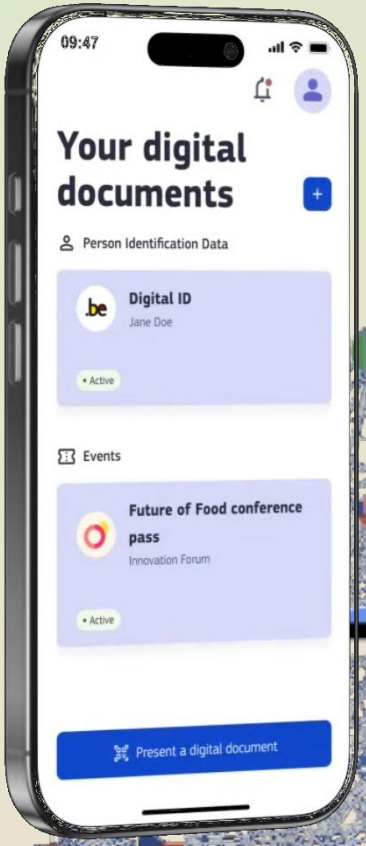
ID-Wallet im Smartphone



Was ist das große Problem wenn unsere Verwaltungen in unserer bunten Republik Deutschland kein Papier mehr verwenden ?

Authentizität

Begriffe eIDAS

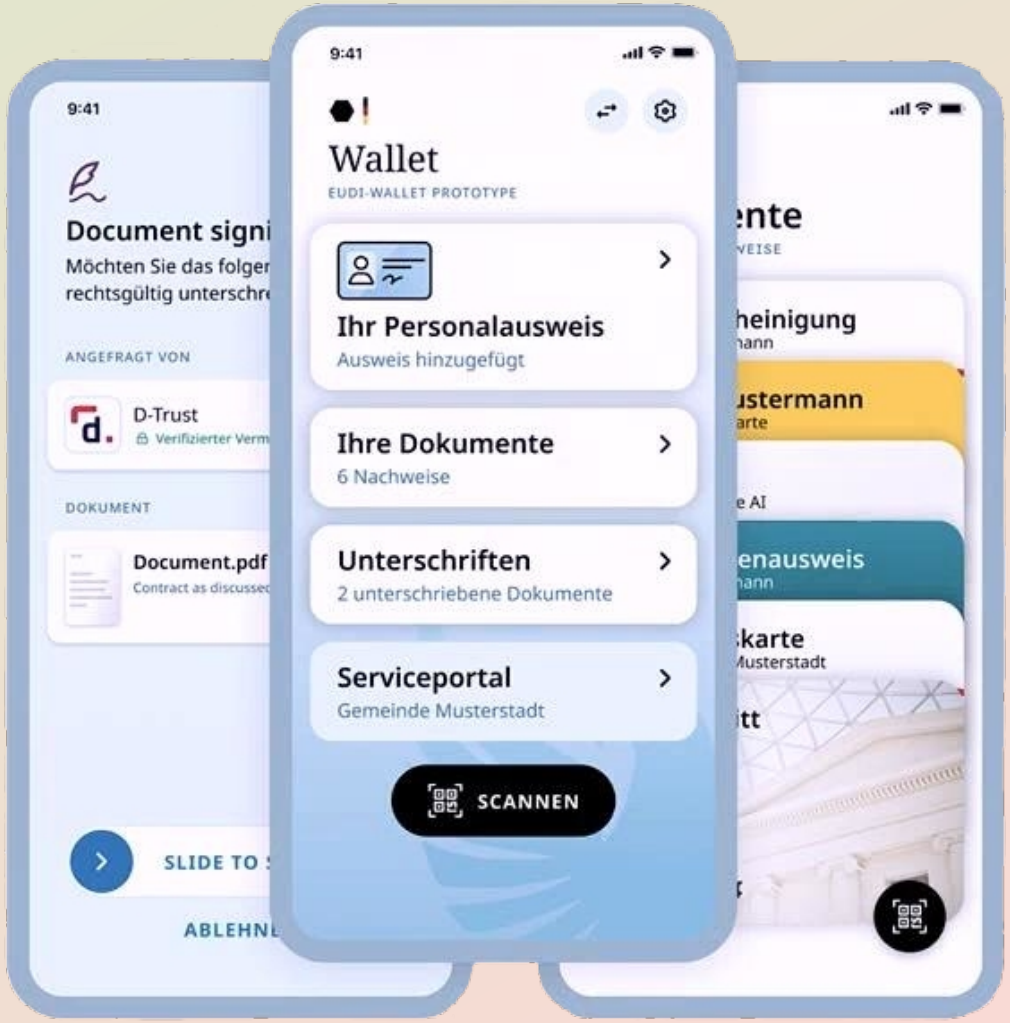
- eIDAS
  - eID
- eIDAS2
  - EUID-Wallet
  - Sicherer Dokumentaustausch

- eIDAS Electronic Identification, Authentication and Trust Services
- eIDAS elektronische Identifizierung und Vertrauensdienste
- Wallet Secure Cryptographic Device (WSCD)
- Electronic Attestations of Attributes (EAA)
- Qualified Electronic Attestations of Attributes (QEAA)
- Non-Qualified Electronic Attestations of Attributes (EAA)
- Public Electronic Attestations of Attributes (PuB-EAA)
- SAML 2.0 (Security Assertion Markup Language]

Situation heute

Ziel


BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
LZ6311T47
MUSTERMANN
GABLER
ERIKA
12.08.1983 DEUTSCH
BERLIN
31.10.2031
38568


9:41
Document signi
Möchten Sie das folger
rechtsgültig unterschr
ANGEFRAGT VON
D-Trust
DOKUMENT
Document.pdf
Contract as discussed
SLIDE TO
ABLEHNE
9:41
Wallet
EUDI-WALLET PROTOTYPE
Ihr Personalausweis
Ausweis hinzugefügt
Ihre Dokumente
6 Nachweise
Unterschriften
2 unterschriebene Dokumente
Serviceportal
Gemeinde Musterstadt
SCANNEN
ente
heinigung
ustermann
e AI
enausweis
skarte
Musterstadt
tt


9:41
Personal data
Age in years
41
Birth year
1984
Age equal or over
12 Age In Years: Yes
14 Age In Years: Yes
16 Age In Years: Yes
18 Age In Years: Yes
21 Age In Years: Yes
65 Age In Years: No
Authority
DE
Issuing country
Deutschland
Created at
14. Oct 2025
Valid until
28. Oct 2025

EUDI Wallet Prototypen
6 von 17

Reference Wallet Implementation

The open-source reference wallet implementation paid for by the European commission.

Explore >

Lissi Wallet

Wallet of Lissi GmbH, participant in the German EUDI Wallet Challenge.

Explore >

iGrant Data Wallet

iGrant's Wallet for natural persons used within the EWC LSP.

Explore >

Paradym Funke Wallet

Animo's Wallet developed for the Funke Wallet Challenge.

Explore >

wwWallet Funke

Sunet's Wallet developed for the German EUDI Wallet Challenge.

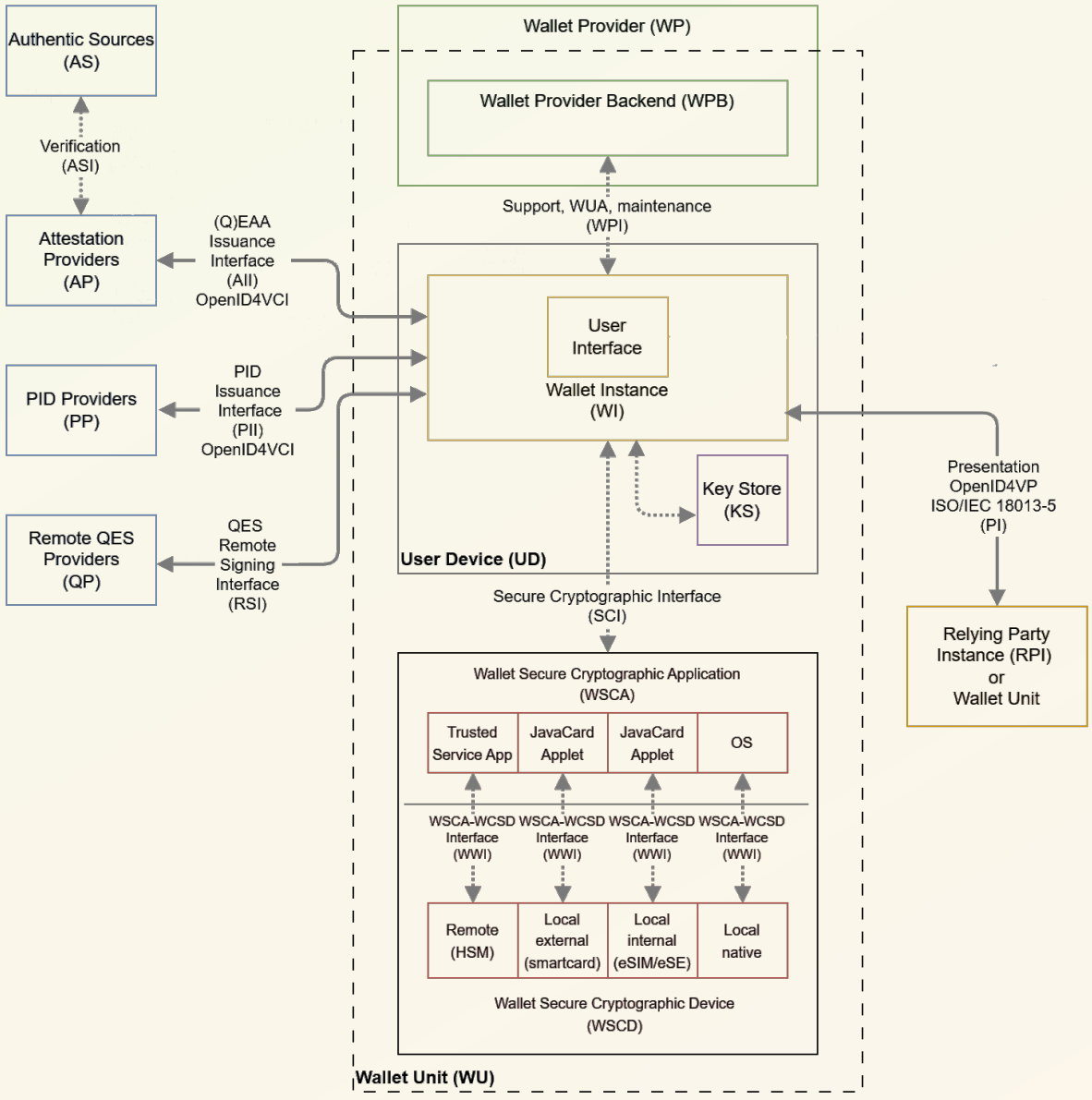
Explore >

Valera Wallet

Wallet Prototype from A-Sit Plus GmbH for the POTENTIAL Playground.

Explore >

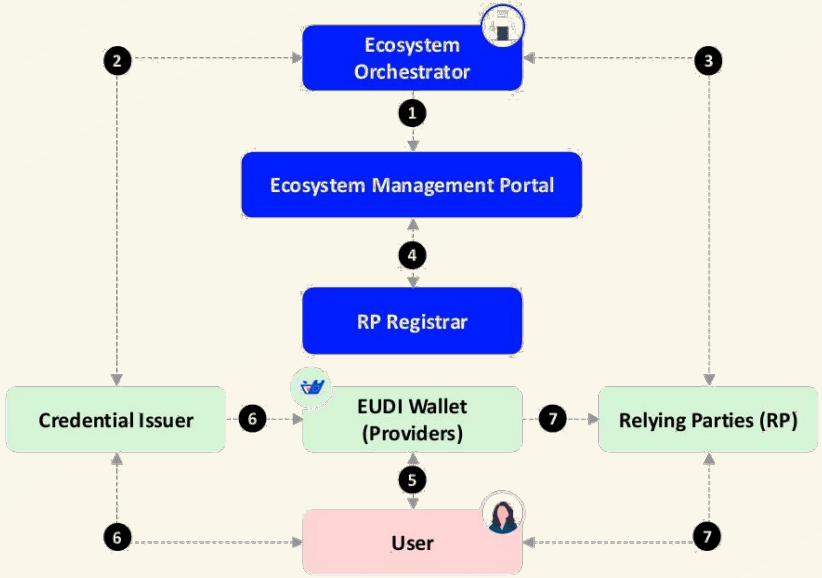

BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
LZ6311T47
MUSTERMANN
GABLER
ERIKA
12.08.1983 DEUTSCH
BERLIN
31.10.2031
38568


Authentic Sources (AS)
Verification (ASI)
Attestation Providers (AP)
(Q)EAA Issuance Interface (AII) OpenID4VCI
PID Providers (PP)
PID Issuance Interface (PII) OpenID4VCI
Remote QES Providers (QP)
QES Remote Signing Interface (RSI)
Wallet Provider (WP)
Wallet Provider Backend (WPB)
Support, WUA, maintenance (WPI)
User Interface
Wallet Instance (WI)
Key Store (KS)
User Device (UD)
Secure Cryptographic Interface (SCI)
Wallet Secure Cryptographic Application (WSCA)
Trusted Service App
JavaCard Applet
JavaCard Applet
OS
WSCA-WCSD Interface (WWI)
WSCA-WCSD Interface (WWI)
WSCA-WCSD Interface (WWI)
WSCA-WCSD Interface (WWI)
Remote (HSM)
Local external (smartcard)
Local internal (eSIM/eSE)
Local native
Wallet Secure Cryptographic Device (WSCD)
Wallet Unit (WU)
Presentation OpenID4VP ISO/IEC 18013-5 (PI)
Relying Party Instance (RPI) or Wallet Unit

EUID-Schema mit Orchestrator

SPRIN-D

THE ECOSYSTEM MANAGEMENT PORTAL PLAYS A CENTRAL ROLE IN THE ROLLOUT OF THE ECOSYSTEM



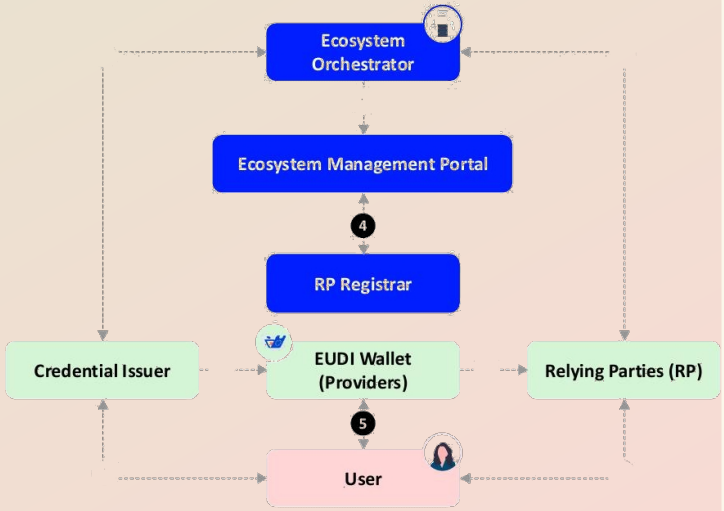
1. The Ecosystem Orchestrator is responsible for the Ecosystem Management Portal and operates it
2. All credential issuers, such as driver's license issuers, register and identify themselves in the Management Portal in order to be able to issue credential to the EUDI Wallet
3. All relying parties (e.g., banks or public authorities) register and identify themselves in the portal in order to obtain certificates that allow them to retrieve attestations from the EUDI Wallet
4. As the central supervisory authority, the RP Registrar can use the portal to check registration and access certificates and revoke them if necessary
5. Users select their EUDI Wallet provider, in whose wallet app they wish to store and manage their credentials
6. At the user's request, credential issuers issue the desired credentials to the selected wallet, e.g., educational qualifications or a health insurance card
7. At the user's request, the EUDI Wallet transfers evidence to relying parties, e.g., personal identification data when opening a bank account

EUID-Schema mit Orchestrator

Server PID Provider

Quelle n Papierchaos

EAA oder PID Provider



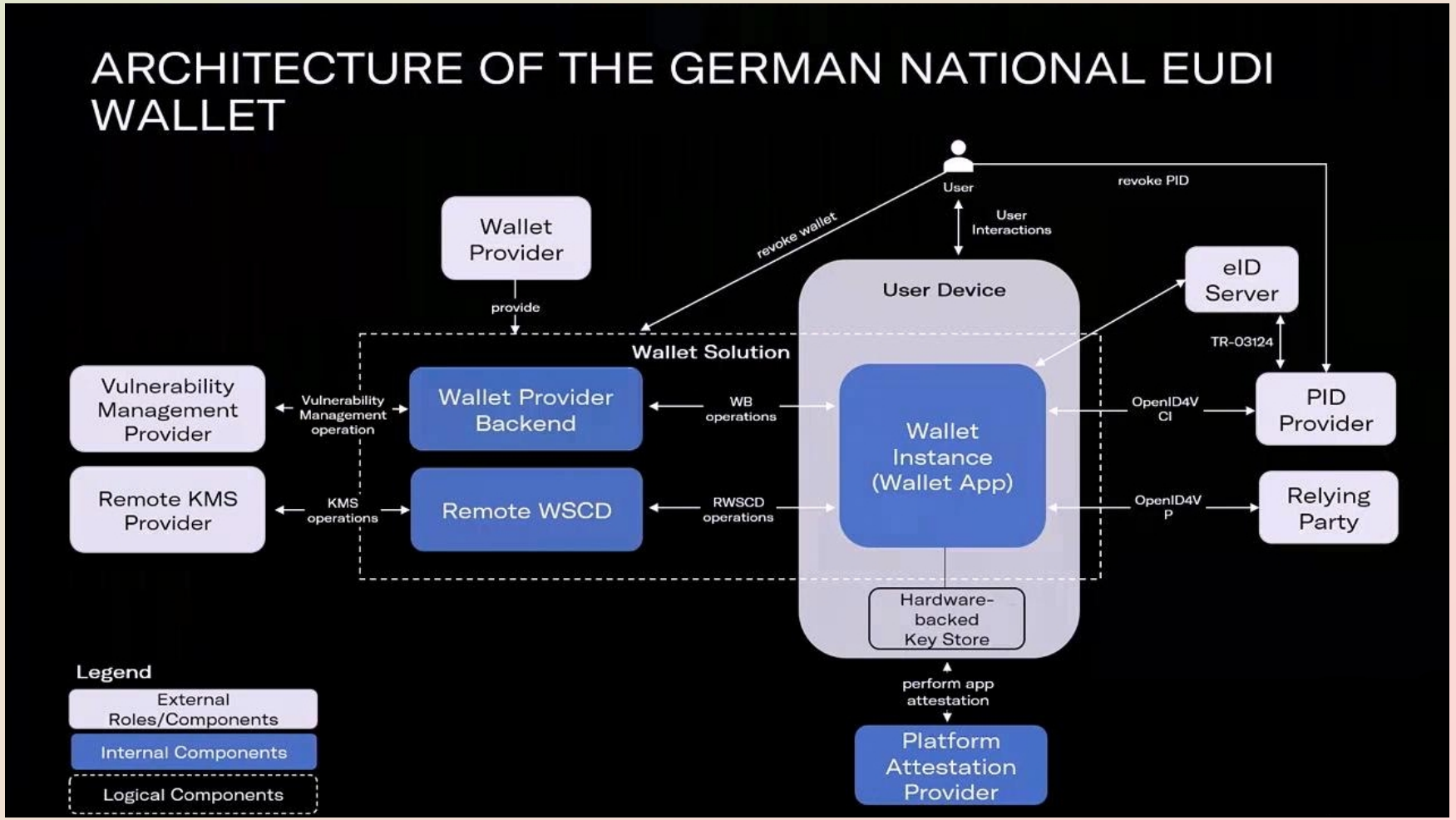
Server DRV

Server n

RP Relying Party

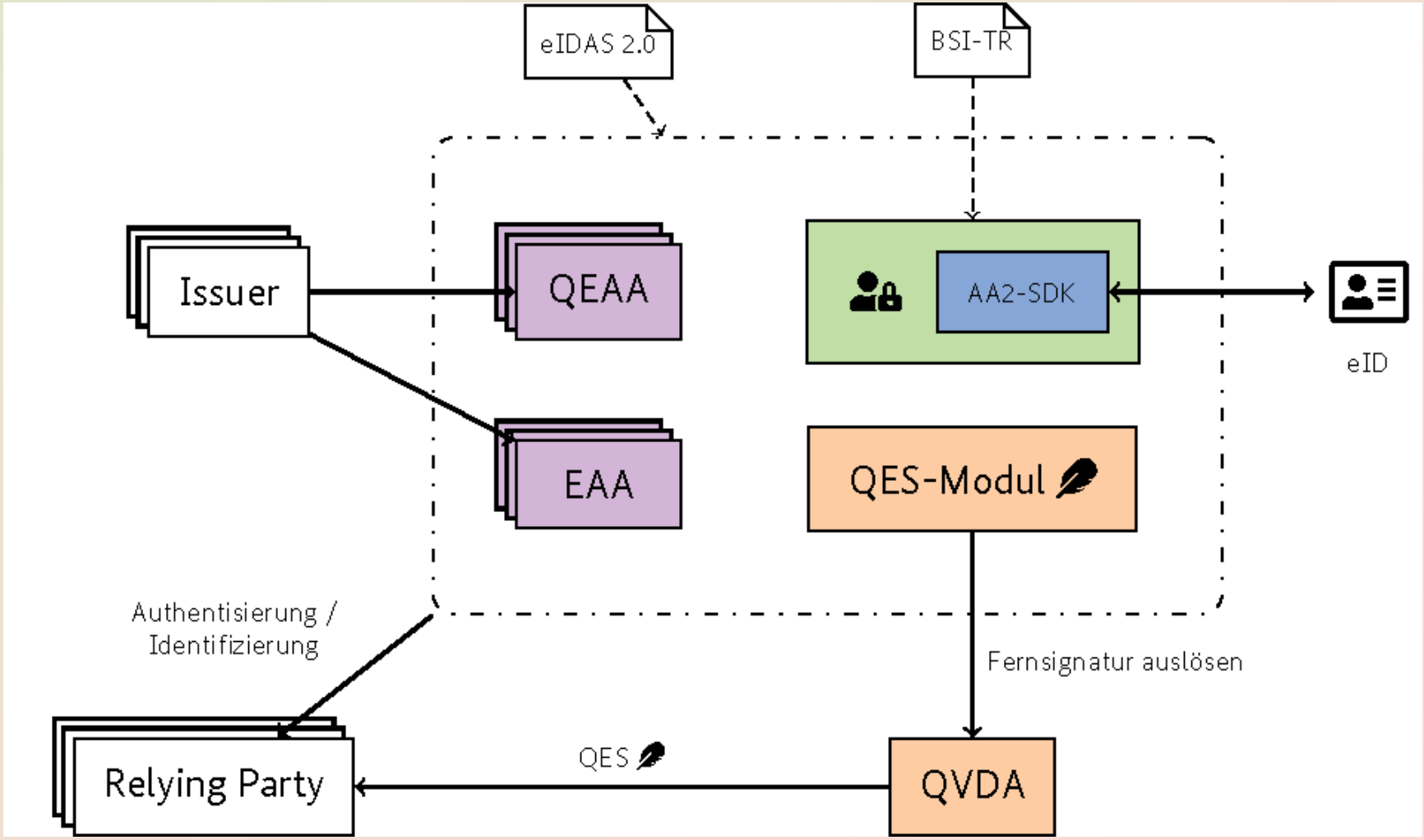
Schema


BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
LZ6311T47
MUSTERMANN
GABLER
ERIKA
12.08.1983 DEUTSCH
BERLIN
31.10.2031
38568

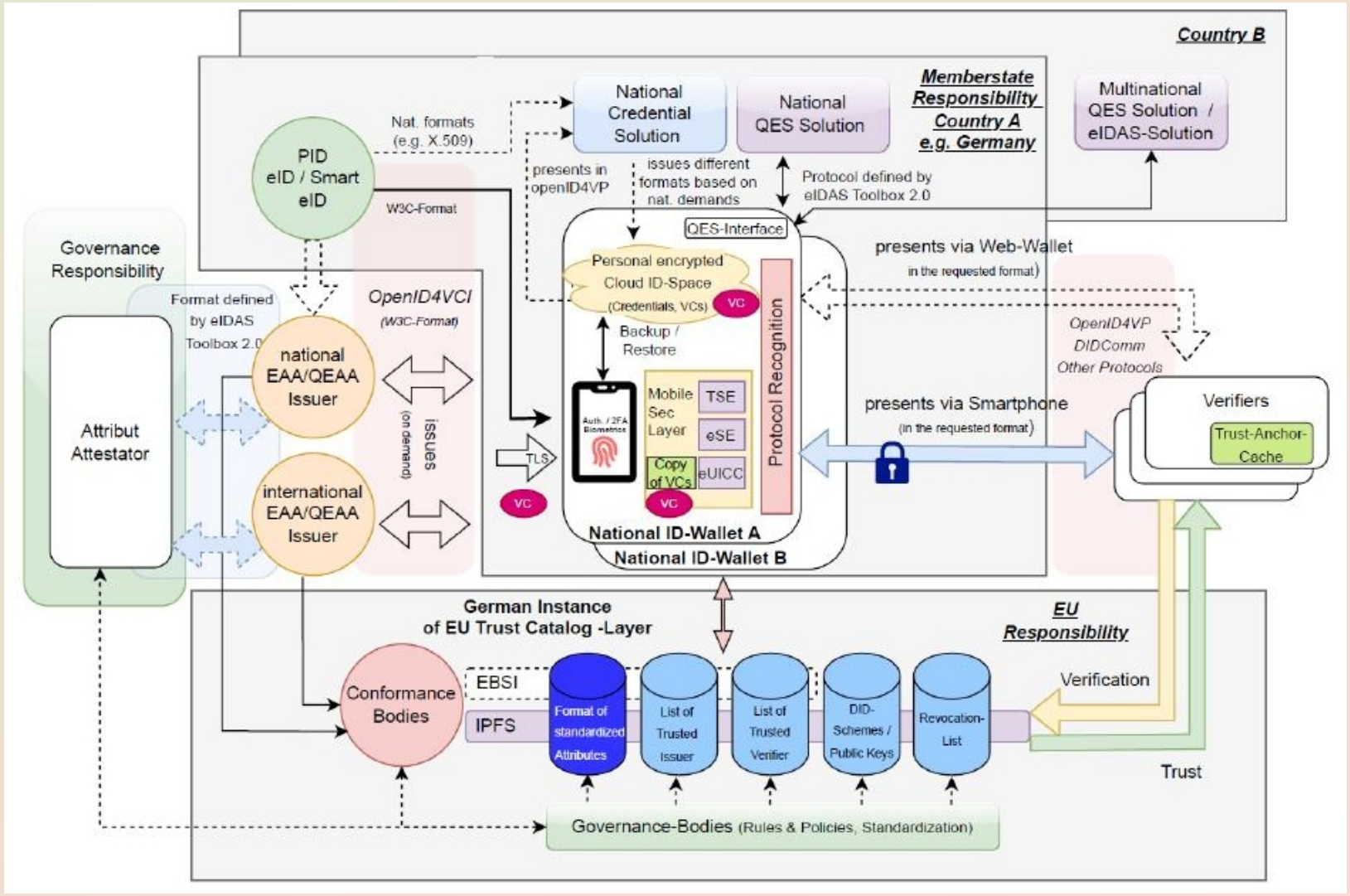

ARCHITECTURE OF THE GERMAN NATIONAL EUDI WALLET
User
revoke PID
User Interactions
Wallet Provider
revoke wallet
provide
User Device
eID Server
Wallet Solution
TR-03124
Vulnerability Management Provider
Vulnerability Management operation
Wallet Provider Backend
WB operations
Wallet Instance (Wallet App)
OpenID4VCI
PID Provider
Remote KMS Provider
KMS operations
Remote WSCD
RWSCD operations
OpenID4VP
Relying Party
Hardware-backed Key Store
perform app attestation
Platform Attestation Provider
Legend
External Roles/Components
Internal Components
Logical Components

Schema


BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
LZ6311T47
MUSTERMANN
GABLER
ERIKA
12.08.1983 DEUTSCH
BERLIN
31.10.2031
38568


eIDAS 2.0
BSI-TR
Issuer
QEAA
EAA
AA2-SDK
eID
QES-Modul
Authentisierung /
Identifizierung
Fernsignatur auslösen
Relying Party
QES
QVDA

