IT-Sicherheit der Vertrauensinfrastruktur

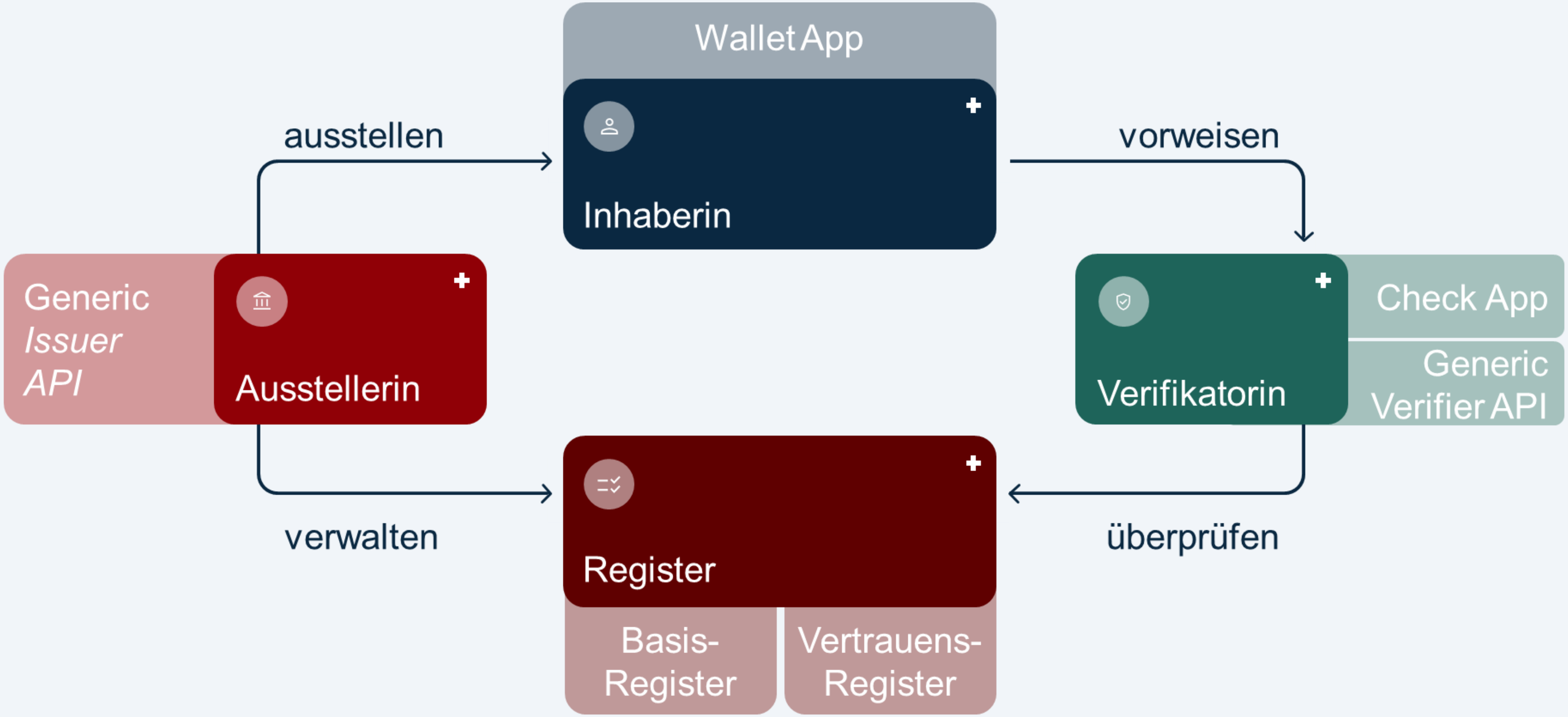
Master Arbeit

Partizipationsmeeting, 10.07.2025
Fabrice Egger

swiyu | A service of the Swiss Confederation

CYD
CYBER
DEFENCE
CAMPUS

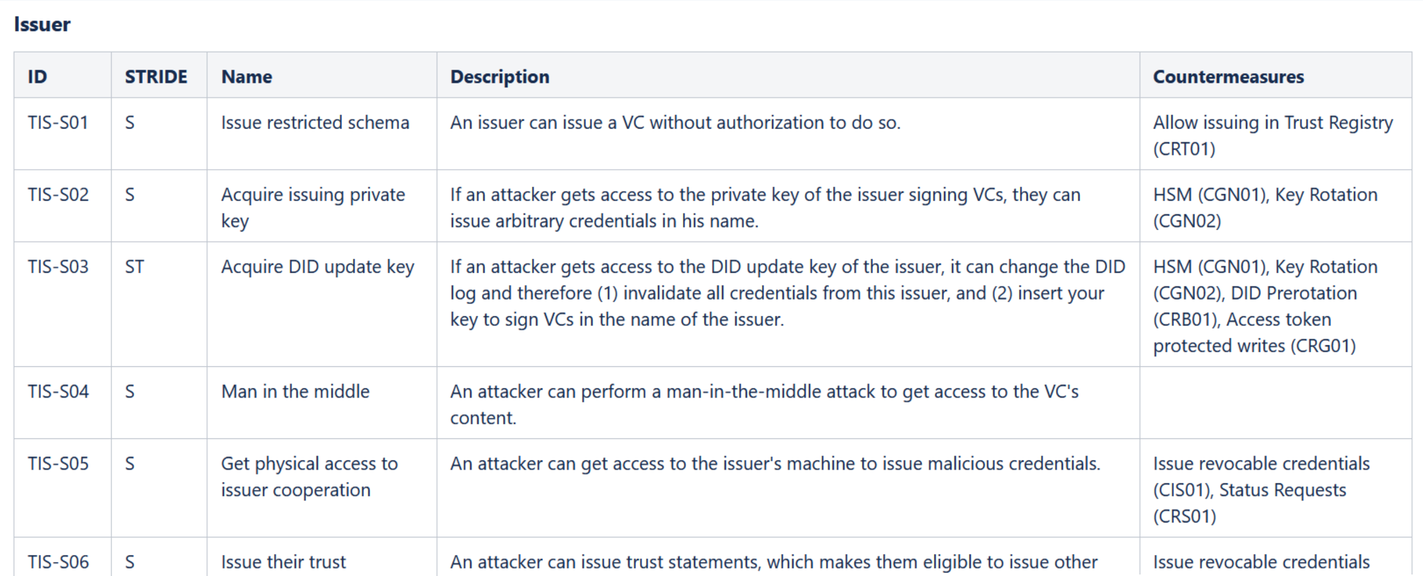
Offenes Ökosystem



Threat Model

- STRIDE Modell
  - **S**poofing (Identitätsverschleierung)
  - **T**ampering (Manipulation)
  - **R**epudiation (Verleugnung)
  - **I**nformation Disclosure (Verletzung der Privatsphäre)
  - **D**enial of Service (Verweigerung des Dienstes)
  - **E**levation of Privilege (Rechteausweitung)

