Federal Office
for Information Security

BSI Technical Guideline 03125

Preservation of Evidence of Cryptographically Signed Documents

Appendix to Annex TR-ESOR-E: Concretisation of the Interfaces based on the eCard API Framework and ETSI TS 119 512

Designation	General Specification **ETSI TS119512 TR-ESOR Transformator**
Abbreviation	BSI TR-ESOR-TRANS
Version	1.3
Date	03. Mai 2022

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn, Germany
Phone: +49 228 99 9582-0
Email: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

Contents

Figures

Tables

1. Summary

The present document specifies the BSI Transformator component 'ETSI TS119512 TR-ESOR Transformator', which maps a suitably profiled instance of the Preservation API defined in [ETSI TS 119 512] to the TR-S.4 interface defined in [TR-ESOR-E], version 1.3.

2. Objective

The Federal Office for Information Security (BSI) is the German government agency responsible for secure information processing and competence centre for electronic signatures.

Acting in these capacities, the BSI has developed a Technical Guideline for the 'Preservation of Evidence of Cryptographically Signed Documents' (TR-03125/TR-ESOR), which encompasses in particular the TR-S.4 interface defined in [TR-ESOR-E], version 1.3.

From the starting-point of the TR-S.4 interface, the BSI has also supported the standardisation of Preservation Services at ETSI ESI, with the Preservation API defined in [ETSI TS 119 512] being a key product of this work.

Working from this basis, an 'ETSI TS119512 TR-ESOR Transformator' has been developed and released as open source following the completion of the project. The Transformator maps calls to the Preservation API developed by ETSI ESI (also called as TR-S.512 for short) to corresponding calls to the TR-S.4 interface. In this way, the ETSI TS119512 TR-ESOR Transformator ensures that version 1.3 TR-ESOR middleware products already supporting the TR-S.4 interface can also offer a suitable Preservation API profile without any need for changing the TR-ESOR product. The designation 'TS 119 512 Transformator' or 'TR-ESOR Transformator' is also used as a short form for the ETSI TS119512 TR-ESOR Transformator, as is the case with the following Figure 1, for example.

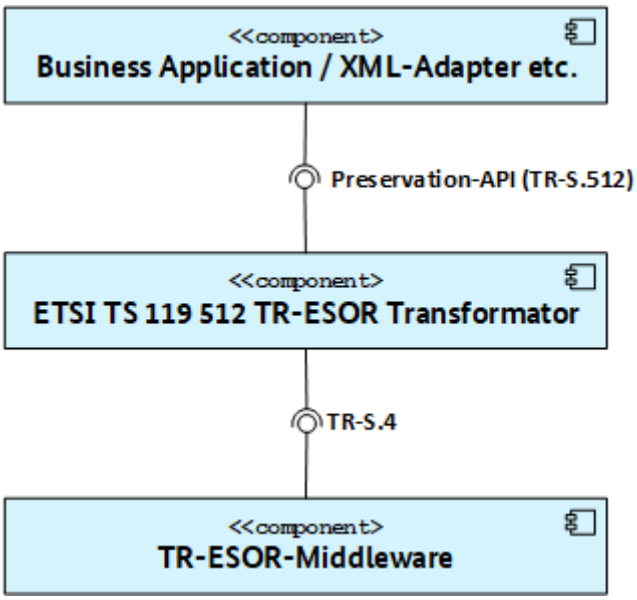

Figure 1 System with the ETSI TS119512 TR-ESOR Transformator

3. Specification

3.1 RetrieveInfo

The `RetrieveInfo` function accourding to [ETSI TS 119 512] returns a statically defined `Profile` element which corresponds to the range of functions of the TR-S.512 interface in use.

The `Profile` element has the following child elements (c.f. [ETSI TS 119512], section 5.4.7):

- `ProfileIdentifier` – http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/V1.1.2
- `Specification` – URL-based references to the published specification documents [TR-ESOR-E] and [ETSI TS 119 512]
- `Operation` – specifies the relevant information regarding the supported functions and formats (see following sections for details, note that the statically defined profile has to reflect the range of functions supported by the used TR-S.4 interface)
- `Policy/PolicyByRef/PolicyID` – URL-based reference to the policy to be defined
- `SchemeIdentifier` – http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers
- `ProfileValidityPeriod/ValidFrom` – configurable date
- `PreservationStorageModel` – in this case predefined fixed as `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 (this value, where applicable, is assumed as the default value if the `EvidenceFormat` element is not specified)
  - urn:ietf:rfc:6283:EvidenceRecord

The return codes can be found in [ETSI TS 119 512], section 5.3.2.2.1.

3.2 PreservePO ↔ ArchiveSubmission

Following a call to `PreservePO` from [ETSI TS 119 512], the input parameter `PreservePO` from [ETSI TS 119 512] is mapped to an input parameter `ArchiveSubmissionRequest` defined in [TR-ESOR-E] and, conversely, the return parameter from `ArchiveSubmissionResponse` defined in [TR-ESOR-E] is mapped to the return parameter `PreservePOResponse` from [ETSI TS 119 512].

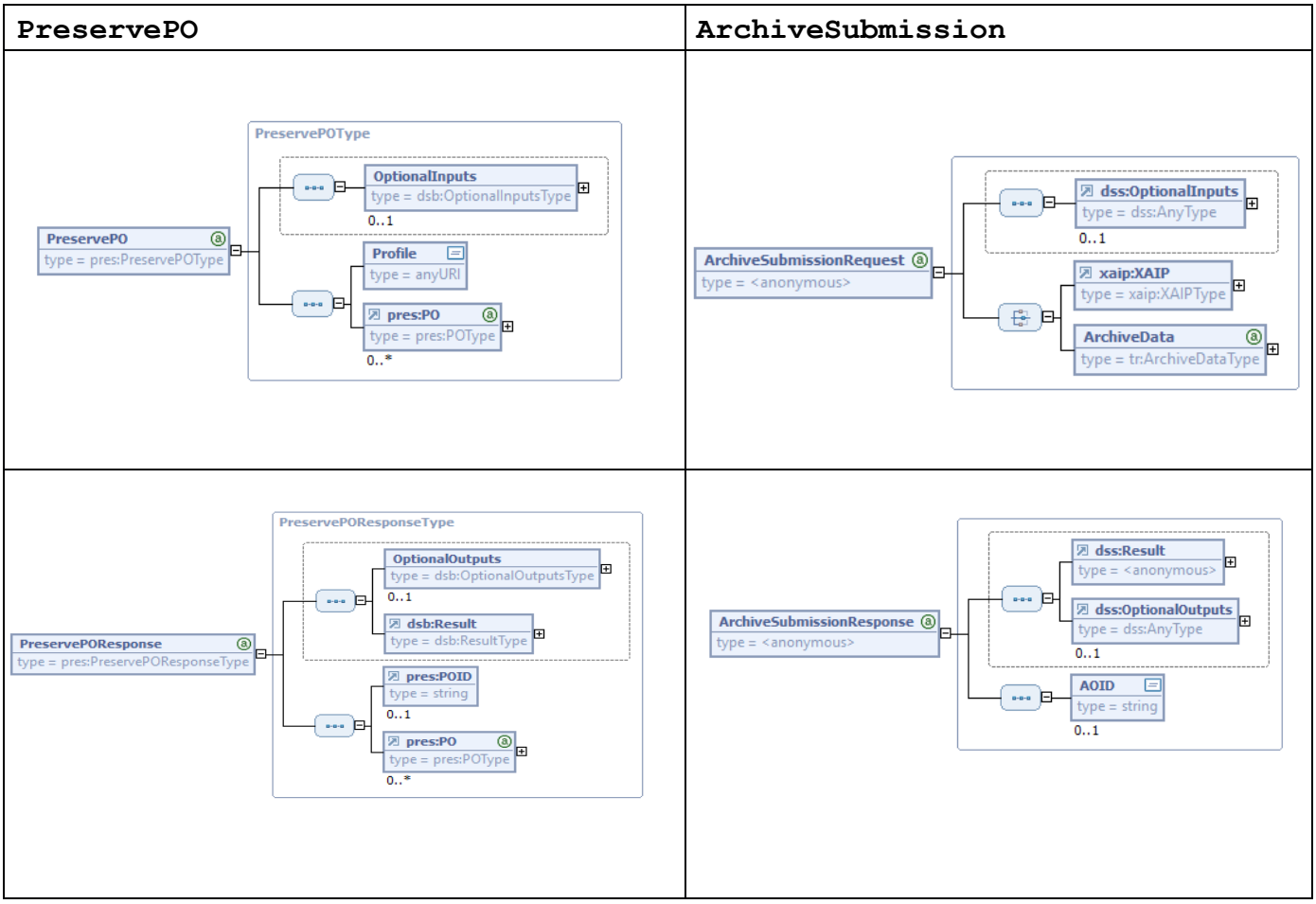

Figure 2 `PreservePO/ArchiveSubmission` – request and response

3.2.1 PreservePO → ArchiveSubmissionRequest

Here, the parameters in `PreservePO` are handled as follows:

- `OptionalInputs` – the `OptionalInputs` (`AOID`, `ReturnVerificationReport` and `ImportEvidence`) defined in [TR-ESOR-E] are passed on to the TR-S.4 interface if they were passed in the `PreservePO` request. Other `OptionalInputs` trigger a corresponding error[1].
- `Profile` – expects http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/V1.1.2http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/V1.1.2, which clarifies the fact that the profile specified in this document (see also section 3.1) is being requested.
- `PO` – contains exactly one 'preservation object', which is passed in the `ArchiveSubmissionRequest`. The following formats are supported here:
  - XAIP v1.3 as defined in [TR-ESOR-F], section 3.1 and as defined in [ETSI TS 119 512], Annexes A1.5 and A.3.2 (http://www.bsi.bund.de/tr-esor/xaip/1.3) is passed in `ArchiveSubmissionRequest/XAIP`.

[1] http://uri.etsi.org/19512/error/notSupported

- LXAIP as defined in [TR-ESOR-F], section 3.2 and as defined in [ETSI TS 119 512] Annex A.3.2 (http://www.bsi.bund.de/tr-esor/lxaip/1.3) is passed in `ArchiveSubmissionRequest/XAIP`.
- ASiC-ERS as defined in [TR-ESOR-F], section 3.3 and as defined in [ETSI TS 119 512] Annex A.3.1 (http://uri.etsi.org/ades/ASiC/type/ASiC-ERS) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [BSI TR-03125-E], section 3.1.1.
- CAdES as defined in [ETSI TS 119 512] Annex A.1.1 (http://uri.etsi.org/ades/CAdES) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [TR-ESOR-E], section 3.1.1. If a MIME type is not set, `application/cms` is used as the default.
- XAdES as defined in [ETSI TS 119 512] Annex A.1.2 (http://uri.etsi.org/ades/XAdES) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [TR-ESOR-E], section 3.1.1. If a MIME type is not set, `application/xml` is used as the default.
- PAdES as defined in [ETSI TS 119 512] Annex A.1.3 (http://uri.etsi.org/ades/PAdES) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [TR-ESOR-E], section 3.1.1.If a MIME type is not set, `application/pdf` is used as the default.
- ASiC-S as defined in [ETSI TS 319 162] (http://uri.etsi.org/ades/ASiC/type/ASiC-S) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [TR-ESOR-E], section 3.1.1. If a MIME type is not set, `application/vnd.etsi.asic-s+zip` is used as the default.
- ASiC-E as defined in [ETSI TS 119 512] Annex A.1.4 (http://uri.etsi.org/ades/ASiC/type/ASiC-E) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [TR-ESOR-E] , section 3.1.1. If a MIME type is not set, `application/vnd.etsi.asic-e+zip` is used as the default.
- DigestList as defined in [ETSI TS 119 512] Annex A.1.6 (http://uri.etsi.org/19512/format/DigestList) is passed in `ArchiveSubmissionRequest/ArchiveData` as a `binaryData` element as defined in [TR-ESOR-E], section 3.1.1.https://www.iana.org/assignments/media-types/application/vnd.etsi.asic-e+ziphttps://www.iana.org/assignments/media-types/application/vnd.etsi.asic-e+zip

3.2.2 ArchiveSubmissionResponse → PreservePOResponse

- `dss`[2]`:Result` – is mapped to `dsb`[3]`:Result`, as explained in more detail below.

[2] Namespace 'dss' is resolved to 'urn:oasis:names:tc:dss:1.0:core:schema'.

[3] Namespace 'dsb' is resolved to 'http://docs.oasis-open.org/dss-x/ns/base'.

- `OptionalOutputs` – the `VerificationReport` element pursuant to [TR-ESOR-E], section 3.1.2 potentially returned in `OptionalOutputs` is passed on to the element of the same name in the Preservation API.
- `AOID` – is mapped to `POID`.

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

ETSI TS 119 512	BSI TR-03125-E
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Prefix for `ResultMinor`	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.3/resultminor
Suffixes for `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[4]	/resultminor/arl/existingAOID

Table 1 Return codes for `PreservePO/ArchiveSubmission`

3.3 UpdatePOC ↔ ArchiveUpdate

The function `UpdatePOC` from [ETSI TS 119 512] is mapped to the function `ArchiveUpdate` defined in [TR-ESOR-E]. The input parameter `UpdatePOC` as defined in [ETSI TS 119 512] is correspondingly mapped to the input parameter `ArchiveUpdateRequest` as defined in [TR-ESOR-E] and, conversely, the return parameter `ArchiveUpdateResponse` as defined in [TR-ESOR-E] is mapped to the return parameter `UpdatePOCResponse` from [ETSI TS 119 512].

[4] This error code does not exist in [ETSI TS 119 512] and arises because of the addition of `OptionalInputs/AOID`.

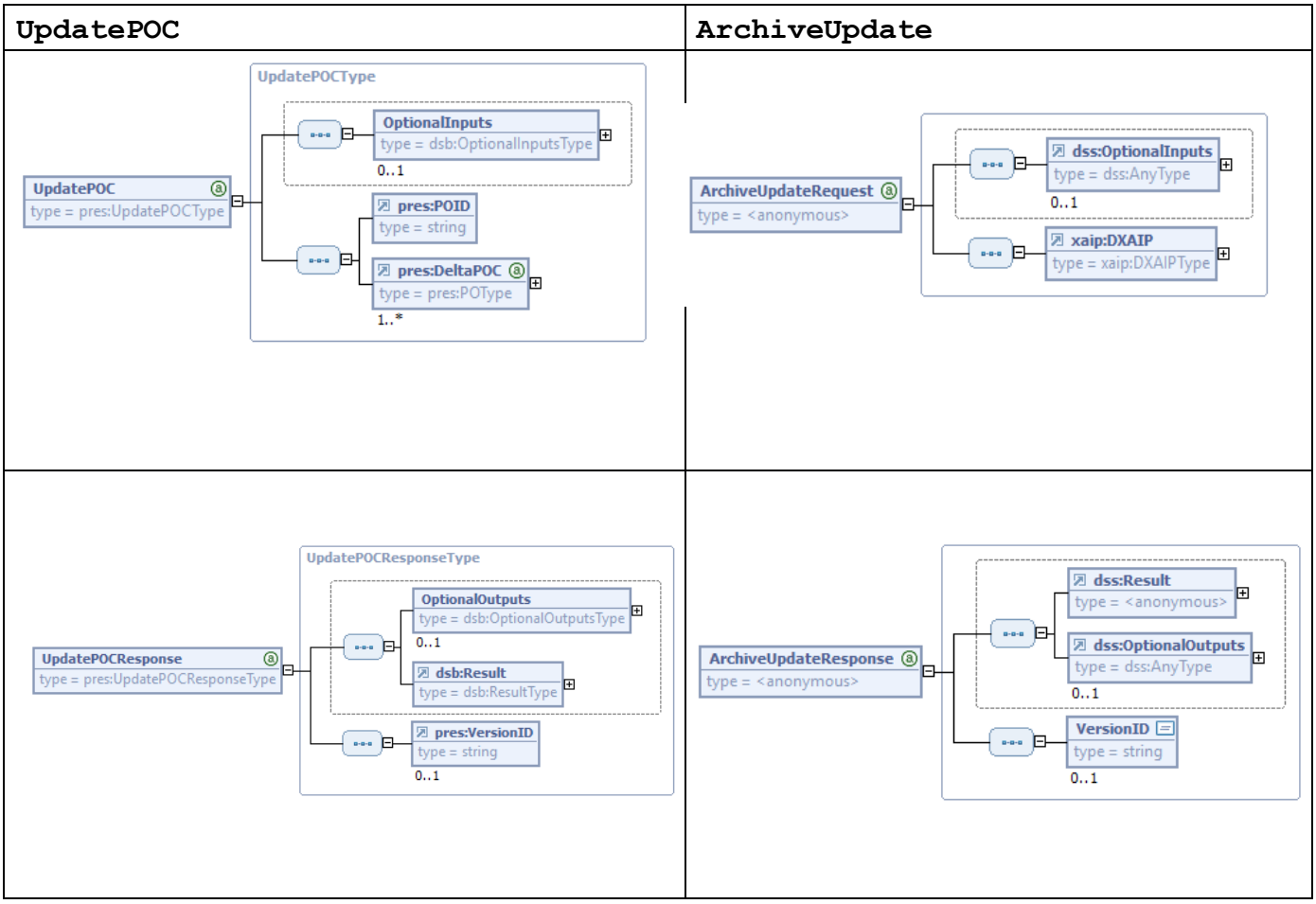

Figure 3 `UpdatePOC/ArchiveUpedate` – request and response

3.3.1 UpdatePOC → ArchiveUpdateRequest

Here, the parameters in `UpdatePOC` are handled as follows:

- `OptionalInputs` – the `OptionalInputs` (in particular `ReturnVerificationReport` and `ImportEvidence`) defined in [TR-ESOR-E] are passed to the TR-S.4 interface via `dss:OptionalInputs`. Other `OptionalInputs` trigger a corresponding error[5].
- `POID` – must be identical to `DXAIP/PackageHeader/AOID`. Used for consistency checking and returns a corresponding error if no match is found [6].
- `DeltaPOC` – is passed in an `ArchiveUpdateRequest/DXAIP` element and must either be a
    - Delta-XAIP element as defined in **[TR-ESOR-F]** section 3.1.6 (`FormatId`=http://www.bsi.bund.de/tr-esor/dxaip/1.3[7]) or a

[5] http://uri.etsi.org/19512/error/notSupported

[6] http://uri.etsi.org/19512/error/DeltaPOCInternalProblem

[7] This URL must be added in a future version of ETSI TS 119 512.

- Delta-LXAIP element as defined in **[TR-ESOR-F]** section 3.2.4 (`FormatId`=http://www.bsi.bund.de/tr-esor/dlxaip/1.3[8]).

3.3.2 ArchiveUpdateResponse → UpdatePOCResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below.
- `OptionalOutputs` – the `VerificationReport` element pursuant to [TR-ESOR-E], section 3.2.2 potentially returned in `dss:OptionalOutputs` is passed on to the element of the same name in the Preservation API.
- `VersionID` – is mapped to the element of the same in the Preservation API.

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

[8] This URL must be added in a future version of ETSI TS 119 512.

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
urn:oasis:names:tc:dss:1.0:resultmajor	http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor
Suffixes for `ResultMajor`	
:Success	#ok #warning
:resultmajor:RequesterError :resultmajor:ResponderError	#error
:resultmajor:InsufficientInformation	-
Prefix for `ResultMinor`	
http://uri.etsi.org/19512	http://www.bsi.bund.de/tr-esor/api/1.3/resultminor
Suffixes for `ResultMinor`	
/error/noPermission	/al/common#noPermission
/error/internalError	/al/common#internalError
/error/externalServiceUnavailable	
/error/parameterError	/al/common#parameterError
/error/transferError	
/error/notSupported	/arl/notSupported
/error/unknownDeltaPOCType	
/error/noSpaceError	/arl/noSpaceError
/error/unknownPOID	/arl/DXAIP_NOK_AOID
/error/DeltaPOCInternalProblem	/arl/existingPackageInfoWarning /arl/DXAIP_NOK /arl/DXAIP_NOK_EXPIRED /arl/DXAIP_NOK_SUBMTIME /arl/DXAIP_NOK_SIG /arl/DXAIP_NOK_ID /arl/DXAIP_NOK_Version
/error/POFormatError	/arl/XAIP_NOK_ER
/warning/lowSpace	/arl/lowSpaceWarning

Table 2 Return codes for `UpdatePOC/ArchiveUpdate`

3.4 RetrieveTrace ↔ ArchiveTrace

The function `RetrieveTrace` from [ETSI TS 119 512] is mapped to the function `ArchiveTrace` defined in [TR-ESOR-E]. The input parameter `RetrieveTrace` as defined in [ETSI TS 119 512] is correspondingly mapped to the input parameter `ArchiveTraceRequest` as defined in [TR-ESOR-E] and, conversely, the return parameter `ArchiveTraceResponse` as defined in [TR-ESOR-E] is mapped to the return parameter `RetrieveTraceResponse` from [ETSI TS 119 512].

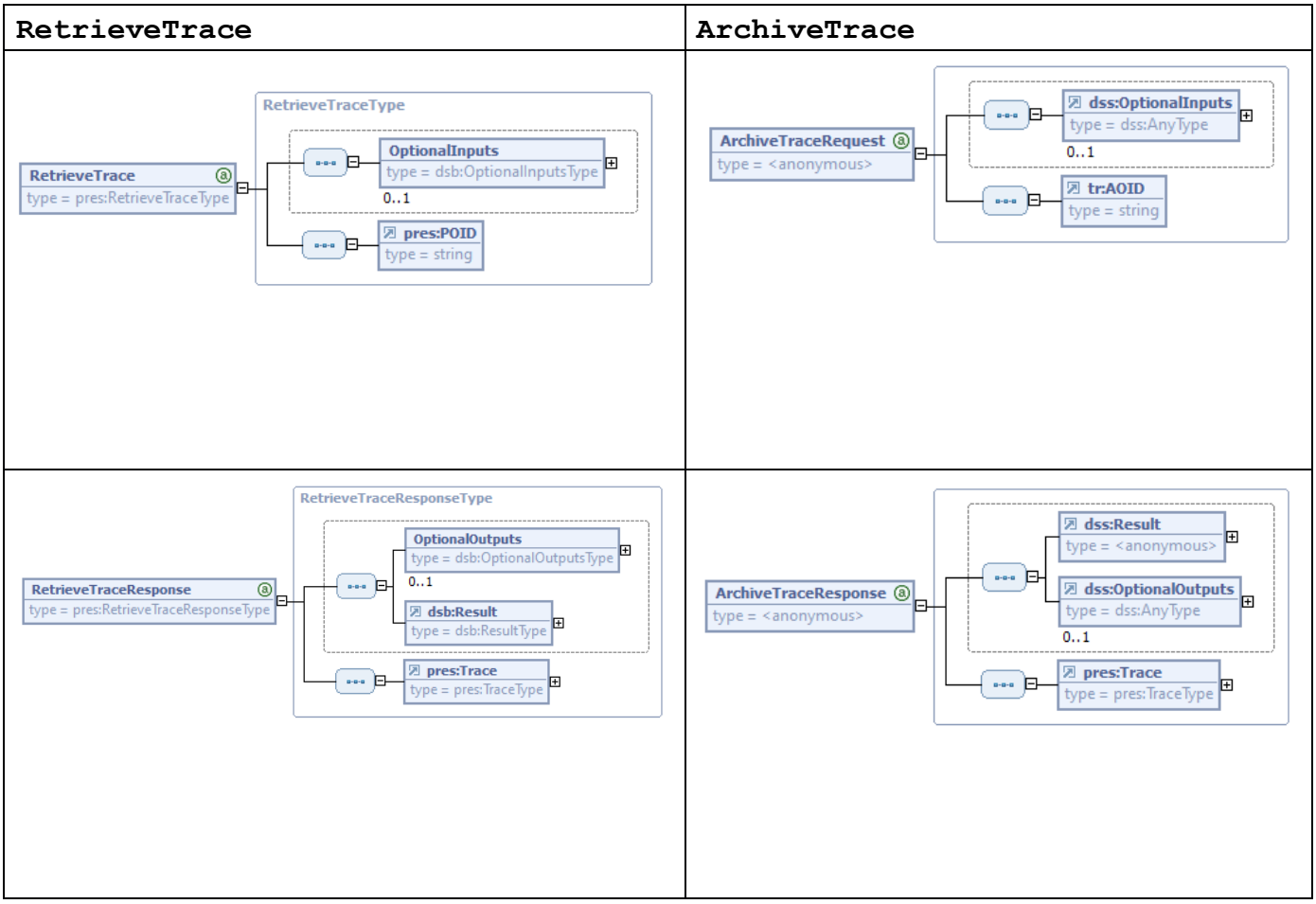

Figure 4 `RetrieveTrace/ArchiveTrace` – request and response

3.4.1 RetrieveTrace ⟶ ArchiveTraceRequest

Here, the parameters in `RetrieveTrace` are handled as follows:

- `OptionalInputs` – any optional input element in `OptionalInputs` is provided to the TR-S.4 interface via `dss:OptionalInputs`. As there are no optional input elements defined in [TR-ESOR-E] any optional input element will trigger a corresponding error[9].
- `pres:POID` – will be mapped to `tr:AOID`.

3.4.2 ArchiveTraceResponse ⟶ RetrieveTraceResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below.
- `OptionalOutputs` – any optional output element from `dss:OptionalOutputs` is passed on to the element of the same name in the Preservation API.
- `pres:Trace` – is mapped to the element of the same name in the Preservation API.

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

[9] http://uri.etsi.org/19512/error/notSupported

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
`urn:oasis:names:tc:dss:1.0:resultmajor`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor`
Suffixes for `ResultMajor`	
`:Success`	`#ok` `#warning`
`:resultmajor:RequesterError` `:resultmajor:ResponderError`	`#error`
`:resultmajor:InsufficientInformation`	-
Prefix for `ResultMinor`	
`http://uri.etsi.org/19512`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultminor`
Suffixes for `ResultMinor`	
`/error/noPermission`	`/al/common#noPermission`
`/error/internalError`	`/al/common#internalError`
`/error/externalServiceUnavailable`	
`/error/parameterError`	`/al/common#parameterError`
`/error/transferError`	
`/error/notSupported`	`/arl/notSupported`

Table 3 Return codes for `RetrieveTrace/ArchiveTrace`

3.5 RetrievePO ↔ ArchiveRetrieval/ArchiveEvidence

The `RetrievePO` call from [ETSI TS 119 512] is mapped to the calls `ArchiveRetrieval` and `ArchiveEvidence` as defined in [TR-ESOR-E]. The input parameter `RetrievePO` as defined in [ETSI TS 119 512] is accordingly mapped to the corresponding `ArchiveRetrievalRequest` or `ArchiveEvidenceRequest` parameter as defined in [TR-ESOR-E]. Conversely, the return parameter `ArchiveRetrievalResponse` or `ArchiveEvidenceResponse` as defined in [TR-ESOR-E] is mapped to the return parameter `RetrievePOResponse` from [ETSI TS 119 512].

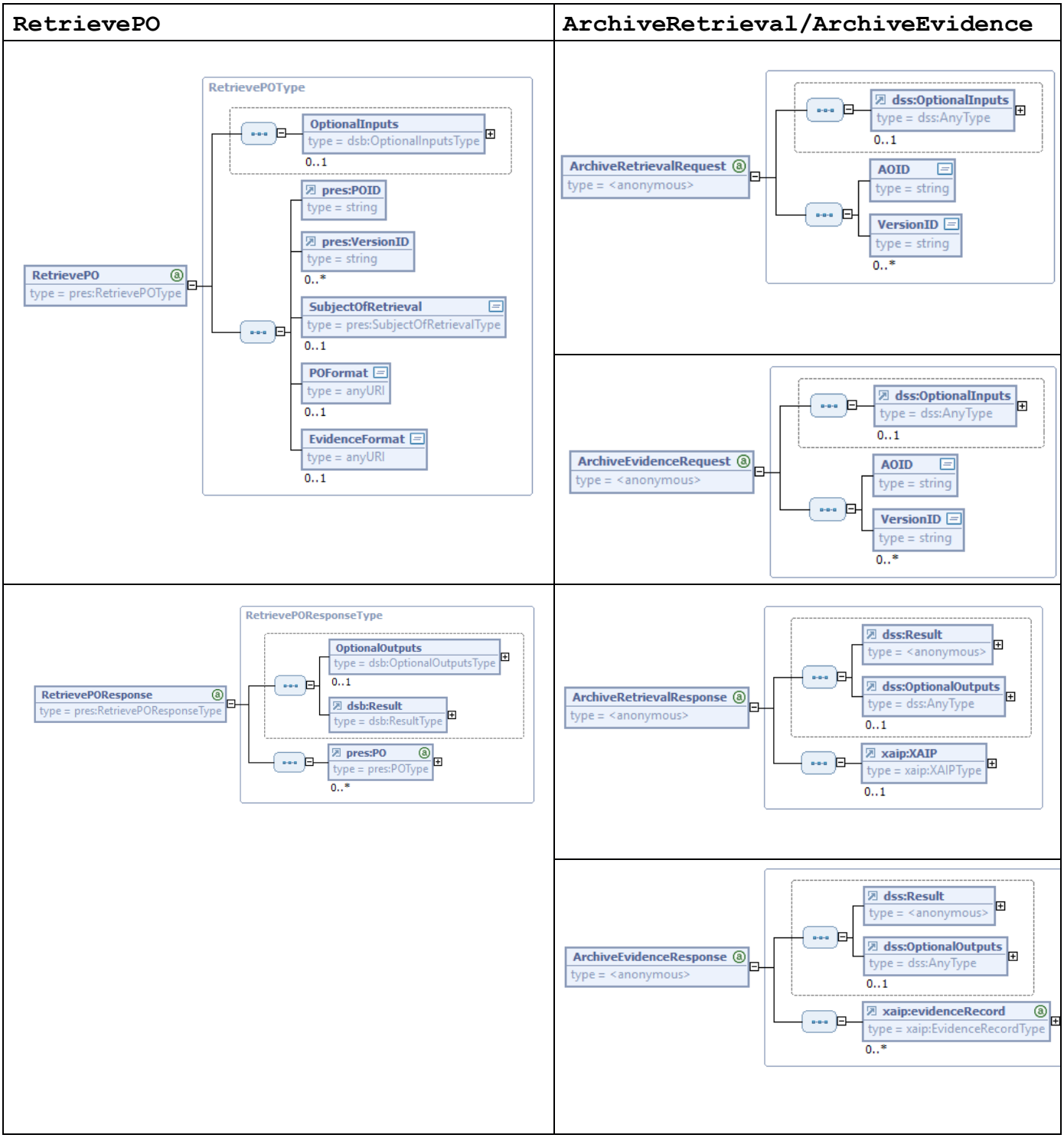

Figure 5 `RetrievePO/ArchiveRetrieval/EvidenceRetrieval` – request and response

3.5.1 RetrievePO ⟶ ArchiveRetrievalRequest/ArchiveEvidenceRequest

Here, the child elements of `RetrievePO` are handled as follows:

- `OptionalInputs` lead to an error when calling `RetrievePO`[10].

[10] http://uri.etsi.org/19512/error/notSupported

- `POID` is mapped to `ArchiveRetrievalRequest/AOID` or `ArchiveEvidenceRequest/AOID`: the choice of `ArchiveEvidenceRequest` or `ArchiveRetrievalRequest` is made based on the `SubjectOfRetrieval` parameter.
- `VersionID` is mapped to `ArchiveRetrievalRequest/VersionID` or `ArchiveEvidenceRequest/VersionID`.
- `SubjectOfRetrieval` specifies whether `ArchiveRetrievalRequest` or `ArchiveEvidenceRequest` is called and is one of the following:
  - `PO` – to retrieve the (L)XAIP or ASiC-ERS without a corresponding Evidence Record, so that `ArchiveRetrievalRequest` is called
  - `Evidence` – to retrieve Evidence Records, so that `ArchiveEvidenceRequest` is called. Here, the Evidence Record is returned as an `xaip:evidenceRecord` element as defined in [TR-ESOR-F], section 3.1.5 of the type `xaip:EvidenceRecordType`, which must also contain the attributes `AOID` and `VersionID`.
  - `POwithEmbeddedEvidence` – to retrieve the (L)XAIP or ASiC-ERS with corresponding Evidence Record, which is implemented by a call to `ArchiveRetrievalRequest` while utilising the `OptionalInputs/IncludeERS` from [TR-ESOR-E], section 3.3.1. This value is assumed as the default value if the `SubjectOfRetrieval` element is not specified.
  - `POwithDetachedEvidence` – is not supported and returns an error[11].
- `POFormat` is mapped to `ArchiveRetrievalRequest/OptionalInputs/POFormat` from [TR-ESOR-E], section 3.3.1 and is one of the following:
  - http://www.bsi.bund.de/tr-esor/xaip/1.3 for XAIP v1.3 as defined in [TR-ESOR-F], section 3). This value is assumed as the default value if the `POFormat` element is not specified.
  - http://www.bsi.bund.de/tr-esor/lxaip/1.3 for LXAIP as defined in [TR-ESOR-F], section 3.2
  - http://uri.etsi.org/ades/ASiC/type/ASiC-ERS for ASiC-ERS

  Please note: within the scope of TR-S.4, an XAIP or LXAIP is returned in the `ArchiveRetrievalResponse/XAIP` element and an ASiC-AIP is returned in an `ArchiveRetrievalResponse/OptionalOutputs/PO`.
- `EvidenceFormat` is one of the following:
  - `urn:ietf:rfc:4998:EvidenceRecord` (This value, where applicable, is assumed as the default value if the `EvidenceFormat` element is not specified.)
  - `urn:ietf:rfc:6283:EvidenceRecord`[12]

  At the TR-S.4 interface, this corresponds to `ArchiveEvidenceRequest/OptionalInputs/ERSFormat` (see [TR-ESOR-E], section 3.4.1) or `ArchiveRetrievalRequest/OptionalInputs/IncludeERS` (see [TR-ESOR-E], section 3.3.1). The `EvidenceRecord` is returned as an `xaip:evidenceRecord` element as defined in [TR-ESOR-F], section 3.5 or [TR-ESOR-E], sections 3.3.1 and 3.4.2 of the type `xaip:EvidenceRecordType`.

11 http://uri.etsi.org/19512/error/notSupported

12 In this context, note that the corresponding URI defined in [BSI TR-03125-E] is `urn:ietf:rfc:6283`.

3.5.2 ArchiveRetrievalResponse ⟶ RetrievePOResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below.
- `OptionalOutputs` – the `PO` Element (cf. [TR-ESOR-E], section 3.3.2) potentially returned in `OptionalOutputs` is returned with a base64Binary-coded ASiC-AIP in the `RetrievePOResponse/PO` element.
- `XAIP` – with an XAIP or LXAIP, mapping to the `RetrievePOResponse/PO` element takes place.

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
`urn:oasis:names:tc:dss:1.0:resultmajor`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor`
Suffixes for `ResultMajor`	
`:Success`	`#ok` `#warning`
`:resultmajor:RequesterError` `:resultmajor:ResponderError`	`#error`
`:resultmajor:InsufficientInformation`	-
Prefix for `ResultMinor`	
`http://uri.etsi.org/19512`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultminor`
Suffixes for `ResultMinor`	
`/error/noPermission`	`/al/common#noPermission`
`/error/internalError`	`/al/common#internalError`
`/error/parameterError`	`/al/common#parameterError`
`/error/transferError`[13]	
`/error/notSupported`	`/arl/notSupported`
`/error/unknownPOFormat`	`/arl/unknownPOFormat`
`/error/unknownPOID`	`/arl/unknownAOID`
`/error/unknownVersionID`	`/arl/unknownVersionID`
`/warning/requestOnlyPartlySuccessful`	`/arl/requestOnlyPartlySuccessfulWarning`

Table 4 Return codes for `RetrievePO/ArchiveRetrieval`

[13] This error code is not currently present in [ETSI TS 119 512] for `RetrievePOResponse`. It might be advisable to add this error code as appropriate at some point in the future.

3.5.3 ArchiveEvidenceResponse → RetrievePOResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below.
- `OptionalOutputs` – not present in `ArchiveEvidenceResponse` as defined in [TR-ESOR-E] (cf. section 3.4.2) and trigger a corresponding error [14] at the Preservation API as defined in [ETSI TS 119 512].
- `evidenceRecord` – is mapped to the `RetrievePOResponse/PO` element, whereby the format for the Evidence Record returned is reflected in the `FormatId` attribute of the `PO` element.

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
`urn:oasis:names:tc:dss:1.0:resultmajor`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor`
Suffixes for `ResultMajor`	
`:Success`	`#ok` `#warning`
`:resultmajor:RequesterError` `:resultmajor:ResponderError`	`#error`
`:resultmajor:InsufficientInformation`	-
Prefix for `ResultMinor`	
`http://uri.etsi.org/19512`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultminor`
Suffixes for `ResultMinor`	
`/error/noPermission`	`/al/common#noPermission`
`/error/internalError`	`/al/common#internalError`
`/error/parameterError`	`/al/common#parameterError`
`/error/notSupported`	`/arl/notSupported`[15]
`/error/unknownEvidenceFormat`	
`/error/unknownPOID`	`/arl/unknownAOID`
`/error/unknownVersionID`	`/arl/unknownVersionID`
`/warning/requestOnlyPartlySuccessful`	`/arl/requestOnlyPartlySuccessfulWarning`

[14] http://uri.etsi.org/19512/error/notSupported

[15] As an alternative, one option in the future would be to add a specific error code …/`arl/unknownEvidenceFormat` for `ArchiveEvidenceResponse` in [TR-ESOR-E].

Table 5 Return codes for `RetrievePO/ArchiveEvidence`

3.6 DeletePO ↔ ArchiveDeletion

The call to `DeletePO` from [ETSI TS 119 512] is mapped to a call to `ArchiveDeletion` as defined in [TR-ESOR-E]. The input parameter `DeletePO` as defined in [ETSI TS 119 512] is correspondingly mapped to the input parameter `ArchiveDeleteRequest` as defined in [TR-ESOR-E] and, conversely, the return parameter `ArchiveDeletionResponse` as defined in [TR-ESOR-E] is mapped to the return parameter `DeletePOResponse` from [ETSI TS 119 512].

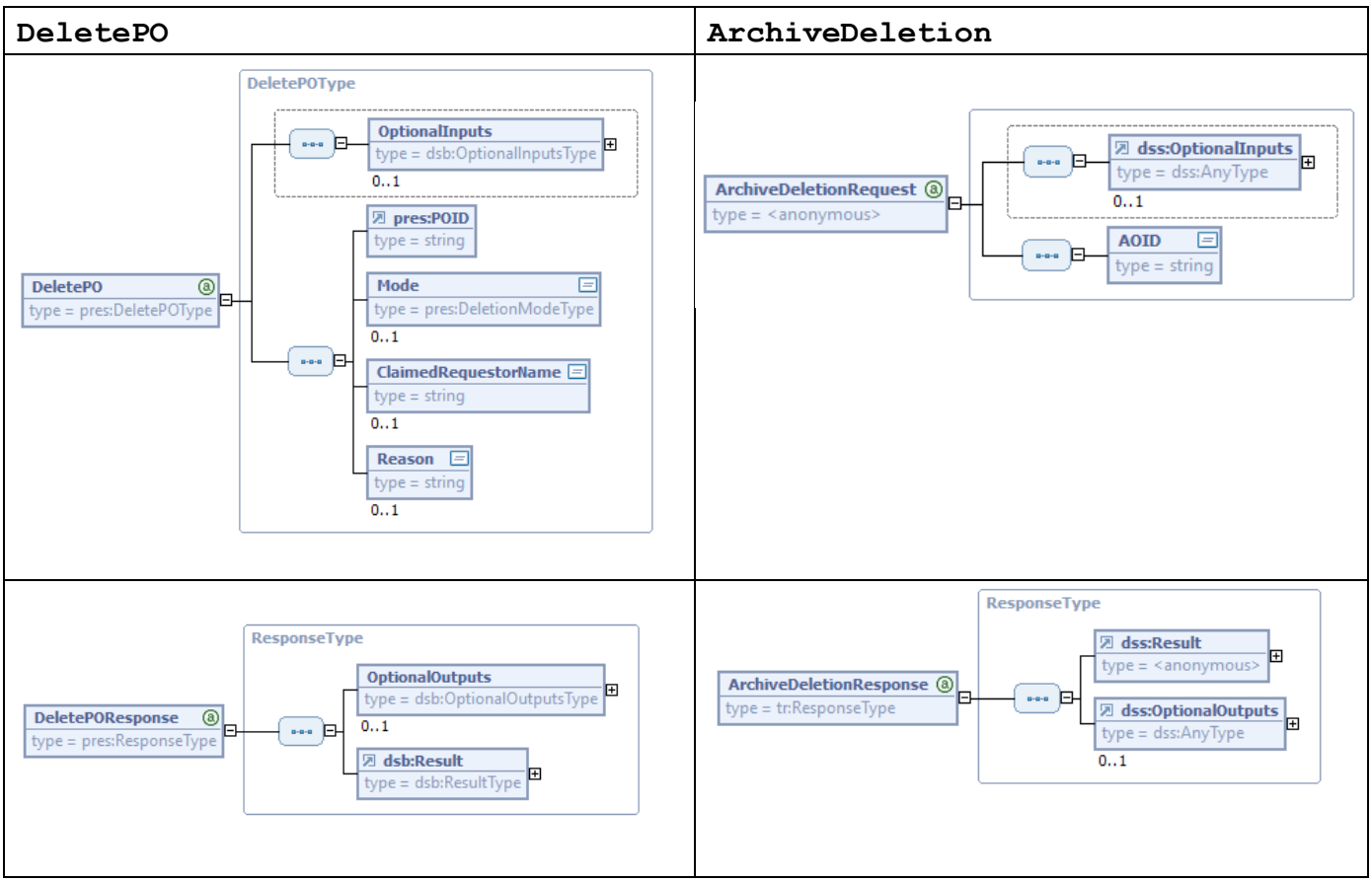

Figure 6 `DeletePO/ArchiveDeletion` – request and response

3.6.1 DeletePO → ArchiveDeletionRequest

Here, the child elements of `DeletePO` are mapped as follows:

- `OptionalInputs` lead to an error when calling `DeletePO`[16].
- `POID` is mapped to `ArchiveDeletionRequest/AOID`.
- `Mode` shall equal `SubDOsAndEvidence` or shall not be present. In the case of a request using correct syntax, but where mode is equal to `OnlySubDOs`, deletion is not performed and an error[17] is returned.

[16] http://uri.etsi.org/19512/error/notSupported

[17] http://uri.etsi.org/19512/error/notSupported

- `ClaimedRequestorName` is mapped to `ArchiveDeletionRequest/OptionalInputs/ReasonOfDeletion/RequestorName`.
- `Reason` is mapped to `ArchiveDeletionRequest/OptionalInputs/ReasonOfDeletion/RequestInfo`.

3.6.2 ArchiveDeletionResponse → DeletePOResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below.
- `OptionalOutputs` – not present in `ArchiveDeletionResponse` as defined in [TR-ESOR-E] (cf. section 3.5.2) and trigger a corresponding error [18] at the Preservation API as defined in [ETSI TS 119 512].

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
`urn:oasis:names:tc:dss:1.0:resultmajor`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor`
Suffixes for `ResultMajor`	
`:Success`	`#ok` `#warning`
`:resultmajor:RequesterError` `:resultmajor:ResponderError`	`#error`
`:resultmajor:InsufficientInformation`	-
Prefix for `ResultMinor`	
`http://uri.etsi.org/19512`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultminor`
Suffixes for `ResultMinor`	
`/error/noPermission`	`/al/common#noPermission`
`/error/internalError`	`/al/common#internalError`
`/error/parameterError`	`/al/common#parameterError`
	`/arl/missingReasonOfDeletion`
`/error/notSupported`	`/arl/notSupported`
`/error/unknownPOID`	`/arl/unknownAOID`

Tabelle 6 Return codes for `DeletePO/ArchiveDeletion`

[18] http://uri.etsi.org/19512/error/notSupported

3.7 ValidateEvidence ↔ Verify

The function `ValidateEvidence` from [ETSI TS 119 512] is mapped to the function `Verify` defined in [TR-ESOR-E] (section 3.7). The input parameter `ValidateEvidence` as defined in [ETSI TS 119 512] is mapped to the input parameter `VerifyRequest` as defined in [TR-ESOR-E] and the return parameter `VerifyResponse` as defined in [TR-TR-ESOR-E] is mapped to the return parameter `ValidateEvidenceResponse` as defined in [ETSI TS 119 512].

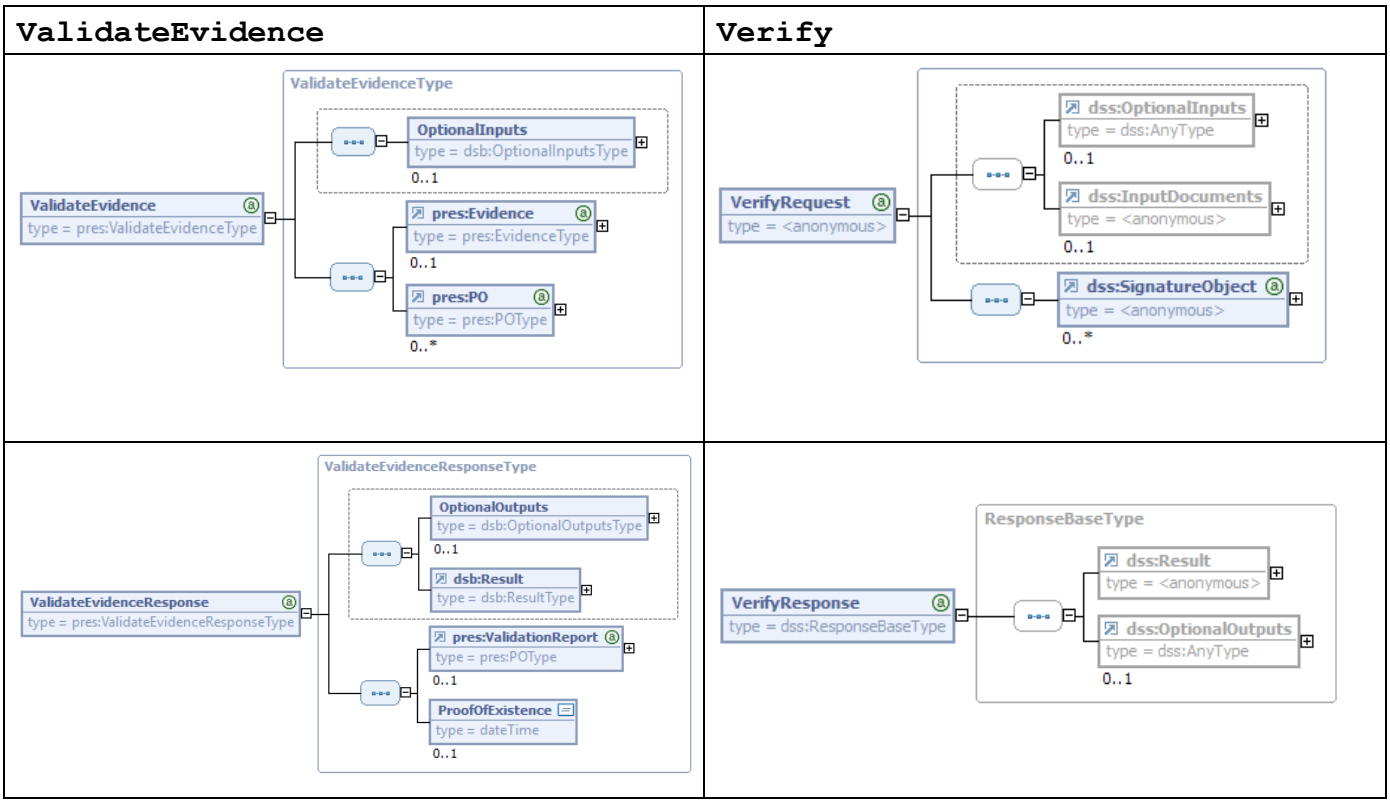

Figure 7 `ValidateEvidence/Verify` – request and response

3.7.1 ValidateEvidence ⟶ VerifyRequest

Here, the child elements of `ValidateEvidence` are mapped as follows:

- `OptionalInputs` – the `OptionalInputs` (`VerifyUnderSignaturePolicy` and `ReturnVerificationReport`) defined in [TR-ESOR-E], section 3.7.1 are passed on to the TR-S.4 interface. Other `OptionalInputs` trigger a corresponding error[19].
- `Evidence` – is mapped to the corresponding child element of `VerifyRequest/SignatureObject` if present, whereby the details depend on the format of the Preservation Evidence as defined in Annex A.2 of [ETSI TS 119 512]:
    - An Evidence Record as defined in RFC 4998 (A.2.2) or RFC 6283 (A.2.3) is mapped to a `VerifyRequest/SignatureObject/Other/EvidenceRecord` element. If the Evidence Record passed references a Preservation Object Container (see `PO` below), the Evidence Record must be passed as an `xaip:evidenceRecord` element as defined in [TR-ESOR-F, section 3.1.5) or [TR-ESOR-E], sections 3.3.1, 3.4.2) of the type `xaip:EvidenceRecordType`.

[19] http://uri.etsi.org/19512/error/notSupported

- A CAdES signature as defined in [ETSI TS 119 122-3], which contains an Evidence Record as defined in RFC 4998, is mapped to a `VerifyRequest/SignatureObject/Base64Signature` element. The `FormatId` attribute of the `Evidence` element is the same as the `http://uri.etsi.org/ades/CAdES/EvidenceRecord` in this case.
- Other Preservation Evidences are not supported and trigger an error[20]

- `PO` is either a simple binary data object, that is protected by the `Evidence` passed separately and is mapped to `VerifyRequest/InputDocuments/Document/Base64Data`, or is a supported Preservation Object Container. The following formats are supported here:
  - XAIP v1.3 as defined in [TR-ESOR-F], section 3) (http://www.bsi.bund.de/tr-esor/xaip/1.3) is passed in `VerifyRequest/InputDocuments/Document/InlineXML`
  - LXAIP as defined in [TR-ESOR-F], section 3.2 (http://www.bsi.bund.de/tr-esor/lxaip/1.3) is passed in `VerifyRequest/InputDocuments/Document/InlineXML`
  - ASiC-ERS as defined in [TR-ESOR-F], section 3.3 and as defined in [ETSI TS 119512] Annex A.3.1 and A.3.1.3 (http://uri.etsi.org/ades/ASiC/type/ASiC-ERS) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`
  - CAdES as defined in [ETSI TS 119 512] Annex A.1.1 (http://uri.etsi.org/ades/CAdES) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`.If a MIME type is not set, `application/cms` is used.
  - XAdES as defined in [ETSI TS 119 512] Annex A.1.2 (http://uri.etsi.org/ades/XAdES) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`. If a MIME type is not set, `application/xml` is used as the default.
  - PAdES as defined in [ETSI TS 119 512] Annex A.1.3 (http://uri.etsi.org/ades/PAdES) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`. If a MIME type is not set, `application/pdf` is used as the default.
  - ASiC-S as defined in [ETSI TS 319 162] (http://uri.etsi.org/ades/ASiC/type/ASiC-S) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`. If a MIME type is not set, `application/vnd.etsi.asic-s+zip` is used as the default.
  - ASiC-E as defined in [ETSI TS 119 512] Annex A.1.4 (http://uri.etsi.org/ades/ASiC/type/ASiC-E) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`. If a MIME type is not set, `application/vnd.etsi.asic-e+zip` is used as the default.
  - DigestList as defined in [ETSI TS 119 512] Annex A.1.6 (http://uri.etsi.org/19512/format/DigestList) is passed in `VerifyRequest/InputDocuments/Document/Base64Data`. If a MIME type is not set, `application/xml` is used as the default.

[20] http://uri.etsi.org/19512/error/notSupported

3.7.2 VerifyResponse → ValidateEvidenceResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below.
- `OptionalOutputs` – potentially contains a `VerificationReport` as defined in [TR-ESOR-VR], which is mapped to the `pres:ValidationEvidenceReport/ValidationReport` element. If successful, the element `ProofOfExistence` is also filled.

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
`urn:oasis:names:tc:dss:1.0:resultmajor`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor`
Suffixes for `ResultMajor`	
`:Success`	`#ok` `#warning`
`:resultmajor:RequesterError` `:resultmajor:ResponderError`	`#error`
`:resultmajor:InsufficientInformation`	-
Prefix for `ResultMinor`	
`http://uri.etsi.org/19512`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultminor`
Suffixes for `ResultMinor`	
`/error/noPermission`	`/al/common#noPermission`
`/error/internalError`	`/al/common#internalError`
`/error/parameterError`	`/al/common#parameterError`
	`/arl/missingReasonOfDeletion`
`/error/notSupported`	`/arl/notSupported`

Table 7 Return codes for `ValidateEvidence/Verify`

3.8 Search ↔ ArchiveData

The function `Search` from [ETSI TS 119 512] is mapped to the function `ArchiveData` defined in [TR-ESOR-E], section 3.6. The input parameter `Search` from [ETSI TS 119 512] is mapped to the input parameter `ArchiveDataRequest` from [TR-ESOR-E] and the return parameter `ArchiveDataReponse` from [TR-ESOR-E] is mapped to the return parameter `SearchResponse` from [ETSI TS 119 512].

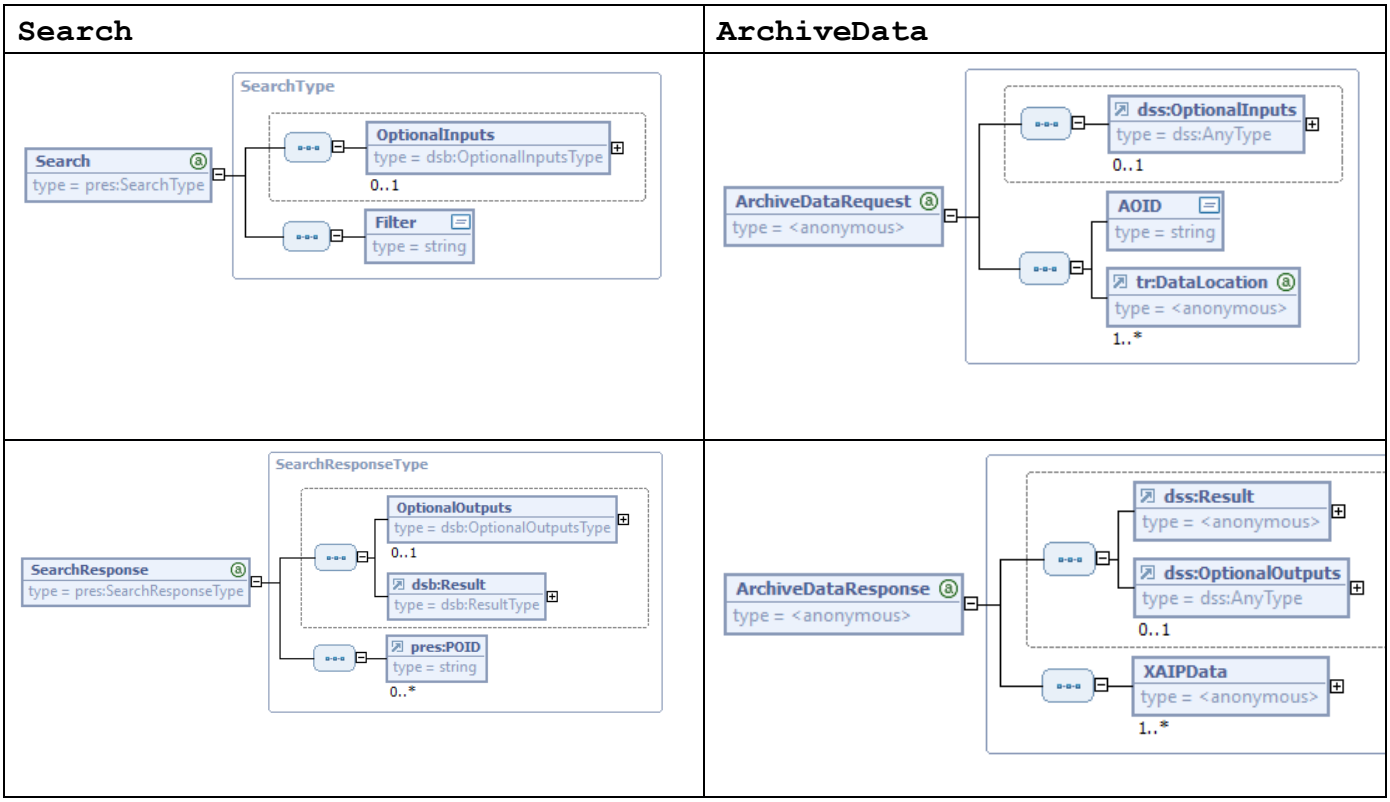

Figure 8 `Search/ArchiveData` – request and reponse

3.8.1 Search ⟶ ArchiveDataRequest

Here, the child elements of `Search` are mapped as follows to `ArchiveDataRequest`:

- `Filter` – contains a structure defined by the following JSON schema:

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

The parameters make use of the following semantics:

- `AOID` – identifies a specific Preservation Object and is mapped to the `ArchiveDataRequest/AOID` element.
- `XPathFilter` – specifies the data object within the XAIP that is addressed by the AOID and is mapped to the `ArchiveDataRequest/DataLocation`. Here, it is assumed that the `ArchiveDataRequest` implementation for the integrated TR-ESOR middleware at least offers support for simple XPath expressions that allow the request of a data element, which is referenced by an ID in the XML structure of the XAIP addressed by the `AOID`.

3.8.2 ArchiveDataResponse → SearchResponse

- `dss:Result` – is mapped to `dsb:Result`, as explained in more detail below
- `OptionalOutputs` – are not present and trigger an error[21]
- `XAIPData` – is mapped to `SearchResponse/OptionalOutputs/Other/XAIPData`

The error codes are constructed from a general prefix and a specific suffix, and are mapped as follows:

ETSI TS 119 512	BSI TR-03125-E
Prefix for `ResultMajor`	
`urn:oasis:names:tc:dss:1.0:resultmajor`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultmajor`
Suffixes for `ResultMajor`	
`:Success`	`#ok` `#warning`
`:resultmajor:RequesterError` `:resultmajor:ResponderError`	`#error`
`:resultmajor:InsufficientInformation`	-
Prefix for `ResultMinor`	
`http://uri.etsi.org/19512`	`http://www.bsi.bund.de/tr-esor/api/1.3/resultminor`
Suffixes for `ResultMinor`	
`/error/noPermission`	`/al/common#noPermission`
`/error/internalError`	`/al/common#internalError`
`/error/parameterError`	`/al/common#parameterError`
	`/arl/unknownLocation`
	`/arl/unknownAOID`
`/error/notSupported`	`/arl/notSupported`

Table 8 Return codes for `Search/ArchiveData`

[21] http://uri.etsi.org/19512/error/notSupported

4. References

[TR-ESOR-E] BSI: Preservation of Evidence of Cryptographically Signed Documents, Annex TR-ESOR-E, Concretisation of the Interfaces on the Basis of the eCard API Framework, version 1.3, www.bsi.bund.de/EN/tr-esor or https://www.bsi.bund.de/tr-esor

[TR-ESOR-F] BSI: Preservation of Evidence of Cryptographically Signed Documents, Annex TR-ESOR-F, Formats, version 1.3, www.bsi.bund.de/EN/tr-esor or https://www.bsi.bund.de/tr-esor

[TR-ESOR-VR] BSI: Preservation of Evidence of Cryptographically Signed Documents, BSI TR-03125, Annex TR-ESOR-VR: Verification Reports for Selected Data Structures, Version 1.3, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_VR_V1_3.pdf

[eCard-2] BSI: eCard API Framework – Part 2 – eCard Interface, BSI TR-03112-2

[ETSI TS 119 122-3] ETSI TS 119122-3: 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 119512: Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services, V1.1.2