.msg .consulting .solutions .partnership

GENERALI

Bundesamt für Sicherheit in der Informationstechnik

DEEPSHORE
HYPERLAKE DATA SOLUTIONS

Vertrauenswürdige digitale Transaktionen – Records Management und Beweiswerterhaltung mit Blockchain

Dr. Ulrike Korte, Bundesamt für Sicherheit in der Informationstechnik

Steffen Schwalm, Principal Business Consultant msg group

Michael Brünker, Deepshore

Florian Boldt, Deepshore

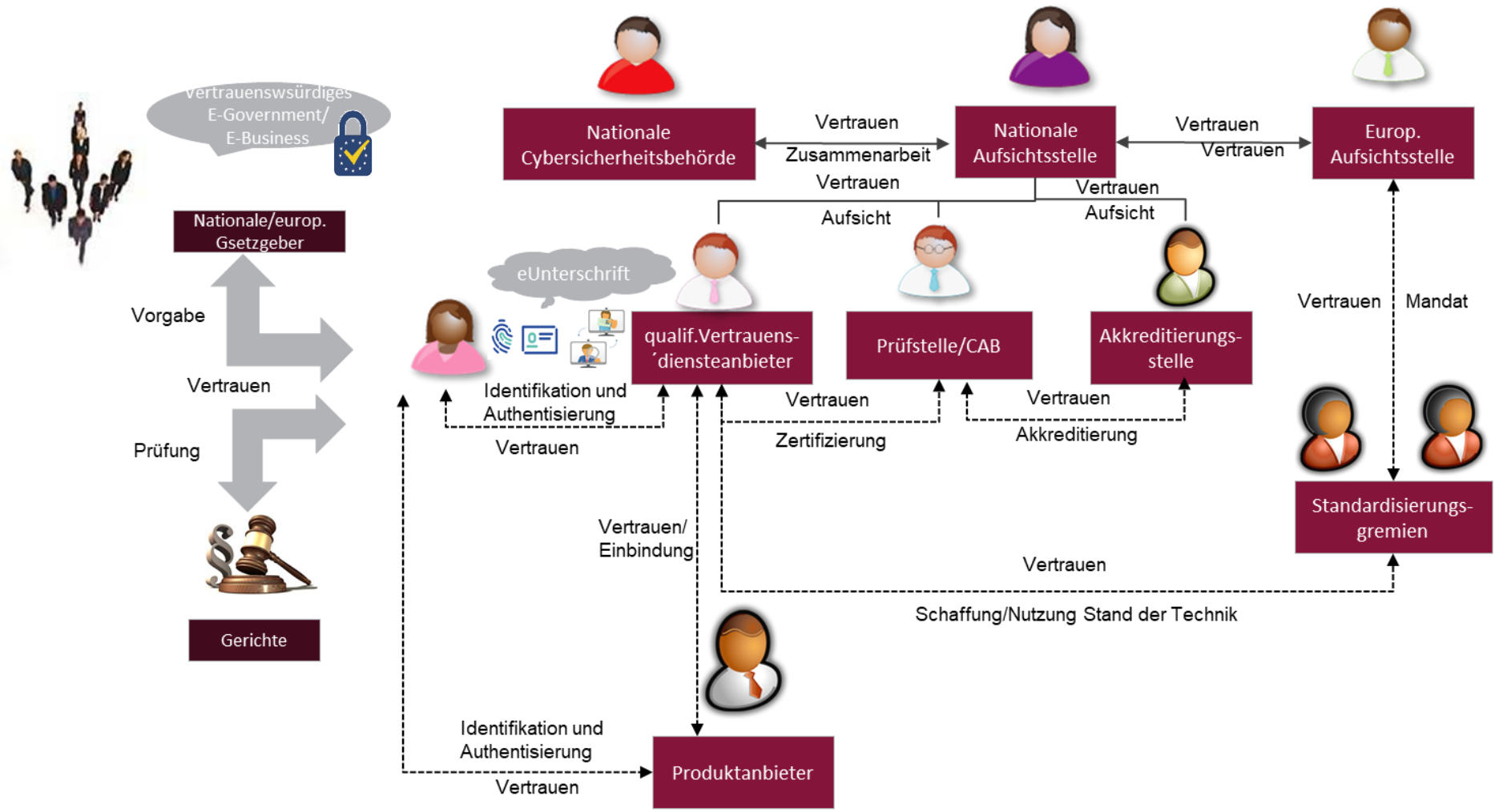
Roberto Schmidt, Generali Deutschland Informatik Services

Agenda

1. Vertrauenswürdigkeit digitaler Transaktionen
2. Aktuelle Entwicklungen zur Beweiswerterhaltung auf Basis von eIDAS,

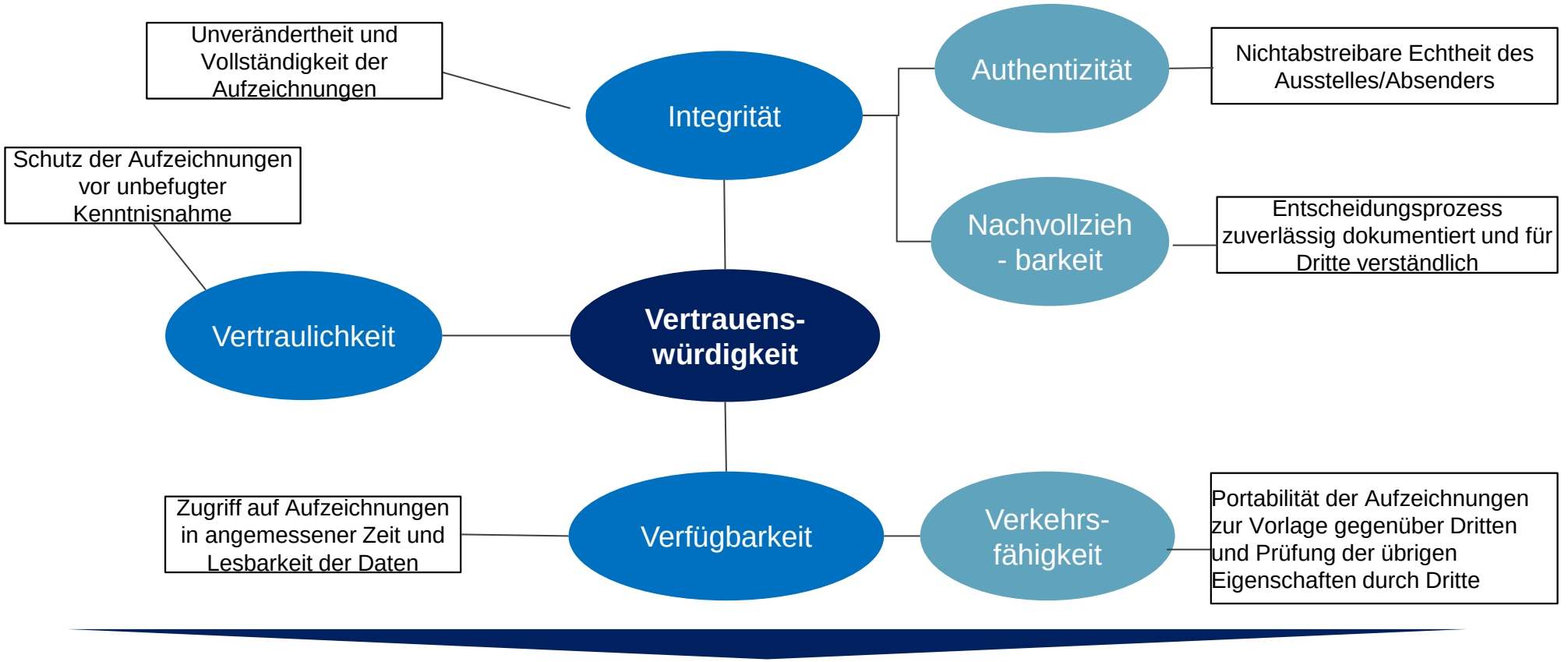
   ETSI- Standards und R-ESOR
3. Vertrauenswürdige Transaktionen und Beweiswerterhaltung mit Blockchain
4. Aktuelle Anwendungsfälle

Vertrauenswürdigkeit im Kontext geschäftsrelevanter Aufzeichnungen beruht auf Vorhandensein und Prüfung durch unabhängige Dritte (Vertrauenskette am Beispiel eIDAS)



Quelle: U.Korte, T. Kusber, S. Schwalm: Vertrauenswürdiges E-Government – Anforderungen und Lösungen zur beweiswerterhaltenden Langzeitspeicherung. 23. Archivwissenschaftliches Kolloqium. Marburg 2018

Für vertrauenswürdige digitale Geschäftsprozesse sind im wesentlichen die folgenden Anforderungen anhand der geschäftsrelevanten Unterlagen nachzuweisen



Gewährleistung durch definierte Prozesse, Organisation, Governance, IT (Records Management)

Ein ordnungsgemäßes Records Management gewährleistet die notwendigen Prozesse, Verantwortlichkeiten und Governance zum Management geschäftsrelevanter Aufzeichnungen – und eIDAS ist eine elementare Basis zur Umsetzung

- Compliance zu geltenden regulatorischen Vorgaben
- Ordnung, Strukturierung
- Klare Rollen und Verantwortlichkeiten
- Beschreibung und zeitnahe Wiederauffindung
- Nachweisfähigkeit bis zum Ablauf der Aufbewahrungsfrist (Information und Beweiswert)

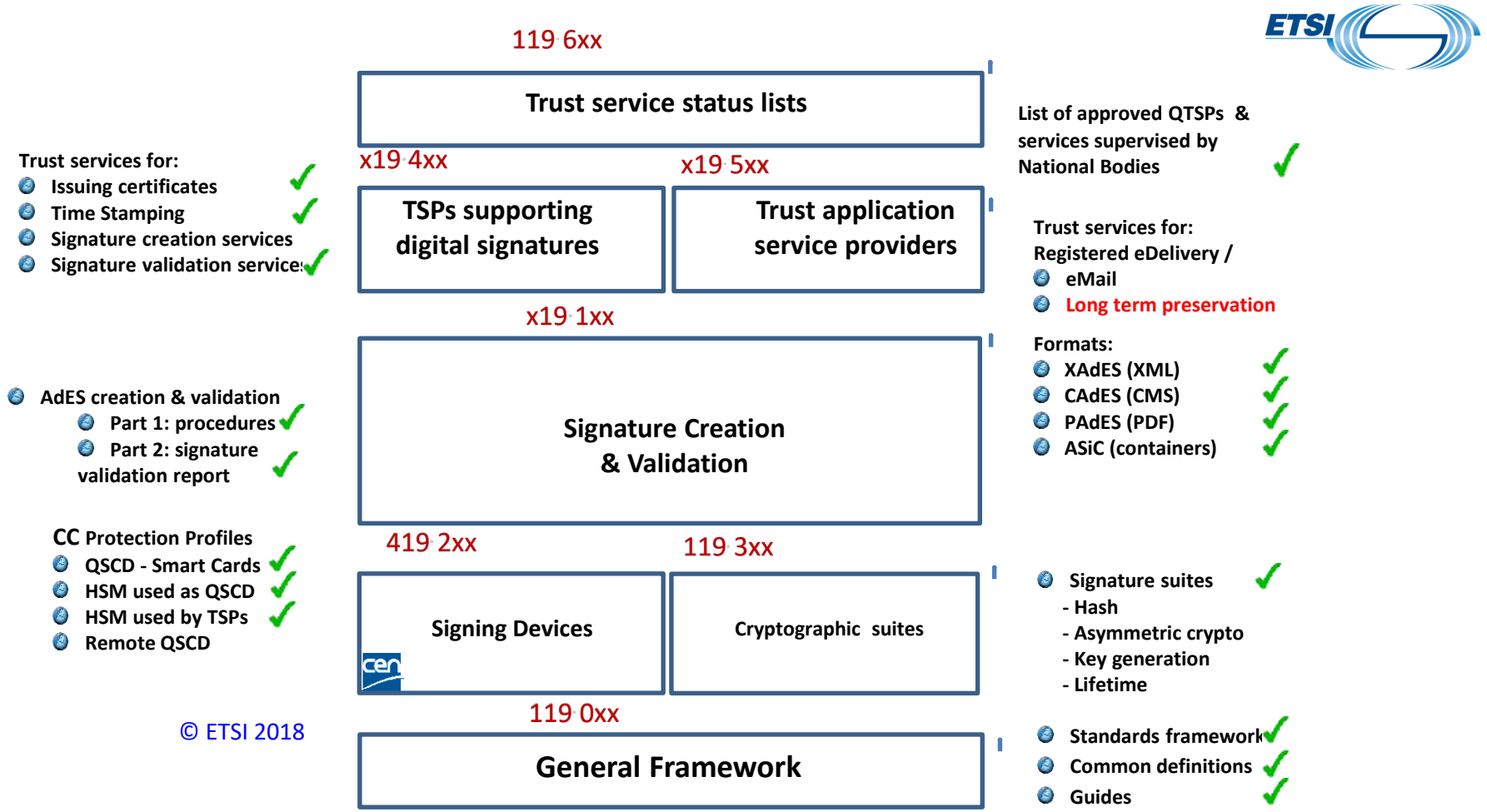
DIN NID 15
WG2 Records Management
(Weber, Schwalm et. al)

creates information which provide the evidence for business transactions against third parties

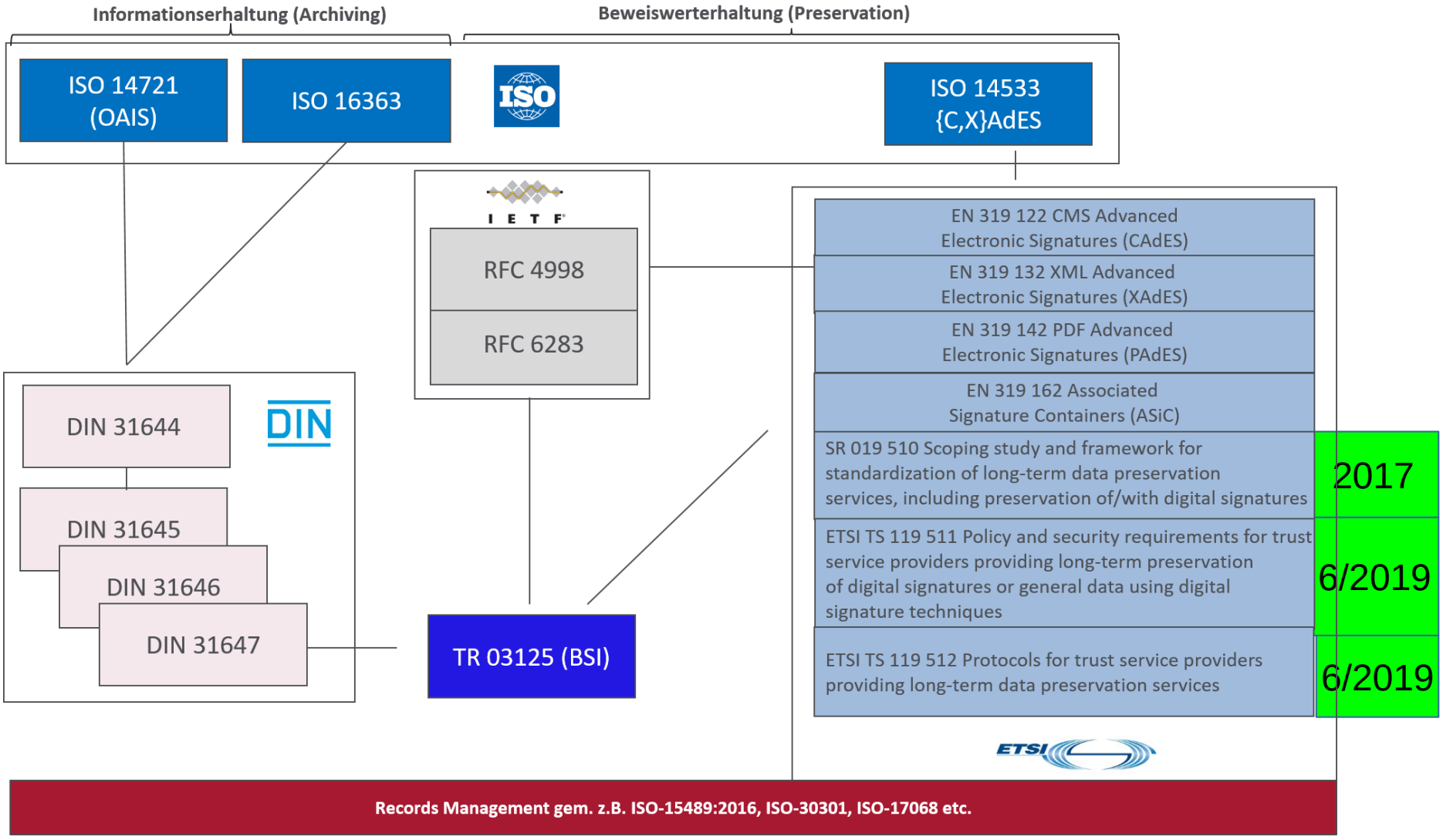
Agenda

1. Vertrauenswürdigkeit digitaler Transaktionen
2. Aktuelle Entwicklungen zur Beweiswerterhaltung auf Basis von eIDAS, ETSI-Standards und R-ESOR
1. Vertrauenswürdige Transaktionen und Beweiswerterhaltung mit Blockchain
2. Aktuelle Anwendungsfälle

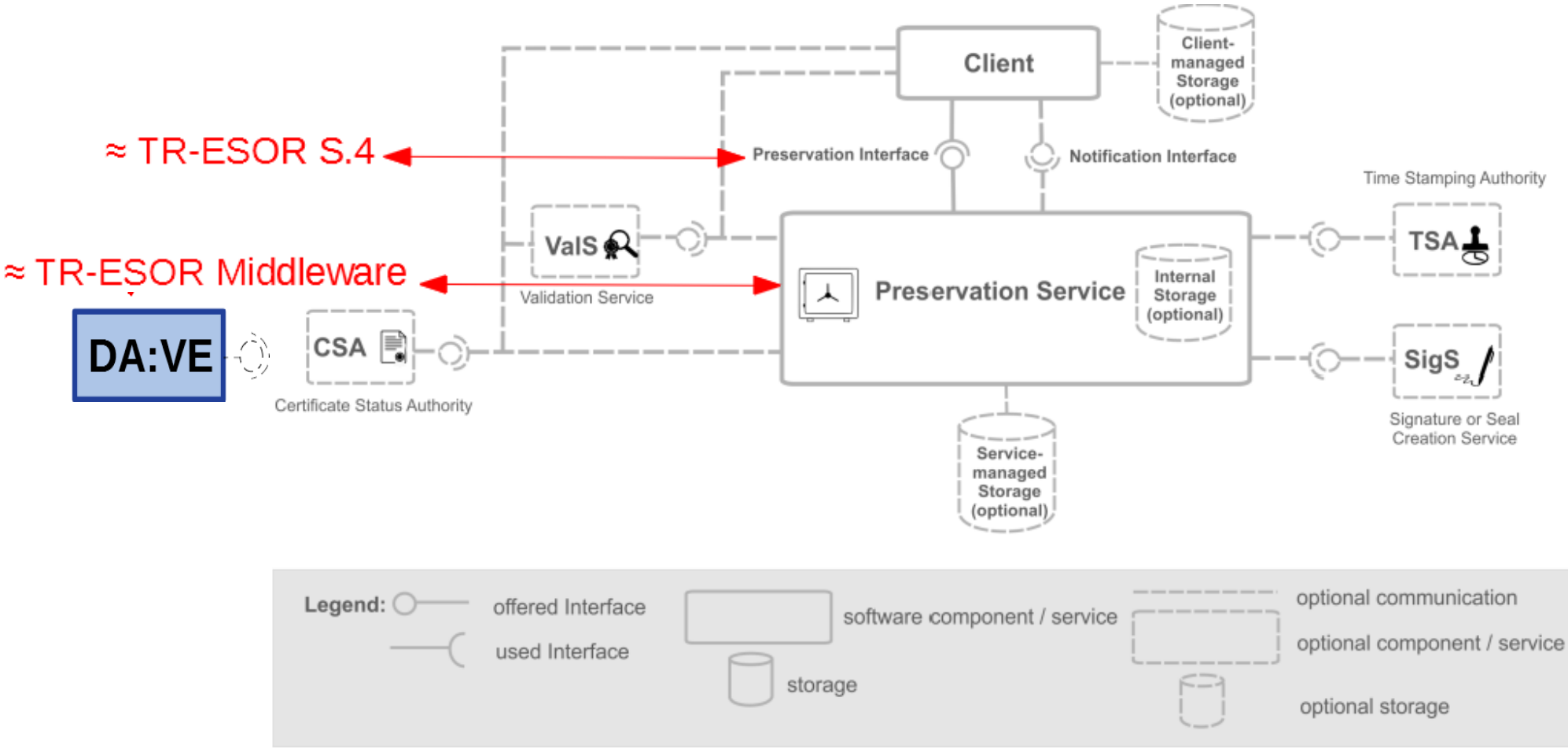
eIDAS Standards Framework: Published Standards



Stand der Technik zur beweiswerterhaltenden Langzeitspeicherung zum langfristigen Nachweis digitaler Transaktionen



Die TR-ESOR-Architektur ist in der Architektur eines Bewahrungsdienstes nach TS119 511/512 auf Basis von eIDAS enthalten.



ETSI TS 119 512 – Preservation Protocol

- Allgemeines Konzept (Architektur, Ziele, Speichermodelle, ..)
- Technische Spezifikation der Bewahrungs-Schnittstellen
  - in generischer Weise und dann spezifiziert als konkrete Syntax (XML/SOAP und JSON/REST) (wird in TR-ESOR V1.2.2 aufgenommen)
- Technische Spezifikation der Parameter/Komponenten der Schnittstelle
- Annexes, e.g.:
  - Preservation Objekt Formate
    - SDOs,
    - Preservation Evidence Formate, u.a. Evidence Record (RFC4998 / TR-ESOR)
    - POC Formats (ASiC withEvicence Record, TR-ESOR-XAIP)
  - XML Schema Dokument und JSON Schema Dokument...

- Link: https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI TS 119 512 / TR-ESOR: Transformierbare Schnittstellen

ETSI TS 119 512				TR-ESOR V1.2 ff	Verbindlich-keitsgrad
			mit Speicher		
PreservePO **m=mandatory**			X	• **ArchiveSubmissionRequest**	m=mandatory
DeletePO	**m**		X	• **ArchiveDeletionRequest**	• m
RetrievePO	**m**		X	• **ArchiveEvidenceRequest**	m
RetrievePO	**m**		X	• **ArchiveRetrievalRequest**	m
UpdatePOC **(optional)**			X	• **ArchiveUpdateRequest**	**optional**
Validate Evidence **(optional)**			X	**VerifyRequest**	**optional**
RetrieveInfo			X		
RetrieveTrace **(optional)**			X		
Search **(optional)**			X	• **ArchiveDataRequest**	**optional**

Umsetzung: modular-skalierbare Architektur der TR-ESOR-Middleware

Applikationsschicht

Applikation ... Applikation ... Applikation ... Applikation

XML-Adapter

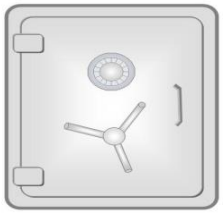
• Preservation-API (TS 119512)

TR-ESOR-Middleware

Enthalten In
ETSI SR 019 510
ETSI TS 119 511
ETSI TS 119 512

ArchiSafe-Schnittstelle (TR-S.4)

ArchiSafe-Modul (TR-M.1)



ArchiSig-Schnittstelle (TR-S.6)

IETF RFC 4998/6283

ArchiSig-Modul (TR-M.3)

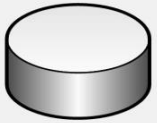
Projekt „ArchSig“, ERS aus RFC 4998 bzw. RFC 6283, eingegangen in ISO14533, ETSI EN 319 102-1, ETSI EN 319 122-3, ETSI EN 319 162, ..

TR-S.2 TR-S.5

Krypto-Schnittstelle (TR-S.1 / TR-S.3)

Krypto-Modul (TR-M.2)

ECM-/Langzeitspeicher-Schnittstelle



ECM-/Langzeitspeicher

Auf Basis eCard-API-Framework

eCard-API / BSI-TR-03112
ISO 24727

Aktuelle Weiterentwicklung der TR 03125 TR-ESOR

TR-ESOR v1.2.1 (seit 2018)

- Keine Änderungen an Architektur, Schnittstellen etc.
- Editorielle Anpassung auf eIDAS
- Änderungen an Funktionen des Krypto-Moduls zur Signaturprüfung und Einholung der beweisrelevanten Daten
  - Schalenmodell und
  - Kettenmodell
  - Anforderung von QES/QESI/QZS beim QTSP statt selbst erzeugen

BSI TR-ESOR (TR zur Beweiswerterhaltung)

TR-ESOR v1.2.2 (3. Q. 2019) / v1.3 (ca. 1. Q. 2020)

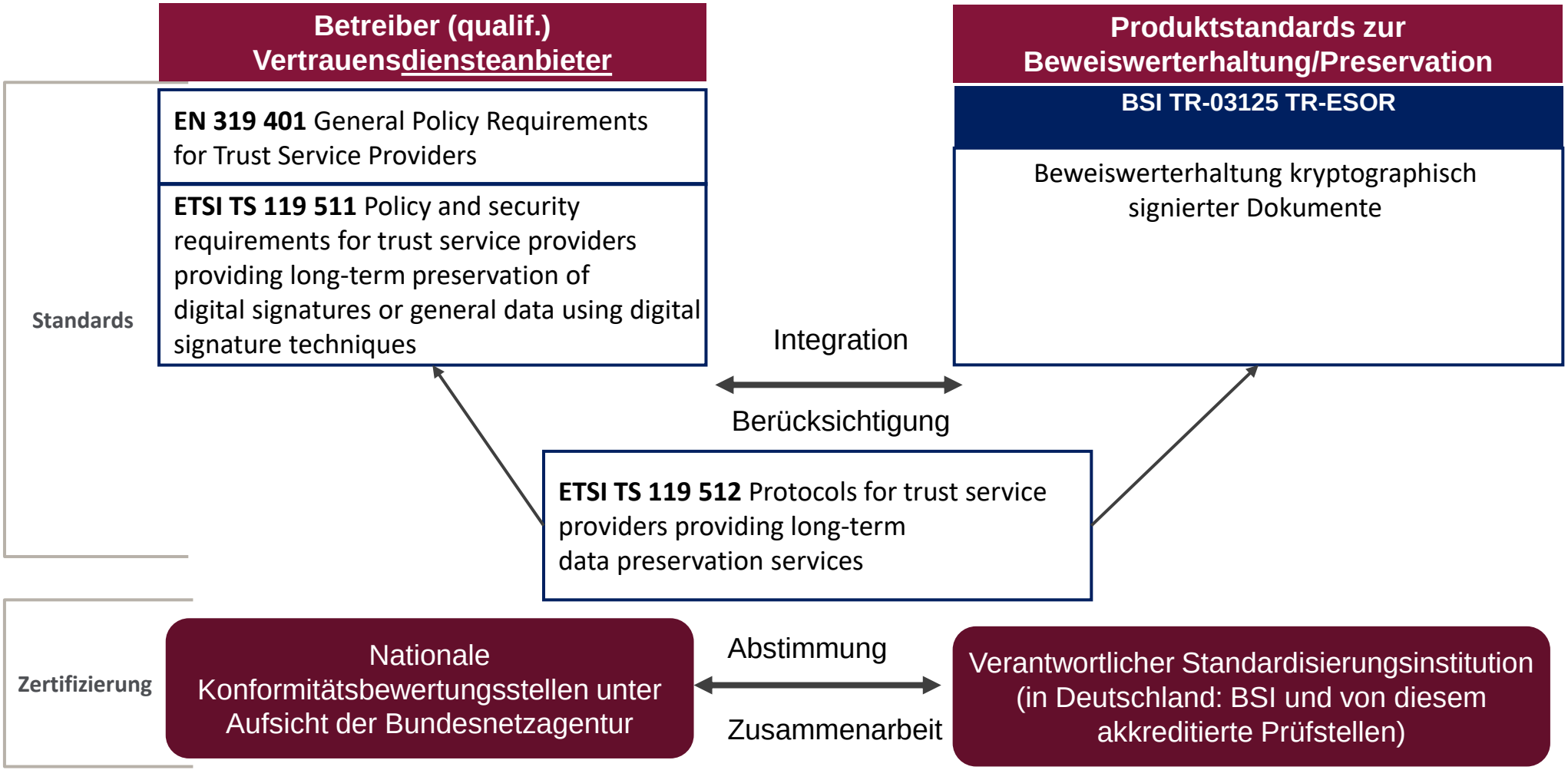
V1.2.2

- AIP-Container
  - Logisches (X-)AIP
  - ASiC-E-Profilierung auf Basis von **ETSI EN 319 162**
- Anpassungen auf eIDAS/ETSI
  - Preservation Protokoll nach **ETSI TS 119 512** als weitere obere Schnittstelle zwecks europaweite Interoperabilität
  - Englische Übersetzung

V1.3

- BSI Interop-Tools
- Anpassung Zertifizierungs-schema

Exemplarisches Zusammenspiel der Standards für (qualifizierte) Bewahrungsdienste (ServiceProvider) und deren Verfahren



Agenda

1. Vertrauenswürdigkeit digitaler Transaktionen
2. Aktuelle Entwicklungen zur Beweiswerterhaltung auf Basis von eIDAS, ETSI-Standards und R-ESOR
3. Vertrauenswürdige Transaktionen und Beweiswerterhaltung mit Blockchain
4. Aktuelle Anwendungsfälle

Blockchain – verteilte Journale in Peer-to.peer-Netzwerk zur effizienten Automatisierung (nicht nur) öffentlicher Register und Verzeichnisdienste?

Bundesamt für Sicherheit in der Informationstechnik

.msg

GENERALI

DEEPSHORE
HYPERLAKE DATA SOLUTIONS

Permissionless/Public Chain

- Keine zentrale Instanz (Vertrauensmodell)
- Vertrauen durch die Community (51%-Modell) ermöglicht schnellen Rollout , birgt jedoch Sicherheitsrisiken
  - Problem: rechtlich nicht verankert
  - Anhand welcher Kriterien ist eine Community vertrauenswürdig?
  - Wie kann ein System/eine Community vertrauenswürdig sein, deren Vertrauen von der faktisch finanziellen Kraft abhängt, 40% der Knoten der Publc Chain zu übernehmen?
  - Kritisch bei nachweispflichtigen Prozessen
- anreizbasierter Konsensmechanismus z.B. PoW
- Mining durch alle Nutzer, keine eindeutige Identifikation, faktisch keine Nutzerkontrolle
- Typisch bspw. für Kryptowährungen wie bei geringen Datendurchsatz

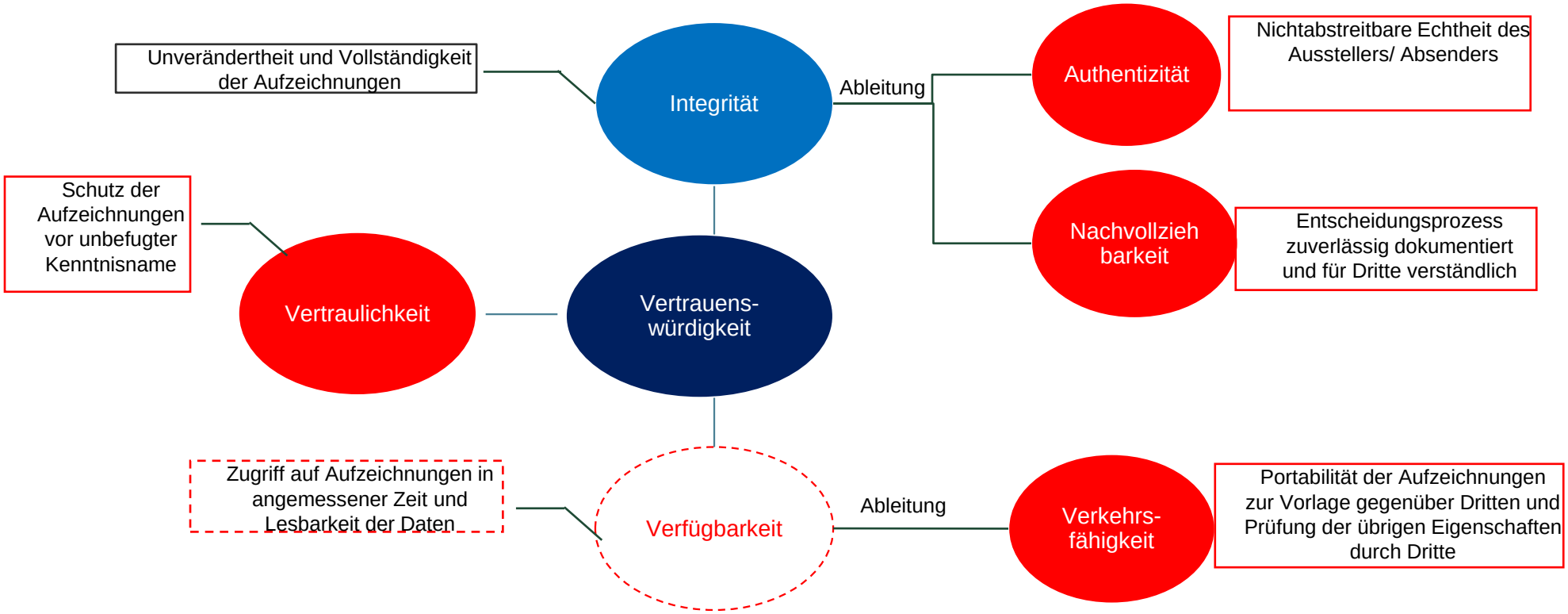
Blockchain

Permissioned/Private Chain

- Stärker zentralisiert
- Vertrauen auch durch betreibende Instanz (vertrauenswürdiger Dritter), als Vor- und Nachteil
- Nachrichtenbasierte Konsensverfahren
- Mining nur durch berechtigte User
- Kein Anreizsystem notwendig
- Begrenzter Energie-/Rechenaufwand
- Nur autorisierte Nutzer
- Eindeutige, sichere Identifizierung notwendig
- Regulatorische Compliance ggf. leichter erreichbar
- Stellt „Blockchainidee“ (unabhängig von Intermediären) in Frage

- Kryptowährungen, Hochfrequenzhandel
- Registerautomatisierung, intelligente Energienetze
- Überwachung von Lieferketten, Vertragsinhalten (SmartContracts)

Derzeit erfüllt Blockchain nur einen marginalen Teil der Anforderungen an vertrauenswürdige digitale Register/Verzeichnisdienste und Transaktionen



Gewährleistung durch definierte Prozesse, Organisation, Governance, IT (Records Management)

Wesentliche Herausforderungen an die Nutzung von Blockchain für vertrauenswürdige digitale Register/Verzeichnisdienste und Transaktionen

Bundesamt für Sicherheit in der Informationstechnik

.msg

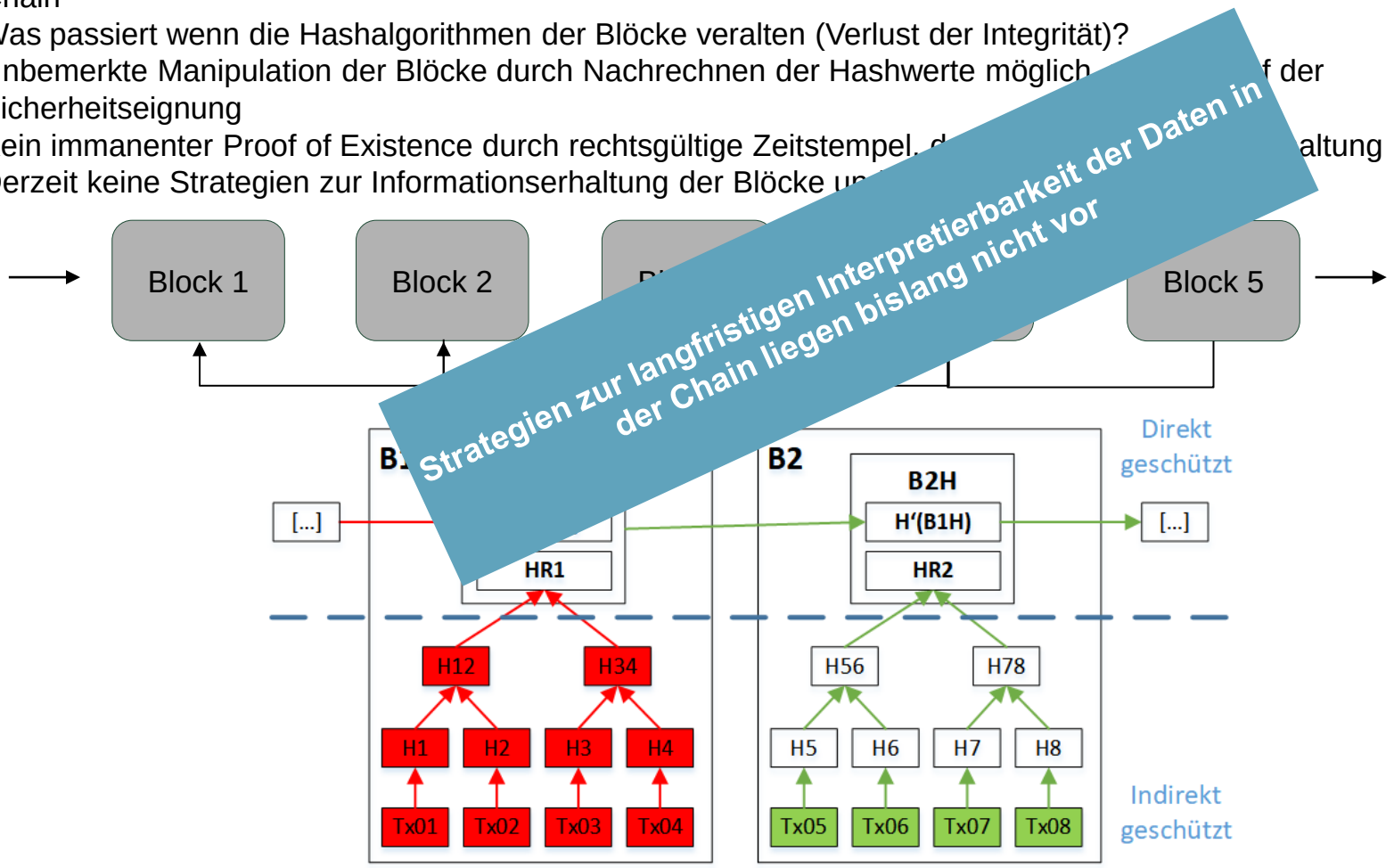
GENERALI

DEEPSHORE
HYPERLAKE DATA SOLUTIONS

- **Sichere Identifizierung und Authentisierung (sichere digitale Identität**
- **Datenschutz gem. DSGVO (z.B. Gewährleistung Rechte des Betroffenen)**
- **Vertrauenswürdigkeit/Nachweis des Abschlusses/Zeitpunkts und Zuordnung von Daten/Transaktion zum Aussteller/Organisation**
- **Langfristiger Nachweis und Sicherheit der Daten sowie Transaktion**
- **Legal Compliance, Machbarkeit und Vorteile der UseCases gegenüber „klassischen Technologien“**

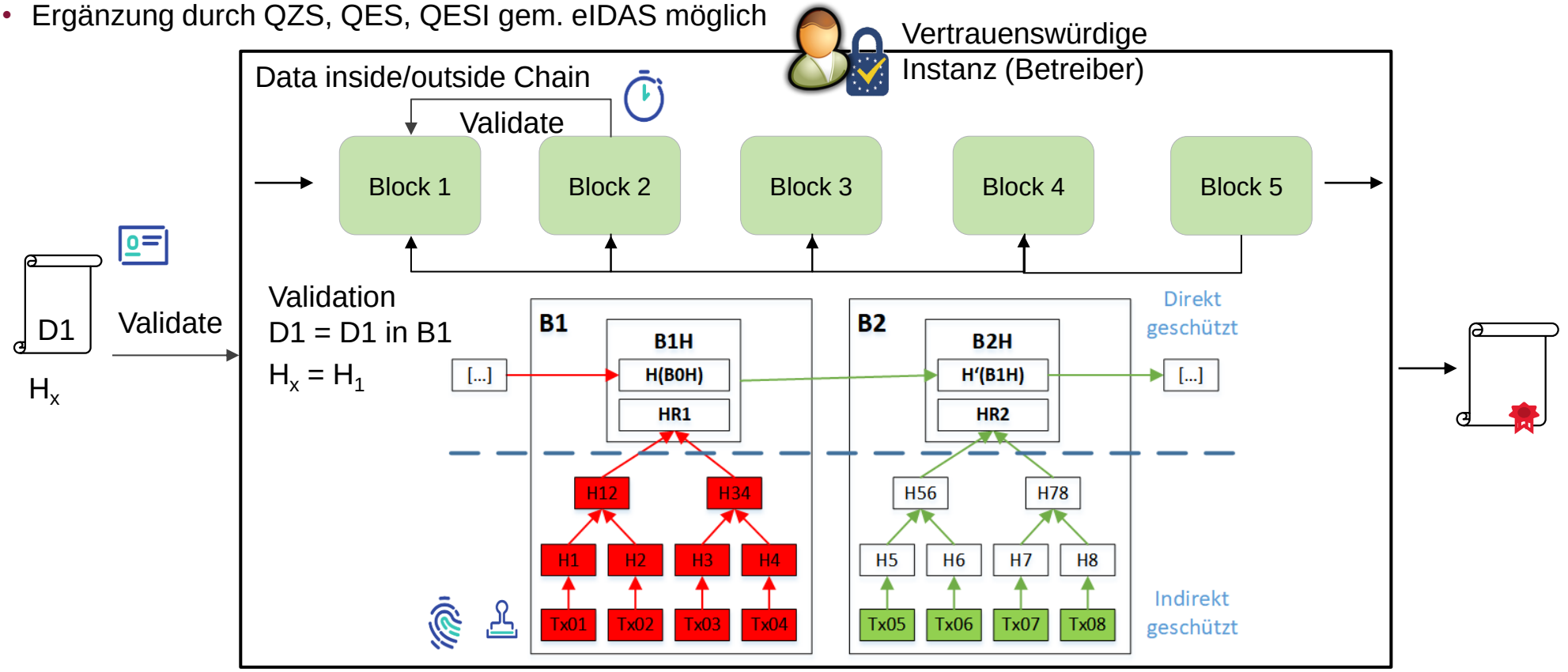
Die Blöcke werden nach dem Vater-Sohn-Prinzip verhasht – es besteht aber kein rehashing der (Block)chain

- Block 2 hasht 1, Block 3 hasht 2, aber kein Block enthält alle Hashs und kein Mechanismus zum Rehashing der Chain
- Was passiert wenn die Hashalgorithmen der Blöcke veralten (Verlust der Integrität)?
- Unbemerkte Manipulation der Blöcke durch Nachrechnen der Hashwerte möglich … f der Sicherheitseignung
- Kein immanenter Proof of Existence durch rechtsgültige Zeitstempel, d… altung
- Derzeit keine Strategien zur Informationserhaltung der Blöcke un…



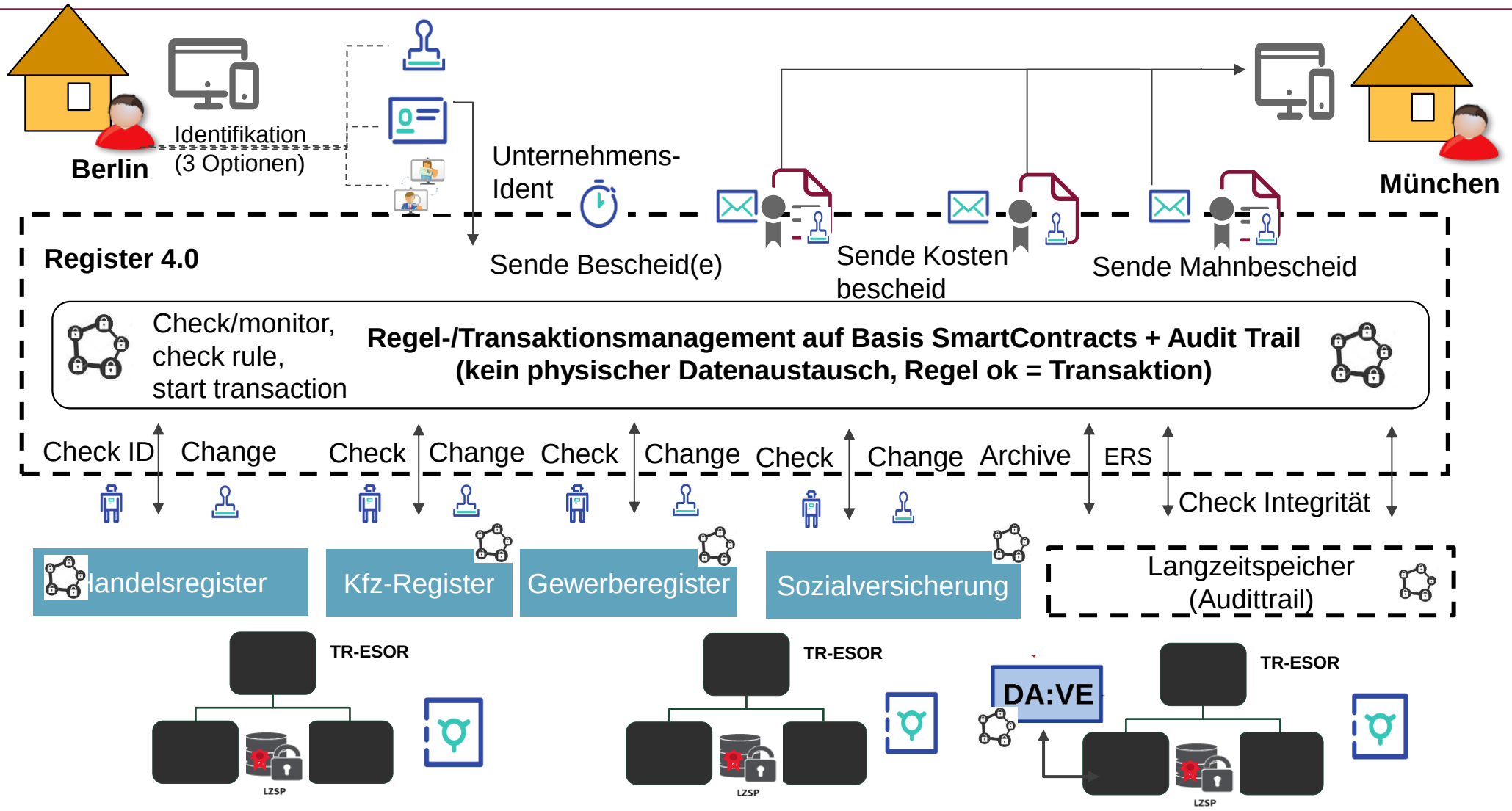
Blockchainbasierte Datenvalidierung in Public (und Private Chains): eIDAS als Schlüssel einer vertrauenswürdigen Blockchain

- Ablage von Daten oder Hash in der Chain, Absicherung durch Merkle Trees
- Bestätigung, dass ein gegebener Datensatz nicht manipuliert wurde und damit objektiv, technisch dem in einem Block der Chain gespeicherten Datensatz entspricht
- Bestätigung per Blockchain-Zeitstempel
- Ergänzung durch QZS, QES, QESI gem. eIDAS möglich



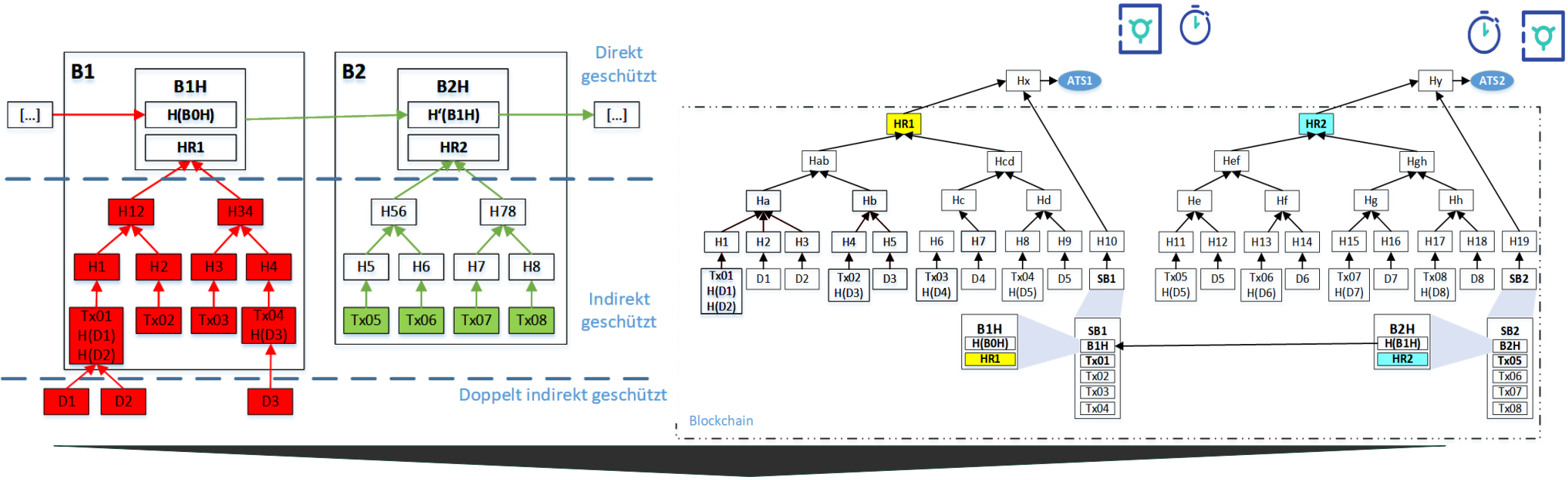
Quelle: Wurster, Ron, Schwalm et. al. DIN SPEC 3104:2019 Blockchainbasierte Datenvalidierung

Vertrauenswürdige Transaktionen durch eIDAS – Registerautomatisierung mit(Private Permissioned) Blockchain



Lösungsoption 3: logische Blockchain auf Basis von RFC4998

Wesentliche Maßgabe: aufbewahrungspflichtige Daten befinden sich außerhalb der Blockchain, Blockchain beinhaltet nur Hashwerte der Daten



+ Gewährleistung langfristiger Integritätsschutz
+ Gewährleistung Beweiswerterhaltung
+ Gewährleistung Datenschutz für Content über Fremdsystem in dem die Daten gespeichert sind (z.B. digitales Langzeitarchiv gem. OAIS [ISO-14721:2012] und TR-ESOR)
- Identifizierungsdaten befinden sich weiterhin in Blockchain mit entspr. Datenschutzproblem

Quelle: U.Korte, C. Berghoff, T. Kusber, S. Schwalm: Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain. DACH-Security 2018. S. 177-191 Frechen 2018

(Inter-)nationale Standardisierung auf Basis der eIDAS-Werkzeuge schafft den Stand der Technik für vertrauenswürdige Transaktionen – Nachweisfähigkeit und Beweiswerterhaltung mit Blockchain

Herausforderungen vertrauenswürdiger Transaktionen mit Blockchain

- Sichere digitale Identität und Authentisierung
- Datenschutz und Informationssicherheit
- Authentizität von Transaktion, Aussteller und Nachweis des Zeitpunkts einer Transaktion
- Vertrauenswürdige Archivierung (Beweiswerterhaltung)

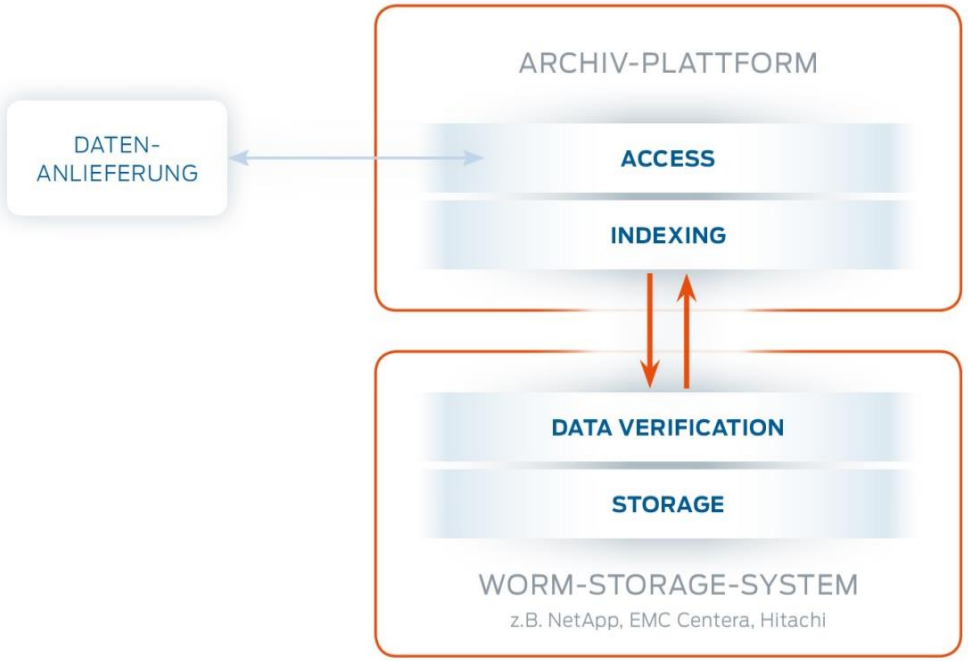
Standardisierung incl. eIDAS Vertrauensraum

Stand der Technik für vertrauenswürdige Transaktionen und Beweiswerterhaltung in Blockchain

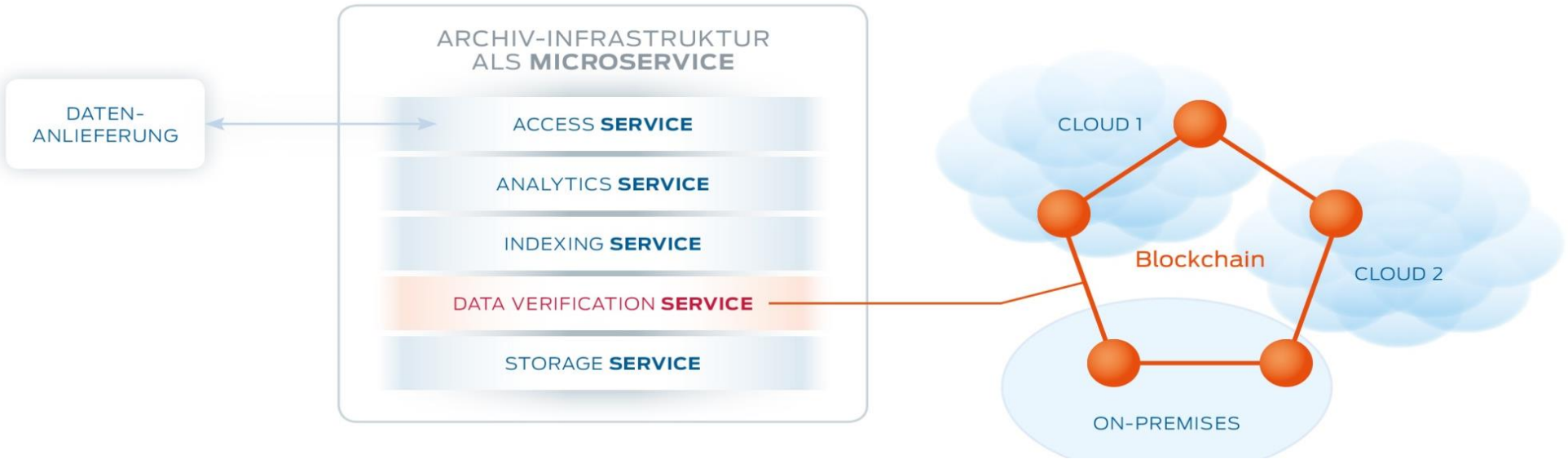
Agenda

1. Vertrauenswürdigkeit digitaler Transaktionen
2. Beweiswerterhaltung zwischen Bewahrungsdiensten und TR-ESOR
3. Vertrauenswürdige Transaktionen und Beweiswerterhaltung mit Blockchain
4. Aktuelle Anwendungsfälle

Archiv-Architektur: aktuelle Technologie



Archiv-Architektur: zukünftige Technologie



Anwendungsbeispiel e-on

Use Case:

- Wind- und Solarparks (Einspeiser) werden bei drohender Überlast des Stromnetzes situativ abgeschaltet und im Nachgang entschädigt
- Rechnungen / Gutschriften werden auf Basis einer gemeinsam akzeptierten Datenbasis (Winddaten, Anlagenleistung, Abschaltdauer) erstellt
- Einspeiser, Netzbetreiber, Bundesnetzagentur, Steuerprüfer haben vertrauenswürdige und unveränderbare Datenbank zu Einspeisemanagement-Maßnahmen und Entschädigungszahlung

-> Blockchain-Einsatz für compliance-relevante Datenbasis in der Cloud

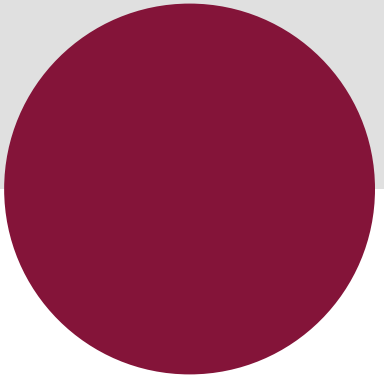
Anwendungsbeispiel METRO

Use Case:

- rechtliche Anforderungen an revisionssichere elektronische Kassenbelegsarchivierung (Rechnungen)
- Vorteile von günstigem Cloudstorage UND Revisionssicherheit abbilden
- Rechnungsbereitstellung und Verarbeitung Sekunden nach dem Kassiervorgang
- Business Analytics und Data Science auf Kassendaten anwenden

-> Blockchain-Einsatz für Compliance Storage in der Cloud

- Dr. Ulrike Korte, Bundesamt für Sicherheit in der Informationstechnik
- Steffen Schwalm, Principal Business Consultant msg group
- Michael Brünker, Deepshore
- Florian Boldt, Deepshore
- Roberto Schmidt, Generali Deutschland Informatik Services



GENERALI

Bundesamt
für Sicherheit in der
Informationstechnik

DEEPSHORE
HYPERLAKE DATA SOLUTIONS

.msg .consulting .solutions .partnership