Technische Anforderungen an eine EUDI-Wallet

Omnisecure - 19.01.26

Bundesamt
für Sicherheit in der
Informationstechnik

Regulatorische Anforderungen

Artikel 5a und 5c + Durchführungsrechtsakte

- Artikel 5a: **Funktionale Anforderungen**
  - Was kann eine EUDI-Wallet?
  - Interoperabilität durch Protokolle und Standards
  - Authentizität von Wallets und RPs
  - …

4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:

(a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;

(b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;

(c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

Regulatorische Anforderungen

Artikel 5a und 5c + Durchführungsrechtsakte

- Artikel 5a: **Funktionale Anforderungen**
  - Was kann eine EUDI-Wallet?
  - Interoperabilität durch Protokolle und Standards
  - Authentizität von Wallets und RPs
  - …

4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:

(a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;

(b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;

(c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

- Artikel 5c: **Anforderungen an eine Zertifizierung**
  - Nationales Zertifizierungsschema
  - Risiko-Register
  - Kein „**Ausdenken**“ von Anforderungen

Article 5c

Certification of European Digital Identity Wallets

1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.

Risiko-Register

CIR 2024/2981 - Annex I

- Übergeordnete Risiken (z.B. Identitätsdiebstahl) und systembezogene Risiken
  - Aber: ohne „formale“ Risikoanalyse

- Teil des Zertifizierungsschemas: **kontinuierliche Erweiterung des Registers**
  - Risiko-Analyse (z.B. nach ETSI TS 102 165-1, BSI-Standard 200-3, etc.)

Risiko-Register

CIR 2024/2981 - Annex I

- Übergeordnete Risiken (z.B. Identitätsdiebstahl) und systembezogene Risiken
  - Aber: ohne „formale“ Risikoanalyse

- Teil des Zertifizierungsschemas: **kontinuierliche Erweiterung des Registers**
  - Risiko-Analyse (z.B. nach ETSI TS 102 165-1, BSI-Standard 200-3, etc.)

- Bedrohungen für die Wallet
  - **Nachweis über Abdeckung der Risiken** im Zertifizierungsschema durch **Sicherheitsanforderungen**