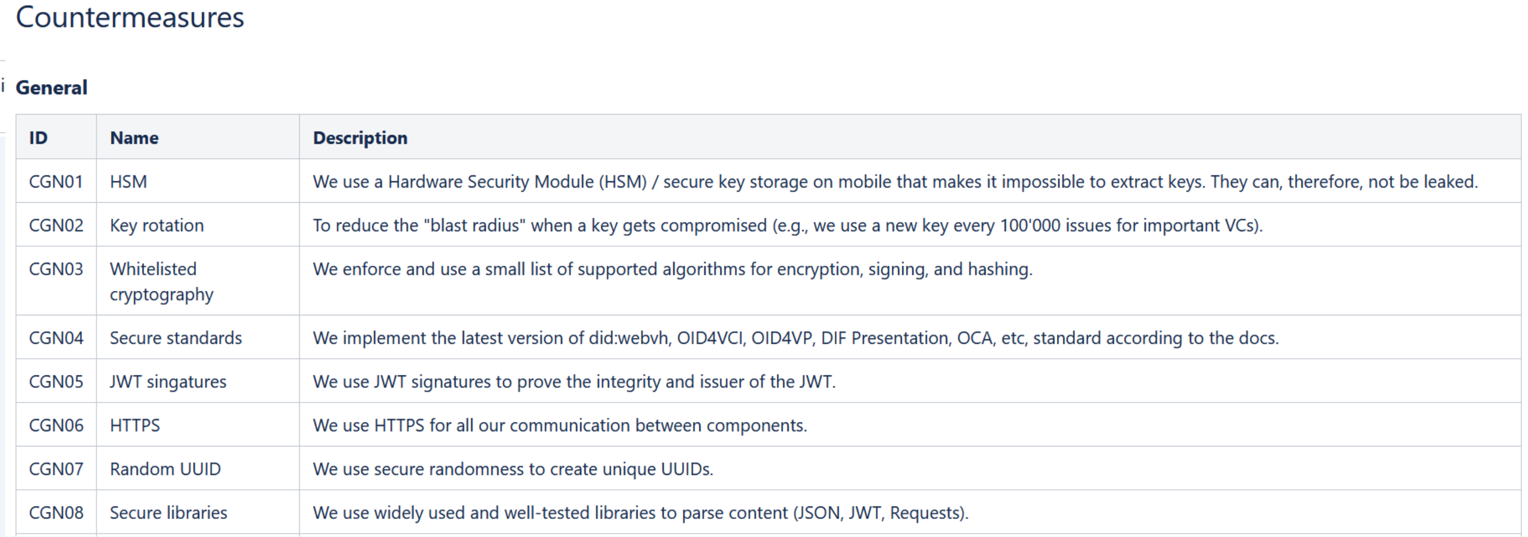
Threat Model



Issuer

ID	STRIDE	Name	Description	Countermeasures
TIS-S01	S	Issue restricted schema	An issuer can issue a VC without authorization to do so.	Allow issuing in Trust Registry (CRT01)
TIS-S02	S	Acquire issuing private key	If an attacker gets access to the private key of the issuer signing VCs, they can issue arbitrary credentials in his name.	HSM (CGN01), Key Rotation (CGN02)
TIS-S03	ST	Acquire DID update key	If an attacker gets access to the DID update key of the issuer, it can change the DID log and therefore (1) invalidate all credentials from this issuer, and (2) insert your key to sign VCs in the name of the issuer.	HSM (CGN01), Key Rotation (CGN02), DID Prerotation (CRB01), Access token protected writes (CRG01)
TIS-S04	S	Man in the middle	An attacker can perform a man-in-the-middle attack to get access to the VC's content.	
TIS-S05	S	Get physical access to issuer cooperation	An attacker can get access to the issuer's machine to issue malicious credentials.	Issue revocable credentials (CIS01), Status Requests (CRS01)
TIS-S06	S	Issue their trust statement	An attacker can issue trust statements, which makes them eligible to issue other VCs.	Issue revocable credentials
TIS-S07	S	Replay VC.	An attacker can act as another issuer by resubmi issuer.	

