Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Herzlich Willkommen!

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Digitaler Schülerausweis und Digitales Zeugnis

Referat DI 15, BSI, 24.11.2021

Inhalt

Vorstellung des BSI und des Referates DI 15

Digitaler Schülerausweis

Digitales Zeugnis

Vorstellung des BSI und des Referates DI 15

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

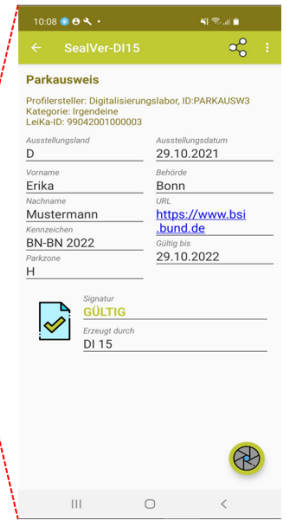
Referat DI 15 – eID-Lösungen für die digitale Verwaltung

OZG: sicherer Online-Zugang zu Verwaltungs-leistungen

Sichere Identifizierung und Authentisierung

Portalverbund

Online-Wahlen



De-Mail

Erstellung Technischer Richtlinien

Digitale Identitäten in der Bildung (Schulzeugnis und Schülerausweis)

ReSiscan

Referat DI 15 – Ansprechpartner

- Jennifer Breuer – DI 15
- jennifer.breuer@bsi.bund.de
- Projektleiterin für das Projekt Digitaler Schülerausweis

- Jasmina Cejvanovic – DI 15
- jasmina.cejvanovic@bsi.bund.de
- Stlv. Projektleiterin für die Projekte Digitaler Schülerausweis und Digitale Zeugnisse

- Sascha Neinert – DI 15
- sascha.neinert@bsi.bund.de
- Projektleiter für das Projekt Digitale Zeugnisse

Bundesamt
für Sicherheit in der
Informationstechnik

Warum beschäftigen wir uns mit dem Themenfeld Bildung?

Warum beschäftigen wir uns mit dem Themenfeld Bildung?

Schülerausweis als digitale Identität nutzbar

Schon den Schülern **sichere Identifizierungsmittel** nutzbar zur Verfügung stellen

Verschiedene Einsatzmöglichkeiten

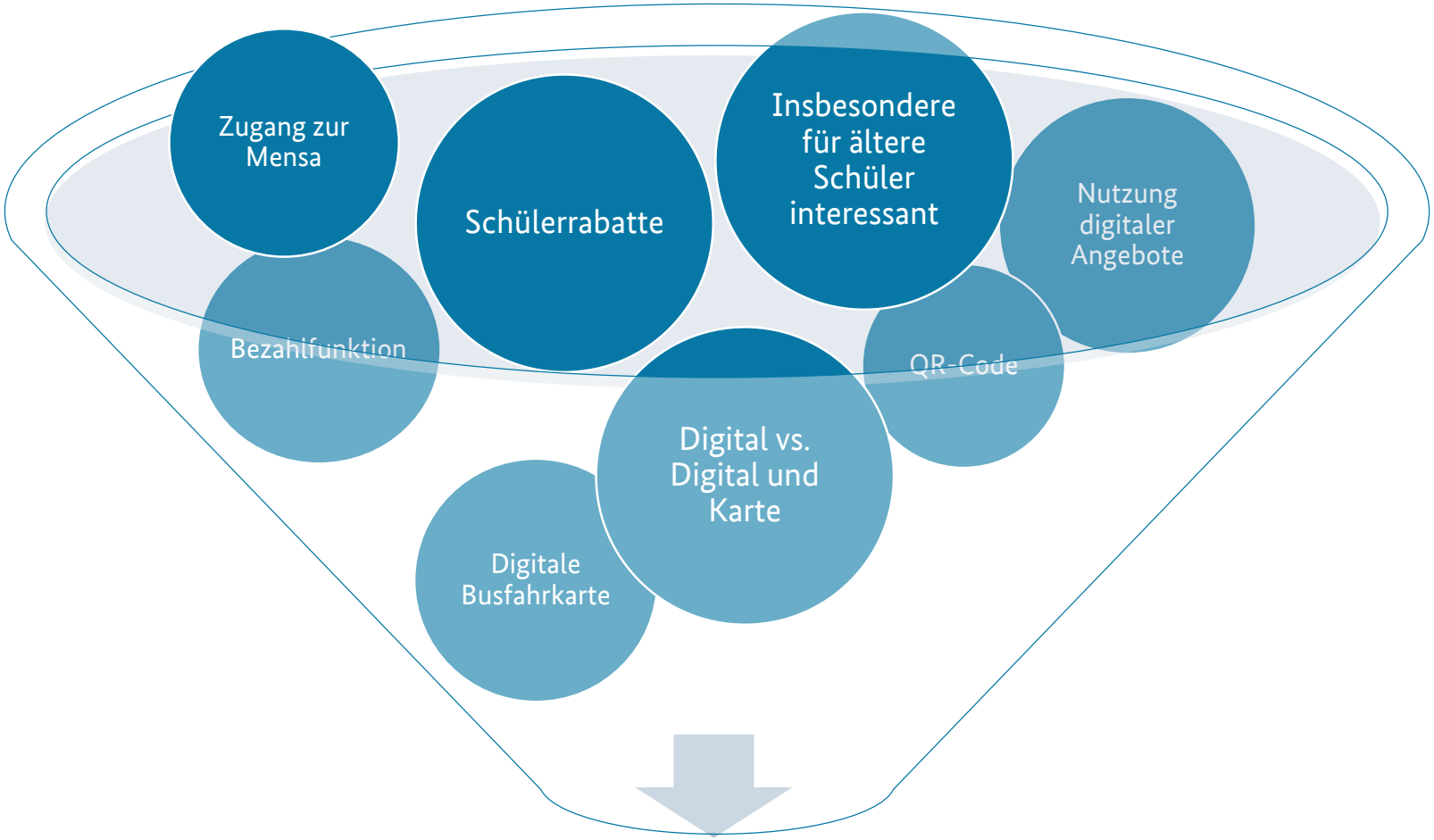
sichere, verifizierbare digitale Zeugnisse ermöglichen

Woher wissen wir, was Schüler brauchen?

Woher wissen wir, was Schüler brauchen?

- Fragebogen an Schulen verteilt
- Zwischenergebnis von Schulen erhalten
- Wofür wird derzeit ein Schülerausweis genutzt und wie soll ein digitaler Schülerausweis aussehen?
- Unterschiedliche Adressaten = verschiedene Blickwinkel

Vorläufige Ergebnisse der Rückmeldungen



Digitaler Schülerausweis

Ideenskizze digitaler Schülerausweis

Ideenskizze digitaler Schülerausweis

- Digitaler Schülerausweis als Ersatz für den derzeitigen Papierausweis
- Unterschiedlichste Einsatzmöglichkeiten im Schulbereich (bspw. Abruf des digitalen Schulzeugnisses von der Schulplattform)
- Weitere Möglichkeiten im Bereich Smart City und digitale Verwaltung
- Viele Gestaltungsmöglichkeiten bei denen immer auch die IT-Sicherheit betrachtet werden muss

Ideenskizze digitaler Schülerausweis

Digital auf dem Smartphone
>> Parallel auch als Karte?

IT-Sicherheitsvorgaben
>> „niedrig“

Welches Vertrauensniveau wird erreicht/benötigt
>> „substanziell“
>> „hoch“

Nutzung im Smart City Kontext
>> Rabatte in Museen etc.
>> Nutzung für E-Scooter

Angriffspotenzial
>> Herausforderung: Schüler „verleiht“ eigene Identität

Als Faktor einer 2-Faktor-Authentifizierung zum Log-In
>> Abruf des digitalen Schulzeugnisses

Projekt „Digitale Zeugnisse“

Projekt „Digitale Zeugnisse“ (DiZe)

- Ziel des Projekts: Erstellung einer „**Leitlinie zur Digitalisierung von Zeugnissen**“
  - Welche technischen Richtlinien des BSI können zur Digitalisierung von Zeugnissen empfohlen werden?
  - Welche aktuellen technischen Entwicklungen können nützlich sein?
- Zeugnisse können dabei Schulzeugnisse, Zeugnisse von Hochschulen oder anderen Bildungseinrichtungen sein
- Annahme 1: Zeugnisse können
  - in Papierform und digital vorliegen
  - ausschließlich digital vorliegen
- Annahme 2: Nutzung und Validierung der Zeugnisse innerhalb der EU (genauer: innerhalb des Geltungsbereichs der eIDAS-VO)

Projekt „Digitale Zeugnisse“ (DiZe)

Inhalte:

- Nutzung **(qualifizierter) elektronischer Signaturen und Siegel** (Zeitstempel, Beweisdaten)
- Optisch verifizierbare digitale Siegel und ersetzendes Scannen
- Beweiswerterhaltende Langzeitspeicherung und Distributed-Ledger-Technologie
- Daten- und Signaturformate
- Vorgaben zu kryptographischen Verfahren
- Vertrauensniveaus und elektronische Identitäten
- Ausblick – Auswahl aus: Beweiswerterhalt in der Blockchain, eIDAS 2.0, Smart-eID, SSI

Elektronische Signaturen und Siegel

Optisch verifizierbare digitale Siegel

Beweissichere Langzeitspeicherung

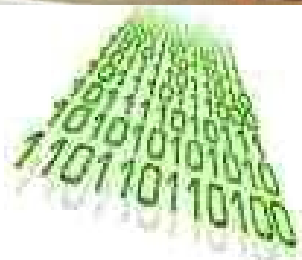
Problemstellung

Dokumente sollen digitalisiert werden, dennoch sollen

- **Authentizität** (Echtheit)
- **Integrität** (Unverfälschtheit)
- **Nachvollziehbarkeit**
- **Verkehrsfähigkeit** (Verfügbarkeit und Lesbarkeit)

erhalten bleiben.

Je nach Anwendungsfall soll (muss) auch der **Beweiswert** für einen langen Zeitraum (Jahrzehnte) erhalten werden.



Begriffsbestimmungen

Elektronische Signatur sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet (s. eIDAS-VO)

- Unterzeichner = natürliche Person
- Fortgeschrittene elektronische Signatur
- Qualifizierte elektronische Signatur = fortgeschrittene elektronische Signatur + qualifizierte elektronischen Signaturerstellungseinheit + von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen (s. eIDAS-VO, Anhang 1)

Elektronisches Siegel:

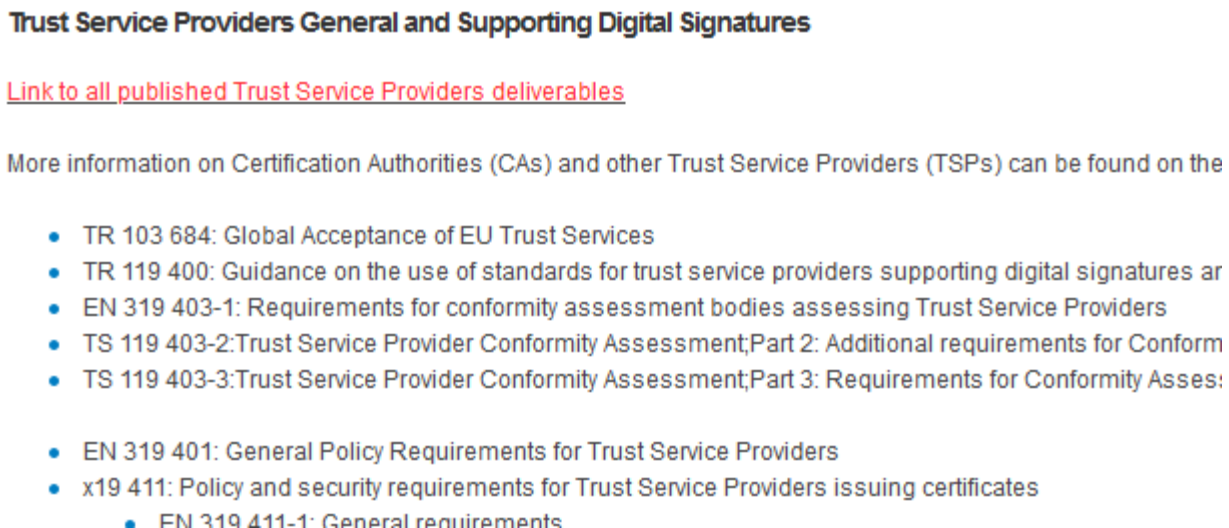
- Siegelersteller = juristische Person
- basiert auf denselben technischen Standards wie die eSignatur (s. Durchführungsbeschluss (EU) 2015/1506, Anhang)

Technische Beweisdaten („Evidence Record“) nach BSI TR-03125, siehe Anlage TR-ESOR-ERS: Profilierung der Evidence Records gemäß RFC4998 und RFC6283 → (vereinfacht) eine Folge von Archivzeitstempeln

Leitlinie und Standards

- **Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten** (Evidence Record) – von BNetzA und BSI
  - Erzeugung, Annahme und Prüfung von Signaturen, Siegeln und Zeitstempeln
  - Erzeugung und Validierung von Archivinformationspaketen und von Evidence Records

  → Verpflichtende Formate und Standards (bspw. PAdES Baseline nach ETSI TS 103 172)
- (zahlreiche) **Standards von ETSI ESI**: https://portal.etsi.org/TB-SiteMap/esi/esi-activities



Trust Service Providers General and Supporting Digital Signatures

Link to all published Trust Service Providers deliverables

More information on Certification Authorities (CAs) and other Trust Service Providers (TSPs) can be found on the

- TR 103 684: Global Acceptance of EU Trust Services
- TR 119 400: Guidance on the use of standards for trust service providers supporting digital signatures ar
- EN 319 403-1: Requirements for conformity assessment bodies assessing Trust Service Providers
- TS 119 403-2:Trust Service Provider Conformity Assessment;Part 2: Additional requirements for Conform
- TS 119 403-3:Trust Service Provider Conformity Assessment;Part 3: Requirements for Conformity Asses

- EN 319 401: General Policy Requirements for Trust Service Providers
- x19 411: Policy and security requirements for Trust Service Providers issuing certificates
  - EN 319 411-1: General requirements

Optisch verifizierbare digitale Siegel

- Elektronisch ausgestellte Genehmigungen, Nachweise und Bescheide: **Qualifizierte elektronische Signaturen und Siegel** liefern Herkunftsnachweis und Integritätsschutz
  - Überprüfung mit entsprechender Software (z. B. PDF Reader)
- Ausgedruckte oder am Endgerät vorgezeigte Nachweise verfügen jedoch über **keine physikalischen Sicherheitsmerkmale** → Eine **Erkennung von Fälschungen** ist daher i. d. R. **nicht möglich**
- **Digitale Siegel** in Form **zweidimensionaler Barcodes** stellen digitale Daten in **optisch verifizierbarer** Form dar.
- Sie enthalten die **wesentlichen Daten** des Dokuments sowie eine **Integritätssicherung**
- Digitale Siegel können **auf Papier ausgedruckt vorgelegt** oder auf dem Mobilgerät vorgezeigt und **mit einer Smartphone-App zweifelsfrei verifiziert** werden.

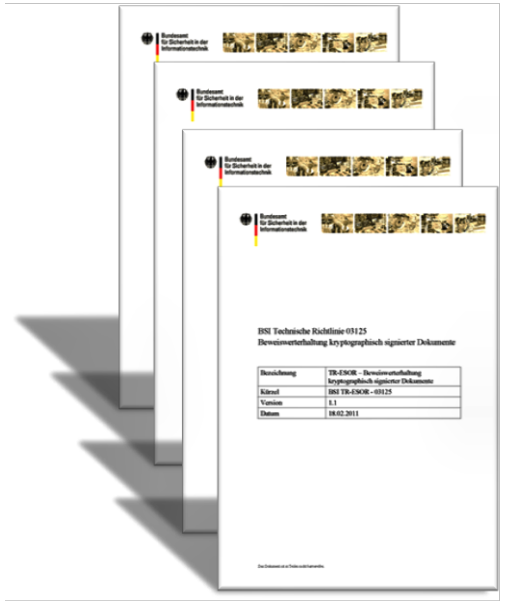
Beweissichere Langzeitspeicherung

- Signaturen basieren auf kryptographischen Algorithmen – Vorgaben bspw. in BSI TR-02102
- Prognose über Eignung nur begrenzt weit in die Zukunft (TR-02102: Jahr 2027) – Zeugnisse müssen aber für Jahrzehnte aufbewahrt werden
- Manche ursprünglich als sicher geltende Verfahren haben bereits ihre **Sicherheitseignung verloren**

→ Idee: Dokumente rechtzeitig neu signieren / siegeln / zeitstempeln **bevor** der Algorithmus als ungeeignet eingestuft wird ←

- Mechanismen zur **Erhaltung des Beweiswerts** sind beschrieben in BSI TR-03125 (TR-ESOR)
- Guter Einstieg: Leitlinie für die beweiswerterhaltende Aufbewahrung gemäß BSI TR-03125

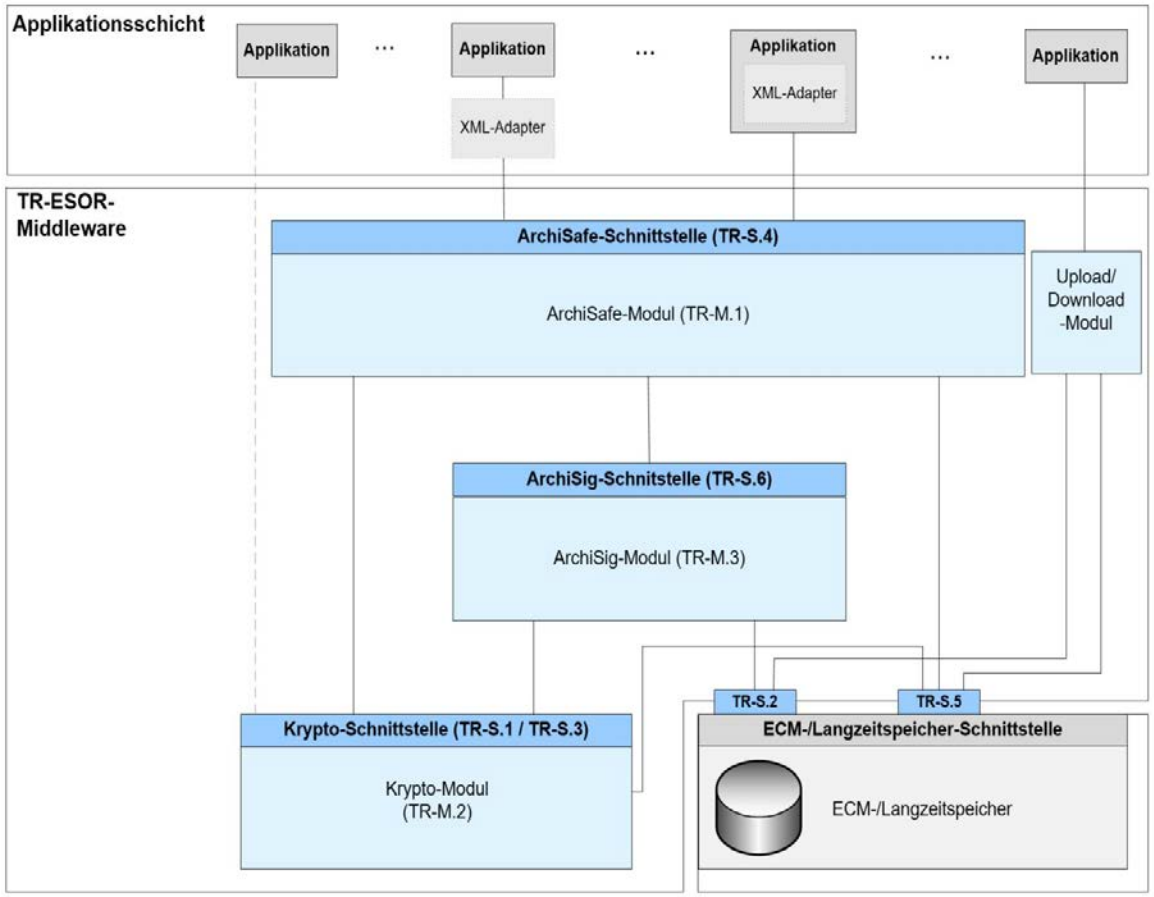
Beweissichere Langzeitspeicherung



Aktuelle Version: 1.2.2
(v1.3 in Entwicklung)

TR-ESOR Hauptdokument

- TR-ESOR-M.1 ArchiSafe Modul
- TR-ESOR-M.2 Krypto Modul
- TR-ESOR-M.3 ArchiSig Modul
- TR-ESOR-S Schnittstellen
- TR-ESOR-B Bundesbehördenprofi
  TR-ESOR-XBDP Profilierung des XAIP
  mit XBARCH, XDOMEA und PREMIS
- 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-C.1 Testspezifikation „Funktionale Konformität“
- TR-ESOR-C.2 Testspezifikation „Technische Konformität“
- TR-ESOR-C.3 Testspezifikation „Bundesbehörden-Profil“



Bundesamt für Sicherheit in der Informationstechnik

Beweissichere Langzeitspeicherung

- Fertige, **nach BSI TR-03125 (TR-ESOR) zertifizierte Produkte** sind verfügbar: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Zertifizierte-Produkte-nach-TR/TR-ESOR/TR-ESOR_node.html
- Anwender: Bund, Länder, Kommunen, Industrie
- Beschaffung über IT-Planungsrat Rahmenverträge einfach möglich: ArchiSig- und Krypto-Modul kostenfrei, nur ArchiSafe ist zu lizensieren zzgl. Wartung und Pflege
- Der Endanwender „sieht“ die TR-ESOR **Middleware** nicht
- TR-ESOR Webseite: www.bsi.bund.de/tr-esor

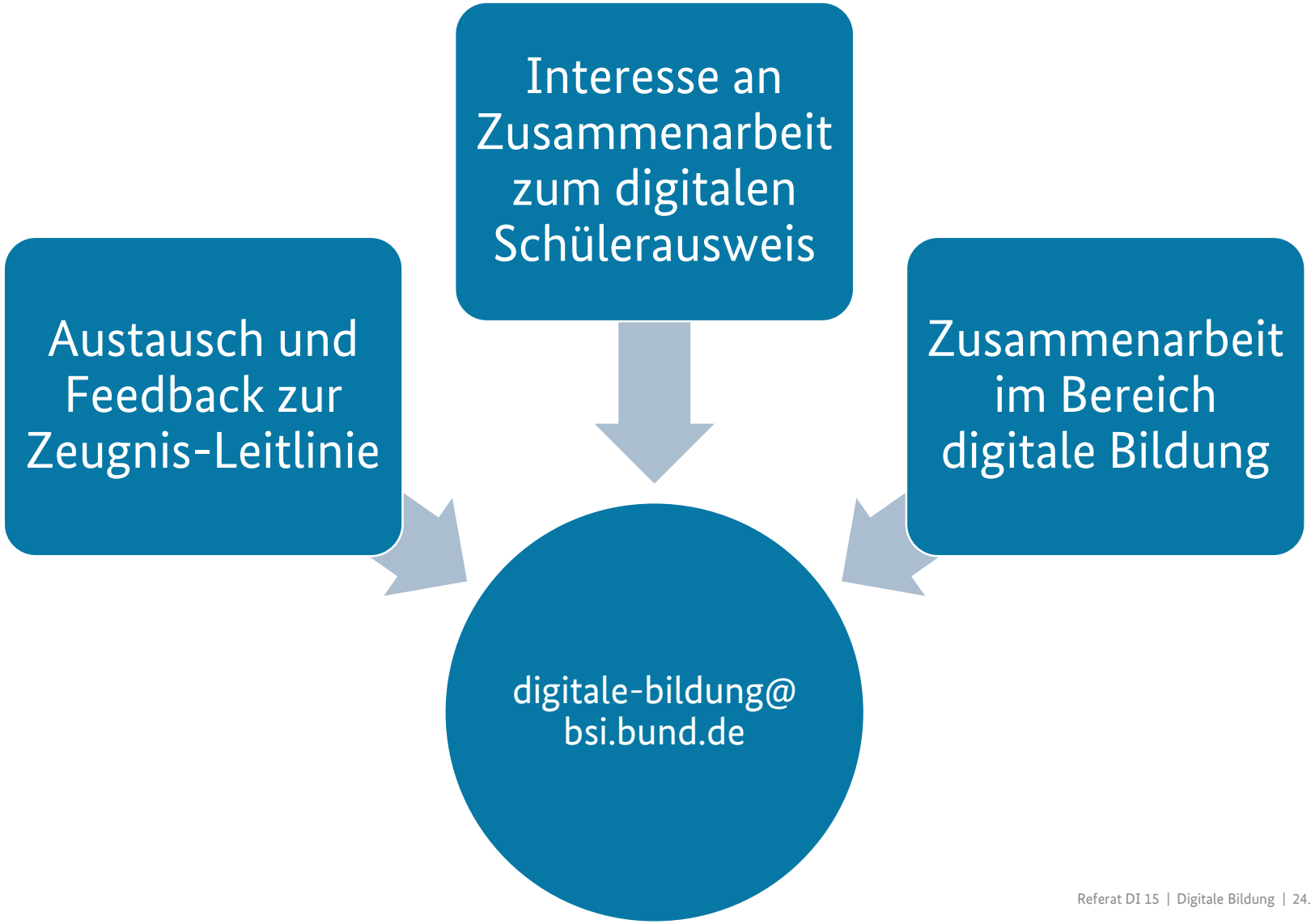
Fazit und Kontakt

Leitlinie zur Digitalisierung von Zeugnissen

- Die Leitlinie versucht einen anwendungsbezogenen, einfacheren Zugang zu den technischen Richtlinien zu schaffen
- Wesentliche Voraussetzung: Austausch mit und Feedback von fachlich Interessierten
- Eine **Version „0.5“ wird Anfang 2022** vorab an Interessierte verteilt – Rückmeldungen und Kommentare gerne!

- Endgültige **Veröffentlichung ist geplant für Q3/2022**

Haben Sie Interesse an einer Zusammenarbeit?



Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt BSI

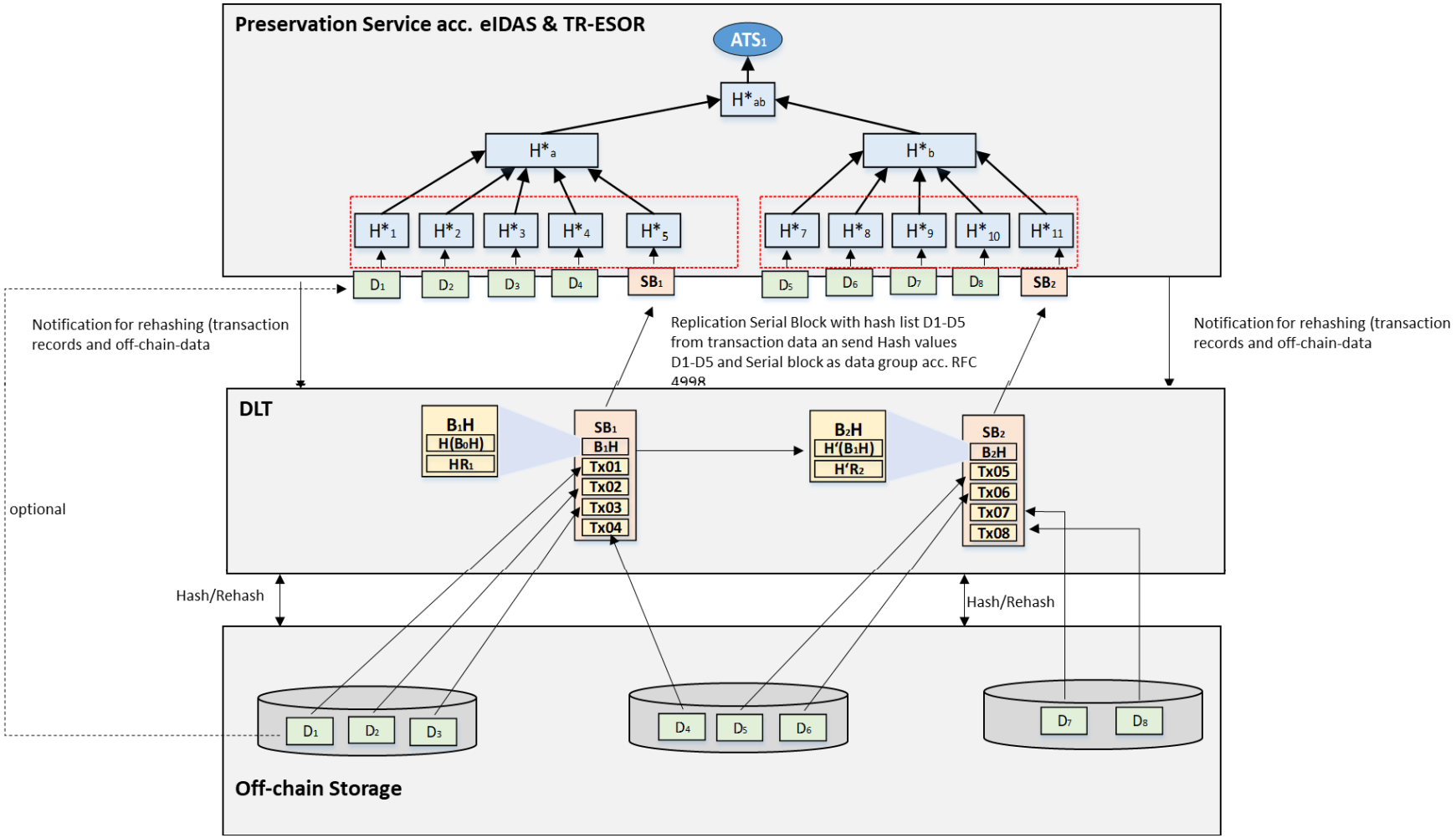
Bundesamt für Sicherheit in der Informationstechnik
Referat DI 15
Godesberger Allee 185 - 189
53175 Bonn

Ansprechpartner
Frau Jennifer Breuer
jennifer.breuer@bsi.bund.de
Frau Jasmina Cejvanovic
jasmina.cejvanovic@bsi.bund.de
Herr Sascha Neinert
sascha.neinert@bsi.bund.de

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Backup: TR-ESOR und DLT



Bundesamt für Sicherheit in der Informationstechnik