(Qualifizierte) Bewahrungsdienste und TR-ESOR Produkte
Zusammenspiel bei der Zertifzierung von Produkt- und Service

eIDAS-Summit, 26.10.2020

Dr. Ulrike Korte, Dr. Christoph Sutter, Steffen Schwalm

Bundesamt für Sicherheit in der Informationstechnik

.msg

TÜViT®

TÜV NORD GROUP

Agenda

1. Neue Anforderungen an Produkte zur Beweiswerterhaltung auf Basis TR-ESOR V1.3
2. Erfahrungsbericht aus der Anwendung der Assessment-Handbücher für Bewahrungsdienste mit TR-ESOR
3. Neue Assessment-Handbücher zur Zertifizierung von (qualifizierten) Bewahrungsdienste gemäß eIDAS/ETSI
4. Zusammenspiel der Zertifizierung von Bewahrungsdiensten (ETSI TS 119 511) und TR-ESOR-Produkten

EU-Verordnung elektronische Vertrauensdienste (eIDAS-VO)

Verbindliche Rechtsgrundlage EU-weit in Kraft seit September 2014, in den Mitgliedstaaten anwendbar seit : Juli 2016

- Einheitliche Maßgaben für sichere elektronische Geschäftsprozesse **in Europa**
- Vorgaben zur **rechtlichen Bedeutung** und **technischen Umsetzung**
- Rechtl. Detaillierung in Durchführungsakten
- Technisch: ETSI/CEN- Normen, auf die die Durchführungsakte referenzieren

- Aufsicht und Prüfung qualifizierter Vertrauensdienste (VD) durch **europäische Aufsichtsbehörden** und **Konformitätsbewertungsstellen (je EU-Land)** und Eintragung der Vertrauensdiensteanbieter (VDA) in **Vertrauensliste (TL)**

- Behörden müssen Signaturen und Siegel in bestimmten Formaten (siehe DRA 2015/1506/EU) akzeptieren und verarbeiten können.
  - Abweichung von vorgeschriebenen ETSI-Formaten möglich bei kostenfreier Bereitstellung eines Prüftools
- Leitlinie für digitale Signatur-/Siegel-, Zeitstempel und Beweisdaten(Evidence Record) - Formate
  - https://www.bundesnetzagentur.de/EVD/SharedDocuments/Downloads/QES/BSI_TR_03125.pdf und https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/tr-03125.html#doc6617308bodyText6)

Kernthemen eIDAS

Neue VDs bzgl. (Q)ES, (Q)ZS, (Q) Siegel

- Erstellen, Validieren von (Q)ES, (Q)ZS, (Q) Siegel
- Siegel und Organisationszertifikate möglich
- Produkte qual. VDA europaweit anzuerkennen

Bewahrungsdienste

- **Beweiswerterhalt der QES, QSiegel,**
- **gem. ETSI aber auch Bewahrung allg. Daten mittels Signaturtechniken (z.B. mit Evidence Records gemäß RFC4998)**

Zustelldienste

- Nachweisbare Zustellung elektronischer Einschreiben europaweit

Authentisierung

Bundesamt für Sicherheit in der Informationstechnik

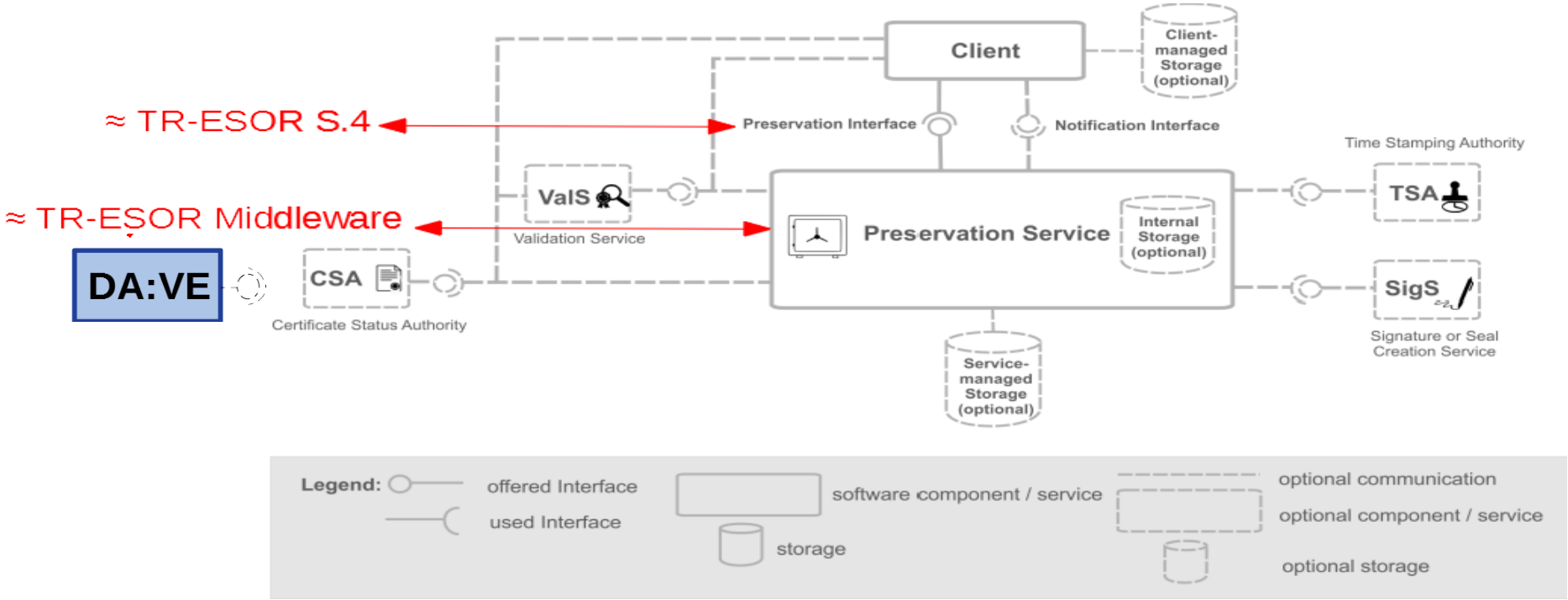
Neue ETSI - Preservation – Standards (unter Mitwirkung des BSI)

- **2017: ETSI SR 119 510:** "Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures"
  - PL: Dr. Andrea Röck, France

- **2019: ETSI TS 119 511:** "Policy & Security Requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques"
  - PL: Dr. Andrea Röck, France

- **2020: ETSI TS 119 512:** "Protocols for trust service providers providing long-term data preservation services"
  - PL: Dr. Detlef Hühnlein, Germany

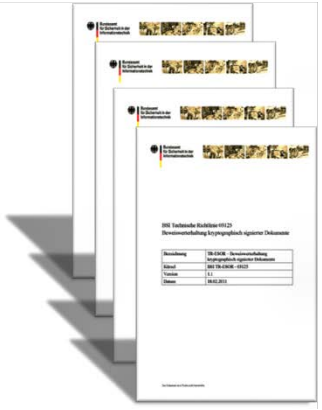
Die TR-ESOR-Architektur ist in der Architektur eines Bewahrungsdienstes nach ETSI TS 119 511/512 auf Basis von eIDAS enthalten



Bundesamt für Sicherheit in der Informationstechnik

TR-ESOR v1.2.2 liegt veröffentlicht vor,

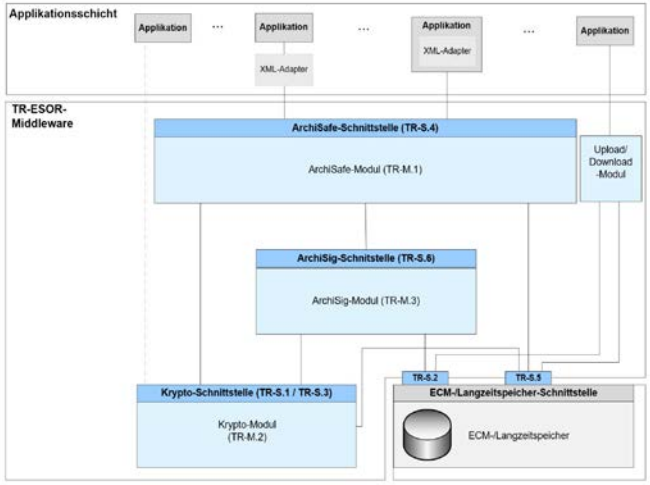
basierend auf der eIDAS-VO und den ETSI Preservation Standards



TR-ESOR Hauptdokument

- TR-ESOR-M.1 ArchiSafe Modul
- TR-ESOR-M.2 Krypto Modul
- TR-ESOR-M.3 ArchiSig Modul
- (TR-ESOR-B Bundesbehördenprofil)
- 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
- (TR-ESOR-XBDP Profilierung des XAIP)

mit **XBARCH, XDOMEA und PREMIS**

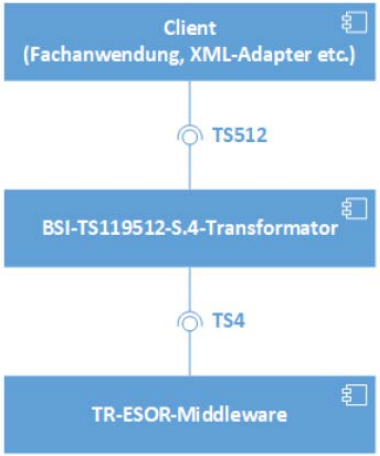


TR-ESOR v1.2.2 (https://www.bsi.bund.de/tr-esor)

Neu:

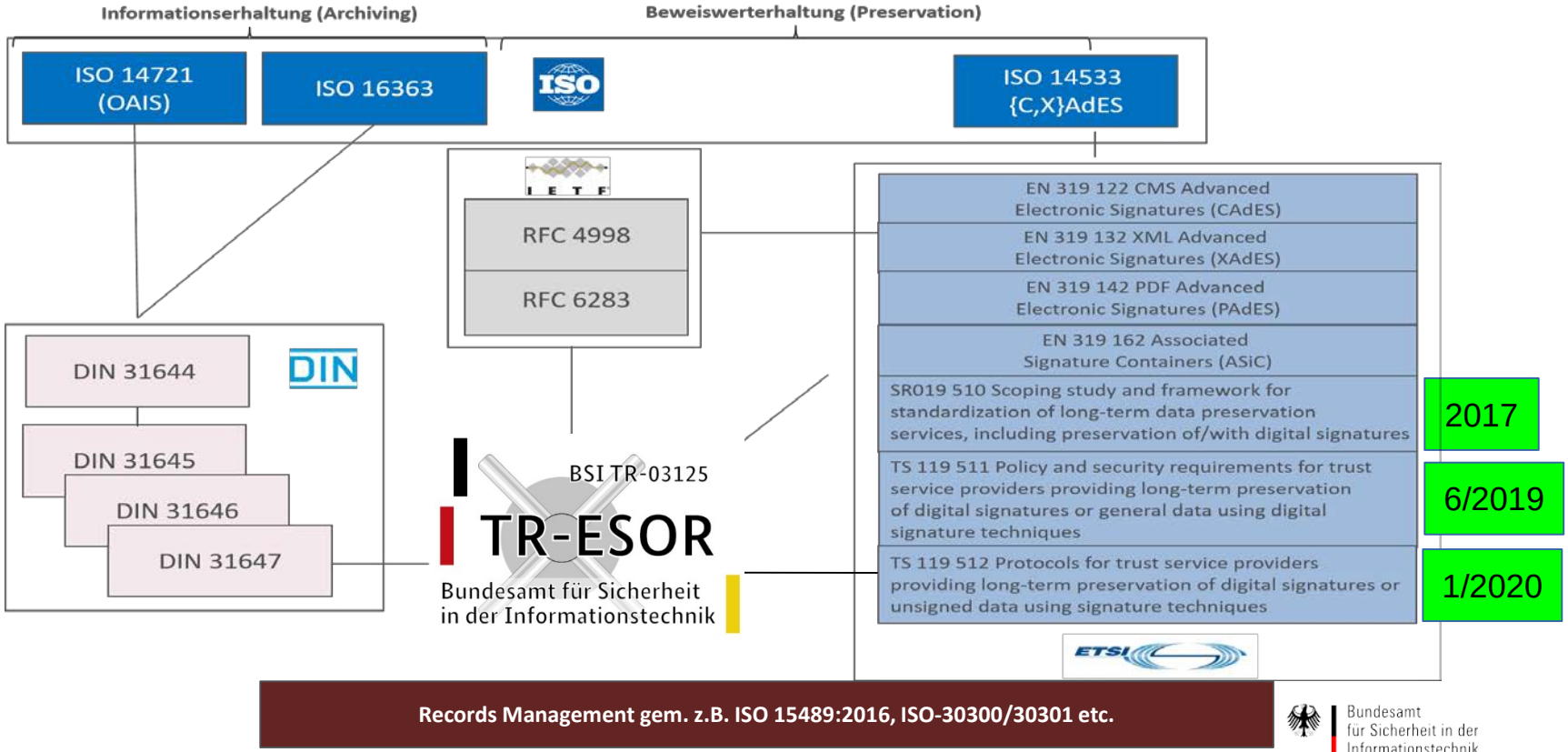
- Archivinformationspaket (AIP) in **TR-ESOR**
  - XAIP, Logisches (L)XAIP - Leichtere Aufnahme großer Datenmengen
  - ETSI ASiC-E -Profilierung auf Basis von ETSI EN 319 162
- Anpassungen auf eIDAS/ETSI
  - Preservation Protokoll nach ETSI TS 119 512 als weitere obere Schnittstelle zwecks europaweite Interoperabilität 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
  - Englische Übersetzung

BSI stellte Open-Source-Werkzeug „ETSI TS 119512 TR-ESOR Transformator“ bereit



Das **Open-Source-Werkzeug „ETSI TS 119512 TR-ESOR Transformator“** ermöglicht Bewahrungsdiensten gemäß eIDAS, hereinkommende Nachrichten im Schnittstellenformat ETSI TS 119 512 (V1.1.1) auf das TR-ESOR S4 - Nachrichtenformat zu transformieren. Diese können anschließend an ein angeschlossenes TR-ESOR-System weitergeleitet werden, ohne das vorher Änderungen an diesem System vorgenommen werden müssen.

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



2020: Aktuelle Entwicklung BSI TR 03125 TR-ESOR V1.3
Schwerpunkt: Ausbau der technischen Interoperabilität

BSI TR-03125
TR-ESOR
Bundesamt für Sicherheit in der Informationstechnik

- TR-ESOR-Interoperabilitäts-Testumgebung auf Basis von RFC4998, ETSI TS 119 512, TR-ESOR
  - Evidence Record Testtool „BSI ErVerifyTool", gemäß **[RFC4998],** **[ETSI TS 119 512, A.3.1]** und **[TR-ESOR]**, (siehe https://github.com/de-bund-bsi-tr-esor/ERVerifyTool)
  - TR-ESOR-ETSITS119512-Transformator (siehe https://github.com/de-bund-bsi-tr-esor/tresor-ETSITS119512-transformator)
  - „*X*AIP-eIDAS-Signatur-Validator" gemäß **[TR-ESOR-F]** und **[ETSI TS 119 512 A.3.2]** (in Arbeit)
  - Schnittstellen-Testtools **für [ETSI TS 119512]** und **[TR-ESOR-E, TR-S.4]** (in Arbeit)
- Fortschreibung: „Testspezifikation Functional Conformity" mit **„Preservation Evidence Policy"-** und **„Preservation Profile"-Muster** gemäß **ETSI**
- Neu-Auflage: Testspezifikation „Technical Conformity " **mit Bezug zu den neuen Open-Source Testwerkzeugen** (siehe oben)
- ***Achtung – Neue Anforderung:*** *Voraussetzung für eine erfolgreiche Zertifizierung eines Produkts gegen TR-ESOR V1.3 ist die funktionale und technische Konformität.*

Agenda

1. Neue Anforderungen an Produkte zur Beweiswerterhaltung auf Basis TR-ESOR V1.3
2. Erfahrungsbericht aus der Anwendung der Assessment-Handbücher für Bewahrungsdienste mit TR-ESOR
3. Neue Assessment-Handbücher zur Zertifizierung von (qualifizierten) Bewahrungsdienste gemäß eIDAS/ETSI
4. Zusammenspiel der Zertifizierung von Bewahrungsdiensten (ETSI TS 119 511) und TR-ESOR-Produkten

TR-ESOR schafft vertrauenswürdige Bewahrungsdienste

TR-ESOR = Produkt

Bewahrungsdienst = Service

> 40% Einsparung bei Zertifizierung für (qualifizierte) Bewahrungsdienste gem. eIDAS

Anwendungsbeispiele

- Hochregulierte Industrien
- Public Sector
- HealthCare
- Banking & Insurance

- Archivierung as a service
- Branchenübergreifende Digitale Ökosysteme
  - DLT & non-DLT
  - Self-Sovereign-Identity
- Ersetzendes Scannen

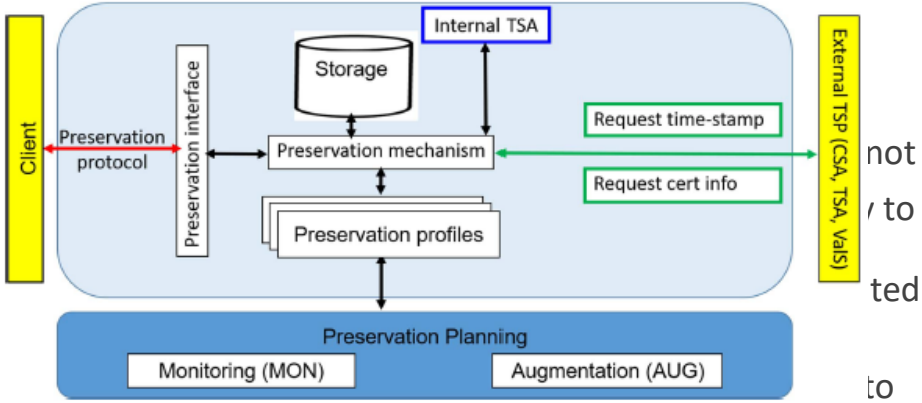
Agenda

1. Neue Anforderungen an Produkte zur Beweiswerterhaltung auf Basis TR-ESOR V1.3
2. Erfahrungsbericht aus der Anwendung der Assessment-Handbücher für Bewahrungsdienste mit TR-ESOR
3. Neue Assessment-Handbücher zur Zertifizierung von (qualifizierten) Bewahrungsdienste gemäß eIDAS/ETSI TS 119 511
4. Zusammenspiel der Zertifizierung von Bewahrungsdiensten (ETSI TS 119 511) und TR-ESOR-Produkten

LONG-TERM PRESERVATION – ETSI TS 119 511

3 preservation services:

- WST – with storage
- WTS – with temporary storage
- WOS – without storage



not

/ to

ted

to

the preservation service

ETSI TS 119 511 V1.1.1 (2019-06)

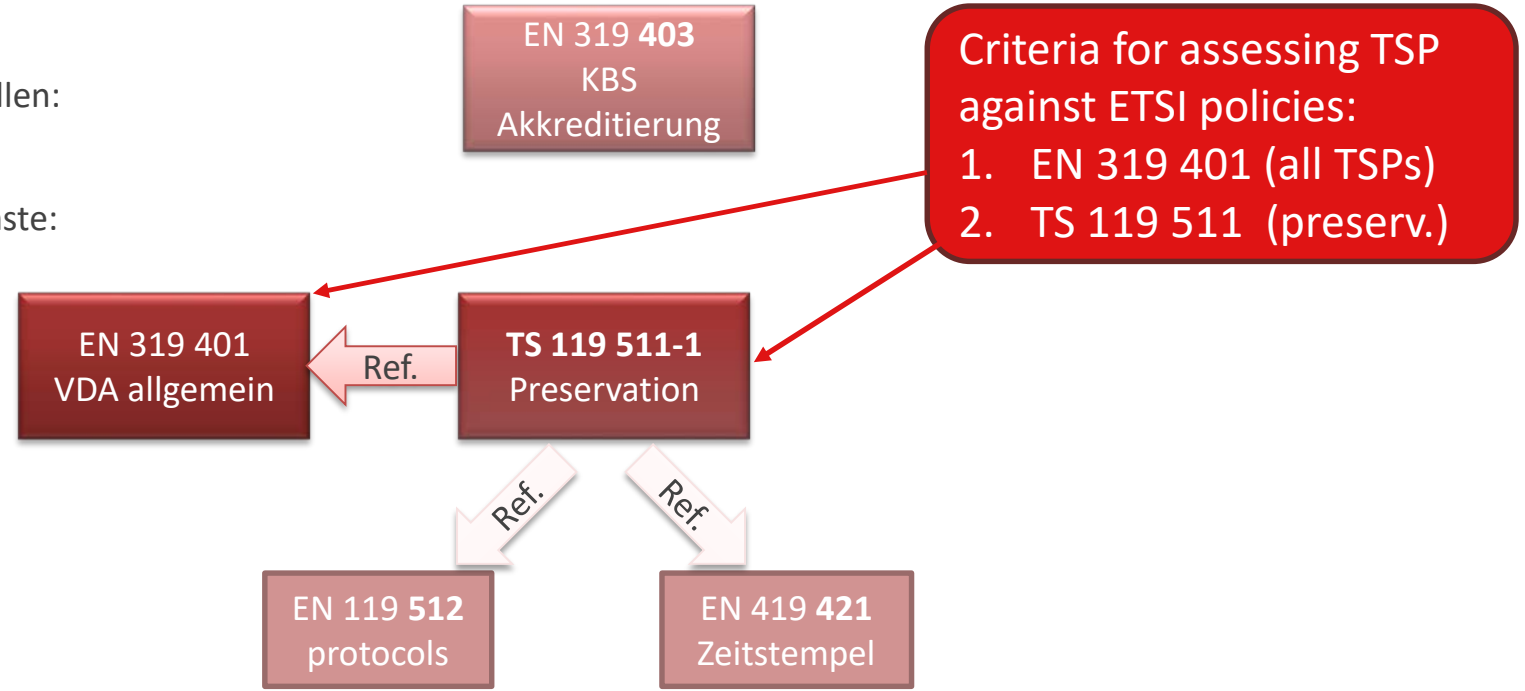
**Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
trust service providers providing long-term preservation
of digital signatures or general data using
digital signature techniques**

KONFORMITÄTSBEWERTUNG NACH EIDAS
FÜR KONFORMITÄTSBEWERTUNG RELEVANTE STANDARDS (AUSZUG)

Konformitäts-
bewertungsstellen:

Vertrauensdienste:

referenzierte
Standards:



TÜVIT®
TÜV NORD GROUP

BEISPIEL: BSI PRÜFKRITERIEN FÜR BEWAHRUNGSDIENSTE (TS 119 511) (BSI ASSESSMENT CRITERIA FOR PRESERVATION SERVICES, PART 2)

OVR-7.10-02: The preservation service shall implement event logs to establish information needed for later proofs.

Assessment Criteria:

- *Stage 1:* The assessor shall assess the documentation of the PSP (e.g. [PSPS] or [T&C]) and verify that the PSP:
  - described the event logs process of the preservation service
- Stage 2: The assessor shall assess the PSP on-site and verify that the PSP:
  - implemented the event logs process by
    - Looking at least one example of an event log for each preservation evidence policy,
    - By comparing the event logs process in practice with the description in the [PSPS] or [T&C] of the PSP.
- *Alternative TR-ESOR certified product:*
  - Verify that the certified product is used at the preservation service and described in the documentation.

EXAMPLE: SCREENSHOT FROM PART 2 OF THE ASSESSMENT CRITERIA

Reference	*Norm Requirement*	*Notes / Auditor Guidance*	*Stage 1 Assessment criteria (document assessment)*	*Verdict Stage 1*	*Stage 2 Assessment criteria (on-site assessment)*	*Verdict Stage 2*	*Observations*	*Findings*
OVR-7.10-02	*The preservation service shall implement event logs to establish information needed for later proofs.*		The assessor shall assess the documentation of the PSP (e.g. [PSPS] or [T&C]) and verify that the PSP: - described the event logs process of the preservation service or - stated which **[TR-ESOR]** certified product of version V1.2.1 or higher is used for providing the service and this requirement by this PSP.		If the claimed **[TR-ESOR]** certified product of version V1.2.1 or higher is in fact deployed for providing the service (checked e.g. by comparing the digital fingerprint of the relevant executables), stage 2 will not be executed. Otherwise: The assessor shall assess the PSP on-site and verify that the PSP: - implemented the event logs process. The assessor shall cause the PSP to show at least one example of an event log for each preservation evidence policy. The assessor shall compare the event logs process in practice with the description in the [PSPS] or [T&C] of the PSP.			

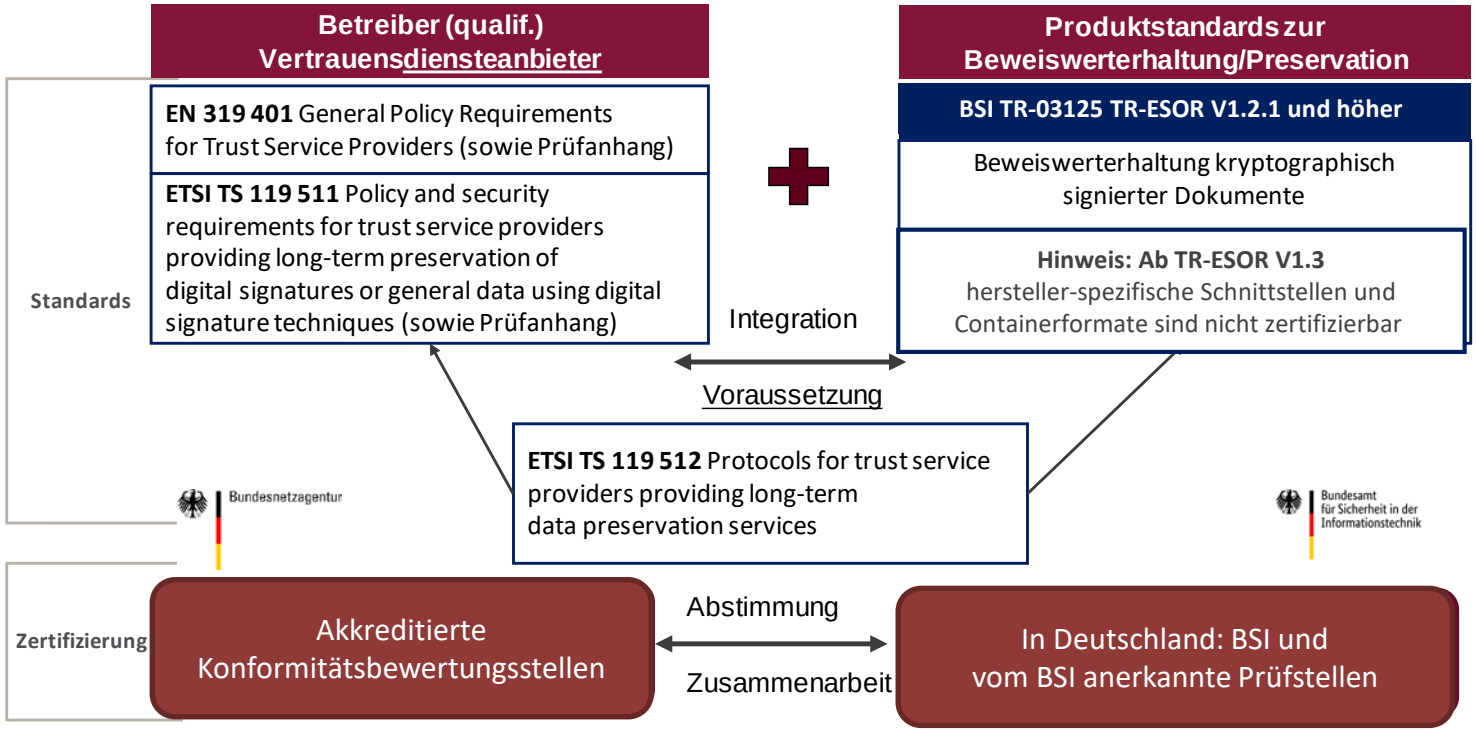
Hinweise / Auflagen

TÜVIT® TÜV NORD GROUP

Agenda

1. Neue Anforderungen an Produkte zur Beweiswerterhaltung auf Basis TR-ESOR V1.3
2. Erfahrungsbericht aus der Anwendung der Assessment-Handbücher für Bewahrungsdienste mit TR-ESOR
3. Neue Assessment-Handbücher zur Zertifizierung von (qualifizierten) Bewahrungsdienste gemäß eIDAS/ETSI
4. Zusammenspiel der Zertifizierung von Bewahrungsdiensten (ETSI TS 119 511) und TR-ESOR-Produkten

INTEGRATION VON BSI TR-ESOR PRODUKTEN IN EINE TS 119 511 ZERTIFIZIERUNG



ZUSAMMENFASSUNG
BSI ASSESSMENT HANDBÜCHER ZUM BEWAHRUNGSDIENST

1. Teil 1 umfasst allgemeine Prüfkriterien für alle VDA nach ETSI EN 319 401

   BSI Criteria for Assessing Trust Service Providers against ETSI Policy Requirements
   - Part 1: Assessment Criteria for all TSP - ETSI EN 319 401

2. Teil 2 umfasst Prüfkriterien für Bewahrungsdienste nach ETSI TS 119 511

   BSI Criteria for Assessing Trust Service Providers against ETSI Policy Requirements
   - Part 2: Assessment Criteria providing long-term preservation of digital signatures or general data using digital signature techniques - ETSI TS 119 511

3. Bewahrungsdienst setzt ein TR-ESOR (ab V1.2.1) zertifiziertes Produkt ein:

   - Die Assessment-Ergebnisse von [ETSI TS 119 511] - Assessment Testschritte, die äquivalent zu TR-ESOR (ab V1.2.1 und höher) -Testschritten sind, **entfallen**

Die Nutzung der BSI-Prüfkriterien für Bewahrungsdienste ist freiwillig
(Empfehlung durch die BNetzA und das BSI)

https://www.bundesnetzagentur.de/EVD/DE/Fachkreis/Empfehlungen/Empfehlungen.html

Vielen Dank für Ihre Aufmerksamkeit!

Dr. rer. nat. Ulrike Korte
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
E-Mail: Ulrike.Korte@bsi.bund.de
www.bsi.bund.de

Dr. Christoph Sutter
Leiter der Zertifizierungsstelle
TÜV Informationstechnik GmbH
IT Infrastructure
+49 201 8999-582
E-Mail: C.Sutter@tuvit.de

Steffen Schwalm
msg.group
Principal Business Consultant
Wittestr. 30
D-13509 Berlin

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

Bundesamt für Sicherheit in der Informationstechnik
TÜVIT TÜV NORD GROUP