178 Bedrohungen
56 Gegenmassnahmen

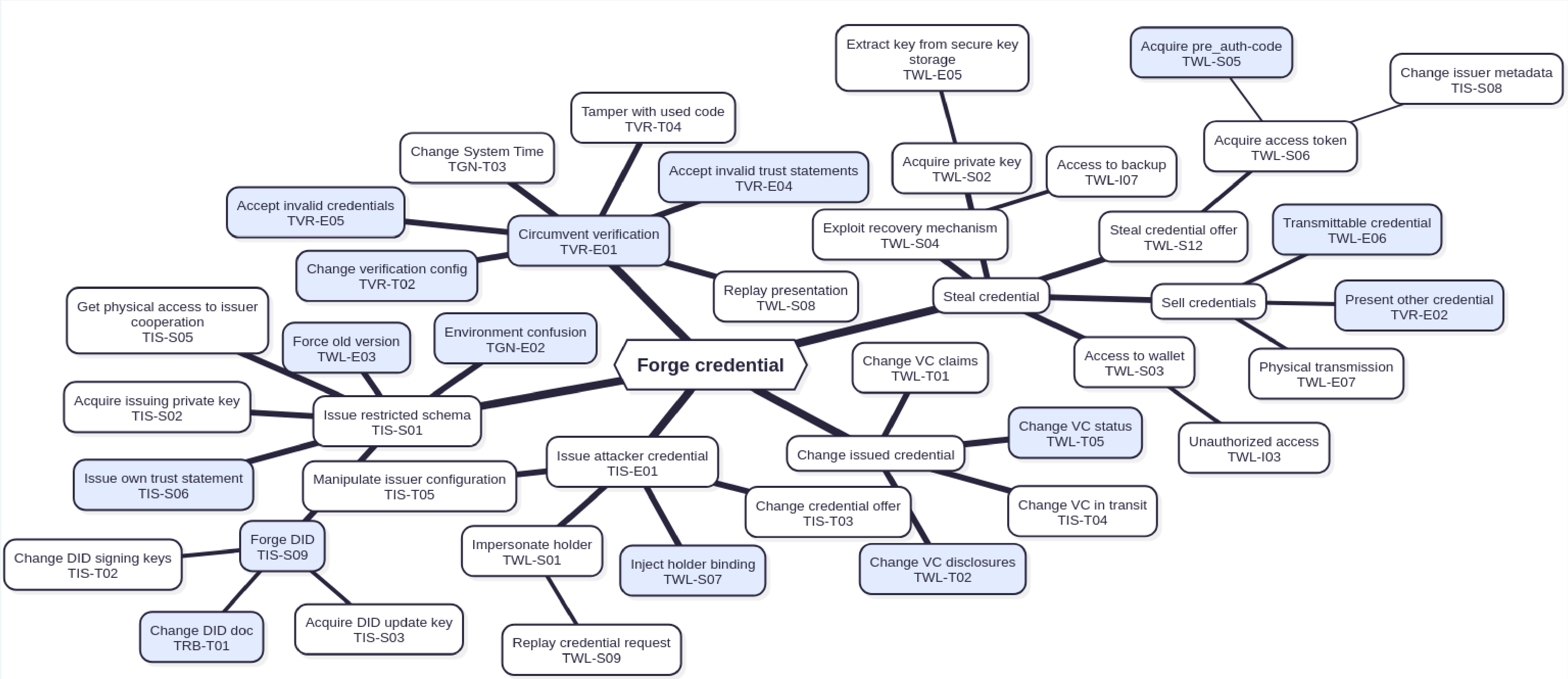


Countermeasures

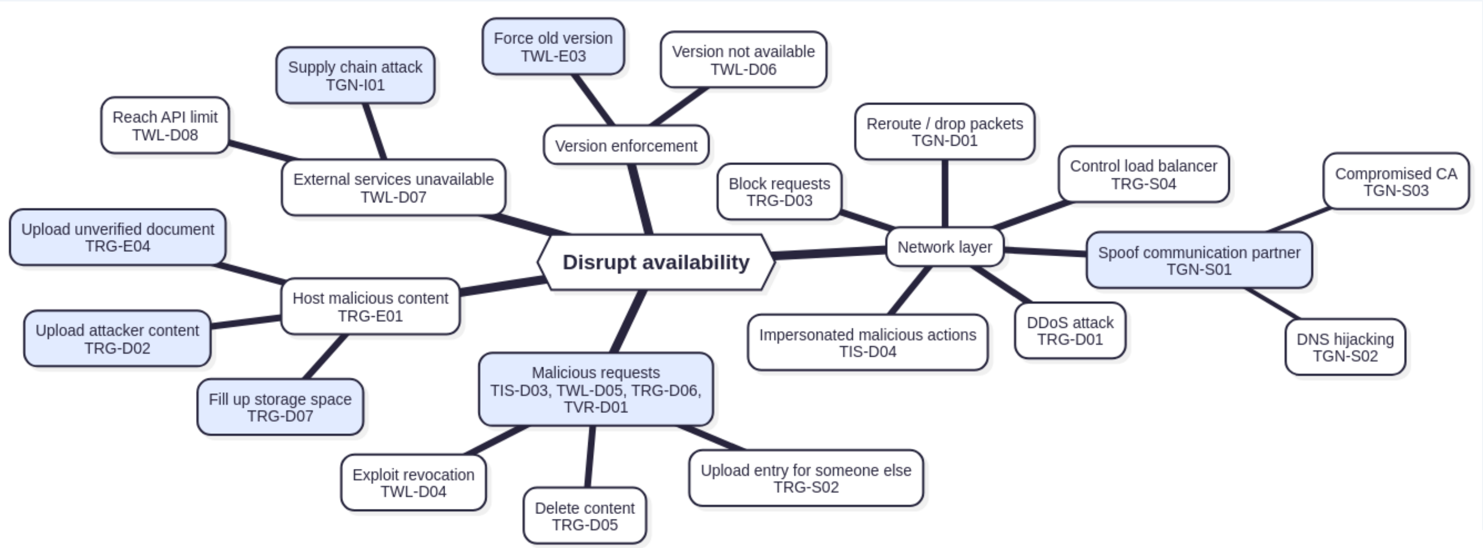
General

ID	Name	Description
CGN01	HSM	We use a Hardware Security Module (HSM) / secure key storage on mobile that makes it impossible to extract keys. They can, therefore, not be leaked.
CGN02	Key rotation	To reduce the "blast radius" when a key gets compromised (e.g., we use a new key every 100'000 issues for important VCs).
CGN03	Whitelisted cryptography	We enforce and use a small list of supported algorithms for encryption, signing, and hashing.
CGN04	Secure standards	We implement the latest version of did:webvh, OID4VCI, OID4VP, DIF Presentation, OCA, etc, standard according to the docs.
CGN05	JWT singatures	We use JWT signatures to prove the integrity and issuer of the JWT.
CGN06	HTTPS	We use HTTPS for all our communication between components.
CGN07	Random UUID	We use secure randomness to create unique UUIDs.
CGN08	Secure libraries	We use widely used and well-tested libraries to parse content (JSON, JWT, Requests).

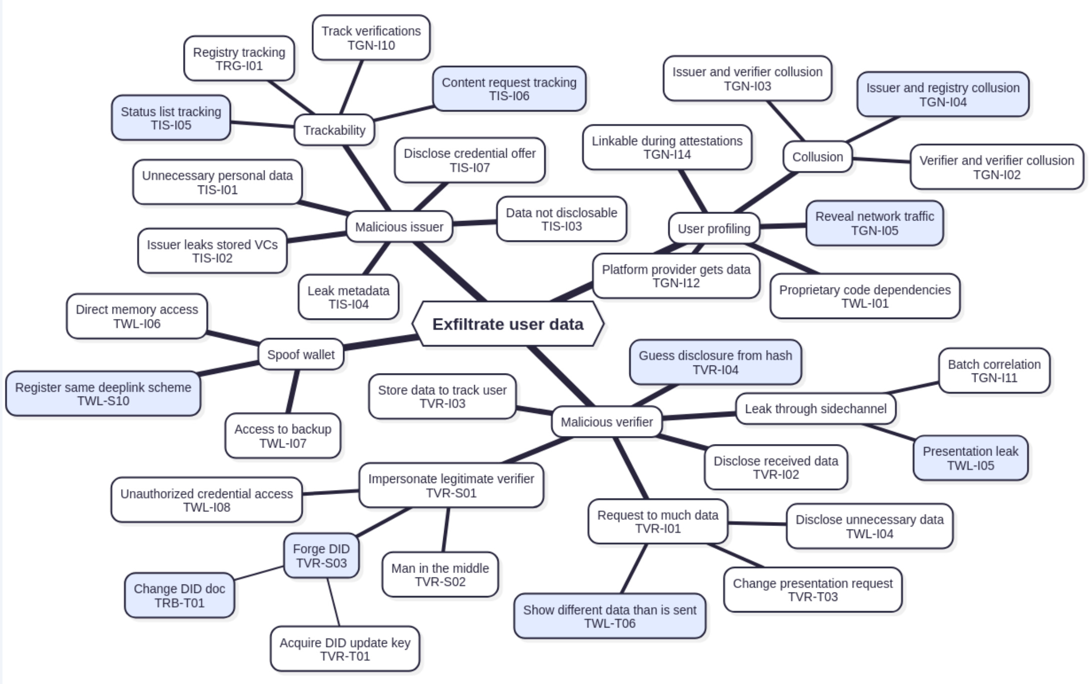
Attack Trees: Nachweis Erschleichen


Forge credential
Extract key from secure key storage TWL-E05
Acquire pre_auth-code TWL-S05
Change issuer metadata TIS-S08
Tamper with used code TVR-T04
Change System Time TGN-T03
Accept invalid trust statements TVR-E04
Acquire private key TWL-S02
Access to backup TWL-I07
Acquire access token TWL-S06
Accept invalid credentials TVR-E05
Circumvent verification TVR-E01
Exploit recovery mechanism TWL-S04
Steal credential offer TWL-S12
Transmittable credential TWL-E06
Change verification config TVR-T02
Replay presentation TWL-S08
Steal credential
Sell credentials
Present other credential TVR-E02
Get physical access to issuer cooperation TIS-S05
Force old version TWL-E03
Environment confusion TGN-E02
Change VC claims TWL-T01
Access to wallet TWL-S03
Physical transmission TWL-E07
Acquire issuing private key TIS-S02
Issue restricted schema TIS-S01
Change VC status TWL-T05
Unauthorized access TWL-I03
Issue own trust statement TIS-S06
Manipulate issuer configuration TIS-T05
Issue attacker credential TIS-E01
Change issued credential
Change credential offer TIS-T03
Change VC in transit TIS-T04
Change DID signing keys TIS-T02
Forge DID TIS-S09
Impersonate holder TWL-S01
Inject holder binding TWL-S07
Change VC disclosures TWL-T02
Change DID doc TRB-T01
Acquire DID update key TIS-S03
Replay credential request TWL-S09

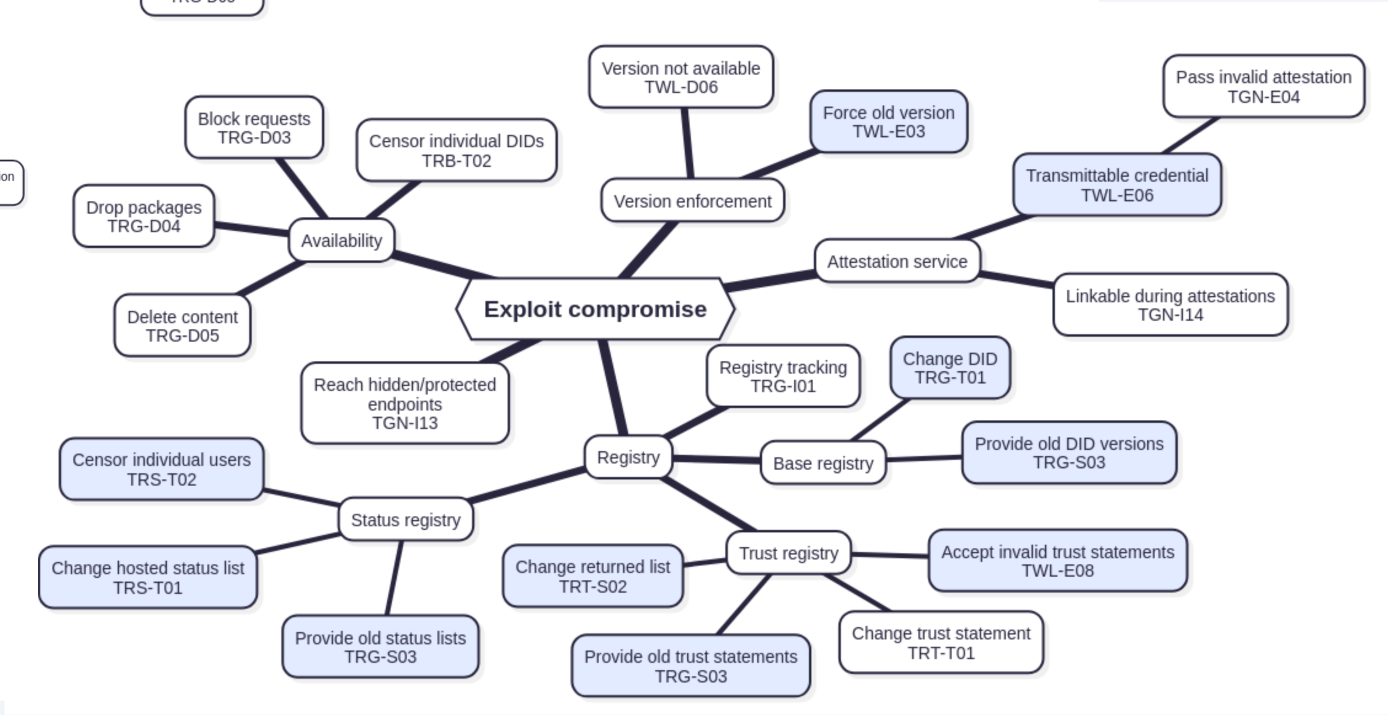
Attack Trees



- Disrupt availability
  - Version enforcement
    - Force old version TWL-E03
    - Version not available TWL-D06
  - External services unavailable TWL-D07
    - Supply chain attack TGN-I01
    - Reach API limit TWL-D08
  - Host malicious content TRG-E01
    - Upload unverified document TRG-E04
    - Upload attacker content TRG-D02
    - Fill up storage space TRG-D07
  - Malicious requests TIS-D03, TWL-D05, TRG-D06, TVR-D01
    - Exploit revocation TWL-D04
    - Delete content TRG-D05
    - Upload entry for someone else TRG-S02
  - Network layer
    - Block requests TRG-D03
    - Reroute / drop packets TGN-D01
    - Control load balancer TRG-S04
    - Spoof communication partner TGN-S01
      - Compromised CA TGN-S03
      - DNS hijacking TGN-S02
    - DDoS attack TRG-D01
    - Impersonated malicious actions TIS-D04



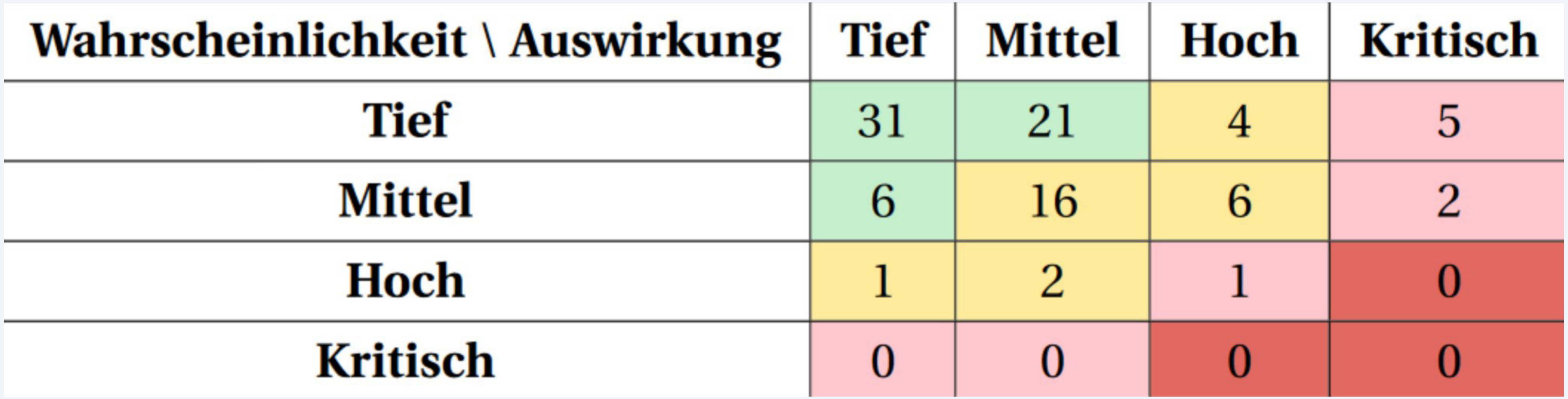
- Exfiltrate user data
  - Malicious issuer
    - Trackability
      - Registry tracking TRG-I01
      - Track verifications TGN-I10
      - Content request tracking TIS-I06
      - Status list tracking TIS-I05
    - Disclose credential offer TIS-I07
    - Data not disclosable TIS-I03
    - Unnecessary personal data TIS-I01
    - Issuer leaks stored VCs TIS-I02
    - Leak metadata TIS-I04
  - User profiling
    - Collusion
      - Issuer and verifier collusion TGN-I03
      - Issuer and registry collusion TGN-I04
      - Verifier and verifier collusion TGN-I02
    - Linkable during attestations TGN-I14
    - Reveal network traffic TGN-I05
    - Platform provider gets data TGN-I12
    - Proprietary code dependencies TWL-I01
  - Spoof wallet
    - Direct memory access TWL-I06
    - Register same deeplink scheme TWL-S10
    - Access to backup TWL-I07
  - Malicious verifier
    - Store data to track user TVR-I03
    - Guess disclosure from hash TVR-I04
    - Leak through sidechannel
      - Batch correlation TGN-I11
      - Presentation leak TWL-I05
    - Disclose received data TVR-I02
    - Request to much data TVR-I01
      - Disclose unnecessary data TWL-I04
      - Change presentation request TVR-T03
      - Show different data than is sent TWL-T06
    - Impersonate legitimate verifier TVR-S01
      - Unauthorized credential access TWL-I08
      - Forge DID TVR-S03
        - Change DID doc TRB-T01
        - Acquire DID update key TVR-T01
      - Man in the middle TVR-S02



- Exploit compromise
  - Availability
    - Block requests TRG-D03
    - Censor individual DIDs TRB-T02
    - Drop packages TRG-D04
    - Delete content TRG-D05
  - Version enforcement
    - Version not available TWL-D06
    - Force old version TWL-E03
  - Attestation service
    - Transmittable credential TWL-E06
      - Pass invalid attestation TGN-E04
    - Linkable during attestations TGN-I14
  - Reach hidden/protected endpoints TGN-I13
  - Registry
    - Status registry
      - Censor individual users TRS-T02
      - Change hosted status list TRS-T01
      - Provide old status lists TRG-S03
    - Base registry
      - Registry tracking TRG-I01
      - Change DID TRG-T01
      - Provide old DID versions TRG-S03
    - Trust registry
      - Change returned list TRT-S02
      - Accept invalid trust statements TWL-E08
      - Provide old trust statements TRG-S03
      - Change trust statement TRT-T01

Sicherheitsanalyse

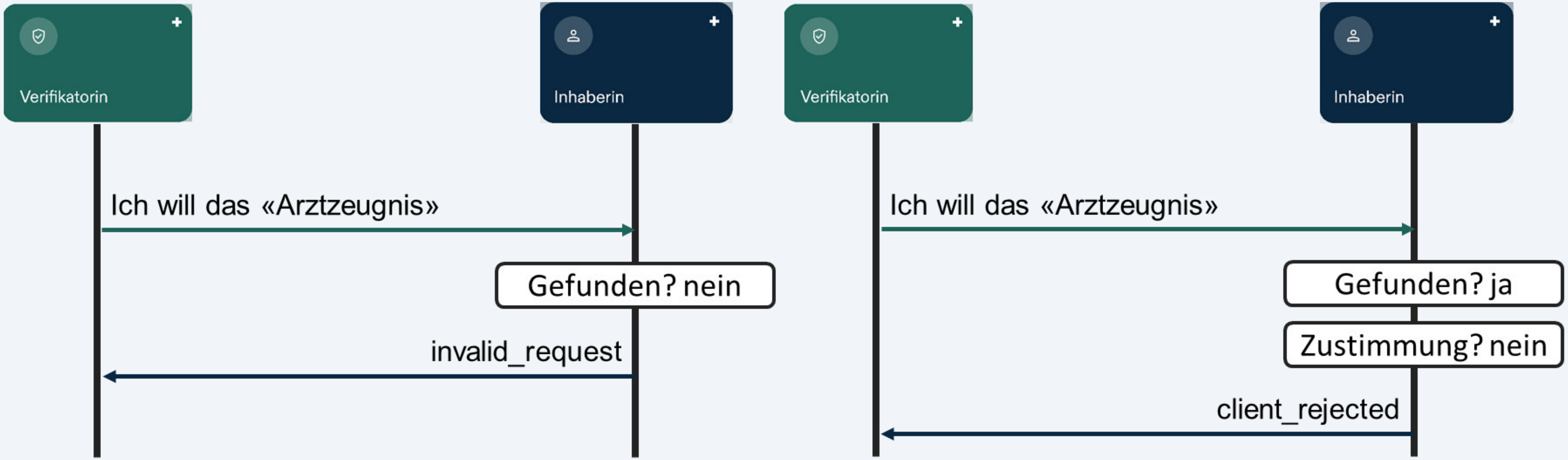
- 95 Schwachstellen / Risiken
- 58 tiefe, 29 mittlere, 8 hohe, and 0 kritische Risiken
- 49 schon behandelt für Public Beta
- Liste aller noch offenen Schwachstellen veröffentlicht



Wahrscheinlichkeit \ Auswirkung	Tief	Mittel	Hoch	Kritisch
Tief	31	21	4	5
Mittel	6	16	6	2
Hoch	1	2	1	0
Kritisch	0	0	0	0

Seitenkanalangriff auf die Präsentation

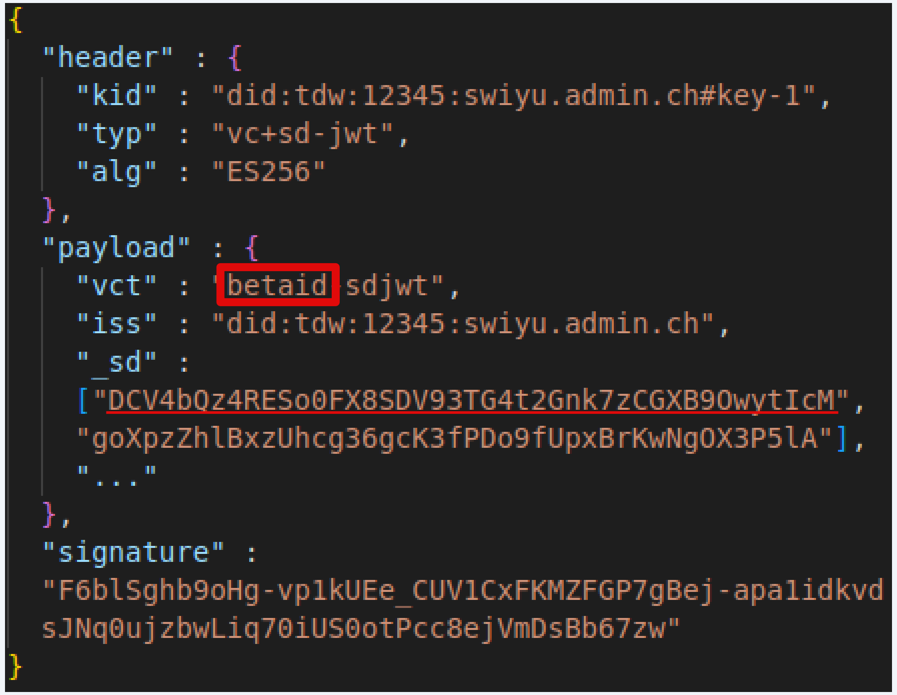
Risiko	Auswirkung	Wahrsch.
Mittel	Mittel	Hoch



Verifikation Umgehen

Risiko	Auswirkung	Wahrsch.
Hoch	Kritisch	Mittel

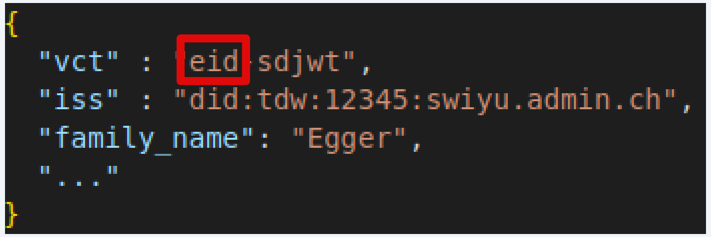
Vor Verifikation



```
{
  "header" : {
    "kid" : "did:tdw:12345:swiyu.admin.ch#key-1",
    "typ" : "vc+sd-jwt",
    "alg" : "ES256"
  },
  "payload" : {
    "vct" : "betaid sdjwt",
    "iss" : "did:tdw:12345:swiyu.admin.ch",
    "_sd" :
    ["DCV4bQz4RESo0FX8SDV93TG4t2Gnk7zCGXB9OwytIcM",
    "goXpzZhlBxzUhcg36gcK3fPDo9fUpxBrKwNgOX3P5lA"],
    "..."
  },
  "signature" :
  "F6blSghb9oHg-vp1kUEe_CUV1CxFKMZFGP7gBej-apalidkvd
  sJNq0ujzbwLiq70iUS0otPcc8ejVmDsBb67zw"
}
```

Überschreiben

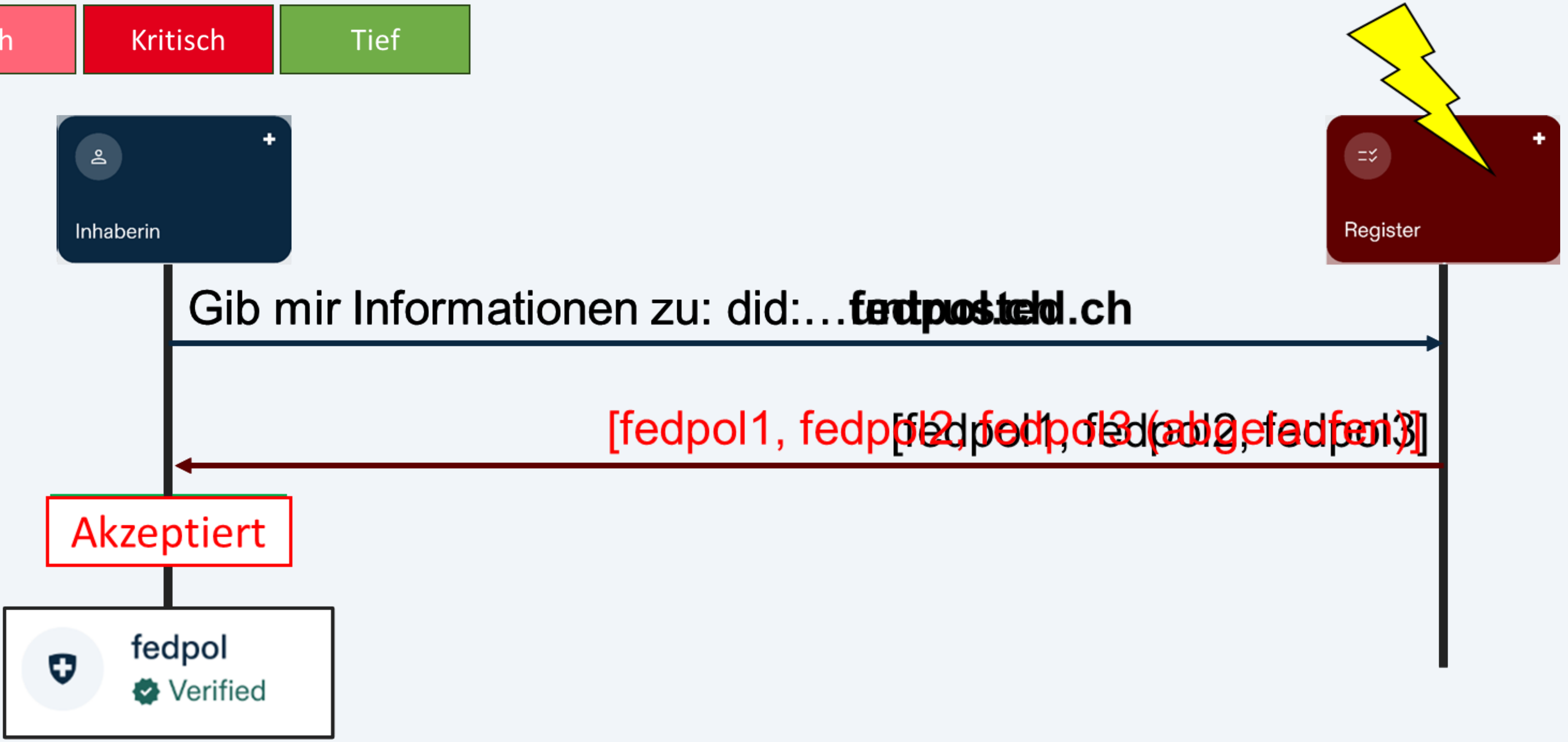
Nach Verifikation



```
{
  "vct" : "eid sdjwt",
  "iss" : "did:tdw:12345:swiyu.admin.ch",
  "family_name": "Egger",
  "..."
}
```

Fehlende Vertrauensregister Validierung

Risiko	Auswirkung	Wahrsch.
Hoch	Kritisch	Tief



Gib mir Informationen zu: did:…fedpol.ch

Gib mir Informationen zu: did:…trusted.ch

[fedpol1, fedpol2, fedpol3]

[fedpol1, fedpol2, fedpol3 (abgelaufen)]

Zusammenfassung

- Erster Entwurf eines Threat Models für 2026
- Attack Trees
- Sicherheitsanalyse
- Unterstützung bei Schwachstellenbehebung (49 / 95 schon behoben)

Mitzunehmen

- Gut, mit der Public Beta zu starten
- Sicherheit ist ein Prozess
- Bug Bounty Programm

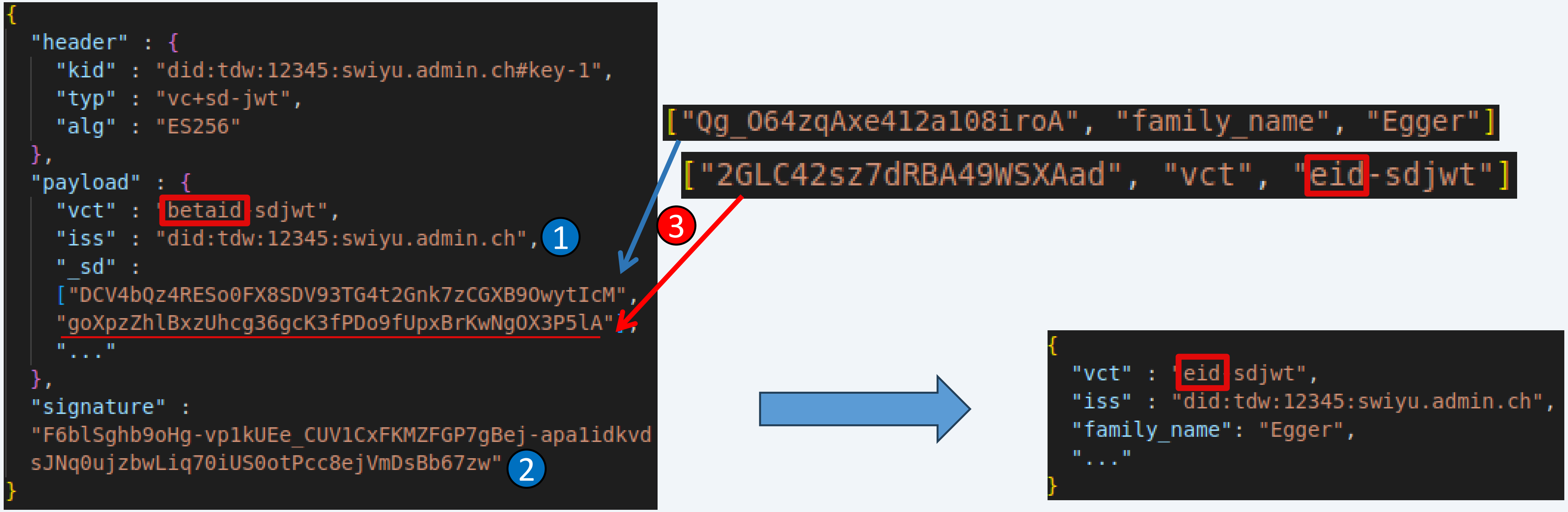
Zukünftige Arbeiten

- Sicherheitsüberprüfung erweitern
- Sicherheitsanalyse der implementierten Standards

Backup

Verifikation Umgehen

Risiko	Auswirkung	Wahrsch.
Hoch	Kritisch	Mittel



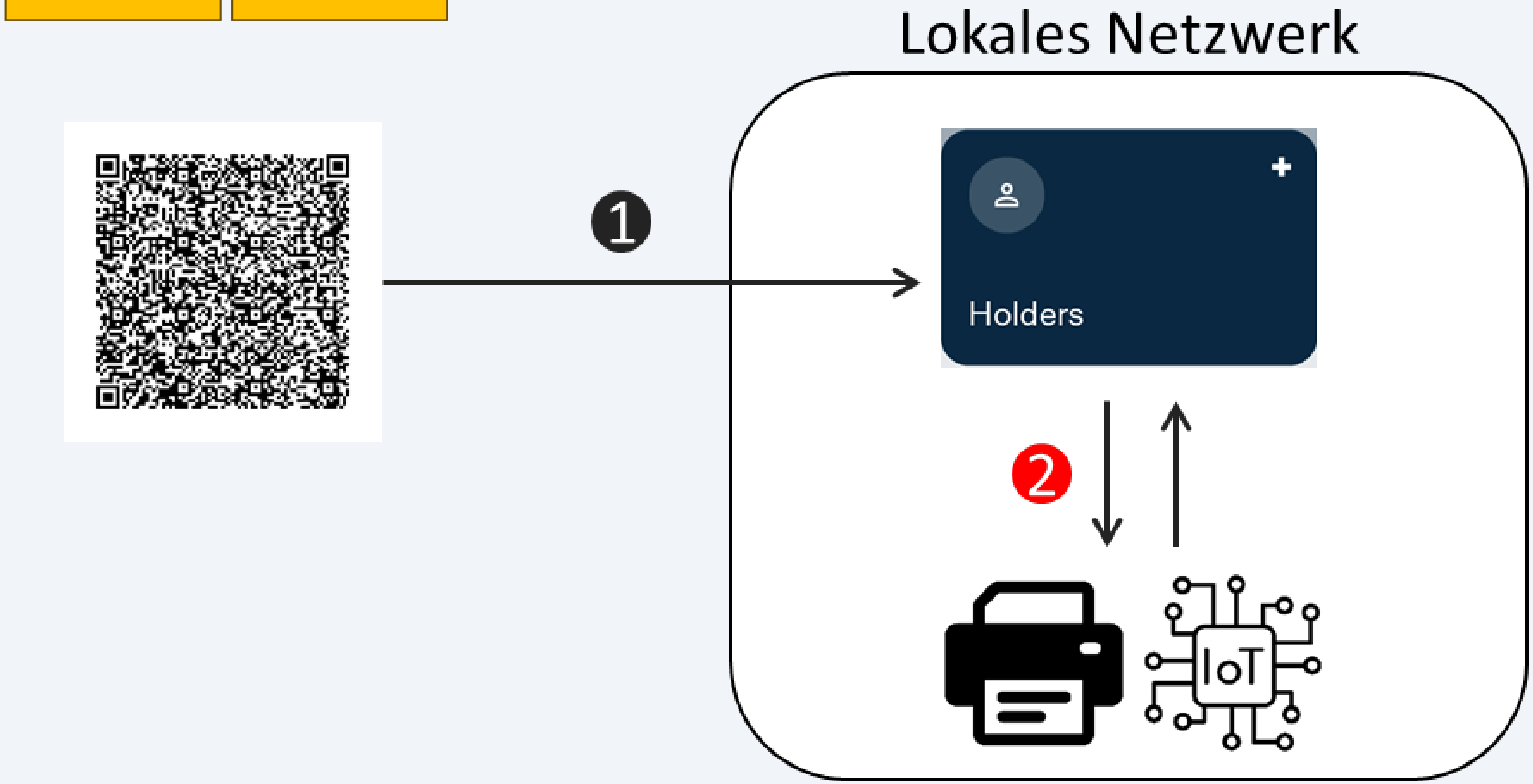
```
{
  "header" : {
    "kid" : "did:tdw:12345:swiyu.admin.ch#key-1",
    "typ" : "vc+sd-jwt",
    "alg" : "ES256"
  },
  "payload" : {
    "vct" : "betaid-sdjwt",
    "iss" : "did:tdw:12345:swiyu.admin.ch",
    "_sd" :
    ["DCV4bQz4RESo0FX8SDV93TG4t2Gnk7zCGXB9OwytIcM",
    "goXpzZhlBxzUhcg36gcK3fPDo9fUpxBrKwNgOX3P5lA",
    "..."
  },
  "signature" :
  "F6blSghb9oHg-vp1kUEe_CUV1CxFKMZFGP7gBej-apa1idkvd
  sJNq0ujzbwLiq70iUS0otPcc8ejVmDsBb67zw"
}
```

```
["Qg_064zqAxe412a108iroA", "family_name", "Egger"]
["2GLC42sz7dRBA49WSXAad", "vct", "eid-sdjwt"]
```

```
{
  "vct" : "eid-sdjwt",
  "iss" : "did:tdw:12345:swiyu.admin.ch",
  "family_name": "Egger",
  "..."
}
```

Lokale Netzwerkanfragen

Risiko	Auswirkung	Wahrsch.
Mittel	Mittel	Mittel


Lokales Netzwerk
1
Holders
2
IoT