**Change Request**

**for the update of ISO 20022 financial repository items**

1. **Origin of the request:**

*A.1 Submitter*: nexo A.I.S.B.L

*A.2 Contact person:* Philippe CECE (Philippe.cece@ingenico.com) / Laure BELTRI (laure.beltri@frenchsys.com) / Evelyne de JONGHE (evelyne.de-jonghe@frenchsys.com) / Philippe MERMOUD (philippe.mermoud@bpce.fr) / Robert FARGIER (robert.fargier@istium.pro)

 *A.3 Sponsors*: nexo A.I.S.B.L.

1. **Related messages:**
* AcceptorAuthorisationRequest V11 caaa.001.001.11,
* AcceptorAuthorisationResponse V11 caaa.002.001.11,
* AcceptorCompletionAdvice V11 caaa.003.001.11,
* AcceptorCompletionAdviceResponse V10 caaa.004.001.10,
* AceptorCancellationRequest V11 caaa.005.001.11,
* AcceptorCancellationResponse V10 caaa.006.001.10,
* AcceptorCancellationAdvice V11 caaa.007.001.11,
* AcceptorCancellationAdviceResponse V10 caaa.008.001.10,
* AcceptorReconciliationRequest V10 caaa.009.001.10,
* AcceptorReconciliationResponse V09 caaa.010.001.09",
* AcceptorBatchTransfer V11 caaa.011.001.11,
* AcceptorBatchTransferResponse V10 caaa.012.001.10,
* AcceptorDiagnosticRequest V10 caaa.013.001.10,
* AcceptorDiagnosticResponse V09 caaa.014.001.09,
* AcceptorCurrencyConversionRequest V09 caaa.016.001.09,
* AcceptorCurrencyConversionResponse V09 caaa.017.001.09,
* AcceptorCurrencyConversionAdvice V06 caaa.018.001.06,
* AcceptorCurrencyConversionAdviceResponse V05 caaa.019.001.05,
* TransactionAdvice V03 caaa.020.001.03,
* TransactionAdviceResponse V03 caaa.021.001.03,
* AcceptorNonFinancialRequest V02 caaa.022.001.02,
* AcceptorNonFinancialResponse V02 caaa.023.001.02,
* AcceptorTransactionLogReportRequest V02 caaa.024.001.02,
* AcceptorTransactionLogReportResponse V02 caaa.025.001.02,
* SaleToPOIServiceRequest V04 casp.001.001.04,
* SaleToPOIserviceResponse V04 casp.002.001.04,
* SaleToPOIReconciliationRequest V04 casp.003.001.04,
* SaleToPOIReconciliationResponse V04 casp.004.001.04,
* SaleToPOISessionManagementRequest V04 casp.005.001.04,
* SaleToPOISessionManagementResponse V04 casp.006.001.04,
* SaleToPOIAdministrativeRequest V04 casp.007.001.04,
* SaleToPOIAdministrativeResponse V04 casp.008.001.04,
* SaleToPOIReportRequest V04 casp.009.001.04,
* SaleToPOIReportResponse V04 casp.010.001.04,
* SaleToPOIAbort V04 casp.011.001.04,
* SaleToPOIEventNotification V04 casp.012.001.04,
* SaleToPOIMessageStatusRequest V04 casp.014.001.04,
* SaleToPOIMessageStatusResponse V04 casp.015.001.04,
* SaleToPOIDeviceRequest V04 casp.016.001.04,
* SaleToPOIDevieResponse V04 casp.017.001.04,
* StatusReport V11 catm.001.001.11,
* ManagementPlanReplacement V10 catm.002.001.10,
* AcceptorConfigurationUpdate V11 catm.003.001.11,
* MaintenanceDelegationRequest V08 catm.005.001.08,
* MaintenanceDelegationResponse V06 catm.006.001.06,
* CertificateManagementRequest V05 catm.007.001.05,
* CertificateManagementResponse V06 catm.008.001.05
1. **Description of the change request:**

According to the RFC 5652, when managing an X509 certificate, we are able to identify this certificate either by the information coming from the issuer of this certificate (issuer information and issuer serial number of this certificate) or from the keys certified (subjectKeyIdentifier).





Unfortunately, the previous and current releases of the protocols don’t comply with these options and provide a *KeyIdentifier* of type *KEKIdentifier7* which is slightly different than a SubjectKeyIdentifier.



This slight modification was misleading, and some members twist the issuer serial number to set the subject key identifier.

Since this behaviour clearly impact interoperability, we create this change request to be in line with ASN.1 notation and fully support both way of identification and then get rid of any interoperability problem.

In order to manage interoperability, we will use the field *Version,* of the parent element *SignerIdentification* of type *Signer6. Version* is currently set to 1.

* We would use *Version =* 1 to identify the current behavior.
* We would use *Version =* 2 to identify that *IssuerAndSerialNumber/SerialNumber* is really the SerialNumber and not the SubjectKeyIdentifier.
* We would use *Version =* 3 (as in ASN.1) to identify that the Signer is identified by its *SubjectKeyIdentifier*

For *Version* set to 3, with previous release of protocols, the *KEKIdentifier7* requires also a subfield named *Version* to identify the Key. Since this sub field *Version* is meaningless, as a workaround for current and previous release of protocols using *KEKIdentifier7*, we will set the sub field *Version* to 0.

1. **Purpose of the change:**





1. **Urgency of the request:**

Urgent.

1. **Business examples:**

Examples illustrating the change request.

1. **SEG/TSG recommendation:**

*This section is not to be taken care of by the submitter of the change request. It will be completed in due time by the SEG(s) in charge of the related ISO 20022 messages or the TSG for changes related to the BAH.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Consider** |  | **Timing** |  |  |  |
|  |  | - **Next yearly cycle: 2022/2023**(the change will be considered for implementation in the yearly maintenance cycle which starts in 2022 and completes with the publication of new message versions in the spring of 2023) |  |  |
|  |  | - **At the occasion of the next maintenance of the messages**(the change will be considered for implementation, but does not justify maintenance of the messages in its own right – will be pending until more critical change requests are received for the messages) |  |  |
|  |  | - **Urgent unscheduled**(the change justifies an urgent implementation outside of the normal yearly cycle) |  |  |
|  |  | - **Other timing:** |  |

Comments:

|  |  |
| --- | --- |
| **Reject** |  |

Reason for rejection: