# BSI-TR-ESOR-ENC

Ein Profil für beweiskrafterhaltende Aufbewahrung von verschlüsselten Dokumenten gem. BSI-TR-03125 (TR-ESOR).

Tomasz Kusber (Fraunhofer FOKUS)
21.02.2024

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer FOKUS

OMNISECURE® THE WORLD OF smart ID SOLUTIONS 2025

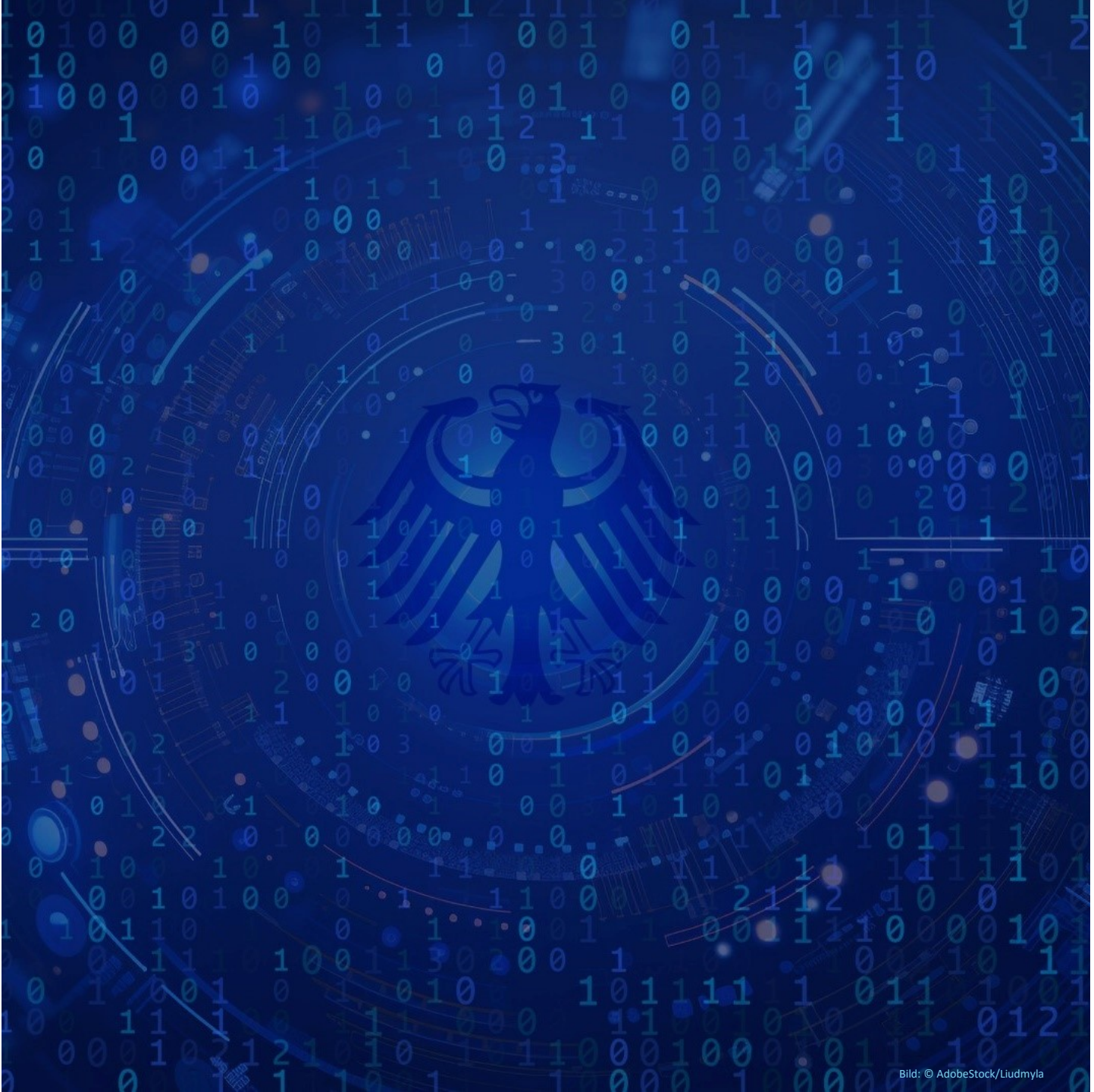


Bild: © AdobeStock/Liudmyla

Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik

- TR-ESOR in a nutshell
- TR-ESOR-ENC
  - Wichtigste Anforderungen
  - Abgeleitete Architektur
  - Zusätzliche Funktionen
  - Beispiele für Anwendungsfälle
  - Ausblick
- Quellen

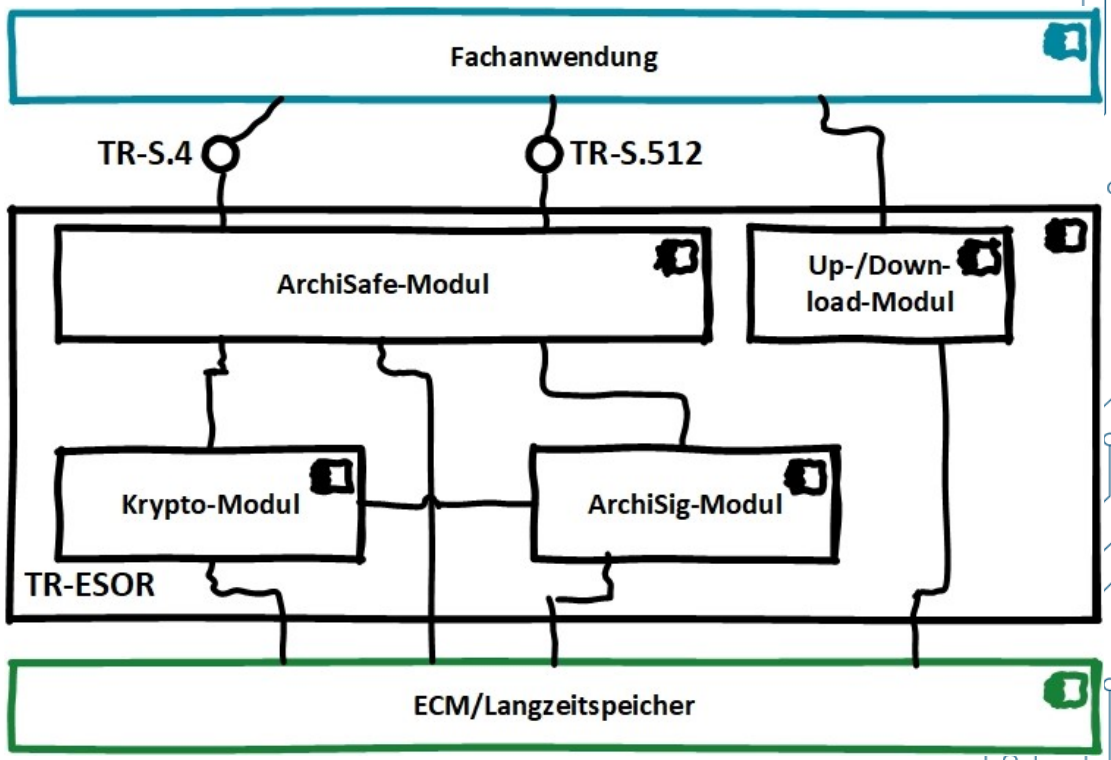
# Aufgabe und Architektur der BSI-TR-03125 (TR-ESOR)

- **TR-ESOR-Aufgabe:**

  *Beweiswerterhaltende Langzeitaufbewahrung von der kryptographisch signierten/versiegelten/zeitgestempelten Information.*

- **TR-ESOR-Komponenten:**
  - ***ArchiSafe-Modul*** – Bereitstellung der Eingangsschnittstellen (TR-S.4 & TR-S.512) und Validierung der Eingangsdaten.
  - ***ArchiSig-Modul*** – Verwaltung der Beweisdaten.
  - ***Krypto-Modul*** – Bereitstellung der notwendigen kryptographischen Funktionen.
  - ***Up-/Download-Modul*** – Hoch und Herunterladen der Daten, die aus einem logischen Container referenziert werden.

- **Dritt-Komponenten**
  - ***Fachanwendung*** – ein Klient für die TR-ESOR-Anwendung, z.B. E-Akte.
  - ***ECM/Langzeitspeicher*** – Speicherung der aufzubewahrenden und der Beweisdaten.



# TR-ESOR-ENC: Wichtigste Anforderungen

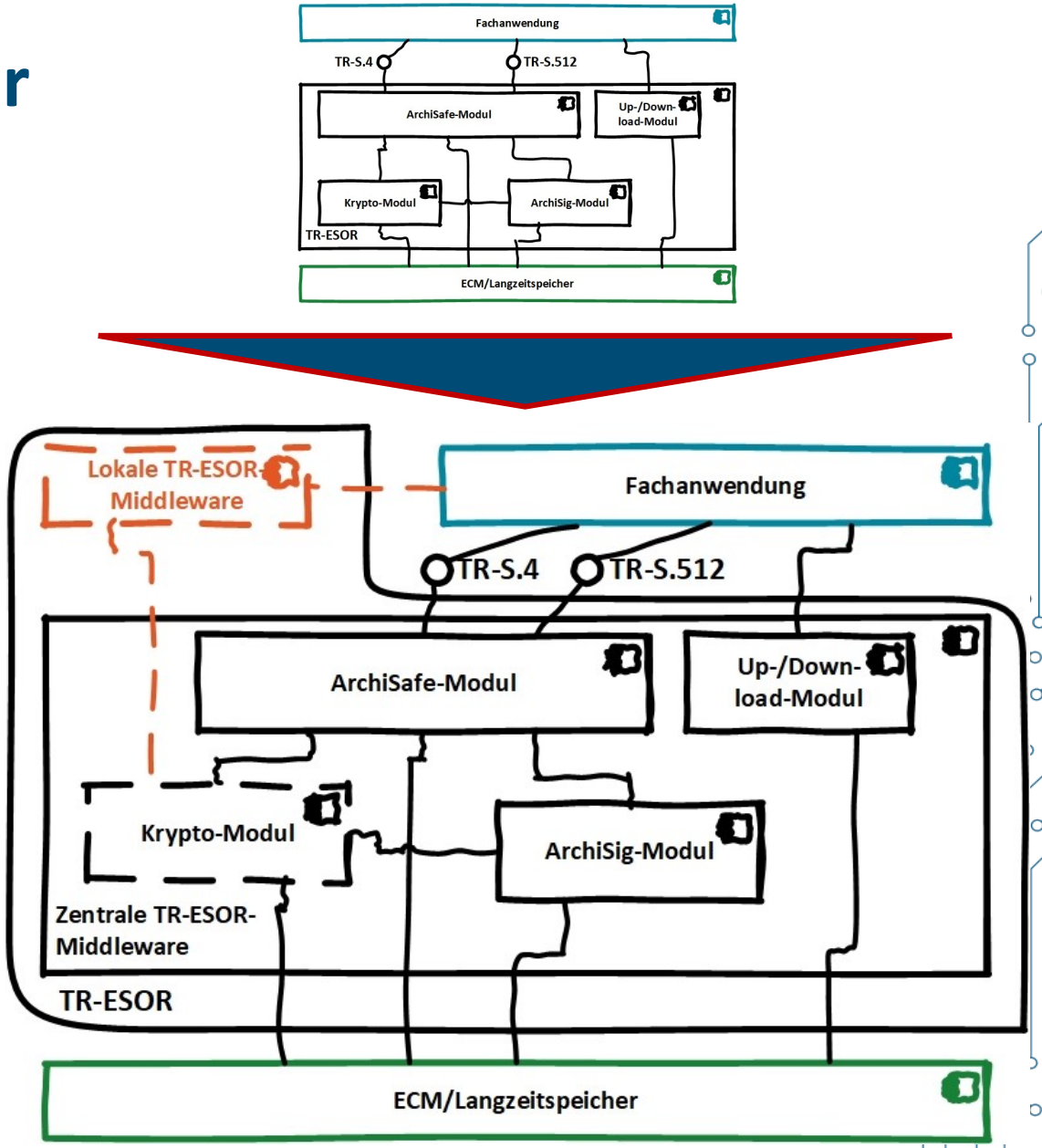
- Zugriff auf die Klartextinformation darf ausschließlich unter voller Kontrolle eines Zugriffsberechtigten erfolgen.
- Die Berechtigung zum Zugriff auf die zu schützende Information muss kryptographisch abgebildet werden.
- Für die Berechnung der für den Aufbau eines Hashbaums benötigten Hashwerte muss die Klartextinformation herangezogen werden.
- Die im Klartext lokal vorliegenden Signaturobjekte müssen vor der Ablage einer erfolgreichen Prüfung unterzogen werden.
- Die für die Verschlüsselung und die Zugriffssteuerung eingesetzte symmetrische und asymmetrische Kryptographie muss vollumfänglich durch die führende Fachanwendung überwacht werden.
- Das zugrundeliegende TR-ESOR-System muss das AIP-Format LXAIP vollumfänglich unterstützen.

# TR-ESOR-ENC: Abgeleitete Architektur

## Die gegenwärtige TR-ESOR-Architektur muss erweitert und angepasst werden.

- Es entsteht ein lokaler Brückenkopf – die ***lokale TR-ESOR-Middleware*** – direkt lokal bei dem Informationsbesitzer, der die TR-ESOR-ENC spezifische Anforderungen, insbesondere Zugriff auf die Klartextinformation, Verschlüsselung und Zugriffssteuerung, realisiert.

