Sécurité informatique de l'infrastructure de confiance

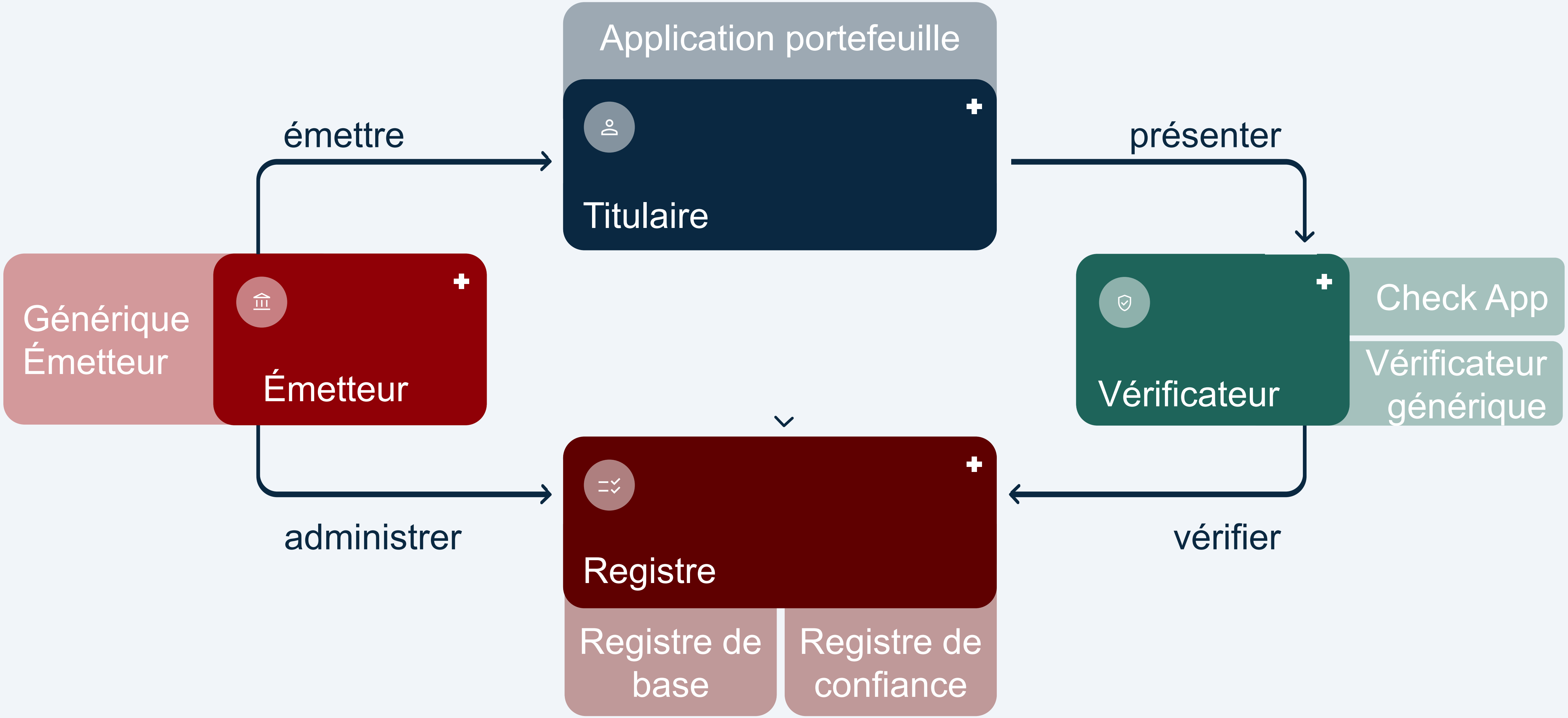
Travail de Master

Réunion participative, 10.07.2025
Fabrice Egger

swiyu | A service of the Swiss Confederation

CYD
CYBER
DEFENCE
CAMPUS

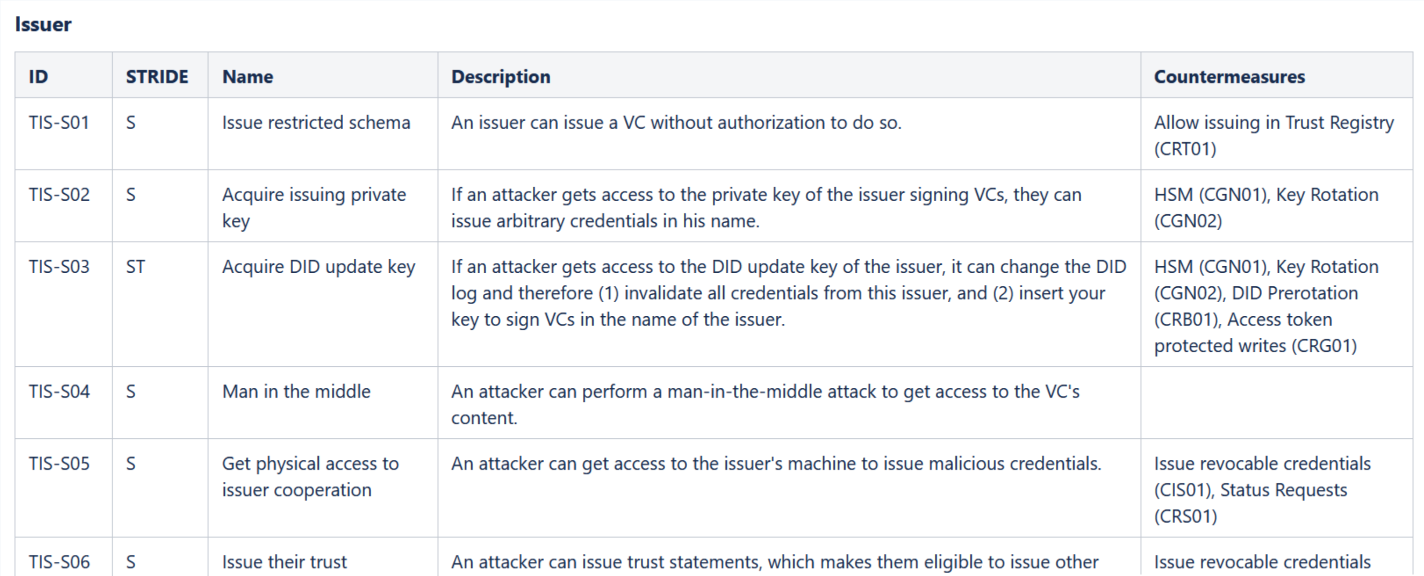
Écosystème ouvert



Modèle de menace

- Modèle STRIDE
  - **S**poofing (dissimulation d'identité)
  - **T**ampering (manipulation)
  - **R**epudiation (déni)
  - **I**nformation Disclosure (violation de la vie privée)
  - **D**enial of Service (refus de service)
  - **E**levation of Privilege (augmentation des droits)

