Bundesamt
für Sicherheit in der
Informationstechnik

BSI

An Archiving Profile for OASIS DSS

Manuel Bach
Federal Office for Information Security, Germany

Dr. Detlef Hühnlein
secunet Security Networks AG, Germany

Dr. Ulrike Korte
Federal Office for Information Security, Germany

DSS Archiving Profile

Agenda

- **Motivation**
- Architecture
- Interfaces
- Outlook

Motivation

- It is well known that cryptographic algorithms may become weak due to increased computational power or improved algorithms
- Hence the conclusiveness of digital signatures may decrease over time …
- … at least if one does not apply appropriate counter-measures such as
  - Archive Time-Stamps according to XAdES / CAdES
  - Evidence Records according to RFC 4998
- Some EU-member-states have explicit legal stipulations for long-term archiving of qualified electronic signatures (e.g. § 17 SigV in Germany)

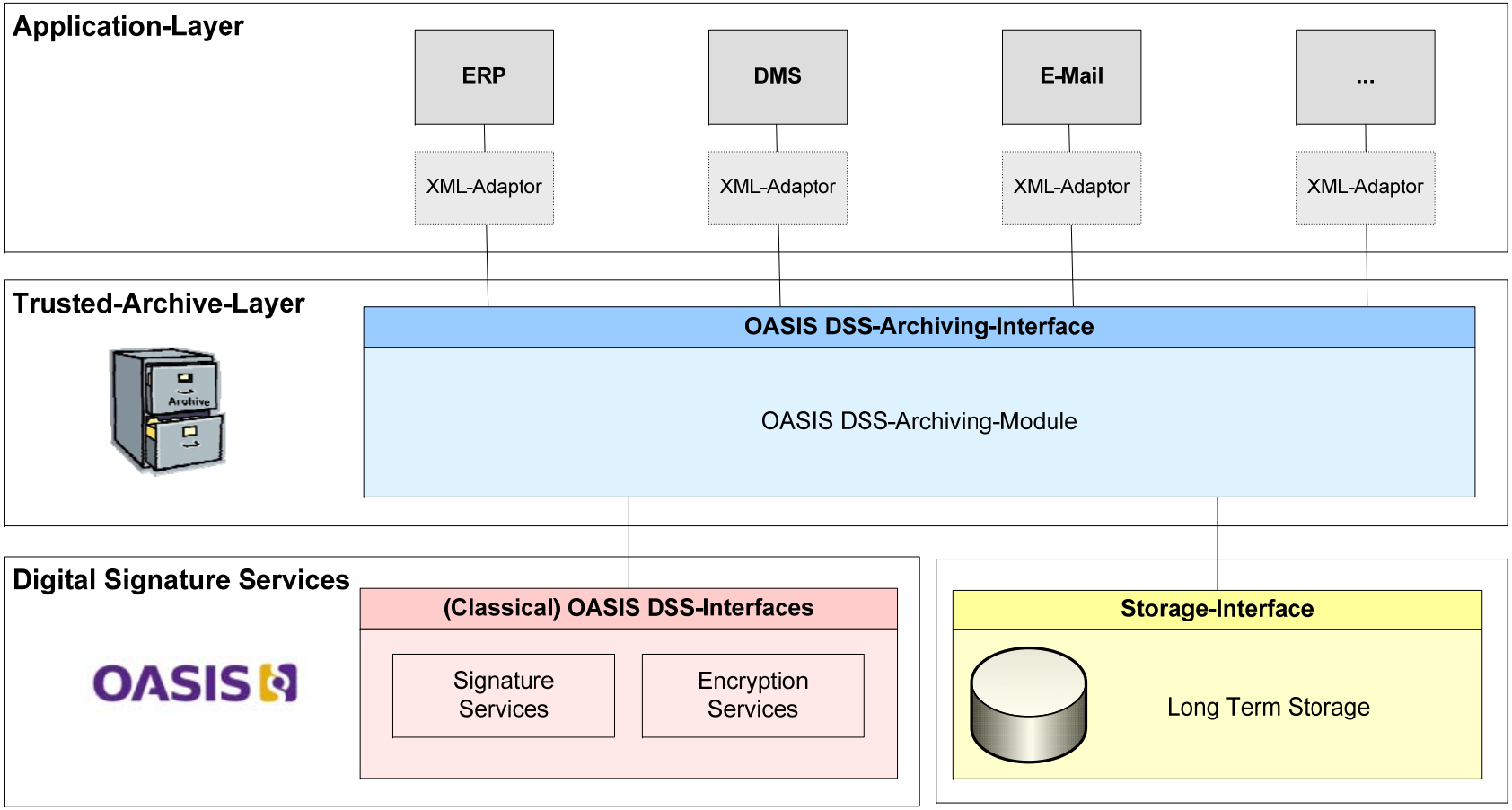
☞ **It is an obvious approach to use DSS for long term archiving of signatures and signed data**

DSS Archiving Profile

Agenda

- Motivation
- **Architecture**
- Interfaces
- Outlook

Architecture

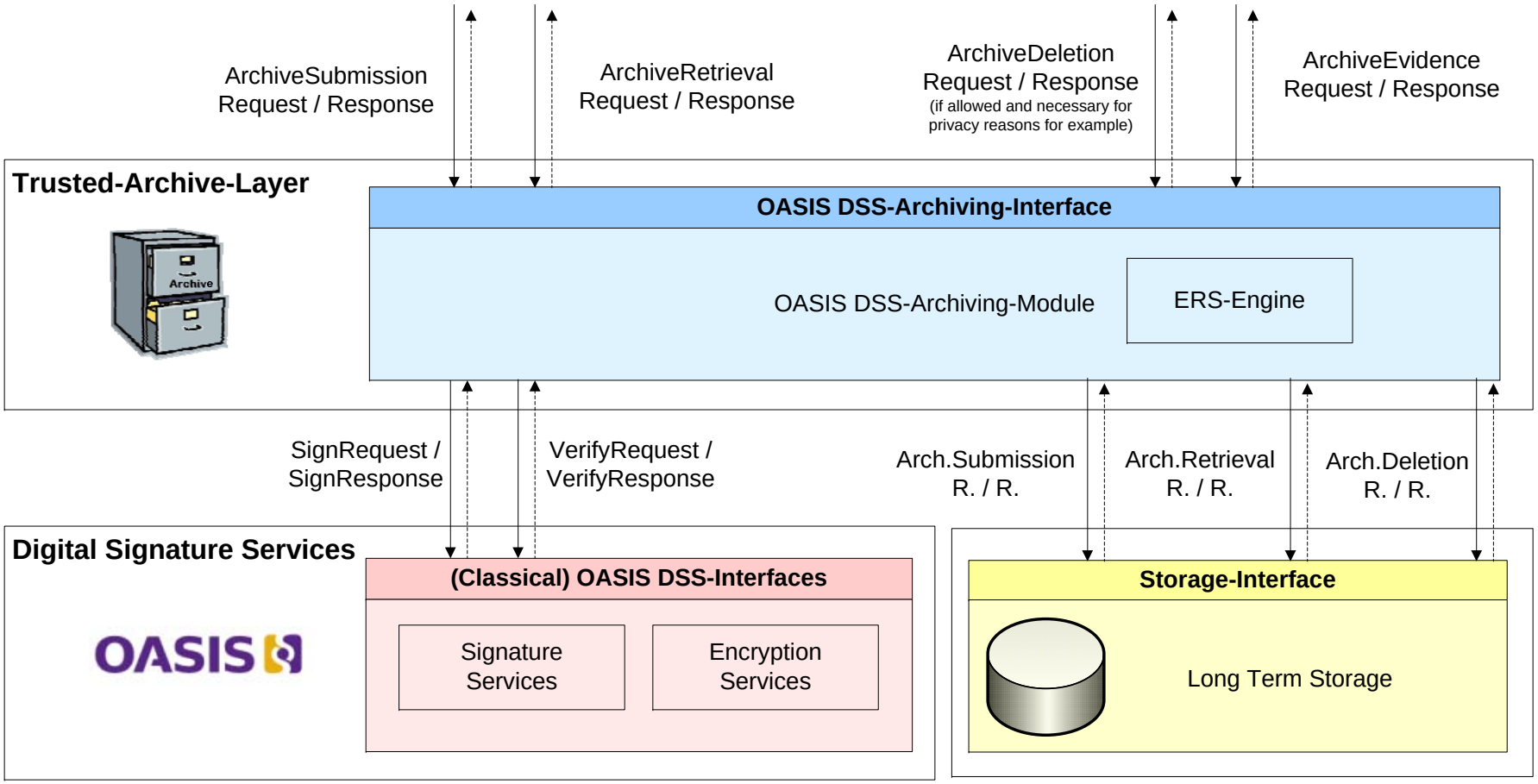


DSS Archiving Profile

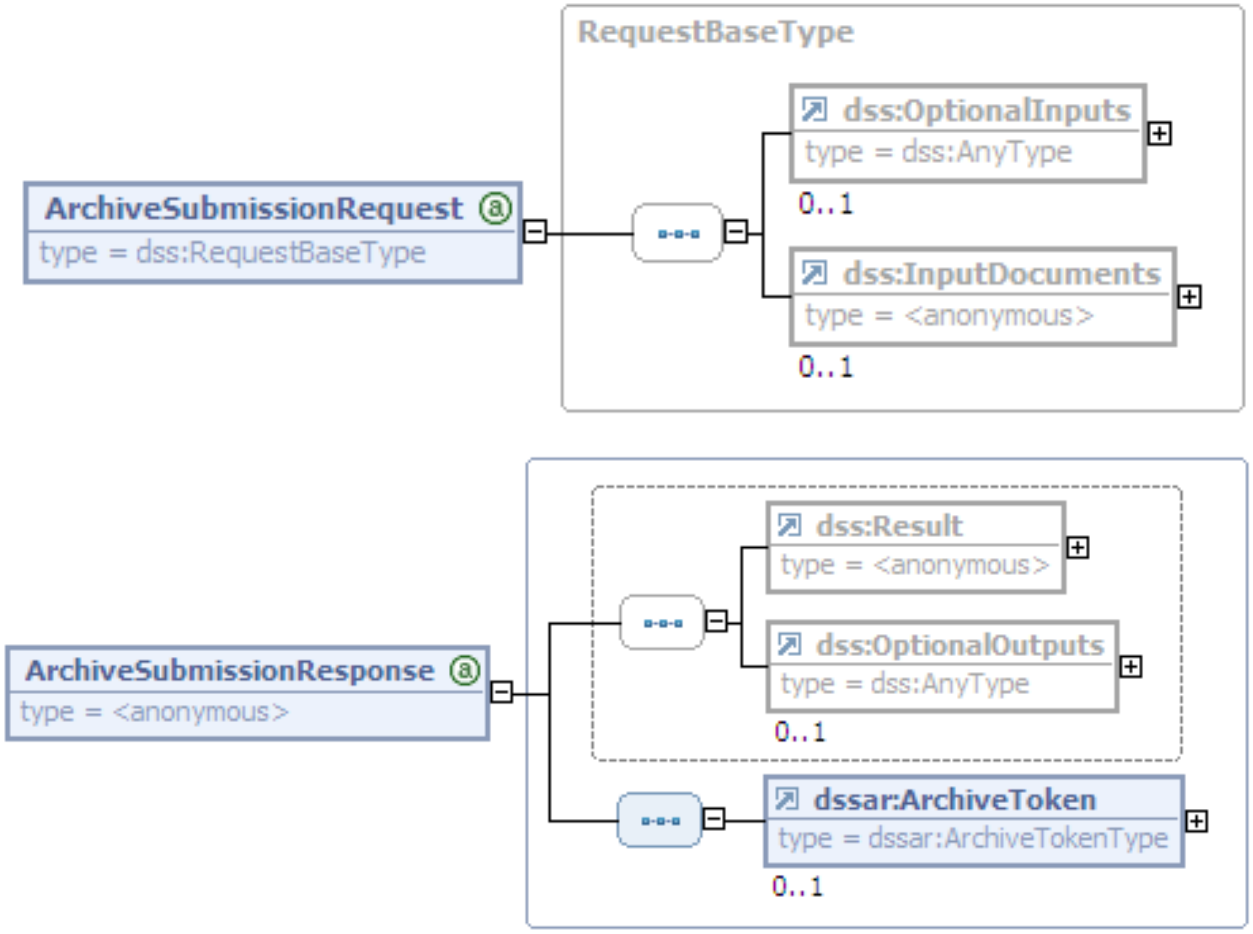
Agenda

- Motivation
- Architecture
- **Interfaces**
- Outlook

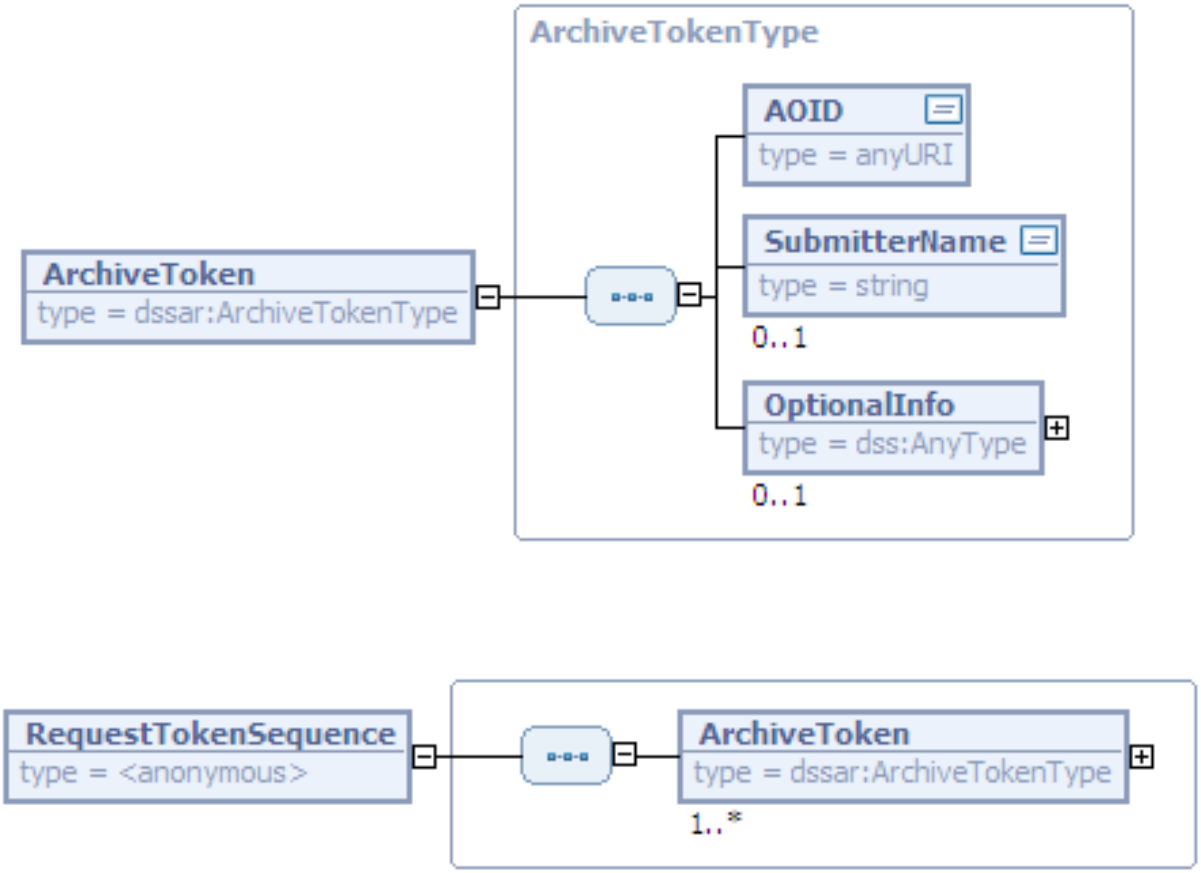
Interfaces


ArchiveSubmission
Request / Response
ArchiveRetrieval
Request / Response
ArchiveDeletion
Request / Response
(if allowed and necessary for
privacy reasons for example)
ArchiveEvidence
Request / Response
Trusted-Archive-Layer
Archive
OASIS DSS-Archiving-Interface
OASIS DSS-Archiving-Module
ERS-Engine
SignRequest /
SignResponse
VerifyRequest /
VerifyResponse
Arch.Submission
R. / R.
Arch.Retrieval
R. / R.
Arch.Deletion
R. / R.
Digital Signature Services
OASIS
(Classical) OASIS DSS-Interfaces
Signature
Services
Encryption
Services
Storage-Interface
Long Term Storage

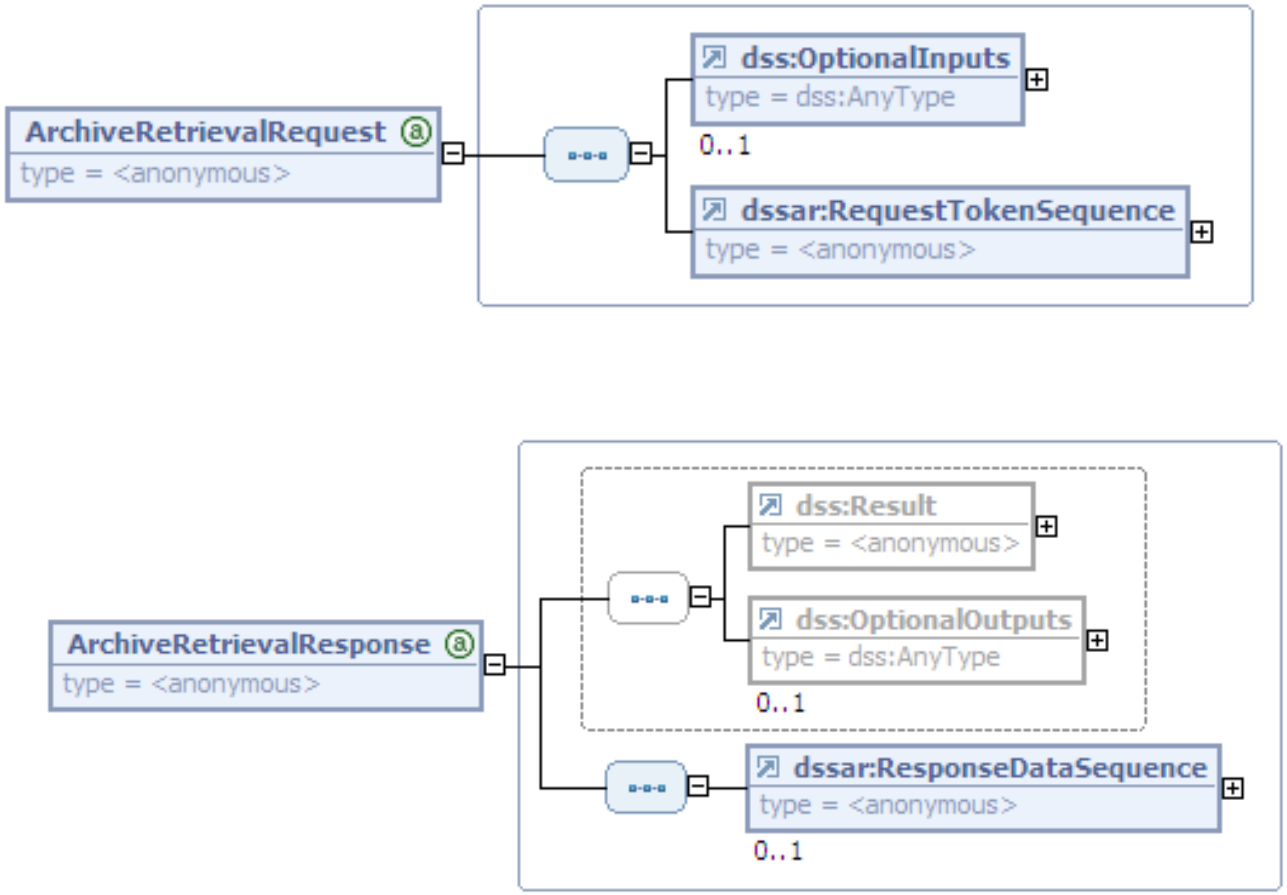
ArchiveSubmission Request / Response



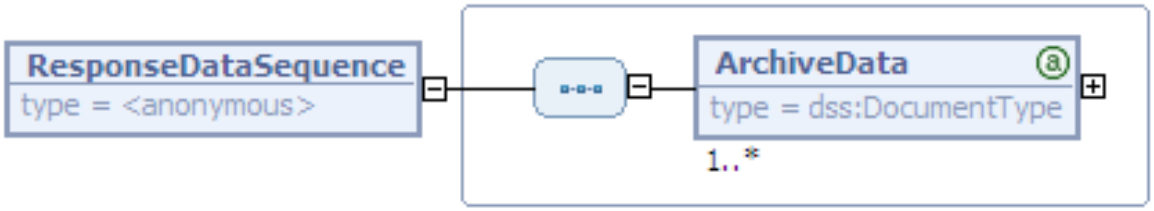
ArchiveToken & RequestTokenSequence



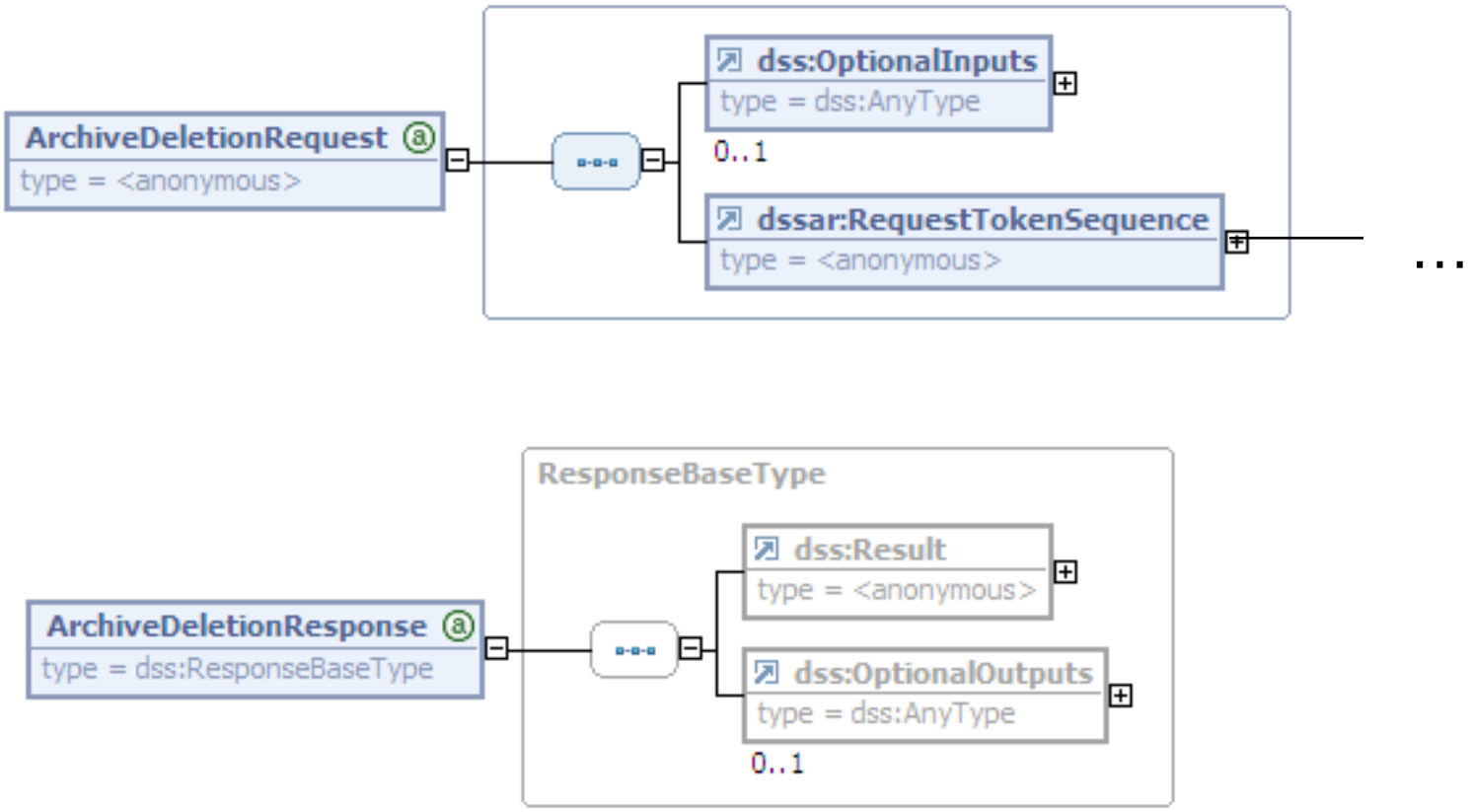
ArchiveRetrieval
Request / Response