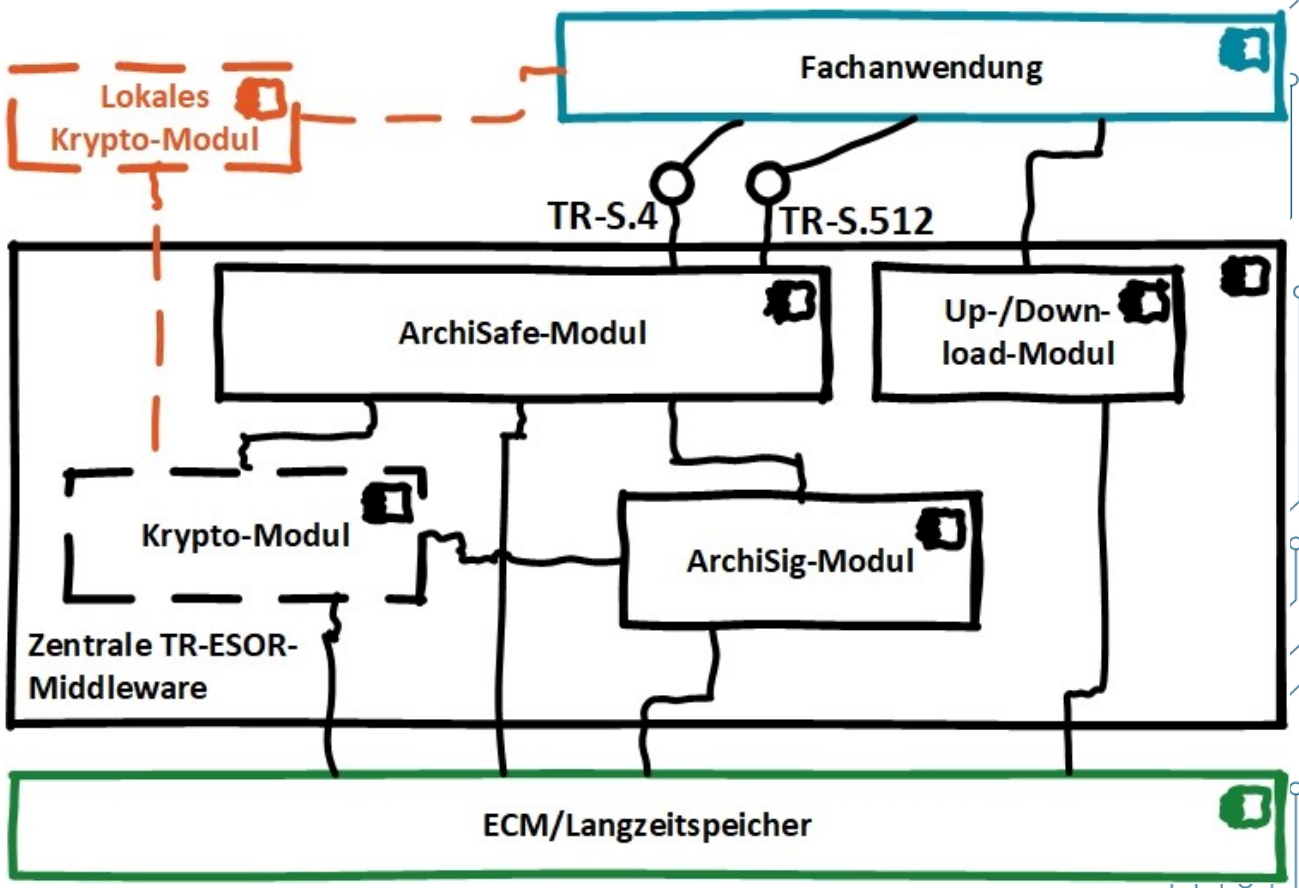
- Das Krypto-Modul der ***zentralen TR-ESOR-Middleware*** muss mit zusätzlicher Funktionalität ausgestattet werde, um die lokale Middleware in die TR-ESOR-Prozesse an geeigneten Stellen einzubinden.



# TR-ESOR-ENC-Architektur ohne lokalen Langzeitspeicher

Im Falle, dass es **keine lokale Datenhaltung** der Klartextdokumente notwendig ist, besteht das lokale TR-ESOR-Middleware aus einer einzigen Komponente:

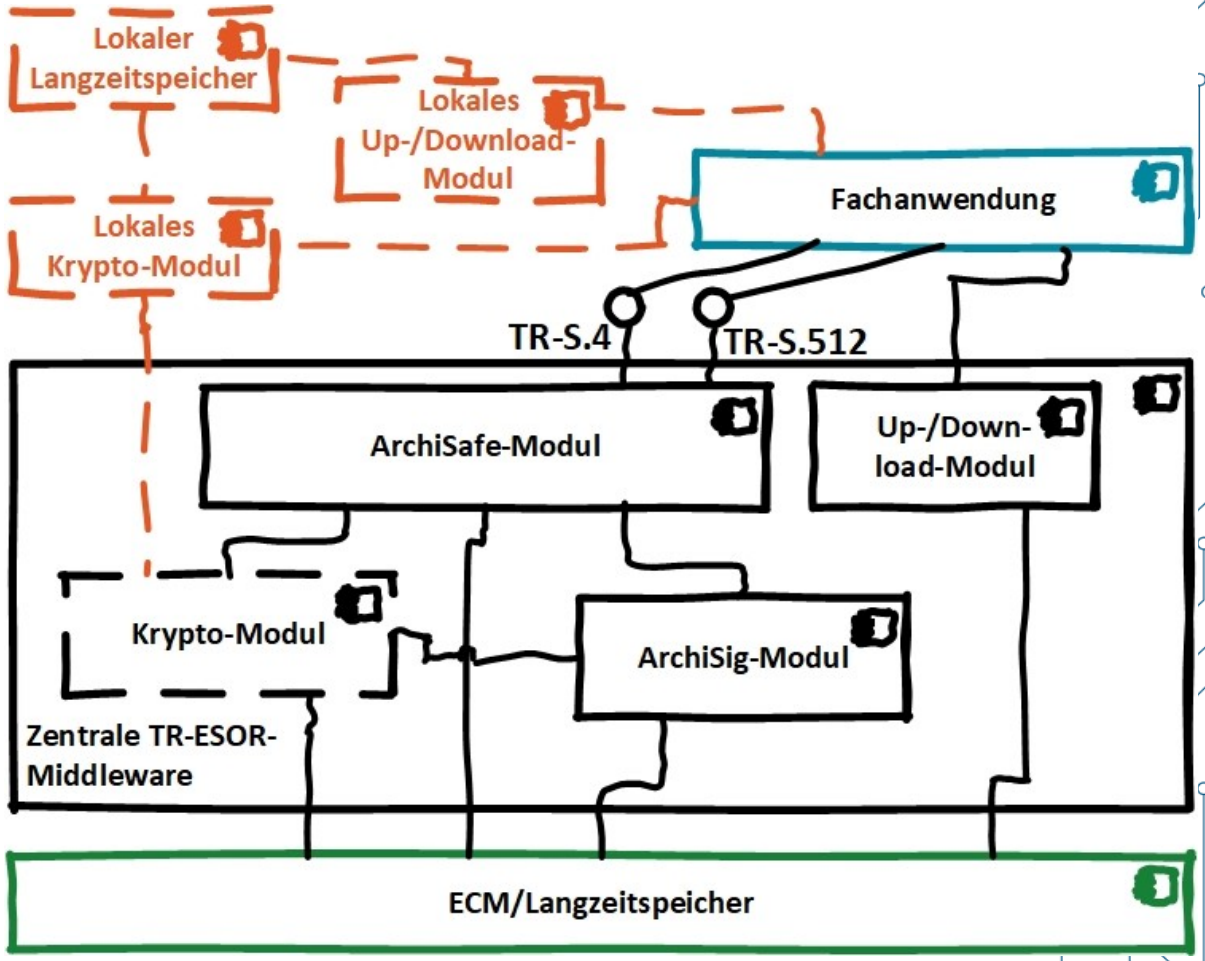
- ***Lokales Krypto-Modul***, das:
  - für die Ausführung der notwendige Funktionen dem zentralen Krypto-Modul zur Verfügung steht und
  - für die führende Fachanwendung die benötigten kryptographischen Dienste (z.B. Hashwertberechnung) anbietet.



# TR-ESOR-ENC-Architektur mit lokalem Langzeitspeicher

Im Falle, dass es **eine lokale Datenhaltung** der Klartextdokumente **notwendig ist**, besteht das lokale TR-ESOR-Middleware aus drei Komponente:

- ***Lokales Krypto-Modul*** – bereits zuvor erwähnt,
- ***Lokales Up-/Download-Modul*** – bietet eine Schnittstelle für die führende Fachanwendung an, um die Daten im lokalen Langzeitspeicher abzulegen und diese daraus auszulesen,
- ***Lokaler Langzeitspeicher*** – speichert die korrespondierenden Daten lokal und bedient dabei das lokale Krypto- und das lokale Up-/Download-Modul.



# Aufgaben der lokalen und zentralen Krypto-Module

Das **lokale Krypto-Modul** muss folgende Funktionen aufweisen:

- ***Verschlüsselung*** – die Klartextinformation muss entsprechend den Anforderungen des zugrundeliegenden Anwendungsfall verschlüsselt und die Zugriffsrechte entsprechend kodiert werden.
- ***Entschlüsselung*** – die verschlüsselte Daten müssen bei Bedarf entschlüsselt werden und liegen im Klartext lokal vor.
- ***Hashwertberechnung*** – die benötigten Hashwerte über den Klartext müssen entsprechend den Vorgaben aus dem zentralen Krypto-Modul berechnet werden.
- ***Signaturprüfung*** – die potentiell auf Klartext bezogenen digitalen Signaturen/Siegel/Zeitstempel müssen identifiziert und geprüft werden. Die Prüfung kann dabei:
  - **Lokal** stattfinden – ausschließlich die Sperrstatusinformation muss bei korrespondierenden ZDAs angefordert werden,
  - Mit Hilfe eines **Validierungsdienstes** erfolgen – in dem Falle darf die Klartextinformation nicht weitergegeben werden sondern deren Hashwert mit Signatur an den Validierungsdienst geschickt werden.

Das **zentrale Krypto-Modul** muss folgende **zusätzliche** Funktionen aufweisen:

- ***Erkennung und Auflösung der Referenzen der verschlüsselten Daten:***
  - die im LXAIP vorhandenen Referenzen auf die ggf. lokal gespeicherten Klartextdaten müssen erkannt werden
  - das korrespondierende lokale Krypto-Modul muss identifiziert werden
  - Eine abgesicherte (authentifiziert und verschlüsselt) Verbindung zum lokalen Krypto-Modul muss aufgebaut werden
- ***Anforderung der Hashwertberechnung*** – die lokale Hashwertberechnung wird via die abgesicherte Verbindung im lokalen Krypto-Modul initiiert
- ***Anforderung der Signaturprüfung*** – die Signaturprüfung wird via die abgesicherte Verbindung im lokalen Krypto-Modul initiiert
- ***Integration der lokal erzeugten Daten*** – die lokal erzeugten und an das zentrale Krypto-Modul zurückgegebenen Daten müssen zwecks Weiterverarbeitung transparent an die aufrufenden Module der zentralen Middleware weitergeleitet werden.

# Anwendungsfälle

**Langzeitbewahrung der elektronischen notariellen Urkunden.**

- Es kommt ein TR-ESOR-ENC-System *mit einem lokalen Langzeitspeicher* zum Einsatz.
- Die Hashwerte werden lokal berechnet.
- Die elektronische Signaturen werden lokal geprüft.
- Die Urkunden werden lokal (im Notariat) im Klartext aufbewahrt und zusätzlich verschlüsselt in der zentralen Middleware.
- Der Zugriff auf die geschützte Information wird durch den Notar mit Hilfe des lokalen Krypto-Moduls gesteuert.

**Aufbewahrung von VS-NfD-eingestufter Information in einem nicht VS-NfD-freigegebenen TR-ESOR-System.**

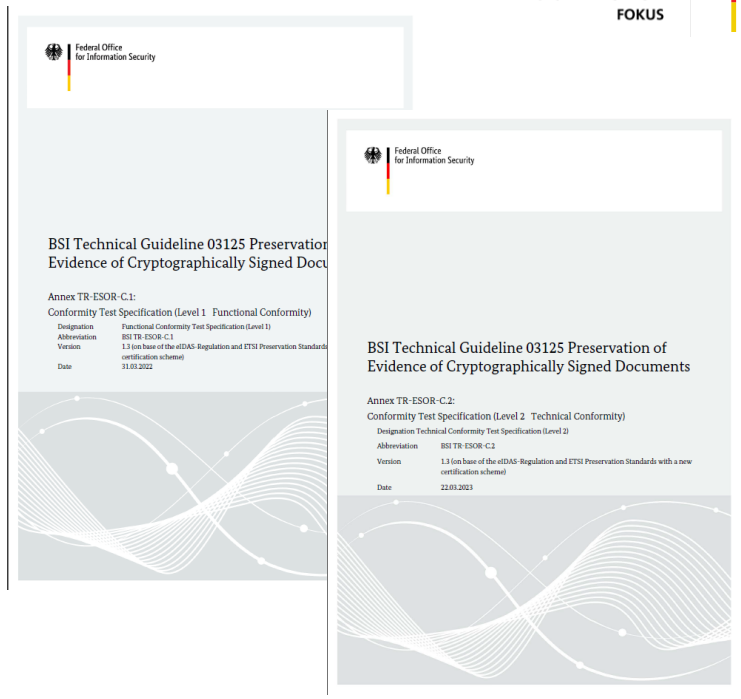
- In einer minimalen Ausprägung kommt ein TR-ESOR-ENC-System *ohne lokalen Langzeitspeicher* zum Einsatz.
- Die Hashwerte werden lokal berechnet.
- Die elektronische Signaturen werden lokal geprüft.
- Die geschützte Information wird nicht in der lokalen Middleware aufbewahrt, sondern entsprechend verschlüsselt in der zentralen Middleware.
- Der Zugriff auf die Verschlüsselte Information wird via lokale Krypto-Modul verwalten.
- Die lokalen Komponenten (hier ausschließlich lokales Krypto-Modul) müssen eine VS-NfD-Freigabe aufweisen.

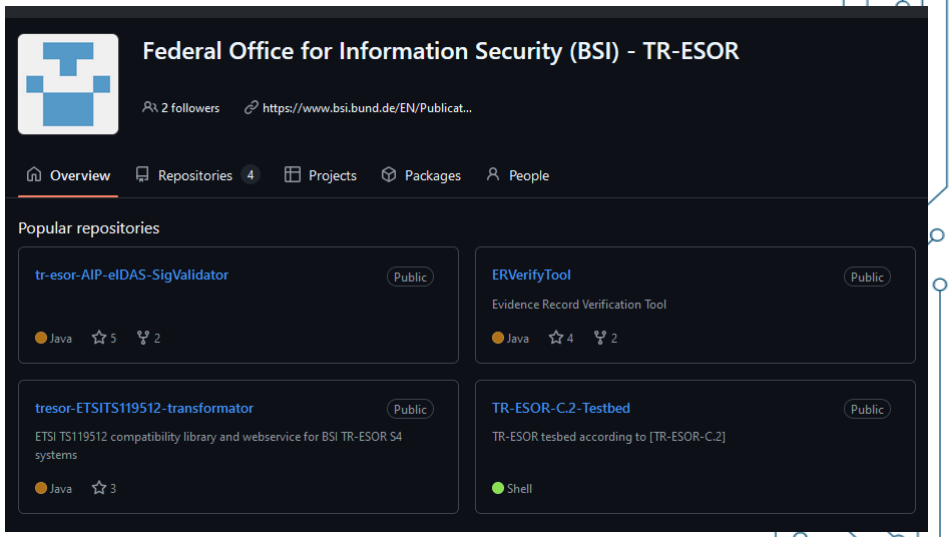
# TR-ESOR-ENC: Ausblick

- Erstellung eines neue TR-ESOR-Anhangs [TR-ESOR-ENC-APP], um:
  - die aktuell in [TR-ESOR-C.1] und [TR-ESOR-C.2] fehlenden, aber für [TR-ESOR-ENC] notwendigen zusätzlichen Testspezifikationen

  zusammen mit
  - den entsprechenden fehlenden Testfällen in den Open Source Testtools
    - [TR-ESOR-C.2-Testbed], sowie in
    - [tresor-AIP-eIDAS-SigValidator]

  zu vervollständigen und für die Zwecke einer [TR-ESOR-ENC]-Zertifizierung bereit zustellen.



# Quellen

- **TR-ESOR-Spezifikation:**
  - Deutsch: https://www.bsi.bund.de/tr-esor, oder
  - Englisch https://www.bsi.bund.de/EN/tr-esor
- **TR-ESOR-Open-Source-Tools:**
  - https://github.com/de-bund-bsi-tr-esor
- **ETSI EN 319 162:**
  - https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf
- **ETSI TS 119 512:**
  - http://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.02.01_60/ts_119512v010201p.pdf
- **RFC4998:**
  - https://datatracker.ietf.org/doc/html/rfc4998
- **RFC6283:**
  - https://datatracker.ietf.org/doc/rfc6283

Dr. Ulrike Korte

Referat D11 - Bewertungsverfahren für Anwendungen von eID-Technologien Bundesamt für die Sicherheit in der Informationstechnik

Tel. +49 (0) 228 9582 5842
Ulrike.Korte@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Tomasz Kusber

DPS – Digital Public Services

Tel. +49 (30) 3456-7139
tomasz.kusber@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de

Bundesamt
für Sicherheit in der
Informationstechnik

Fraunhofer
FOKUS

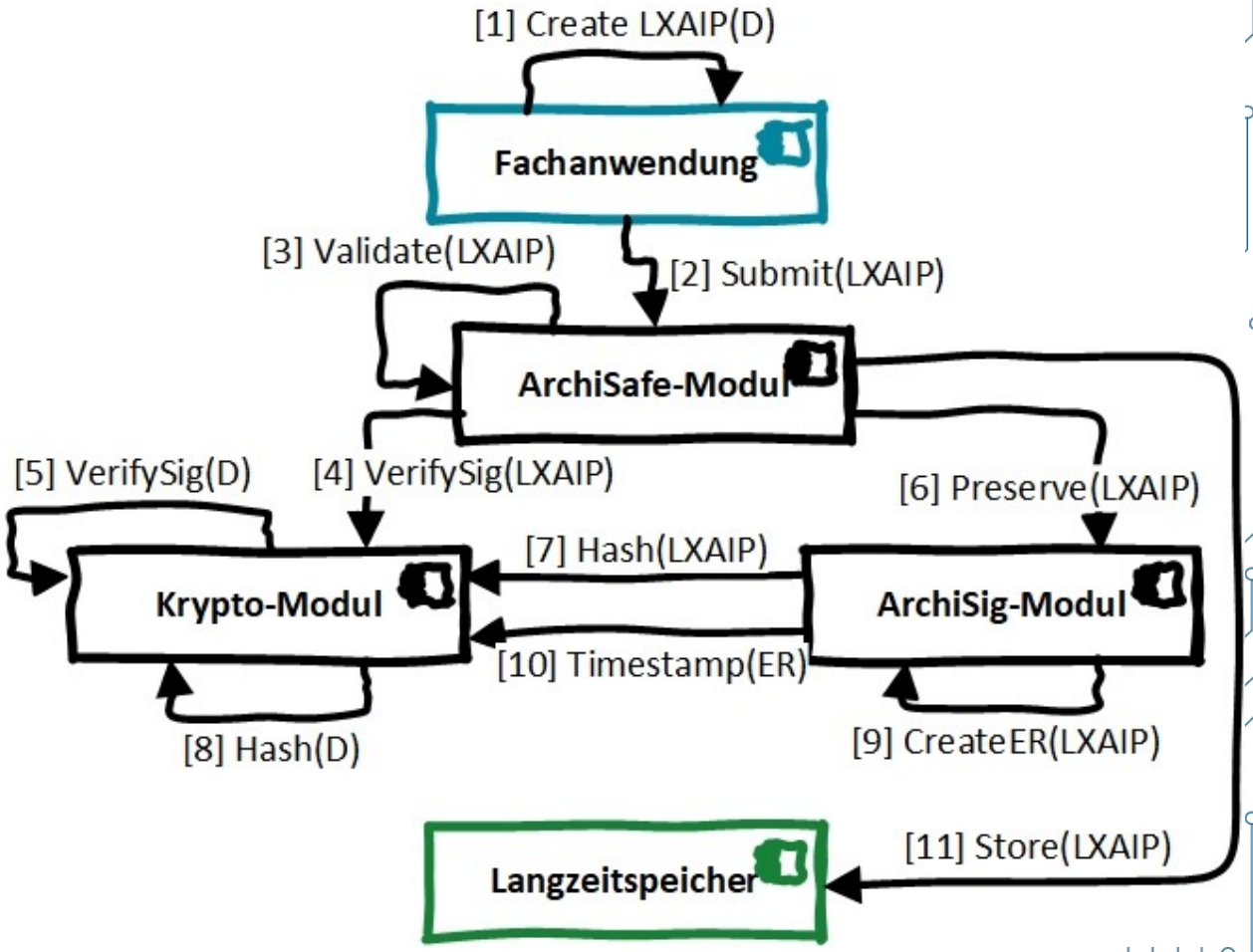
Follow us:

# Ergänzungsfolien

Bild: © AdobeStock/Azazul

# TR-ESOR: Standard-Flow für Ablage eines LXAIP (vereinfacht)

1. Ein LXAIP wird gebaut und das Dokument D darin abgelegt.
2. Das LXAIP wird via TR-S.4/TR-S.512 an das TR-ESOR-System übertragen
3. Das LXAIP wird validiert
4. Validierung der Signaturen wird veranlasst.
5. Signaturen werden validiert.
6. Die Erstellung der Beweisdaten wird veranlasst.
7. Die relevanten Teile müssen verhasht werden (z.B. D).
8. Der Hashwert wird berechnet.
9. Der Evidence Record für XAIP wird erzeugt.
10. Der Evidence Record wird mit einem Zeitstempel versiegelt (RFC4998/RFC6283).
11. Das LXAIP wird im Speicher abgelegt.



# TR-ESOR-ENC: Beispiel für die Ablage eines LXAIP (vereinfacht)

1. Das Dokument D wird verschlüsselt → ED.
2. Ein LXAIP wird gebaut und das ED darin abgelegt.
3. Das LXAIP wird via TR-S.4/TR-S.512 an das TR-ESOR-System übertragen
4. Das LXAIP wird validiert
5. Validierung der Signaturen wird veranlasst.
   a) Validierung von ED wird an das lokale Krypto-Modul delegiert.
   b) ED wird lokal entschlüsselt und
   c) Signaturen validiert.
6. Die Erstellung der Beweisdaten wird veranlasst.
7. Die relevanten Teile müssen verhasht werden (z.B. D).
   a) Hashberechnung wird an das lokale Krypto-Modul delegiert.
   b) ED wird entschlüsselt.
   c) Hashwert über das Klartextdokument D wird berechnet.
8. Der Evidence Record für LXAIP wird erzeugt.
9. Der Evidence Record wird mit einem Zeitstempel versiegelt (RFC4998).
10. Das LXAIP wird im Speicher abgelegt.