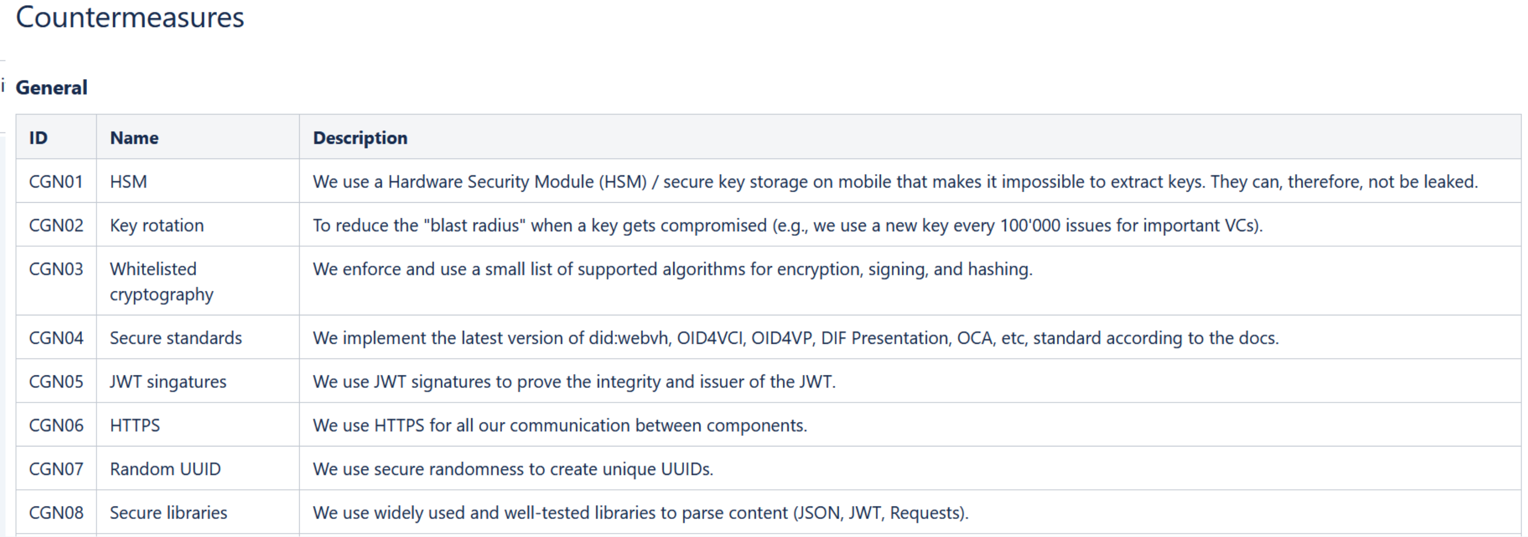
Modèle de menaces



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 Menaces
56 Contre-mesures

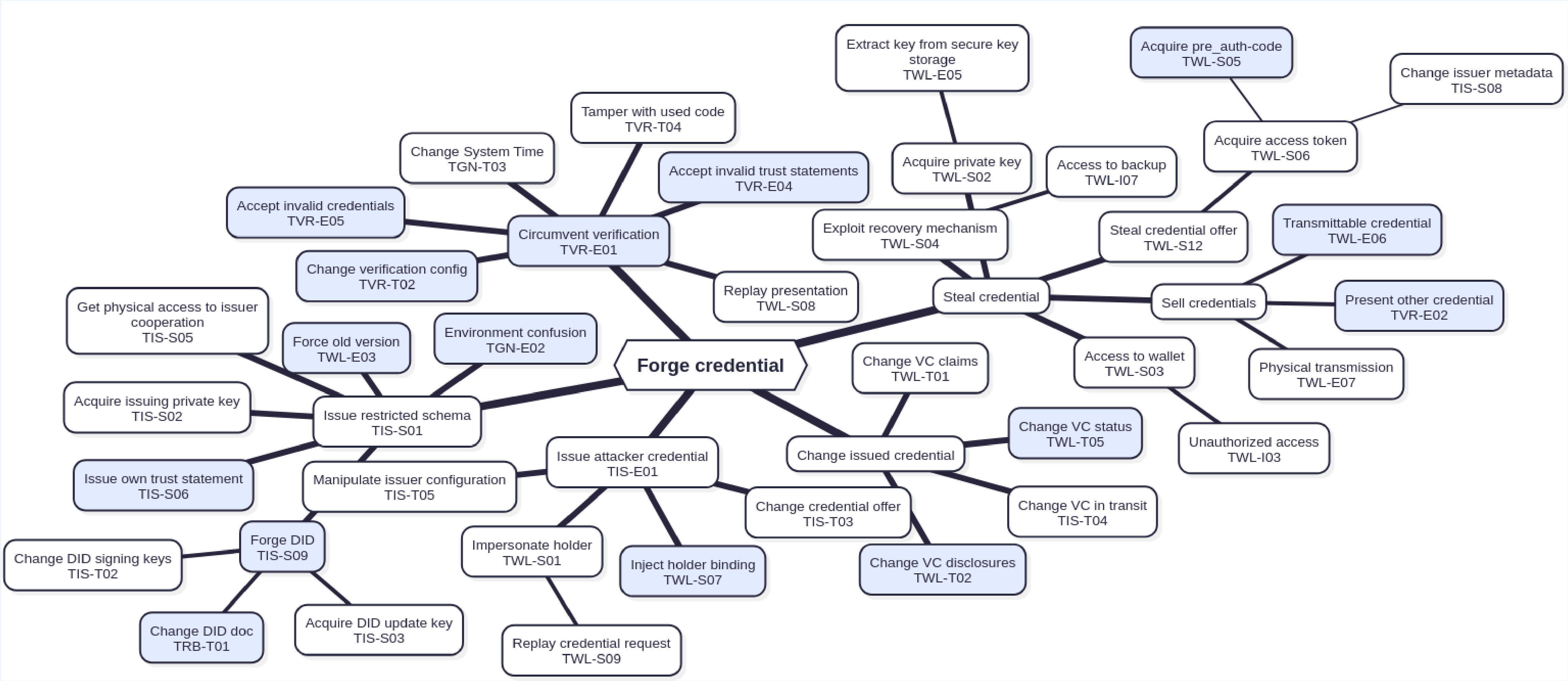


Countermeasures

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).

Arbres d'attaque: Preuve d'obtention



Forge credential

Circumvent verification
TVR-E01

Accept invalid credentials
TVR-E05

Change System Time
TGN-T03

Tamper with used code
TVR-T04

Accept invalid trust statements
TVR-E04

Change verification config
TVR-T02

Replay presentation
TWL-S08

Steal credential

Exploit recovery mechanism
TWL-S04

Acquire private key
TWL-S02

Extract key from secure key storage
TWL-E05

Access to backup
TWL-I07

Steal credential offer
TWL-S12

Acquire access token
TWL-S06

Acquire pre_auth-code
TWL-S05

Change issuer metadata
TIS-S08

Sell credentials

Transmittable credential
TWL-E06

Present other credential
TVR-E02

Physical transmission
TWL-E07

Access to wallet
TWL-S03

Unauthorized access
TWL-I03

Change issued credential

Change VC claims
TWL-T01

Change VC status
TWL-T05

Change VC in transit
TIS-T04

Change VC disclosures
TWL-T02

Change credential offer
TIS-T03

Issue attacker credential
TIS-E01

Impersonate holder
TWL-S01

Replay credential request
TWL-S09

Inject holder binding
TWL-S07

Manipulate issuer configuration
TIS-T05

Issue restricted schema
TIS-S01

Force old version
TWL-E03

Environment confusion
TGN-E02

Get physical access to issuer cooperation
TIS-S05

Acquire issuing private key
TIS-S02

Issue own trust statement
TIS-S06

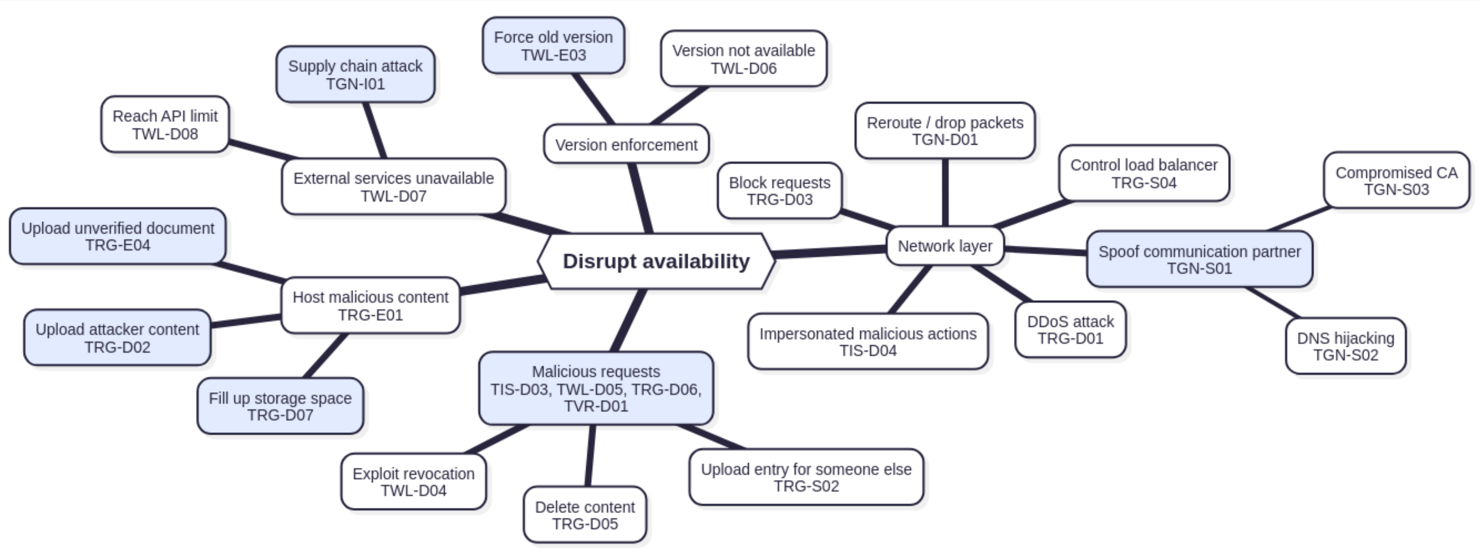
Forge DID
TIS-S09

Change DID signing keys
TIS-T02

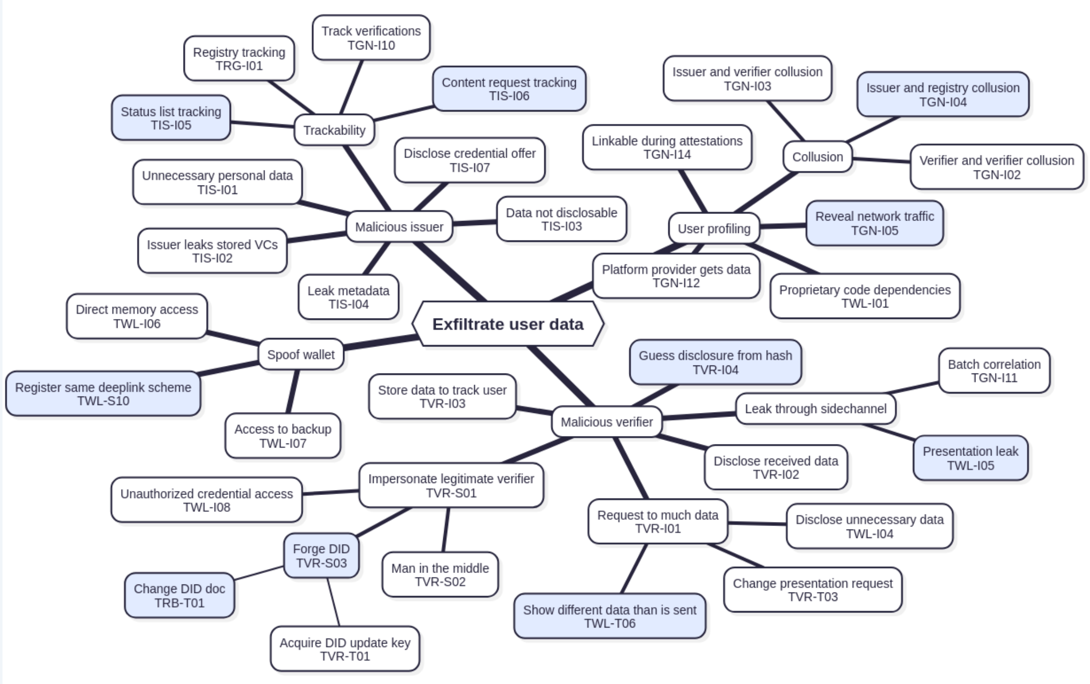
Change DID doc
TRB-T01

Acquire DID update key
TIS-S03

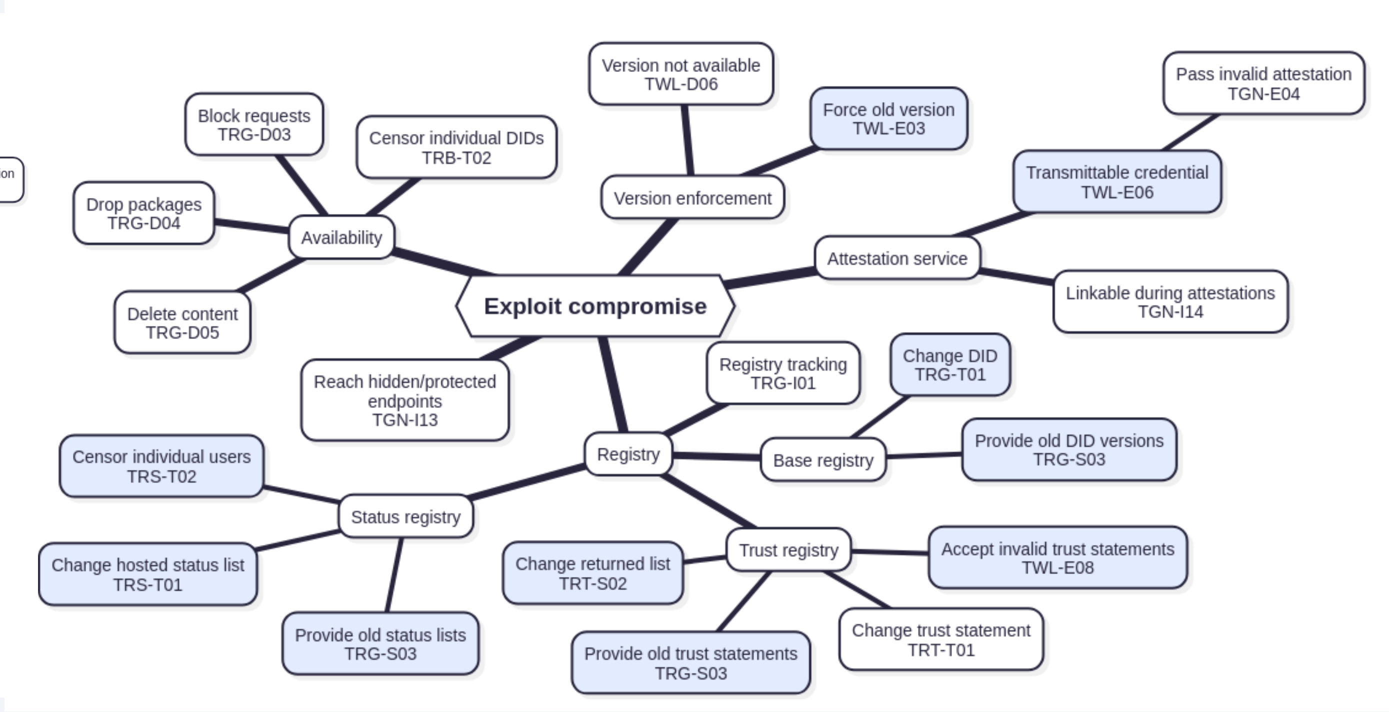
Arbres d'attaque



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



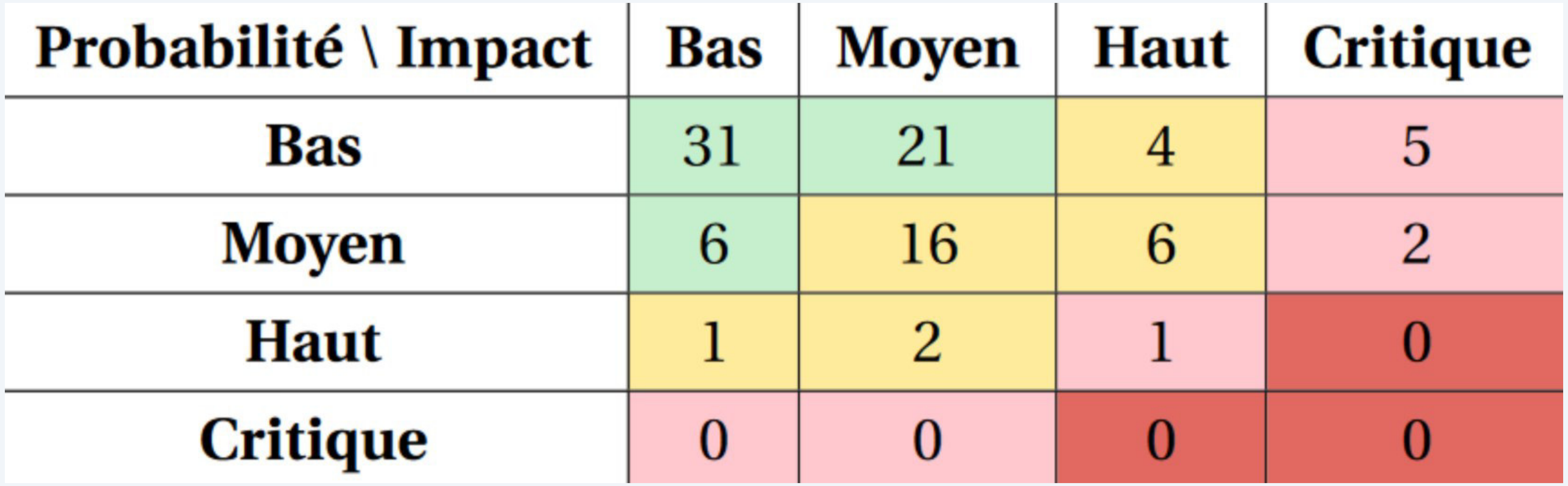
Exfiltrate user data
- Malicious issuer
  - Trackability
    - Registry tracking TRG-I01
    - Track verifications TGN-I10
    - Content request tracking TIS-I06
    - Status list tracking TIS-I05
  - Disclose credential offer TIS-I07
  - Data not disclosable TIS-I03
  - Unnecessary personal data TIS-I01
  - Issuer leaks stored VCs TIS-I02
  - Leak metadata TIS-I04
- User profiling
  - Linkable during attestations TGN-I14
  - Collusion
    - Issuer and verifier collusion TGN-I03
    - Issuer and registry collusion TGN-I04
    - Verifier and verifier collusion TGN-I02
  - Reveal network traffic TGN-I05
  - Proprietary code dependencies TWL-I01
  - Platform provider gets data TGN-I12
- 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
  - Registry tracking TRG-I01
  - Base registry
    - Change DID TRG-T01
    - Provide old DID versions TRG-S03
  - Status registry
    - Censor individual users TRS-T02
    - Change hosted status list TRS-T01
    - Provide old status lists 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

Analyse de la sécurité

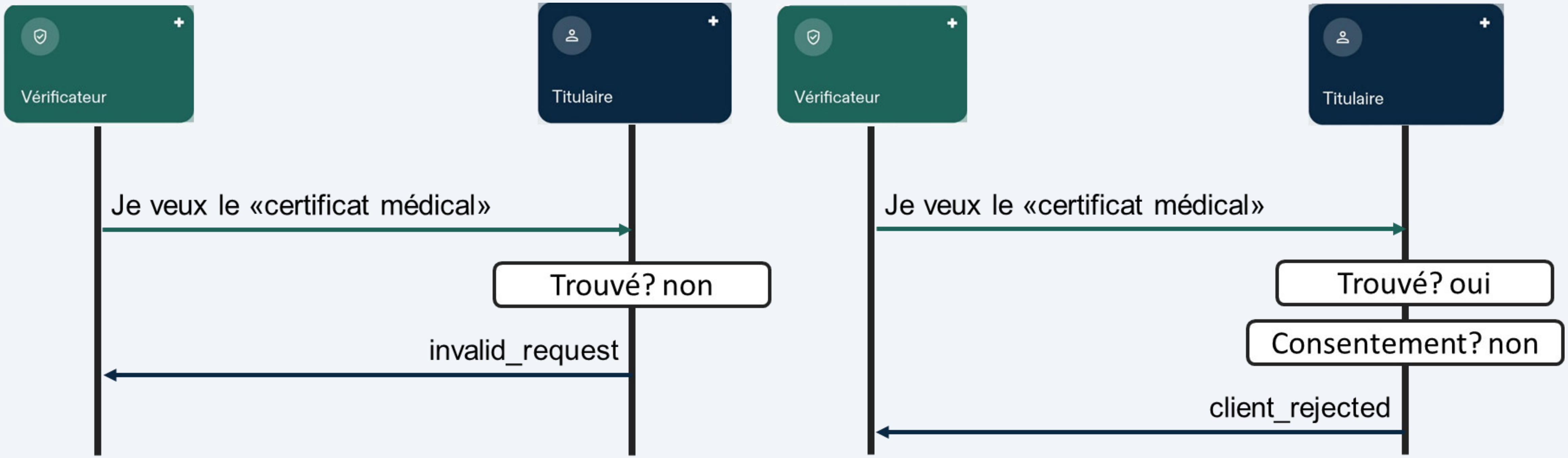
- 95 points faibles / risques
- 58 risques faibles, 29 risques moyens, 8 risques élevés et 0 risque critique
- 49 déjà traités pour la bêta publique
- Liste de toutes les vulnérabilités encore ouvertes publiée



Probabilité \ Impact	Bas	Moyen	Haut	Critique
Bas	31	21	4	5
Moyen	6	16	6	2
Haut	1	2	1	0
Critique	0	0	0	0

Attaque par canal latéral sur la présentation

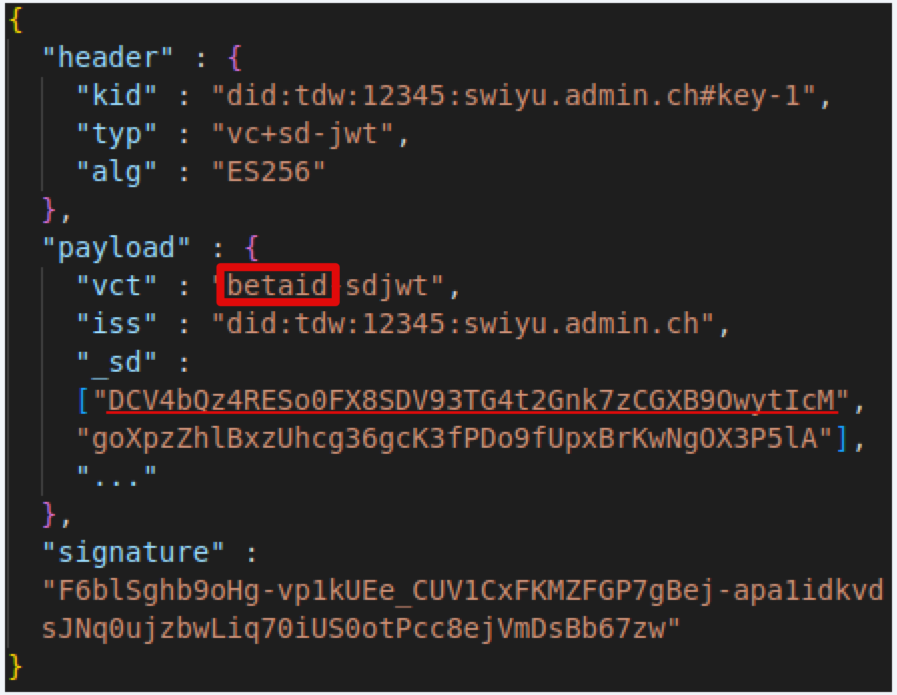
Risque	Impact	Probabilité
Moyen	Moyen	Hoch



Contourner la vérification

Risque	Impact	Probabilité
Haut	Critique	Moyen

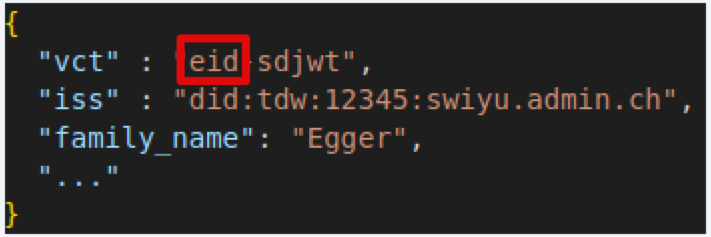
Avant la vérification



```
{
  "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"
}
```

Echanger

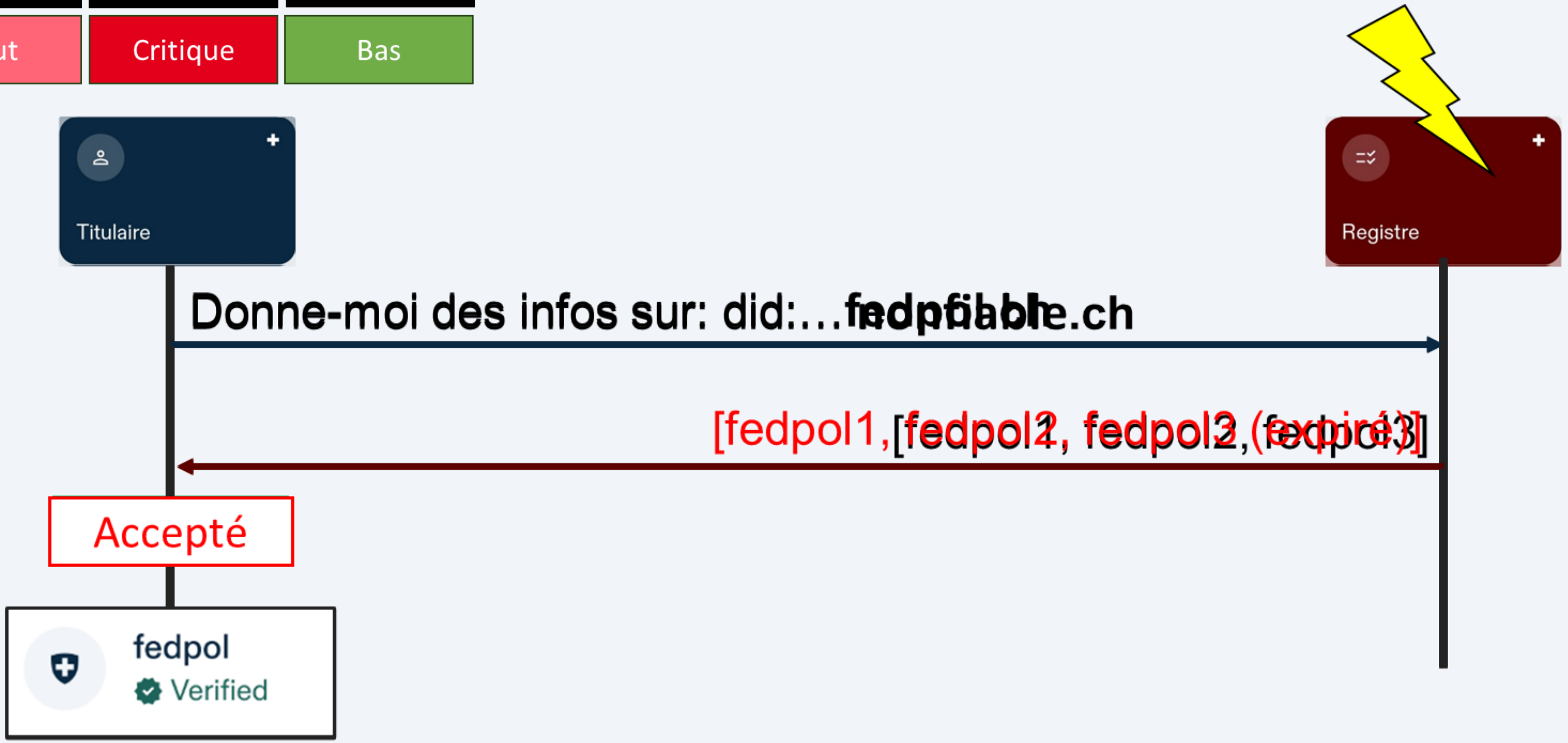
Après la vérification



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

Absence de validation du registre de confiance

Risque	Impact	Probabilité
Haut	Critique	Bas


Titulaire
Registre
Donne-moi des infos sur: did:…fedpol.ch
Donne-moi des infos sur: did:…nonfiable.ch
[fedpol1, fedpol2, fedpol3]
[fedpol1, fedpol2, fedpol3 (expiré)]
Accepté
fedpol
Verified

Résumé

- Première ébauche d'un modèle de menaces pour 2026
- Arbres d'attaque
- Analyse de la sécurité
- Assistance à la correction des vulnérabilités (49 / 95 déjà corrigées)

À emporter

- Bon de commencer avec la bêta publique
- La sécurité est un processus
- Programme de bug bounty

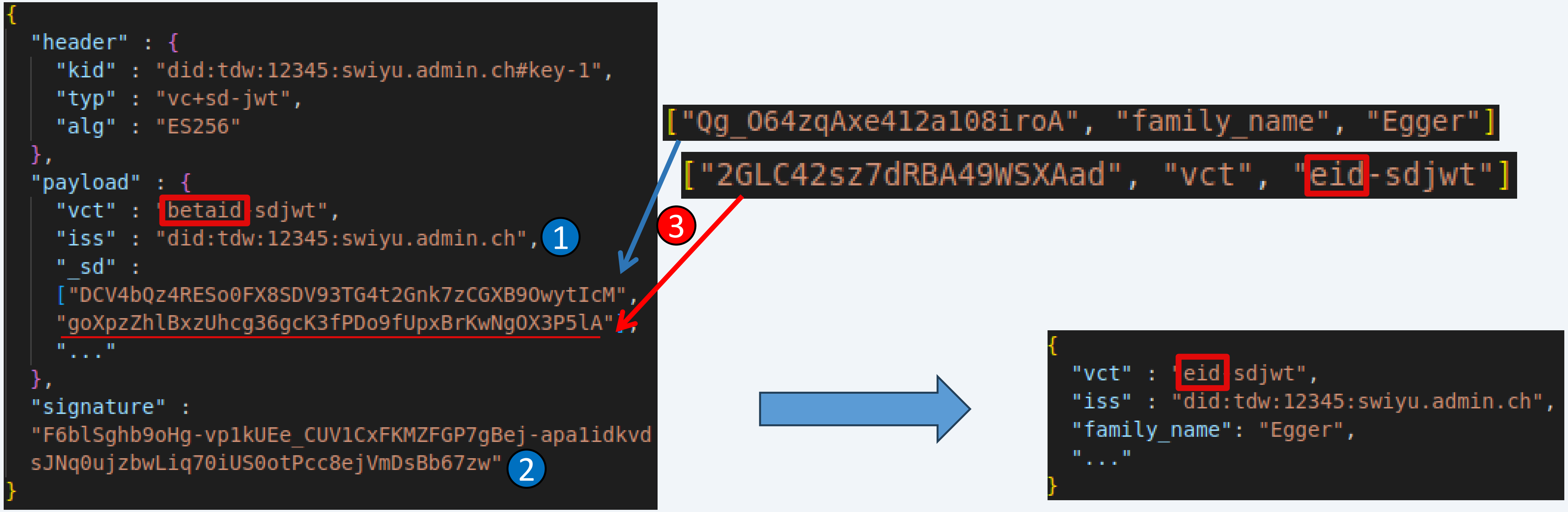
Travaux futurs

- Étendre le contrôle de la sécurité
- Analyse de la sécurité des standards implémentés

Diapositives supplémentaires

Vérification Contourner

Risque	Impact	Probabilité
Haut	Critique	Moyen



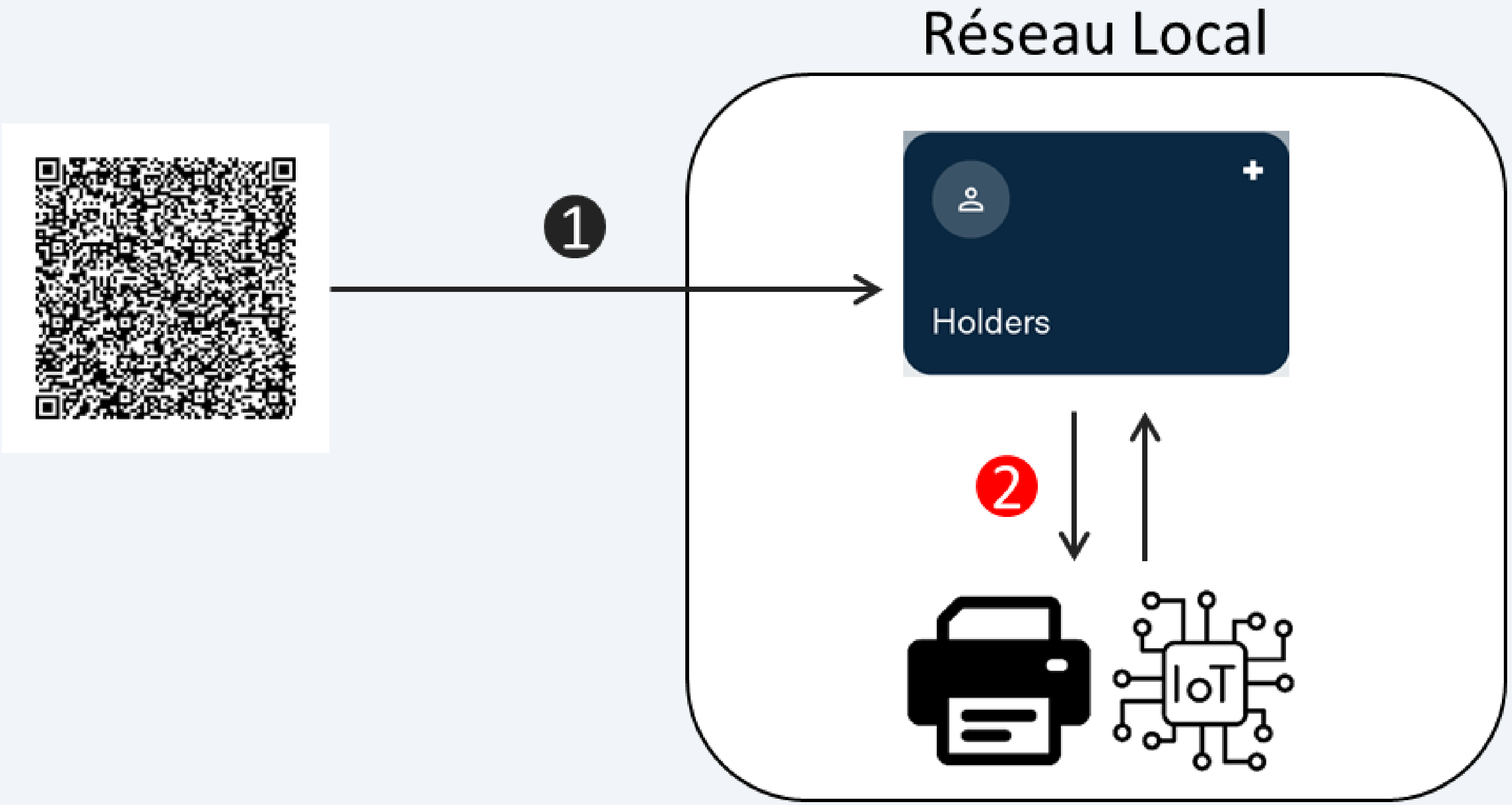
```
{
  "header" : {
    "kid" : "did:tdw:12345:swiyu.admin.ch#key-1",
    "typ" : "vc+sd-jwt",
    "alg" : "ES256"
  },
  "payload" : {
    "vct" : "betaid-sdjwt",
    "iss" : "did:tdw:12345:swiyu.admin.ch",
    "_sd" :
    ["DCV4bQz4RESo0FX8SDV93TG4t2Gnk7zCGXB9OwytIcM",
    "goXpzZhlBxzUhcg36gcK3fPDo9fUpxBrKwNgOX3P5lA"],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

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

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

Demandes de réseau local

Risque	Impact	Probabilité
Moyen	Moyen	Moyen


Réseau Local
1
Holders
2
IoT