		115
	CreationDateTime <CreDtTm>	[1..1]	DateTime		115
	InitiatingParty <InitgPty>	[1..1]	±		115
	RecipientParty <RcptPty>	[0..1]	±		116
	Traceability <Tracblt>	[0..*]	±		116

9.3.1.1 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 295):

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

9.3.1.2 FormatVersion <FrmtVrsn>

Presence: [1..1]

Definition: Version of file format.

Datatype: ["Max6Text"](#) on page 297

9.3.1.3 ExchangeIdentification <XchgId>

Presence: [1..1]

Definition: Unique identification of an exchange occurrence.

Datatype: ["Number"](#) on page 295

9.3.1.4 CreationDateTime <CreDtTm>

Presence: [1..1]

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

Datatype: ["ISODateTime"](#) on page 294

9.3.1.5 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

9.3.1.6 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 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

9.3.1.7 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 212 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	RelayIdentification <RlayId>	[1..1]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

9.3.2 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]	±		117
	TMIIdentification <TMId>	[0..1]	±		118
	CertificateService <CertSvc>	[1..1]	CodeSet		118
	Result <Rslt>	[1..1]			119
	Response <Rspn>	[1..1]	CodeSet		119
	ResponseDetail <RspnDtl>	[0..1]	CodeSet		119
	AdditionalResponse <AddtlRspn>	[0..1]	Text		119
	SecurityProfile <SctyPrfl>	[0..1]	Text		119
	ClientCertificate <CIntCert>	[0..1]	Binary		119
	ClientCertificatePath <CIntCertPth>	[0..*]	Binary		120
	ServerCertificatePath <SvrCertPth>	[0..*]	Binary		120

9.3.2.1 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

9.3.2.2 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

9.3.2.3 CertificateService <CertSvc>

Presence: [1..1]

Definition: Requested certificate management service.

Datatype: "[CardPaymentServiceType10Code](#)" on page 277

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.

9.3.2.4 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		119
	ResponseDetail <RspnDtl>	[0..1]	CodeSet		119
	AdditionalResponse <AddtlRspn>	[0..1]	Text		119

9.3.2.4.1 Response <Rspn>

Presence: [1..1]

Definition: Response of the terminal manager.

Datatype: "Response2Code" on page 291

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

9.3.2.4.2 ResponseDetail <RspnDtl>

Presence: [0..1]

Definition: Detail of the response.

Datatype: "ResultDetail3Code" on page 291

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

9.3.2.4.3 AdditionalResponse <AddtlRspn>

Presence: [0..1]

Definition: Additional information on the response for further examination.

Datatype: "Max140Text" on page 296

9.3.2.5 SecurityProfile <SctyPrfl>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

9.3.2.6 ClientCertificate <CIntCert>

Presence: [0..1]

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

Datatype: ["Max3000Binary" on page 266](#)

9.3.2.7 ClientCertificatePath <CIntCertPth>

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 265](#)

9.3.2.8 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 265](#)

9.3.3 SecurityTrailer <SctyTrlr>

Presence: [0..1]

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

SecurityTrailer <SctyTrlr> contains the following elements (see ["ContentInformationType21" on page 244](#) for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

10 Message Items Types

10.1 MessageComponents

10.1.1 Acquirer

10.1.1.1 KEKIdentifier2

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		121
	KeyVersion <KeyVrsn>	[1..1]	Text		121
	SequenceNumber <SeqNb>	[0..1]	Quantity		121
	DerivationIdentification <DerivtnId>	[0..1]	Binary		121

10.1.1.1.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 296

10.1.1.1.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 296

10.1.1.1.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 295

10.1.1.1.4 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 267

10.1.2 Configuration

10.1.2.1 TMSProtocolParameters5

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		122
	TerminalManagerIdentification <TermnlMgrld>	[1..1]	±		122
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		123
	MaintenanceService <MntncSvc>	[1..*]	CodeSet		123
	Version <Vrsn>	[1..1]	Text		124
	ApplicationIdentification <ApplId>	[0..*]	Text		124
	HostIdentification <HstId>	[1..1]	Text		124
	POIIdentification <POIId>	[0..1]	Text		124
	InitiatingPartyIdentification <InitgPtyId>	[0..1]	Text		124
	RecipientPartyIdentification <RcptPtyId>	[0..1]	Text		124
	FileTransfer <FileTrf>	[0..1]	Indicator		124
	MessageItem <Msgltn>	[0..*]	±		124

10.1.2.1.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.1.2 TerminalManagerIdentification <TermnlMgrld>

Presence: [1..1]

Definition: Identification of the master terminal manager or the terminal manager.

TerminalManagerIdentification <TermnlMgrId> contains the following elements (see
"GenericIdentification176" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

10.1.2.1.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Protocol version to use when using these parameters.

Datatype: "Max8Text" on page 297

10.1.2.1.4 MaintenanceService <MntncSvc>

Presence: [1..*]

Definition: Maintenance services provided by the terminal manager.

Datatype: "DataSetCategory10Code" on page 278

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.

10.1.2.1.5 Version <Vrsn>

Presence: [1..1]

Definition: Version of the TMS protocol parameters.

Datatype: "Max256Text" on page 296

10.1.2.1.6 ApplicationIdentification <ApplId>

Presence: [0..*]

Definition: Identification of applications which may be managed by the TM, partially or globally.

Datatype: "Max35Text" on page 296

10.1.2.1.7 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification of the terminal manager host.

Datatype: "Max35Text" on page 296

10.1.2.1.8 POIIdentification <POIId>

Presence: [0..1]

Definition: New identification of the POI for the terminal manager.

Datatype: "Max35Text" on page 296

10.1.2.1.9 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 296

10.1.2.1.10 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 296

10.1.2.1.11 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 295):

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

10.1.2.1.12 MessageItem <MsgItm>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <Msgltm> contains the following elements (see "MessageItemCondition1" on page 174 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemIdentification <ItmId>	[1..1]	Text		174
	Condition <Cond>	[1..1]	CodeSet		175
	Value <Val>	[0..*]	Text		175

10.1.2.2 TerminalPackageType1

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..*]			125
	ItemNumber <ItmNb>	[0..1]	Text		126
	ProviderIdentification <PrvdrlId>	[0..1]	Text		126
	Identification <Id>	[0..1]	Text		126
	SerialNumber <SrlNb>	[0..1]	Text		126
	Package <Packg>	[1..*]			126
	PackageIdentification <PackgId>	[0..1]	±		127
	PackageLength <PackgLngh>	[0..1]	Quantity		127
	OffsetStart <OffsetStart>	[0..1]	Quantity		127
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		127
	PackageBlock <PackgBlck>	[0..*]			128
	Identification <Id>	[1..1]	Text		128
	Value <Val>	[0..1]	Binary		128
	ProtectedValue <PrctcdVal>	[0..1]	±		128
	Type <Tp>	[0..1]	Text		129

10.1.2.2.1 POIComponentIdentification <POICmpntId>

Presence: [0..*]

Definition: Identification of the POI (Point Of Interaction) component.

POIComponentIdentification <POICmpntId> contains the following
PointOfInteractionComponentIdentification1 elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemNumber <ItmNb>	[0..1]	Text		126
	ProviderIdentification <PrvdrId>	[0..1]	Text		126
	Identification <Id>	[0..1]	Text		126
	SerialNumber <SrINb>	[0..1]	Text		126

10.1.2.2.1.1 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 296

10.1.2.2.1.2 ProviderIdentification <PrvdrId>

Presence: [0..1]

Definition: Identifies the provider of the software, hardware or parameters of the POI component.

Datatype: "Max35Text" on page 296

10.1.2.2.1.3 Identification <Id>

Presence: [0..1]

Definition: Identification of the POI component assigned by its provider.

Datatype: "Max35Text" on page 296

10.1.2.2.1.4 SerialNumber <SrINb>

Presence: [0..1]

Definition: Serial number identifying an occurrence of an hardware component.

Datatype: "Max35Text" on page 296

10.1.2.2.2 Package <Packg>

Presence: [1..*]

Definition: Chunk of a software package.

Package <Packg> contains the following **PackageType1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	PackageIdentification <PackgId>	[0..1]	±		127
	PackageLength <PackgLngh>	[0..1]	Quantity		127
	OffsetStart <OffsetStart>	[0..1]	Quantity		127
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		127
	PackageBlock <PackgBlck>	[0..*]			128
	Identification <Id>	[1..1]	Text		128
	Value <Val>	[0..1]	Binary		128
	ProtectedValue <PrtctdVal>	[0..1]	±		128
	Type <Tp>	[0..1]	Text		129

10.1.2.2.2.1 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

10.1.2.2.2.2 PackageLength <PackgLngh>

Presence: [0..1]

Definition: Full length of software package identified through PackageIdentification.

Datatype: "[PositiveNumber](#)" on page 295

10.1.2.2.2.3 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 295

10.1.2.2.2.4 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 295

10.1.2.2.2.5 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 **ExternallyDefinedData1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		128
	Value <Val>	[0..1]	Binary		128
	ProtectedValue <PrctcdVal>	[0..1]	±		128
	Type <Tp>	[0..1]	Text		129

10.1.2.2.2.5.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the set of data to exchange.

Datatype: "Max1025Text" on page 296

10.1.2.2.2.5.2 Value <Val>

Presence: [0..1]

Definition: Data to exchange according to an external standard.

Datatype: "Max100KBinary" on page 265

10.1.2.2.2.5.3 ProtectedValue <PrctcdVal>

Presence: [0..1]

Definition: Protection of the values to exchange.

ProtectedValue <PrctcdVal> contains the following elements (see "ContentInformationType23" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

10.1.2.2.5.4 Type <Tp>

Presence: [0..1]

Definition: Identification of the standard used to encode the values to exchange.

Datatype: "Max1025Text" on page 296

10.1.2.3 SaleToPOIProtocolParameter1

Definition: Configuration parameters to communicate with a sale system.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		129
	MerchantIdentification <MrchntId>	[0..1]			129
	CommonName <CmonNm>	[1..1]	Text		130
	Address <Adr>	[0..1]	Text		130
	CountryCode <CtryCd>	[1..1]	CodeSet		130
	MerchantCategoryCode <MrchntCtgyCd>	[1..1]	Text		130
	RegisteredIdentifier <RegIdIdr>	[1..1]	Text		130
	Version <Vrsn>	[1..1]	Text		130
	HostIdentification <HstId>	[1..1]	Text		131
	MerchantPOIIdentification <MrchntPOIId>	[0..1]	Text		131
	SaleIdentification <SaleId>	[0..1]	Text		131

10.1.2.3.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.3.2 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		130
	Address <Adr>	[0..1]	Text		130
	CountryCode <CtryCd>	[1..1]	CodeSet		130
	MerchantCategoryCode <MrchntCtgyCd>	[1..1]	Text		130
	RegisteredIdentifier <RegIdIdr>	[1..1]	Text		130

10.1.2.3.2.1 CommonName <CmonNm>

Presence: [1..1]

Definition: Name of the merchant.

Datatype: "Max70Text" on page 297

10.1.2.3.2.2 Address <Adr>

Presence: [0..1]

Definition: Location of the merchant.

Datatype: "Max140Text" on page 296

10.1.2.3.2.3 CountryCode <CtryCd>

Presence: [1..1]

Definition: Country of the merchant.

Datatype: "ISO3NumericCountryCode" on page 283

10.1.2.3.2.4 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 298

10.1.2.3.2.5 RegisteredIdentifier <RegIdIdr>

Presence: [1..1]

Definition: Identifier of the sponsored merchant assigned by the payment facilitator of their acquirer.

Datatype: "Max35Text" on page 296

10.1.2.3.3 Version <Vrsn>

Presence: [1..1]

Definition: Version of the parameters.

Datatype: "Max256Text" on page 296

10.1.2.3.4 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification used to retrieve HostCommunicationParameters.

Datatype: "Max35Text" on page 296

10.1.2.3.5 MerchantPOIIdentification <MrchntPOId>

Presence: [0..1]

Definition: Identification of the POI during communication with sale system.

Datatype: "Max35Text" on page 296

10.1.2.3.6 SaleIdentification <SaleId>

Presence: [0..1]

Definition: Identification of the SaleSystem connected to the POI.

Datatype: "Max35Text" on page 296

10.1.2.4 SecurityParameters12

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		131
	Version <Vrsn>	[1..1]	Text		131
	POIChallenge <POIChllng>	[0..1]	Binary		132
	TMChallenge <TMChllng>	[0..1]	Binary		132
	SecurityElement <SctyElmt>	[0..*]	±		132

10.1.2.4.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.4.2 Version <Vrsn>

Presence: [1..1]

Definition: Version of the security parameters.

Datatype: "Max256Text" on page 296

10.1.2.4.3 POIChallenge <POIChllng>

Presence: [0..1]

Definition: Point of interaction challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 266

10.1.2.4.4 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "Max140Binary" on page 266

10.1.2.4.5 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 "CryptographicKey14" on page 221 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		221
	AdditionalIdentification <AddtlId>	[0..1]	Binary		222
	Name <Nm>	[0..1]	Text		222
	SecurityProfile <SctyPrfl>	[0..1]	Text		222
	ItemNumber <ItmNb>	[0..1]	Text		222
	Version <Vrsn>	[1..1]	Text		222
	Type <Tp>	[0..1]	CodeSet		222
	Function <Fctn>	[0..*]	CodeSet		223
	ActivationDate <ActvtnDt>	[0..1]	DateTime		224
	DeactivationDate <DeactvtnDt>	[0..1]	DateTime		224
	KeyValue <KeyVal>	[0..1]	±		224
	KeyCheckValue <KeyChckVal>	[0..1]	Binary		224
	AdditionalManagementInformation <AddtlMgmtInf>	[0..*]			224
	Name <Nm>	[1..1]	Text		225
	Value <Val>	[0..1]	Text		225

10.1.2.5 HostCommunicationParameter6

Definition: Configuration parameters to communicate with a host.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		133
	HostIdentification <Hstld>	[1..1]	Text		133
	Address <Adr>	[0..1]	±		134
	Key <Key>	[0..*]			134
	KeyIdentification <Keyld>	[1..1]	Text		134
	KeyVersion <KeyVrsn>	[1..1]	Text		134
	SequenceNumber <SeqNb>	[0..1]	Quantity		135
	DerivationIdentification <Derivtnld>	[0..1]	Binary		135
	Type <Tp>	[0..1]	CodeSet		135
	Function <Fctn>	[0..*]	CodeSet		135
	NetworkServiceProvider <NtwkSvcPrvdr>	[0..1]	±		136
	PhysicalInterface <PhysIntrfc>	[0..1]			137
	InterfaceName <IntrfcNm>	[1..1]	Text		137
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		137
	UserName <UsrNm>	[0..1]	Text		138
	AccessCode <AccsCd>	[0..1]	Binary		138
	SecurityProfile <SctyPrfl>	[0..1]	Text		138
	AdditionalParameters <AddtlParams>	[0..1]	Binary		138

10.1.2.5.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.5.2 HostIdentification <Hstld>

Presence: [1..1]

Definition: Identification of the host.

Datatype: "Max35Text" on page 296

10.1.2.5.3 Address <Adr>

Presence: [0..1]

Definition: Network parameters of the host.

Address <Adr> contains the following elements (see "NetworkParameters7" on page 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.2.5.4 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		134
	KeyVersion <KeyVrsn>	[1..1]	Text		134
	SequenceNumber <SeqNb>	[0..1]	Quantity		135
	DerivationIdentification <DerivtnId>	[0..1]	Binary		135
	Type <Tp>	[0..1]	CodeSet		135
	Function <Fctn>	[0..*]	CodeSet		135

10.1.2.5.4.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 296

10.1.2.5.4.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 296

10.1.2.5.4.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 295

10.1.2.5.4.4 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 267

10.1.2.5.4.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 278

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 Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).
EDE4	DES168	Data encryption standard key of 168 bits (without the parity bits).

10.1.2.5.4.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 283

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.

10.1.2.5.5 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 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.2.5.6 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		137
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		137
	UserName <UsrNm>	[0..1]	Text		138
	AccessCode <AccsCd>	[0..1]	Binary		138
	SecurityProfile <SctyPrfl>	[0..1]	Text		138
	AdditionalParameters <AddtlParams>	[0..1]	Binary		138

10.1.2.5.6.1 InterfaceName <IntrfcNm>

Presence: [1..1]

Definition: Identification of the interface.

