Bild: macrovector / Freepik

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

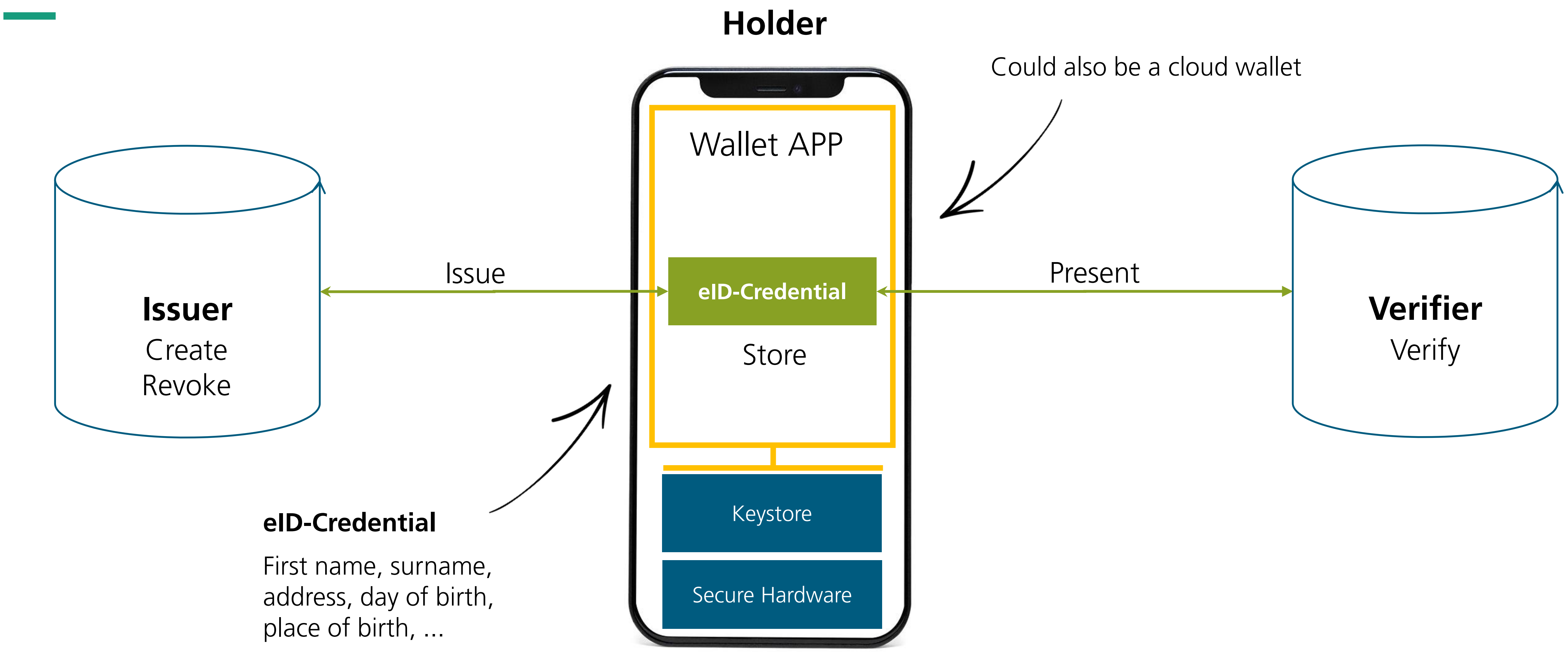
OMNISECURE

Security & Privacy Requirements
Secure Digital Identities

23.01.2024

Rollen Modell

Smartphone-based eID



Could also be a cloud wallet

eID-Credential

First name, surname, address, day of birth, place of birth, ...

Anforderungen

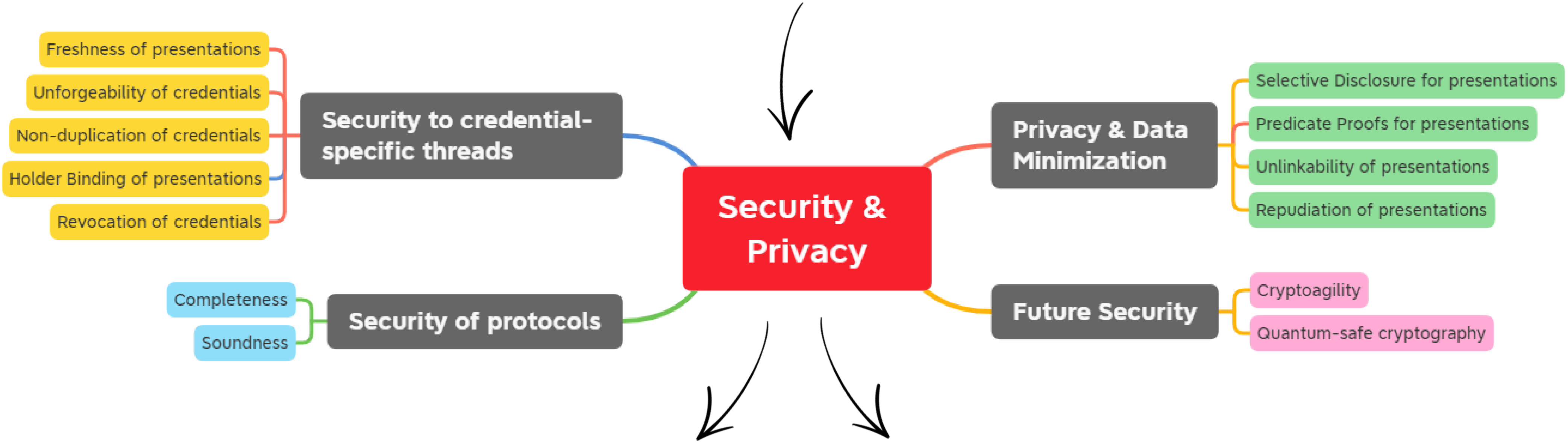
Security & Privacy by Design

ISO/IEC 29115 [1]

eIDAS Implementing Regulation (EU) 2015/1501 [3]

Revision of eIDAS Regulation (EU) No 910/2014 [5]

Non-digital ID cards [6]



Security & Privacy

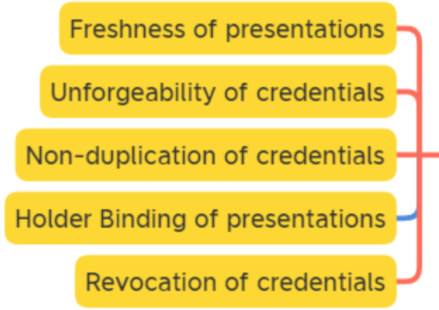
- **Security to credential-specific threads**
  - Freshness of presentations
  - Unforgeability of credentials
  - Non-duplication of credentials
  - Holder Binding of presentations
  - Revocation of credentials
- **Security of protocols**
  - Completeness
  - Soundness
- **Privacy & Data Minimization**
  - Selective Disclosure for presentations
  - Predicate Proofs for presentations
  - Unlinkability of presentations
  - Repudiation of presentations
- **Future Security**
  - Cryptoagility
  - Quantum-safe cryptography

Design **Compare**

eID-Credential Systems

Anforderungen

eID Security → prevent Impersonation



Freshness of presentations

Unforgeability of credentials

Non-duplication of credentials

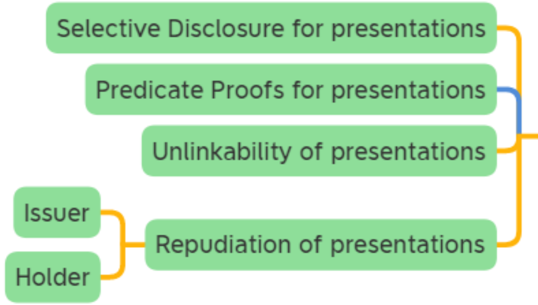
Holder Binding of presentations

Revocation of credentials

Requirement	Threat	Possible Controls
Freshness of presentation Every verifiable presentation must be created new for every verification.	Replay Attack	Dynamic Authentication
Unforgeability of credentials Credentials can only be created by the issuer.	Unauthorized creation, Tampering	Authenticate by Signing, Issuer Authenticated Channel
Non-duplication of credentials Credentials cannot be duplicated.	Credential Duplication	Bind to Secure Storage (e.g. TEE, TRH, SE, HSM)
Holder Binding of presentations Presentations can only be created under the control of the Holder.	Unauthorized use	Multi Factor Authentication
Revocation of credentials Valid credentials can be revoked by the issuer at any time.	Credential is compromised	Revocation List, API based, Short validity, …

Anforderungen

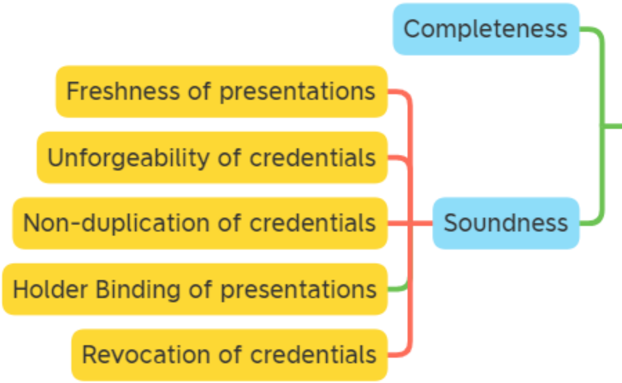
eID Privacy → Data Minimization


Selective Disclosure for presentations
Predicate Proofs for presentations
Unlinkability of presentations
Issuer
Holder
Repudiation of presentations

Requirement	Threat	Possible Controls
Selective Disclosure for Presentations Empowering the holder to disclose only selected attributes of a credential during the presentation.	Overidentification	Issuer Authenticated Channel, Salted Hashes, Advanced Signature Schemes
Predicate Proofs for Presentations Proof of a logical statement about an attribute. e.g. age is older than x, place of residence is in the region y.	Overidentification	Issuer Authenticated Channel, Dedicated Attributes, Advanced Signature Schemes
Unlinkability of Presentations It cannot sufficiently distinguished whether two Presentations are related to the same Holder or not.	Tracking	Avoid unique identifiers within the Presentation
Repudiation of Presentations Denial in having participated in the presentation by one of the entities involved.	Confidentiality of highly reliable ID data	Issuer Authenticated Channel, Publish signing keys, Advanced Signature Schemes

Anforderungen

Protocol Security → Verification


Completeness

Soundness

Freshness of presentations

Unforgeability of credentials

Non-duplication of credentials

Holder Binding of presentations

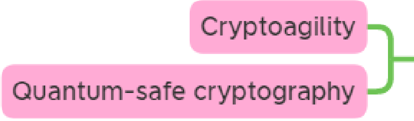
Revocation of credentials

Requirement	Threat	Possible Controls
Completeness Valid authentication attempts are accepted.	eID Availability	Verification of eID-Lifecycle Protocols & Cryptography: Create, Issue, Store, Present, Verify, Revoke
Soundness Invalid authentication attempts are declined.	Impersonation	Verification of Controls & Cryptography to prevent Impersonation

Desired level of assurance determines …

… verification of resistance to attack potential: enhanced-basic, moderate, high [3][2]

… verification method: documentation, external evaluation, cryptographic security proofs, certification [4]



Cryptoagility

Quantum-safe cryptography

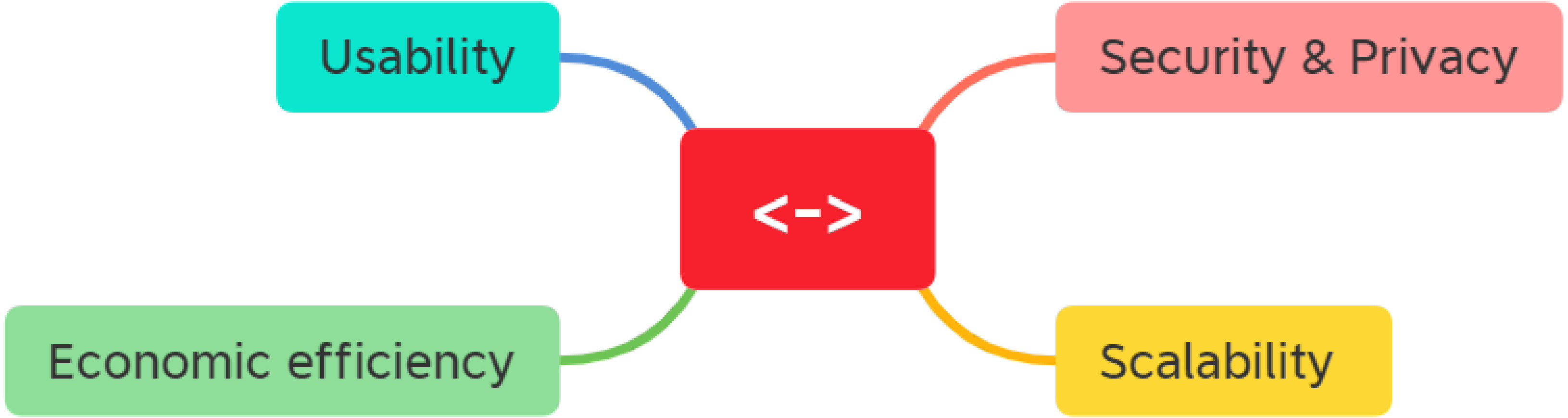
Anforderungen

Future Security

Requirement	Threat	Control
Crypto-Agility The underlying cryptography can be easily replaced during operation.	Broken Cryptography	Protocol Support, Hardware Support (challenging, takes time, better use established/proven cryptography)
Quantum-safe cryptography The underlying cryptography is not broken by the availability of quantum computing.	Quantum Computing	Research & Rollout of Quantum-safe cryptography for mobile devices, Crypto-Agility

Anforderungen

Choice of controls



Choice of controls should optimize requirements in total!

Quellen

...

[1] ISO/IEC 29115:2013, Information technology - Security techniques - Entity authentication assurance framework, 2013 (confirmed 2020)

[2] ISO/IEC 18045:2008, Information technology - Security techniques - Methodology for IT security evaluation, 2020

[3] European Commission, COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, 2015, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002)

[4] BSI - Bewertung von Authentisierungslösungen gemäß TR-03107 in Version 1.1.1, 2022

[5] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 2021 (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A281%3AFIN)

[6] Richter et al., “Cryptographic Requirements of Verifiable Credentials for Digital Identification Documents.” In 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), IEEE, 2023. https://doi.org/10.1109/COMPSAC57700.2023.00257

Kontakt

Martin Seiffert

Departement Secure Systems Engineering

Tel. +49 89 32299 86 231

Martin.Seiffert@aisec.fraunhofer.de

Fraunhofer AISEC
Breite Straße 12
14199 Berlin
https://www.aisec.fraunhofer.de

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC