

Neue Entwicklungen bzgl. Preservation und Archiving im Umfeld von eIDAS v1 und v2 und in Deutschland



Bundesamt
für Sicherheit in der
Informationstechnik

Berlin, 21.01.2025

Dr. Ulrike Korte (BSI)

Inhaltsverzeichnis

Preservation & elektrische Archivierung in eIDAS 1.0 and eIDAS 2.0

1. Preservation (Bewahrung)

2. Elektronische Archivierung

3. Ausblick

ETSI Preservation Standards

auf Basis von eIDAS v1 und eIDAS v2

eIDAS VO

☐ Artikel 34 „Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen“

Ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen **kann nur von qualifizierten Vertrauensdiensteanbietern** erbracht werden, die Verfahren und Technologien verwenden, die es ermöglichen, die **Vertrauenswürdigkeit der qualifizierten elektronischen Signatur über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern**.

☐ Artikel 40 „Validierung und Bewahrung qualifizierter elektronischer Siegel“

Die Artikel 32, 33 und 34 gelten **sinngemäß** für die Validierung und Bewahrung qualifizierter elektronischer Siegel.

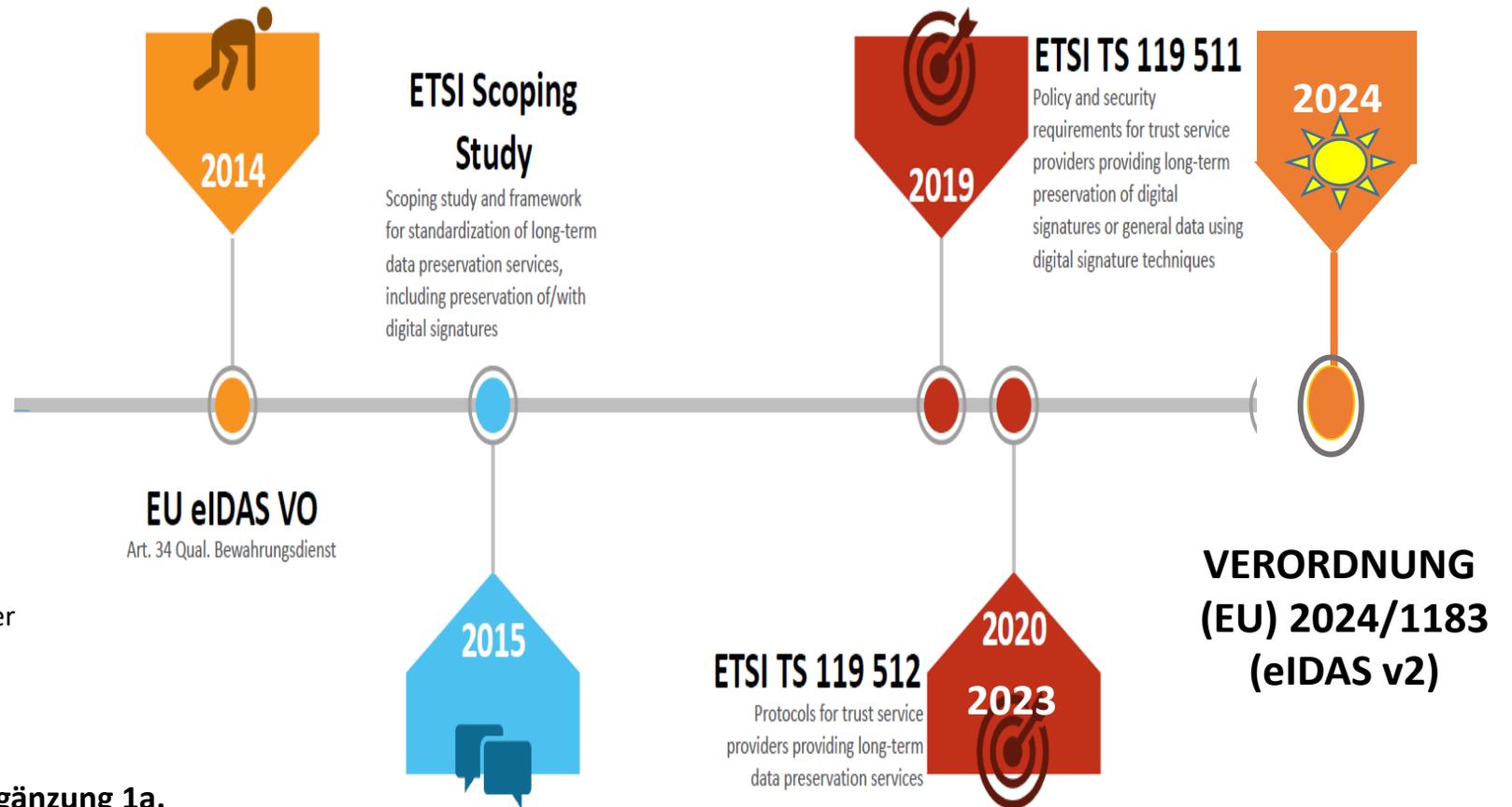
eIDAS 2.0

☐ Artikel 34 und 40 unverändert bis auf die Ergänzung 1a.

1a. Bei Regelungen für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen, die **den in Absatz 2 genannten Standards, Spezifikationen und Verfahren entsprechen**, wird **davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen**.“

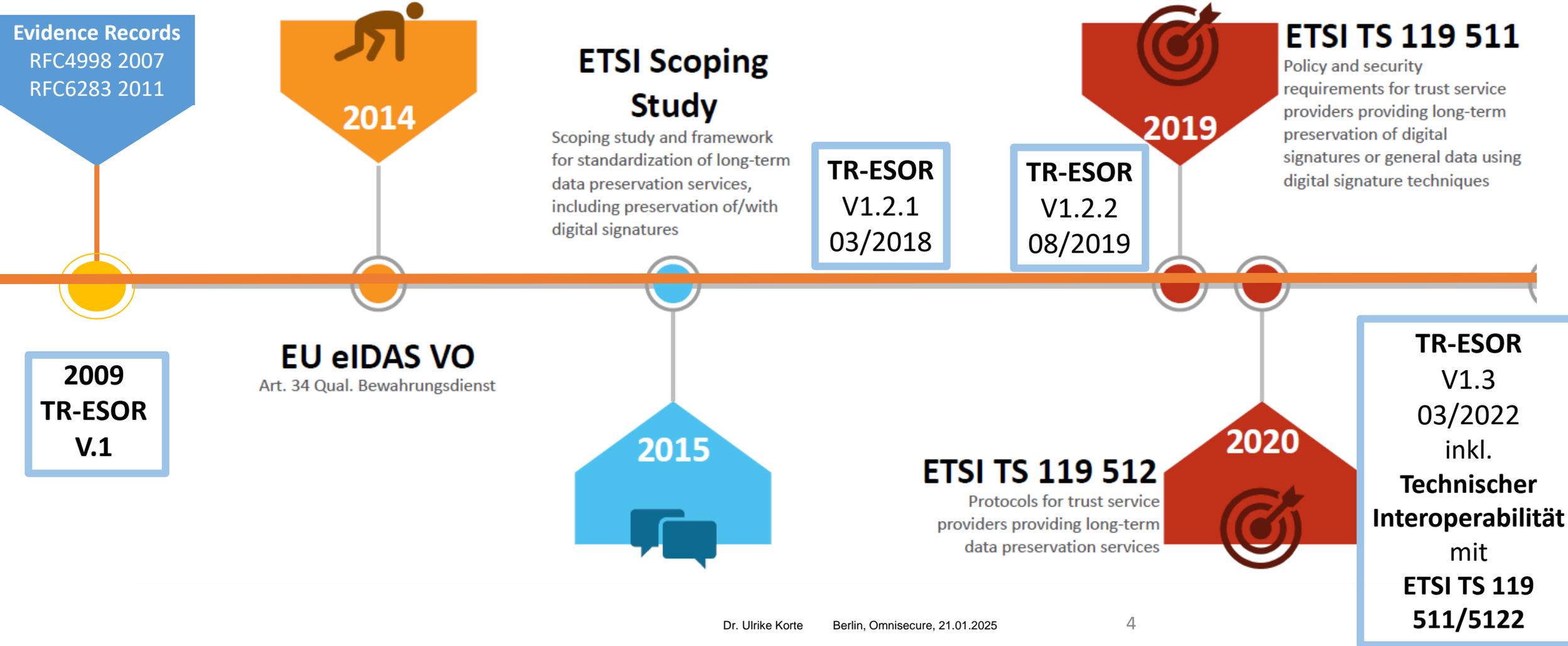
und die Änderung des **Punktes 2**.

2. Bis zum 21. Mai 2025 erstellt die Kommission im Wege von **Durchführungsrechtsakten** eine **Liste von Referenzstandards** und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen fest.



Stand Preservation in Deutschland

BSI TR 03125 TR-ESOR harmonisiert mit ETSI TS 119 511 + ETSI TS 119 51



Technische Interoperabilität auf Basis von ETSI TS 119 512/TR-ESOR

Umfang und Funktionen

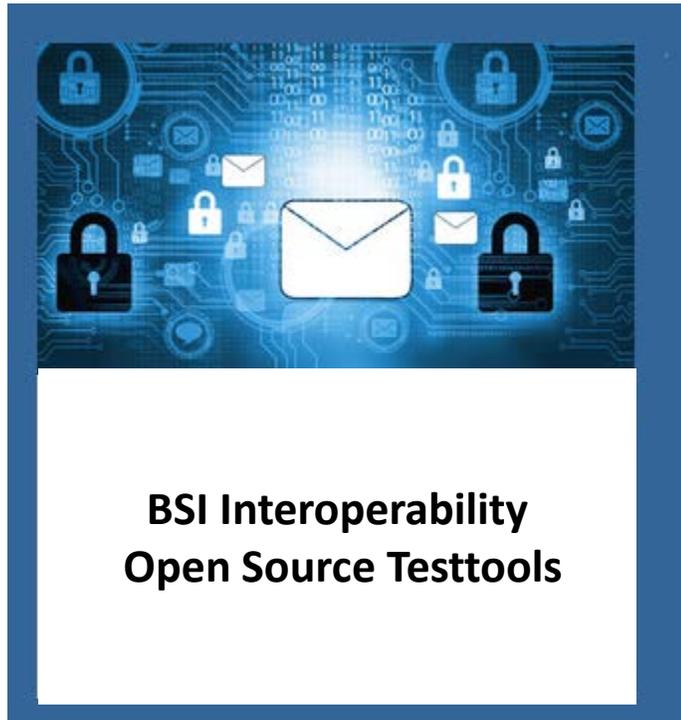
- Unterstützung für drei unterschiedlichen Informationscontainerformate:
 - **XAIP** – XML-basiertes Archiving Information Package *)
 - **LXAIP** – ein logisches XAIP *)
 - **ASiC-ERS** – ein ETSI EN 319 162 basiertes AIP (ein ZIP-Container) *)
- Unterstützung für Preservation Evidence Format:
 - Evidence Record gemäß RFC4998 *)
 - Evidence Record gemäß RFC6283 *)
- Unterstützung für zwei unterschiedlichen Eingangsschnittstellen:
 - **TR-S.4** – die TR-ESOR-native Schnittstelle *)
 - **TR-S.512** – die Schnittstelle gem. ETSI TS 119 512 *)
- BSI Open Source Testtools für die vorgenannten Komponenten und die 2 Eingangsschnittstellen

TR-S.4	TR-S.512	Beschreibung
ArchiveSubmission	PreservePO **)	Ablage der Daten.
ArchiveUpdate	UpdatePOC	Update der abgelegten Daten.
ArchiveRetrieval	RetrievePO **)	Herausgabe der aufbewahrten Daten.
ArchiveEvidence	RetrievePO	Herausgabe der Beweisdaten.
ArchiveDelete	DeletePO **)	Löschung der Daten und Beweisdaten.
ArchiveData	Search	Herausgabe bestimmter Daten (speziell Teile eines Containers).
Verify	ValidateEvidence	Validierung der Beweisdaten.
RetrieveInfo	RetrieveInfo	Herausgabe der Informationen zum Aufbewahrungsdienst.
ArchiveTrace	RetrieveTrace	Herausgabe der Tracing-Information zu einem bestimmten AIP.

*) sowohl Bestandteil von ETSI TS 119 512 als auch von BSI TR 03125 TR-ESOR

**) logisch-funktional auch in CEN 468 ..elektronische Archivierung.. vorhanden

Interoperabilität unterstützt durch “BSI Open Source Test Tools”



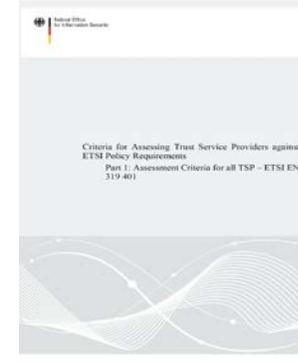
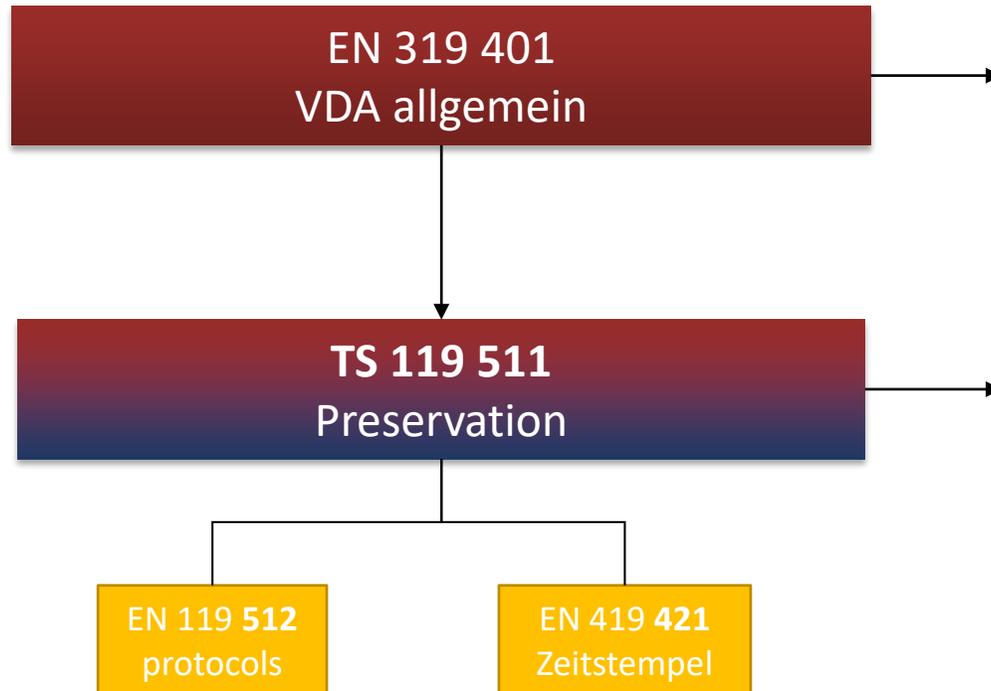
Tool	Focus
Evidence Record Test Tool „ERVerify“	Verification of conformity of Evidence Records to RFC4998/6283 for the purpose of interoperability
ETSI TS119512 TR-ESOR Transformer	Transforms the preservation API interface TR-S.512 from [ETSI TS 119 512] to the TR-ESOR input interface TR-S.4
(L)XAIP Validator: „AIP eIDAS Signature Validator“	Testtool for Validation of (L)XAIP, ASiC, including the signatures, seals and time stamps and Evidence Records contained therein, for the purposes of correctness and interoperability
BSI TR-S.4-TR-S.512-Testbed	TR-ESOR-S.4- and S.512-interface Testbed of the upper TR-ESOR interfaces



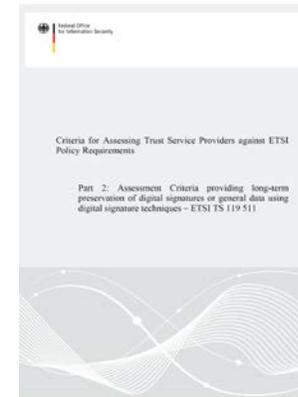
Siehe: <https://github.com/de-bund-bsi-tr-esor>

Erleichterung der Konformitätsbewertung für Bewahrungsdienste

mittels Assessmenthandbücher von BNetzA und BSI



Assessment
Handbuch für ETSI EN
319 401 *1)



Assessment
Handbuch für ETSI TS
119 511 *2)

➡ **Hinweis 1:** Falls ein Bewahrungsdienst **auf ein TR-ESOR (ab V1.2.1) zertifiziertes Produkt aufsetzt**, dann **entfallen** die bereits im Rahmen von TR-ESOR geprüften Assessment- Testschritte

➡ **Hinweis 2:** Die Entwicklung des Assessment-Handbuchs für ETSI TS 119 421 ist in Arbeit

*1) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/Assessment-Handbuch_ETSI_319_401.pdf

*2) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/Assessment-Handbuch_ETSI_319_511.pdf

Inhaltsverzeichnis

Preservation & elektrische Archivierung in eIDAS 1.0 and eIDAS 2.0

1. Preservation (Bewahrung)

2. Elektronische Archivierung

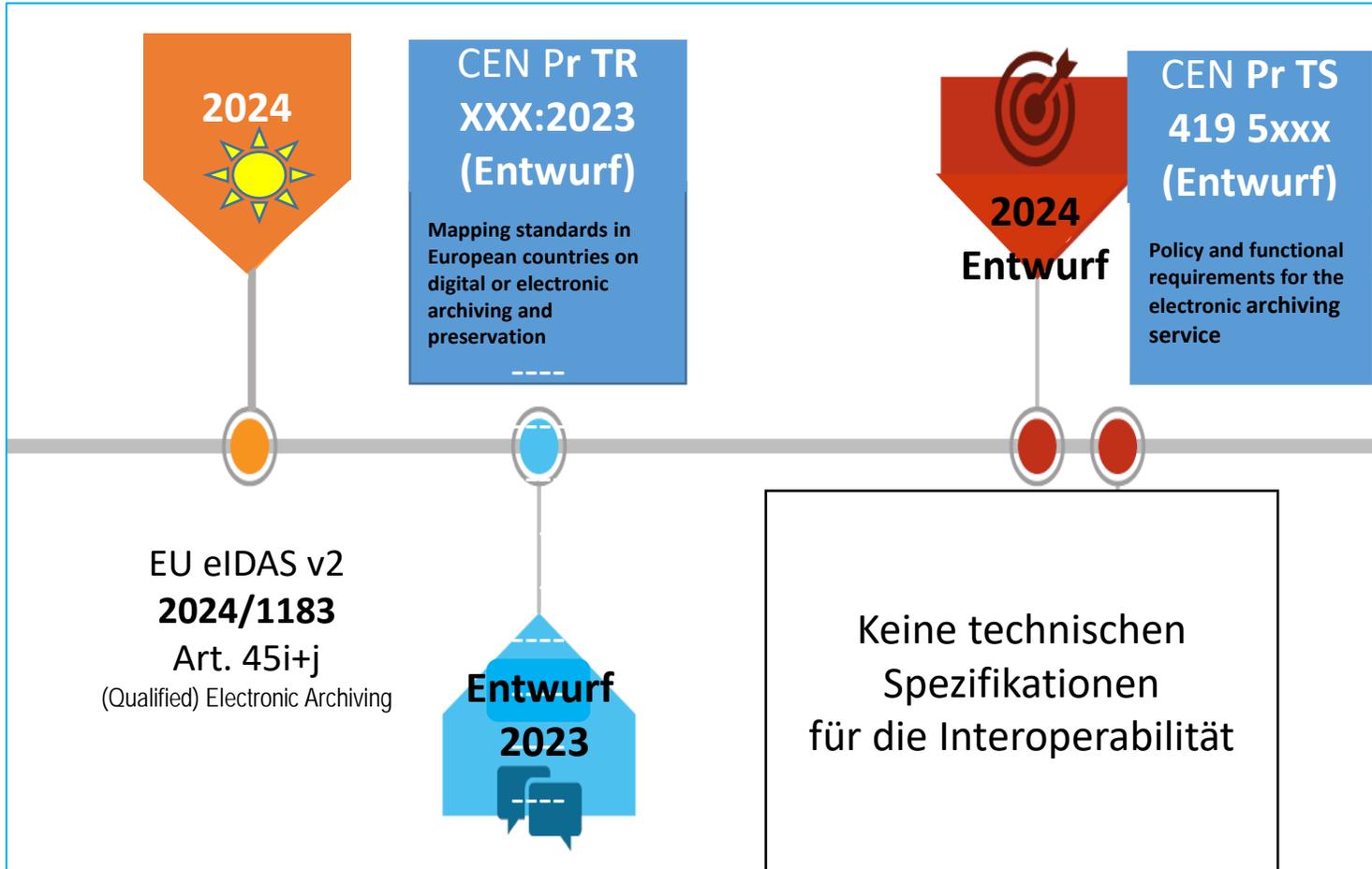
3. Ausblick

Ziel des elektronischen Archivierungsdienstes gemäß eIDAS 2.0

- Elektronische Archivierung‘ ist ein Dienst für die **Entgegennahme**, die **Speicherung**, den **Abruf** und die **Löschung** elektronischer Daten und elektronischer Dokumente, der ihre **Dauerhaftigkeit** und **Lesbarkeit** gewährleistet sowie ihre **Unversehrtheit**, **Vertraulichkeit** und den **Nachweis ihrer Herkunft** während des gesamten Bewahrungszeitraums erhält (eIDAS v2, Artikel 3 (48))
- Sie stellen sicher, dass diese elektronischen Daten und diese elektronischen Dokumente so aufbewahrt werden, dass sie vor **Verlust und Veränderung geschützt** sind, mit **Ausnahme von Änderungen** in Bezug auf das **Medium** oder das **elektronische Format** (eIDAS v2, Artikel 45j)
- Sie ermöglichen es autorisierten vertrauenden Beteiligten, einen **Bericht auf automatisierte Weise** zu erhalten, mit dem bestätigt wird, dass für aus einem qualifizierten elektronischen Archiv abgerufene elektronische Daten und elektronische Dokumente die **Vermutung der Unversehrtheit der Daten** ab **dem Beginn des Bewahrungszeitraums bis zum Zeitpunkt des Abrufs** gilt (eIDAS v2, Artikel 45j)
- Der .. genannte Bericht wird in zuverlässiger und effizienter Weise bereitgestellt und trägt die **qualifizierte elektronische Signatur** oder das qualifizierte elektronische Siegel des Anbieters des qualifizierten elektronischen Archivierungsdienstes.
- eIDAS v2, Artikel 45j 2.:
 - „Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte elektronische Archivierungsdienste fest. Bei qualifizierten elektronischen Archivierungsdiensten, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen für qualifizierte elektronische Archivierungsdienste erfüllen. ...“

Aktuelle Standardisierung „elektronische Archivierung“ in Europa

CEN 468 WG 1: General Concepts for Preservation of digital conservation



Pr TS 419 5xx:2024

Policy and functional requirements for the electronic archiving service

Gegenstand u.a.:

- Individuelle Service-Agreements
- Annahme, Prüfung, Archivieren, Abruf und Löschen der zu archivierenden Meta- und Nutzdaten,
- Integrationsschutz der Datenobjekte und „critical events“
- Anreicherung von Metadaten u. Datenformat-Transformationen
- Reporting, etc.

Noch offen, aktuell nicht Gegenstand dieses Standards:

- Nur logische Funktionalität, **keine technische Spezifikation mit dem Ziel der technischen Interoperabilität**
- keine eigenen digitale Signaturtechniken bis auf Hashing
- keine Spezifikation des Zusammenspiels des elektr. Archivierungsdienstes mit dem Bewahrungsdienst und anderen Vertrauensdiensten
- **Entgegen der Ankündigung in eIDAS v2** aktuell **nicht Gegenstand dieses Standards:**
 - Keine Annahme eingescannter digitalisierter Daten/Dok.
 - keine Unterstützung der **Vertraulichkeit**, etc.

Status:

- **Termin der Veröffentlichung noch offen, da Review noch ausstehend.**
- **Angestrebt:** Aufnahme als Standard für den Durchführungsrechtsakt bzgl. „elektronische Archivierung“,

Unterscheidung Preservation & Archivierung

Anforderungen	Unterstützung durch Preservation	Unterstützung durch Archivierung
Unterstützung der Operationen Entgegennahme, Speicherung, Abruf und Löschung elektronischer Daten und Dokumente	ja	ja
Konservierung der el. Daten und Dokumente mittels Hash-Algorithmen	Ja	ja
Metadatenanreicherung und Format Transformationen	Eingeschränkt, durch Bildung einer neuen Version per „Update“-Fkt.	ja
Digitaler Signaturtechniken (ST) <ul style="list-style-type: none"> • Erzeugung bzw. Validierung der digitalen Signaturtechniken • Erstellung Existenzbeweise von Daten mittels (ST), • Bewahrung der Beweisdaten (Preservation Evidences) 	ja	Nein
Authentizität auf Basis der digitalen Signaturtechniken	ja	nein
Verkehrsfähigkeit unter Beibehaltung der Integrität und Authentizität des Informations-Conainers	ja	nein
Technische Interoperabilität mit Tool-basierten Testmöglichkeiten	ja	nein
Aufnahme eingescannter Dokumente bzw. Daten	Ja, im Zusammenspiel mit TR 03138 RESISCAN	nein, aktuell zurückgestellt
Vertraulichkeit: Verschlüsselung der el. Dokumente/Daten	Ja, falls Integration eines TR-ESOR-ENC-Produktes (neu) , siehe die folgenden 2 Vorträge	nein, aktuell zurückgestellt

Inhaltsverzeichnis

Preservation & elektrische Archivierung in eIDAS 1.0 and eIDAS 2.0

1. Preservation (Bewahrung)

2. Elektronische Archivierung

3. Ausblick

ToDo: Ausarbeitung der Kombinationsmöglichkeiten für Preservation & Archivierung

Achtung: Die Bewahrung von elektronischen Signaturen und Siegeln ist **außerhalb des „Scopes“ eines Archivierungsdienstes**. Dazu sind entsprechende Interaktionen zwischen den beiden Vertrauensdiensten erforderlich.

Variante	Dienste bzw. deren Verkettung	Besitzer des Langzeitspeichers	Policy
1.	Archivierungsdienst	Archivierungsdienst	Archivdienst-Eigenschaften: <ul style="list-style-type: none"> • Archivierung, keine digitale Signaturtechnik, aber Metadatenanreicherung und Format Transformation • Konservierung des eingereichten Archivdatenobjekts von der Einreichung bis zur Löschung (Integrität) • Keine Verkehrsfähigkeit unter Beibehaltung der Integrität und Authentizität des eingereichten Archivdatenobjektes
2.	Bewahrungsdienst	Bewahrungsdienst	Bewahrungsdienst-Eigenschaften: <ul style="list-style-type: none"> • langfristige, beweiswerterhaltende Bewahrung digitaler Signaturen oder allgemeiner Daten unter Verwendung digitaler Signaturtechniken (Signaturen, Zeitstempel, Evidence Records) • Erhalt der Verifizierbarkeit während der Aufbewahrungsperiode gemäß [ETSI EN 319 102-1, Kap. 5.6]; • Erzeugung von Existenzbeweisen mit digitalen Signaturtechniken • Bewahrung der Verkehrsfähigkeit der eingereichten plattform- und herstellerunabhängigen Archivdatenobjekte
3a.	Archivierungsdienst → Bewahrungsdienst	Bewahrungsdienst	Archivierungsdienst ruft auf Bewahrungsdienst <ul style="list-style-type: none"> • Vorstehende Archivierungsdienste-Eigenschaften, ergänzt um vorstehende Bewahrungsdienste-Eigenschaften und • der Archivierungsdienst fungiert hier als AIP-Erzeuger, z.B. XAIP Adapter [TR-ESOR].
3b.	Bewahrungsdienst → Archivierungsdienst	Archivierungsdienst als ECM Long-term- storage	Bewahrungsdienst ruft auf Archivierungsdienst <ul style="list-style-type: none"> • Vorstehende Bewahrungsdienste-Eigenschaften, ergänzt um vorstehende Archivierungsdienste-Eigenschaften und • der Archivierungsdienst fungiert hier zusätzlich als ECM-Langzeit-Speicher.
3c.	Archivierungsdienst → Bewahrungsdienst → Archivierungsdienst	Archivierungsdienst	Archivierungsdienst ruft auf Bewahrungsdienst (Middleware) ruft auf Archivierungsdienst <ul style="list-style-type: none"> • vorstehende Archivierungsdienste-Eigenschaften und • Der Archivierungsdienst fungiert als AIP- Erzeuger • und ergänzt um die vorstehenden Bewahrungsdienste-Eigenschaften • und ergänzt um den Archivierungsdienst in der Funktion als „ECM-Langzeit-Speicher“

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Ulrike Korte

E-Mail: Ulrike.Korte@bsi.bund.de

Telephone: +49 (0) 228 9582 5842

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 87

53175 Bonn

www.bsi.bund.de

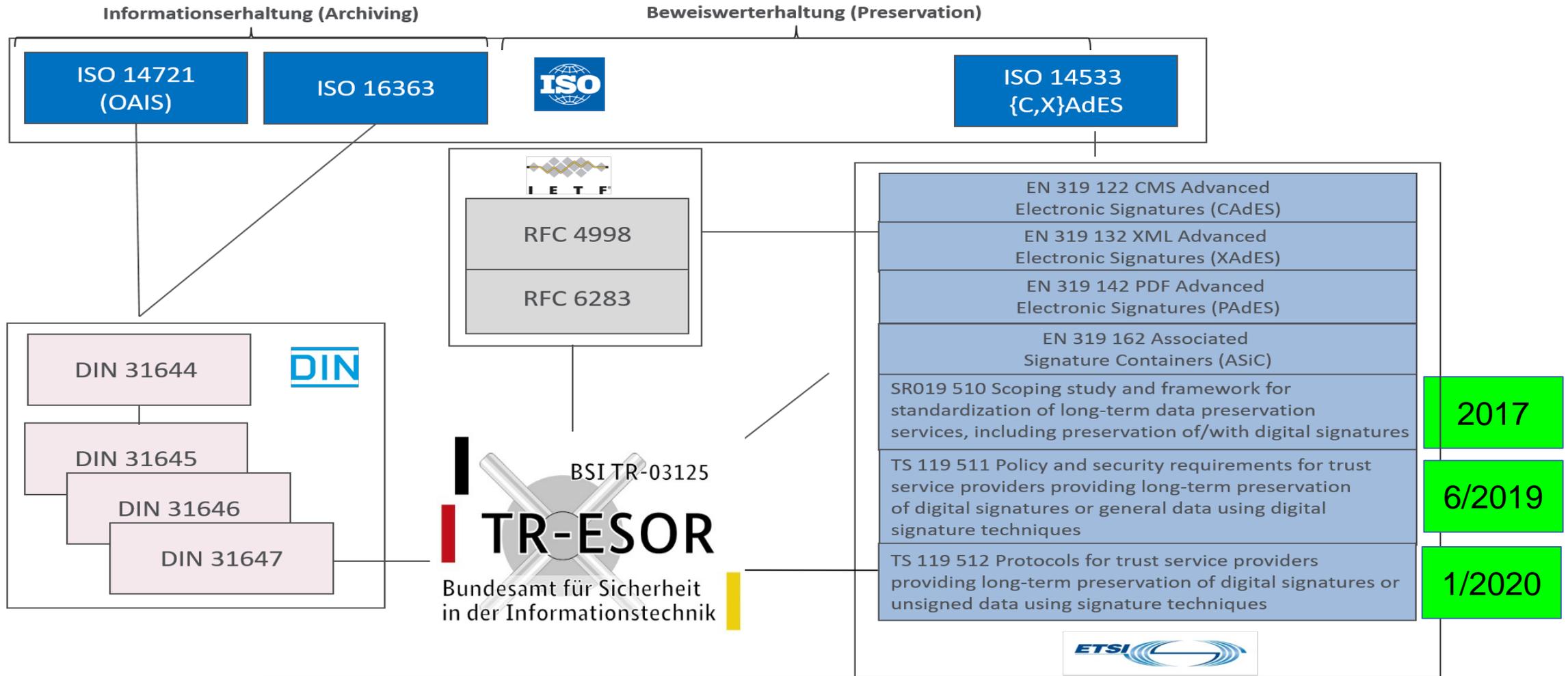


Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:



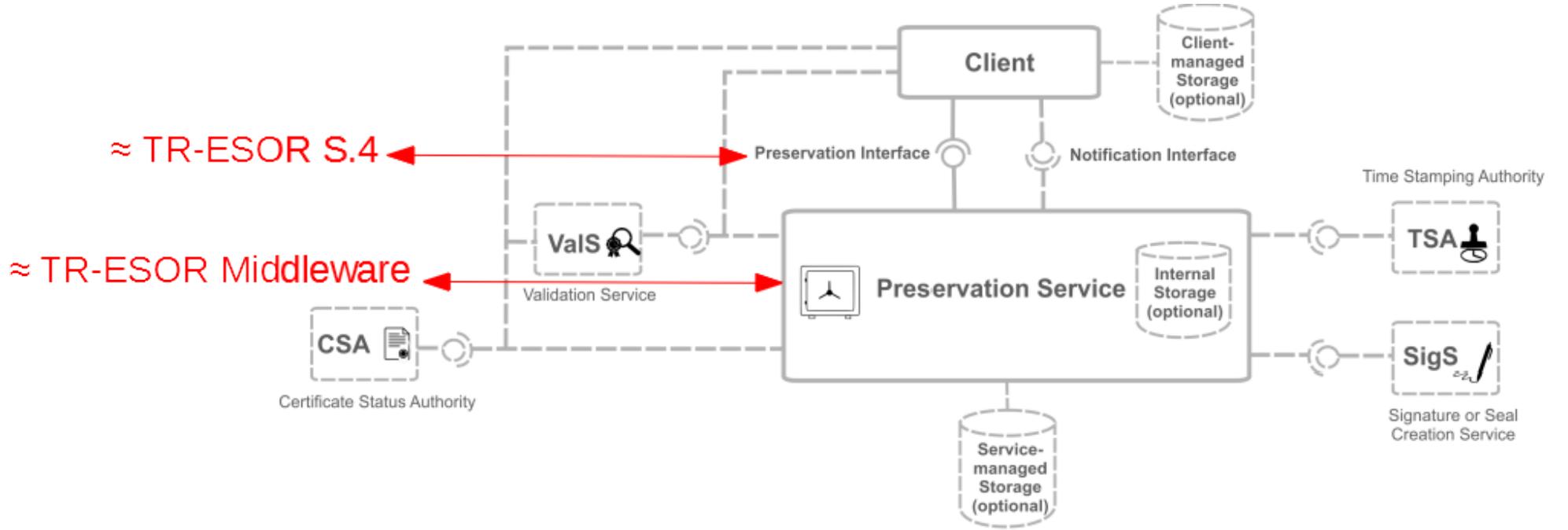
BSI TR 03125 TR-ESOR ab V1.2.1 = Stand der Technik bzgl. beweiswerterhaltenden Langzeitspeicherung zum langfristigen Nachweis digitaler Transaktionen



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

Preservation Architektur

gemäß ETSI TS119 511 / 512, harmonisiert mit **TR-ESOR**



Legend:

○ — offered Interface
— (used Interface

software component / service
storage

optional communication
optional component / service
optional storage