

BSI Technische Richtlinie 03125

Beweiswerterhaltung kryptographisch signierter Dokumente

Appendix zu Anlage TR-ESOR-E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks

Bezeichnung	Grobkonzept ETSI TS119512 TR-ESOR Transformator
Kürzel	BSI TR-ESOR-TRANS
Version	1.2.1 und 1.2.2
Datum	08.01.2021

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 228 99 9582-0

E-Mail: tresor@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2020

Inhalt

1.	Zusammenfassung	5
2.	Zielsetzung	6
3.	Spezifikation	7
3.1	RetrieveInfo	7
3.2	PreservePO ↔ ArchiveSubmission	8
3.2.1	PreservePO → ArchiveSubmissionRequest	9
3.2.2	ArchiveSubmissionResponse → PreservePOResponse	10
3.3	UpdatePOC ↔ ArchiveUpdate	11
3.3.1	UpdatePOC → ArchiveUpdateRequest	12
3.3.2	ArchiveUpdateResponse → UpdatePOCResponse	13
3.4	RetrievePO ↔ ArchiveRetrieval / ArchiveEvidence	14
3.4.1	RetrievePO → ArchiveRetrievalRequest / ArchiveEvidenceRequest	15
3.4.2	ArchiveRetrievalResponse → RetrievePOResponse	17
3.4.3	ArchiveEvidenceResponse → RetrievePOResponse	18
3.5	DeletePO ↔ ArchiveDeletion	19
3.5.1	DeletePO → ArchiveDeletionRequest	19
3.5.2	ArchiveDeletionResponse → DeletePOResponse	20
3.6	ValidateEvidence ↔ Verify	21
3.6.1	ValidateEvidence → VerifyRequest	21
3.6.2	VerifyResponse → ValidateEvidenceResponse	23
3.7	Search ↔ ArchiveData	24
3.7.1	Search → ArchiveDataRequest	24
3.7.2	ArchiveDataResponse → SearchResponse	25
4.	Referenzen	27

Abbildung

Abbildung 1	System mit dem „ETSI TS119512- TR-ESOR-Transformator“	6
Abbildung 2	RetrieveInfo – Aufruf und Antwort	7
Abbildung 3	PreservePo/ArchiveSubmission – Aufruf und Antwort	9
Abbildung 4	UpdatePOC/ArchiveUpdate – Aufruf und Antwort	12
Abbildung 5	RetrievePO/ArchiveRetrieval/EvidenceRetrieval – Aufruf und Antwort	15
Abbildung 7	DeletePO/ArchiveDeletion – Aufruf und Antwort	19
Abbildung 8	ValidateEvidence/Verify – Aufruf und Antwort	21
Abbildung 9	Search / ArchiveData – Aufruf und Antwort	24

Tabelle

Tabelle 1	Returncodes für PreservePO / ArchiveSubmission	11
-----------	--	----

Tabelle 2 Returncodes für UpdatePOC / ArchiveUpdate	14
Tabelle 4 Returncodes für RetrievePO / ArchiveRetrieval.....	18
Tabelle 5 Returncodes für RetrievePO / ArchiveEvidence	19
Tabelle 6 Returncodes für DeletePO / ArchiveDeletion	21
Tabelle 7 Returncodes für ValidateEvidence / Verify	23
Tabelle 8 Returncodes für Search / ArchiveData	26

1. Zusammenfassung

Das vorliegende Dokument spezifiziert die BSI-Transformator-Komponente „ETSI TS119512-TR-ESOR-Transformator“, welche eine geeignet profilierte Ausprägung der Preservation-API gemäß [ETSI TS 119 512] auf die TR-ESOR S.4-Schnittstelle gemäß [BSI TR-03125-E] Version 1.2.1 und 1.2.2 abbildet.

2. Zielsetzung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die zuständige Behörde für sichere Informationsverarbeitung und Kompetenzträger im Umfeld der elektronischen Signatur.

Vor diesem Hintergrund hat das BSI eine Technische Richtlinie für die „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-03125 / TR-ESOR) entwickelt, die insbesondere die TR-ESOR-S.4-Schnittstelle gemäß [BSI TR-03125-E], Version 1.2.1 bzw. Version 1.2.2 umfasst.

Außerdem hat das BSI ausgehend von der „TR-ESOR-S.4“-Schnittstelle die Standardisierung von Preservation Services bei ETSI ESI unterstützt, wobei insbesondere die „Preservation-API“ gemäß [ETSI TS 119 512] entstanden ist.

Auf dieser Basis wurde ein so genannter „ETSI TS119512-TR-ESOR-Transformator“ entwickelt und nach Projektabschluss als Open Source bereitgestellt, der Aufrufe an der bei ETSI ESI entwickelten „Preservation-API“ auf entsprechende Aufrufe an der „TR-ESOR-S.4“-Schnittstelle abbildet, so dass TR-ESOR-Middleware-Produkte Version 1.2.1 bzw. Version 1.2.2, die bereits die „TR-ESOR-S.4“-Schnittstelle unterstützen, durch den „ETSI TS119512-TR-ESOR- Transformator“ automatisch auch ein geeignetes Profil der „Preservation-API“ anbieten können. Als Kurzname wird im Bedarfsfall für „ETSI TS119512-TR-ESOR-Transformator“ auch die Bezeichnung „TS 119 512-Transformator“ oder „TR-ESOR-Transformator“ genutzt, z.B. in der nachstehenden Abbildung 1.

Hinweis: Wenn im folgenden Text nur [BSI TR-03125-E] bzw. [BSI TR-03125-F] steht, gilt es für [BSI TR-03125-E], Version 1.2.1 und Version 1.2.2. Ansonsten wird die Ergänzung „nur Version 1.2.2“ hinzugefügt.

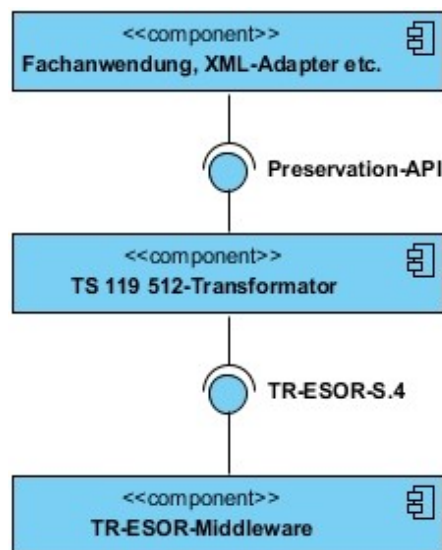


Abbildung 1 System mit dem „ETSI TS119512- TR-ESOR-Transformator“

3. Spezifikation

3.1 RetrieveInfo

Der Aufruf der RetrieveInfo Funktion liefert ein statisch hinterlegtes Profile-Element zurück.

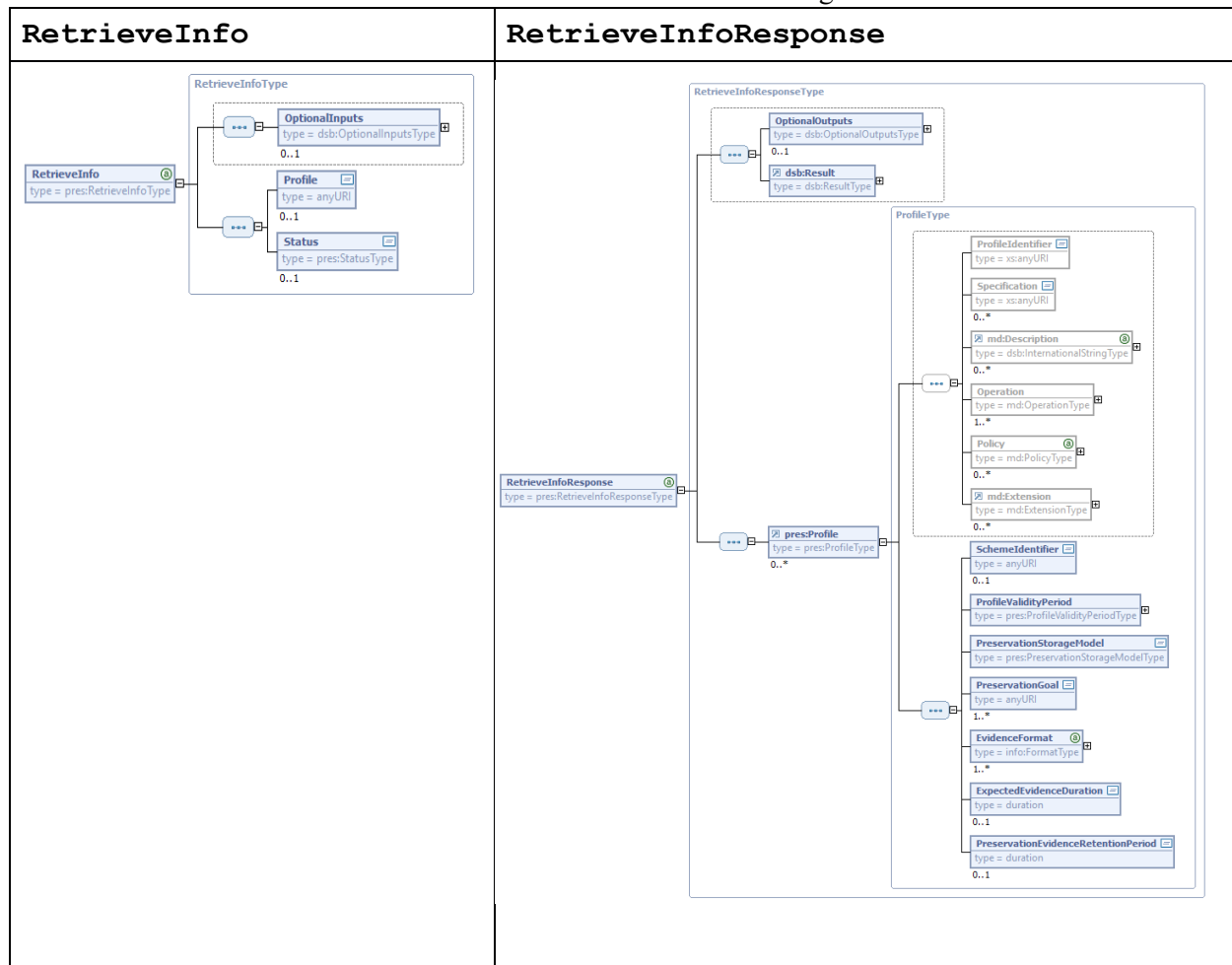


Abbildung 2 RetrieveInfo – Aufruf und Antwort

Das Profile-Element hat folgende Kindelemente:

- ProfileIdentifier – <http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-api/V1.1.2> bzw. <http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/V1.1.2>¹.
- Specification – URL-basierte Verweise auf veröffentlichte Spezifikationsdokumente [BSI TR-03125-E] und [ETSI TS 119 512]
- Operation – spezifiziert die relevanten Informationen zu den unterstützten Funktionen und Formaten (für Details siehe folgende Abschnitte)
- Policy/PolicyByRef/PolicyID – URL-basierter Verweis auf noch zu definierende Policy
- SchemeIdentifier – <http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers>
- ProfileValidityPeriod/ValidFrom – konfigurierbares Datum

¹ Das dem Quellcode beigelegte beispielhafte Profile-Element beinhaltet den folgenden ProfileIdentifier: <http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/V1.1.2>.

- PreservationStorageModel – WithStorage
- PreservationGoal
 - <http://uri.etsi.org/19512/goal/pds>
 - <http://uri.etsi.org/19512/goal/pgd>
 - <http://uri.etsi.org/19512/goal/aug>
- EvidenceFormat
 - urn:ietf:rfc:4998:EvidenceRecord (Dieser Wert, sofern anwendbar, wird als default angenommen falls das EvidenceFormat Element nicht angegeben ist)²
 - urn:ietf:rfc:6283:EvidenceRecord³

Die Returncodes sind [ETSI TS 119 512] zu entnehmen.

3.2 PreservePO ↔ ArchiveSubmission

Beim Aufruf von PreservePO aus [ETSI TS 119 512] wird der Inputparameter PreservePO aus [ETSI TS 119 512] auf einen Eingabeparameter ArchiveSubmissionRequest gemäß [BSI TR-03125-E] sowie umgekehrt der Rückgabeparameter von ArchiveSubmissionResponse gemäß [BSI TR-03125-E] wird auf den Rückgabeparameter PreservePOResponse aus [ETSI TS 119 512] abgebildet.

² Hierbei ist zu beachten, dass die entsprechende URI gemäß [BSI TR-03125-E] <urn:ietf:rfc:4998> ist.

³ Hierbei ist zu beachten, dass die entsprechende URI gemäß [BSI TR-03125-E] urn:ietf:rfc:6283 ist.

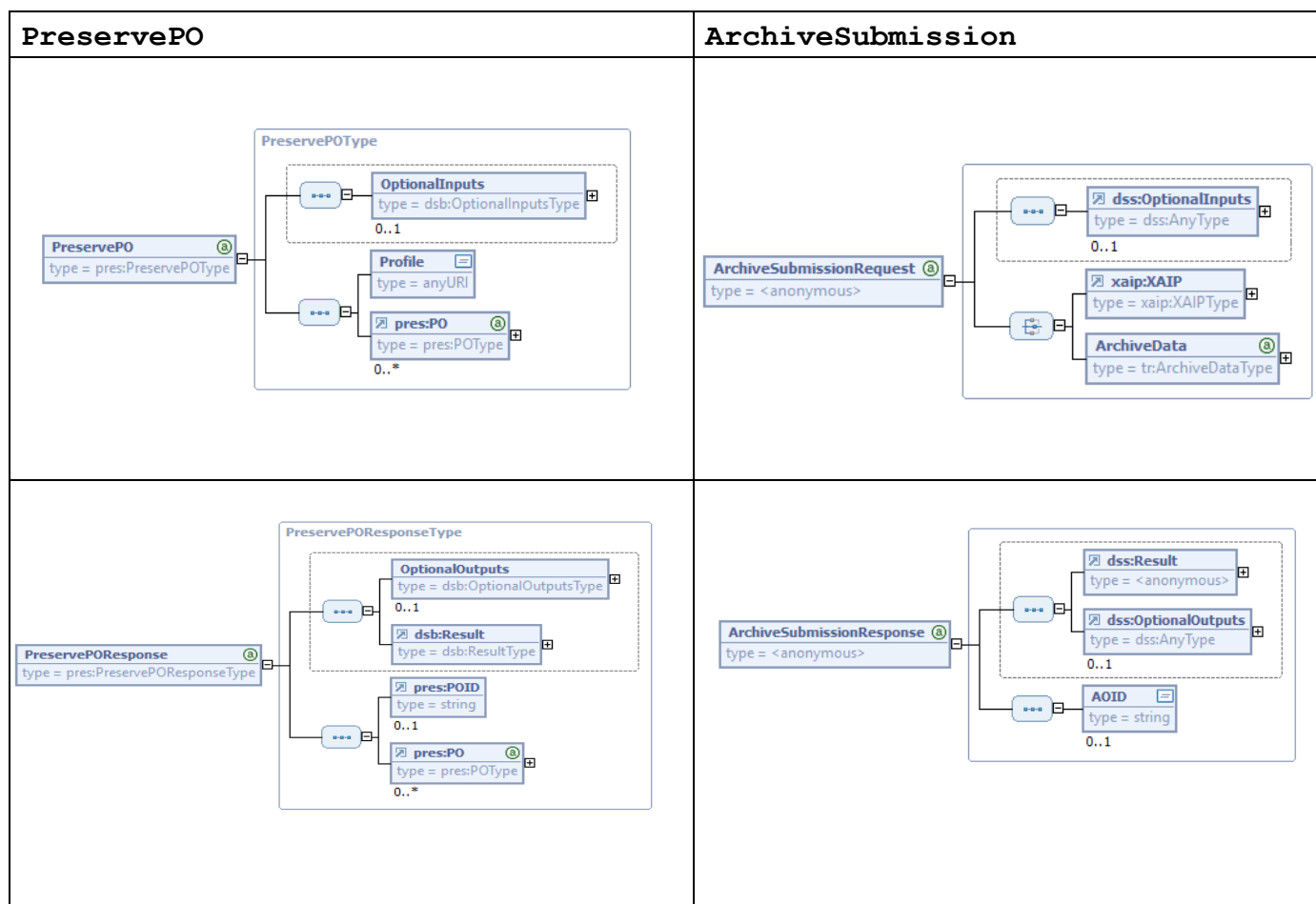


Abbildung 3 PreservePo/ArchiveSubmission – Aufruf und Antwort

3.2.1 PreservePO → ArchiveSubmissionRequest

Hierbei werden die Parameter im PreservePO folgendermaßen behandelt:

- OptionalInputs – die in [BSI TR-03125-E] definierten OptionalInputs (AOID, ReturnVerificationReport und ImportEvidence) werden an die TR-ESOR-S.4-Schnittstelle durchgereicht, sofern sie im PreservePO-Aufruf übergeben worden sind. Andere OptionalInputs führen zu einem entsprechenden Fehler⁴.
- Profile – erwartet <http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-api/V1.1.2> bzw. <http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/V1.1.2>, wodurch klargestellt wird, dass das in diesem Dokument spezifizierte Profil (siehe auch Abschnitt 3.1) angefordert wird.
- PO – enthält genau ein Preservation Object, das im ArchiveSubmissionRequest übergeben wird. Hierbei werden folgende Formate unterstützt:

⁴ <http://uri.etsi.org/19512/error/notSupported>

- XAIP v1.2⁵ gemäß [BSI TR-03125-F] (V1.2.2, Abschnitt 3.1 bzw. V1.2.1, Abschnitt 3) und gemäß [ETSI TS 119 512] Annex A.3.2 (<http://www.bsi.bund.de/tr-esor/xaip/1.2>) wird in `ArchiveSubmissionRequest/XAIP` übergeben.
- LXAIIP gemäß [BSI TR-03125-F] (nur V1.2.2, Abschnitt 3.2) und gemäß [ETSI TS 119 512] Annex A.3.2 (<http://www.bsi.bund.de/tr-esor/lxaip/1.3>) wird in `ArchiveSubmissionRequest/XAIP` übergeben.
- ASiC-ERS gemäß [BSI TR-03125-F] (nur V1.2.2, Abschnitt 3.3) und gemäß [ETSI TS 119 512] Annex A.3.1 (<http://uri.etsi.org/ades/ASiC/type/ASiC-ERS>) wird in `ArchiveSubmissionRequest/ArchiveData` als `binaryData` Element gemäß [BSI TR-03125-E] (nur Version 1.2.2, Abschnitt 3.1.1) übergeben.
- CAdES gemäß [ETSI TS 119 512] Annex A.1.1 (<http://uri.etsi.org/ades/CAdES>) wird in `ArchiveSubmissionRequest/ArchiveData` als `binaryData` Element gemäß [BSI TR-03125-E] (nur Version 1.2.2, Abschnitt 3.1.1) übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/cms](http://uri.etsi.org/ades/CAdES) verwendet.
- XAdES gemäß [ETSI TS 119 512] Annex A.1.2 (<http://uri.etsi.org/ades/XAdES>) wird in `ArchiveSubmissionRequest/ArchiveData` als `binaryData` Element gemäß [BSI TR-03125-E], Version 1.2.2, Abschnitt 3.1.1 übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/xml](http://uri.etsi.org/ades/XAdES) verwendet.
- PAdES gemäß [ETSI TS 119 512] Annex A.1.3 (<http://uri.etsi.org/ades/PAdES>) wird in `ArchiveSubmissionRequest/ArchiveData` als `binaryData` Element gemäß [BSI TR-03125-E] (nur Version 1.2.2, Abschnitt 3.1.1) übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/pdf](http://uri.etsi.org/ades/PAdES) verwendet.
- ASiC-E gemäß [ETSI TS 119 512] Annex A.1.4 (<http://uri.etsi.org/ades/ASiC/type/ASiC-E>) wird in `ArchiveSubmissionRequest/ArchiveData` als `binaryData` Element gemäß [BSI TR-03125-E] (nur Version 1.2.2, Abschnitt 3.1.1) übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/vnd.etsi.asic-e+zip](http://uri.etsi.org/ades/ASiC/type/ASiC-E) verwendet.
- DigestList gemäß [ETSI TS 119 512] Annex A.1.6 (<http://uri.etsi.org/19512/format/DigestList>) wird in `ArchiveSubmissionRequest/ArchiveData` als `binaryData` Element gemäß [BSI TR-03125-E] (nur Version 1.2.2, Abschnitt 3.1.1) übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/xml](http://uri.etsi.org/19512/format/DigestList) verwendet.

3.2.2 ArchiveSubmissionResponse → PreservePOResponse

- `dss6:Result` – wird wie unten näher dargestellt auf `dsb7:Result` abgebildet.
- `OptionalOutputs` – das möglicherweise in `OptionalOutputs` zurückgelieferte `VerificationReport` Element (vgl. [BSI TR-03125-E], Abschnitt 3.1.2) wird an das gleichnamige Element der Preservation-API weitergereicht.
- `AOID` – wird auf `POID` abgebildet.

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

⁵ Hinweis! Die mit der Version 1.2.2 der BSI TR-03125 freigegebene XAIP-Schema unterscheidet sich gegenüber der vorherigen Ausprägung (Version 1.2.1) in der Definition des Typs `xaip:metaDataObjectType`. Die gegenwärtige Version erlaubt mehrere Objekte (die durch die Metadaten beschrieben werden) zu referenzieren (`xs:IDREFS`). In der vorherigen Version durfte nur ein Datenobjekt referenziert werden (`xs:IDREF`). Die Änderung ist vollständig rückwärtskompatibel.

⁶ Namensraum „dss“ wird in „urn:oasis:names:tc:dss:1.0:core:schema“ aufgelöst.

⁷ Namensraum „dsb“ wird in „http://docs.oasis-open.org/dss-x/ns/base“ aufgelöst.

ETSI TS 119 512	BSI TR-03125-E
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Präfix für ResultMinor	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.2/resultminor
Suffixes für ResultMinor	
/error/noPermission	/al/common#noPermission
/error/internalError	/al/common#internalError
/error/externalServiceUnavailable	
/error/parameterError	/al/common#parameterError
/error/noSpaceError	/arl/noSpaceError
/warning/lowSpace	/arl/lowSpaceWarning
/error/notSupported	/arl/notSupported
/error/unknownPOFormat	/arl/unknownArchiveDataType
/error/POFormatError	/arl/XAIP_NOK /arl/XAIP_NOK_EXPIRED /arl/XAIP_NOK_SUBMTIME /arl/XAIP_NOK_SIG /arl/XAIP_NOK_ER
/error/existingAOID ⁸	/resultminor/arl/existingAOID

Tabelle 1 Returncodes für PreservePO / ArchiveSubmission

3.3 UpdatePOC ↔ ArchiveUpdate

Die Funktion UpdatePOC aus [ETSI TS 119 512] wird auf die Funktion ArchiveUpdate gemäß [BSI TR-03125-E] abgebildet. Entsprechend wird der Eingabeparameter UpdatePOC gem. [ETSI TS 119 512] auf den Eingabeparameter ArchiveUpdateRequest gem. [BSI TR-03125-E], sowie umgekehrt wird der Rückgabeparameter ArchiveUpdateResponse gemäß [BSI TR-03125-E] auf den Rückgabeparameter UpdatePOCResponse aus [ETSI TS 119 512] abgebildet.

⁸ Dieser Fehlercode existiert nicht in [ETSI TS 119 512] und entsteht durch die Ergänzung von OptionalInputs/AOID.

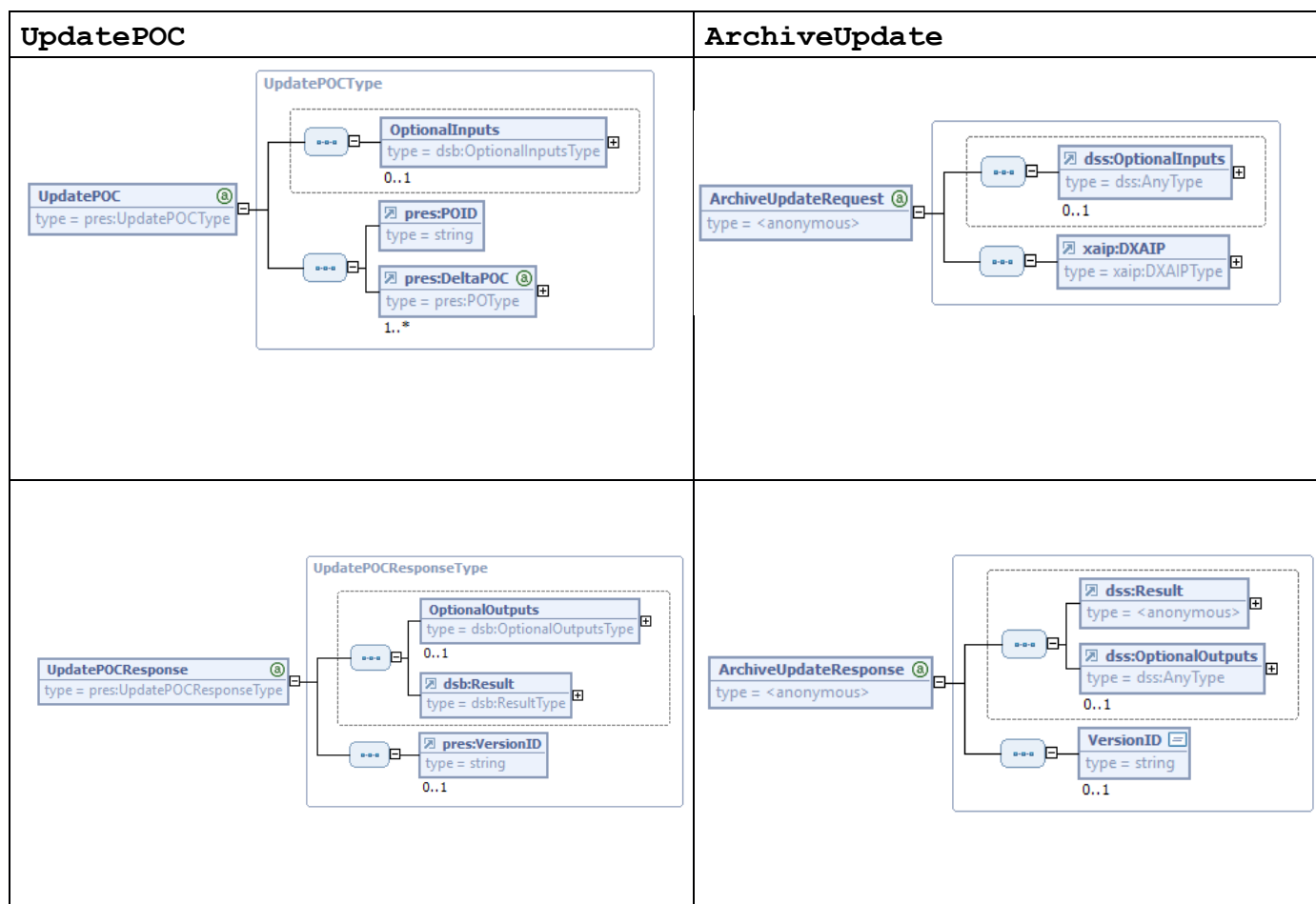


Abbildung 4 UpdatePOC/ArchiveUpdate – Aufruf und Antwort

3.3.1 UpdatePOC → ArchiveUpdateRequest

Hierbei werden die Parameter im UpdatePOC folgendermaßen behandelt:

- OptionalInputs – die in [BSI TR-03125-E] definierten OptionalInputs (Return-VerificationReport und ImportEvidence) werden an die TR-ESOR-S.4-Schnittstelle an dss:OptionalInputs durchgereicht. Andere OptionalInputs führen zu einem entsprechenden Fehler⁹.
- POID – muss identisch zu DXAIP/PackageHeader/AOID sein und wird zur Konsistenzprüfung genutzt und liefert bei fehlender Übereinstimmung einen entsprechenden Fehler¹⁰.
- DeltaPOC – wird in ArchiveUpdateRequest/DXAIP-Element übergeben und muss entweder ein
 - Delta-XAIP-Element gemäß [BSI TR-03125-F] (V1.2.1 Abschnitt 3.6 bzw. V1.2.2, Abschnitt 3.1.6) (FormatId=<http://www.bsi.bund.de/tr-esor/dxaip/1.2¹¹>) oder ein
 - Delta-LXAIP-Element gemäß [BSI TR-03125-F] (nur V1.2.2, Abschnitt 3.2.2) (FormatId=<http://www.bsi.bund.de/tr-esor/dlxaip/1.2¹²>)

⁹ <http://uri.etsi.org/19512/error/notSupported>

¹⁰ <http://uri.etsi.org/19512/error/DeltaPOCInternalProblem>

¹¹ Diese URL muss in einer zukünftigen Version von ETSI TS 119 512 ergänzt werden.

sein.

3.3.2 ArchiveUpdateResponse → UpdatePOCResponse

- `dss:Result` – wird wie unten näher dargestellt auf `dsb:Result` abgebildet.
- `OptionalOutputs` – das möglicherweise in `dss:OptionalOutputs` zurückgelieferte `VerificationReport` Element (vgl. [BSI TR-03125-E], Abschnitt 3.2.2) wird an das gleichnamige Element der Preservation-API weitergereicht.
- `VersionID` – wird auf das gleichnamige Element der Preservation-API abgebildet.

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
<code>urn:oasis:names:tc:dss:1.0:resultmajor</code>	<code>http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor</code>
Suffixes für ResultMajor	
<code>:Success</code>	<code>#ok</code> <code>#warning</code>
<code>:resultmajor:RequesterError</code> <code>:resultmajor:ResponderError</code>	<code>#error</code>
<code>:resultmajor:InsufficientInformation</code>	-
Präfix für ResultMinor	
<code>http://uri.etsi.org/19512</code>	<code>http://www.bsi.bund.de/tr-esor/api/1.2/resultminor</code>
Suffixes für ResultMinor	
<code>/error/noPermission</code>	<code>/al/common#noPermission</code>
<code>/error/internalError</code>	<code>/al/common#internalError</code>
<code>/error/externalServiceUnavailable</code>	
<code>/error/parameterError</code>	
<code>/error/transferError</code>	<code>/al/common#parameterError</code>
<code>/error/notSupported</code>	
<code>/error/unknownDeltaPOCType</code>	
<code>/error/noSpaceError</code>	<code>/arl/noSpaceError</code>
<code>/error/unknownPOID</code>	<code>/arl/DXAIP_NOK_AOID</code>
<code>/error/DeltaPOCInternalProblem</code>	<code>/arl/existingPackageInfoWarning</code> <code>/arl/DXAIP_NOK</code> <code>/arl/DXAIP_NOK_EXPIRED</code> <code>/arl/DXAIP_NOK_SUBMTIME</code> <code>/arl/DXAIP_NOK_SIG</code> <code>/arl/DXAIP_NOK_ID</code> <code>/arl/DXAIP_NOK_Version</code>

¹² Diese URL muss in einer zukünftigen Version von ETSI TS 119 512 ergänzt werden.

ETSI TS 119 512	BSI TR-03125-E
/error/POFormatError	/arl/XAIP_NOK_ER
/warning/lowSpace	/arl/lowSpaceWarning

Tabelle 2 Returncodes für UpdatePOC / ArchiveUpdate

3.4 RetrievePO ↔ ArchiveRetrieval / ArchiveEvidence

Der Aufruf RetrievePO aus [ETSI TS 119 512] wird auf die Aufrufe ArchiveRetrieval bzw. ArchiveEvidence gemäß [BSI TR-03125-E] abgebildet. Entsprechend wird der Eingabeparameter RetrievePO gem. [ETSI TS 119 512] auf die korrespondierende Parameter ArchiveRetrievalRequest bzw. ArchiveEvidenceRequest gem. [BSI TR-03125-E] abgebildet. Umgekehrt werden die Rückgabeparameter ArchiveRetrievalResponse bzw. ArchiveEvidenceResponse gemäß [BSI TR-03125-E] auf den Rückgabeparameter RetrievePOResponse aus [ETSI TS 119 512] abgebildet.

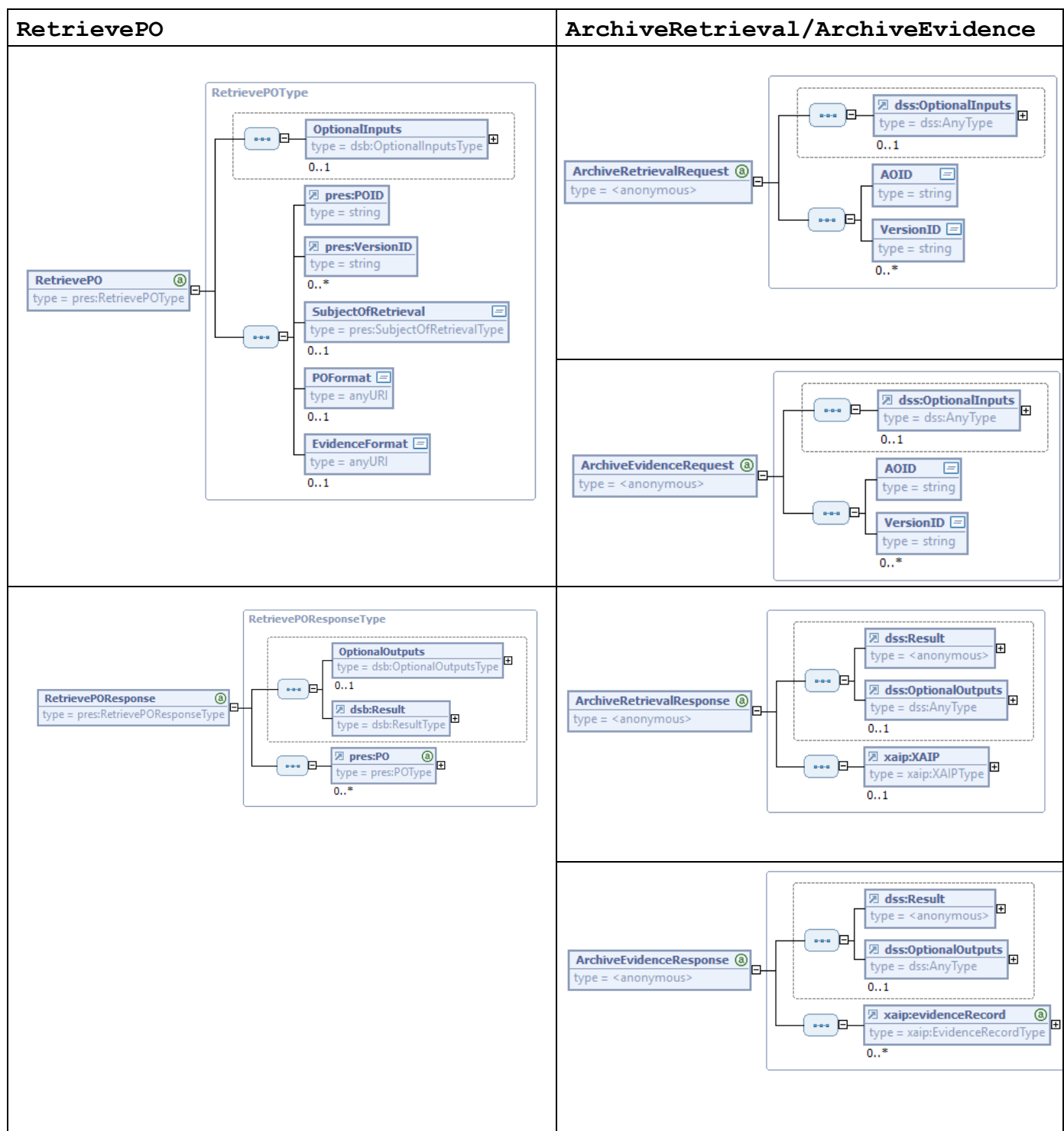


Abbildung 5 RetrievePO/ArchiveRetrieval/EvidenceRetrieval – Aufruf und Antwort

3.4.1 RetrievePO → ArchiveRetrievalRequest / ArchiveEvidenceRequest

Hierbei werden die Kindelemente von RetrievePO folgendermaßen behandelt:

- OptionalInputs führen beim Aufruf von RetrievePO zu einem Fehler¹³.

¹³ <http://uri.etsi.org/19512/error/notSupported>

- POID wird auf ArchiveRetrievalRequest/AOID bzw. ArchiveEvidenceRequest/AOID abgebildet, wobei die Unterscheidung zwischen ArchiveEvidenceRequest oder ArchiveRetrievalRequest anhand des SubjectOfRetrievalParameters erfolgt.
- VersionID wird auf ArchiveRetrievalRequest/VersionID bzw. ArchiveEvidenceRequest/VersionID abgebildet.
- SubjectOfRetrieval legt fest, ob ArchiveRetrievalRequest oder ArchiveEvidenceRequest aufgerufen wird und ist entweder
 - PO – zum Abholen des (L)XAIP oder ASiC-ERS ohne entsprechenden Evidence Record, so dass ArchiveRetrievalRequest aufgerufen wird,
 - Evidence – zum Abholen von Evidence Records, so dass ArchiveEvidenceRequest aufgerufen wird, wobei der Evidence Record als xaip:evidenceRecord-Element gemäß [BSI TR-03125-F] (Version 1.2.1, Abschnitt 3.5 bzw. Version 1.2.2, Abschnitt 3.1.5) vom Typ xaip:EvidenceRecordType zurückgegeben wird, der als Erweiterung des ec:EvidenceRecordType aus [eCard-2] definiert ist und zusätzlich die Attribute AOID und VersionID, enthalten muss.
 - POwithEmbeddedEvidence – zum Abholen des (L)XAIP oder ASiC-ERS mit entsprechendem Evidence Record, was durch einen Aufruf von ArchiveRetrievalRequest unter Verwendung des OptionalInputs/IncludeERS aus [BSI TR-03125-E] (Abschnitt 3.4.1) realisiert wird. Dieser Wert wird als default angenommen falls das SubjectOfRetrieval Element nicht angegeben ist.
 - POwithDetachedEvidence – wird nicht unterstützt und liefert einen Fehler¹⁴.
- POFormat wird auf ArchiveRetrievalRequest/OptionalInputs/POFormat aus [BSI TR-03125-E] (Abschnitt 3.4.1) abgebildet und ist entweder
 - <http://www.bsi.bund.de/tr-esor/xaip/1.2> für XAIP v1.2 gemäß [BSI TR-03125-F] (V1.2.1, Abschnitt 3 bzw. V1.2.2, Abschnitt 3.1) (Dieser Wert wird als default angenommen falls das POFormat Element nicht angegeben ist),
 - <http://www.bsi.bund.de/tr-esor/lxaip/1.3> für LXAIP gemäß [BSI TR-03125-F] (nur V1.2.2, Abschnitt 3.2) oder
 - <http://uri.etsi.org/ades/ASiC/type/ASiC-ERS> für ASiC-ERS.

Hinweis: Im Rahmen von S.4 erfolgt die Rückgabe eines XAIP oder LXAIP im ArchiveRetrievalResponse/XAIP Element und die Rückgabe eines ASiC-AIP über ein ArchiveRetrievalResponse/OptionalOutputs/PO Element.

- EvidenceFormat ist entweder
 - urn:ietf:rfc:4998:EvidenceRecord (Dieser Wert, sofern anwendbar, wird als default angenommen falls das EvidenceFormat Element nicht angegeben ist) oder
 - urn:ietf:rfc:6283:EvidenceRecord¹⁵,was an der S.4-Schnittstelle zu ArchiveEvidenceRequest/OptionalInputs/ERSFormat (siehe [BSI TR-03125-E], Abschnitt 3.4.1), bzw. ArchiveRetrievalRequest/OptionalInputs/IncludeERS (siehe [BSI TR-03125-E],

¹⁴ <http://uri.etsi.org/19512/error/notSupported>

¹⁵ Hierbei ist zu beachten, dass die entsprechende URI gemäß [BSI TR-03125-E] urn:ietf:rfc:6283 ist.

Abschnitt 3.3.1) korrespondiert. Der EvidenceRecord wird als xaip:evidenceRecord-Element gemäß [BSI TR-03125-F] (V1.2.1, Abschnitt 3.5 bzw. V1.2.2, Abschnitt 3.1.5) bzw. [BSI TR-03125-E] (Abschnitt 3.3.1 bzw. 3.4.2) vom Typ xaip:EvidenceRecordType zurückgegeben.

3.4.2 ArchiveRetrievalResponse → RetrievePOResponse

- dss:Result – wird wie unten näher dargestellt auf dsb:Result abgebildet.
- OptionalOutputs – das möglicherweise in OptionalOutputs zurückgelieferte PO Element (vgl. [BSI TR-03125-E], Abschnitt 3.3.2) mit einem base64Binary-codierten ASiC-AIP im RetrievePOResponse/PO Element zurückgeliefert.
- XAIP – mit einem XAIP oder LXAIP wird auf das RetrievePOResponse/PO Element abgebildet.

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
urn:oasis:names:tc:dss:1.0:resultmajor	http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor
Suffixes für ResultMajor	
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Präfix für ResultMinor	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.2/resultminor
Suffixes für ResultMinor	
/error/noPermission	/al/common#noPermission
/error/internalError	/al/common#internalError
/error/parameterError	/al/common#parameterError
/error/transferError ¹⁶	
/error/notSupported	/arl/notSupported
/error/unknownPOFormat	/arl/unknownPOFormat
/error/unknownPOID	/arl/unknownAOID
/error/unknownVersionID	/arl/unknownVersionID

¹⁶ Diesen Fehlercode gibt es aktuell in [ETSI TS 119 512] nicht für RetrievePOResponse. Sinnvoll wäre es hier ggf., diesen Fehlercode bei Gelegenheit entsprechend zu ergänzen.

ETSI TS 119 512	BSI TR-03125-E
/warning/requestOnlyPartlySuccessful	/arl/requestOnlyPartlySuccessfulWarning

Tabelle 3 Returncodes für RetrievePO / ArchiveRetrieval

3.4.3 ArchiveEvidenceResponse → RetrievePOResponse

- `dss:Result` – wird wie unten näher dargestellt auf `dsb:Result` abgebildet.
- `OptionalOutputs` – sind in `ArchiveEvidenceResponse` gemäß (vgl. [BSI TR-03125-E], Abschnitt 3.4.2) nicht vorhanden bzw. führen zu einem entsprechenden Fehler¹⁷ an der Preservation API gemäß [ETSI TS 119 512].
- `evidenceRecord` – wird auf das `RetrievePOResponse/PO` Element abgebildet, wobei sich das Format des zurückgelieferten Evidence Records im `FormatId`-Attribut des PO-Elementes widerspiegelt.

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
urn:oasis:names:tc:dss:1.0:resultmajor	http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor
Suffixes für ResultMajor	
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Präfix für ResultMinor	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.2/resultminor
Suffixes für ResultMinor	
/error/noPermission	/al/common#noPermission
/error/internalError	/al/common#internalError
/error/parameterError	/al/common#parameterError
/error/notSupported	/arl/notSupported ¹⁸

¹⁷ <http://uri.etsi.org/19512/error/notSupported>

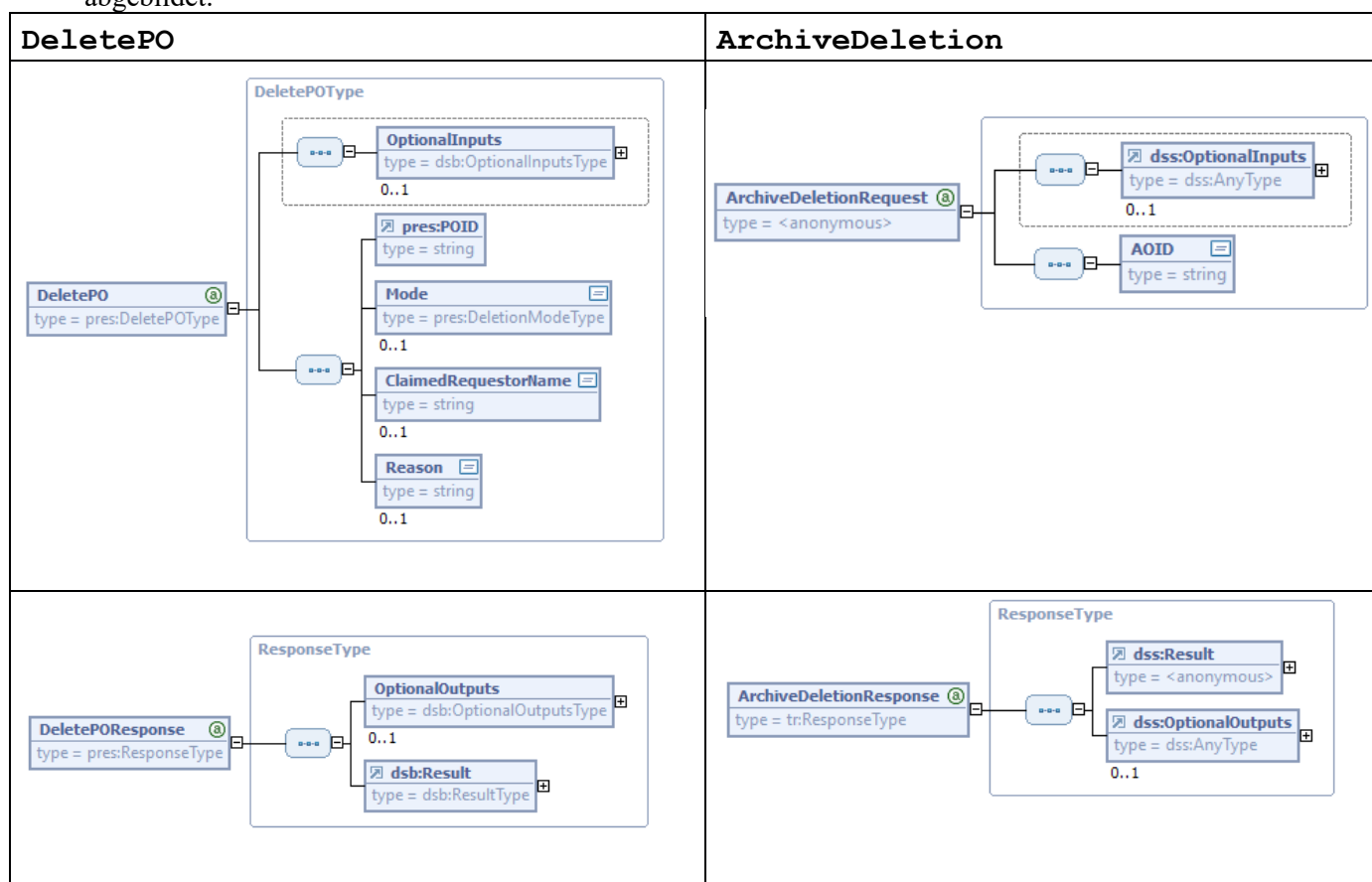
¹⁸ Alternativ wäre es perspektivisch denkbar, einen spezifischen Fehlercode `.../arl/unknownEvidenceFormat` für `ArchiveEvidenceResponse` in [BSI TR-03125-E] zu ergänzen.

ETSI TS 119 512	BSI TR-03125-E
/error/unknownEvidenceFormat	
/error/unknownPOID	/arl/unknownAOID
/error/unknownVersionID	/arl/unknownVersionID
/warning/requestOnlyPartlySuccessful	/arl/requestOnlyPartlySuccessfulWarning

Tabelle 4 Returncodes für RetrievePO / ArchiveEvidence

3.5 DeletePO ↔ ArchiveDeletion

Der Aufruf von DeletePO aus [ETSI TS 119 512] wird auf den Aufruf von ArchiveDeletion gemäß [BSI TR-03125-E] abgebildet. Entsprechend wird der Eingabeparameter DeletePO aus [ETSI TS 119 512] auf den Eingabeparameter ArchiveDeleteRequest aus [BSI TR-03125-E], bzw. umgekehrt der Rückgabeparameter ArchiveDeletionResponse gemäß [BSI TR-03125-E] wird auf den Rückgabeparameter DeletePOResponse aus [ETSI TS 119 512] abgebildet.


Abbildung 6 DeletePO/ArchiveDeletion – Aufruf und Antwort

3.5.1 DeletePO → ArchiveDeletionRequest

Hierbei werden die Kindelemente von DeletePO folgendermaßen abgebildet:

- OptionalInputs führen beim Aufruf von DeletePO zu einem Fehler¹⁹.
- POID wird auf ArchiveDeletionRequest/AOID abgebildet.
- Mode muss gleich SubDOsAndEvidence oder nicht vorhanden sein. Im Fall eines syntaktisch korrekten Aufrufs, bei dem Mode gleich OnlySubDOs ist, wird die Löschung nicht durchgeführt und ein Fehler²⁰ zurückgeliefert.
- ClaimedRequestorName wird auf ArchiveDeletionRequest/OptionalInputs/ReasonOfDeletion/RequestorName abgebildet.
- Reason wird auf ArchiveDeletionRequest/OptionalInputs/ReasonOfDeletion/RequestInfo abgebildet.

3.5.2 ArchiveDeletionResponse → DeletePOResponse

- dss:Result – wird wie unten näher dargestellt auf dsb:Result abgebildet.
- OptionalOutputs – sind in ArchiveDeletionResponse gemäß (vgl. [BSI TR-03125-E], Abschnitt 3.5.2) nicht vorhanden bzw. führen zu einem entsprechenden Fehler²¹ an der Preservation API gemäß [ETSI TS 119 512].

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
urn:oasis:names:tc:dss:1.0:resultmajor	http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor
Suffixes für ResultMajor	
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Präfix für ResultMinor	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.2/resultminor
Suffixes für ResultMinor	
/error/noPermission	/al/common#noPermission
/error/internalError	/al/common#internalError

¹⁹ <http://uri.etsi.org/19512/error/notSupported>

²⁰ <http://uri.etsi.org/19512/error/notSupported>

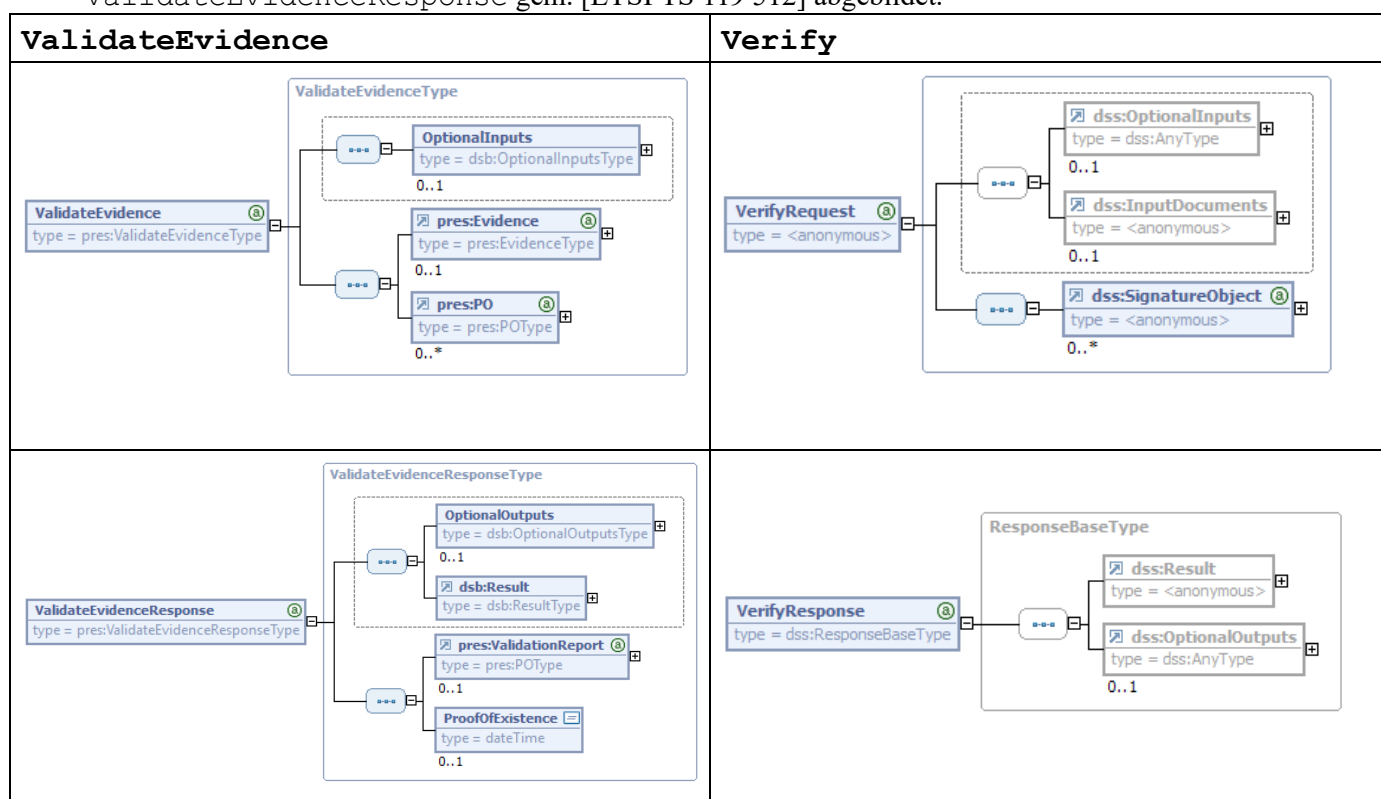
²¹ <http://uri.etsi.org/19512/error/notSupported>

ETSI TS 119 512	BSI TR-03125-E
/error/parameterError	/al/common#parameterError
	/arl/missingReasonOfDeletion
/error/notSupported	/arl/notSupported
/error/unknownPOID	/arl/unknownAOID

Tabelle 5 Returncodes für DeletePO / ArchiveDeletion

3.6 ValidateEvidence ↔ Verify

Die Funktion `ValidateEvidence` aus [ETSI TS 119 512] wird auf die Funktion `Verify` gemäß [BSI TR-03125-E] (Abschnitt 3.7) abgebildet. Der Eingabeparameter `ValidateEvidence` gem. [ETSI TS 119 512] wird auf den Eingabeparameter `VerifyRequest` gem. [BSI TR-03125-E] sowie der Rückgabeparameter `VerifyResponse` gem. [BSI TR-03125-E] auf den Rückgabeparameter `ValidateEvidenceResponse` gem. [ETSI TS 119 512] abgebildet.


Abbildung 7 ValidateEvidence/Verify – Aufruf und Antwort

3.6.1 ValidateEvidence → VerifyRequest

Hierbei werden die Kindelemente von `ValidateEvidence` folgendermaßen abgebildet:

- OptionalInputs – die in [BSI TR-03125-E] (Abschnitt 3.7.1) definierten OptionalInputs (VerifyUnderSignaturePolicy²² und ReturnVerificationReport)

²² Dieses Element ist im TR-ESOR 1.2.2 Schema Bundle nicht enthalten und wird in der nächsten Version in tr-esor-interfaces-v1.3.xsd ergänzt.

werden an die TR-ESOR-S.4-Schnittstelle durchgereicht. Andere OptionalInputs führen zu einem entsprechenden Fehler²³.

- Evidence – wird, sofern vorhanden, auf das entsprechende Kindelement von VerifyRequest/SignatureObject abgebildet, wobei die Details vom Format der Preservation Evidence gemäß Annex A.2 von [ETSI TS 119 512] abhängen:
 - ein Evidence Record gemäß RFC 4998 (A.2.2) oder RFC 6283 (A.2.3)²⁴ wird auf ein VerifyRequest/SignatureObject/Other/EvidenceRecord-Element abgebildet. Falls sich der übergebene Evidence Record auf einen Preservation Object Container (siehe PO nachstehend) bezieht, muss der Evidence Record als xaip:evidenceRecord-Element gemäß [BSI TR-03125-F] (V1.2.1, Abschnitt 3.5 bzw. V1.2.2, Abschnitt 3.1.5) bzw. [BSI TR-03125-E] (Abschnitt 3.3.1, 3.4.2) vom Typ xaip:EvidenceRecordType übergeben werden.
 - eine CAdES-Signatur gemäß [ETSI TS 119 122-3], die einen Evidence Record gemäß RFC 4998 enthält, wird auf ein VerifyRequest/SignatureObject/Base64Signature-Element abgebildet. Das FormatId-Attribut des Evidence-Elementes ist in diesem Fall gleich <http://uri.etsi.org/ades/CAdES/EvidenceRecord>.
 - andere Preservation Evidences werden nicht unterstützt und führen zu einem Fehler²⁵.
- PO ist entweder ein einfaches binäres Datenobjekt, das von der separat übergebenen Evidence geschützt wird und auf VerifyRequest/InputDocuments/Document/Base64Data abgebildet wird, oder ein unterstützter Preservation Object Container. Hierbei werden folgende Formate unterstützt:
 - XAIP v1.2 gemäß [BSI TR-03125-F] (V1.2.1, Abschnitt 3 bzw. V1.2.2, Abschnitt 3.1) (<http://www.bsi.bund.de/tr-esor/xaip/1.2>) wird in VerifyRequest/InputDocuments/Document/InlineXML übergeben.
 - LXAIP gemäß [BSI TR-03125-F] (nur V1.2.2, Abschnitt 3.2) (<http://www.bsi.bund.de/tr-esor/lxaip/1.3>) wird in VerifyRequest/InputDocuments/Document/InlineXML übergeben.
 - ASiC-ERS gemäß [BSI TR-03125-F] (nur V1.2.2, Abschnitt 3.3) und gemäß [ETSI TS 119 512] Annex A.3.1 und A.3.1.3 (<http://uri.etsi.org/ades/ASiC/type/ASiC-ERS>) wird in VerifyRequest/InputDocuments/Document/Base64Data übergeben.
 - CAdES gemäß [ETSI TS 119 512] Annex A.1.1 (<http://uri.etsi.org/ades/CAdES>) wird in VerifyRequest/InputDocuments/Document/Base64Data übergeben. Sofern kein MIME Type gesetzt ist, wird als Default <application/cms> verwendet.
 - XAdES gemäß [ETSI TS 119 512] Annex A.1.2 (<http://uri.etsi.org/ades/XAdES>) wird in VerifyRequest/InputDocuments/Document/Base64Data übergeben. Sofern kein MIME Type gesetzt ist, wird als Default <application/xml> verwendet.
 - PAdES gemäß [ETSI TS 119 512] Annex A.1.3 (<http://uri.etsi.org/ades/PAdES>) wird in VerifyRequest/InputDocuments/Document/Base64Data übergeben.

²³ <http://uri.etsi.org/19512/error/notSupported>

²⁴ XML Evidence Records nach RFC 6283 sind inkompatibel zu dem in TR-ESOR 1.2.2 verwendeten draft schema (<http://www.setcce.org/schemas/ers>). Dies wird in einer folgenden Schemaversion harmonisiert.

²⁵ <http://uri.etsi.org/19512/error/notSupported>

Sofern kein MIME Type gesetzt ist, wird als Default [application/pdf](#) verwendet.

- ASiC-E gemäß [ETSI TS 119 512] Annex A.1.4 (<http://uri.etsi.org/ades/ASiC/type/ASiC-E>) wird in `VerifyRequest/InputDocuments/Document/Base64Data` übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/vnd.etsi.asic-e+zip](#) verwendet.
- DigestList gemäß [ETSI TS 119 512] Annex A.1.6 (<http://uri.etsi.org/19512/format/DigestList>) wird in `VerifyRequest/InputDocuments/Document/Base64Data` übergeben. Sofern kein MIME Type gesetzt ist, wird als Default [application/xml](#) verwendet.

3.6.2 VerifyResponse → ValidateEvidenceResponse

- `dss:Result` – wird wie unten näher dargestellt auf `dsb:Result` abgebildet.
- `OptionalOutputs` – enthält möglicherweise einen `VerificationReport` gemäß [BSI TR-03125-VR], der auf das `pres:ValidationEvidenceReport/ValidationReport-Element` abgebildet wird. Außerdem wird im Erfolgsfall das Element `ProofOfExistence` gefüllt.

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
<code>urn:oasis:names:tc:dss:1.0:resultmajor</code>	<code>http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor</code>
Suffixes für ResultMajor	
<code>:Success</code>	<code>#ok</code> <code>#warning</code>
<code>:resultmajor:RequesterError</code> <code>:resultmajor:ResponderError</code>	<code>#error</code>
<code>:resultmajor:InsufficientInformation</code>	-
Präfix für ResultMinor	
<code>http://uri.etsi.org/19512</code>	<code>http://www.bsi.bund.de/tr-esor/api/1.2/resultminor</code>
Suffixes für ResultMinor	
<code>/error/noPermission</code>	<code>/al/common#noPermission</code>
<code>/error/internalError</code>	<code>/al/common#internalError</code>
<code>/error/parameterError</code>	<code>/al/common#parameterError</code>
<code>/error/notSupported</code>	<code>/arl/notSupported</code>

Tabelle 6 Returncodes für `ValidateEvidence` / `Verify`

3.7 Search ↔ ArchiveData

Die Funktion Search aus [ETSI TS 119 512] wird auf die Funktion ArchiveData gemäß [BSI TR-03125-E] (Abschnitt 3.6) abgebildet. Der Eingabeparameter Search aus [ETSI TS 119 512] wird auf den Eingabeparameter ArchiveDataRequest aus [BSI TR-03125-E] und der Rückgabeparameter ArchiveDataResponse aus [BSI TR-03125-E] auf den Rückgabeparameter SearchResponse aus [ETSI TS 119 512] abgebildet.

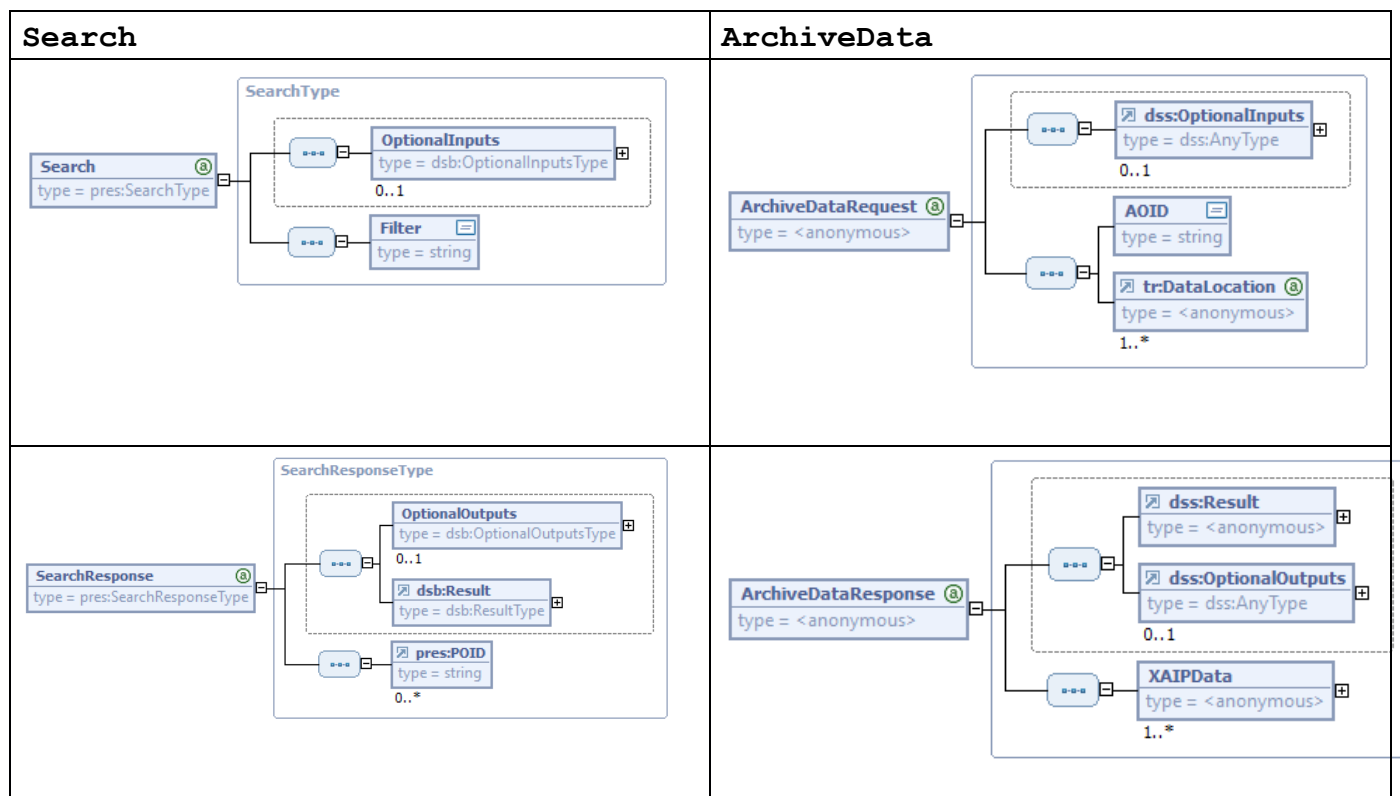


Abbildung 8 Search / ArchiveData – Aufruf und Antwort

3.7.1 Search → ArchiveDataRequest

Hierbei werden die Kindelemente von Search folgendermaßen auf ArchiveDataRequest abgebildet:

- Filter – enthält eine durch das folgende JSON-Schema definierte Struktur:

```

"FilterType": {
  "type": "object",
  "properties": {
    "AOID": {
      "type": "string"
    },
    "XPath": {
      "type": "string"
    }
  },
  "required": ["AOID", "XPath"]
}

```


Hierbei besitzen die Parameter folgende Semantik:

- AOID – identifiziert ein bestimmtes Preservation Object und wird auf das ArchiveDataRequest/AOID-Element abgebildet.
- XPathFilter – spezifiziert das Datenobjekt innerhalb des XAIP, das über die AOID adressiert und auf das ArchiveDataRequest/DataLocation abgebildet wird. Dieses Element wurde im Schema tr-esor-interfaces-v1.2+xmlmime.xsd ergänzt.

Hierbei wird unterstellt, dass die ArchiveDataRequest-Implementierung der angeschlossenen TR-ESOR-Middleware zumindest einfache XPath-Ausdrücke unterstützt, die den Abruf eines Datenelements ermöglichen, das durch eine ID in der XML-Struktur des per AOID adressierten XAIP ermöglicht.

3.7.2 ArchiveDataResponse → SearchResponse

- dss:Result – wird wie unten näher dargestellt auf dsb:Result abgebildet.
- OptionalOutputs – sind nicht vorhanden und führen zu einem Fehler²⁶.
- XAIPData – werden auf SearchResponse/OptionalOutputs/Other/XAIPData abgebildet.

Die Fehlercodes setzen sich aus einem generellen Präfix und einem spezifischen Suffix zusammen und werden folgendermaßen abgebildet:

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
urn:oasis:names:tc:dss:1.0:resultmajor	http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor
Suffixes für ResultMajor	
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Präfix für ResultMinor	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.2/resultminor
Suffixes für ResultMinor	
/error/noPermission	/al/common#noPermission
/error/internalError	/al/common#internalError
/error/parameterError	/al/common#parameterError

²⁶ <http://uri.etsi.org/19512/error/notSupported>

ETSI TS 119 512	BSI TR-03125-E
Präfix für ResultMajor	
urn:oasis:names:tc:dss:1.0:resultmajor	http://www.bsi.bund.de/tr-esor/api/1.2/resultmajor
Suffixes für ResultMajor	
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Präfix für ResultMinor	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.2/resultminor
Suffixes für ResultMinor	
	/arl/unknownLocation
	/arl/unknownAOID
/error/notSupported	/arl/notSupported

Tabelle 7 Returncodes für Search / ArchiveData

4. Referenzen

- [BSI TR-03125-E] BSI: Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-E, Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, Version 1.2.2 oder Version 1.2.1, www.bsi.bund.de/EN/tr-esor oder <https://www.bsi.bund.de/tr-esor>
- [BSI TR-03125-F] BSI: Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-F, Formate, Version 1.2.2 oder Version 1.2.1, www.bsi.bund.de/EN/tr-esor oder <https://www.bsi.bund.de/tr-esor>
- [BSI TR-03125-VR] BSI: Preservation of Evidence of Cryptographically Signed Documents, BSI TR-03125, Annex TR-ESOR-VR: Verification Reports for Selected Data Structures, Version 1.2.1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_VR_V1_2_1.pdf
- [eCard-2] BSI: eCard-API-Framework – Part 2 – eCard-Interface, BSI TR-03112-2
- [ETSI TS 119 122-3] ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CADES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CADES, V1.1.1
- [ETSI TS 119 512] ETSI TS 119 512: Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services, V1.1.2