

TeleTrust/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 20.09.2022

**Vertrauenswürdige Bewahrung und Archivierung -
Schlüssel für langfristig sichere wie selbstsouveräne
digitale Nachweise**

**Steffen Schwalm, Principal Business Consultant,
msg security advisors**

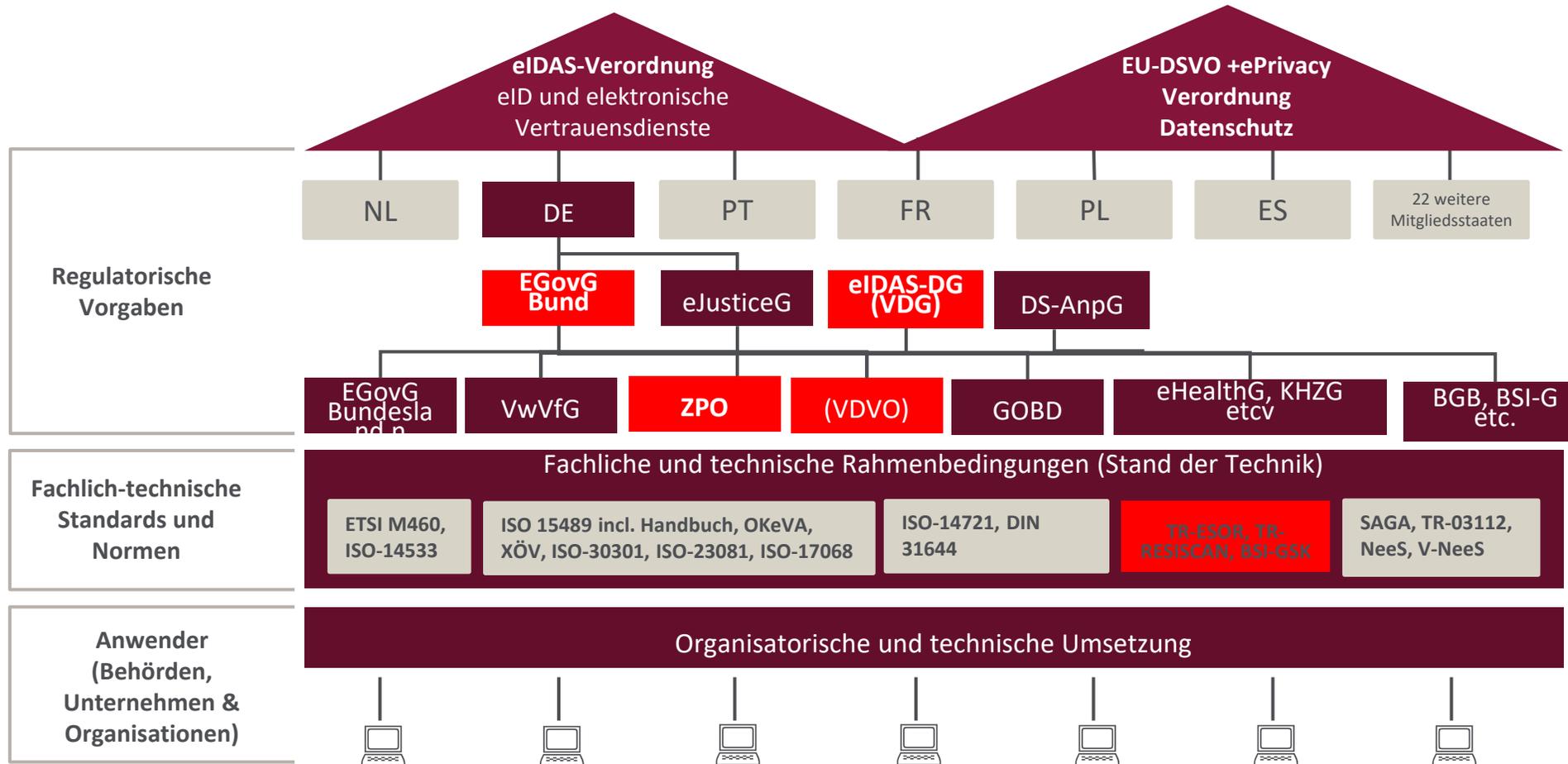
Aufbewahrungsfristen zwischen 2 und 100 Jahren oder dauernd

Umfassende Nachweispflichten

Technische Entwicklung HW/SW

Verlust Sicherheitseignung kryptographischer Sicherungsmittel

Regulatorischer Rahmen Bewahrung und Archivierung

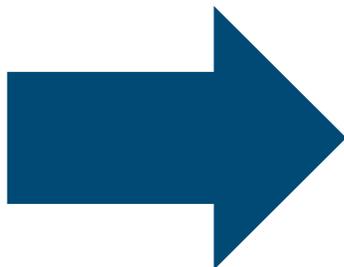


Digitale Nachweise sind nur so viel wert wie ihr Beweiswert und wie er erhalten werden kann

| | | | |
|--|---|---|--|
| private elektronische Dokumente (von Bürger/Unternehmen) ohne qualifizierte elektronische Signatur | private elektronische Dokumente (von Bürger/Unternehmen) mit qualifizierter elektronischer Signatur | Öffentliche elektronische Dokumente (von Behörde) ohne qualifizierte elektronische Signatur | öffentliche elektronische Dokumente (von Behörde) mit qualifizierter elektronischer Signatur |
| Freie Beweiswürdigung des Richters | Anschein für Echtheit | Freie Beweiswürdigung des Richters | Vermutung für Echtheit |

Beweiswert des qualif. eSiegel ergibt sich aus Art. 35 eIDAS: Authentizität und Integrität (faktischer Anscheinsbeweis)

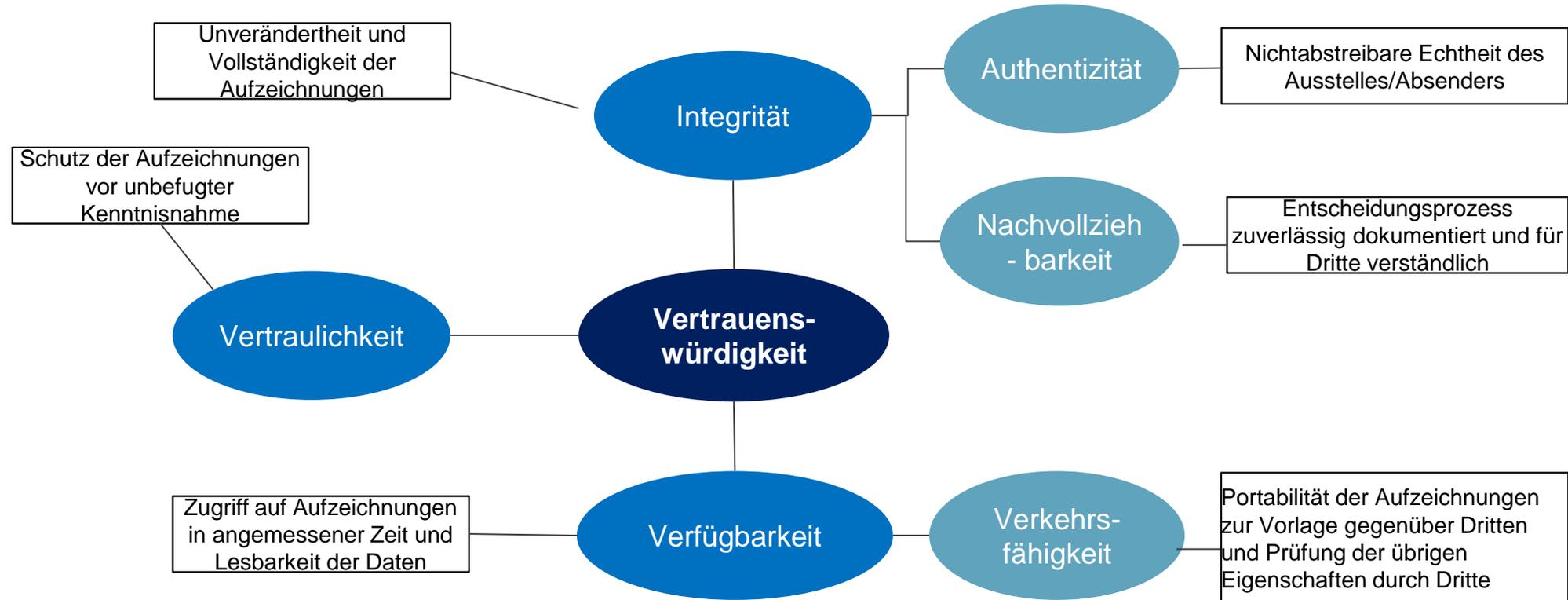
Öffentliche Stellen führen den Beweis durch Akten, einzelne Dokumente sind also regelmäßig nicht ausreichend, gleichzeitig ist Einhaltung TR-RESISCAN und TR-ESOR nachzuweisen. (§ 99 VwGO, OVG Greifswald, Urteile VG Wiesbaden)



Für **ersetzend gescannte** Dokumente gilt:

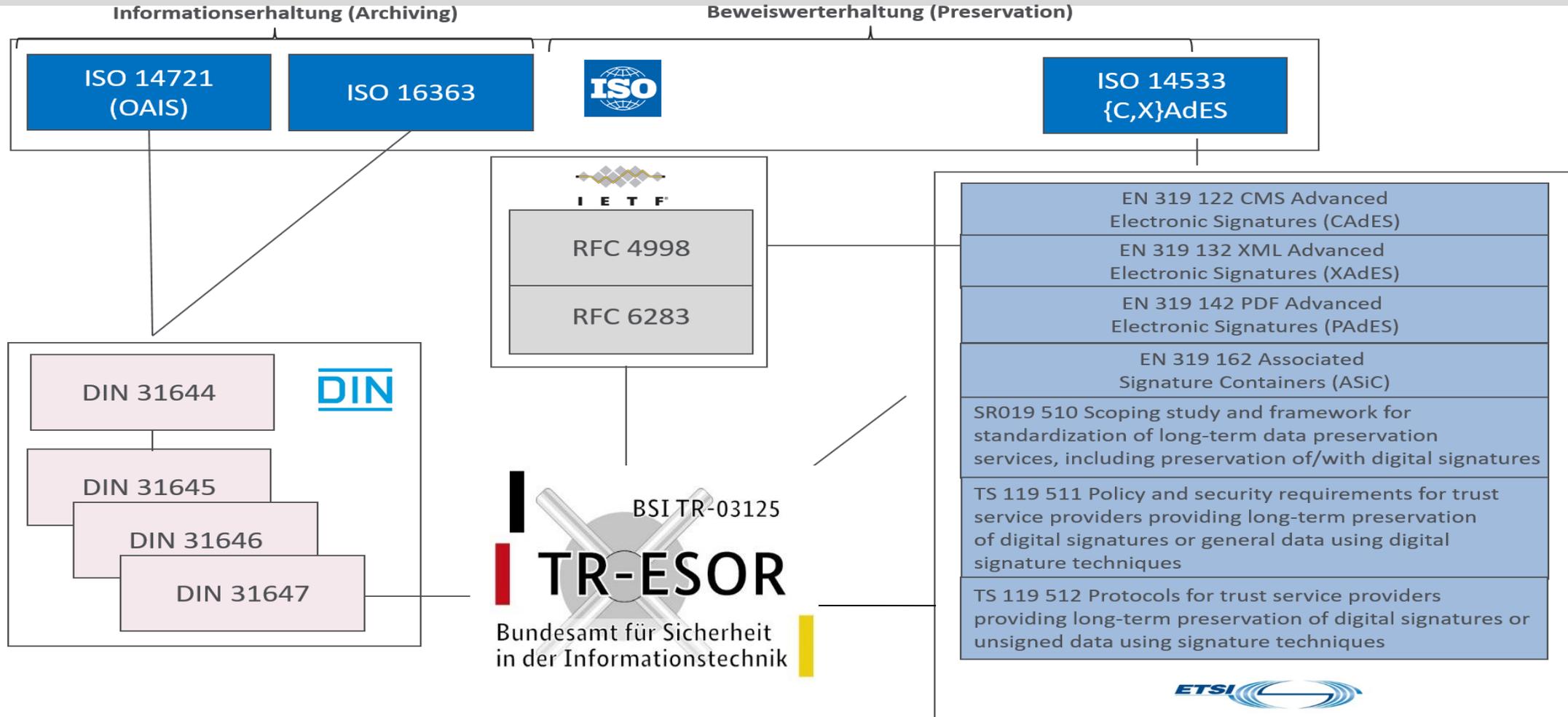
- Behörden (§371b):
Scan nach Stand der Technik (TR-RESISCAN) und QESignatur = Vermutung für Echtheit
Scan nach Stand der Technik TR-RESISCAN und QESiegel = Anscheinsbeweis
- Unternehmen: Scan nach TR-RESISCAN und QES/QESI = Anscheinsbeweis (Vgl. Simulationsstudie Roßnagel, Nebel 2015)

Anforderungen an digitale Nachweise



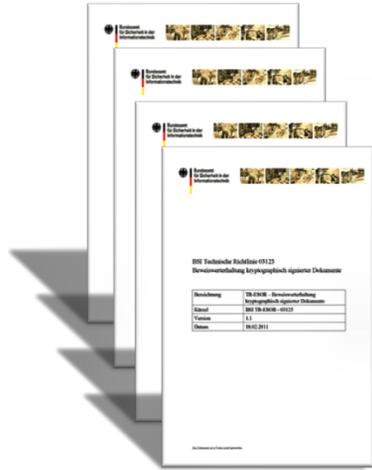
Gewährleistung durch definierte Prozesse, Verantwortlichkeiten, Ablagestrukturen, IT (Records Management acc. ISO 303xx & ISO 15489)

Stand der Technik zur Bewahrung und Archivierung



Records Management gem. z.B. ISO 15489:2016, ISO-30300/30301 etc.

TR-ESOR ist Stand der Technik für Bewahrungsprodukte (qualif.) Bewahrungsdienste



TR-ESOR v1.2.2
TR-ESOR v1.3

TR-ESOR Hauptdokument

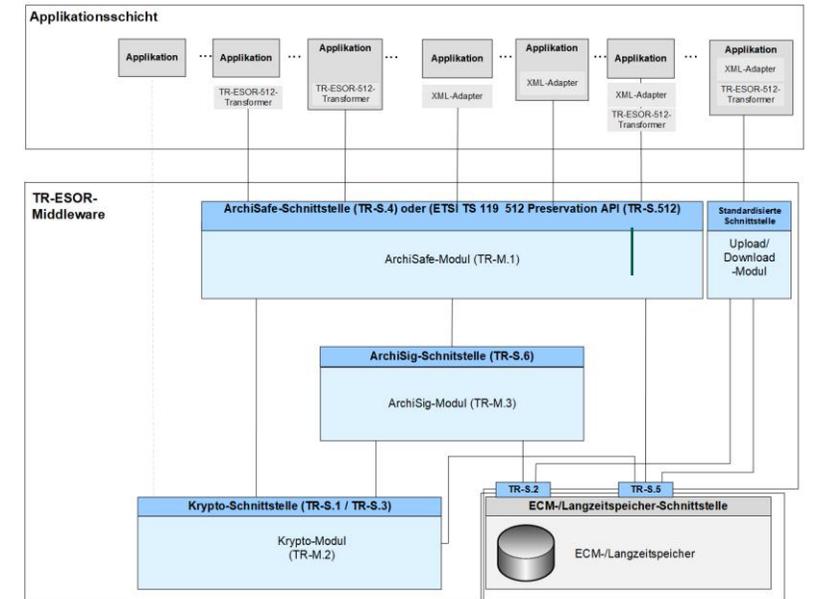
- TR-ESOR-M.1 ArchiSafe Modul
- TR-ESOR-M.2 Krypto Modul
- TR-ESOR-M.3 ArchiSig Modul

- TR-ESOR-F Formate
- TR-ESOR-E Konkretisierung d. Schnittstellen auf Basis des eCard-API Frameworks
- TR-ESOR-VR Verifikationsreport für ausgewählte Datenstrukturen
- TR-ESOR-ERS Profilierung der Evidence Records auf Basis von RFC 4998 und RFC 6283

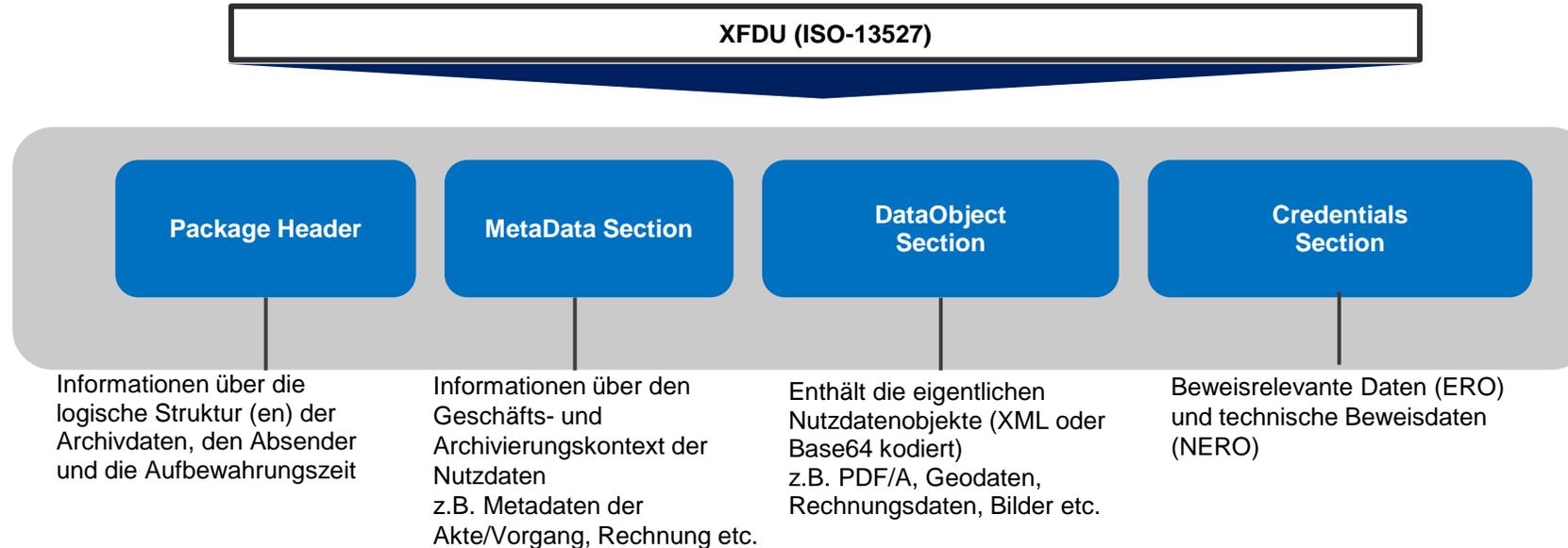
Neu in v1.3

- TR-ESOR-C.1
- TR-ESOR-C.2
- Testtools (Evidence Record, XAIP, S.4 (S.512 in Planung))

- AIP-Container
 - Logisches (X-)AIP
 - **ASiC-E**-Profilierung auf Basis von ETSI EN 319 162 in **TR-ESOR** aufgenommen
 - Leichtere Aufnahme großer Datenmengen
- Anpassungen auf eIDAS/ETSI
 - **Preservation Protokoll** nach ETSI TS 119 512 **S.512** als weitere obere Schnittstelle zwecks europaweite Interoperabilität in **TR-ESOR** aufgenommen, technisch abbildbar auf die TR-ESOR-Schnittstelle TR-S.4
 - Archivinformationspaket **(L)XAIP** und Beweisdatenformat **Evidence Record** in **ETSI TS 119 512** aufgenommen
 - Erleichterung Integration in Bewahrungsdienst durch TR-ESOR APP, PEP, Profile & Assessment Handbücher
- Zukunftsfähigkeit
 - Aufnahme Hashwerte damit DLT-Kryptostabilität via TR-ESOR möglich

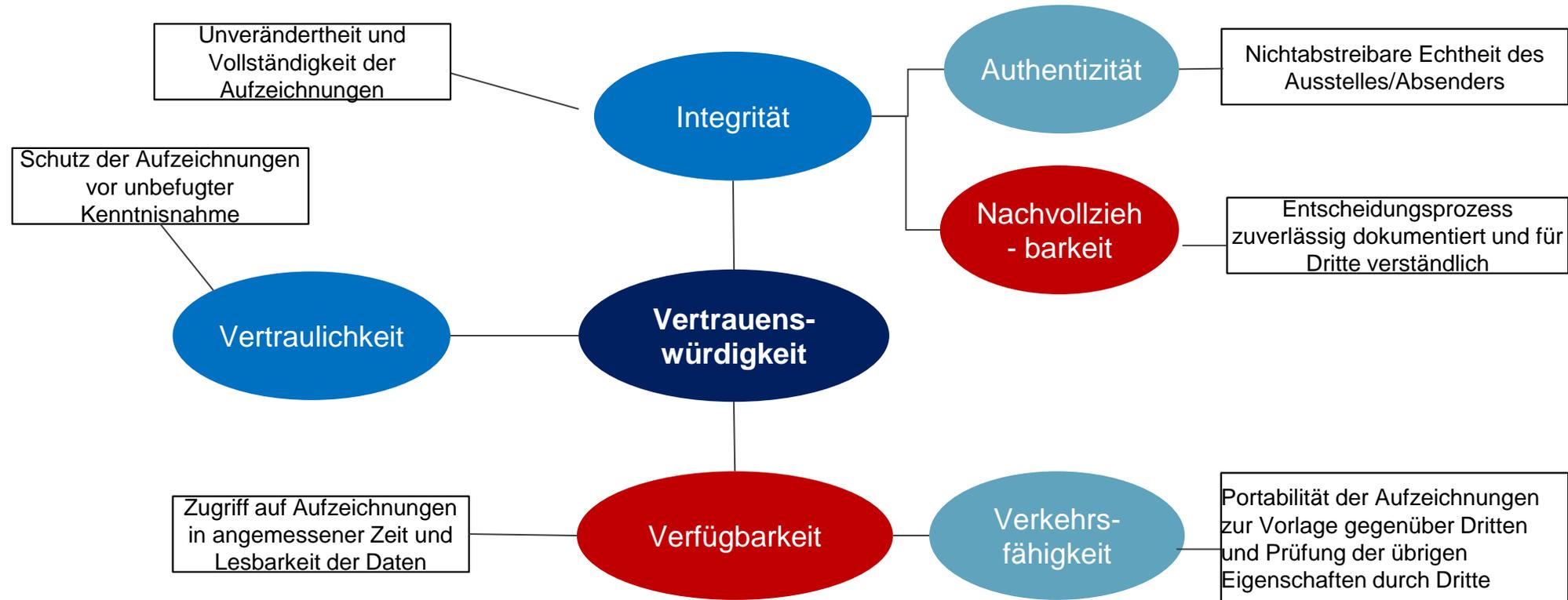


Selbsttragende Archivinformationspakete ermöglichen langfristige Bewahrung & Archivierung



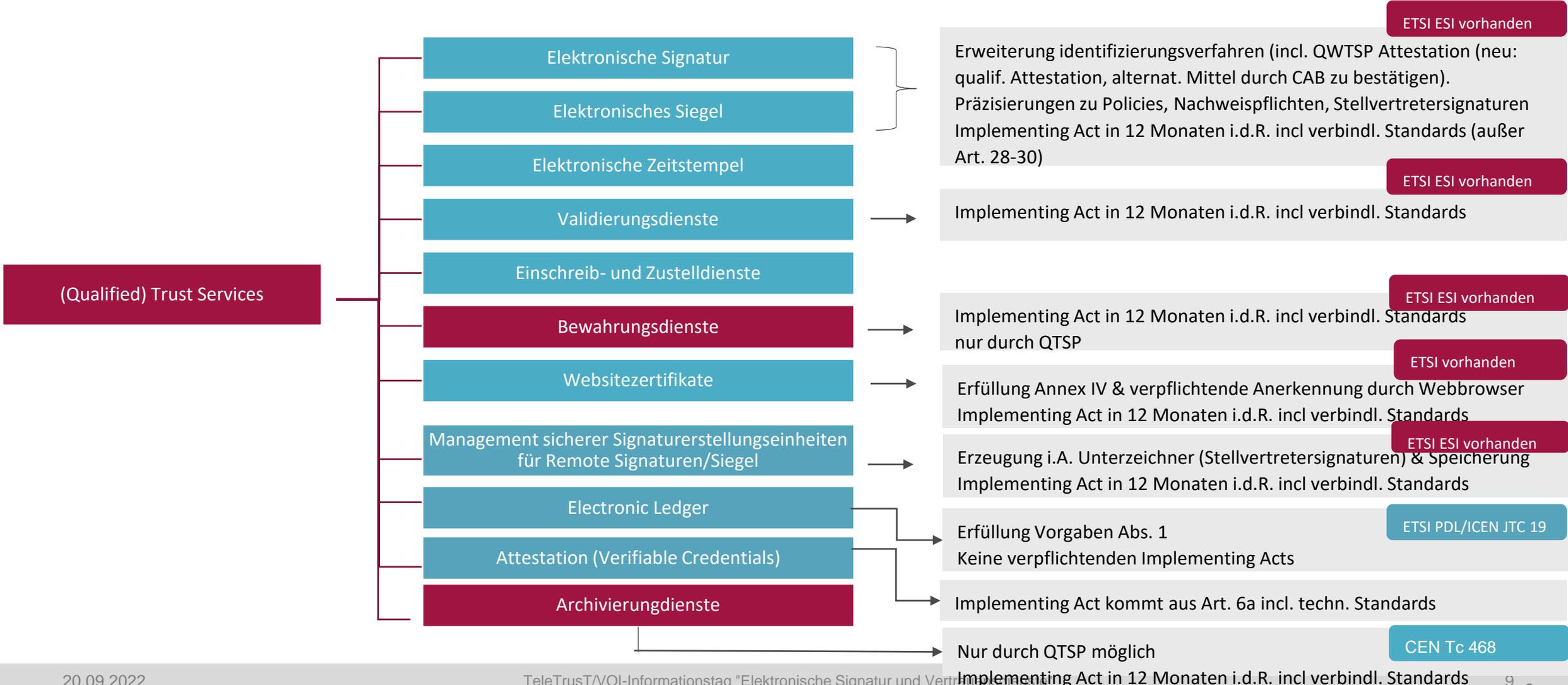
- **3 Ausprägungen gem. Anhang F der TR-ESOR**
 - **Physisches XAIP**
 - **Logisches XAIP**
 - **ASiC-AIP in Arbeit (beruhend auf ASiC-E nach ETSI EN 319 162, inkludiert logisches XAIP)**
- **Versionierung möglich und damit flexibles „Anwachsen“ im Lebenszyklus**
- **Individueller Schutz der gespeicherten Daten durch Protected Pointer möglich**
- **Vollständig selbsttragend, mit Ablage der technischen Beweisdaten (Evidence Records) im Container**

Bewahrung erfüllt nur einen Teil der Anforderungen an digitale Nachweise – Archivierung den anderen.



Gewährleistung durch definierte Prozesse, Verantwortlichkeiten, Ablagestrukturen, IT (Records Management acc. ISO 303xx & ISO 15489)

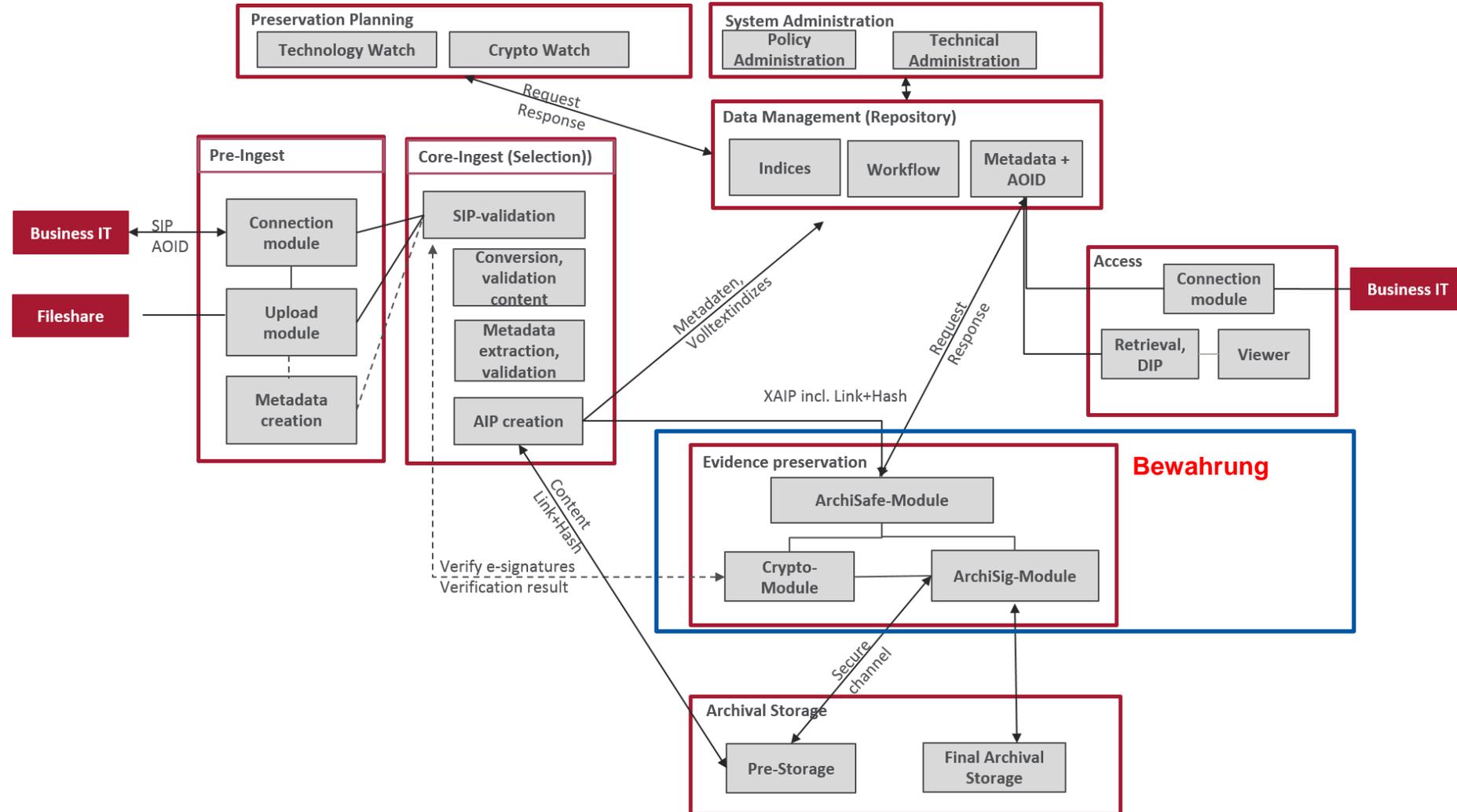
eIDAS 2.0 unterstützt vollständige vertrauenswürdige Langzeitarchiv(vertrauensdienste)



Ein vertrauenswürdiges Langzeitarchiv integriert Preservation & Archiving.



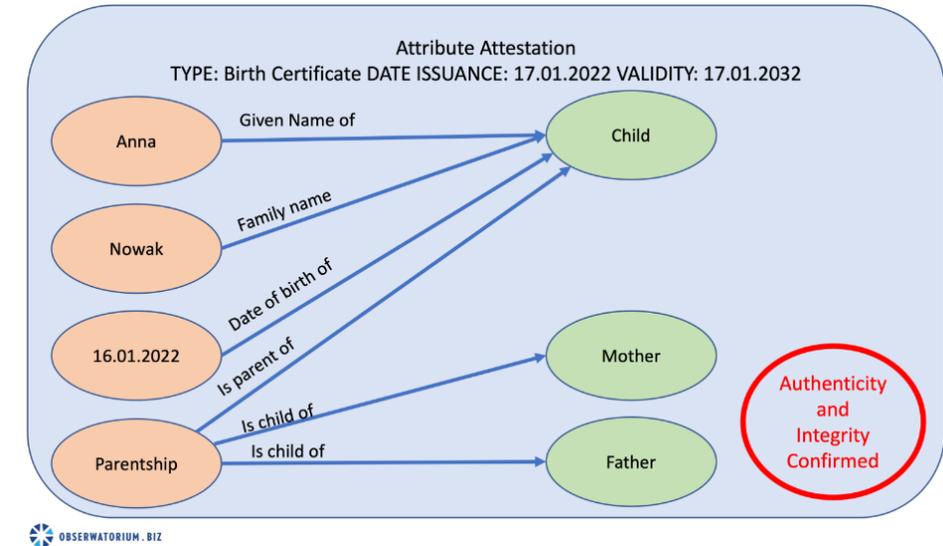
Bundesverband IT-Sicherheit e.V.



Qualified Attestations of Attributes sind nur so viel wert, wie sie langfristig nachgewiesen werden können.

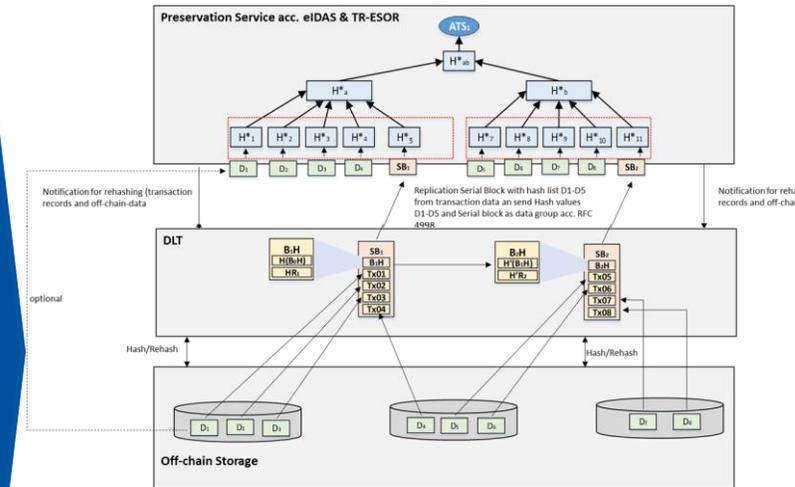
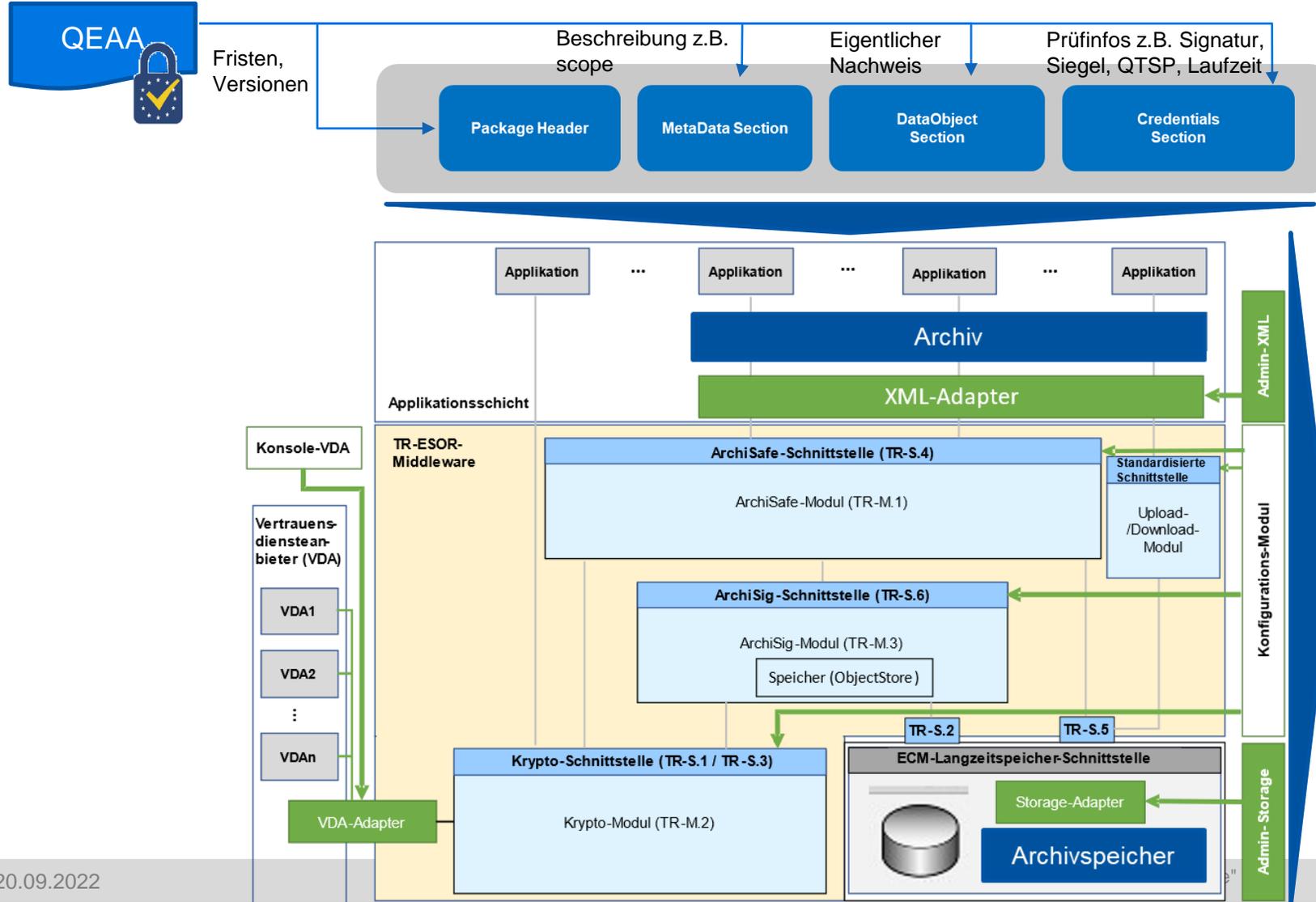
QEAA

- an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;
- a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes
- a set of data unambiguously representing the entity to which the attested attributes is referring;
- the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;
- details of the beginning and end of the attestation's period of validity;
- the attestation identity code, which must be unique for the qualified trust service provider and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of;
- the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- the location where the certificate supporting the advanced electronic signature or advanced electronic seal is available free of charge;
- the information or location of the services that can be used to enquire about the validity status of the qualified attestation.



Geburtsurkunde hat Aufbewahrungsfrist von 110 Jahren bzw. dauernd!

Qualified Attestations of Attributes sind nur so viel wert, wie sie langfristig nachgewiesen werden können.



TeleTrust/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 20.09.2022

Steffen Schwalm, Principal Business Consultant

msg security advisors

Amelia Earhart-Str. 14

D-60549 Frankfurt/Main

Mobile +49 162 280 64 72

E-Mail: steffen.schwalm@msg.group