SECTION IV

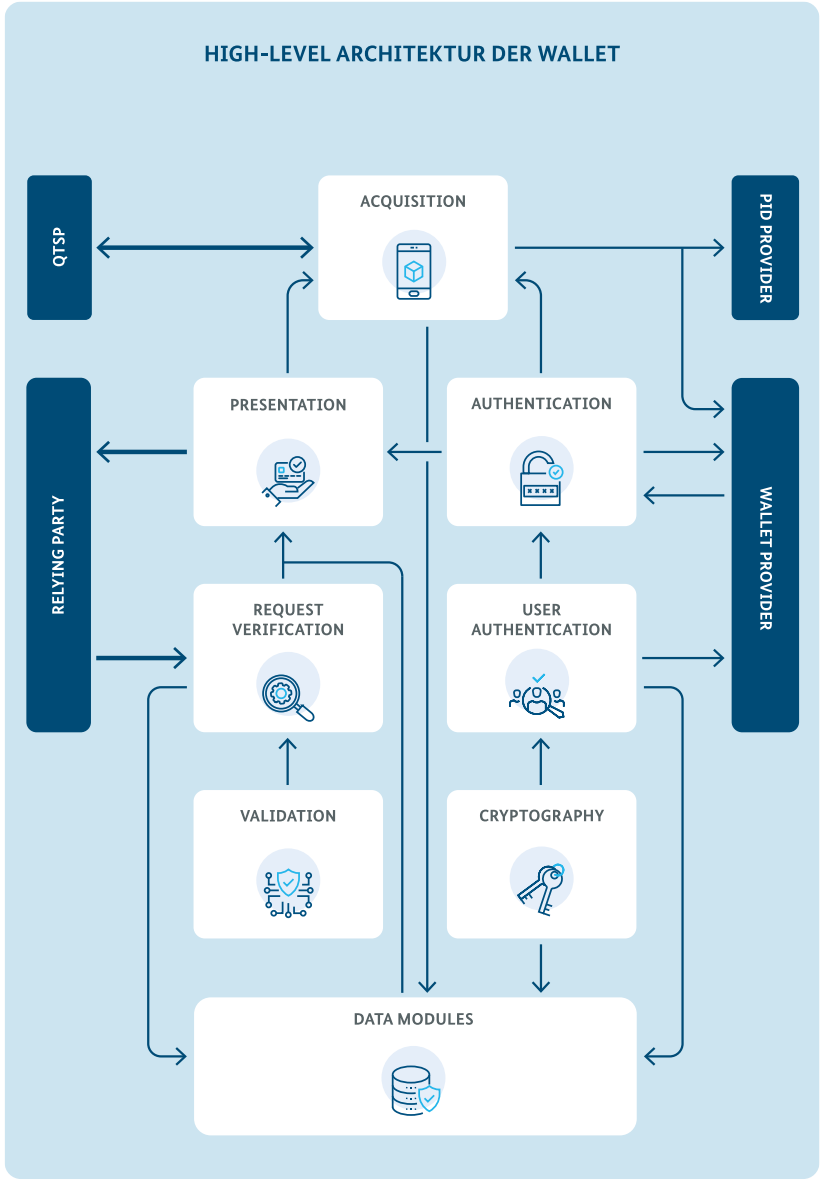
Threats to the wallets

This last section presents a selection of typical threat scenarios specific to the wallets, which are mapped to the key related high-level risks, as listed above. This list indicates threats that need to be covered, but it does not constitute an exhaustive list of threats, which depends greatly on the architecture of the selected wallet solution and on the evolution of the threat environment. Additionally, in the risk assessment and proposed measures, the wallet provider can only be responsible for those components in scope of certification (*).

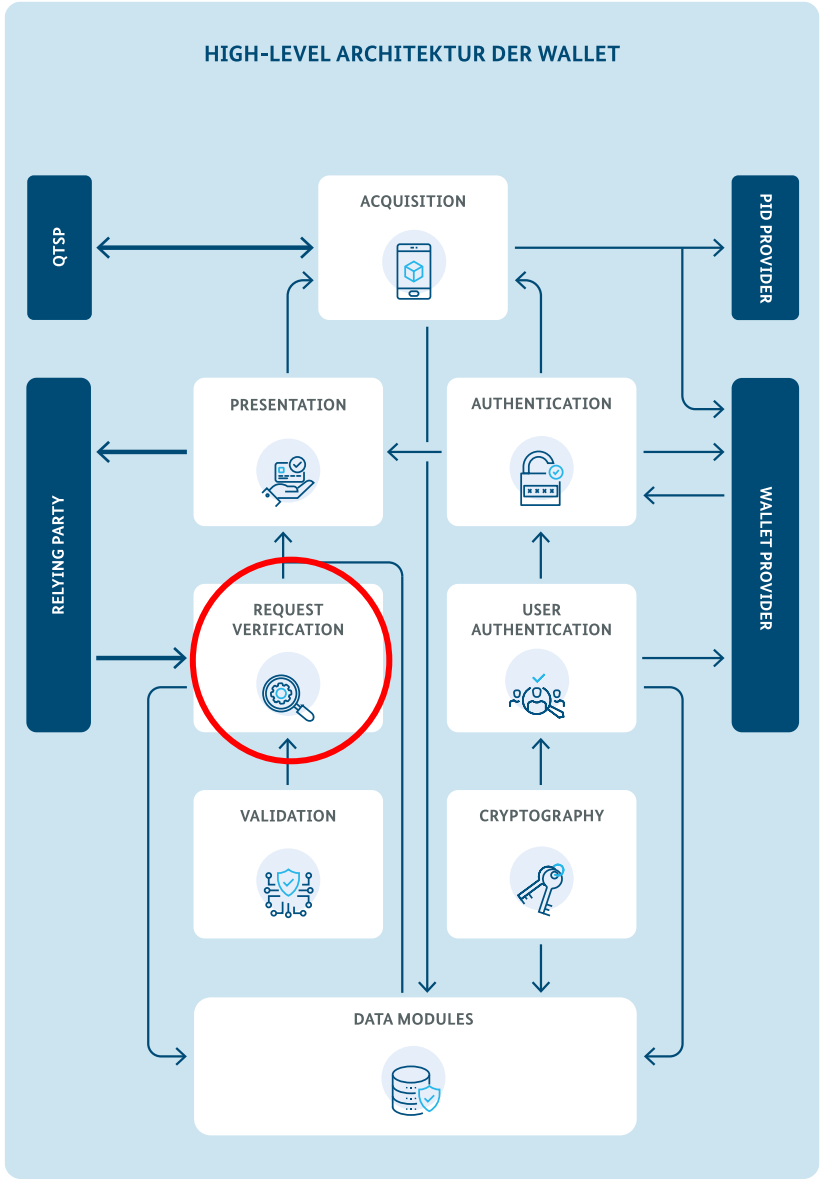
ID ***Identifier***	**Threat description** ***Description of the identified threat* (*)**	**Risk title** ***Related risks***
TR1	An attacker can revoke pseudonyms without justified reason.	Creation or use of a fake electronic identity (R2)
TR2	An attacker can issue fabricated electronic identities that do not exist.	Creation or use of a fake electronic identity (R2)
TR3	An attacker can start to issue unauthorised PIDs.	Creation or use of a fake electronic identity (R2)
TR4	An attacker can get an administrator to enter a wrong PID provider into the PID provider trusted list.	Creation or use of a fake electronic identity (R2)
TR5	An attacker can bypass the remote identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR6	An attacker can bypass the physical identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR7	An attacker can bypass the identity proofing services related to the use of a remote (qualified) certificate.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR8	An attacker can get access to a wallet that is not bound to a person.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)

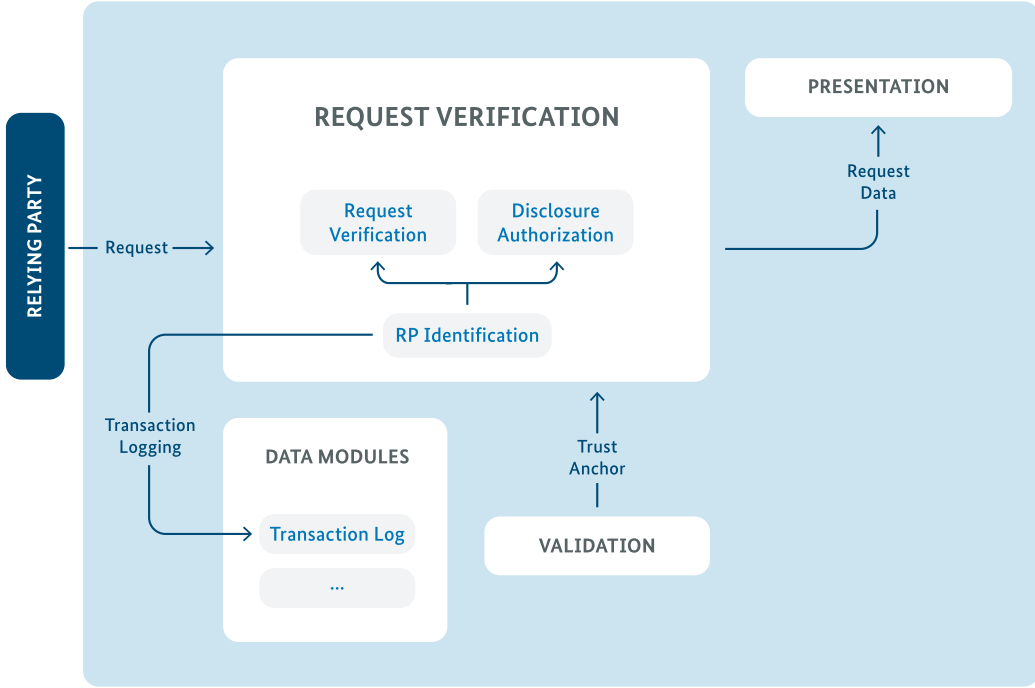
Sicherheitsanforderungen an eine EUDI-Wallet anhand zuvor definierter Risiken

Woran stellt man nun Sicherheitsanforderungen? - Komponenten

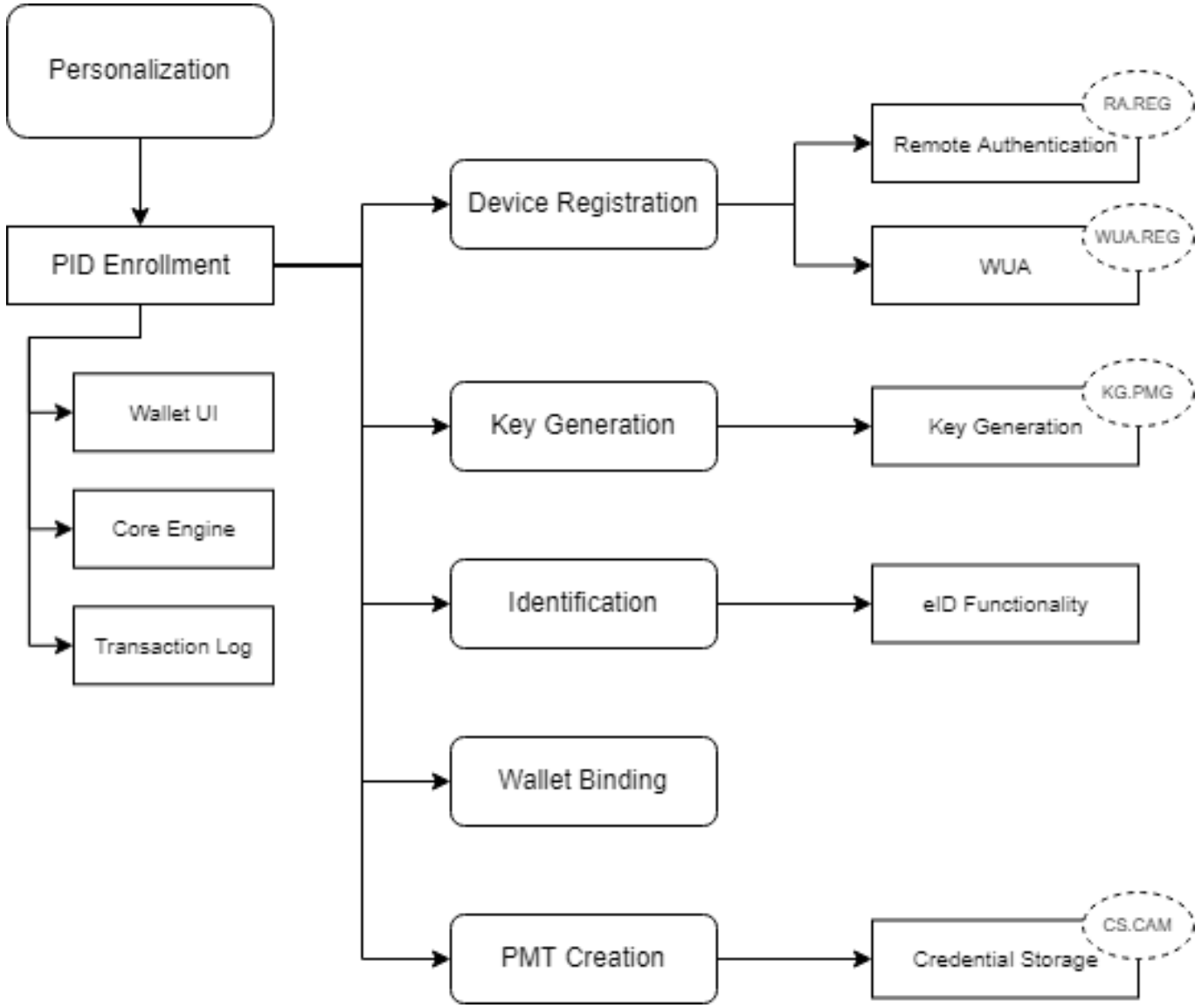


Woran stellt man nun Sicherheitsanforderungen? - Komponenten





Woran stellt man nun Sicherheitsanforderungen? - Prozesse

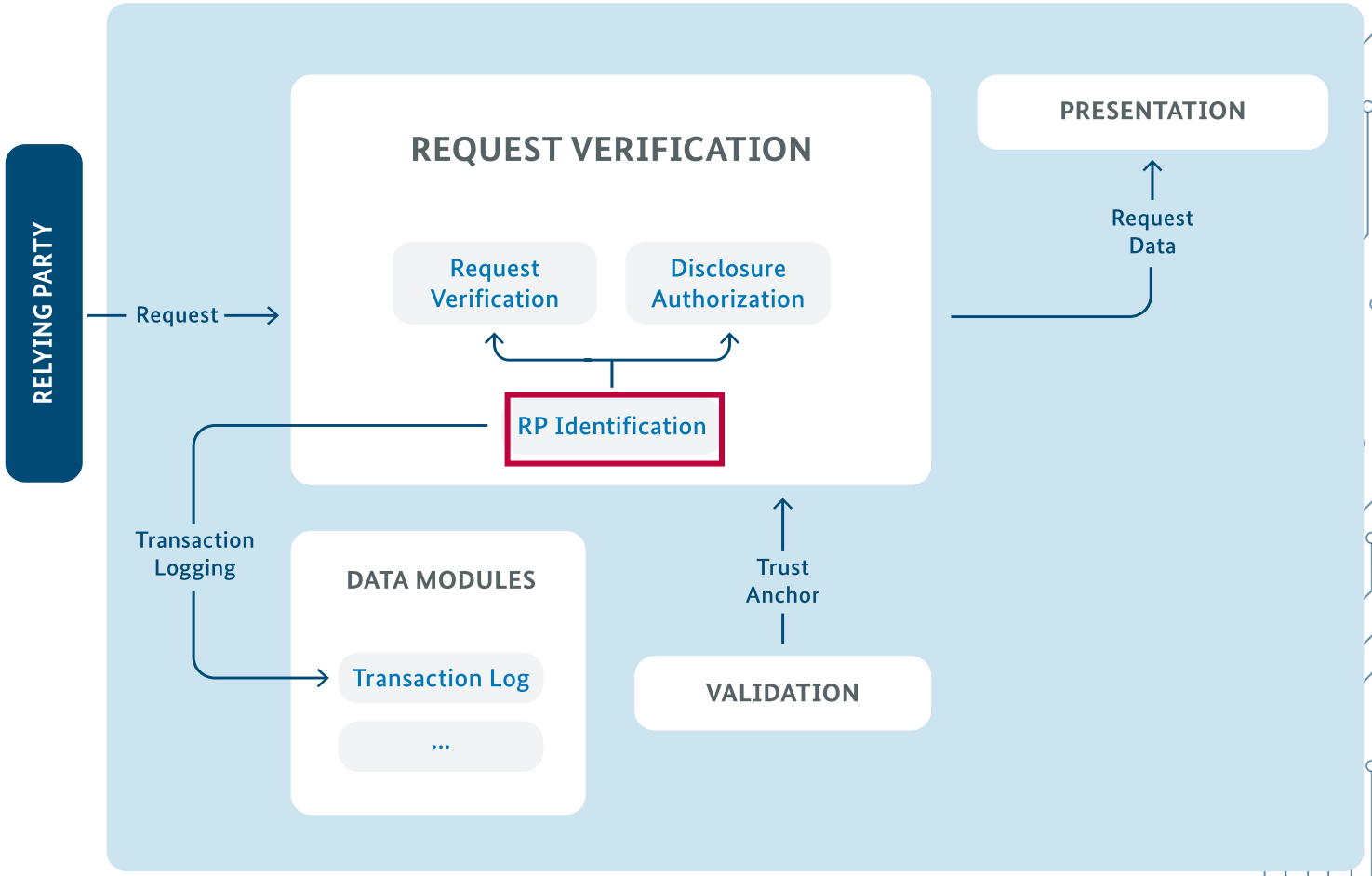


Beispiel 1: RP Identifizierung

Präsentationen von PID und Nachweisen

- Bedrohung: „TR26 – PID, (Q)EAAs oder Pseudonyme können einem **falschen** vertrauenden Beteiligten **vorgewiesen** werden.“

- Ziel: „Das RP-Identification Modul MUSS die RP aus der Präsentationsanfrage **identifizieren**.“



Beispiel 1: RP Identifizierung

Präsentationen von PID und Nachweisen

- Bedrohung: „TR26 – PID, (Q)EAAs oder Pseudonyme können einem **falschen** vertrauenden Beteiligten **vorgewiesen** werden.“

- Ziel: „Das RP-Identification Modul MUSS die RP aus der Präsentationsanfrage **identifizieren**.“

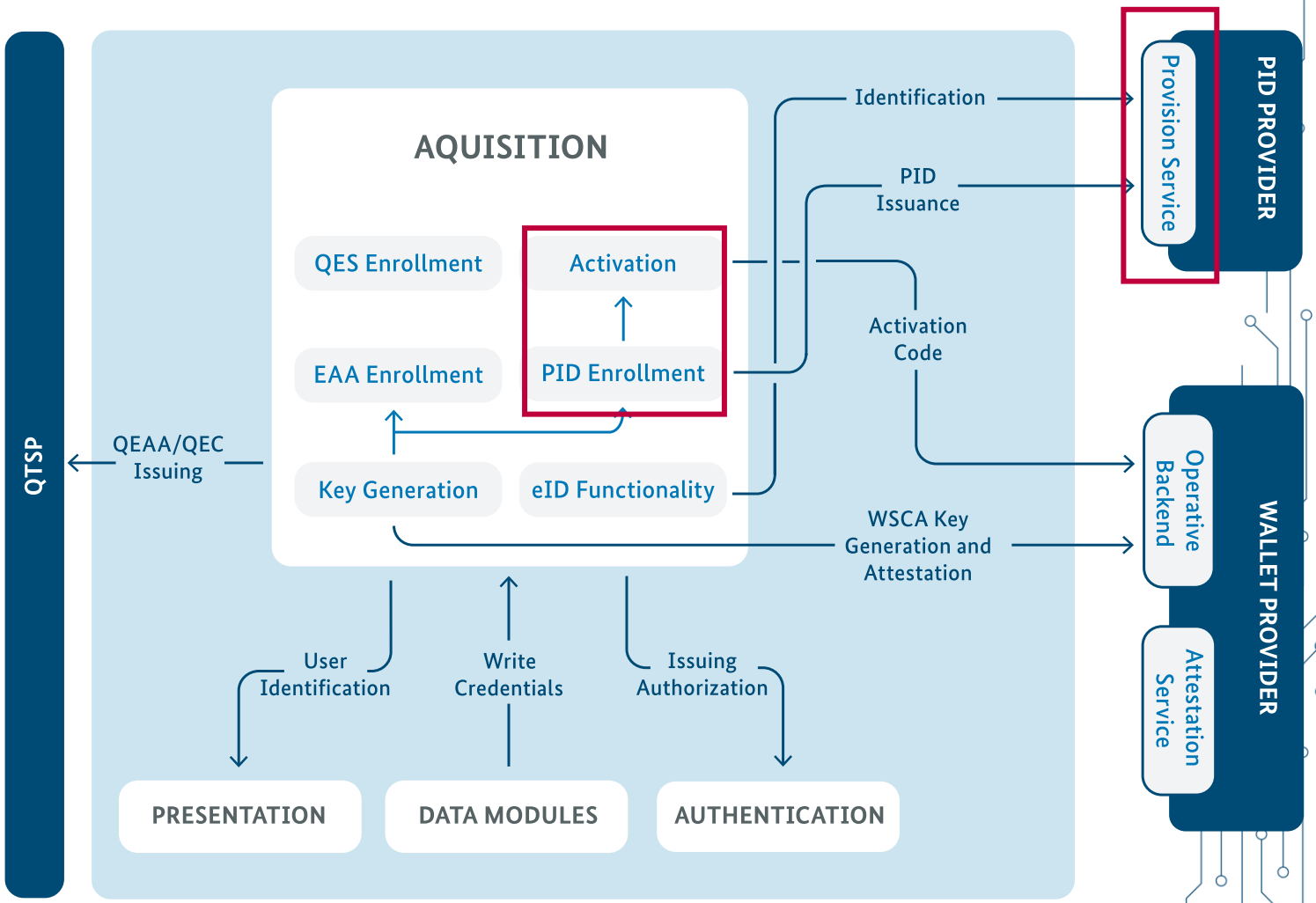
- Anforderung: „...MUSS das **Zugriffszertifikat validieren**.“
  - „…MUSS die **Präsentationsanfrage ablehnen** sofern die Validierung fehlschlägt.“

Beispiel 2: PID Acquisition

Personalisierung der Wallet

- Bedrohung*:* „TR12 – Ein Angreifer kann die **Überprüfung durch den PID-Anbieter**, ob die Brieftasche von ihrem Nutzer kontrolliert wird, umgehen und PID an eine **beeinträchtigte, vom Angreifer kontrollierte Brieftasche** ausstellen lassen.“

- Ziel*:* „Das PID Enrolment Modul MUSS dem PID-Provider die **Nachweise** über die **Gültigkeit der Wallet Unit** und der **Schlüssel im Besitz des Nutzers** übermitteln.“
  - Konkretisierung in Anforderungen*,* bspw. hier durch Nennung der tatsächlichen „Assets“ (WUA, Key Attestation)



Erreichbare Sicherheit und Reichweite

Risiko-Akzeptanz

- Wallet als App in einer mobilen „ungeprüften“ Umgebung
  - eIDAS fordert LoA high

- Verlässlichkeit und Risiko-Abwägung
  - Hardware vs Software
  - Technische/kryptographische Prüfung vs organisatorische Limitierung
  - Annahmen vs Anforderungen
  - Umsetzbarkeit der Maßnahmen
  - …

Kommentierung zur Wallet TR

BSI Technische Richtline 03189

- Erstellung einer TR für das Zertifizierungsschema mit Anforderungen insbesondere an:
  - Wallet
  - Wallet Provider
  - PID Provider
- Aktuell 7 Teile (+ Annex): z.B. Lebenszyklus, WSCA/D, Ökosystem & Vertrauensmodell, …

- Aktuelle Kommentierungsrunde läuft noch bis zum **30.01.26**
- Zukünftig auch weitere Kommentierungsrunden geplant

- Anmeldung über DIF AG eID Verteiler: **dif-eid@bsi.bund.de**

Vielen Dank für Ihre Aufmerksamkeit!

Nils Michael
Referat D12

nils.michael@bsi.bund.de
Tel.: +49 (0) 228 9582 5086
Mobil: +49 151 – 54 61 37 42

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

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: