

eIDAS Certification in Germany

at 12th edition of ENISA Trust Services and eID Forum

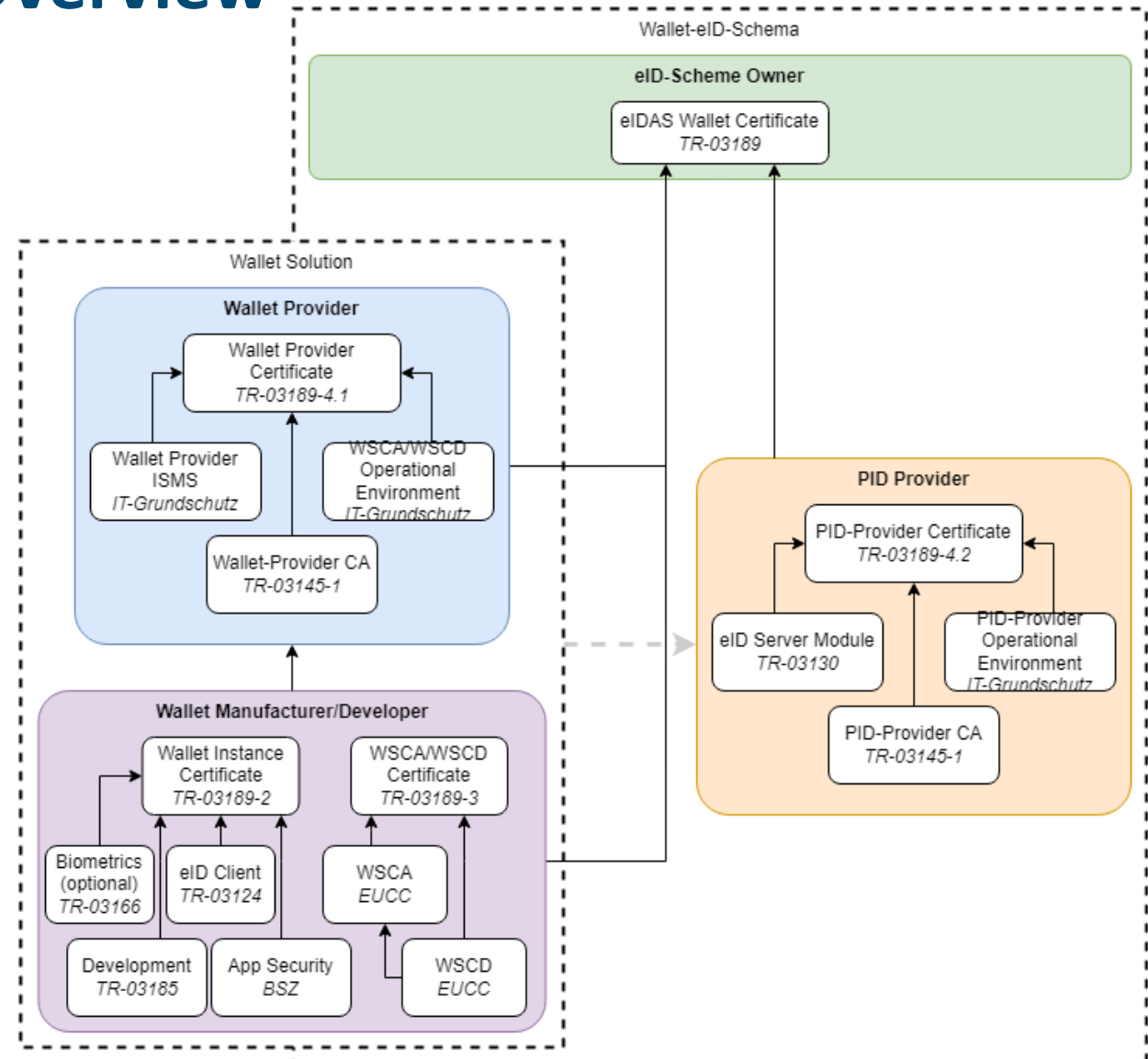


Bundesamt
für Sicherheit in der
Informationstechnik

German Certificate Scheme - Overview

Sub-Certificates in the TR-03189

- **General:** *TR-03189-“1”, -2, -3, -4.1, -4.2*
- **eID-means and LoA:** *TR-03107* (DE application of *CIR 2015/1502*)
- **ISMS:** *IT-Grundschutz* (DE application of *ISO 27001*)
- **Identification:** *TR-03124* (eID-Client) and *TR-03130* (eID-Server) (PZS-TR)
- **PKI and CA:** *TR-03145* (MZIP-TR)
- **Secure Software Development Lifecycle:** *TR-03185* (based on *IT-Grundschutz*)
- **WSCA/WSCD:** *EUCC*
- **Wallet Instance/App:** *BSZ* (DE application of *FITCEM*)
- **MDVM:** *BSZ* (planned)
- **Biometrics:** *TR-03166*



German Certificate Scheme - Profiles and Extensibility

Different architectures and integration into new schemes

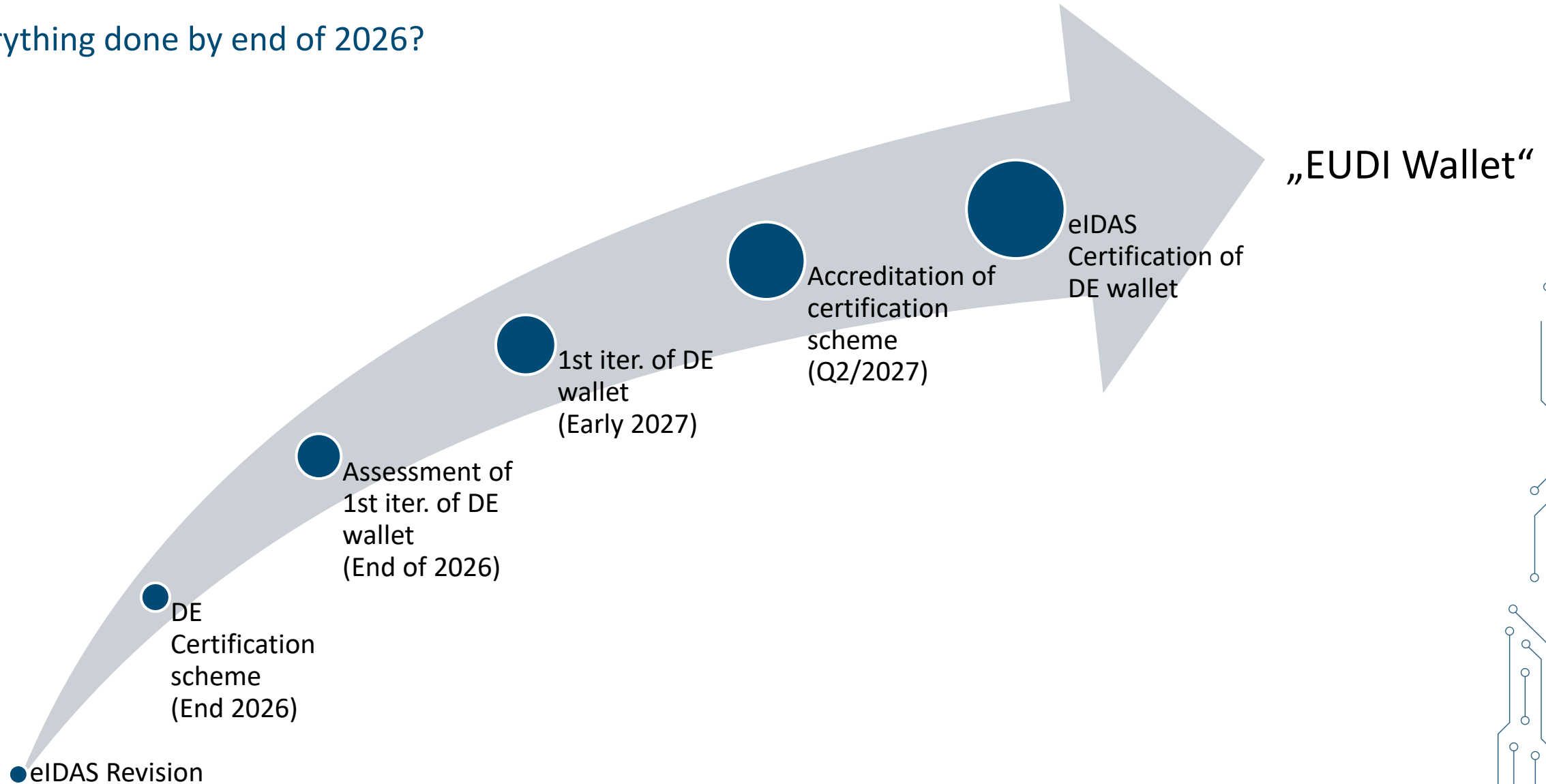
- First certification scheme targeted for german national wallet
 - HSM Backend solution
 - Enrollment based on german eID Card
 - Reliance on certification schemes established in germany (BSZ, IT-Grundschutz, etc.)
- Support of different systems planned in the future
 - New architectures (Secure Elements, external tokens, etc.)
 - New eID Schemes and enrollment mechanisms
 - Applicability of other existing certification programs (e.g. CSPN or other national certifications)

→ Usage of different **profiles** for new architectures and schemes

- Each profile describes a certification scheme
 - Defines the applicable requirements (utilizing a shared catalogue) and sub certificates
 - Each profile described in it's own TR (part) and requires new accreditation

Status and What comes next?

Is everything done by end of 2026?



Open Challenges

- ...
- Finalize certification scheme, submit it to EUDICG and complete accreditation
- Finalize German national wallet (following incremental approach → PID and (Q)EAA in the beginning of 2026)
- Finally: Carry out complete eIDAS compliant certification of complete national Wallet

BUT: What about national and cross border usage etc. until this is all done??

Thank you!

Dr. Felix Bleckmann

Head of Division D12 - eID Components und Sovereign Documents

E-Mail: felix.bleckmann@bsi.bund.de

Federal Office for Information Security

Godesberger Allee 87

53175 Bonn



Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:





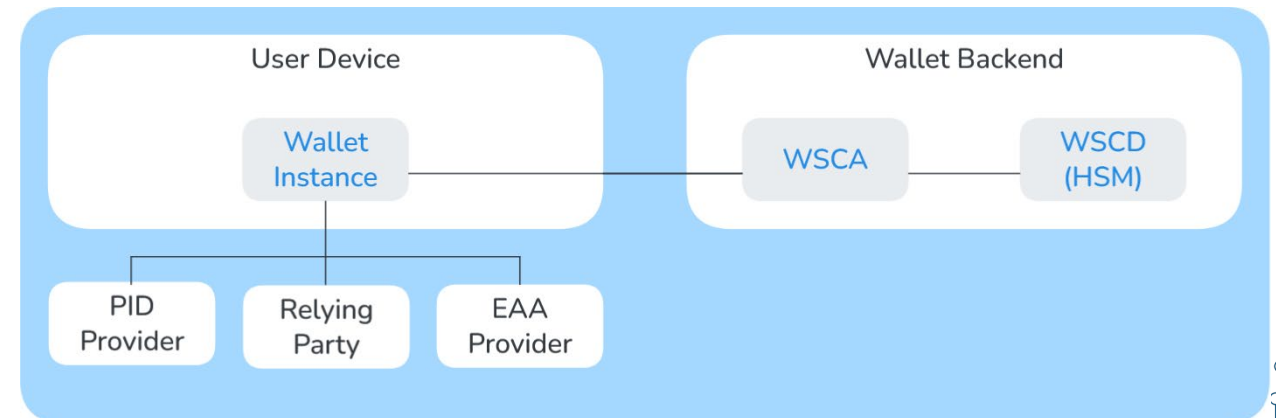
German national Certification System

TR Product Certification for BSI TR-03189

- Main Document: BSI TR-03189 with multiple parts
- Certification based on „Produktzertifizierungssystem Technische Richtlinie“ (PZS-TR)
 - BSI as Certification Body accredited by NAB for each TR individually
- „Checklist“ evaluation for conformance test based on test specification
 - Not feasible for cyber security evaluation
 - Requiring additional certificates (EUCC, BSZ/FITCEM, ISO 27001) to cover the gaps
 - Other involved PZS programs involved: TR-03124, TR-03130, TR-03166
- Special case: TR certification for Management Systems (MZP-TR)
 - No formal underlying certification system (e.g. no accreditation under ISO 17065)
 - Still used in national certification, e.g. TR-03145

Coverage of TR-03189

- Provides **eIDAS-complete (functional and cybersecurity) conformity assessment**
- Component Modularization according to required eIDAS functionality (partly in line with CEN Decomposition)
- **Part-2:** Wallet Instance -> Product certification
- **Part-3:** WSCA/WSCD -> Product certification
- **Part-4.1:** Wallet Provider
 - ISMS/Management certification: *Lifecycle Management, Development, Provisioning and operative Backend*
 - Product certification: *Mobile Device Vulnerability Management and Wallet (Unit) Attestation service*
- **Part-4.2:** PID-Provider -> ISMS/Management certification



eID-Scheme: Integration and Re-Evaluation

Private Wallets and Wallets with different Architecture Profiles

- Overarching certificate maps **one eID-Scheme** to (possibly **multiple**) **Wallet Solutions**
- Additional Wallet Solutions within the eID-Scheme, or interchanging components within a Wallet Solution or even the eID-Scheme, requires the **issuance of a new overarching certificate**
 - **Certification overhead is minimal** as existing certificates for unaltered components can be re-used
 - Certificate of conformity of the new components via sub-certificates as well as verification of the integration in the overarching scheme via „entity-certificates“ (Wallet- and/or PID-Provider) are needed
 - E.g., in case of PID, **existing PID-Provider certificate can be re-used** for other (private) Wallet-Providers within the scheme
- Additional architecture (profiles) as well as the ENISA CSA Scheme can be added or interchanged with existing components or certification programs
 - This includes **expanding to other member states** as well