Datatype: "Max35Text" on page 296

10.1.2.5.6.2 InterfaceType <IntrfcTp>

Presence: [0..1]

Definition: Identification of the physical link layer.

Datatype: "POICommunicationType2Code" on page 288

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.

10.1.2.5.6.3 UserName <UsrNm>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.2.5.6.4 AccessCode <AccsCd>

Presence: [0..1]

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

Datatype: "Max35Binary" on page 266

10.1.2.5.6.5 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the optional security profile to use with this interface.

Datatype: "Max35Text" on page 296

10.1.2.5.6.6 AdditionalParameters <AddtlParams>

Presence: [0..1]

Definition: Any other parameters relevant for this interface.

Datatype: "Max2KBinary" on page 266

10.1.2.6 ApplicationParameters9

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		139
	ApplicationIdentification <ApplId>	[1..1]	Text		139
	Version <Vrsn>	[0..1]	Text		139
	ParameterFormatIdentifier <ParamFrmtIdr>	[0..1]	Text		139
	Parameters <Params>	[0..*]	Binary		140
	EncryptedParameters <NcrptdParams>	[0..1]	±		140

10.1.2.6.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.6.2 ApplicationIdentification <ApplId>

Presence: [1..1]

Definition: Identification of the payment application.

Datatype: "Max35Text" on page 296

10.1.2.6.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the payment application configuration parameters.

Datatype: "Max256Text" on page 296

10.1.2.6.4 ParameterFormatIdentifier <ParamFrmtIdr>

Presence: [0..1]

Definition: Version of the parameters' format.

Datatype: "Max8Text" on page 297

10.1.2.6.5 Parameters <Params>

Presence: [0..*]

Definition: Configuration parameters used by the related payment application.

Datatype: "Max100KBinary" on page 265

10.1.2.6.6 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 "ContentInformationType22" on page 239 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		239
	EnvelopedData <EnvlpdData>	[1..1]	±		240

10.1.2.7 PaymentTerminalParameters7

Definition: Manufacturer configuration parameters of the point of interaction (POI).

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		140
	VendorIdentification <Vndrld>	[0..1]	Text		141
	Version <Vrsn>	[0..1]	Text		141
	ParameterFormatIdentifier <ParamFrmtldr>	[0..1]	Text		141
	ClockSynchronisation <ClckSynctn>	[0..1]			141
	POITimeZone <POITmZone>	[1..1]	Text		141
	SynchronisationServer <SynctnSvr>	[0..*]	±		142
	Delay <Dely>	[0..1]	Time		142
	TimeZoneLine <TmZoneLine>	[0..*]	Text		142
	LocalDateTime <LclDtTm>	[0..*]			142
	FromDateTime <FrDtTm>	[0..1]	DateTime		143
	ToDateTime <ToDtTm>	[0..1]	DateTime		143
	UTCOffset <UTCOffset>	[1..1]	Quantity		143
	OtherParameters <OthrParams>	[0..1]	Binary		143

10.1.2.7.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.7.2 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 296

10.1.2.7.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the terminal parameters.

Datatype: "Max256Text" on page 296

10.1.2.7.4 ParameterFormatIdentifier <ParamFrmtIdr>

Presence: [0..1]

Definition: Version of the parameters' format.

Datatype: "Max8Text" on page 297

10.1.2.7.5 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		141
	SynchronisationServer <SynctnSvr>	[0..*]	±		142
	Delay <Dely>	[0..1]	Time		142

10.1.2.7.5.1 POITimeZone <POITmZone>

Presence: [1..1]

Definition: Name of the time zone where is located the POI (Point Of Interaction), as defined by the IANA (Internet Assigned Number Authority) time zone data base.

Datatype: "Max70Text" on page 297

10.1.2.7.5.2 SynchronisationServer <SynctnSvr>

Presence: [0..*]

Definition: Parameters to contact a time server.

SynchronisationServer <SynctnSvr> contains the following elements (see "NetworkParameters7" on page 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.2.7.5.3 Delay <Dely>

Presence: [0..1]

Definition: Delay between two contacts of the server.

Datatype: "ISOTime" on page 298

10.1.2.7.6 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 297

10.1.2.7.7 LocalDateTime <LcIdtTm>

Presence: [0..*]

Definition: Local time offset to UTC (Coordinated Universal Time).

LocalDateTime <LcIdtTm> contains the following **LocalDateTime1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	FromDateTime <FrDtTm>	[0..1]	DateTime		143
	ToDateTime <ToDtTm>	[0..1]	DateTime		143
	UTCOffset <UTCOffset>	[1..1]	Quantity		143

10.1.2.7.7.1 FromDateTime <FrDtTm>

Presence: [0..1]

Definition: Date time of the beginning of the period (inclusive).

Datatype: "ISODatetime" on page 294

10.1.2.7.7.2 ToDateTime <ToDtTm>

Presence: [0..1]

Definition: Date time of the end of the period (exclusive).

Datatype: "ISODatetime" on page 294

10.1.2.7.7.3 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 295

10.1.2.7.8 OtherParameters <OthrParams>

Presence: [0..1]

Definition: Others manufacturer configuration parameters of the point of interaction.

Datatype: "Max10000Binary" on page 265

10.1.2.8 MerchantConfigurationParameters5

Definition: Acceptor parameters dedicated to the merchant.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		143
	MerchantIdentification <MrchntId>	[0..1]	Text		144
	Version <Vrsn>	[0..1]	Text		144
	ParameterFormatIdentifier <ParamFrmtIdr>	[0..1]	Text		144
	Proxy <Prxy>	[0..1]			144
	Type <Tp>	[1..1]	CodeSet		144
	Access <Accs>	[1..1]	±		145
	OtherParameters <OthrParams>	[0..1]	Binary		145

10.1.2.8.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.8.2 MerchantIdentification <MrchntId>

Presence: [0..1]

Definition: Identification of the merchant for the MTM, if the POI manages several merchants.

Datatype: "Max35Text" on page 296

10.1.2.8.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the merchant parameters.

Datatype: "Max256Text" on page 296

10.1.2.8.4 ParameterFormatIdentifier <ParamFrmtIdr>

Presence: [0..1]

Definition: Version of the parameters' format.

Datatype: "Max8Text" on page 297

10.1.2.8.5 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		144
	Access <Accs>	[1..1]	±		145

10.1.2.8.5.1 Type <Tp>

Presence: [1..1]

Definition: Type of proxy.

Datatype: "NetworkType2Code" on page 286

CodeName	Name	Definition
SCK5	Sock5	Sock5 proxy.
SCK4	Sock4	Sock4 proxy.
HTTP	HTTP	HTTP proxy.

10.1.2.8.5.2 Access <Accs>

Presence: [1..1]

Definition: Access information to the proxy.

Access <Accs> contains the following elements (see "NetworkParameters7" on page 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.2.8.6 OtherParameters <OthrParams>

Presence: [0..1]

Definition: Other merchant parameters.

Datatype: "Max10000Binary" on page 265

10.1.2.9 AcquirerProtocolParameters13

Definition: Acceptor parameters dedicated to the acquirer protocol.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		148
	AcquirerIdentification <Acqrrld>	[1..*]	±		148
	Version <Vrsn>	[1..1]	Text		149
	ApplicationIdentification <Applld>	[0..*]	Text		149
	Host <Hst>	[0..*]			149
	HostIdentification <Hstld>	[1..1]	Text		149
	MessageToSend <MsgToSnd>	[0..*]	CodeSet		149
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		150
	OnLineTransaction <OnLineTx>	[0..1]			150
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		151
	BatchTransfer <BtchTrf>	[0..1]			152
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		152
	MaximumNumber <MaxNb>	[0..1]	Quantity		153
	MaximumAmount <MaxAmt>	[0..1]	Amount		153
	ReTry <ReTry>	[0..1]	±		153
	TimeCondition <TmCond>	[0..1]			153
	StartTime <StartTm>	[0..1]	DateTime		153
	EndTime <EndTm>	[0..1]	DateTime		154
	Period <Prd>	[0..1]	Text		154
	CompletionExchange <CmpltnXchg>	[0..1]			154
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		154
	MaximumNumber <MaxNb>	[0..1]	Quantity		155
	MaximumAmount <MaxAmt>	[0..1]	Amount		155
	ReTry <ReTry>	[0..1]	±		155
	TimeCondition <TmCond>	[0..1]			155
	StartTime <StartTm>	[0..1]	DateTime		156
	EndTime <EndTm>	[0..1]	DateTime		156
	Period <Prd>	[0..1]	Text		156
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		156
	OffLineTransaction <OffLineTx>	[0..1]			156
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		157

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	BatchTransfer <BtchTrf>	[0..1]			158
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		158
	MaximumNumber <MaxNb>	[0..1]	Quantity		159
	MaximumAmount <MaxAmt>	[0..1]	Amount		159
	ReTry <ReTry>	[0..1]	±		159
	TimeCondition <TmCond>	[0..1]			159
	StartTime <StartTm>	[0..1]	DateTime		159
	EndTime <EndTm>	[0..1]	DateTime		160
	Period <Prd>	[0..1]	Text		160
	CompletionExchange <CmpltnXchg>	[0..1]			160
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		160
	MaximumNumber <MaxNb>	[0..1]	Quantity		161
	MaximumAmount <MaxAmt>	[0..1]	Amount		161
	ReTry <ReTry>	[0..1]	±		161
	TimeCondition <TmCond>	[0..1]			161
	StartTime <StartTm>	[0..1]	DateTime		162
	EndTime <EndTm>	[0..1]	DateTime		162
	Period <Prd>	[0..1]	Text		162
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		162
	ReconciliationExchange <RcncltnXchg>	[0..1]			162
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		163
	MaximumNumber <MaxNb>	[0..1]	Quantity		164
	MaximumAmount <MaxAmt>	[0..1]	Amount		164
	ReTry <ReTry>	[0..1]	±		164
	TimeCondition <TmCond>	[0..1]			164
	StartTime <StartTm>	[0..1]	DateTime		164
	EndTime <EndTm>	[0..1]	DateTime		164
	Period <Prd>	[0..1]	Text		164
	ReconciliationByAcquirer <RcncltnByAcqrr>	[0..1]	Indicator		165
	TotalsPerCurrency <TtlsPerCcy>	[0..1]	Indicator		165
	SplitTotals <SplTtls>	[0..1]	Indicator		165

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ReconciliationError <RcncltnErr>	[0..1]	Indicator		165
	CardDataVerification <CardDataVrfctn>	[0..1]	Indicator		165
	NotifyOffLineCancellation <NtfyOffLineCxl>	[0..1]	Indicator		166
	BatchTransferContent <BtchTrfCntt>	[0..*]	CodeSet		166
	FileTransferBatch <FileTrfBtch>	[0..1]	Indicator		166
	BatchDigitalSignature <BtchDgtlSgntr>	[0..1]	Indicator		166
	MessageItem <Msgltn>	[0..*]	±		166
	ProtectCardData <PrctctCardData>	[1..1]	Indicator		167
	PrivateCardData <PrvtCardData>	[0..1]	Indicator		167
	MandatorySecurityTrailer <MndtrySctyTrlr>	[0..1]	Indicator		167

10.1.2.9.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Type of action for the configuration parameters.

Datatype: "TerminalManagementAction3Code" on page 291

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.

10.1.2.9.2 AcquirerIdentification <Acqrrld>

Presence: [1..*]

Definition: Identification of the acquirer using this protocol.

AcquirerIdentification <Acqrrld> contains the following elements (see "GenericIdentification176" on page 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

10.1.2.9.3 Version <Vrsn>

Presence: [1..1]

Definition: Version of the acquirer protocol parameters.

Datatype: "Max256Text" on page 296

10.1.2.9.4 ApplicationIdentification <ApplId>

Presence: [0..*]

Definition: Identification of the payment application, user of the acquirer protocol.

Datatype: "Max35Text" on page 296

10.1.2.9.5 Host <Hst>

Presence: [0..*]

Definition: Acquirer host configuration.

Host <Hst> contains the following **AcquirerHostConfiguration7** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	HostIdentification <HstId>	[1..1]	Text		149
	MessageToSend <MsgToSnd>	[0..*]	CodeSet		149
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		150

10.1.2.9.5.1 HostIdentification <HstId>

Presence: [1..1]

Definition: Identification of a host.

Datatype: "Max35Text" on page 296

10.1.2.9.5.2 MessageToSend <MsgToSnd>

Presence: [0..*]

Definition: Types of message to sent to this host.

Datatype: "MessageFunction40Code" on page 284

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 transaction.

CodeName	Name	Definition
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.

10.1.2.9.5.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Protocol version to use when using these parameters.

Datatype: "Max8Text" on page 297

10.1.2.9.6 OnLineTransaction <OnLineTx>

Presence: [0..1]

Definition: Acquirer protocol parameters of transactions performing an online authorisation.

OnLineTransaction <OnLineTx> contains the following **AcquirerProtocolExchangeBehavior1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		151
	BatchTransfer <BtchTrf>	[0..1]			152
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		152
	MaximumNumber <MaxNb>	[0..1]	Quantity		153
	MaximumAmount <MaxAmt>	[0..1]	Amount		153
	ReTry <ReTry>	[0..1]	±		153
	TimeCondition <TmCond>	[0..1]			153
	StartTime <StartTm>	[0..1]	DateTime		153
	EndTime <EndTm>	[0..1]	DateTime		154
	Period <Prd>	[0..1]	Text		154
	CompletionExchange <CmpltnXchg>	[0..1]			154
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		154
	MaximumNumber <MaxNb>	[0..1]	Quantity		155
	MaximumAmount <MaxAmt>	[0..1]	Amount		155
	ReTry <ReTry>	[0..1]	±		155
	TimeCondition <TmCond>	[0..1]			155
	StartTime <StartTm>	[0..1]	DateTime		156
	EndTime <EndTm>	[0..1]	DateTime		156
	Period <Prd>	[0..1]	Text		156
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		156

10.1.2.9.6.1 FinancialCapture <FinCaptr>

Presence: [1..1]

Definition: Mode for the financial capture of the transaction by the acquirer.

Datatype: "FinancialCapture1Code" on page 282

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.

CodeName	Name	Definition
BTCH	Batch	Financial capture of the transaction is performed by the acquirer at the reception of a batch transfer.

10.1.2.9.6.2 BatchTransfer <BtchTrf>

Presence: [0..1]

Definition: Configuration of the batch transfers.

BatchTransfer <BtchTrf> contains the following **ExchangeConfiguration8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		152
	MaximumNumber <MaxNb>	[0..1]	Quantity		153
	MaximumAmount <MaxAmt>	[0..1]	Amount		153
	ReTry <ReTry>	[0..1]	±		153
	TimeCondition <TmCond>	[0..1]			153
	StartTime <StartTm>	[0..1]	DateTime		153
	EndTime <EndTm>	[0..1]	DateTime		154
	Period <Prd>	[0..1]	Text		154

10.1.2.9.6.2.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 282

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.

CodeName	Name	Definition
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.

10.1.2.9.6.2.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 295

10.1.2.9.6.2.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 265

10.1.2.9.6.2.4 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.2.9.6.2.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following **ProcessTiming4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	StartTime <StartTm>	[0..1]	DateTime		153
	EndTime <EndTm>	[0..1]	DateTime		154
	Period <Prd>	[0..1]	Text		154

10.1.2.9.6.2.5.1 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODateTime" on page 294

10.1.2.9.6.2.5.2 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODateTime" on page 294

10.1.2.9.6.2.5.3 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 297

10.1.2.9.6.3 CompletionExchange <CmpltnXchg>

Presence: [0..1]

Definition: Configuration parameters of completion exchanges.

CompletionExchange <CmpltnXchg> contains the following **ExchangeConfiguration8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		154
	MaximumNumber <MaxNb>	[0..1]	Quantity		155
	MaximumAmount <MaxAmt>	[0..1]	Amount		155
	ReTry <ReTry>	[0..1]	±		155
	TimeCondition <TmCond>	[0..1]			155
	StartTime <StartTm>	[0..1]	DateTime		156
	EndTime <EndTm>	[0..1]	DateTime		156
	Period <Prd>	[0..1]	Text		156

10.1.2.9.6.3.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 282

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.

CodeName	Name	Definition
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.

10.1.2.9.6.3.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 295

10.1.2.9.6.3.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 265

10.1.2.9.6.3.4 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.2.9.6.3.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following **ProcessTiming4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	StartTime <StartTm>	[0..1]	DateTime		156
	EndTime <EndTm>	[0..1]	DateTime		156
	Period <Prd>	[0..1]	Text		156

10.1.2.9.6.3.5.1 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODatetime" on page 294

10.1.2.9.6.3.5.2 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODatetime" on page 294

10.1.2.9.6.3.5.3 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 297

10.1.2.9.6.4 CancellationExchange <CxlXchg>

Presence: [0..1]

Definition: Configuration of the cancellation exchanges.

Datatype: "CancellationProcess2Code" on page 275

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.

10.1.2.9.7 OffLineTransaction <OffLineTx>

Presence: [0..1]

Definition: Acquirer protocol parameters of transactions performing an offline authorisation.

OffLineTransaction <OffLineTx> contains the following **AcquirerProtocolExchangeBehavior1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	FinancialCapture <FinCaptr>	[1..1]	CodeSet		157
	BatchTransfer <BtchTrf>	[0..1]			158
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		158
	MaximumNumber <MaxNb>	[0..1]	Quantity		159
	MaximumAmount <MaxAmt>	[0..1]	Amount		159
	ReTry <ReTry>	[0..1]	±		159
	TimeCondition <TmCond>	[0..1]			159
	StartTime <StartTm>	[0..1]	DateTime		159
	EndTime <EndTm>	[0..1]	DateTime		160
	Period <Prd>	[0..1]	Text		160
	CompletionExchange <CmpltnXchg>	[0..1]			160
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		160
	MaximumNumber <MaxNb>	[0..1]	Quantity		161
	MaximumAmount <MaxAmt>	[0..1]	Amount		161
	ReTry <ReTry>	[0..1]	±		161
	TimeCondition <TmCond>	[0..1]			161
	StartTime <StartTm>	[0..1]	DateTime		162
	EndTime <EndTm>	[0..1]	DateTime		162
	Period <Prd>	[0..1]	Text		162
	CancellationExchange <CxlXchg>	[0..1]	CodeSet		162

10.1.2.9.7.1 FinancialCapture <FinCaptr>

Presence: [1..1]

Definition: Mode for the financial capture of the transaction by the acquirer.

Datatype: "FinancialCapture1Code" on page 282

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.

CodeName	Name	Definition
BTCH	Batch	Financial capture of the transaction is performed by the acquirer at the reception of a batch transfer.

10.1.2.9.7.2 BatchTransfer <BtchTrf>

Presence: [0..1]

Definition: Configuration of the batch transfers.

BatchTransfer <BtchTrf> contains the following **ExchangeConfiguration8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		158
	MaximumNumber <MaxNb>	[0..1]	Quantity		159
	MaximumAmount <MaxAmt>	[0..1]	Amount		159
	ReTry <ReTry>	[0..1]	±		159
	TimeCondition <TmCond>	[0..1]			159
	StartTime <StartTm>	[0..1]	DateTime		159
	EndTime <EndTm>	[0..1]	DateTime		160
	Period <Prd>	[0..1]	Text		160

10.1.2.9.7.2.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 282

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.

CodeName	Name	Definition
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.

10.1.2.9.7.2.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 295

10.1.2.9.7.2.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 265

10.1.2.9.7.2.4 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.2.9.7.2.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following **ProcessTiming4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	StartTime <StartTm>	[0..1]	DateTime		159
	EndTime <EndTm>	[0..1]	DateTime		160
	Period <Prd>	[0..1]	Text		160

10.1.2.9.7.2.5.1 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODatetime" on page 294

10.1.2.9.7.2.5.2 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODateTime" on page 294

10.1.2.9.7.2.5.3 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 297

10.1.2.9.7.3 CompletionExchange <CmpltnXchg>

Presence: [0..1]

Definition: Configuration parameters of completion exchanges.

CompletionExchange <CmpltnXchg> contains the following **ExchangeConfiguration8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		160
	MaximumNumber <MaxNb>	[0..1]	Quantity		161
	MaximumAmount <MaxAmt>	[0..1]	Amount		161
	ReTry <ReTry>	[0..1]	±		161
	TimeCondition <TmCond>	[0..1]			161
	StartTime <StartTm>	[0..1]	DateTime		162
	EndTime <EndTm>	[0..1]	DateTime		162
	Period <Prd>	[0..1]	Text		162

10.1.2.9.7.3.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 282

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.

CodeName	Name	Definition
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.

10.1.2.9.7.3.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 295

10.1.2.9.7.3.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 265

10.1.2.9.7.3.4 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.2.9.7.3.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following **ProcessTiming4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	StartTime <StartTm>	[0..1]	DateTime		162
	EndTime <EndTm>	[0..1]	DateTime		162
	Period <Prd>	[0..1]	Text		162

10.1.2.9.7.3.5.1 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODatetime" on page 294

10.1.2.9.7.3.5.2 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODatetime" on page 294

10.1.2.9.7.3.5.3 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 297

10.1.2.9.7.4 CancellationExchange <CxlXchg>

Presence: [0..1]

Definition: Configuration of the cancellation exchanges.

Datatype: "CancellationProcess2Code" on page 275

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.

10.1.2.9.8 ReconciliationExchange <RcncltnXchg>

Presence: [0..1]

Definition: Configuration parameters of reconciliation exchanges.

ReconciliationExchange <RcncltnXchg> contains the following **ExchangeConfiguration8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ExchangePolicy <XchgPlcy>	[1..*]	CodeSet		163
	MaximumNumber <MaxNb>	[0..1]	Quantity		164
	MaximumAmount <MaxAmt>	[0..1]	Amount		164
	ReTry <ReTry>	[0..1]	±		164
	TimeCondition <TmCond>	[0..1]			164
	StartTime <StartTm>	[0..1]	DateTime		164
	EndTime <EndTm>	[0..1]	DateTime		164
	Period <Prd>	[0..1]	Text		164

10.1.2.9.8.1 ExchangePolicy <XchgPlcy>

Presence: [1..*]

Definition: Exchange policy between parties.

Datatype: "ExchangePolicy2Code" on page 282

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.

10.1.2.9.8.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of transactions without exchange.

Datatype: "Number" on page 295

10.1.2.9.8.3 MaximumAmount <MaxAmt>

Presence: [0..1]

Definition: Maximum cumulative amount of the transactions without exchange.

Datatype: "ImpliedCurrencyAndAmount" on page 265

10.1.2.9.8.4 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.2.9.8.5 TimeCondition <TmCond>

Presence: [0..1]

Definition: Timing condition for periodic exchanges.

TimeCondition <TmCond> contains the following **ProcessTiming4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	StartTime <StartTm>	[0..1]	DateTime		164
	EndTime <EndTm>	[0..1]	DateTime		164
	Period <Prd>	[0..1]	Text		164

10.1.2.9.8.5.1 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODateTime" on page 294

10.1.2.9.8.5.2 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODateTime" on page 294

10.1.2.9.8.5.3 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 297

10.1.2.9.9 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 295):

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

10.1.2.9.10 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 295):

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

10.1.2.9.11 SplitTotals <SplTtIs>

Presence: [0..1]

Definition: Indicates that totals in reconciliation or batch must be split per group of points of interaction and card product profiles when these information are present in the transactions.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 295):

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

10.1.2.9.12 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 295):

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

10.1.2.9.13 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 295):

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

10.1.2.9.14 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 295](#)):

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

10.1.2.9.15 BatchTransferContent <BtchTrfCntt>

Presence: [0..*]

Definition: Types of transaction to include in the batch.

Datatype: ["BatchTransactionType1Code" on page 275](#)

CodeName	Name	Definition
DTCT	DebitCredit	Debit and credit transactions.
CNCL	Cancellation	Cancellation of a previous transaction.
FAIL	Failed	Failed transactions.
DCLN	Declined	Declined transactions.

10.1.2.9.16 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 295](#)):

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

10.1.2.9.17 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 295](#)):

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

10.1.2.9.18 MessageItem <Msgltn>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <Msgltn> contains the following elements (see "[MessageItemCondition1](#)" on page 174 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemIdentification <ItmId>	[1..1]	Text		174
	Condition <Cond>	[1..1]	CodeSet		175
	Value <Val>	[0..*]	Text		175

10.1.2.9.19 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 295):

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

10.1.2.9.20 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 295):

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

10.1.2.9.21 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 295):

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

10.1.3 Identification Information

10.1.3.1 GenericIdentification176

Definition: Identification of an entity.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

10.1.3.1.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the entity.

Datatype: "Max35Text" on page 296

10.1.3.1.2 Type <Tp>

Presence: [0..1]

Definition: Type of identified entity.

Datatype: "PartyType33Code" on page 286

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	Delegatelssuer	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.

10.1.3.1.3 Issuer <Issr>

Presence: [0..1]

Definition: Entity assigning the identification (for example merchant, acceptor, acquirer, or tax authority).

Datatype: "PartyType33Code" on page 286

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	DelegatIssuer	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.

10.1.3.1.4 Country <Ctry>

Presence: [0..1]

Definition: Country of the entity (ISO 3166-1 alpha-2 or alpha-3).

Datatype: "Min2Max3AlphaText" on page 298

10.1.3.1.5 ShortName <ShrtNm>

Presence: [0..1]

Definition: Name of the entity.

Datatype: "Max35Text" on page 296

10.1.3.2 GenericIdentification177

Definition: Identification of an entity.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

10.1.3.2.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the entity.

Datatype: "Max35Text" on page 296

10.1.3.2.2 Type <Tp>

Presence: [0..1]

Definition: Type of identified entity.

Datatype: "PartyType33Code" on page 286

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	Delegatelssuer	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.

10.1.3.2.3 Issuer <Issr>

Presence: [0..1]

Definition: Entity assigning the identification (for example merchant, acceptor, acquirer, or tax authority).

Datatype: "PartyType33Code" on page 286

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	Delegatelssuer	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.

10.1.3.2.4 Country <Ctry>

Presence: [0..1]

Definition: Country of the entity (ISO 3166-1 alpha-2 or alpha-3).

Datatype: "Min2Max3AlphaText" on page 298

10.1.3.2.5 ShortName <ShrtNm>

Presence: [0..1]

Definition: Name of the entity.

Datatype: "Max35Text" on page 296

10.1.3.2.6 RemoteAccess <RmotAccs>

Presence: [0..1]

Definition: Access information to reach the target host.

RemoteAccess <RmotAccs> contains the following elements (see "[NetworkParameters7](#)" on [page 218](#) for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.3.2.7 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]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

10.1.3.2.7.1 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		173
	Longitude <Long>	[1..1]	Text		173

10.1.3.2.7.1.1 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 296

10.1.3.2.7.1.2 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 296

10.1.3.2.7.2 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		173
	UTMEastward <UTMEstwr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwr>	[1..1]	Text		174

10.1.3.2.7.2.1 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 296

10.1.3.2.7.2.2 UTMEastward <UTMEstwr>

Presence: [1..1]

Definition: X-coordinate of the Universal Transverse Mercator

coordinate system.

Datatype: "Max35Text" on page 296

10.1.3.2.7.2.3 UTMNorthward <UTMNrthwrd>

Presence: [1..1]

Definition: Y-coordinate of the Universal Transverse Mercator

coordinate system.

Datatype: "Max35Text" on page 296

10.1.4 Miscellaneous

10.1.4.1 MaintenanceldentificationAssociation1

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		174
	TMIdentification <TMId>	[1..1]	Text		174

10.1.4.1.1 MasterTMIdentification <MstrTMId>

Presence: [1..1]

Definition: Identifier for the master terminal manager.

Datatype: "Max35Text" on page 296

10.1.4.1.2 TMIdentification <TMId>

Presence: [1..1]

Definition: Identifier for the terminal manager requesting the delegation.

Datatype: "Max35Text" on page 296

10.1.4.2 MessageItemCondition1

Definition: Presence condition of a message item.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemIdentification <ItmId>	[1..1]	Text		174
	Condition <Cond>	[1..1]	CodeSet		175
	Value <Val>	[0..*]	Text		175

10.1.4.2.1 ItemIdentification <ItmId>

Presence: [1..1]

Definition: Unique identification of the message and the message item.

Datatype: "Max140Text" on page 296

10.1.4.2.2 Condition <Cond>

Presence: [1..1]

Definition: Condition of presence of the message item.

Datatype: "MessageItemCondition1Code" on page 285

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.

10.1.4.2.3 Value <Val>

Presence: [0..*]

Definition: Value to be used for the message item.

Datatype: "Max140Text" on page 296

10.1.4.3 MaintenanceDelegateAction5

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		177
	TMRemoteAccess <TMRmotAccs>	[0..1]	±		177
	TMSProtocol <TMSPrtcol>	[0..1]	Text		177
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		178
	DataSetIdentification <DataSetId>	[0..1]	±		178
	ReTry <ReTry>	[0..1]	±		178
	AdditionalInformation <AddtlInf>	[0..*]	Binary		178
	Action <Actn>	[0..*]			178
	Type <Tp>	[1..1]	CodeSet		179
	RemoteAccess <RmotAccs>	[0..1]	±		180
	Key <Key>	[0..*]			181
	KeyIdentification <KeyId>	[1..1]	Text		181
	KeyVersion <KeyVrsn>	[1..1]	Text		181
	SequenceNumber <SeqNb>	[0..1]	Quantity		181
	DerivationIdentification <DerivtnId>	[0..1]	Binary		181
	Type <Tp>	[0..1]	CodeSet		181
	Function <Fctn>	[0..*]	CodeSet		182
	TerminalManagerIdentification <TermnlMgrId>	[0..1]	±		183
	TMSProtocol <TMSPrtcol>	[0..1]	Text		183
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		183
	DataSetIdentification <DataSetId>	[0..1]	±		183
	ComponentType <CmpntTp>	[0..*]	CodeSet		184
	DelegationScopelIdentification <DlgttnScplId>	[0..1]	Text		185
	DelegationScopeDefinition <DlgttnScpDef>	[0..1]	Binary		185
	DelegationProof <DlgttnProof>	[0..1]	Binary		185
	ProtectedDelegationProof <PrctcdDlgttnProof>	[0..1]	±		185
	Trigger <Trggr>	[1..1]	CodeSet		186
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		186
	ReTry <ReTry>	[0..1]	±		186
	TimeCondition <TmCond>	[0..1]	±		187
	TMChallenge <TMChllng>	[0..1]	Binary		187

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		187
	ErrorAction <ErrActn>	[0..*]	±		187
	AdditionalInformation <AddtlInf>	[0..*]	Binary		187
	MessageItem <Msgltn>	[0..*]	±		188

10.1.4.3.1 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 295):

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

10.1.4.3.2 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 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.4.3.3 TMSProtocol <TMSPrtcol>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.4.3.4 TMSProtocolVersion <TMSPrtcolVrsn>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.4.3.5 DataSetIdentification <DataSetId>

Presence: [0..1]

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

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification8" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

10.1.4.3.6 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "ProcessRetry2" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.4.3.7 AdditionalInformation <AddtlInf>

Presence: [0..*]

Definition: Additional information to include in the maintenance action.

Datatype: "Max3000Binary" on page 266

10.1.4.3.8 Action <Actn>

Presence: [0..*]

Definition: Sequence of action to include in the next MTM management plan.

Action <Actn> contains the following **TMSAction8** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Type <Tp>	[1..1]	CodeSet		179
	RemoteAccess <RmotAccs>	[0..1]	±		180
	Key <Key>	[0..*]			181
	KeyIdentification <KeyId>	[1..1]	Text		181
	KeyVersion <KeyVrsn>	[1..1]	Text		181
	SequenceNumber <SeqNb>	[0..1]	Quantity		181
	DerivationIdentification <DerivtnId>	[0..1]	Binary		181
	Type <Tp>	[0..1]	CodeSet		181
	Function <Fctn>	[0..*]	CodeSet		182
	TerminalManagerIdentification <TermnlMgrld>	[0..1]	±		183
	TMSProtocol <TMSPrtcol>	[0..1]	Text		183
	TMSProtocolVersion <TMSPrtcolVrsn>	[0..1]	Text		183
	DataSetIdentification <DataSetId>	[0..1]	±		183
	ComponentType <CmpntTp>	[0..*]	CodeSet		184
	DelegationScopeIdentification <DlgtScpld>	[0..1]	Text		185
	DelegationScopeDefinition <DlgtScpDef>	[0..1]	Binary		185
	DelegationProof <DlgtProof>	[0..1]	Binary		185
	ProtectedDelegationProof <PrtctdDlgtProof>	[0..1]	±		185
	Trigger <Trggr>	[1..1]	CodeSet		186
	AdditionalProcess <AddtlPrc>	[0..*]	CodeSet		186
	ReTry <ReTry>	[0..1]	±		186
	TimeCondition <TmCond>	[0..1]	±		187
	TMChallenge <TMChllng>	[0..1]	Binary		187
	KeyEnciphermentCertificate <KeyNcphrmntCert>	[0..*]	Binary		187
	ErrorAction <ErrActn>	[0..*]	±		187
	AdditionalInformation <AddtlInf>	[0..*]	Binary		187
	MessageItem <Msgltn>	[0..*]	±		188

10.1.4.3.8.1 Type <Tp>

Presence: [1..1]

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

Datatype: "TerminalManagementAction4Code" on page 291

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.

10.1.4.3.8.2 RemoteAccess <RmotAccs>

Presence: [0..1]

Definition: Host access information.

RemoteAccess <RmotAccs> contains the following elements (see "[NetworkParameters7](#)" on page 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <CIntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.4.3.8.3 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		181
	KeyVersion <KeyVrsn>	[1..1]	Text		181
	SequenceNumber <SeqNb>	[0..1]	Quantity		181
	DerivationIdentification <DerivtnId>	[0..1]	Binary		181
	Type <Tp>	[0..1]	CodeSet		181
	Function <Fctr>	[0..*]	CodeSet		182

10.1.4.3.8.3.1 KeyIdentification <KeyId>

Presence: [1..1]

Definition: Identification of the cryptographic key.

Datatype: "Max140Text" on page 296

10.1.4.3.8.3.2 KeyVersion <KeyVrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max140Text" on page 296

10.1.4.3.8.3.3 SequenceNumber <SeqNb>

Presence: [0..1]

Definition: Number of usages of the cryptographic key.

Datatype: "Number" on page 295

10.1.4.3.8.3.4 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 267

10.1.4.3.8.3.5 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 278

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).

10.1.4.3.8.3.6 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 283

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	TranslatelInput	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.

10.1.4.3.8.4 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

10.1.4.3.8.5 TMSProtocol <TMSPrtcol>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.4.3.8.6 TMSProtocolVersion <TMSPrtcolVrsn>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.4.3.8.7 DataSetIdentification <DataSetId>

Presence: [0..1]

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

DataSetIdentification <DataSetId> contains the following elements (see "DataSetIdentification8" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

10.1.4.3.8.8 ComponentType <CmpntTp>

Presence: [0..*]

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

Datatype: "DataSetCategory14Code" on page 280

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.
SOFT	SoftwareApplication	Software Application or module of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

10.1.4.3.8.9 DelegationScopelIdentification <DlgnScpld>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.4.3.8.10 DelegationScopeDefinition <DlgnScpDef>

Presence: [0..1]

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

Datatype: "Max3000Binary" on page 266

10.1.4.3.8.11 DelegationProof <DlgnProof>

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 266

10.1.4.3.8.12 ProtectedDelegationProof <PrctdDlgnProof>

Presence: [0..1]

Definition: Protected proof of delegation.

ProtectedDelegationProof <PrtctdDlgtProof> contains the following elements (see "ContentInformationType23" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

10.1.4.3.8.13 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 293

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.

10.1.4.3.8.14 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 293

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.

10.1.4.3.8.15 ReTry <ReTry>

Presence: [0..1]

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

ReTry <ReTry> contains the following elements (see "[ProcessRetry2](#)" on page 263 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Delay <Dely>	[1..1]	Text		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.4.3.8.16 TimeCondition <TmCond>

Presence: [0..1]

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

TimeCondition <TmCond> contains the following elements (see "[ProcessTiming3](#)" on page 264 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	WaitingTime <WtgTm>	[0..1]	Text		264
	StartTime <StartTm>	[0..1]	DateTime		264
	EndTime <EndTm>	[0..1]	DateTime		264
	Period <Prd>	[0..1]	Text		264
	MaximumNumber <MaxNb>	[0..1]	Quantity		264

10.1.4.3.8.17 TMChallenge <TMChllng>

Presence: [0..1]

Definition: Terminal manager challenge for cryptographic key injection.

Datatype: "[Max140Binary](#)" on page 266

10.1.4.3.8.18 KeyEnciphermentCertificate <KeyNcphrmntCert>

Presence: [0..*]

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

Datatype: "[Max10KBinary](#)" on page 265

10.1.4.3.8.19 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 "[ErrorAction4](#)" on page 216 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionResult <ActnRslt>	[1..*]	CodeSet		217
	ActionToProcess <ActnToPrc>	[1..1]	CodeSet		218

10.1.4.3.8.20 AdditionalInformation <AddtlInf>

Presence: [0..*]

Definition: Additional information about the maintenance action.

Datatype: "Max3000Binary" on page 266

10.1.4.3.8.21 MessageItem <Msgltm>

Presence: [0..*]

Definition: Configuration of a message item.

MessageItem <Msgltm> contains the following elements (see "MessageItemCondition1" on page 174 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemIdentification <ItmId>	[1..1]	Text		174
	Condition <Cond>	[1..1]	CodeSet		175
	Value <Val>	[0..*]	Text		175

10.1.4.4 DataSetIdentification8

Definition: Identification of a data set.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

10.1.4.4.1 Name <Nm>

Presence: [0..1]

Definition: Name of the data set.

Datatype: "Max256Text" on page 296

10.1.4.4.2 Type <Tp>

Presence: [1..1]

Definition: Category of data set.

Datatype: "DataSetCategory14Code" on page 280

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).

CodeName	Name	Definition
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.
CMRQ	CertificateManagementRequest	Trigger for CertificateManagementRequest.
MDFL	MediaFile	Media file managed by an application of the POI.
SOFT	SoftwareApplication	Software Application or module of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

10.1.4.4.3 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data set.

Datatype: "Max256Text" on page 296

10.1.4.4.4 CreationDateTime <CreDtTm>

Presence: [0..1]

Definition: Date and time of creation of the data set.

Datatype: "ISODateTime" on page 294

10.1.4.5 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		190
	CardholderVerificationCapabilities <CrhdldrVrfctnCpblties>	[0..*]	CodeSet		191
	PINLengthCapabilities <PINLnghCpblties>	[0..1]	Quantity		191
	ApprovalCodeLength <ApprvICdLngh>	[0..1]	Quantity		192
	MaxScriptLength <MxScrptLngh>	[0..1]	Quantity		192
	CardCaptureCapable <CardCaptrCpbl>	[0..1]	Indicator		192
	OnLineCapabilities <OnLineCpblties>	[0..1]	CodeSet		192
	MessageCapabilities <MsgCpblties>	[0..*]			192
	Destination <Dstn>	[1..*]	CodeSet		193
	AvailableFormat <AvlblFrmt>	[0..*]	CodeSet		193
	NumberOfLines <NbOfLines>	[0..1]	Quantity		193
	LineWidth <LineWidth>	[0..1]	Quantity		193
	AvailableLanguage <AvlblLang>	[0..*]	CodeSet	C1	194

10.1.4.5.1 CardReadingCapabilities <CardRdngCpblties>

Presence: [0..*]

Definition: Card reading capabilities of the POI (Point Of Interaction) performing the transaction.

Datatype: "CardDataReading8Code" on page 276

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.

CodeName	Name	Definition
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.)

10.1.4.5.2 CardholderVerificationCapabilities <CrdhldrVrfctnCpblties>

Presence: [0..*]

Definition: Cardholder verification capabilities of the POI (Point Of Interaction) performing the transaction.

Datatype: "CardholderVerificationCapability4Code" on page 276

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.

10.1.4.5.3 PINLengthCapabilities <PINLnghCpblties>

Presence: [0..1]

Definition: Maximum number of digits the POI is able to accept when the cardholder enters its PIN.

Datatype: "PositiveNumber" on page 295

10.1.4.5.4 ApprovalCodeLength <ApprvlCdLngh>

Presence: [0..1]

Definition: Maximum number of characters of the approval code the POI is able to manage.

Datatype: "PositiveNumber" on page 295

10.1.4.5.5 MaxScriptLength <MxScrpLtLngh>

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 295

10.1.4.5.6 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 295):

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

10.1.4.5.7 OnLineCapabilities <OnLineCpblties>

Presence: [0..1]

Definition: On-line and off-line capabilities of the POI (Point Of Interaction).

Datatype: "OnLineCapability1Code" on page 286

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.

10.1.4.5.8 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		193
	AvailableFormat <AvlblFrmt>	[0..*]	CodeSet		193
	NumberOfLines <NbOfLines>	[0..1]	Quantity		193
	LineWidth <LineWidth>	[0..1]	Quantity		193
	AvailableLanguage <AvlblLang>	[0..*]	CodeSet	C1	194

10.1.4.5.8.1 Destination <Dstn>

Presence: [1..*]

Definition: Destination of the message to present.

Datatype: "UserInterface4Code" on page 294

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.

10.1.4.5.8.2 AvailableFormat <AvlblFrmt>

Presence: [0..*]

Definition: Available message format.

Datatype: "OutputFormat1Code" on page 286

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.

10.1.4.5.8.3 NumberOfLines <NbOfLines>

Presence: [0..1]

Definition: Number of lines of the display.

Datatype: "Number" on page 295

10.1.4.5.8.4 LineWidth <LineWidth>

Presence: [0..1]

Definition: Number of columns of the display or printer.

Datatype: "Number" on page 295

10.1.4.5.8.5 AvailableLanguage <AvlblLang>

Presence: [0..*]

Definition: Available language for the message. Reference ISO 639-1 (alpha-2) et ISO 639-2 (alpha-3).

Impacted by: C1 "ValidationByTable"

Datatype: "LanguageCode" on page 284

Constraints

- **ValidationByTable**

Must be a valid terrestrial language.

10.1.4.6 PointOfInteractionComponent10

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		196
	SubTypeInfoInformation <SubTpInf>	[0..1]	Text		197
	Identification <Id>	[1..1]			198
	ItemNumber <ItmNb>	[0..1]	Text		198
	ProviderIdentification <PrvdrlId>	[0..1]	Text		198
	Identification <Id>	[0..1]	Text		198
	SerialNumber <SrlNb>	[0..1]	Text		198
	Status <Sts>	[0..1]			198
	VersionNumber <VrsnNb>	[0..1]	Text		199
	Status <Sts>	[0..1]	CodeSet		199
	ExpiryDate <XpryDt>	[0..1]	Date		199
	StandardCompliance <StdCmplc>	[0..*]			199
	Identification <Id>	[1..1]	Text		199
	Version <Vrsn>	[1..1]	Text		200
	Issuer <Issr>	[1..1]	Text		200
	Characteristics <Chrtcs>	[0..1]			200
	Memory <Mmry>	[0..*]			201
	Identification <Id>	[1..1]	Text		202
	TotalSize <TtlSz>	[1..1]	Quantity		202
	FreeSize <FreeSz>	[1..1]	Quantity		202
	Unit <Unit>	[1..1]	CodeSet		202
	Communication <Com>	[0..*]			202
	CommunicationType <ComTp>	[1..1]	CodeSet		203
	RemoteParty <RmotPty>	[1..*]	CodeSet		204
	Active <Actv>	[1..1]	Indicator		204
	Parameters <Params>	[0..1]	±		204
	PhysicalInterface <PhysIntrfc>	[0..1]			205
	InterfaceName <IntrfcNm>	[1..1]	Text		205
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		205
	UserName <UsrNm>	[0..1]	Text		206
	AccessCode <AccsCd>	[0..1]	Binary		206

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	SecurityProfile <SctyPrfl>	[0..1]	Text		206
	AdditionalParameters <AddtlParams>	[0..1]	Binary		206
	SecurityAccessModules <SctyAccsMdl>	[0..1]	Quantity		207
	SubscriberIdentityModules <SbcbrldntyMdl>	[0..1]	Quantity		207
	SecurityElement <SctyElmt>	[0..*]	±		207
	Assessment <Assmnt>	[0..*]			207
	Type <Tp>	[1..1]	CodeSet		208
	Assigner <Assgnr>	[1..*]	Text		208
	DeliveryDate <DlvryDt>	[0..1]	DateTime		208
	ExpirationDate <XprtnDt>	[0..1]	DateTime		208
	Number <Nb>	[1..1]	Text		208
	Package <Packg>	[0..*]			209
	PackageIdentification <PackgId>	[0..1]	±		209
	PackageLength <PackgLngh>	[0..1]	Quantity		209
	OffsetStart <OffsetStart>	[0..1]	Quantity		209
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		210
	PackageBlock <PackgBlck>	[0..*]			210
	Identification <Id>	[1..1]	Text		210
	Value <Val>	[0..1]	Binary		210
	ProtectedValue <PrtctdVal>	[0..1]	±		210
	Type <Tp>	[0..1]	Text		211

10.1.4.6.1 Type <Tp>

Presence: [1..1]

Definition: Type of component belonging to a POI (Point Of Interaction) Terminal.

Datatype: "POIComponentType6Code" on page 289

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.

10.1.4.6.2 SubTypeInformation <SubTpInf>

Presence: [0..1]

Definition: Additional information regarding the type of the component.

Datatype: "Max70Text" on page 297

10.1.4.6.3 Identification <Id>

Presence: [1..1]

Definition: Identification of the POI (Point Of Interaction) component.

Identification <Id> contains the following **PointOfInteractionComponentIdentification1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ItemNumber <ItmNb>	[0..1]	Text		198
	ProviderIdentification <PrvdrId>	[0..1]	Text		198
	Identification <Id>	[0..1]	Text		198
	SerialNumber <SrlNb>	[0..1]	Text		198

10.1.4.6.3.1 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 296

10.1.4.6.3.2 ProviderIdentification <PrvdrId>

Presence: [0..1]

Definition: Identifies the provider of the software, hardware or parameters of the POI component.

Datatype: "Max35Text" on page 296

10.1.4.6.3.3 Identification <Id>

Presence: [0..1]

Definition: Identification of the POI component assigned by its provider.

Datatype: "Max35Text" on page 296

10.1.4.6.3.4 SerialNumber <SrlNb>

Presence: [0..1]

Definition: Serial number identifying an occurrence of an hardware component.

Datatype: "Max35Text" on page 296

10.1.4.6.4 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		199
	Status <Sts>	[0..1]	CodeSet		199
	ExpiryDate <XpryDt>	[0..1]	Date		199

10.1.4.6.4.1 VersionNumber <VrsnNb>

Presence: [0..1]

Definition: Current version of the component that might include the release number.

Datatype: "Max256Text" on page 296

10.1.4.6.4.2 Status <Sts>

Presence: [0..1]

Definition: Current status of the component.

Datatype: "POIComponentStatus1Code" on page 289

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.

10.1.4.6.4.3 ExpiryDate <XpryDt>

Presence: [0..1]

Definition: Expiration date of the component.

Datatype: "ISODate" on page 294

10.1.4.6.5 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		199
	Version <Vrsn>	[1..1]	Text		200
	Issuer <Issr>	[1..1]	Text		200

10.1.4.6.5.1 Identification <Id>

Presence: [1..1]

Definition: Proprietary information, often a code, issued by the data source scheme issuer.

Datatype: "Max35Text" on page 296

10.1.4.6.5.2 Version <Vrsn>

Presence: [1..1]

Definition: Version of the identification.

Datatype: "Max35Text" on page 296

10.1.4.6.5.3 Issuer <Issr>

Presence: [1..1]

Definition: Entity that assigns the identification.

Datatype: "Max35Text" on page 296

10.1.4.6.6 Characteristics <Chrtcs>

Presence: [0..1]

Definition: Characteristics of a POI (Point Of Interaction) component.

Characteristics <Chrtcs> contains the following **PointOfInteractionComponentCharacteristics6** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Memory <Mmry>	[0..*]			201
	Identification <Id>	[1..1]	Text		202
	TotalSize <TtlSz>	[1..1]	Quantity		202
	FreeSize <FreeSz>	[1..1]	Quantity		202
	Unit <Unit>	[1..1]	CodeSet		202
	Communication <Com>	[0..*]			202
	CommunicationType <ComTp>	[1..1]	CodeSet		203
	RemoteParty <RmotPty>	[1..*]	CodeSet		204
	Active <Actv>	[1..1]	Indicator		204
	Parameters <Params>	[0..1]	±		204
	PhysicalInterface <PhysIntrfc>	[0..1]			205
	InterfaceName <IntrfcNm>	[1..1]	Text		205
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		205
	UserName <UsrNm>	[0..1]	Text		206
	AccessCode <AccsCd>	[0..1]	Binary		206
	SecurityProfile <SctyPrfl>	[0..1]	Text		206
	AdditionalParameters <AddtlParams>	[0..1]	Binary		206
	SecurityAccessModules <SctyAccsMdl>	[0..1]	Quantity		207
	SubscriberIdentityModules <SbcbrldntyMdl>	[0..1]	Quantity		207
	SecurityElement <SctyElmt>	[0..*]	±		207

10.1.4.6.6.1 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		202
	TotalSize <TtlSz>	[1..1]	Quantity		202
	FreeSize <FreeSz>	[1..1]	Quantity		202
	Unit <Unit>	[1..1]	CodeSet		202

10.1.4.6.6.1.1 Identification <Id>

Presence: [1..1]

Definition: Identification or name of the memory.

Datatype: "Max35Text" on page 296

10.1.4.6.6.1.2 TotalSize <TtISz>

Presence: [1..1]

Definition: Total size of the memory unit.

Datatype: "DecimalNumber" on page 295

10.1.4.6.6.1.3 FreeSize <FreeSz>

Presence: [1..1]

Definition: Total size of the available memory.

Datatype: "DecimalNumber" on page 295

10.1.4.6.6.1.4 Unit <Unit>

Presence: [1..1]

Definition: Memory unit of the sizes.

Datatype: "MemoryUnit1Code" on page 284

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.

10.1.4.6.6.2 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		203
	RemoteParty <RmotPty>	[1..*]	CodeSet		204
	Active <Actv>	[1..1]	Indicator		204
	Parameters <Params>	[0..1]	±		204
	PhysicalInterface <PhysIntrfc>	[0..1]			205
	InterfaceName <IntrfcNm>	[1..1]	Text		205
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		205
	UserName <UsrNm>	[0..1]	Text		206
	AccessCode <AccsCd>	[0..1]	Binary		206
	SecurityProfile <SctyPrfl>	[0..1]	Text		206
	AdditionalParameters <AddtlParams>	[0..1]	Binary		206

10.1.4.6.6.2.1 CommunicationType <ComTp>

Presence: [1..1]

Definition: Type of low level communication.

Datatype: "POICommunicationType2Code" on page 288

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.

10.1.4.6.6.2.2 RemoteParty <RmotPty>

Presence: [1..*]

Definition: Entity that communicate with the current component, using this communication device.

Datatype: "PartyType7Code" on page 287

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.

10.1.4.6.6.2.3 Active <Actv>

Presence: [1..1]

Definition: Communication hardware is activated.

Datatype: One of the following values must be used (see "TrueFalseIndicator" on page 295):

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

10.1.4.6.6.2.4 Parameters <Params>

Presence: [0..1]

Definition: Network parameters of the communication link.

Parameters <Params> contains the following elements (see "[NetworkParameters7](#)" on page 218 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertldr>	[0..*]	Binary		219
	ClientCertificate <ClntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.4.6.6.2.5 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		205
	InterfaceType <IntrfcTp>	[0..1]	CodeSet		205
	UserName <UsrNm>	[0..1]	Text		206
	AccessCode <AccsCd>	[0..1]	Binary		206
	SecurityProfile <SctyPrfl>	[0..1]	Text		206
	AdditionalParameters <AddtlParams>	[0..1]	Binary		206

10.1.4.6.6.2.5.1 InterfaceName <IntrfcNm>

Presence: [1..1]

Definition: Identification of the interface.

Datatype: "[Max35Text](#)" on page 296

10.1.4.6.6.2.5.2 InterfaceType <IntrfcTp>

Presence: [0..1]

Definition: Identification of the physical link layer.

Datatype: "[POICommunicationType2Code](#)" on page 288

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.

10.1.4.6.6.2.5.3 UserName <UsrNm>

Presence: [0..1]

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

Datatype: "Max35Text" on page 296

10.1.4.6.6.2.5.4 AccessCode <AccsCd>

Presence: [0..1]

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

Datatype: "Max35Binary" on page 266

10.1.4.6.6.2.5.5 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the optional security profile to use with this interface.

Datatype: "Max35Text" on page 296

10.1.4.6.6.2.5.6 AdditionalParameters <AddtlParams>

Presence: [0..1]

Definition: Any other parameters relevant for this interface.

Datatype: "Max2KBinary" on page 266

10.1.4.6.6.3 SecurityAccessModules <SctyAccsMdl>

Presence: [0..1]

Definition: Number of security access modules (SAM).

Datatype: "Number" on page 295

10.1.4.6.6.4 SubscriberIdentityModules <SbcbrldntyMdl>

Presence: [0..1]

Definition: Number of subscriber identity modules (SIM).

Datatype: "Number" on page 295

10.1.4.6.6.5 SecurityElement <SctyElmt>

Presence: [0..*]

Definition: Security characteristics of the component.

SecurityElement <SctyElmt> contains the following elements (see "CryptographicKey14" on page 221 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		221
	AdditionalIdentification <AddtlId>	[0..1]	Binary		222
	Name <Nm>	[0..1]	Text		222
	SecurityProfile <SctyPrfl>	[0..1]	Text		222
	ItemNumber <ItmNb>	[0..1]	Text		222
	Version <Vrsn>	[1..1]	Text		222
	Type <Tp>	[0..1]	CodeSet		222
	Function <Fctn>	[0..*]	CodeSet		223
	ActivationDate <ActvtnDt>	[0..1]	DateTime		224
	DeactivationDate <DeactvtnDt>	[0..1]	DateTime		224
	KeyValue <KeyVal>	[0..1]	±		224
	KeyCheckValue <KeyChckVal>	[0..1]	Binary		224
	AdditionalManagementInformation <AddtlMgmtInf>	[0..*]			224
	Name <Nm>	[1..1]	Text		225
	Value <Val>	[0..1]	Text		225

10.1.4.6.7 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		208
	Assigner <Assgnr>	[1..*]	Text		208
	DeliveryDate <DlvryDt>	[0..1]	DateTime		208
	ExpirationDate <XprtnDt>	[0..1]	DateTime		208
	Number <Nb>	[1..1]	Text		208

10.1.4.6.7.1 Type <Tp>

Presence: [1..1]

Definition: Type of assessment of the component.

Datatype: "POIComponentAssessment1Code" on page 289

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.

10.1.4.6.7.2 Assigner <Assgnr>

Presence: [1..*]

Definition: Body which has delivered the assessment.

Datatype: "Max35Text" on page 296

10.1.4.6.7.3 DeliveryDate <DlvryDt>

Presence: [0..1]

Definition: Date when the assessment has been delivered.

Datatype: "ISODateTime" on page 294

10.1.4.6.7.4 ExpirationDate <XprtnDt>

Presence: [0..1]

Definition: Date when the assessment will expire.

Datatype: "ISODateTime" on page 294

10.1.4.6.7.5 Number <Nb>

Presence: [1..1]

Definition: Unique assessment number for the component.

Datatype: "Max35Text" on page 296

10.1.4.6.8 Package <Packg>

Presence: [0..*]

Definition: Chunk of a software package.

Package <Packg> contains the following **PackageType1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	PackageIdentification <PackgId>	[0..1]	±		209
	PackageLength <PackgLngh>	[0..1]	Quantity		209
	OffsetStart <OffsetStart>	[0..1]	Quantity		209
	OffsetEnd <OffsetEnd>	[0..1]	Quantity		210
	PackageBlock <PackgBlck>	[0..*]			210
	Identification <Id>	[1..1]	Text		210
	Value <Val>	[0..1]	Binary		210
	ProtectedValue <PrctcdVal>	[0..1]	±		210
	Type <Tp>	[0..1]	Text		211

10.1.4.6.8.1 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 167 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		168
	Type <Tp>	[0..1]	CodeSet		168
	Issuer <Issr>	[0..1]	CodeSet		168
	Country <Ctry>	[0..1]	Text		169
	ShortName <ShrtNm>	[0..1]	Text		169

10.1.4.6.8.2 PackageLength <PackgLngh>

Presence: [0..1]

Definition: Full length of software package identified through PackageIdentification.

Datatype: "[PositiveNumber](#)" on page 295

10.1.4.6.8.3 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 295

10.1.4.6.8.4 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 295

10.1.4.6.8.5 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 **ExternallyDefinedData1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		210
	Value <Val>	[0..1]	Binary		210
	ProtectedValue <PrctcdVal>	[0..1]	±		210
	Type <Tp>	[0..1]	Text		211

10.1.4.6.8.5.1 Identification <Id>

Presence: [1..1]

Definition: Identification of the set of data to exchange.

Datatype: "Max1025Text" on page 296

10.1.4.6.8.5.2 Value <Val>

Presence: [0..1]

Definition: Data to exchange according to an external standard.

Datatype: "Max100KBinary" on page 265

10.1.4.6.8.5.3 ProtectedValue <PrctcdVal>

Presence: [0..1]

Definition: Protection of the values to exchange.

ProtectedValue <PrtctdVal> contains the following elements (see "[ContentInformationType23](#)" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

10.1.4.6.8.5.4 Type <Tp>

Presence: [0..1]

Definition: Identification of the standard used to encode the values to exchange.

Datatype: "[Max1025Text](#)" on page 296

10.1.4.7 EncapsulatedContent3

Definition: Data to authenticate.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		211
	Content <Cntt>	[0..1]	Binary		212

10.1.4.7.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data which have been authenticated.

Datatype: "[ContentType2Code](#)" on page 277

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).

10.1.4.7.2 Content <Cntt>

Presence: [0..1]

Definition: Actual data to authenticate.

Datatype: "Max100KBinary" on page 265

10.1.5 Monitoring

10.1.5.1 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]	±		212
	ProtocolName <PrtcolNm>	[0..1]	Text		213
	ProtocolVersion <PrtcolVrsn>	[0..1]	Text		213
	TraceDateTimeIn <TracDtTmIn>	[1..1]	DateTime		213
	TraceDateTimeOut <TracDtTmOut>	[1..1]	DateTime		213

10.1.5.1.1 RelayIdentification <RlayId>

Presence: [1..1]

Definition: Identification of a partner of a message exchange.

RelayIdentification <RlyId> contains the following elements (see "[GenericIdentification177](#)" on page 169 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		170
	Type <Tp>	[0..1]	CodeSet		170
	Issuer <Issr>	[0..1]	CodeSet		171
	Country <Ctry>	[0..1]	Text		171
	ShortName <ShrtNm>	[0..1]	Text		171
	RemoteAccess <RmotAccs>	[0..1]	±		172
	Geolocation <Glctn>	[0..1]			172
	GeographicCoordinates <GeogcCordints>	[0..1]			172
	Latitude <Lat>	[1..1]	Text		173
	Longitude <Long>	[1..1]	Text		173
	UTMCoordinates <UTMCordints>	[0..1]			173
	UTMZone <UTMZone>	[1..1]	Text		173
	UTMEastward <UTMEstwrdr>	[1..1]	Text		173
	UTMNorthward <UTMNrthwrdr>	[1..1]	Text		174

10.1.5.1.2 ProtocolName <PrtcolNm>

Presence: [0..1]

Definition: Name of the outgoing protocol used by the node.

Datatype: "[Max35Text](#)" on page 296

10.1.5.1.3 ProtocolVersion <PrtcolVrsn>

Presence: [0..1]

Definition: Version of the protocol.

Datatype: "[Max6Text](#)" on page 297

10.1.5.1.4 TraceDateTimeln <TracDtTmln>

Presence: [1..1]

Definition: Date and time of incoming data exchange for relaying or processing.

Datatype: "[ISODateTime](#)" on page 294

10.1.5.1.5 TraceDateTimeOut <TracDtTmOut>

Presence: [1..1]

Definition: Date and time of the outgoing exchange for relaying or processing.

Datatype: "[ISODateTime](#)" on page 294

10.1.5.2 TMSEvent7

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		214
	Result <RsIt>	[1..1]	CodeSet		214
	ActionIdentification <ActnId>	[1..1]			215
	ActionType <ActnTp>	[1..1]	CodeSet		215
	DataSetIdentification <DataSetId>	[0..1]	±		216
	AdditionalErrorInformation <AddtlErrInf>	[0..1]	Text		216
	TerminalManagerIdentification <TermnlMgrld>	[0..1]	Text		216

10.1.5.2.1 TimeStamp <TmStmp>

Presence: [1..1]

Definition: Date time of the terminal management action performed by the point of interaction.

Datatype: "ISODatetime" on page 294

10.1.5.2.2 Result <RsIt>

Presence: [1..1]

Definition: Final result of the processed terminal management action.

Datatype: "TerminalManagementActionResult4Code" on page 292

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.
SUCC	Success	Action was successfully performed.
SYNE	SyntaxError	Data transferred has a wrong syntax.
TIMO	Timeout	Timeout expired during the data transfer.
UKDT	UnknownData	Data set identification invalid.

CodeName	Name	Definition
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.

10.1.5.2.3 ActionIdentification <ActnId>

Presence: [1..1]

Definition: Identification of the terminal management action performed by the point of interaction.

ActionIdentification <ActnId> contains the following **TMSActionIdentification6** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ActionType <ActnTp>	[1..1]	CodeSet		215
	DataSetIdentification <DataSetId>	[0..1]	±		216

10.1.5.2.3.1 ActionType <ActnTp>

Presence: [1..1]

Definition: Types of terminal management action performed by a point of interaction.

Datatype: "TerminalManagementAction4Code" on page 291

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.

CodeName	Name	Definition
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.

10.1.5.2.3.2 DataSetIdentification <DataSetId>

Presence: [0..1]

Definition: Data set on which the action has been performed.

DataSetIdentification <DataSetId> contains the following elements (see "[DataSetIdentification8](#)" on page 188 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Name <Nm>	[0..1]	Text		188
	Type <Tp>	[1..1]	CodeSet		188
	Version <Vrsn>	[0..1]	Text		189
	CreationDateTime <CreDtTm>	[0..1]	DateTime		189

10.1.5.2.4 AdditionalErrorInformation <AddtlErrInf>

Presence: [0..1]

Definition: Additional information related to a failure.

Datatype: "[Max70Text](#)" on page 297

10.1.5.2.5 TerminalManagerIdentification <TermnlMgrId>

Presence: [0..1]

Definition: Identification of the terminal management system (TMS) used with the action.

Datatype: "[Max35Text](#)" on page 296

10.1.5.3 ErrorAction4

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		217
	ActionToProcess <ActnPrc>	[1..1]	CodeSet		218

10.1.5.3.1 ActionResult <ActnRslt>

Presence: [1..*]

Definition: List of error action result codes.

Datatype: "TerminalManagementActionResult4Code" on page 292

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.
SUCC	Success	Action was successfully performed.
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.

CodeName	Name	Definition
ULER	UnlistedError	Any error that is not defined by a code value inside the TerminalManagementActionResultCode.

10.1.5.3.2 ActionToProcess <ActnPrc>

Presence: [1..1]

Definition: Action to be processed for the related errors.

Datatype: "TerminalManagementErrorAction2Code" on page 293

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.

10.1.6 Network Access

10.1.6.1 NetworkParameters7

Definition: Parameters to communicate with a host.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Address <Adr>	[1..*]			218
	NetworkType <NtwkTp>	[1..1]	CodeSet		219
	AddressValue <AdrVal>	[1..1]	Text		219
	UserName <UsrNm>	[0..1]	Text		219
	AccessCode <AccsCd>	[0..1]	Binary		219
	ServerCertificate <SvrCert>	[0..*]	Binary		219
	ServerCertificateIdentifier <SvrCertIdr>	[0..*]	Binary		219
	ClientCertificate <ClntCert>	[0..*]	Binary		220
	SecurityProfile <SctyPrfl>	[0..1]	Text		220

10.1.6.1.1 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		219
	AddressValue <AdrVal>	[1..1]	Text		219

10.1.6.1.1.1 NetworkType <NtwkTp>

Presence: [1..1]

Definition: Type of communication network.

Datatype: "NetworkType1Code" on page 285

CodeName	Name	Definition
IPNW	InternetProtocol	Protocol of an IP network.
PSTN	PublicTelephone	Protocol of a Public Switched Telephone Network (PSTN).

10.1.6.1.1.2 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 297

10.1.6.1.2 UserName <UsrNm>

Presence: [0..1]

Definition: User name identifying the client.

Datatype: "Max35Text" on page 296

10.1.6.1.3 AccessCode <AccsCd>

Presence: [0..1]

Definition: Password authenticating the client.

Datatype: "Max35Binary" on page 266

10.1.6.1.4 ServerCertificate <SvrCert>

Presence: [0..*]

Definition: X.509 Certificate required to authenticate the server.

Datatype: "Max10KBinary" on page 265

10.1.6.1.5 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 266](#)

10.1.6.1.6 ClientCertificate <CIntCert>

Presence: [0..*]

Definition: X.509 Certificate required to authenticate the client.

Datatype: ["Max10KBinary" on page 265](#)

10.1.6.1.7 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the set of security elements to access the host.

Datatype: ["Max35Text" on page 296](#)

10.1.7 Secure Element

10.1.7.1 DigestedData5

Definition: Digest computed on the identified data.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		220
	DigestAlgorithm <DgstAlgo>	[1..1]	±		220
	EncapsulatedContent <NcpsltdCntt>	[1..1]	±		220
	Digest <Dgst>	[1..1]	Binary		221

10.1.7.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: ["Number" on page 295](#)

10.1.7.1.2 DigestAlgorithm <DgstAlgo>

Presence: [1..1]

Definition: Identification of the digest algorithm.

DigestAlgorithm <DgstAlgo> contains the following elements (see ["AlgorithmIdentification21" on page 249](#) for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		249

10.1.7.1.3 EncapsulatedContent <NcpsltdCntt>

Presence: [1..1]

Definition: Data on which the digest is computed.

EncapsulatedContent <NcpsltdCntt> contains the following elements (see "[EncapsulatedContent3](#)" on page 211 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		211
	Content <Cntt>	[0..1]	Binary		212

10.1.7.1.4 Digest <Dgst>

Presence: [1..1]

Definition: Result of data-digesting process.

Datatype: "[Max140Binary](#)" on page 266

10.1.7.2 CryptographicKey14

Definition: Cryptographic Key.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Identification <Id>	[1..1]	Text		221
	AdditionalIdentification <AddtlId>	[0..1]	Binary		222
	Name <Nm>	[0..1]	Text		222
	SecurityProfile <SctyPrfl>	[0..1]	Text		222
	ItemNumber <itmNb>	[0..1]	Text		222
	Version <Vrsn>	[1..1]	Text		222
	Type <Tp>	[0..1]	CodeSet		222
	Function <Fctn>	[0..*]	CodeSet		223
	ActivationDate <ActvtnDt>	[0..1]	DateTime		224
	DeactivationDate <DeactvtnDt>	[0..1]	DateTime		224
	KeyValue <KeyVal>	[0..1]	±		224
	KeyCheckValue <KeyChckVal>	[0..1]	Binary		224
	AdditionalManagementInformation <AddtlMgmtInf>	[0..*]			224
	Name <Nm>	[1..1]	Text		225
	Value <Val>	[0..1]	Text		225

10.1.7.2.1 Identification <Id>

Presence: [1..1]

Definition: Name of the cryptographic key.

Datatype: "[Max140Text](#)" on page 296

10.1.7.2.2 AdditionalIdentification <AddtId>

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 266

10.1.7.2.3 Name <Nm>

Presence: [0..1]

Definition: Name of the Cryptographic Element.

Datatype: "Max140Text" on page 296

10.1.7.2.4 SecurityProfile <SctyPrfl>

Presence: [0..1]

Definition: Identification of the set of security elements to which this element belongs.

Datatype: "Max35Text" on page 296

10.1.7.2.5 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 296

10.1.7.2.6 Version <Vrsn>

Presence: [1..1]

Definition: Version of the cryptographic key.

Datatype: "Max256Text" on page 296

10.1.7.2.7 Type <Tp>

Presence: [0..1]

Definition: Type of algorithm used by the cryptographic key.

Datatype: "CryptographicKeyType3Code" on page 278

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).

CodeName	Name	Definition
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).

10.1.7.2.8 Function <Fctn>

Presence: [0..*]

Definition: Allowed usage of the key.

Datatype: "KeyUsage1Code" on page 283

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.

CodeName	Name	Definition
KEYX	KeyExport	Key may export keys.
KEYD	KeyDerivation	Key may derive keys.

10.1.7.2.9 ActivationDate <ActvtnDt>

Presence: [0..1]

Definition: Date and time on which the key must be activated.

Datatype: "ISODatetime" on page 294

10.1.7.2.10 DeactivationDate <DeactvtnDt>

Presence: [0..1]

Definition: Date and time on which the key must be deactivated.

Datatype: "ISODatetime" on page 294

10.1.7.2.11 KeyVal <KeyVal>

Presence: [0..1]

Definition: Encrypted cryptographic key.

KeyVal <KeyVal> contains the following elements (see "ContentInformationType23" on page 225 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

10.1.7.2.12 KeyCheckValue <KeyChckVal>

Presence: [0..1]

Definition: Value for checking a cryptographic key security parameter.

Datatype: "Max35Binary" on page 266

10.1.7.2.13 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		225
	Value <Val>	[0..1]	Text		225

10.1.7.2.13.1 Name <Nm>

Presence: [1..1]

Definition: Name of the generic information to exchange.

Datatype: "Max70Text" on page 297

10.1.7.2.13.2 Value <Val>

Presence: [0..1]

Definition: Value of the generic information to exchange.

Datatype: "Max140Text" on page 296

10.1.7.3 ContentInformationType23

Definition: General cryptographic message syntax (CMS) containing protected data.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		225
	EnvelopedData <EnvlpdData>	[0..1]	±		226
	AuthenticatedData <AuthntcdData>	[0..1]	±		226
	SignedData <SgndData>	[0..1]	±		226
	DigestedData <DgstdData>	[0..1]	±		227

10.1.7.3.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data protection.

Datatype: "ContentType2Code" on page 277

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).

CodeName	Name	Definition
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).

10.1.7.3.2 EnvelopedData <EnvlpdData>

Presence: [0..1]

Definition: Data protection by encryption, with a session key.

EnvelopedData <EnvlpdData> contains the following elements (see "[EnvelopedData7](#)" on page 228 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		228
	OriginatorInformation <OrgtrlInf>	[0..1]			228
	Certificate <Cert>	[0..*]	Binary		228
	Recipient <Rcpt>	[1..*]	±		228
	EncryptedContent <NcrptdCntt>	[0..1]			229
	ContentType <CnttTp>	[1..1]	CodeSet		229
	ContentEncryptionAlgorithm <CnttNcrptnAlgo>	[0..1]	±		230
	EncryptedData <NcrptdData>	[1..1]	Binary		230

10.1.7.3.3 AuthenticatedData <AuthntcdData>

Presence: [0..1]

Definition: Data protection by a message authentication code (MAC).

AuthenticatedData <AuthntcdData> contains the following elements (see "[AuthenticatedData6](#)" on page 237 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		237
	Recipient <Rcpt>	[1..*]	±		237
	MACAlgorithm <MACAlgo>	[1..1]	±		238
	EncapsulatedContent <NcpsltdCntt>	[1..1]	±		239
	MAC <MAC>	[1..1]	Binary		239

10.1.7.3.4 SignedData <SgndData>

Presence: [0..1]

Definition: Data protected by a digital signatures.

SignedData <SgndData> contains the following elements (see "SignedData5" on page 257 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		258
	DigestAlgorithm <DgstAlgo>	[0..*]	±		258
	EncapsulatedContent <NcpsltdCntt>	[0..1]	±		259
	Certificate <Cert>	[0..*]	Binary		259
	Signer <Sgnr>	[0..*]			259
	Version <Vrsn>	[0..1]	Quantity		260
	SignerIdentification <SgnrId>	[0..1]			260
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			260
	Issuer <Issr>	[1..1]			260
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261
	SerialNumber <SrlNb>	[1..1]	Binary		261
Or}	KeyIdentifier <Keyldr>	[1..1]	±		262
	DigestAlgorithm <DgstAlgo>	[1..1]	±		262
	SignedAttributes <SgndAttrbts>	[0..*]			262
	Name <Nm>	[1..1]	Text		262
	Value <Val>	[0..1]	Text		262
	SignatureAlgorithm <SgntrAlgo>	[1..1]	±		263
	Signature <Sgntr>	[1..1]	Binary		263

10.1.7.3.5 DigestedData <DgstData>

Presence: [0..1]

Definition: Data protected by a digest.

DigestedData <DgstData> contains the following elements (see "DigestedData5" on page 220 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		220
	DigestAlgorithm <DgstAlgo>	[1..1]	±		220
	EncapsulatedContent <NcpsltdCntt>	[1..1]	±		220
	Digest <Dgst>	[1..1]	Binary		221

10.1.7.4 EnvelopedData7

Definition: Encrypted data with encryption key.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		228
	OriginatorInformation <OrgtrInf>	[0..1]			228
	Certificate <Cert>	[0..*]	Binary		228
	Recipient <Rcpt>	[1..*]	±		228
	EncryptedContent <NcrptdCntt>	[0..1]			229
	ContentType <CnttTp>	[1..1]	CodeSet		229
	ContentEncryptionAlgorithm <CnttNcrptnAlgo>	[0..1]	±		230
	EncryptedData <NcrptdData>	[1..1]	Binary		230

10.1.7.4.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 295

10.1.7.4.2 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		228

10.1.7.4.2.1 Certificate <Cert>

Presence: [0..*]

Definition: It may contain originator certificates associated with several different key management algorithms.

Datatype: "Max5000Binary" on page 266

10.1.7.4.3 Recipient <Rcpt>

Presence: [1..*]

Definition: Session key or identification of the protection key used by the recipient.

Recipient <Rcpt> contains one of the following elements (see "Recipient8Choice" on page 230 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
{Or	KeyTransport <KeyTrnsprt>	[1..1]			231
	Version <Vrsn>	[0..1]	Quantity		232
	RecipientIdentification <RcptId>	[1..1]			232
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			232
	Issuer <Issr>	[1..1]			233
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234
	SerialNumber <SrlNb>	[1..1]	Binary		234
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		234
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		234
	EncryptedKey <NcrptdKey>	[1..1]	Binary		235
Or	KEK <KEK>	[1..1]			235
	Version <Vrsn>	[0..1]	Quantity		235
	KEKIdentification <KEKId>	[1..1]	±		235
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		236
	EncryptedKey <NcrptdKey>	[1..1]	Binary		236
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		236

10.1.7.4.4 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		229
	ContentEncryptionAlgorithm <CnttNcrptnAlgo>	[0..1]	±		230
	EncryptedData <NcrptdData>	[1..1]	Binary		230

10.1.7.4.4.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data which have been encrypted.

Datatype: "ContentType2Code" on page 277

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).

10.1.7.4.4.2 ContentEncryptionAlgorithm <CnttNcrptnAlgo>

Presence: [0..1]

Definition: Algorithm used to encrypt the data.

ContentEncryptionAlgorithm <CnttNcrptnAlgo> contains the following elements (see "AlgorithmIdentification29" on page 240 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		240
	Parameter <Param>	[0..1]			242
	EncryptionFormat <NcrptnFrmt>	[0..1]	CodeSet		243
	InitialisationVector <InitlstnVctr>	[0..1]	Binary		243
	BytePadding <BPddg>	[0..1]	CodeSet		243

10.1.7.4.4.3 EncryptedData <NcrptdData>

Presence: [1..1]

Definition: Encrypted data, result of the content encryption.

Datatype: "Max100KBinary" on page 265

10.1.7.5 Recipient8Choice

Definition: Transport key or key encryption key (KEK) for the recipient.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
{Or	KeyTransport <KeyTrnsprt>	[1..1]			231
	Version <Vrsn>	[0..1]	Quantity		232
	RecipientIdentification <RcptId>	[1..1]			232
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			232
	Issuer <Issr>	[1..1]			233
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234
	SerialNumber <SrlNb>	[1..1]	Binary		234
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		234
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		234
	EncryptedKey <NcrptdKey>	[1..1]	Binary		235
Or	KEK <KEK>	[1..1]			235
	Version <Vrsn>	[0..1]	Quantity		235
	KEKIdentification <KEKId>	[1..1]	±		235
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		236
	EncryptedKey <NcrptdKey>	[1..1]	Binary		236
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		236

10.1.7.5.1 KeyTransport <KeyTrnsprt>

Presence: [1..1]

Definition: Encryption key using previously distributed asymmetric public key.

KeyTransport <KeyTrnsprt> contains the following **KeyTransport5** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		232
	RecipientIdentification <Rcptld>	[1..1]			232
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			232
	Issuer <Issr>	[1..1]			233
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234
	SerialNumber <SrlNb>	[1..1]	Binary		234
Or}	KeyIdentifier <Keyldr>	[1..1]	±		234
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		234
	EncryptedKey <NcrptdKey>	[1..1]	Binary		235

10.1.7.5.1.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 295

10.1.7.5.1.2 RecipientIdentification <Rcptld>

Presence: [1..1]

Definition: Identification of a cryptographic asymmetric key for the recipient.

RecipientIdentification <Rcptld> contains one of the following **Recipient5Choice** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			232
	Issuer <Issr>	[1..1]			233
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234
	SerialNumber <SrlNb>	[1..1]	Binary		234
Or}	KeyIdentifier <Keyldr>	[1..1]	±		234

10.1.7.5.1.2.1 IssuerAndSerialNumber <IssrAndSrlNb>

Presence: [1..1]

Definition: Certificate issuer name and serial number (see ITU X.509).

IssuerAndSerialNumber <IssrAndSrInb> contains the following **IssuerAndSerialNumber1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Issuer <Issr>	[1..1]			233
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234
	SerialNumber <SrInb>	[1..1]	Binary		234

10.1.7.5.1.2.1.1 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..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234

10.1.7.5.1.2.1.1.1 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		233
	AttributeValue <AttrVal>	[1..1]	Text		234

10.1.7.5.1.2.1.1.1.1 AttributeType <AttrTp>

Presence: [1..1]

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

Datatype: "AttributeType1Code" on page 274

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).

10.1.7.5.1.2.1.1.2 AttributeValue <AttrVal>

Presence: [1..1]

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

Datatype: "Max140Text" on page 296

10.1.7.5.1.2.1.2 SerialNumber <SrINb>

Presence: [1..1]

Definition: Certificate serial number (see X.509).

Datatype: "Max35Binary" on page 266

10.1.7.5.1.2.2 KeyIdentifier <Keyldr>

Presence: [1..1]

Definition: Identifier of a cryptographic asymmetric key, previously exchanged between initiator and recipient.

KeyIdentifier <Keyldr> contains the following elements (see "KEKIdentifier2" on page 121 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	KeyIdentification <Keyld>	[1..1]	Text		121
	KeyVersion <KeyVrsn>	[1..1]	Text		121
	SequenceNumber <SeqNb>	[0..1]	Quantity		121
	DerivationIdentification <DerivtnId>	[0..1]	Binary		121

10.1.7.5.1.3 KeyEncryptionAlgorithm <KeyNcrptnAlgo>

Presence: [1..1]

Definition: Algorithm to encrypt the key encryption key (KEK).

KeyEncryptionAlgorithm <KeyNcrptnAlgo> contains the following elements (see
"AlgorithmIdentification19" on page 253 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		254
	Parameter <Param>	[0..1]			254
	EncryptionFormat <NcrptnFrmt>	[0..1]	CodeSet		254
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		255
	MaskGeneratorAlgorithm <MskGnrtrAlgo>	[0..1]	±		255

10.1.7.5.1.4 EncryptedKey <NcrptdKey>

Presence: [1..1]

Definition: Encrypted key encryption key (KEK).

Datatype: "Max5000Binary" on page 266

10.1.7.5.2 KEK <KEK>

Presence: [1..1]

Definition: Key encryption key using previously distributed symmetric key.

KEK <KEK> contains the following **KEK7** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		235
	KEKIdentification <KEKId>	[1..1]	±		235
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		236
	EncryptedKey <NcrptdKey>	[1..1]	Binary		236

10.1.7.5.2.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 295

10.1.7.5.2.2 KEKIdentification <KEKId>

Presence: [1..1]

Definition: Identification of the key encryption key (KEK).

KEKIdentification <KEKId> contains the following elements (see "[KEKIdentifier2](#)" on page 121 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	KeyIdentification <KeyId>	[1..1]	Text		121
	KeyVersion <KeyVrsn>	[1..1]	Text		121
	SequenceNumber <SeqNb>	[0..1]	Quantity		121
	DerivationIdentification <DerivtnId>	[0..1]	Binary		121

10.1.7.5.2.3 KeyEncryptionAlgorithm <KeyNcrptnAlgo>

Presence: [1..1]

Definition: Algorithm to encrypt the key encryption key (KEK).

KeyEncryptionAlgorithm <KeyNcrptnAlgo> contains the following elements (see "[AlgorithmIdentification29](#)" on page 240 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		240
	Parameter <Param>	[0..1]			242
	EncryptionFormat <NcrptnFrmt>	[0..1]	CodeSet		243
	InitialisationVector <InitlstnVctr>	[0..1]	Binary		243
	BytePadding <BPddg>	[0..1]	CodeSet		243

10.1.7.5.2.4 EncryptedKey <NcrptdKey>

Presence: [1..1]

Definition: Encrypted key encryption key (KEK).

Datatype: "[Max500Binary](#)" on page 267

10.1.7.5.3 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 "[KEKIdentifier2](#)" on page 121 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	KeyIdentification <KeyId>	[1..1]	Text		121
	KeyVersion <KeyVrsn>	[1..1]	Text		121
	SequenceNumber <SeqNb>	[0..1]	Quantity		121
	DerivationIdentification <DerivtnId>	[0..1]	Binary		121

10.1.7.6 AuthenticatedData6

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		237
	Recipient <Rcpt>	[1..*]	±		237
	MACAlgorithm <MACAlgo>	[1..1]	±		238
	EncapsulatedContent <NcpsltdCntt>	[1..1]	±		239
	MAC <MAC>	[1..1]	Binary		239

10.1.7.6.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 295

10.1.7.6.2 Recipient <Rcpt>

Presence: [1..*]

Definition: Session key or protection key identification used by the recipient.

Recipient <Rcpt> contains one of the following elements (see "Recipient8Choice" on page 230 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
{Or	KeyTransport <KeyTrnsprt>	[1..1]			231
	Version <Vrsn>	[0..1]	Quantity		232
	RecipientIdentification <RcptId>	[1..1]			232
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			232
	Issuer <Issr>	[1..1]			233
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			233
	AttributeType <AttrTp>	[1..1]	CodeSet		233
	AttributeValue <AttrVal>	[1..1]	Text		234
	SerialNumber <SrlNb>	[1..1]	Binary		234
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		234
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		234
	EncryptedKey <NcrptdKey>	[1..1]	Binary		235
Or	KEK <KEK>	[1..1]			235
	Version <Vrsn>	[0..1]	Quantity		235
	KEKIdentification <KEKId>	[1..1]	±		235
	KeyEncryptionAlgorithm <KeyNcrptnAlgo>	[1..1]	±		236
	EncryptedKey <NcrptdKey>	[1..1]	Binary		236
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		236

10.1.7.6.3 MACAlgorithm <MACAlgo>

Presence: [1..1]

Definition: Algorithm to compute message authentication code (MAC).

MACAlgorithm <MACAlgo> contains the following elements (see "AlgorithmIdentification22" on page 245 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		246
	Parameter <Param>	[0..1]			248
	InitialisationVector <InitlStnVctr>	[0..1]	Binary		248
	BytePadding <BPddg>	[0..1]	CodeSet		248

10.1.7.6.4 EncapsulatedContent <NcpsltdCntt>

Presence: [1..1]

Definition: Data to authenticate.

EncapsulatedContent <NcpsltdCntt> contains the following elements (see "[EncapsulatedContent3](#)" on page 211 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		211
	Content <Cntt>	[0..1]	Binary		212

10.1.7.6.5 MAC <MAC>

Presence: [1..1]

Definition: Message authentication code value.

Datatype: "[Max140Binary](#)" on page 266

10.1.7.7 ContentInformationType22

Definition: General cryptographic message syntax (CMS) containing encrypted data.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		239
	EnvelopedData <EnvlpdData>	[1..1]	±		240

10.1.7.7.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data protection.

Datatype: "[ContentType2Code](#)" on page 277

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).

10.1.7.7.2 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 "EnvelopedData7" on page 228 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		228
	OriginatorInformation <OrgtrInf>	[0..1]			228
	Certificate <Cert>	[0..*]	Binary		228
	Recipient <Rcpt>	[1..*]	±		228
	EncryptedContent <NcrptdCntt>	[0..1]			229
	ContentType <CnttTp>	[1..1]	CodeSet		229
	ContentEncryptionAlgorithm <CnttNcrptnAlgo>	[0..1]	±		230
	EncryptedData <NcrptdData>	[1..1]	Binary		230

10.1.7.8 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		240
	Parameter <Param>	[0..1]			242
	EncryptionFormat <NcrptnFrmt>	[0..1]	CodeSet		243
	InitialisationVector <InitlstnVctr>	[0..1]	Binary		243
	BytePadding <BPddg>	[0..1]	CodeSet		243

10.1.7.8.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the algorithm.

Datatype: "Algorithm24Code" on page 271

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

CodeName	Name	Definition
		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 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

CodeName	Name	Definition
		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).

10.1.7.8.2 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		243
	InitialisationVector <InitlstnVctr>	[0..1]	Binary		243
	BytePadding <BPddg>	[0..1]	CodeSet		243

10.1.7.8.2.1 EncryptionFormat <NcrptnFrmt>

Presence: [0..1]

Definition: Format of data before encryption, if the format is not plaintext or implicit.

Datatype: "EncryptionFormat2Code" on page 282

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.

10.1.7.8.2.2 InitialisationVector <InitlstnVctr>

Presence: [0..1]

Definition: Initialisation vector of a cipher block chaining (CBC) mode encryption.

Datatype: "Max500Binary" on page 267

10.1.7.8.2.3 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 275

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.

10.1.7.9 ContentInformationType21

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		244
	AuthenticatedData <AuthntcdData>	[0..1]	±		244
	SignedData <SgndData>	[0..1]	±		245

10.1.7.9.1 ContentType <CnttTp>

Presence: [1..1]

Definition: Type of data protection.

Datatype: "ContentType2Code" on page 277

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).

10.1.7.9.2 AuthenticatedData <AuthntcdData>

Presence: [0..1]

Definition: Data protection by a message authentication code (MAC).

AuthenticatedData <AuthntcdData> contains the following elements (see "AuthenticatedData6" on page 237 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		237
	Recipient <Rcpt>	[1..*]	±		237
	MACAlgorithm <MACAlgo>	[1..1]	±		238
	EncapsulatedContent <NcpsltdCntt>	[1..1]	±		239
	MAC <MAC>	[1..1]	Binary		239

10.1.7.9.3 SignedData <SgndData>

Presence: [0..1]

Definition: Data protected by a digital signatures.

SignedData <SgndData> contains the following elements (see "SignedData5" on page 257 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		258
	DigestAlgorithm <DgstAlgo>	[0..*]	±		258
	EncapsulatedContent <NcpsltdCntt>	[0..1]	±		259
	Certificate <Cert>	[0..*]	Binary		259
	Signer <Sgnr>	[0..*]			259
	Version <Vrsn>	[0..1]	Quantity		260
	SignerIdentification <SgnrId>	[0..1]			260
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			260
	Issuer <Issr>	[1..1]			260
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261
	SerialNumber <SrlNb>	[1..1]	Binary		261
Or}	KeyIdentifier <Keyldr>	[1..1]	±		262
	DigestAlgorithm <DgstAlgo>	[1..1]	±		262
	SignedAttributes <SgndAttrbts>	[0..*]			262
	Name <Nm>	[1..1]	Text		262
	Value <Val>	[0..1]	Text		262
	SignatureAlgorithm <SgntrAlgo>	[1..1]	±		263
	Signature <Sgntr>	[1..1]	Binary		263

10.1.7.10 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		246
	Parameter <Param>	[0..1]			248
	InitialisationVector <InitlstnVctr>	[0..1]	Binary		248
	BytePadding <BPddg>	[0..1]	CodeSet		248

10.1.7.10.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the MAC algorithm.

Datatype: "Algorithm17Code" on page 268

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

CodeName	Name	Definition
		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). 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),

CodeName	Name	Definition
		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).

10.1.7.10.2 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		248
	BytePadding <BPddg>	[0..1]	CodeSet		248

10.1.7.10.2.1 InitialisationVector <InitlStnVctr>

Presence: [0..1]

Definition: Initialisation vector of a cipher block chaining (CBC) mode encryption.

Datatype: "Max500Binary" on page 267

10.1.7.10.2.2 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 275

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.

CodeName	Name	Definition
RAND	RandomPadding	Message to encrypt is completed by random value, the last byte containing the total number of added bytes.

10.1.7.11 AlgorithmIdentification21

Definition: Cryptographic algorithm and parameters of digests.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		249

10.1.7.11.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the digest algorithm.

Datatype: "Algorithm16Code" on page 267

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).

10.1.7.12 AlgorithmIdentification20

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		250
	Parameter <Param>	[0..1]			251
	DigestAlgorithm <DgstAlgo>	[1..1]	CodeSet		251
	MaskGeneratorAlgorithm <MskGnrtrAlgo>	[1..1]			252
	Algorithm <Algo>	[1..1]	CodeSet		252
	Parameter <Param>	[0..1]			253
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		253
	SaltLength <SaltLngth>	[1..1]	Quantity		253
	TrailerField <TrlrFld>	[0..1]	Quantity		253

10.1.7.12.1 Algorithm <Algo>

Presence: [1..1]

Definition: Identification of the algorithm.

Datatype: "Algorithm19Code" on page 270

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).
ECC5	EllipticCryptographicCurveFifthAlgorithm	Fifth Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC1	EllipticCryptographicCurveFirstAlgorithm	First Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC4	EllipticCryptographicCurveFourthAlgorithm	Fourth Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC2	EllipticCryptographicCurveSecondAlgorithm	Second Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC3	EllipticCryptographicCurveThirdAlgorithm	Third Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ERS3	SHA3-256WithRSA	Signature algorithms with RSA, using SHA3-256 digest algorithm. (ASN.1

CodeName	Name	Definition
		Object Identifier: id-rsassa-pkcs1-v1-5-with-sha3-256).
ECP2	SignatureWithEllipticCurveP-256	Elliptic Curve Signature with the Curve P-256 as defined by the Federal Information Processing Standards (FIPS 186-4 - July, 2013 - Digital Signature Standard).
ECP3	SignatureWithEllipticCurveP-384	Elliptic Curve Signature with the Curve P-384 as defined by the Federal Information Processing Standards (FIPS 186-4 - July, 2013 - Digital Signature Standard).
ECP5	SignatureWithEllipticCurveP-512	Elliptic Curve Signature with the Curve P-512 as defined by the Federal Information Processing Standards (FIPS 186-4 - July, 2013 - Digital Signature Standard).

10.1.7.12.2 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 **Parameter11** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	DigestAlgorithm <DgstAlgo>	[1..1]	CodeSet		251
	MaskGeneratorAlgorithm <MskGnrtrAlgo>	[1..1]			252
	Algorithm <Algo>	[1..1]	CodeSet		252
	Parameter <Param>	[0..1]			253
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		253
	SaltLength <SaltLngth>	[1..1]	Quantity		253
	TrailerField <TrlrFld>	[0..1]	Quantity		253

10.1.7.12.2.1 DigestAlgorithm <DgstAlgo>

Presence: [1..1]

Definition: Identification of the digest algorithm.

Datatype: "Algorithm16Code" on page 267

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).

10.1.7.12.2.2 MaskGeneratorAlgorithm <MskGnrtrAlgo>

Presence: [1..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		252
	Parameter <Param>	[0..1]			253
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		253

10.1.7.12.2.2.1 Algorithm <Algo>

Presence: [1..1]

Definition: Mask generator function cryptographic algorithm.

Datatype: "Algorithm8Code" on page 274

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).

10.1.7.12.2.2.2 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		253

10.1.7.12.2.2.2.1 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Digest algorithm used in the mask generator function.

Datatype: "Algorithm11Code" on page 267

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).

10.1.7.12.2.3 SaltLength <SaltLngth>

Presence: [1..1]

Definition: Length of the salt to include in the signature.

Datatype: "Number" on page 295

10.1.7.12.2.4 TrailerField <TrlrFld>

Presence: [0..1]

Definition: Trailer field number.

Datatype: "Number" on page 295

10.1.7.13 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		254
	Parameter <Param>	[0..1]			254
	EncryptionFormat <NcrptnFrmt>	[0..1]	CodeSet		254
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		255
	MaskGeneratorAlgorithm <MskGnrtrAlgo>	[0..1]	±		255

10.1.7.13.1 Algorithm <Algo>

Presence: [1..1]

Definition: Asymmetric encryption algorithm of a transport key.

Datatype: "Algorithm7Code" on page 273

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).

10.1.7.13.2 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		254
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		255
	MaskGeneratorAlgorithm <MskGnrtrAlgo>	[0..1]	±		255

10.1.7.13.2.1 EncryptionFormat <NcrptnFrmt>

Presence: [0..1]

Definition: Format of data before encryption, if the format is not plaintext or implicit.

Datatype: "EncryptionFormat2Code" on page 282

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.

10.1.7.13.2.2 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Identification of the digest algorithm.

Datatype: "Algorithm16Code" on page 267

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).

10.1.7.13.2.3 MaskGeneratorAlgorithm <MskGnrtrAlgo>

Presence: [0..1]

Definition: Mask generator function cryptographic algorithm and parameters.

MaskGeneratorAlgorithm <MskGnrtrAlgo> contains the following elements (see "AlgorithmIdentification18" on page 256 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		256
	Parameter <Param>	[0..1]			256
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		256

10.1.7.14 AlgorithmIdentification18

Definition: Mask generator function cryptographic algorithm and parameters.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		256
	Parameter <Param>	[0..1]			256
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		256

10.1.7.14.1 Algorithm <Algo>

Presence: [1..1]

Definition: Mask generator function cryptographic algorithm.

Datatype: "Algorithm8Code" on page 274

CodeName	Name	Definition
MGF1	MGF1	Generator Function, used for RSA encryption and RSA digital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).

10.1.7.14.2 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		256

10.1.7.14.2.1 DigestAlgorithm <DgstAlgo>

Presence: [0..1]

Definition: Digest algorithm used in the mask generator function.

Datatype: "Algorithm16Code" on page 267

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).

10.1.7.15 SignedData5

Definition: Digital signatures of data from one or several signers.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		258
	DigestAlgorithm <DgstAlgo>	[0..*]	±		258
	EncapsulatedContent <NcpsltdCntt>	[0..1]	±		259
	Certificate <Cert>	[0..*]	Binary		259
	Signer <Sgnr>	[0..*]			259
	Version <Vrsn>	[0..1]	Quantity		260
	SignerIdentification <SgnrId>	[0..1]			260
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			260
	Issuer <Issr>	[1..1]			260
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261
	SerialNumber <SrlNb>	[1..1]	Binary		261
Or}	KeyIdentifier <Keyldr>	[1..1]	±		262
	DigestAlgorithm <DgstAlgo>	[1..1]	±		262
	SignedAttributes <SgndAttrbts>	[0..*]			262
	Name <Nm>	[1..1]	Text		262
	Value <Val>	[0..1]	Text		262
	SignatureAlgorithm <SgntrAlgo>	[1..1]	±		263
	Signature <Sgntr>	[1..1]	Binary		263

10.1.7.15.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the data structure.

Datatype: "Number" on page 295

10.1.7.15.2 DigestAlgorithm <DgstAlgo>

Presence: [0..*]

Definition: Identification of digest algorithm applied before signature.

DigestAlgorithm <DgstAlgo> contains the following elements (see "AlgorithmIdentification21" on page 249 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		249

10.1.7.15.3 EncapsulatedContent <NcpsltdCntt>

Presence: [0..1]

Definition: Data to sign.

EncapsulatedContent <NcpsltdCntt> contains the following elements (see "[EncapsulatedContent3](#)" on page 211 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	ContentType <CnttTp>	[1..1]	CodeSet		211
	Content <Cntt>	[0..1]	Binary		212

10.1.7.15.4 Certificate <Cert>

Presence: [0..*]

Definition: Chain of X.509 certificates.

Datatype: "Max5000Binary" on page 266

10.1.7.15.5 Signer <Sgnr>

Presence: [0..*]

Definition: Digital signature and identification of a signer.

Signer <Sgnr> contains the following **Signer4** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Version <Vrsn>	[0..1]	Quantity		260
	SignerIdentification <SgnrId>	[0..1]			260
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			260
	Issuer <Issr>	[1..1]			260
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261
	SerialNumber <SrlNb>	[1..1]	Binary		261
Or}	KeyIdentifier <Keyldr>	[1..1]	±		262
	DigestAlgorithm <DgstAlgo>	[1..1]	±		262
	SignedAttributes <SgndAttrbts>	[0..*]			262
	Name <Nm>	[1..1]	Text		262
	Value <Val>	[0..1]	Text		262
	SignatureAlgorithm <SgntrAlgo>	[1..1]	±		263
	Signature <Sgntr>	[1..1]	Binary		263

10.1.7.15.5.1 Version <Vrsn>

Presence: [0..1]

Definition: Version of the Cryptographic Message Syntax (CMS) data structure.

Datatype: "Number" on page 295

10.1.7.15.5.2 SignerIdentification <SgnrId>

Presence: [0..1]

Definition: Identification of the entity who has signed the data.

SignerIdentification <SgnrId> contains one of the following **Recipient5Choice** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
{Or	IssuerAndSerialNumber <IssrAndSrlNb>	[1..1]			260
	Issuer <Issr>	[1..1]			260
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261
	SerialNumber <SrlNb>	[1..1]	Binary		261
Or}	KeyIdentifier <KeyIdr>	[1..1]	±		262

10.1.7.15.5.2.1 IssuerAndSerialNumber <IssrAndSrlNb>

Presence: [1..1]

Definition: Certificate issuer name and serial number (see ITU X.509).

IssuerAndSerialNumber <IssrAndSrlNb> contains the following **IssuerAndSerialNumber1** elements

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Issuer <Issr>	[1..1]			260
	RelativeDistinguishedName <RltvDstngshdNm>	[1..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261
	SerialNumber <SrlNb>	[1..1]	Binary		261

10.1.7.15.5.2.1.1 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..*]			261
	AttributeType <AttrTp>	[1..1]	CodeSet		261
	AttributeValue <AttrVal>	[1..1]	Text		261

10.1.7.15.5.2.1.1.1 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		261
	AttributeValue <AttrVal>	[1..1]	Text		261

10.1.7.15.5.2.1.1.1.1 AttributeType <AttrTp>

Presence: [1..1]

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

Datatype: "AttributeType1Code" on page 274

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).

10.1.7.15.5.2.1.1.1.2 AttributeValue <AttrVal>

Presence: [1..1]

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

Datatype: "Max140Text" on page 296

10.1.7.15.5.2.1.2 SerialNumber <SrINb>

Presence: [1..1]

Definition: Certificate serial number (see X.509).

Datatype: "Max35Binary" on page 266

10.1.7.15.5.2 KeyIdentifier <Keyldr>

Presence: [1..1]

Definition: Identifier of a cryptographic asymmetric key, previously exchanged between initiator and recipient.

KeyIdentifier <Keyldr> contains the following elements (see "KEKIdentifier2" on page 121 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	KeyIdentification <Keyld>	[1..1]	Text		121
	KeyVersion <KeyVrsn>	[1..1]	Text		121
	SequenceNumber <SeqNb>	[0..1]	Quantity		121
	DerivationIdentification <DerivtnId>	[0..1]	Binary		121

10.1.7.15.5.3 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 249 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		249

10.1.7.15.5.4 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		262
	Value <Val>	[0..1]	Text		262

10.1.7.15.5.4.1 Name <Nm>

Presence: [1..1]

Definition: Name of the generic information to exchange.

Datatype: "Max70Text" on page 297

10.1.7.15.5.4.2 Value <Val>

Presence: [0..1]

Definition: Value of the generic information to exchange.

Datatype: "Max140Text" on page 296

10.1.7.15.5.5 SignatureAlgorithm <SgntrAlgo>

Presence: [1..1]

Definition: Cryptographic digital signature algorithm.

SignatureAlgorithm <SgntrAlgo> contains the following elements (see "[AlgorithmIdentification20](#)" on page 250 for details)

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	Algorithm <Algo>	[1..1]	CodeSet		250
	Parameter <Param>	[0..1]			251
	DigestAlgorithm <DgstAlgo>	[1..1]	CodeSet		251
	MaskGeneratorAlgorithm <MskGnrtrAlgo>	[1..1]			252
	Algorithm <Algo>	[1..1]	CodeSet		252
	Parameter <Param>	[0..1]			253
	DigestAlgorithm <DgstAlgo>	[0..1]	CodeSet		253
	SaltLength <SaltLngh>	[1..1]	Quantity		253
	TrailerField <TrlrFld>	[0..1]	Quantity		253

10.1.7.15.5.6 Signature <Sgntr>

Presence: [1..1]

Definition: Digital signature.

Datatype: "[Max3000Binary](#)" on page 266

10.1.8 Synchronisation

10.1.8.1 ProcessRetry2

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		263
	MaximumNumber <MaxNb>	[0..1]	Quantity		263

10.1.8.1.1 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 297

10.1.8.1.2 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of retries.

Datatype: "Number" on page 295

10.1.8.2 ProcessTiming3

Definition: Parameters defining the timing conditions to process an action.

Or	MessageElement<XML Tag>	Mult.	Type	Constr. No.	Page
	WaitingTime <WtgTm>	[0..1]	Text		264
	StartTime <StartTm>	[0..1]	DateTime		264
	EndTime <EndTm>	[0..1]	DateTime		264
	Period <Prd>	[0..1]	Text		264
	MaximumNumber <MaxNb>	[0..1]	Quantity		264

10.1.8.2.1 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 297

10.1.8.2.2 StartTime <StartTm>

Presence: [0..1]

Definition: Date and time to start the action.

Datatype: "ISODateTime" on page 294

10.1.8.2.3 EndTime <EndTm>

Presence: [0..1]

Definition: Date and time after which the action cannot be processed.

Datatype: "ISODateTime" on page 294

10.1.8.2.4 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 297

10.1.8.2.5 MaximumNumber <MaxNb>

Presence: [0..1]

Definition: Maximum number of cyclic calls.

Datatype: "Number" on page 295

10.2 Message Datatypes

10.2.1 Amount

10.2.1.1 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

10.2.2 Binary

10.2.2.1 Max10000Binary

Definition: Specifies a binary string with a maximum length of 10000 binary bytes.

Type: Binary

Format

minLength	1
maxLength	10000

10.2.2.2 Max100KBinary

Definition: Binary data of 100K maximum.

Type: Binary

Format

minLength	1
maxLength	102400

10.2.2.3 Max10KBinary

Definition: Binary data of 10K maximum.

Type: Binary

Format

minLength	1
maxLength	10240

10.2.2.4 Max140Binary

Definition: Specifies a binary string with a maximum length of 140 binary bytes.

Type: Binary

Format

minLength	1
maxLength	140

10.2.2.5 Max2KBinary

Definition: Binary data of 2K maximum.

Type: Binary

Format

minLength	1
maxLength	2048

10.2.2.6 Max3000Binary

Definition: Specifies a binary string with a maximum length of 3000 binary bytes.

Type: Binary

Format

minLength	1
maxLength	3000

10.2.2.7 Max35Binary

Definition: Specifies a binary string with a maximum length of 35 binary bytes.

Type: Binary

Format

minLength	1
maxLength	35

10.2.2.8 Max5000Binary

Definition: Specifies a binary string with a maximum length of 5000 binary bytes.

Type: Binary

Format

minLength	1
maxLength	5000

10.2.2.9 Max500Binary

Definition: Specifies a binary string with a maximum length of 500 binary bytes.

Type: Binary

Format

minLength	1
maxLength	500

10.2.2.10 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

10.2.3 CodeSet

10.2.3.1 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).

10.2.3.2 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).
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).

10.2.3.3 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

CodeName	Name	Definition
		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.
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),

CodeName	Name	Definition
		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).
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).

10.2.3.4 Algorithm19Code

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).
ECC5	EllipticCryptographicCurveFifthAlgorithhm	Fifth Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC1	EllipticCryptographicCurveFirstAlgorithm	First Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC4	EllipticCryptographicCurveFourthAlgorithm	Fourth Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC2	EllipticCryptographicCurveSecondAlgorithm	Second Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ECC3	EllipticCryptographicCurveThirdAlgorithm	Third Elliptic Cryptographic Curve Algorithm identified by EMVCo Nextgen.
ERS3	SHA3-256WithRSA	Signature algorithms with RSA, using SHA3-256 digest algorithm. (ASN.1 Object Identifier: id-rsassa-pkcs1-v1-5-with-sha3-256).
ECP2	SignatureWithEllipticCurveP-256	Elliptic Curve Signature with the Curve P-256 as defined by the Federal Information Processing Standards (FIPS 186-4 - July, 2013 - Digital Signature Standard).
ECP3	SignatureWithEllipticCurveP-384	Elliptic Curve Signature with the Curve P-384 as defined by the Federal Information Processing Standards (FIPS 186-4 - July, 2013 - Digital Signature Standard).
ECP5	SignatureWithEllipticCurveP-512	Elliptic Curve Signature with the Curve P-512 as defined by the Federal Information Processing Standards (FIPS 186-4 - July, 2013 - Digital Signature Standard).

10.2.3.5 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).

10.2.3.6 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).

10.2.3.7 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 digital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).

10.2.3.8 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.
UATT	Unattended	Unattended payment, no attendant present.

10.2.3.9 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).

CodeName	Name	Definition
CATT	CountryName	Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).

10.2.3.10 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.

10.2.3.11 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.

10.2.3.12 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.

10.2.3.13 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.

10.2.3.14 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.)

10.2.3.15 CardholderVerificationCapability4Code

Definition: Cardholder verification capabilities by the terminal.

Type: CodeSet

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.

10.2.3.16 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	RenewCertificate	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.

10.2.3.17 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).

10.2.3.18 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 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).

10.2.3.19 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.

10.2.3.20 DataSetCategory11Code

Definition: Maintenance service to delegate.

Type: CodeSet

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.
KMGH	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.

10.2.3.21 DataSetCategory14Code

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.
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.

CodeName	Name	Definition
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.
SOFT	SoftwareApplication	Software Application or module of the POI.
CONF	ConfigurationFile	Configuration file relevant for the POI.
RPFL	ReportFile	Report file generated by the POI.

10.2.3.22 DataSetCategory15Code

Definition: Maintenance service to delegate.

Type: CodeSet

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.
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.

CodeName	Name	Definition
CONF	ConfigurationFile	Configuration file relevant for the POI.

10.2.3.23 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.

10.2.3.24 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.
NONE	None	No exchange.
BLCK	Blocking	All pending process must be paused until exchange is exclusively performed just after the transaction completion.

10.2.3.25 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.

10.2.3.26 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}

10.2.3.27 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.
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.

10.2.3.28 LanguageCode

Definition: Specifies a language.

Type: CodeSet

Constraints

- **ValidationByTable**

Must be a valid terrestrial language.

10.2.3.29 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.

10.2.3.30 MessageFunction40Code

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.

CodeName	Name	Definition
BTCH	BatchTransfer	Transfer the financial data as a collection of transaction.
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.

10.2.3.31 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.

10.2.3.32 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).

10.2.3.33 NetworkType2Code

Definition: Type of proxy.

Type: CodeSet

CodeName	Name	Definition
SCK5	Sock5	Sock5 proxy.
SCK4	Sock4	Sock4 proxy.
HTTP	HTTP	HTTP proxy.

10.2.3.34 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.

10.2.3.35 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.

10.2.3.36 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.

10.2.3.37 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	DelegatIssuer	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.

10.2.3.38 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.
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.

10.2.3.39 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.

10.2.3.40 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.
WT5G	WirelessTechnology5G	Includes all communication technologies which can be qualified as being part of the 5G technology.

10.2.3.41 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.

10.2.3.42 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.

10.2.3.43 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.
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).

CodeName	Name	Definition
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.

10.2.3.44 RejectReason2Code

Definition: Reason of transmission of a rejection message in response to a request or an advice.

Type: CodeSet

CodeName	Name	Definition
UNPR	UnableToProcess	Not possible to process the message, for instance the security module is unavailable, the hardware is unavailable, or there is a problem of resource.
IMSG	InvalidMessage	Invalid envelope of the message.
PARS	ParsingError	Invalid message: At least one of the data element or data structure is not present, the format, or the content of one data element or one data structure is not correct.
SECU	Security	Security error (for example an invalid key or an incorrect MAC value).
INTP	InitiatingParty	Invalid identification data for the sender.
RCPD	RecipientParty	Invalid identification data for the receiver.

CodeName	Name	Definition
VERS	ProtocolVersion	Version of the protocol couldn't be supported by the recipient.
MSGT	MessageType	Type of message the recipient receives is unknow or unsupported.

10.2.3.45 Response2Code

Definition: Response to a request of service.

Type: CodeSet

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

10.2.3.46 ResultDetail3Code

Definition: Detail of the response.

Type: CodeSet

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

10.2.3.47 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.

10.2.3.48 TerminalManagementAction4Code

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.

CodeName	Name	Definition
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.

10.2.3.49 TerminalManagementActionResult4Code

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.
SUCC	Success	Action was successfully performed.
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.

CodeName	Name	Definition
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.

10.2.3.50 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.

10.2.3.51 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.
RCNC	Reconciliation	Acquirer reconciliation to be performed before the terminal management action.
RSRT	RestartSystem	Restart the system after performing the terminal management action.

10.2.3.52 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.

10.2.3.53 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.

10.2.4 Date

10.2.4.1 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

10.2.5 DateTime

10.2.5.1 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

10.2.6 Indicator

10.2.6.1 TrueFalseIndicator

Definition: A flag indicating a True or False value.

Type: Indicator

Meaning When True: True

Meaning When False: False

10.2.7 Quantity

10.2.7.1 DecimalNumber

Definition: Number of objects represented as a decimal number, for example 0.75 or 45.6.

Type: Quantity

Format

totalDigits	18
fractionDigits	17

10.2.7.2 Number

Definition: Number of objects represented as an integer.

Type: Quantity

Format

totalDigits	18
fractionDigits	0

10.2.7.3 PositiveNumber

Definition: Number of objects represented as a positive integer.

Type: Quantity

Format

minInclusive	1
totalDigits	18
fractionDigits	0

10.2.8 Text

10.2.8.1 Max1025Text

Definition: Specifies a character string with a maximum length of 1025 characters.

Type: Text

Format

minLength	1
maxLength	1025

10.2.8.2 Max140Text

Definition: Specifies a character string with a maximum length of 140 characters.

Type: Text

Format

minLength	1
maxLength	140

10.2.8.3 Max20000Text

Definition: Specifies a character string with a maximum length of 20, 000 characters.

Type: Text

Format

minLength	1
maxLength	20000

10.2.8.4 Max256Text

Definition: Specifies a character string with a maximum length of 256 characters.

Type: Text

Format

minLength	1
maxLength	256

10.2.8.5 Max35Text

Definition: Specifies a character string with a maximum length of 35 characters.

Type: Text

Format

minLength	1
-----------	---

maxLength	35
-----------	----

10.2.8.6 Max500Text

Definition: Specifies a character string with a maximum length of 500 characters.

Type: Text

Format

minLength	1
maxLength	500

10.2.8.7 Max6Text

Definition: Specifies a character string with a maximum length of 6 characters.

Type: Text

Format

minLength	1
maxLength	6

10.2.8.8 Max70Text

Definition: Specifies a character string with a maximum length of 70characters.

Type: Text

Format

minLength	1
maxLength	70

10.2.8.9 Max8Text

Definition: Specifies a character string with a maximum length of 8 characters.

Type: Text

Format

minLength	1
maxLength	8

10.2.8.10 Max9NumericText

Definition: Specifies a numeric string with a maximum length of 9 digits.

Type: Text

Format

pattern	[0-9]{1,9}
---------	------------

10.2.8.11 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}
---------	---------------

10.2.8.12 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

10.2.9 Time

10.2.9.1 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