Bundesamt für Sicherheit in der Informationstechnik

.msg

Fraunhofer FOKUS

Records Management and Long-Term Preservation of Evidence in DLT

Dr. Ulrike Korte, Federal Office for Information Security
Tomasz Kusber, Fraunhofer Institute for Open Communication Systems
Kalinda Shamburger, Senior Business Consultant, msg group
Steffen Schwalm, Principal Business Consultant, msg group

02. June 2021

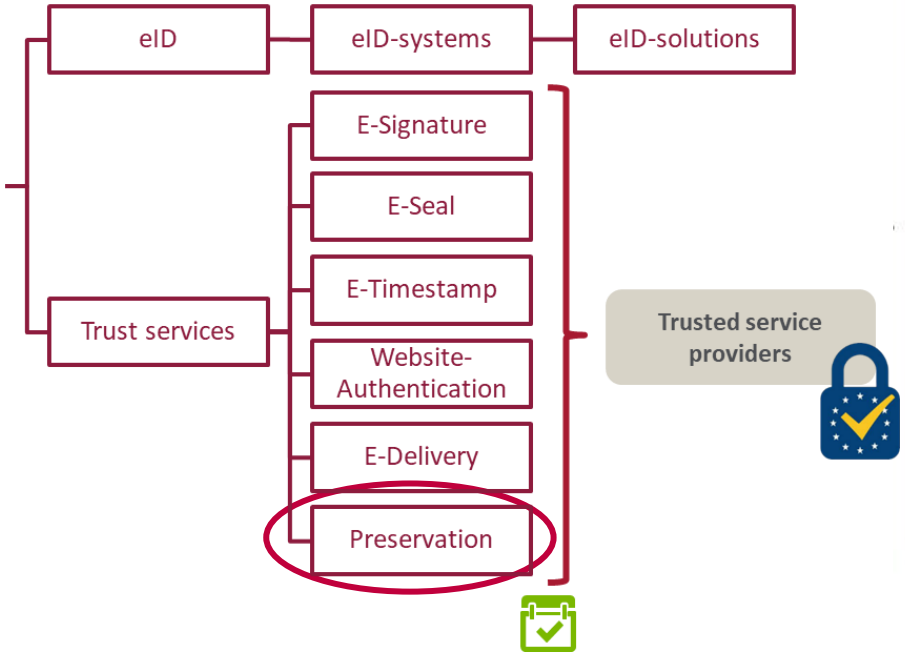
1. Regulatory Framework

eIDAS defines mandatory regulatory framework for trustworthy digital transactions in EU & EFTA

eIDAS

- Mandatory in EU & EFTA
- Holistic international standardization
- National certification – international recognition
- Preservation of evidence necessary
- Certified QTSP in European wide TSL
- Obligation of acception for public administrationx

eID & Trust Services



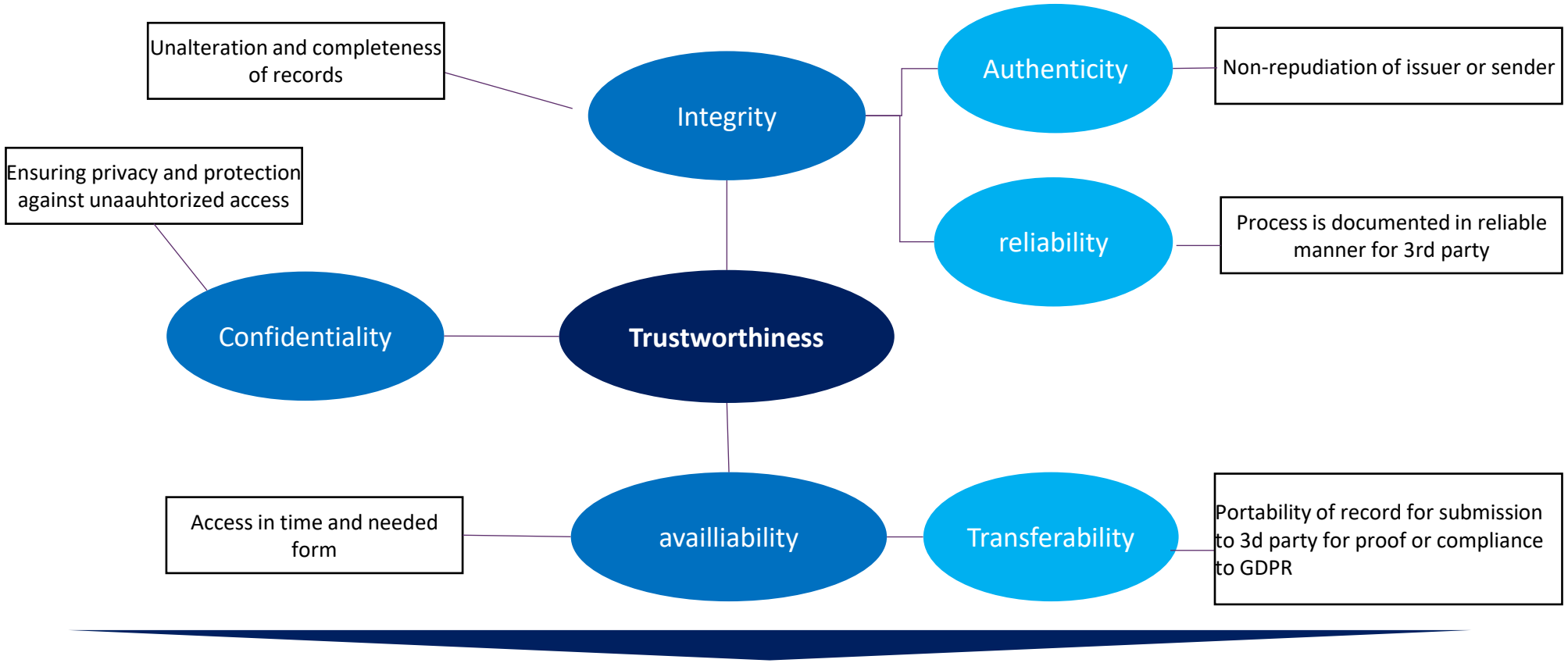
Standardization Framework

General Policy Requirements	ETSI EN 319 401
Requirements for Conformity Assessments	ETSI EN 319 403
Website Certs	ETSI EN 319 411-1
Qualified Certs	ETSI EN 319 411-2
Public Key Certs	ETSI EN 319 411-3
Attribute Certs	ETSI EN 319 411-4
Time Stamps	ETSI EN 319 421

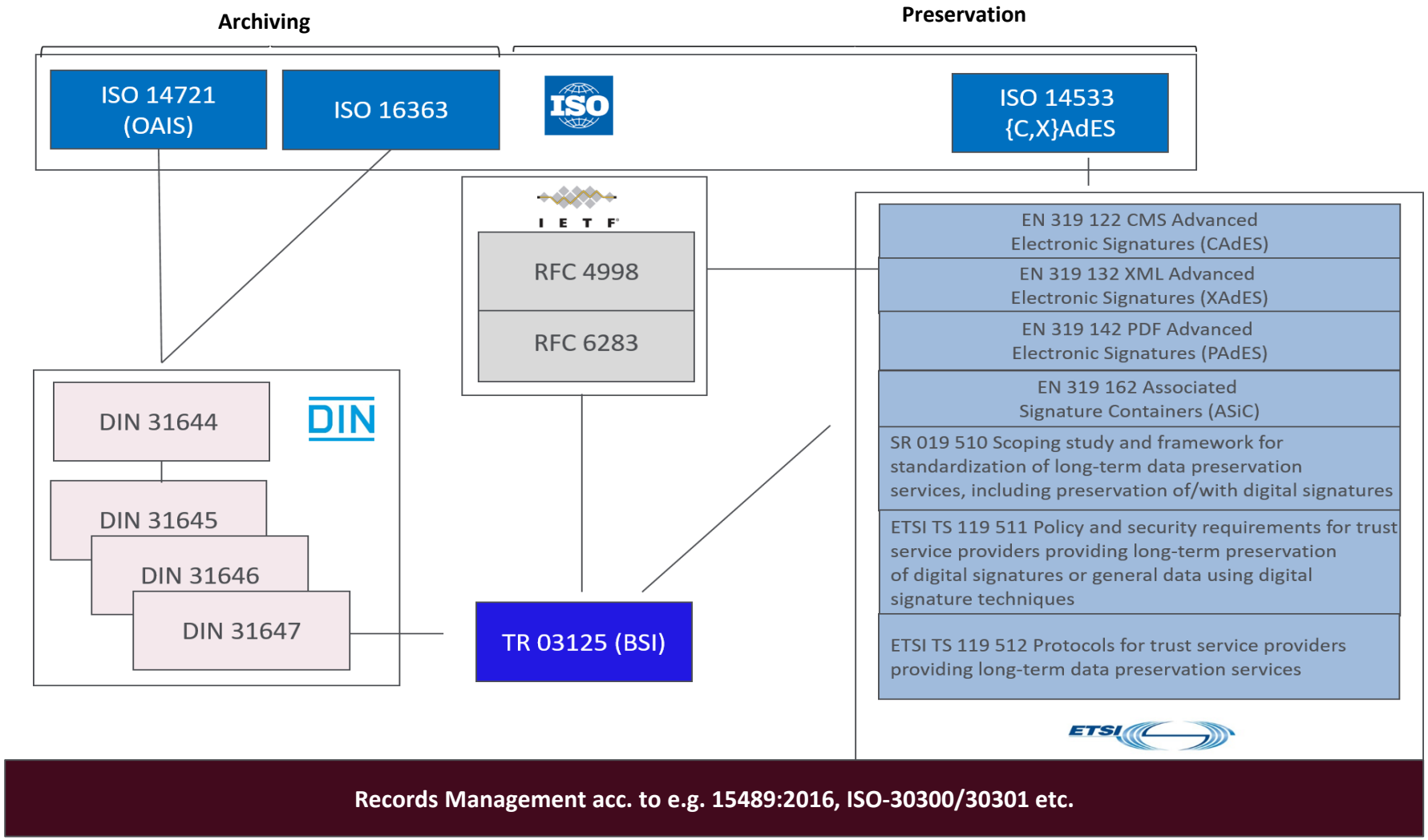
Bundesamt für Sicherheit in der Informationstechnik
.msg
Fraunhofer FOKUS

2. Requirements on trustworthy digital transactions

The main requirements on electronic records and transactions have to made evidence against 3rd parties as long as they are needed – appropriate measures necessary in DLT



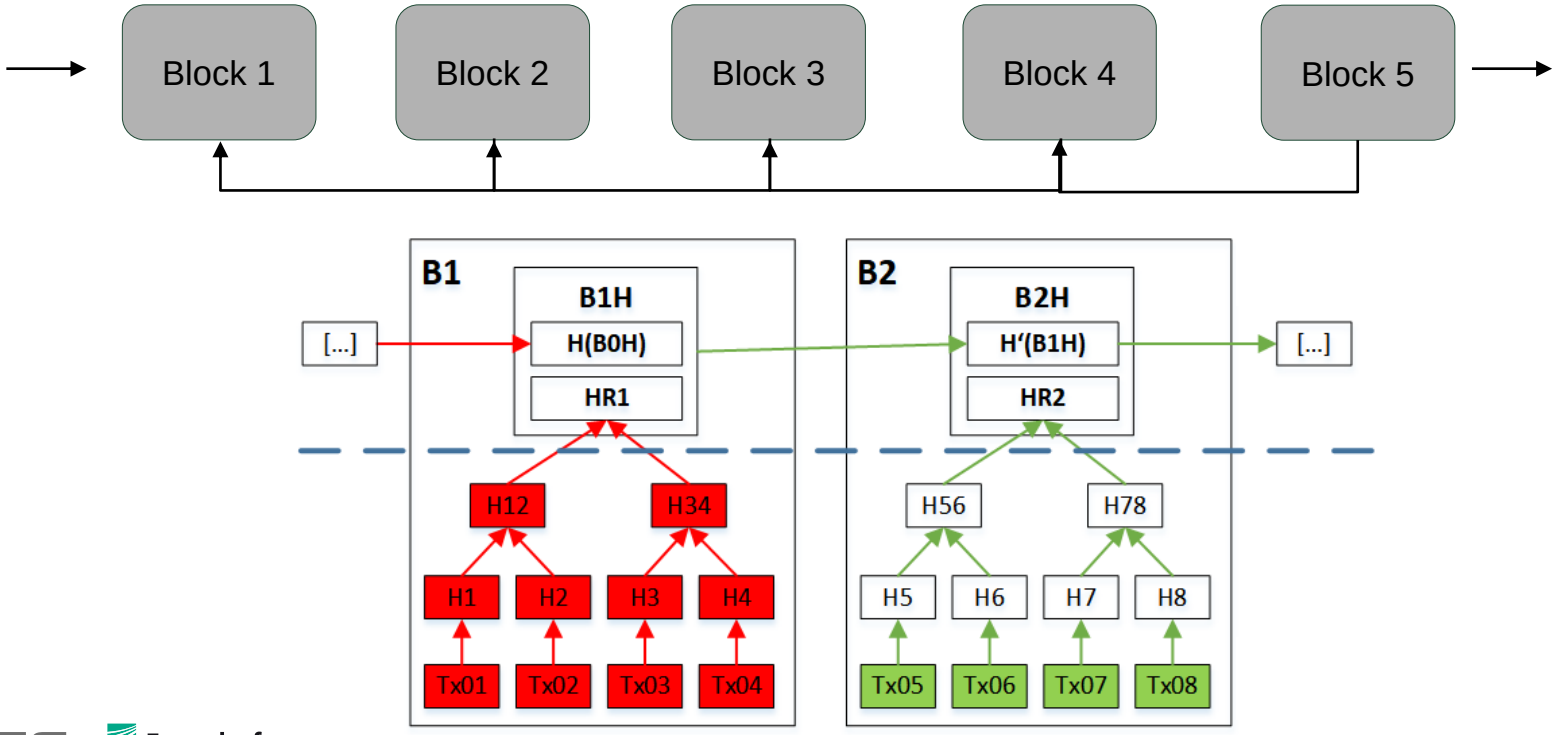
Utilisation of state of the art standards ensures long-term preservation & archiving of electronic records



Bundesamt für Sicherheit in der Informationstechnik .msg Fraunhofer FOKUS

Challenges in DLT: There`s no rehashing or Proof Of Existence for the integrity protection

- Block 2 hash 1, Block 3 hash 2, but no standardized rehashing exists
- Unnoticed manipulation possible due to recalculation of hash values acc. to expiration of security suitability of algorithm
- No valid and standardized Proof of Existence due to lack of eIDAS-compliant timestamps
- Currently no standardized measures for preservation of evidence and on-chain records



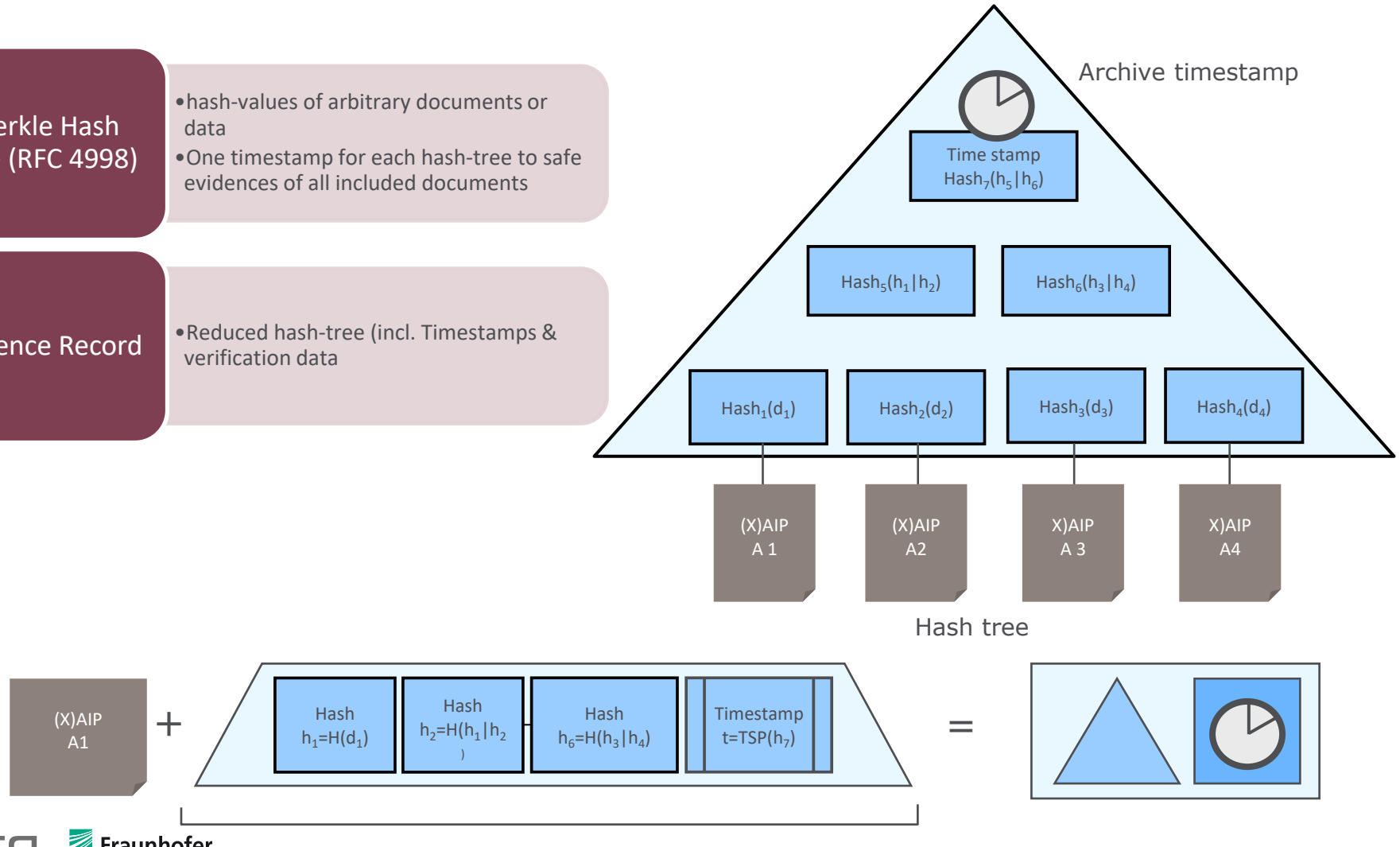
Current solution on preservation of evidence acc. To Art. 34 + 40 eIDAS as well as ETSI TS 119 511 + 512: One Hashtree for the preservation of evidence for n-data

Merkle Hash Tree (RFC 4998)

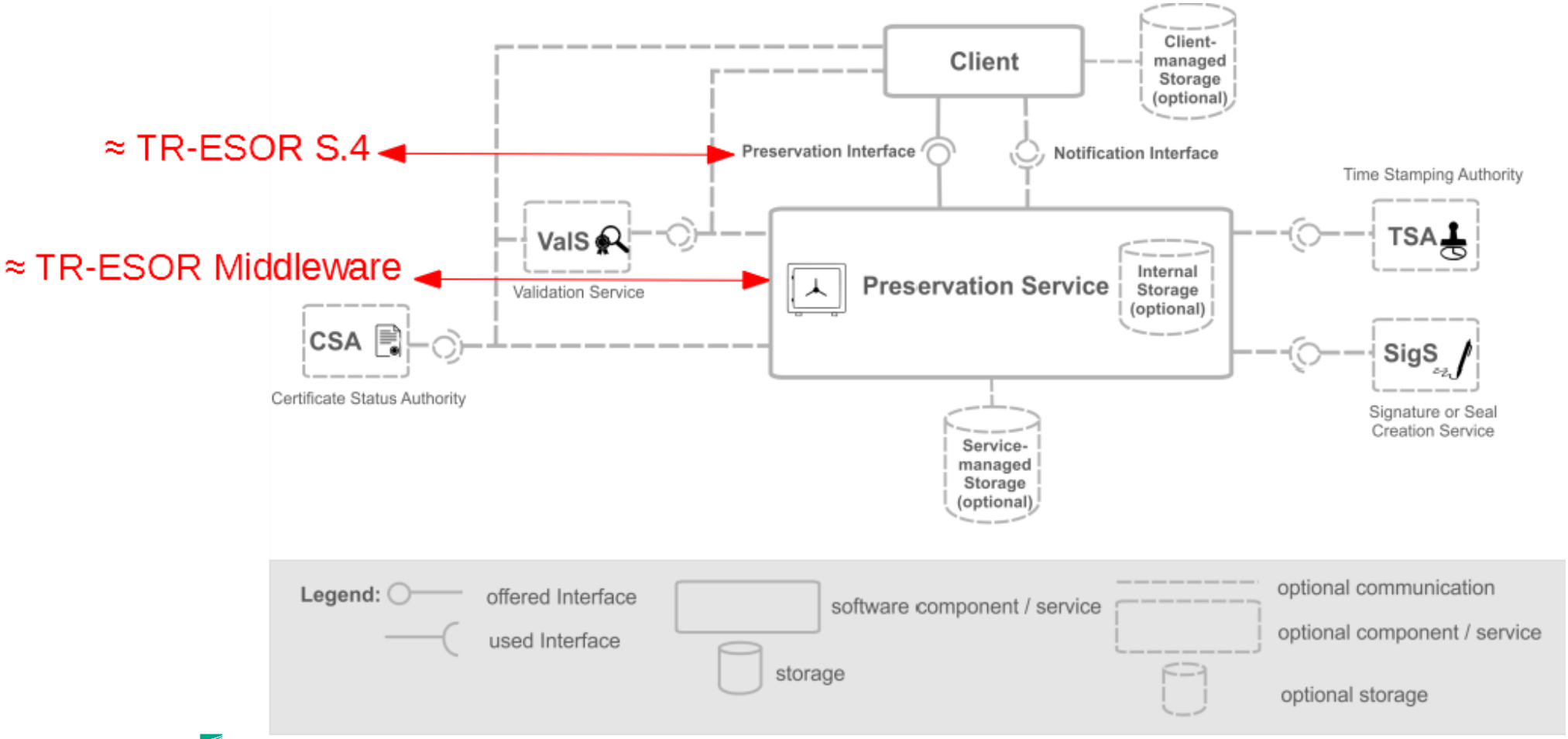
- hash-values of arbitrary documents or data
- One timestamp for each hash-tree to safe evidences of all included documents

Evidence Record

- Reduced hash-tree (incl. Timestamps & verification data

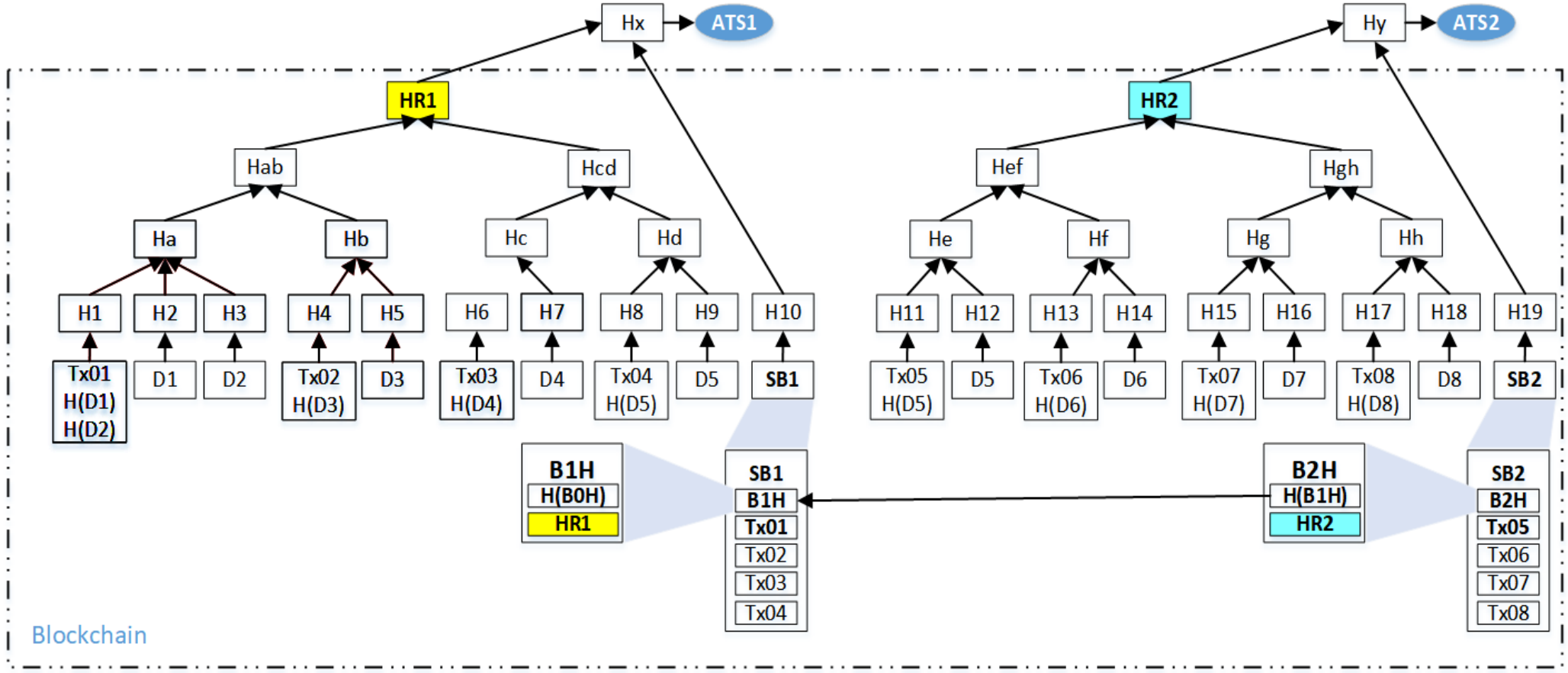


Preservation Service acc. to ETSI TS 119 512: applicable for preservation of any data



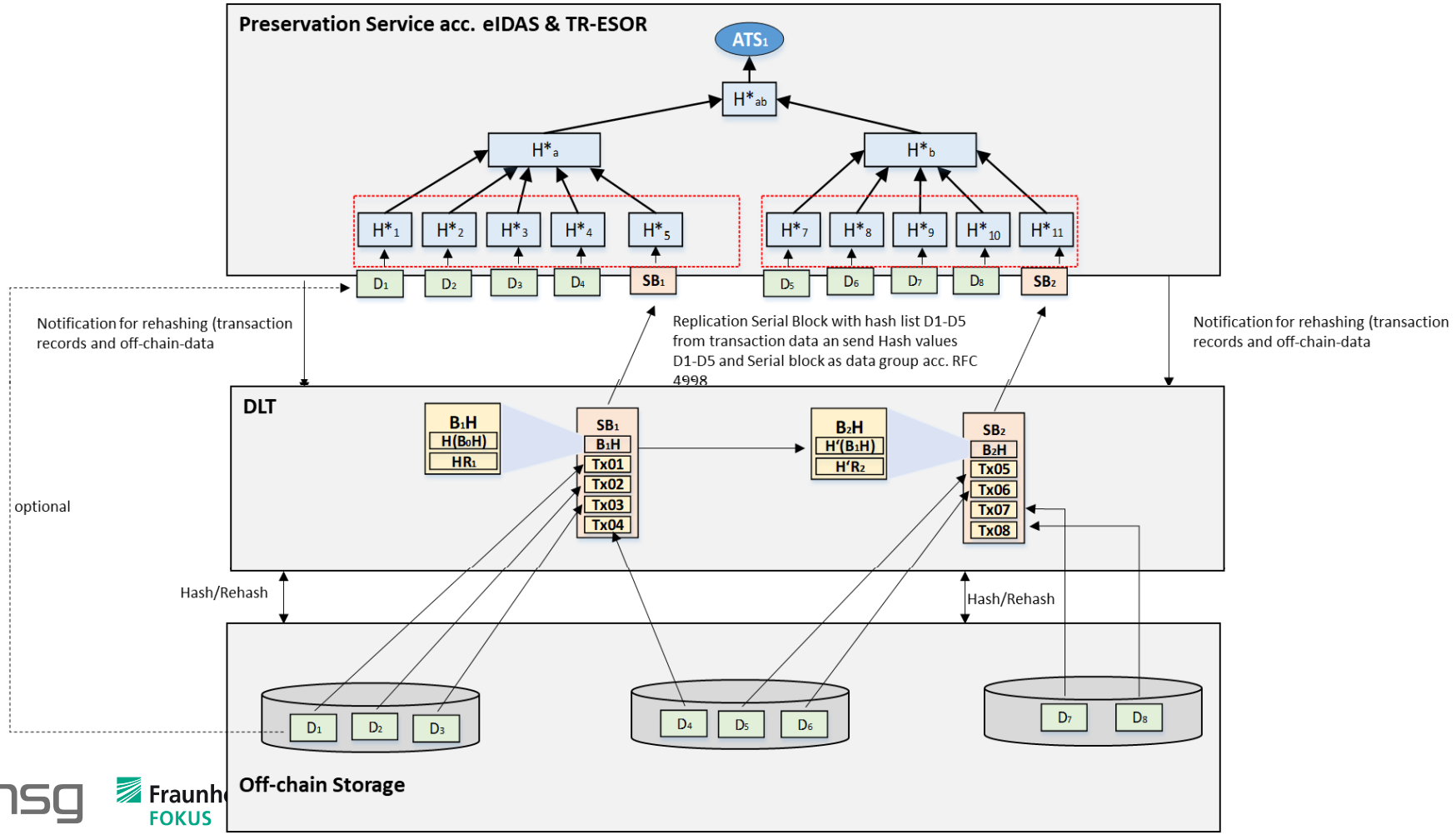
4. Possible solution

Utilisation of preservation services acc. to eIDAS solve the rehashing and PoE-challenge in DLT and achieve preservation of evidence for on-chain and off-chain data (1/2)



Bundesamt für Sicherheit in der Informationstechnik
.msg
Fraunhofer FOKUS

Utilisation of preservation services acc. to eIDAS solve the rehashing and PoE-challenge in DLT and achieve preservation of evidence for on-chain and off-chain data (2/2)



Conclusion and needs for further standardization

- Increasing utilisation of DLT leads to the need to fulfill burden of proof and documentation requirements
- Lack of crypto stability and requirements on authoritative records limit possible fields of application where DLT could achieve forseeable added value e.g.
  - Distributed digital ecosystems
  - Supply Chain
  - Digital proofs
  - SSI
- Combination of existing trust services and DLT enables feasible solution
- Solutions presumably has to be adopted for each DLT-protocol
- (inter)national Standardization necessary and ongoing for international interoperabilityx & adoption

Standardization

- **ISO Tc 46 Sc 11/Tc 307 JWG 1: ISO TR 24332**
- **ETSI Special Report on eIDAS & DLT**
- **DIN TS 31648: published in April 2021**

Bundesamt für Sicherheit in der Informationstechnik .msg Fraunhofer FOKUS

Thank you very much for your attention.

Kontakt

Federal Office for Information Security
Referat DI 15
Godesberger Allee 185 - 189
D-53175 Bonn

Dr. Ulrike Korte
Phone +49 (228) 99 9582-5842
ulrike.korte@bsi.bund.de

msg.group
Steffen Schwalm
Principal Business Consultant
Amelia Earhart-Str. 14
D-60549 Frankfurt/Main

Mobile +49 162 280 64 72
E-Mail: steffen.schwalm@msg.group

Fraunhofer Institute for Open Communication Systems
Tomasz Kusber
DPS - Digital Public Services
Kaiserin-Augusta-Allee 31
D-10589 Berlin

Phone: +49 (0) 30 / 3463-7139
E-Mail: tomasz.kusber@fokus.fraunhofer.de

msg.group
Kalinda Shamburger
Senior Business Consultant
Amelia Earhart-Str. 14
D-60549 Frankfurt/Main

Mobile +49 152 269 28 574
E-Mail: kalinda.shamburger@msg.group

Bundesamt für Sicherheit in der Informationstechnik .msg Fraunhofer FOKUS