Vorschlag Deutsche Telekom



Arbeitsmethodik

PRIVACY & SECURITY (PS) + AGILITY & ADAPTABILITY (AA) + OPEN & TRANSPARENCY (OT) +

DIGITAL & USER-CENTRICITY (DU) + SCALING & ORCHESTRATION (SO) +

PUBLIC & PRIVATE (PP)

=

SUCCESSFUL EUDI WALLET ECOSYSTEM IN GERMANY

Open Source Bibliotheken

How you can use what we built

ANIMO

- Animo EasyPID / Funke Wallet
- Animo Funke Playground

Open Wallet Foundation Projects

- Credo - TypeScript framework to build verifiable credential based solutions
- OpenID4VC - Low level OpenID4VCI / OpenID4VP implementation in TypeScript
- DCQL - TypeScript implementation of the DCQL query language
- OpenID Federation - TypeScript implementation of OpenID Federation

More lower level libraries

- Expo mDOC Data Transfer - React Native library for in-person proximity presentation of mDOCs
- Expo Digital Credentials API - React Native library to add support for W3C Digital Credentials API
- Expo Secure Environment - React Native library to integrate with iOS and Android Secure Element
- EUDI Wallet Functionality - EUDI specific extensions for Credo (e.g. RP A&A)
- mDOC - TypeScript implementation of mDL/mDOC specification

Other

- Animo EUDI Wallet SDK (early Alpha) - A Typescript SDK for building cross-platform Wallet applications in React Native

Bibliotheken/Libraries

```
Programm-Header:
  Typ             Offset             VirtAdr            PhysAdr
                  DateiGr            SpeiGr              Flags  Ausr.
  PHDR            0x0000000000000040 0x0000000000000040 0x0000000000000040
                  0x00000000000002d8 0x00000000000002d8  R      0x8
  INTERP          0x0000000000000318 0x0000000000000318 0x0000000000000318
                  0x000000000000001c 0x000000000000001c  R      0x1
  LOAD            0x0000000000000000 0x0000000000000000 0x0000000000000000
                  0x000000000002e188 0x000000000002e188  R      0x1000
  LOAD            0x000000000002f000 0x000000000002f000 0x000000000002f000
                  0x00000000000def6d 0x00000000000def6d  R E    0x1000
  LOAD            0x000000000010e000 0x000000000010e000 0x000000000010e000
                  0x0000000000039b08 0x0000000000039b08  R      0x1000
  LOAD            0x0000000000148a90 0x0000000000149a90 0x0000000000149a90
                  0x000000000000bbc0 0x0000000000016b28  RW     0x1000
  DYNAMIC         0x000000000014b4c0 0x000000000014c4c0 0x000000000014c4c0
                  0x0000000000000200 0x0000000000000200  RW     0x8
ldd /bin/bash
     linux-vdso.so.1 (0x00007fff2d13d000)
     libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007f751e955000)
     libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f751e72c000)
     /lib64/ld-linux-x86-64.so.2 (0x00007f751eb20000)
ldd /usr/bin/busybox
     Das Programm ist nicht dynamisch gelinkt

ldd /usr/bin/gocryptfs
     linux-vdso.so.1 (0x00007ffc50dda000)
     libcrypto.so.3 => /lib/x86_64-linux-gnu/libcrypto.so.3 (0x00007f8bcaf6d000)
     libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f8bcad44000)
     /lib64/ld-linux-x86-64.so.2 (0x00007f8bcb3e9000)
```

DCQL Abfragesprache

The new **query language (DCQL)** supports a variety of use cases

PID
Issuer A

+

Certificate of Residence
Issuer B

+

Tax ID
Issuer C

PID
Issuer A

or

PID
Issuer B

Certificate of Residence
Issuer B

- First Name
- Last Name
- Address

or

- First Name
- Last Name
- Mailbox

Multiple Credentials

As a verifier request multiple credentials at once

Credential Sets

Define alternative credential combinations that fulfill the same request

Claim Sets

Define different options that allow for optional claims

Anwendungsfälle

LSP-RP TESTING

LSP POTENTIAL Use-Case	Team	
Use Case 1: eGov Services	wwWallet	
Use Case 2: Bank Account Opening	Lissi	Animo
Use Case 3: SIM Card Registration	Ubique	Animo
Use Case 4: Mobile Driving License	Animo	
Use Case 5: Qualified eSignature	wwWallet, Lissi, Animo, Ubique	
Use Case 6: ePrescription	Ubique	Animo

German Relying Parties

Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen

COMMERZBANK · ING · Deutsche Bank · Finanzgruppe Deutscher Sparkassen- und Giroverband

T · vodafone · Telefónica

LAPID · AMADEUS · SIXT · VOLKSWAGEN FINANCIAL SERVICES · enterprise

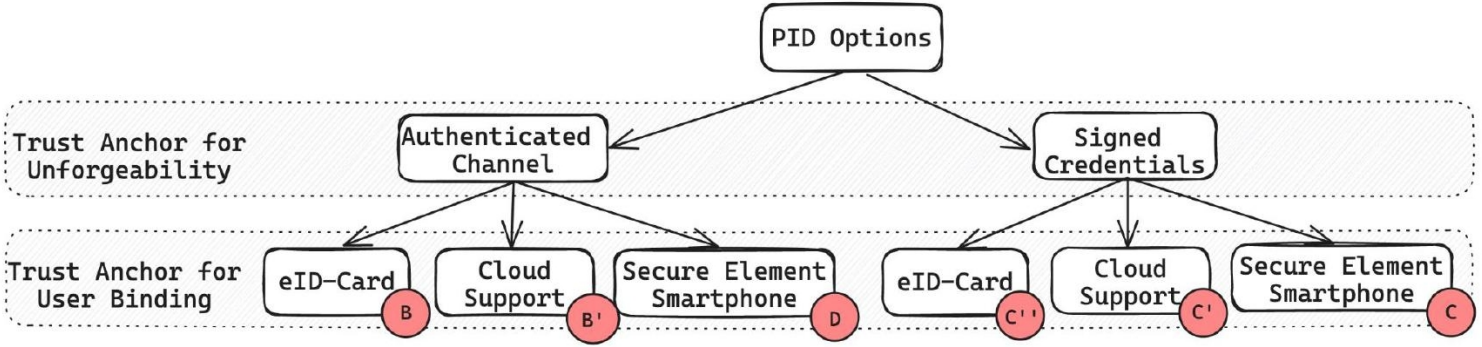
d-trust.

Redcare PHARMACY

Sicherheitselemente

SPRIN-D

WALLET ARCHITECTURE PROPOSES 6 DIFFERENT OPTIONS HOW TO REALIZE THE PID FOR THE GERMAN EUDI WALLET



- Options differ in regard to **(Non-)repudiation**, **cryptographic key storage and architecture design**
- All PID design options will be implemented and tested in the FUNKE Challenge

Sicherheitselemente

- Mikrochips
  - rfid Chip im ePerso
  - rfid Chipkarten
  - tpm Module in Laptops
  - eSIM Module in Smartphones
  - usb Dongle
- HSM Boxen an Servern
- multicompute Party (online)

aber Geräte müssen damit ausgestattet sein und es sind immer Treiber erforderlich

Viele Interessenten

Gefahr Overasking

Orchestrator legt fest was RPs abfragen dürfen und blockiert weitere Abfragen

erreichbar bis ende 2026

PART3: TRUSTING A RELYING PARTY

How Credential Presentation Works in Practice

Invocation

1. Relying Party prepares a credential request and renders it on its website
2. User invokes the wallet by clicking a link or scanning a QR code

Show credential

Request

3. Wallet retrieves and validates the request before any data is shared
4. User is asked for consent to present the requested credential(s)

Presentation & Validation

5. Wallet constructs and sends the response
6. Relying Party validates the response

At no point, data is shared automatically – each step is controlled by the user and the wallet.

erreichbar bis ende 2026

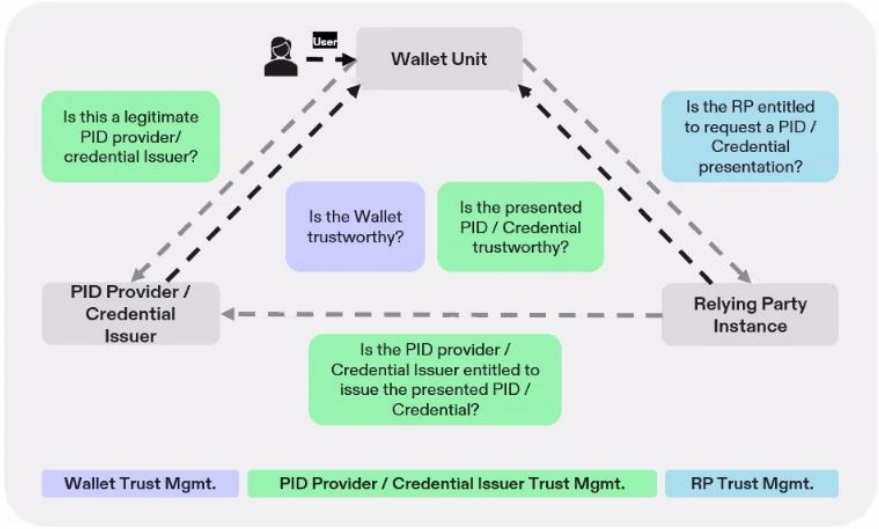
PART3: TRUSTING A RELYING PARTY

Trust is Created Through Complementary Decisions by Issuer, Holder, and Verifier

ISSUER
Entity that creates & issues the PID credential
Do I trust the wallet & credential enrollment?

HOLDER
User who stores the PID in their wallet
Do I trust the Relying Party?

VERIFIER
Relying Party that receives the presentation
Do I trust the presented credential?



und die Daten Seite ???

Kryptographie Grundlagen

- symmetrische Kies
- asymmetrische Kies
- hasche
- Zufallszahlengeneratoren
- Schlüsselprozeduren
- Verschleierungen
- zero knowledge proofs
- Verkettungen
- token
- Blockchains
- Schlüsselhärte
- pubkey Signaturen
- secure elemente

Kryptographie Probleme

- Der Mensch ist das größte Sicherheitsproblem denn
  - komplexe Phrasen merken fällt schwer
  - nur wenige Phrasen werden erinnert
  - verwendet immer die gleichen Phrasen
  - verwendet zu einfache Phrasen
- Schlüsselsicherung
- Benutzerfreundlichkeit
- Benutzerakzeptanz

SSH Keyauth

```
ich@sys01 uname -a
Linux sys01 5.15.0-143-generic #153-Ubuntu SMP Fri Jun 13 19:10:45 UTC 2025 x86_64 GNU/Linux

ich@sys01$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCp7ULPwS6KxvJZYTW8n6O84Suaqr5J8Vr1PA/
2Zbx0FROlzSdSeWbb1D9QC615WrFps49DOAO9WVpz7Mr+QplOfdqQySlFlWIfnUbb5yecYZhvOMXmHPkwktgM6MSCHQr7Tr
IwbdFnJTkHNluyV7qtvShykmXRD7ZgsNN7S6g/z6KDmhJy/aVKzb+Zt4pb5ps7wGo0Kmdb7MuktXdNfK49m/
Xl+T7S4nssx8XXCQOPCW1+ICM08EQHxo0PN17/5IES/Lv227/a+MBzbnXC7LG968RyX8/XNTespFgegg+WSUH9
CtBqGeyzZ6AMdunh03L3za1gcPnY3A844XMQjTBi6rC3XKqOFHDl+ZdfLbwjevNAWp+e7QGAgcD5c50jY8NPDit/
y2OeF3+0abb5ciwY/IwD0OtZURuLjRCZ2OJp5lo5sCFwriTYUroEwsa+bu+Ue9JxMPzRfz8ohzXNVB7Hob
1hQgsazQ8j0g6KjkgxAu4RGcIwUtNpwJpnO5fJehYyUVXogclFrJES2RhCLyddtzPdlj3OlaFMac0HJwwJLfyfQnURprq7u
/VEBCWe02PXgxbb5Cao53j6uV2/x1oZFWrU13/wkdayhTGzIJ3PolDGHYDB3l9Huz+xCl/3Xhak
WzflXWsZp3JUVh9d/ZBjxUS8EdiGc6csx41vWrBxwQ== ich@sys01


ich@sys02:~$ uname -a
Linux ubuntu01 5.15.0-174-generic #184-Ubuntu SMP Fri Mar 13 18:41:50 UTC 2026 x86_64 GNU/Linux

ich@sys02:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCp7ULPwS6KxvJZYTW8n6O84Suaqr5J8Vr1PA/
2Zbx0FROlzSdSeWbb1D9QC615WrFps49DOAO9WVpz7Mr+QplOfdqQySlFlWIfnUbb5yecYZhvOMXmHPkwktgM6MSCHQr7Tr
IwbdFnJTkHNluyV7qtvShykmXRD7ZgsNN7S6g/z6KDmhJy/aVKzb+Zt4pb5ps7wGo0Kmdb7MuktXdNfK49m/
Xl+T7S4nssx8XXCQOPCW1+ICM08EQHxo0PN17/5IES/Lv227/a+MBzbnXC7LG968RyX8/XNTespFgegg+WSUH9
CtBqGeyzZ6AMdunh03L3za1gcPnY3A844XMQjTBi6rC3XKqOFHDl+ZdfLbwjevNAWp+e7QGAgcD5c50jY8NPDit/
y2OeF3+0abb5ciwY/IwD0OtZURuLjRCZ2OJp5lo5sCFwriTYUroEwsa+bu+Ue9JxMPzRfz8ohzXNVB7Hob
1hQgsazQ8j0g6KjkgxAu4RGcIwUtNpwJpnO5fJehYyUVXogclFrJES2RhCLyddtzPdlj3OlaFMac0HJwwJLfyfQnURprq7u
/VEBCWe02PXgxbb5Cao53j6uV2/x1oZFWrU13/wkdayhTGzIJ3PolDGHYDB3l9Huz+xCl/3Xhak
WzflXWsZp3JUVh9d/ZBjxUS8EdiGc6csx41vWrBxwQ== ich@sys01
```

x509 Zertifikatskette

```
ich@meiner:~ collect-tls-info -chain www.drv.de:443 | grep -A 1 -i Identifier
            X509v3 Authority Key Identifier:
                8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1
            X509v3 Subject Key Identifier:
                E0:BD:DA:E4:AF:7A:60:82:8E:A1:F1:B4:A2:2F:77:C6:1B:DE:96:6D
--
            X509v3 Authority Key Identifier:
                53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
            X509v3 Subject Key Identifier:
                8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1
--
            X509v3 Authority Key Identifier:
                53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
            X509v3 Subject Key Identifier:
                8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1
--
            X509v3 Authority Key Identifier:
                53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
            X509v3 Subject Key Identifier:
                8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1
```

tls chipher/Chiffren

```
ich@meiner:~ collect-tls-info -qp www.drv.de:443
===== begin ciphertest www.drv.de:443 ===============
TLS_AES_256_GCM_SHA384              failed
TLS_CHACHA20_POLY1305_SHA256        failed
TLS_AES_128_GCM_SHA256              failed
ECDHE-ECDSA-AES256-GCM-SHA384       success
ECDHE-RSA-AES256-GCM-SHA384         success
DHE-RSA-AES256-GCM-SHA384           success
ECDHE-ECDSA-CHACHA20-POLY1305       success
ECDHE-RSA-CHACHA20-POLY1305         success
DHE-RSA-CHACHA20-POLY1305           success
ECDHE-ECDSA-AES128-GCM-SHA256       success
ECDHE-RSA-AES128-GCM-SHA256         success
DHE-RSA-AES128-GCM-SHA256           success
ECDHE-ECDSA-AES256-SHA384           success
ECDHE-RSA-AES256-SHA384             success
DHE-RSA-AES256-SHA256               success
ECDHE-ECDSA-AES128-SHA256           success
ECDHE-RSA-AES128-SHA256             success
DHE-RSA-AES128-SHA256               success
ECDHE-ECDSA-AES256-SHA              success
ECDHE-RSA-AES256-SHA                success
DHE-RSA-AES256-SHA                  success
ECDHE-ECDSA-AES128-SHA              success
ECDHE-RSA-AES128-SHA                success
.........
AES128-SHA                          success
PSK-AES128-CBC-SHA256               success
===== end ciphertest www.drv.de:443 ===============
```

VORDERSEITE FRONT

1 Personalisierung / Personalisation

Das farbige Lichtbild und die Dokumentennummer werden mittels Inkjet-Technologie sicher in das Material der Karte integriert. Alle weiteren Personalisierungsdaten werden mittels Lasergravur kontrastreich auf der Vorder- und Rückseite eingebracht.

The colour photo and the document number are securely integrated into the card material using inkjet technology. All other personal data is laser-engraved in high contrast on the front and back of the card.

2 Taktile Merkmale / Tactile features

Das Ablaufdatum des Dokuments und die sechsstellige Kartenzugangsnummer (CAN) werden per Lasergravur als fühlbare Schrift eingebracht.

The card's date of expiry and the six-digit card access number (CAN) are laser-engraved in numbers that can be felt.

3 Identigram® / Identigram®

Abhängig vom Kippwinkel der Karte werden kinematische Strukturen sowie das holografische Lichtbild in Grün und der 3D-Adler in Rot sichtbar. Nach einer Drehung der Karte um 90° erscheinen weitere Designelemente in Blau.

Kinematic structures, a hologram of the holder's image in green and a red 3D image of the federal eagle are visible depending on the viewing angle. Additional design elements appear in blue when the card is rotated 90 degrees.

4 UV-Merkmale / UV features

Unter UV-Beleuchtung sind der Bundesadler und ein in mehreren Farben lumineszierender Schriftzug zu erkennen. Beide Elemente sind im Irisdruck (kontinuierlicher Farbverlauf) umgesetzt.

The federal eagle and a line of luminescent print in multiple colours are visible in UV illumination. Both elements are printed using the rainbow printing process.

5 Optisch variable Farbe / Optically variable ink

Beim Kippen der Karte wechselt die Farbe des ICAO „chip inside" Logos je nach Betrachtungs- und Beleuchtungswinkel zwischen Grün und Blau.

When the card is tilted, the colour of the ICAO "chip inside" logo changes between green and blue depending on viewing and illumination angle.

6 Sicherheitsdruck / Security printing

Der Sicherheitsdruck setzt sich aus komplexen Mustern, mehrfarbigen Guillochen und Kopierschutzstrukturen zusammen.

The security printing is made up of complex patterns, multi-coloured guilloches and structures to protect against copying.

7 Mikroschrift / Microprinting

Im Design des Sicherheitsdrucks sind positive und negative Mikroschriftelemente in verschiedenen Größen integriert.

Positive and negative microprinting elements in varying sizes are integrated in the security printing design.

RÜCKSEITE REVERSE

8 Oberflächenprägung
Surface embossing

Auf der Kartenrückseite befindet sich eine fühlbare Oberflächenprägung, die Mikroschriften und eine Deutschlandkarte enthält.
Embossed microprinting and a map of Germany can be felt on the back of the card.

9 Laserkippbild
Variable laser image

Beim Kippen der Karte werden je nach Betrachtungswinkel das Ablaufdatum des Dokuments oder das Portrait der Karteninhaberin/des Karteninhabers sichtbar.
When the card is tilted, either the date of expiry or the cardholder's image is visible depending on the viewing angle.

10 Melierfasern
Security fibres

Auf der Kartenrückseite sind transparente Melierfasern integriert, die unter UV-Beleuchtung lumineszieren.
Transparent security fibres which are luminescent under UV illumination are integrated in the back of the card.

11 Sicherheitsfaden
Security thread

Auf der Kartenrückseite ist ein maschinell prüfbarer Sicherheitsfaden integriert, der mit der Dokumentennummer und Namen/Vorname(n) personalisiert ist.
A machine-verifiable security thread is embedded into the reverse of the card and personalized with the document number and the name/given name(s) of the cardholder.

12 Änderung der Anschrift
Change of address

Änderungen der Anschrift werden durch einen Aufkleber angezeigt, der mit einer transparenten Folie geschützt sein kann. Statt eines Siegelaufdrucks können Aufkleber alternativ einen 2D-Barcode enthalten, der mittels eines Smartphones und App geprüft werden kann.
If the cardholder's address changes, the new address is displayed on a label which can be protected with a transparent foil. Instead of a stamp, labels may display a two-dimensional barcode which can be checked using a smartphone app.

13 eID-Logo
eID logo

Dieses Logo kennzeichnet die Unterstützung der eID-Funktion.
This logo indicates that the eID function is supported.

Prüfung
Verification

- Visuell — visual
- Lupe — magnifying glass
- Fühlen — touch
- Kippen — tilting
- Licht von oben — light from above
- Streiflicht — oblique light
- UV-Beleuchtung — UV illumination
- App — app

Vorderseite VIZ

- Familienname – siehe § 5 Abs. 2 PAuswG. Adelstitel sind in Deutschland als Namensvorsatz Teil des Familiennamens.
- gegebenenfalls Geburtsname
- gegebenenfalls Doktorgrad
- Vorname
- gegebenenfalls weitere Vornamen
- Geburtstag
- Staatsangehörigkeit
- Geburtsort
- Gültigkeitsdatum
- alphanumerische Ausweisnummer/Seriennummer (oben rechts)
  - 1 – 4 = Aussteller/Behörde
  - 5 – 9 = Inhaber Nummer

Vorderseite VIZ

- Zugangsnummer/Card Access Number (kurz: CAN, 6-stellige Zahl rechts neben dem Gültigkeitsdatum) (zweite offline PIN)
- Unterschrift des Inhabers
- Passbild (biometrietaugliches Graustufen- oder Farbbild). Das Foto sollte bei Beantragung eines neuen Personalausweises nicht älter als sechs Monate sein.
- bei alten Personalausweisen die maschinenlesbare Datenzone MRZ

Rückseite VIZ MRZ

- Wohnanschrift mit fünfstelliger Postleitzahl (Hauptwohnsitz; bei Auslandsdeutschen kann der Vermerk „keine Wohnung in Deutschland“ eingetragen sein, seit 1. November 2019 aber auch eine Adresse im Ausland)
- Augenfarbe
- Körpergröße
- Ausstellungsdatum
- ausstellende Behörde
- gegebenenfalls Ordens- oder Künstlername
- gegebenenfalls Doktorgrad
- dreizeilige maschinenlesbare Datenzone in OCR-B Schrift (ECMA) mit Ausweisnummer plus Prüfziffer MRZ

Chip Zugriff und eID

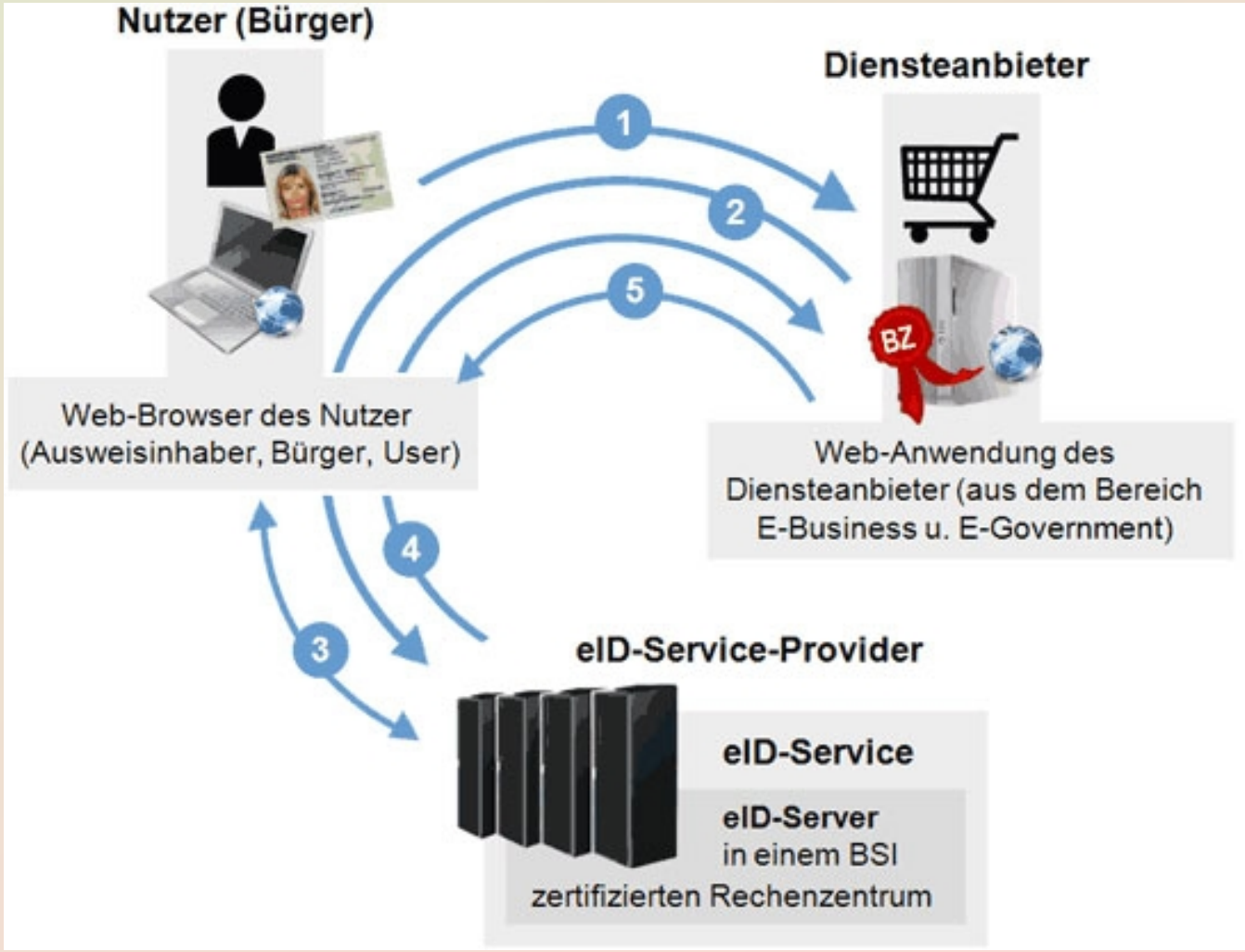
- Zugriff auf ePerso Chip
  - erfolgt nach x509 Standard verschlüsselt
  - erfordert immer ein gültiges x509 Zertifikat
- Chip enthält 20 Datengruppen
  - Diese sind abhängig vom berechtigenden Zertifikat lesbar oder beschreibbar
- Ohne gültiges x509 Zertifikat ist der Chip nicht lesbar
- eID Serverkomponenten haben keinerlei Daten

eID

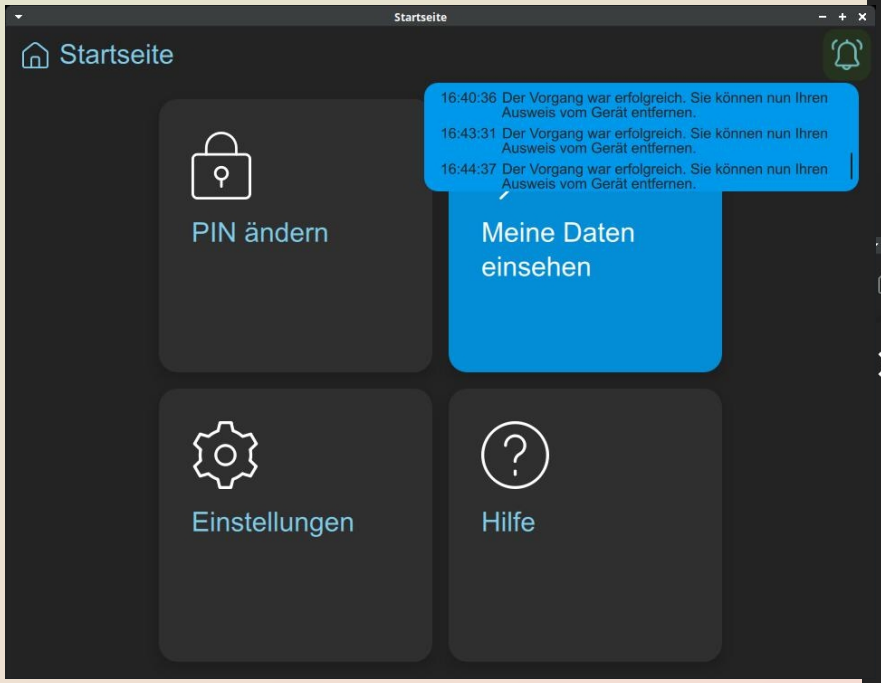

BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
LZ6311T47
MUSTERMANN
GABLER
ERIKA
12.08.1983 DEUTSCH
BERLIN
31.10.2031
38568

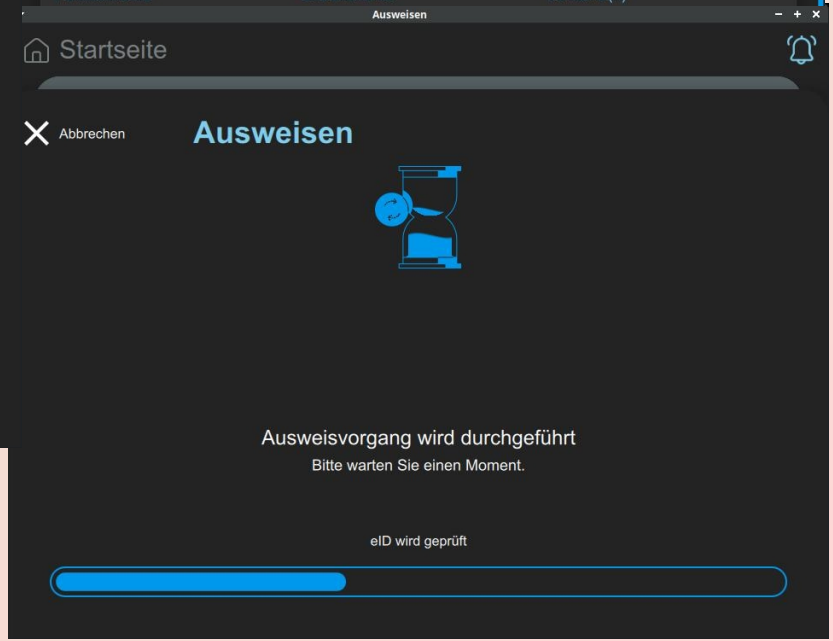

T22000129
938568
REINERSCT
Bitte Geheimzahl eingeben
PIN
1 2 3 C
4 5 6 CLR
7 8 9 @
0 OK
BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964 DEUTSCH
BERLIN
31.10.2020
938568

eID Authablauf



eID Ausweisapp2





eID AusweisApp

```
-rw-rw-r-- 1 ich ich 52237747 Apr 8 10:48 AusweisApp-2.5.0-arm64-v8a.apk
-rw-rw-r-- 1 ich ich       97 Apr 8 10:47 AusweisApp-2.5.0-arm64-v8a.apk.sha256
-rw-rw-r-- 1 ich ich 39536225 Apr 8 10:48 AusweisApp-2.5.0-armeabi-v7a.apk
-rw-rw-r-- 1 ich ich       99 Apr 8 10:47 AusweisApp-2.5.0-armeabi-v7a.apk.sha256
-rw-rw-r-- 1 ich ich 25241663 Apr 8 10:48 AusweisApp-2.5.0.dmg
-rw-rw-r-- 1 ich ich       87 Apr 8 10:47 AusweisApp-2.5.0.dmg.sha256
-rw-rw-r-- 1 ich ich    38381 Apr 8 10:47 AusweisApp-2.5.0-Lizenz.txt
-rw-rw-r-- 1 ich ich 25939968 Apr 8 10:48 AusweisApp-2.5.0.msi
-rw-rw-r-- 1 ich ich       87 Apr 8 10:47 AusweisApp-2.5.0.msi.sha256
-rw-rw-r-- 1 ich ich   277094 Apr 8 10:47 AusweisApp-2.5.0-NetInstallation_Integration_de.pdf
-rw-rw-r-- 1 ich ich   273052 Apr 8 10:47 AusweisApp-2.5.0-NetInstallation_Integration_en.pdf
-rw-rw-r-- 1 ich ich   383434 Apr 8 10:47 AusweisApp-2.5.0-ReleaseNotes.pdf
-rw-rw-r-- 1 ich ich   722779 Apr 8 10:47 AusweisApp-2.5.0-SDK.pdf
-rw-rw-r-- 1 ich ich  6045231 Apr 8 10:48 AusweisApp-2.5.0.tar.gz
-rw-rw-r-- 1 ich ich      833 Apr 8 10:47 AusweisApp-2.5.0.tar.gz.asc
-rw-rw-r-- 1 ich ich       90 Apr 8 10:47 AusweisApp-2.5.0.tar.gz.sha256
-rw-rw-r-- 1 ich ich 52094126 Apr 8 10:48 AusweisApp-2.5.0-x86_64.apk
-rw-rw-r-- 1 ich ich       94 Apr 8 10:47 AusweisApp-2.5.0-x86_64.apk.sha256

ich@meiner:~$ apt-cache search ausweisapp
ausweisapp2 - Official authentication app for German ID cards and residence permits

ich@meiner:~$ flatpak search ausweisapp
Name              Beschreibung
AusweisApp        Official authentication app for German ID card and residence permit

Application ID                          Version        Zweig        Remotes
de.bund.ausweisapp.ausweisapp2          2.5.0          stable       flathub
```

https://github.com/Governikus/AusweisApp/releases
https://f-droid.org/de/packages/com.governikus.ausweisapp2

Governicus hat für die Linux Version leider keinen Supportauftrag!

eID SW Teile Netzwerk Knoten

```
-rw-rw-r-- 1 ich ich 254099 Jan 12 04:52 eidas-commons-3.0.0.jar
-rw-rw-r-- 1 ich ich  76817 Jan 12 04:53 eidas-encryption-3.0.0.jar
-rw-rw-r-- 1 ich ich 119025 Jan 12 04:52 eidas-light-commons-3.0.0.jar
-rw-rw-r-- 1 ich ich  40052 Jan 12 04:52 eidas-logging-3.0.0.jar
-rw-rw-r-- 1 ich ich 324156 Jan 12 04:53 eidas-saml-engine-3.0.0.jar
-rw-rw-r-- 1 ich ich  89004 Jan 12 04:53 eidas-saml-metadata-3.0.0.jar
-rw-rw-r-- 1 ich ich  26129 Jan 12 04:53 eidas-security-3.0.0.jar
-rw-rw-r-- 1 ich ich  54199 Jan 12 04:53 eidas-specific-communication-definition-3.0.0.jar
-rw-rw-r-- 1 ich ich  14782 Jan 12 04:53 eidas-telemetry-3.0.0.jar
```

```
jar tvf eidas-saml-engine-3.0.0.jar | grep -i saml
     0 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/auth/engine/xml/opensaml/
  2214 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/auth/engine/xml/opensaml/CorrelatedResponse.class
 15489 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/auth/engine/xml/opensaml/ResponseUtil.class
  2414 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/auth/engine/xml/opensaml/SAMLConsent.class
  6096 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/auth/engine/xml/opensaml/SAMLEngineUtils.class
  4372 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/auth/engine/xml/opensaml/XmlSchemaUtil.class
  1780 Thu Oct 09 10:09:18 CEST 2025 eu/eidas/engine/exceptions/EIDASSAMLEngineException.class
  6083 Thu Oct 09 10:08:40 CEST 2025 META-INF/maven/eu.eidas/eidas-saml-engine/pom.xml
    63 Thu Oct 09 10:09:20 CEST 2025 META-INF/maven/eu.eidas/eidas-saml-engine/pom.properties
```

https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/920064886/Download+individual+jars

ePerso optische Kopien

ePerso optische Kopien

- **sind eine schlechte Idee**
- sensible Information wie CAN Nummer ePerso Nummer und Geburtsdatum sollen geschwärzt sein
- nur an verlässliche Ziele, nie an offene Plattformen
- nur verschlüsselt übertragen
- die Verbreitung und Löschung ist nicht kontrollierbar
- **erzeugen die sehr große Gefahr des Identitätsdiebstahls**
- niemand darf Kopien verlangen
- nur der Inhaber darf Kopien anfertigen
- PID Daten sind sensible Daten

Probleme

- Problem Authentizität bei elektronischen Daten
- Identifizierung von Menschen
- Totale Internetvernetzung
- Jeder hat eine Wanze und das Internet in der Tasche, Handys sind durch und durch verwanzt
- veraltetes Staatswesen in Deutschland
- Datenbanken wie Meldedaten sind schlecht geschützt und Ämter schleudern Daten
- politisch verquaste und veraltete Gesetze
- Zwingende Notwendigkeit von Anonymität in zu vielen Fällen
- Biometrie mit nicht kontrollierbarer Verbreitung
- Wort Sicher, für mich oder gegen mich ?

Datenabfragen

- eine Bank braucht keine Adressen
- Alterscheck mit ePerso und Wallet
- Alle Staaten wollen an Metadaten herankommen
  - unsägliche Diskussion Vorratsdaten Speicherung
  - zwingende Auth bei Mobilfunkfreischaltungen, wurde aus finanziellen Gründen eingeführt und wird heute leider sehr oft missbraucht
- Viele Apps spionieren
- proprietäre Betriebssysteme können Daten senden den der Quellcode ist nicht einsehbar

Gefahr Biometrie

- Ausbreitung ist nicht kontrollierbar bei unsicherer Biometrie
  - Fingerabdrücke
  - Bilder und Gesichtsfotos
  - Bewegungsschemas
  - DNA Spuren
- Sichere Biometrie sind nur Merkmale
  - deren Verbreitung jeder bewusst kontrollieren kann
  - nicht ohne Wissen des/der jeweiligen prüfbar sind
- Pauschales Scannen
- Pauschales Rastern mit Biometrie.

Gefahr Datenabfluss

- Apps sammeln massenhaft Daten die in einen Sumpf von Datenhändlern und Datenmissbrauch verschwinden ohne dass Überblick über diese Geschäfte besteht und teilweise im Darknet
- immense geschäftliche und politische Interessen Menschen und deren Gewohnheiten, Verhalten und Aufenthaltsorte zu kategorisieren für
  - Werber
  - Datenhändler
  - Banken, Bankgeschäfte (Kreditvergabe in der heutigen Form für Privatpersonen ist asozial)
  - Auskunfteien, Geoscoring ist asozial
  - Politik
  - Dienste
- KI und deren Bildung von Datenstrukturen

Gefahr Datenabfluss

- Staatliche Rasterungen
- Überwachung öffentlicher Flächen, Parks und Verkehr
- Gesichtserkennung funktioniert inzwischen sehr zuverlässig und performant
- Sammlung Biometrischer Informationen, Passbilder, Fingerabdrücke
- diktatorisch regierte Staaten die Allmacht beanspruchen
  - Staaten mit minimalem Datenschutz
  - Verschlüsselung, jede Verschlüsselung kann an der hohen Datenentropie erkannt werden
  - Fehlender Wille in der Politik Interessen klar zu benennen und zu behandeln
  - Geschäftsinteressen
  - politische Interessen

Polizeidatenbanken sollen

- im Wesentlichen Negativdaten sammeln
- keine Überwachung ohne Anlass ermöglichen
- immer aktuell sein und zeitnah bereinigt werden
- sollen nur gesetzlich zulässige Verknüpfungen herstellen
- keine proprietären nicht durchschaubare Software von dubiosen Firmen einsetzen
- immer Informationen über den Grund der Speicherung enthalten
- immer mitloggen wer fragt ab und wozu

Problem deutsche Behörden

- Papier ist meist Datenmaster
- alle elektronischen Daten sind manipulierbar
- Informationsdefizit da alles umständlich erfragt werden muss
- Kein Verständnis für Datenschutz im Internetzeitalter
- wenn Apps dann viele nicht zusammenhängende
- Behörden arbeiten isoliert
- dieselben Daten werden mehrfach abgefragt
- Viele Karten und IDs
- mangelnde Sachkenntnis bei deutschen Behörden und Polizei
- Zur Identifizierung wir fast nur die VIZ verwendet
- Es wird permanent kopiert inklusive des ePerso
- Keine Kenntnisse über Verschlüsselung

PID Daten Fixierung

- Fixierung auf PID-Daten ist veraltet und sollte durch eine eindeutige durch eine Bundesbehörde geführte ID ersetzt werden denn
  - Gefahr des ID Diebstahls
  - PID Daten mit Wohnadresse sind Überbleibsel aus einer alten und oft schlimmen Zeit
  - ladungsfähige Anschrift zur Zeugenaussage, etc ist mangels Alternative bis heute so
- Papierpostadresse ist wegen Überalterung deutscher Behörden bis heute so
- Daten zum Geschlecht sind nicht erforderlich, schon gar nicht über nicht binäre Menschen.
- Ummeldungen innerhalb Deutschlands oder EU sind vermeidbare Behördenbeschäftigung
- IDs sollen einmal bei Geburt und Tod festgestellt werden mittels sicherer Biometrie

Mobiltelefone und Software

- Empfehlung alternative ROMs verwenden
  - GrapheneOS
  - LineageOS
  - /e/OS
- Damit betriebsbereit installierte Geräte kaufen
  - Nitrophone
  - Shiftphone
  - Fairphone
- Empfehlung alternative APP Stores verwenden
  - auf F-Droid sind alle APPs open source und werden mit öffentlichen Lizenzen wie GPL veröffentlicht und der Quellcode ist auf GitHub, Gitlab, etc. für alle einsehbar
- **Daten hungrige APPs löschen**
- Windows11 Recall oder Dinge wie NSAKEY
- **Rootshell installieren reißt großes Sicherheitsloch auf**
- **Alternativen bei Händlern nachfragen**

Möglichkeiten

- alle Quellen, Bilder Videos, bekommen eine anonyme ID
- KFZ Kennzeichen werden anonymisiert
- Anonyme ID für mehrere Zwecke wie Social Media
- Altersverifikation wird mit ID-Wallet sicher möglich
- telefonisch oder online geschlossene Verträge sicher bestätigen
- Unterlagen und Anträge digital unterschreiben
- alle Daten und Erlaubnisse wie Fahrerlaubnis an einem Ort elektronisch verfügbar.
- Sichere Systemzugriffe
- verlässliche Authentisierungen

Herausforderungen

- Besser informieren
- alles kann früher oder später geknackt werden, Hase Igel Jagd verlässlich annehmen
- es braucht braucht vernünftig, gesetzlich und materiell ausreichend ausgestattete Justiz die erst noch geschaffen werden muss um handlungsfähig zu sein.
- Mangel an Information kann Mythen nähren

Vorhandene IDs

- PID Daten
- ePerso Nummer
- Steuer-ID
- Künftig elektronische EU-ID

Projekte zur Lösung

- EUID-Wallet, Deutschland Wallet
- Deutschland APP
- Aufrüstung der BundID APP als Authserver
- enge Verzahnung der beiden Apps
- Gerichtspostfach
- vereinheitlichte Behördenkontakte und Datenaustausch mit Deutschland APP

Ist aber nur ein Anfang

Projektbeteiligte

- SPRIN-D
- BSI
- Pilot Wallet Programmierende
- Bibliothekslieferanten
- Open Source

Möglichkeiten ID-Wallet

- PID-Daten
- Online-ID auch anonymisiert
- Steuer-ID
- Vollmachten
- Erziehungsberechtigung
- Fahrerlaubnisse
- Gesundheitskarte ersetzen
- Speicherung von ÖPNV Tickets
- Authentisierter Zugang zu eKFZ
- vieles mehr

aber noch in Diskussion

Hinweise

- Politische Probleme sind technisch nicht lösbar
- veraltete Gesetz sind für zu viele Probleme die Ursache, falsche Ideologie, Überbleibsel aus der deutschen Kaiserzeit oder religiöser Einfluss
- der Deutsche Staat und seine Verwaltungen bedürfen massivster Modernisierungen
- die oft gescholtenen Beamten und Behörden Mitarbeiter arbeiten so gut wie wir sie arbeiten lassen
- Politik muss
  - aufhören Fakten zu verdrehen
  - durch Inkompetenz zu glänzen
  - sich der Situation wirklich bewusst werden um zu verstehen was endlich gemacht werden muss

Gesellschaftliche Themen

- in Deutschland finden immer mehr Menschen keine Wohnung. Ohne Wohnungsbestätigung ist keine Anmeldung möglich und wenn Meldeämter Information haben dass Häuser abgerissen sind löschen diese die dort gemeldeten Einwohner ohne jede Rückfrage. Folgen sind dann
  - Ausweise laufen ab
  - Krankenversicherungen gehen verloren da Krankenkassen auf Papierpostadressen bestehen identisch zu PID-Daten
  - viele ärztliche Behandlungen sind nicht mehr möglich
- in Deutschland leben viele nicht gemeldete Menschen

Gesellschaftliche Themen

- nur wenige oft teure Smartphones erfüllen Voraussetzungen
- Smartphone Markt ist sehr vermachtet
- nicht jeder Deutsche kann sich die erforderliche Technik finanziell leisten
- es gibt aus verschiedenen Gründen Ablehnungen wie zum Beispiel Alter
- Viele Teile benötigen internationale Vereinbarungen, EU ist hier wesentlicher Unterstützer
- Es ist offene aktive Information zwingend die informiert und erklärt was wie und wozu gebaut wird
- Informationsmangel nähert Mythen

Quellenverweise

- SPRIN-D
- BSI
- Bundesdruckerei
- Wikipedia
- European Commision
- Pilotwallet Programmierende
- Bibliothekslieferanten

Vielen Dank

Quellenverweise

- https://gitlab.opencode.de/bmi/eudi-wallet/eidas2/-/tree/main
- https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md
- https://www.sprind.org/taten/strategische-projekte/eudi-wallet
- https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2024/BMI24020-personalausweis-flyer.pdf?__blob=publicationFile&v=5
- https://de.wikipedia.org/wiki/Personalausweis_(Deutschland)#Der_elektronische_Personalausweis_(nPA)
- https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/ausweise/maschinenlesbare-zone-paesse-ausweise.pdf?__blob=publicationFile&v=19
- https://personalausweis-mrz.idcards.me
- https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home
- https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/eudiwallet-was-sie-zur-digitalen-brieftasche-wissen-muessen-95821
- https://bmds.bund.de/themen/digitaler-staat/digitale-identitaeten/eudi-wallet
- https://www.bundesdruckerei.de/de/innovation-hub/eudi-wallet-sicher-digital-identifizieren-europa
- https://www.ausweisapp.bund.de/sdk/desktop.html
- https://eidas.ec.europa.eu/efda/wallet
- https://eidas.ec.europa.eu/efda/browse/notification/eid-chapter-contacts/DE

Vielen Dank

Cloudlink

https://e.pcloud.link/publink/show?code=kZmyQaZwMu6mLCnPByQvxvIhdddjmb9wkmV

Vielen Dank

CCCStuttgart