Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Herzlich Willkommen

OZG Themenfeld Bildung - 3. Themenfeldkonferenz
05.09.2022

IT-Sicherheit für digitale Bildung

Sascha Neinert und Wojciech Paciorek

Referat DI 15 – eID-Lösungen für die digitale Verwaltung

Vorstellung BSI / Referat DI 15

Digitale Zeugnisse

Beweiswerterhaltende Langzeitspeicherung

Leitsatz

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Kurzprofil des BSI

Gründung
01. Januar 1991

197 Mio. Euro
Budget Haushalt 2021

Stellen 2021

1550 ↗

116 Neue Stellen zum Vorjahr

BSI vor Ort

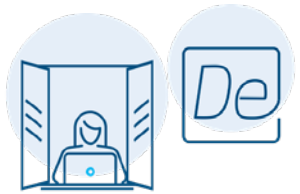
- Standorte
- Stützpunkte
- Verbindungsstellen

Darüber hinaus engagiert sich das BSI seit langem intensiv im internationalen und nationalen Rahmen, unter anderem in enger Zusammenarbeit mit bilateralen Partnern sowie in multilateralen Handlungsfeldern rund um EU und NATO.

Referat DI 15

Bürger
Antragsprozess

Nutzerkonto oder
De-Mail besuchen
Portalverbund/De-Mail



Sichere Identifizierung
und Authentisierung
Online-Ausweisfunktion

Antrag ausfüllen,
elektronisch signieren und senden
(qualifizierte) elektronische Signatur/
Zusendung auch über De-Mail möglich

Zustellung der Bestätigung
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel
Zustellung über Nutzerkonto oder De-Mail

Verwaltung
Bearbeitung
durch das Fachverfahren

Rechtssicheres Scannen
von Papiereingängen
TR-RESISCAN

Antrag elektronisch senden
Portalverbund/De-Mail

Antragseingang
mit (Qualifizierten)
elektronischen Zeitstempel

Eingangsbestätigung wird erstellt
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel

Vorgang archivieren
Beweissichere
Langzeitspeicherung
(TR-ESOR)

Moderner Staat

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Referat DI 15

Bürger
Antragsprozess

Nutzerkonto oder
De-Mail besuchen
Portalverbund/De-Mail

Sichere Identifizierung
und Authentisierung
Online-Ausweisfunktion

Antrag ausfüllen,
elektronisch signieren und senden
(qualifizierte) elektronische Signatur/
Zusendung auch über De-Mail möglich

Zustellung der Bestätigung
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel
Zustellung über Nutzerkonto oder De-Mail

Verwaltung
Bearbeitung durch das Fachverfahren

Rechtssicheres Scannen
von Papiereingängen
TR-RESISCAN

Antrag elektronisch senden
Portalverbund/De-Mail

Antragseingang
mit (Qualifizierten)
elektronischen Zeitstempel

Eingangsbestätigung wird erstellt
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel

Vorgang archivieren
Beweissichere
Langzeitspeicherung
(TR-ESOR)

Moderner Staat

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Referat DI 15

Bürger
Antragsprozess

Nutzerkonto oder
De-Mail besuchen
Portalverbund/De-Mail

Sichere Identifizierung
und Authentisierung
Online-Ausweisfunktion

Antrag ausfüllen,
elektronisch signieren und senden
(qualifizierte) elektronische Signatur/
Zusendung auch über De-Mail möglich

Zustellung der Bestätigung
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel
Zustellung über Nutzerkonto oder De-Mail

Verwaltung
Bearbeitung
durch das Fachverfahren

Rechtssicheres Scannen
von Papiereingängen
TR-RESISCAN

Antrag elektronisch senden
Portalverbund/De-Mail

Antragseingang
mit (Qualifizierten)
elektronischen Zeitstempel

Eingangsbestätigung wird erstellt
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel

Vorgang archivieren
Beweissichere
Langzeitspeicherung
(TR-ESOR)

Moderner Staat

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Referat DI 15

Bürger
Antragsprozess

Nutzerkonto oder
De-Mail besuchen
Portalverbund/De-Mail

Sichere Identifizierung
und Authentisierung
Online-Ausweisfunktion

Antrag ausfüllen,
elektronisch signieren und senden
(qualifizierte) elektronische Signatur/
Zusendung auch über De-Mail möglich

Zustellung der Bestätigung
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel
Zustellung über Nutzerkonto oder De-Mail

Verwaltung
Bearbeitung durch das Fachverfahren

Rechtssicheres Scannen
von Papiereingängen
TR-RESISCAN

Antrag elektronisch senden
Portalverbund/De-Mail

Antragseingang
mit (Qualifizierten)
elektronischen Zeitstempel

Eingangsbestätigung wird erstellt
Qualifiziertes elektronisches Siegel/
Optisch verifizierbares Digitales Siegel

Vorgang archivieren
Beweissichere
Langzeitspeicherung
(TR-ESOR)

Moderner Staat

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Digitale Zeugnisse

BSI Aktivitäten im Kontext „digitale Zeugnisse“

- Referatsübergreifende Arbeitsgruppe „digitale Bildung“
- Beteiligung an den Aktivitäten zur „eIDAS 2.0“ und dem Use Case „diploma“
- Projekt zur Erstellung eines Dokuments „Handreichung digitale Zeugnisse“
  - keine Vorgaben / nicht normativ
  - Hauptzweck ist aufzuzeigen welche Technischen Richtlinien und welche technischen Standards herangezogen werden können
  - es wird einen Abschnitt mit Empfehlungen geben

Handreichung „Digitale Zeugnisse“

Erstellung digitaler Zeugnisse	Daten- und Dateiformate Kryptographische Sicherung: elektronische Signatur, elektronisches Siegel
Scannen papierner Zeugnisse	TR RESISCAN
Ausgabe digitaler Zeugnisse	Identifizierung und Authentisierung Vertrauensniveaus
Prüfung digitaler Zeugnisse	Validierung der Datenformate + Verifizierung der Signatur/des Siegels
Langzeitspeicherung digitaler Zeugnisse	TR-ESOR

Handreichung „Digitale Zeugnisse“ – Beispiel
Signieren eines Zeugnisses

- Eine Signatur unterhalb der EU trusted List (EUTL) kann überall in der EU geprüft werden
- Eine qualifizierte elektronische Signatur hat bereits eine Rechtswirkung
- Ein (qualifiziertes) elektronisches Siegel bietet denselben Integritätsschutz und besagt „von juristischer Person“ bspw. „von Schule/Schulbehörde x“
- Möglicherweise wird ein Zeitstempel benötigt – Konformitätsstufe >= „T“ wird benötigt (s.a. Leitlinie Signaturformate BSI)
- Ein konkreter technischer Standard schränkt eventuell variantenreiche Umsetzungen ein – bspw. ETSI TS 103 172 und ETSI EN 319 142-1 für PDF-Signaturen

Handreichung „Digitale Zeugnisse“ – Beispiel
Ausgabe eines Zeugnisses

Der Zeugnisempfänger (Schüler, Student) ODER bspw. eine erziehungsberechtigte Person muss sich vor Empfang des Zeugnisses identifizieren und authentisieren.

- Welches Vertrauensniveau wird benötigt – für Zeugnisse allgemein, speziell für Abschlusszeugnisse? (normal / substantiell / hoch)
- Ab 16 Jahren kann die Online-Ausweisfunktion genutzt werden → Vertrauensniveau „hoch“, s.a. Personalausweisportal
  - eine aktuelle Entwicklung ist die Smart-eID
- Servicekonten des Bundes / der Länder können möglw. genutzt werden zur Identifizierung/Authentisierung
  - oder sofern vorhanden: das jeweilige Servicekonten-Postfach

Handreichung „Digitale Zeugnisse“ – Empfehlungen (*nicht final - Ausschnitt*)

1. Auswahl geeigneter Datenformate (bspw. PDF/A, bspw. XML)
2. Schutzziele Integrität und Authentizität: Verwendung **digitaler Signaturen**
   - Ggf. zusätzlich ergänzt um optisch verifizierbares Siegel
3. Mindest-**Vertrauensniveau** für Identifizierung *und* Authentisierung definieren: normal, substantiell oder hoch
   - bspw. Identifizierung „vor Ort“ oder per eID-Funktion
4. Digitale, signierte Zeugnisse die lange Zeit gespeichert werden: **Beweiswerterhalt frühzeitig** berücksichtigen
5. **IT-Grundschutz** berücksichtigen: Grundschutz-Profil für Schulen bzw. Hochschulen

Aktuelle Entwicklungen - eIDAS 2.0

- Bislang gilt noch die „Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt …“ (eIDAS VO)
- Prozess hin zur „eIDAS 2.0“ läuft, seit Ende 2020
- Stichworte in dem Zusammenhang sind bspw.

