Electronic Archive of Authentic Acts with Decentralized Key Management

Dr. Armin Lunkeit

Senior Security Architect

procilon

procilon

Who we are

90
EMPLOYEES

4
LOCATIONS

2.500+
CLIENTS

100%
PERMANENT EMPLOYMENT

procilon

Who we are

- Central security and communication platform for more than **8,000 notary employees**
- **2** eIDAS accredited **trust centers** established
- Maintenance and development of **SAFE (Secure Access to Federated e-Justice/e-Government) for Federal Ministry of Justice**
- proGOV as security and communication platform for more than **850 municipalities, counties and municipal data centers**
- Participation in electronic legal transactions for self-employed persons and **companies** from industry & medium-sized businesses
- **12 accident insurance companies** for the process of scanning, signing and TR-ESOR compliant long-term storage of evidence
- More than **450 municipal utilities and energy suppliers** for secure market communication according to the specifications of the Federal Network Agency
- Central OSCI platform for more than **50 chambers of industry and commerce**

Customer project

Key facts of the electronic archive at Bundesnotarkammer

Electronic storage of documents

Since 2022 all ca. **7.300 notaries** store their acts both electronically and physically. The acts need to be **stored for 100 years**.

Expected number of documents

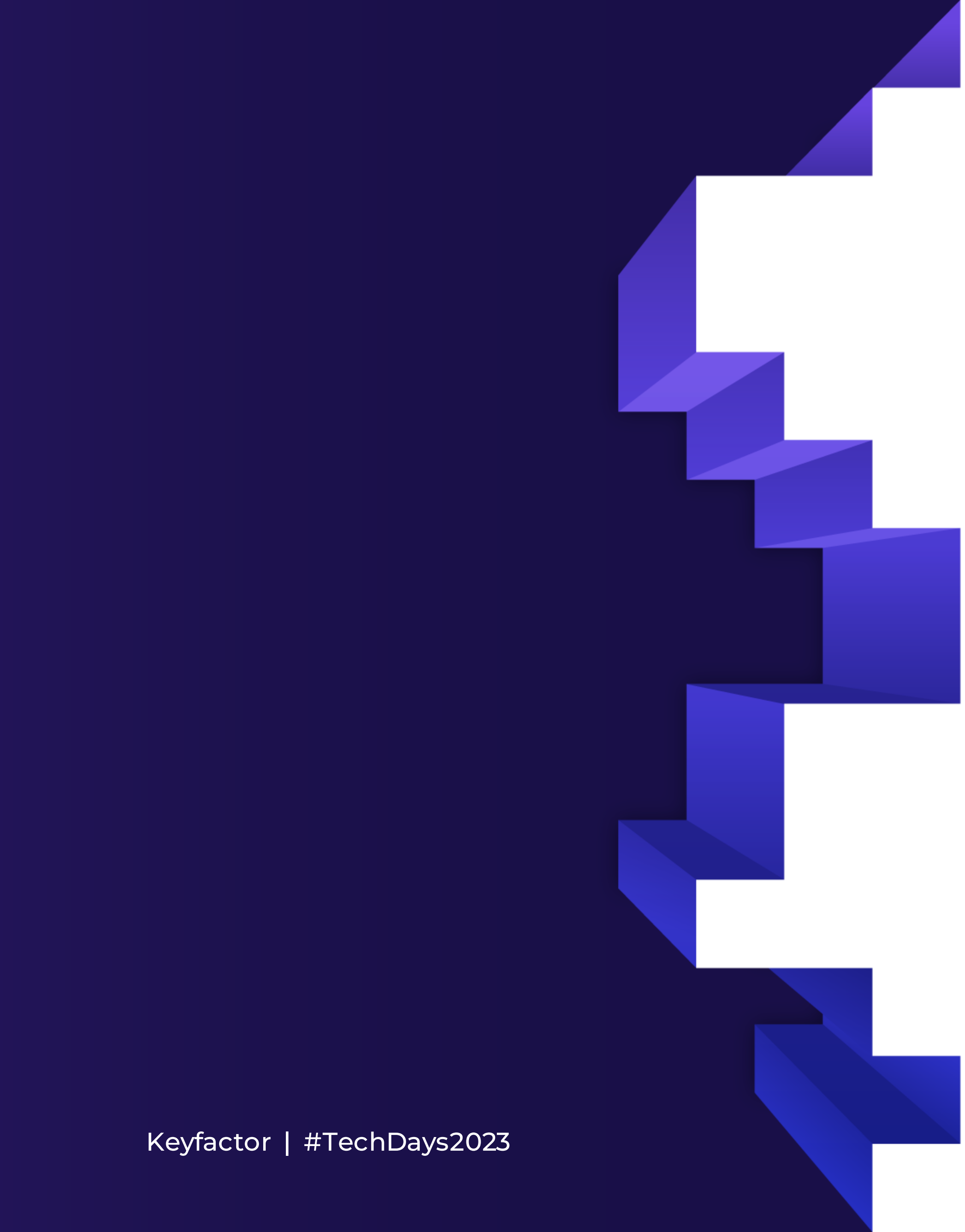
Over **7.000.000 acts per year** with each act consisting of one or more documents. All acts are signed with a **qualified electronic signature**.

Document formats

Nearly all documents are **colour scans in PDF format** ranging from a couple of megabytes to several hundreds megabytes in size.

Encryption

The documents are **locally encrypted** using **hardware tokens** by **50.000 users** in ca. 5.500 locations and uploaded via VPN to the data centers.



The idea

general idea and some insights

The idea – build an archive

Long story short

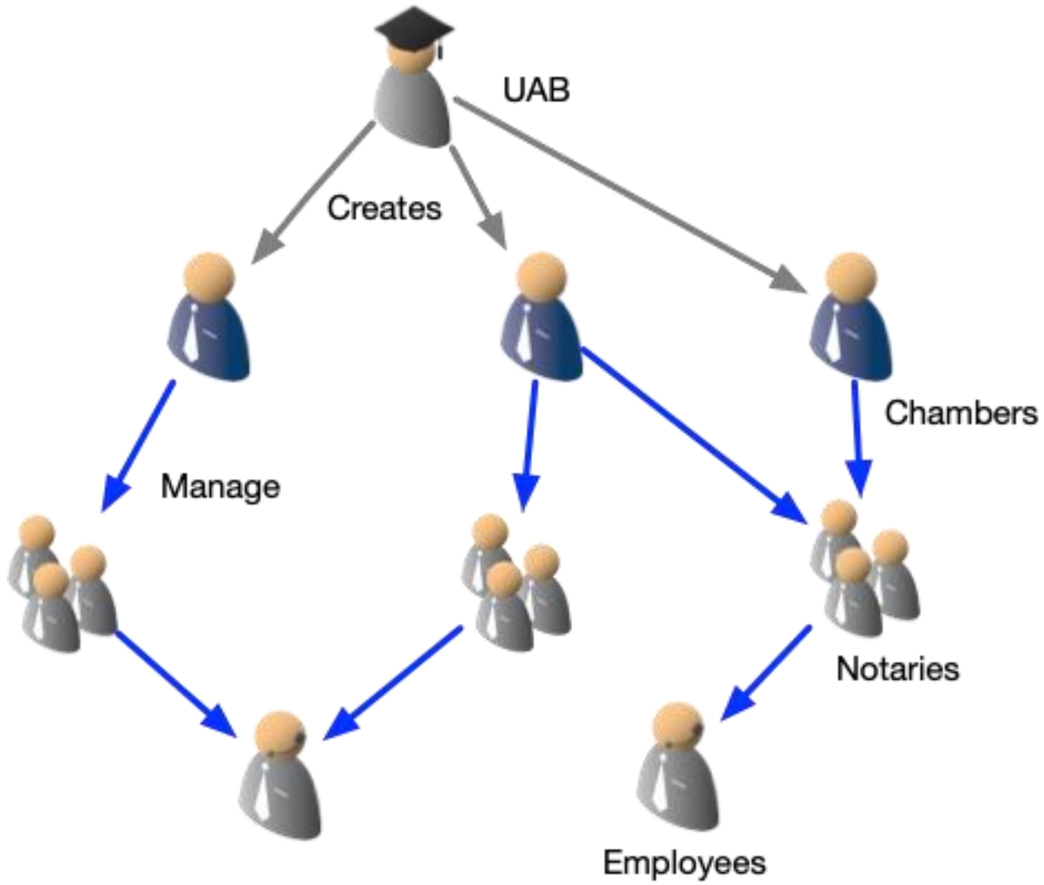
Notaries…

- must be able to store documents in an electronic archive
- act independently, access to the data is **under full control of the notary**
- must be able to proxy each other
- can resign and must be able to **hand over their documents** to a successor

ℹ The security goals of the CIA triad apply

Hierarchy and roles

By example



UAB – organizational root instance

Chamber – sub-organization managing a subset of notaries

Notaries – users of the archive

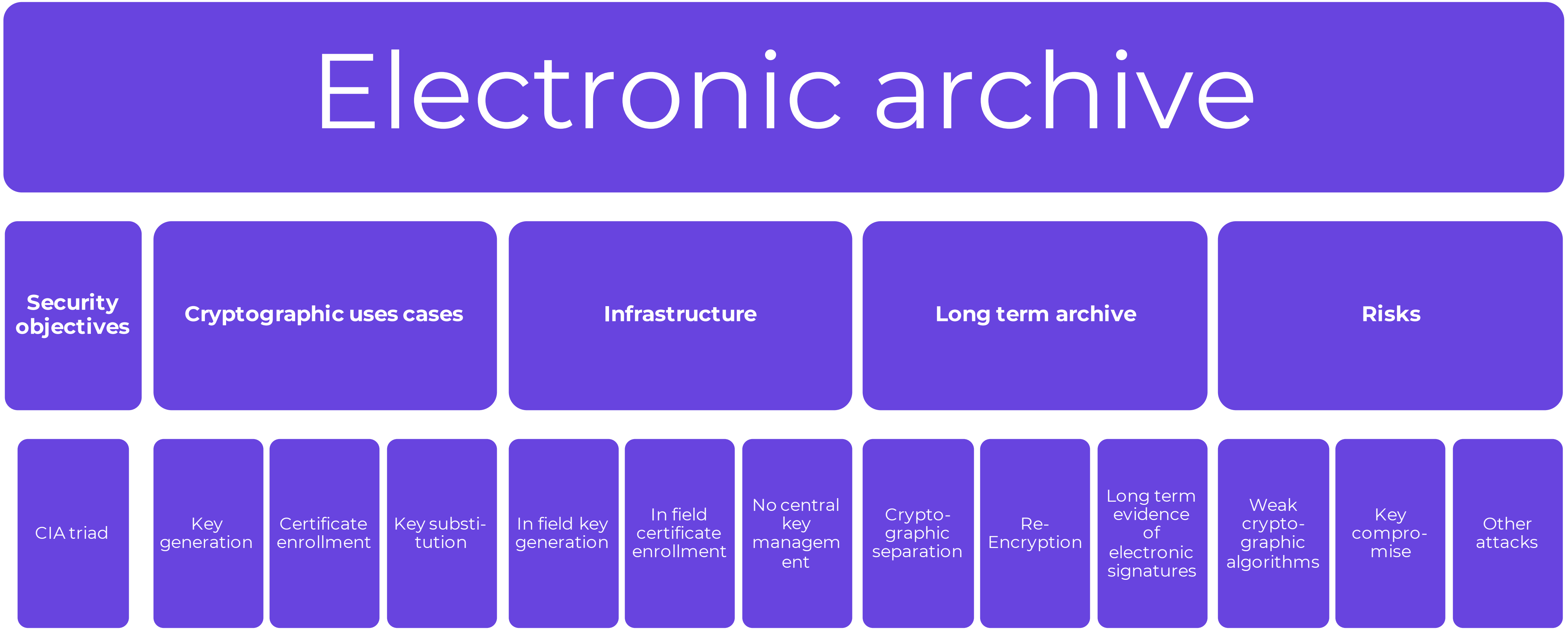
Employees – work on behalf of notaries

→ Stakeholders of the potential solution

Requirements and use cases

Map of Requirements

... some of them



Electronic archive

- **Security objectives**
  - CIA triad
- **Cryptographic uses cases**
  - Key generation
  - Certificate enrollment
  - Key substitution
- **Infrastructure**
  - In field key generation
  - In field certificate enrollment
  - No central key management
- **Long term archive**
  - Cryptographic separation
  - Re-Encryption
  - Long term evidence of electronic signatures
- **Risks**
  - Weak cryptographic algorithms
  - Key compromise
  - Other attacks

Use cases

Excerpt of some use cases

- In field generation of key material and certificates
- Access to certificates to a limited set of other entities
- In field symmetric key generation and encryption of documents for at least two recipients
- Handover of key material between notaries
- Initial archiving of documents
- Reencryption of documents
- Signature validation and evidence of signature validity over a long period

Architecture

System architecture and focus on long term archiving

Design aspects

Factors influencing the design

- existing infrastructure at customer site is very heterogeneous
- service-oriented architecture: divide and conquer, separate responsibilities, consider SOLID criteria, use REST for loose coupling
- address redundancy and availability, ensure performance
- use of existing standards and create only new components and services if necessary (e. g. adoption of KMIP, BSI TR-03125)

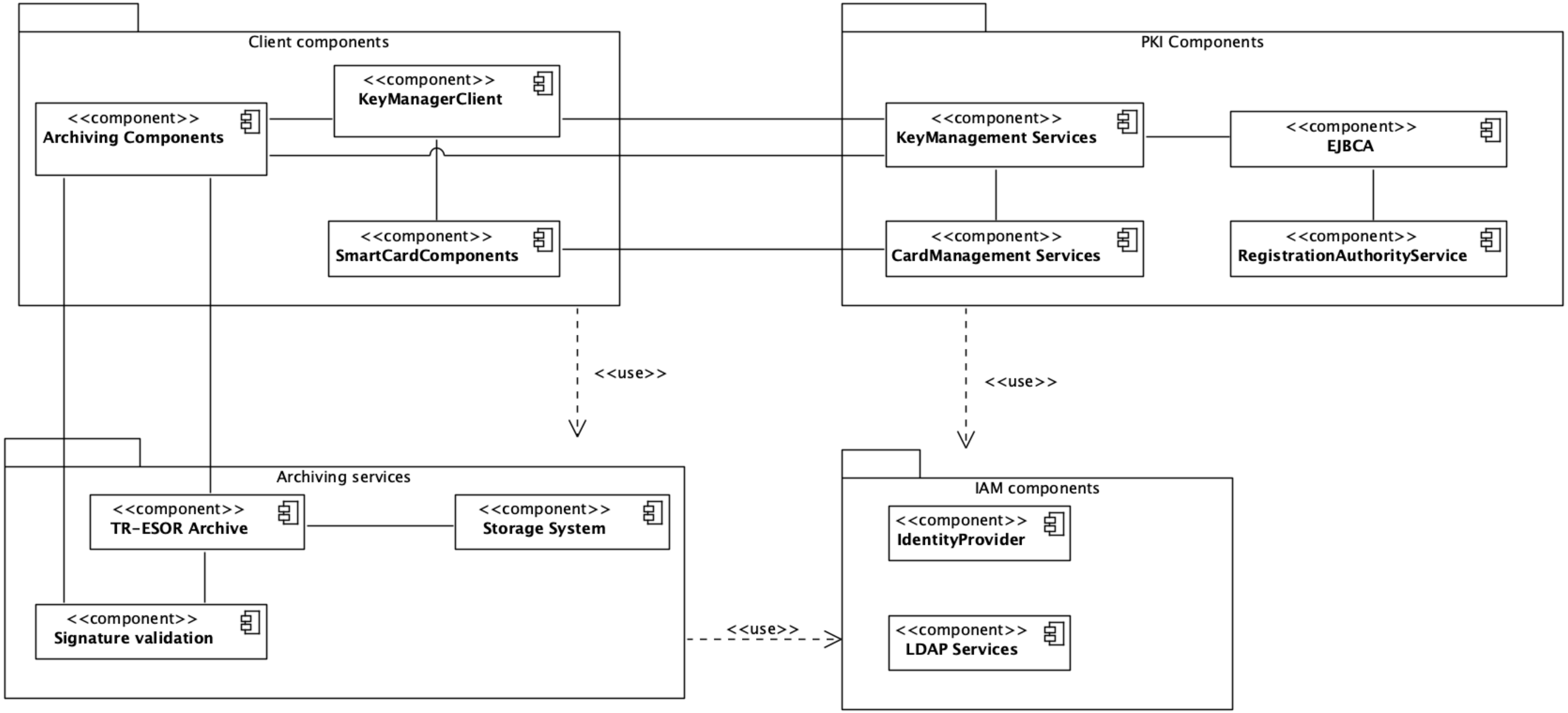
From requirements to design

Mapping requirements to design and architecture

Requirement	Design decision
In field key generation and certificate enrollment	• Use of certified smartcard key generation mechanisms • Provide certificate signing requests, enroll to chipcard, publish certificates in KMIP compliant key management service
Key handover	• Use of cryptographic key domains for export and import of cryptographically wrapped keys
Decentralized key management	• Independent key generation • Ad hoc key generation and certificate enrollment • No encryption for central or root entity
Archiving services and long term evidence of electronic signatures	• Use of archiving middleware pursuant to BSI TR-03125 (TR-ESOR)
Notaries must have full control, ability to handover documents	• End to end encryption using hybrid encryption scheme

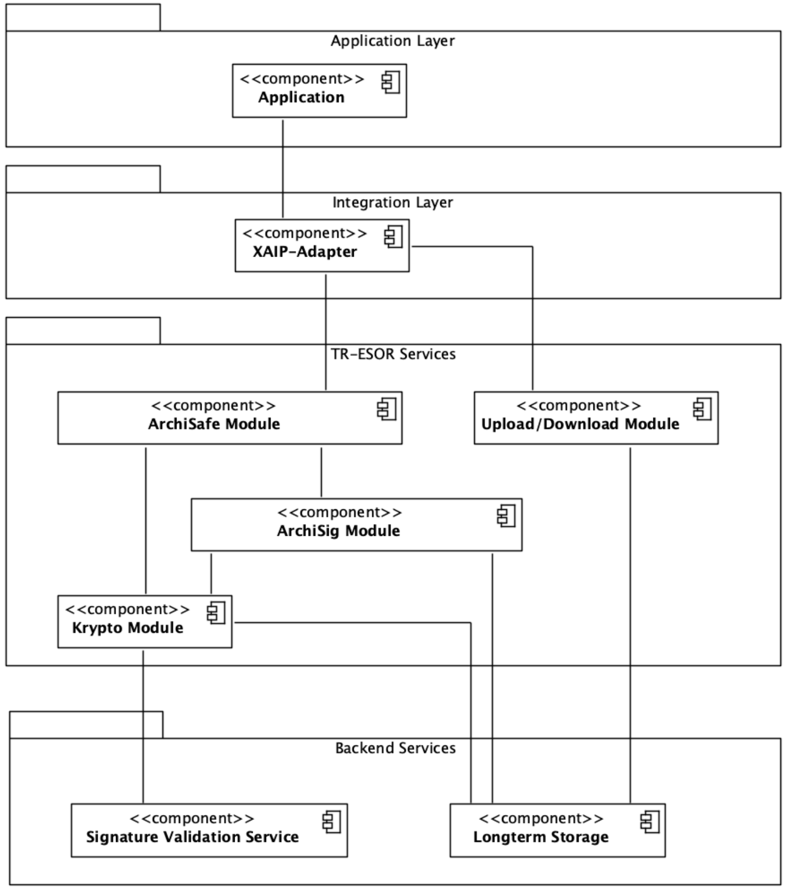
System architecture

Components of the solution



Focus: Archiving components

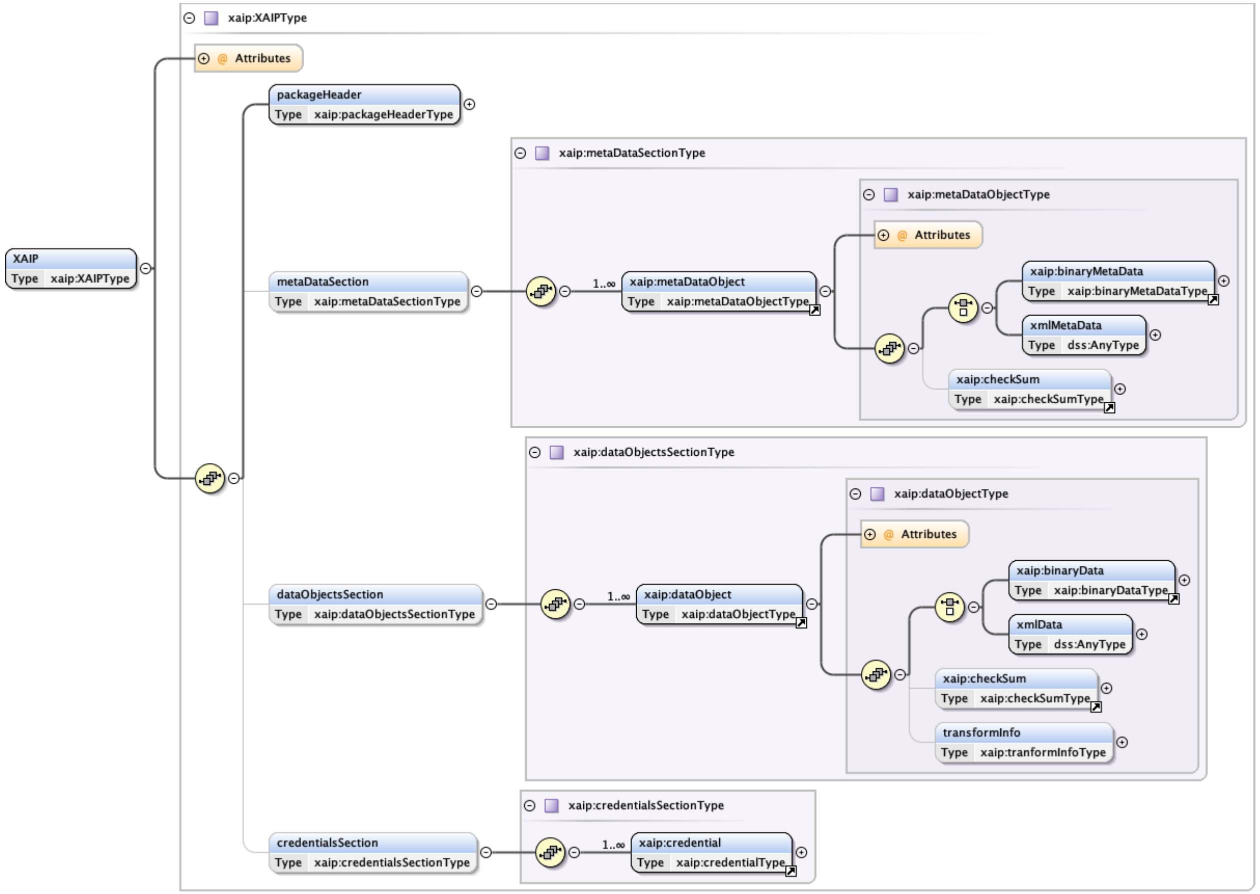
Closer look at the archiving components



Components	Purpose
Application	Generates specific data for the customers use case
XAIP-Adapter	Enforce security policies for data: access control, encryption, handover procedures
TR-ESOR Services pursuant to BSI TR-03125	Provides the building blocks for a trustworthy long term archive • Signature renewal and preservation of the evidentiary value of electronically signed data • Trusted cryptographic implementations
Signature Validation Service	Provides validation services for digital signatures
Longterm storage	Storage capabilities

The XAIP concept

The core concept of TR-03125 (TR-ESOR)



Section	Purpose
packageHeader	Archive object id (AOID), version manifest
metaDataSection	Meta data of the archive object
dataObjectsSection	Stores the data object (e.g. PDF document or other binary or XML data)
credentialsSection	Stores additional digital signatures, seals or timestamps

XAIP is an extensible archive container. Profile customization is a core capability of TR-ESOR.

Focus: key handover

Exchanging keys between notaries

Fundamentals: Archived documents are encrypted with a hybrid encryption scheme, each notary has its own unique key pair

Challenge: transfer cryptographic keys between notaries so they can proxy each other => hard goal in the requirements landscape

Solution: use of cryptographic key domains for key handover

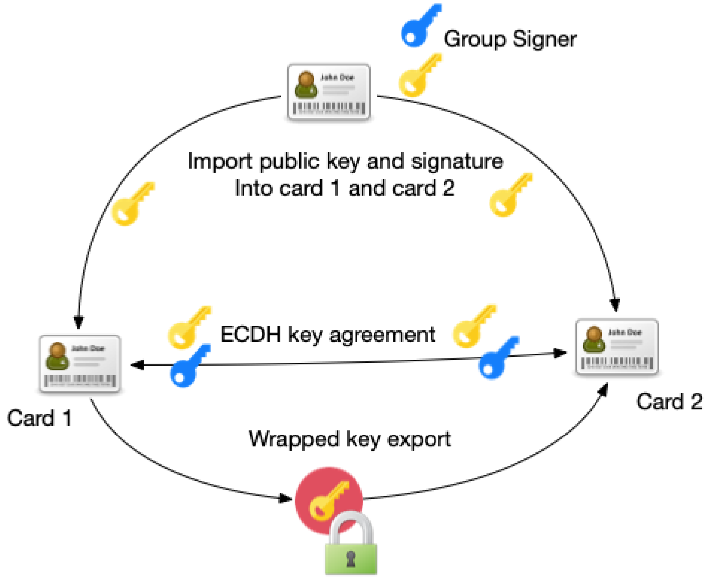
Concept of key domains

General idea and overview

Key domain: logical construct to enable key exchange between multiple entities

Procedure:

- create a trusted key pair (group signer) and import the public key into a chip card together with the signature over the card verifiable certificate, public key and signature build the trust anchor
- create a key domain referencing the group signers public key and the signature
- Generate an individual ECDH key pair within that key domain
- Use ECDH for key exchange with other entities being part of the same key domain



More challenges

Challenges arising in the context of the customers use case

How to…

- … preserve evidence of electronic signatures of encrypted documents?
- … handover documents between notaries considering performance requirements?
- … handle key compromise and lost cryptographic keys?

Dr. Armin Lunkeit

Senior Security Architect

procilon