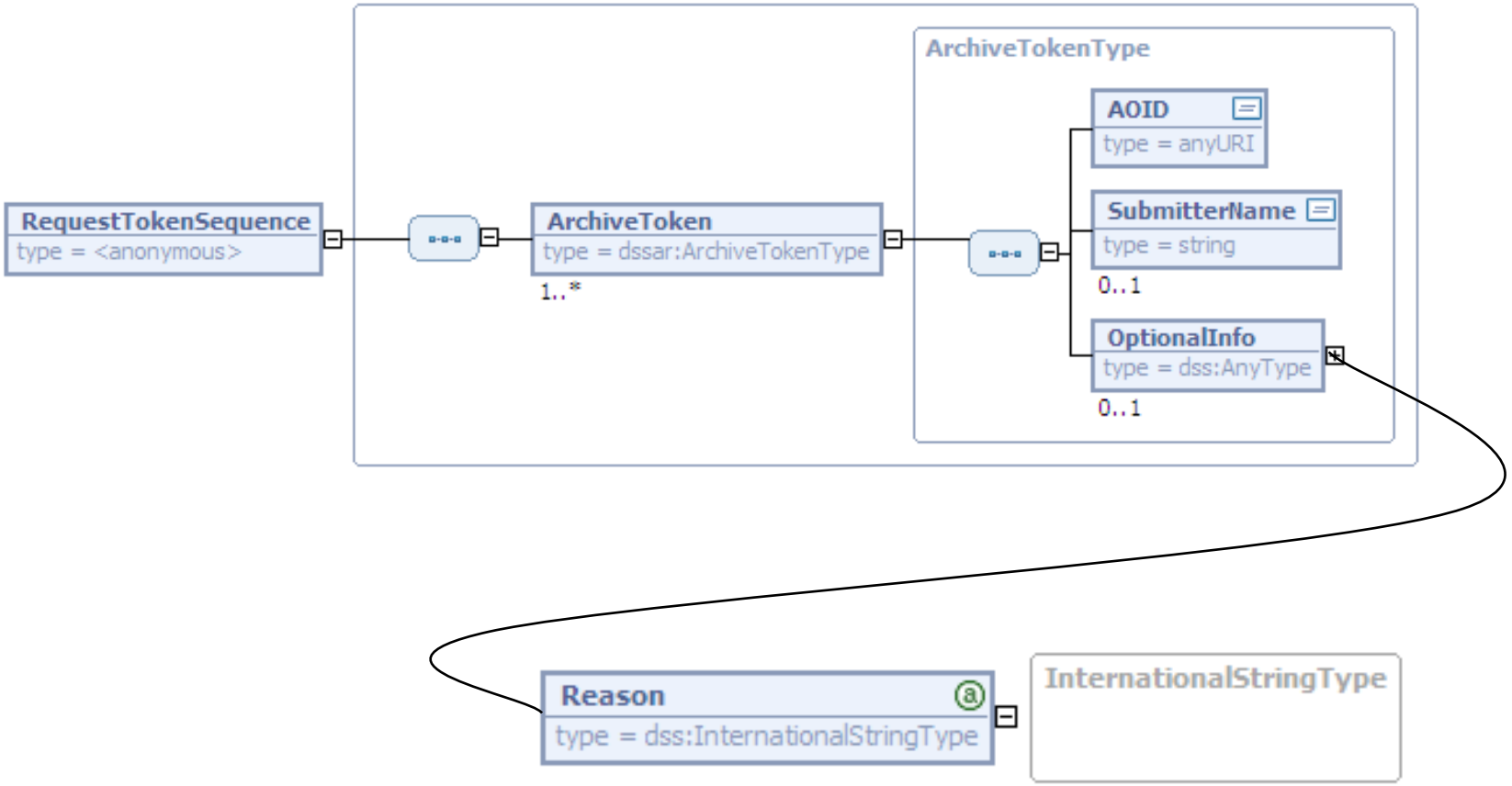
ResponseDataSequence



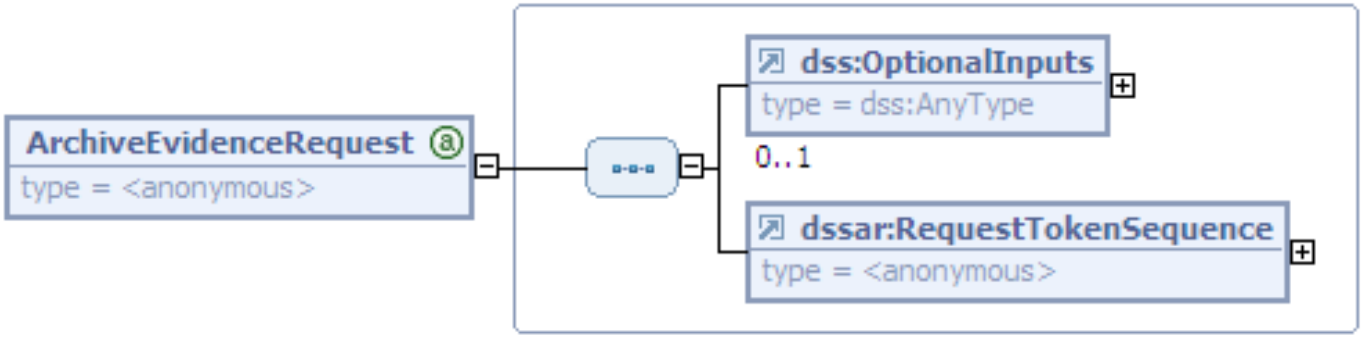
ArchiveDeletion
Request / Response

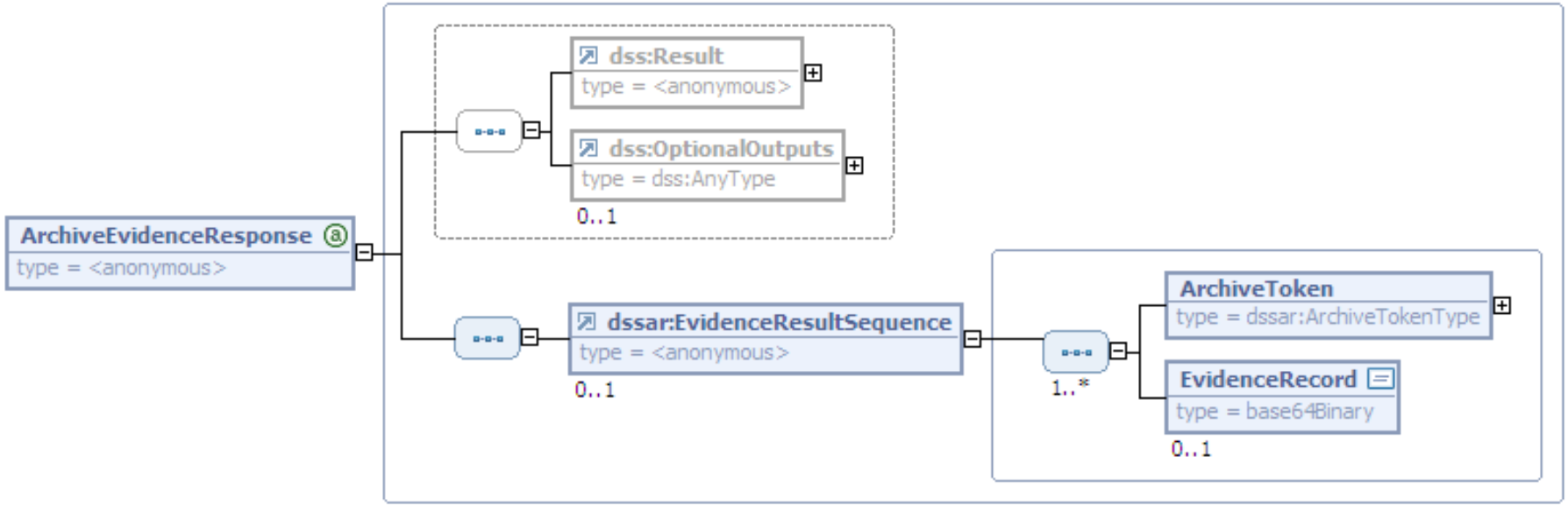


RequestTokenSequence @ ArchiveDeletionRequest

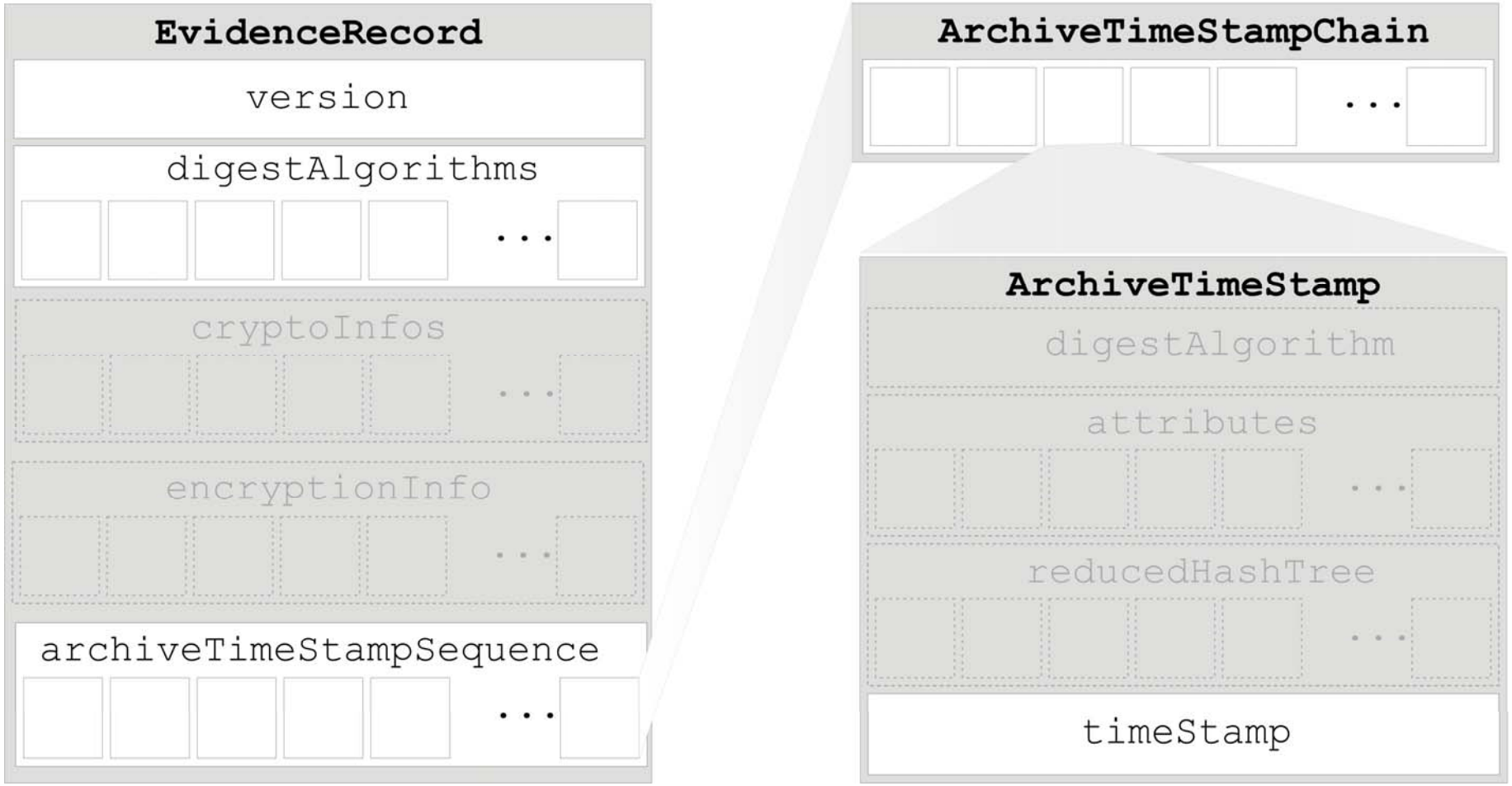


ArchiveEvidence
Request / Response





Evidence Record Syntax

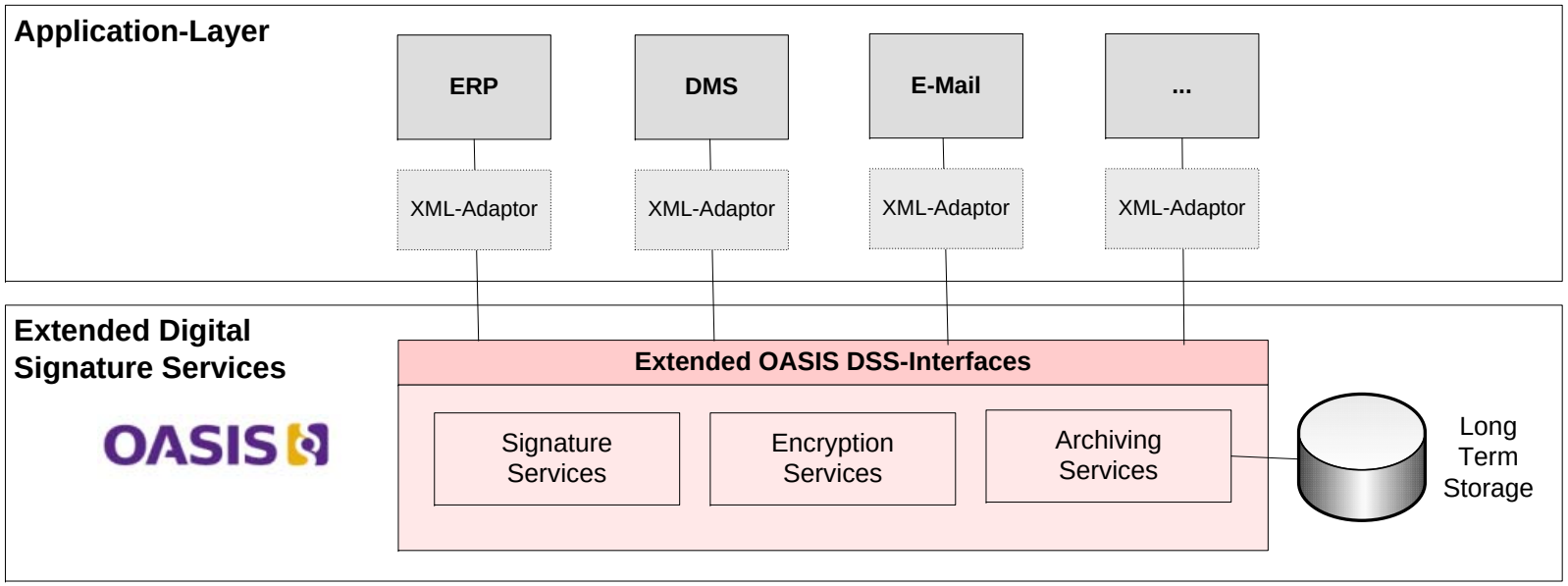


DSS Archiving Profile

Agenda

- Motivation
- Architecture
- Interfaces
- **Outlook**

Outlook



urn:oasis:names:tc:dss:1.0:profiles:archiving:operation:archiveall
urn:oasis:names:tc:dss:1.0:profiles:archiving:operation:archivedocuments
urn:oasis:names:tc:dss:1.0:profiles:archiving:operation:archivesignature
…

Thank you very much for your kind attention!

Contact:

Manuel Bach
Federal Office for Information Security
manuel.bach@bsi.bund.de

Dr. Detlef Hühnlein
secunet Security Networks AG
detlef.huehnlein@secunet.com

Dr. Ulrike Korte
Federal Office for Information Security
manuel.bach@bsi.bund.de