„**wallet**“ bzw. „European Digital Identity Wallet“

„SSI“

„qualified electronic ledger“

- Stand heute (09/2022) gibt es noch an verschiedenen Stellen eine Reihe von Fragezeichen…

Aktuelle Entwicklungen - SSI

- **Self-sovereign Identities** (kurz: SSI), auf deutsch: selbstverwaltete Identitäten
  - eine neue Entwicklung zu digitalen Identitäten
  - (leider) oft vermengt mit DLT, obwohl das nicht zwingend so sein müsste
  - die technischen Standards sind teils noch in der Entwicklung
  - die Argumente pro/contra SSI/DLT vs. „klassische“ Technologien sind nicht immer klar und nicht immer technisch
- Veröffentlichungen des BSI:
  - „Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT)“
  - weitere Informationen zu DLT unter https://www.bsi.bund.de/Blockchain/

Aktuelle Entwicklungen und digitale Zeugnisse

Was hat das Ganze nun mit digitalen Zeugnissen zu tun?

- es gibt verschiedene Use Cases die im Rahmen des eIDAS 2.0 Prozesses betrachtet werden, u.a. „diploma“
- es gibt verschiedene Veröffentlichen, Whitepapers und Projekte zum Beispiel zu „digital credentials“ und SSI

Aber:

1. Es gibt bereits in der eIDAS 1 Technologien die digitale Zeugnisse ermöglichen
2. Es gibt auch in verschiedenen Bereichen entsprechende passende Rechtsverordnungen und Gesetze
3. Es gibt ebenso fertige Produkte, Dienste und Zertifizierungen

Planungen

- Handreichung „digitale Zeugnisse“: Feedback einholen und fortschreiben

- Erarbeitung einer (mehrerer) technischer Richtlinien **mit** Vorgaben zu digitalen Infrastrukturen im Bildungsbereich
  - bspw. zu digitalen Identitäten
  - bspw. zu digitalen Nachweisen bzw. Zeugnissen
  - in Abstimmung mit den jeweiligen Institutionen und Ministerien

- Digitale Identitäten im Bildungsbereich – welche (neuen) Entwicklungen gibt es, was ist bspw. nützlich für Verwaltungen ganz allgemein, wie sicher sind existierende Ansätze?

Beweiswerterhaltende Langzeitspeicherung

Beweiswerterhaltende Langzeitspeicherung

Vor allem **Zeugnisse** müssen über mehrere Jahrzehnte erhalten werden

Es muss **zweifelsfrei** (= *rechtssicher*) nachgewiesen werden, dass die Daten in dieser Zeit nicht verändert oder ausgetauscht wurden (Sicherstellung der Integrität und Authentizität)

→ in der digitalen Welt sind *kryptographische (Hash-/Signatur-)-Algorithmen* notwendig

Diese Algorithmen können nach einiger Zeit ihre **Sicherheitseignung** verlieren (z.B. werden gebrochen)

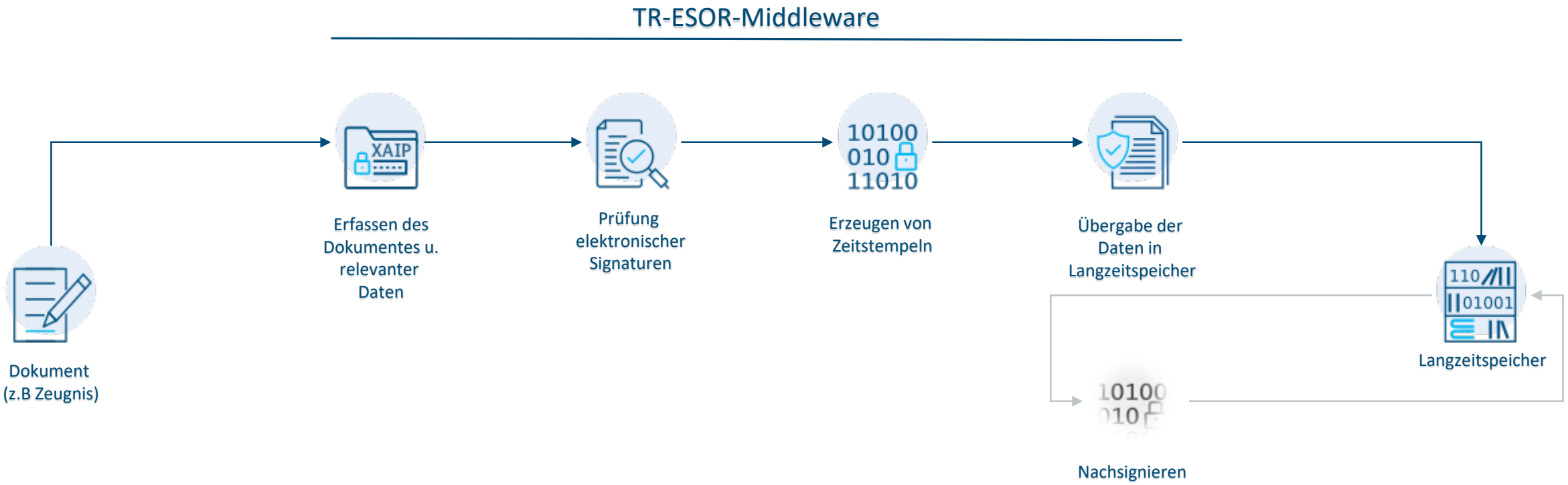
Beweiswerterhaltende Langzeitspeicherung mit TR-03125

Lösungsansatz der BSI TR-03125 (TR-ESOR) folgt aus **§ 15 VDG**:

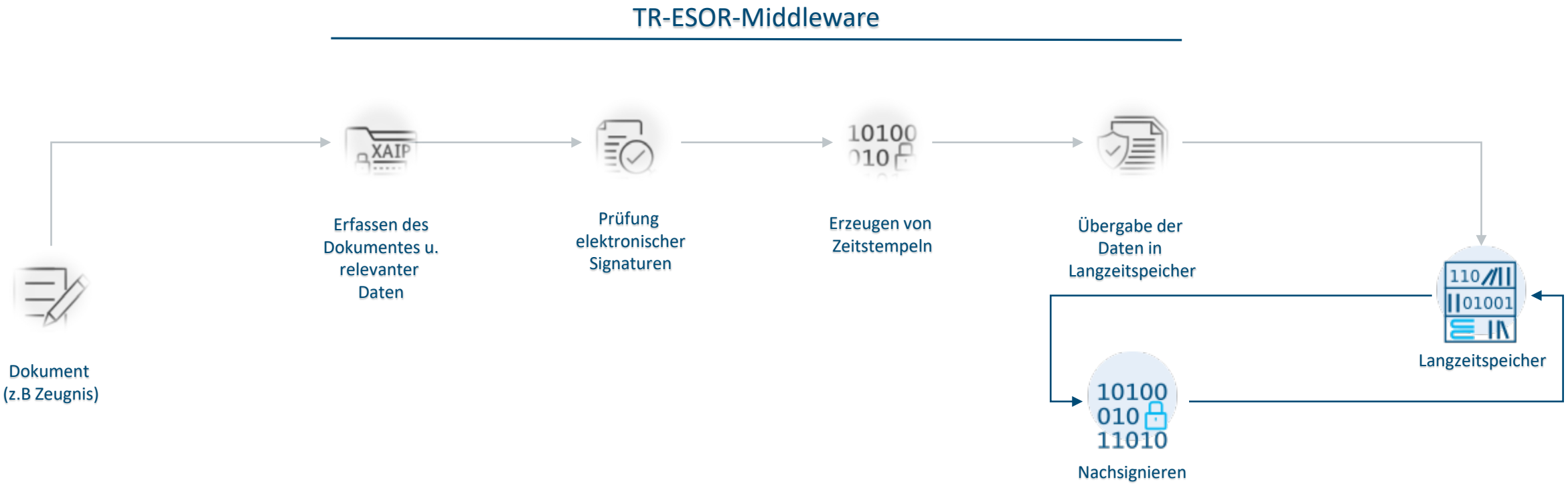
– „Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird.“

→ **Nachsignierung der Dokumente** erlaubt eine rechtssichere Langzeiterhaltung

TR-ESOR in der Anwendung



TR-ESOR in der Anwendung



TR-ESOR in der Anwendung

TR-ESOR in der Anwendung

Prozess für den Anwender nicht wahrnehmbar!

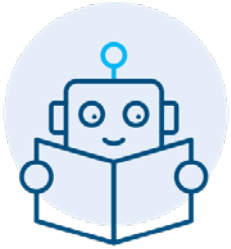
Zugewinn und derzeitiger Stand

– nach BSI TR-03125 zertifizierte Lösungen stellen die **Integrität und Authentizität** von gespeicherten Dokumenten über eine längere Zeitspanne sicher

Derzeitige Entwicklungen:

- Veröffentlichung von **TR-03125 in der Version 1.3**
- Fokus auf Erhöhung und Verbesserungen von technischer Interoperabilität zwischen verschiedenen Lösungen unter Beachtung europäischer Standards (v.a. ETSI TS 119 511)

Quellen, weitere Informationen



- Übersichtsseite zur technische Richtlinie TR-ESOR: https://www.bsi.bund.de/tr-esor
  - Leitlinie für die Beweiswerterhaltende Aufbewahrung gemäß TR-ESOR – eine Handlungshilfe für Behörden und Unternehmen: Veröffentlichung Q2/2021 (*)
- Informationen zum Zertifizierungsverfahren: https://www.bsi.bund.de/zertifizierungtr
- Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record), 26.03.2020 (*)

(*) Auf der BSI-Website https://www.bsi.bund.de oder mittels QR-Code:

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

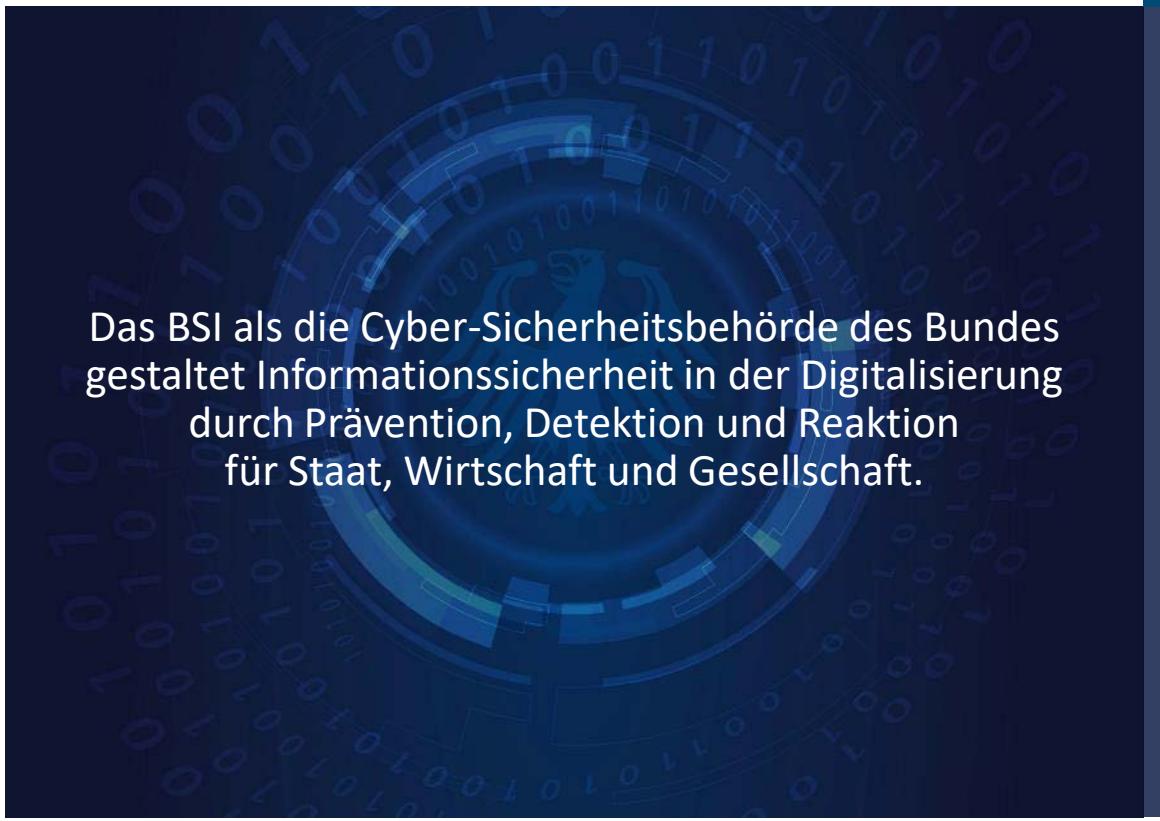
Kontakt

Sascha Neinert und Wojciech Paciorek

Referat DI 15 – eID-Lösungen für die digitale Verwaltung
E-Mail: referat-di15@bsi.bund.de

Postfach Digitale Bildung: digitale-bildung@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik