A practical trust registry for SSI

Master thesis outline

Hes·so Master

adnovum Security Solutions

Student	Nathan Séville
Teacher in charge	Sylvain Pasini
Adnovum mentoring	Michel & Roman
Academic year	2022-2023

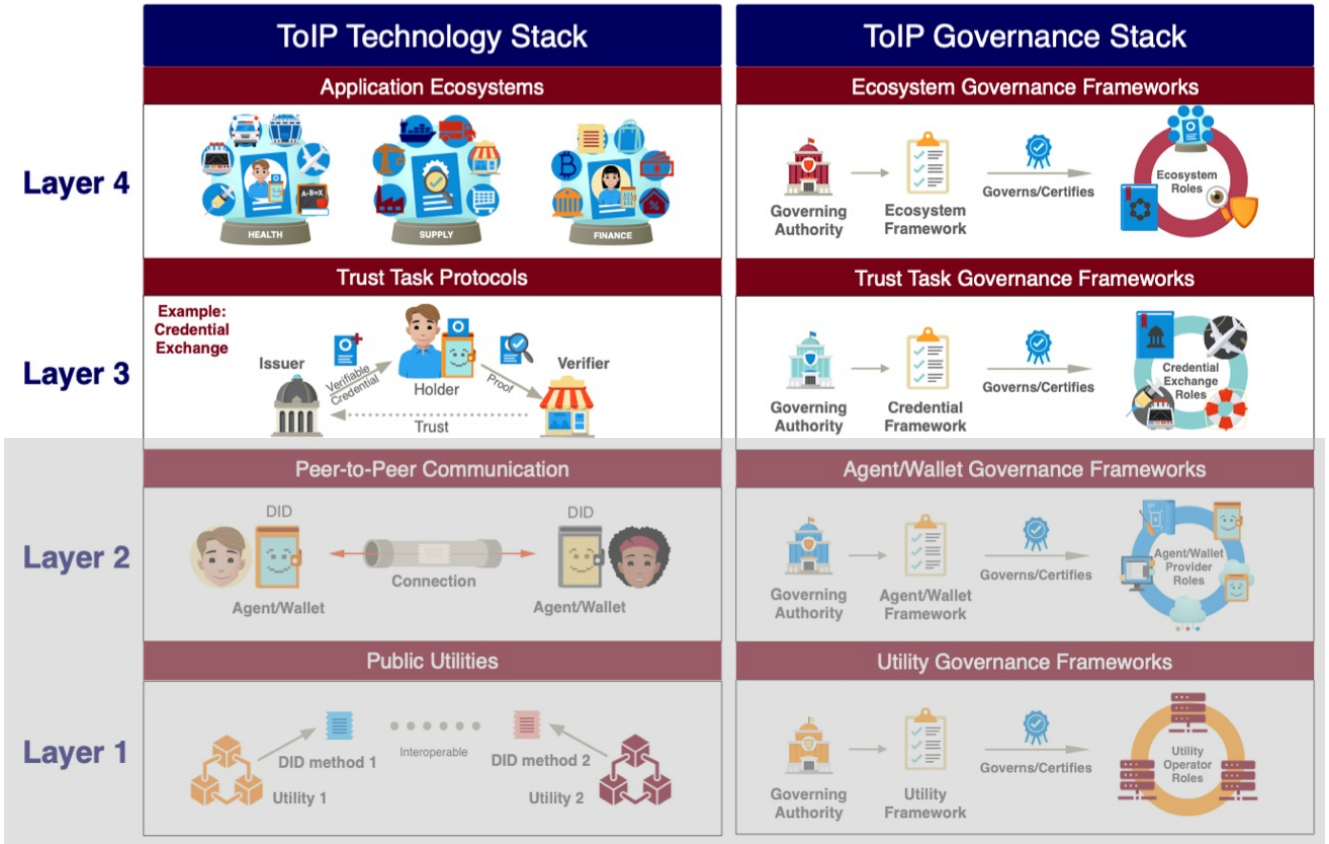
Trust registries in SSI

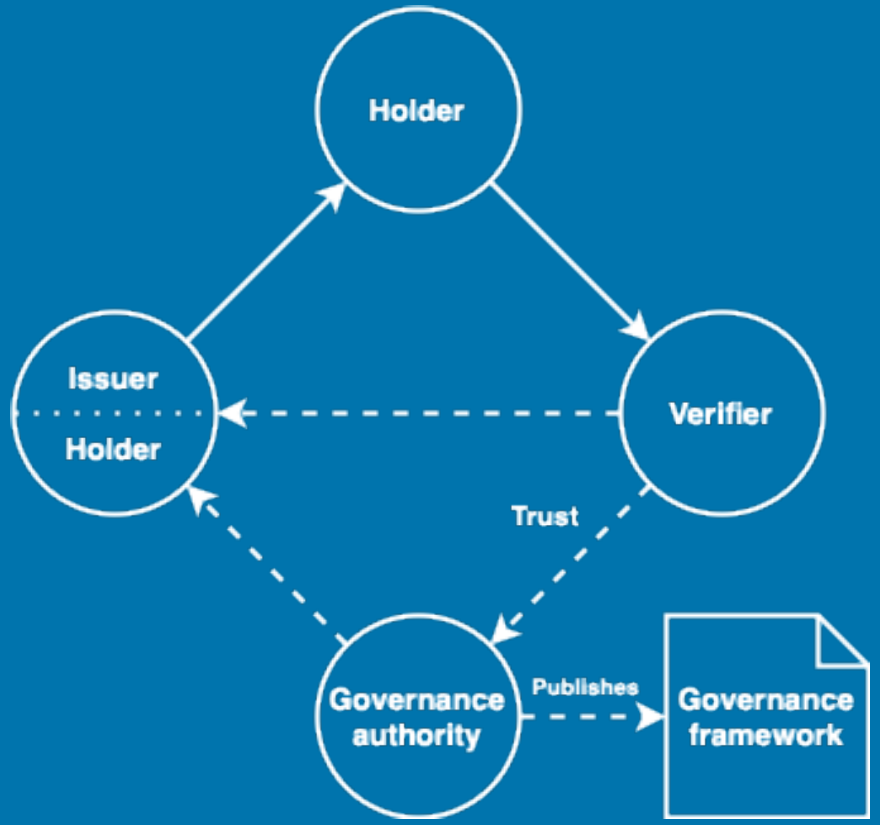
Why is it required ?

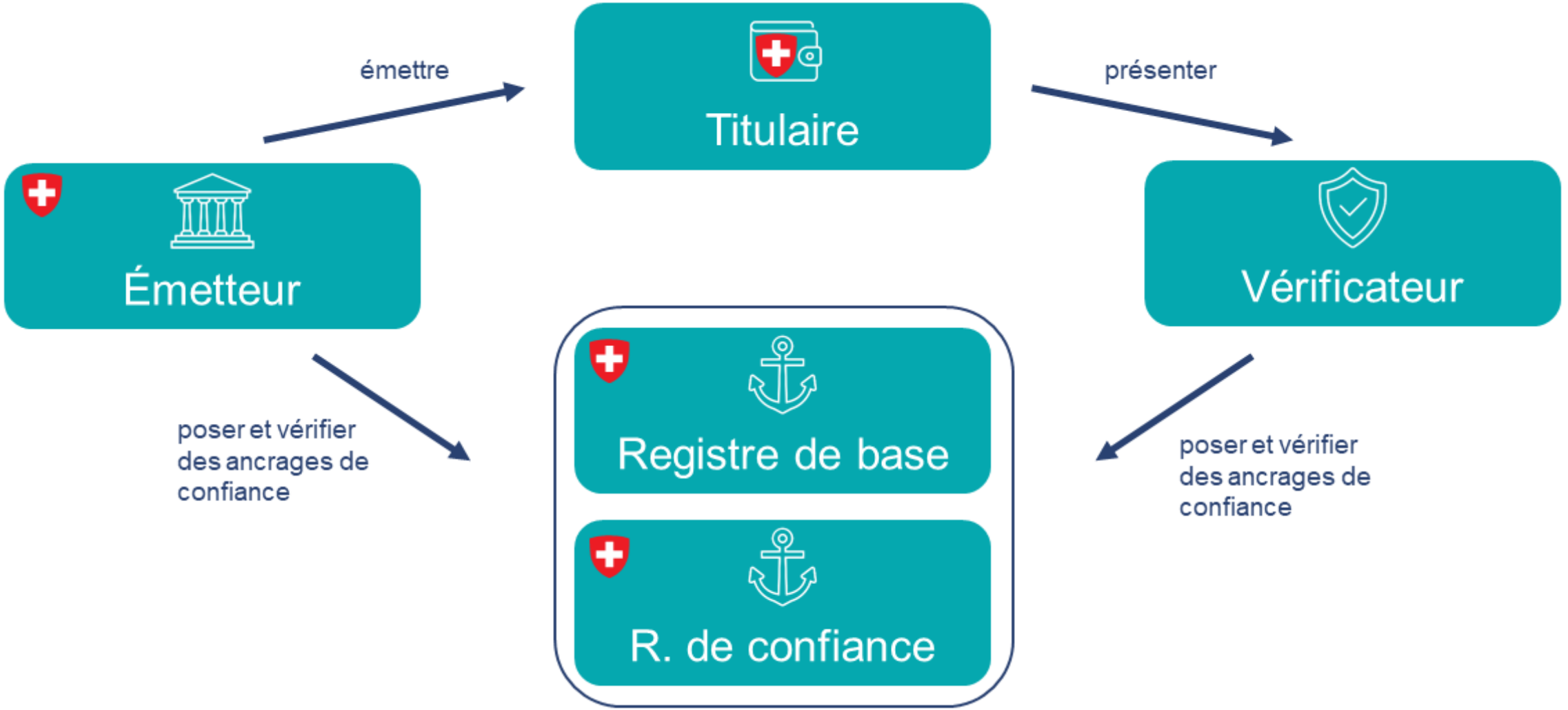
- SSI aims to be an open system

- There is a need be able to identify authorised issuer and verifier
- A reliable and automated procedure must be used

Ecosystems & Governance

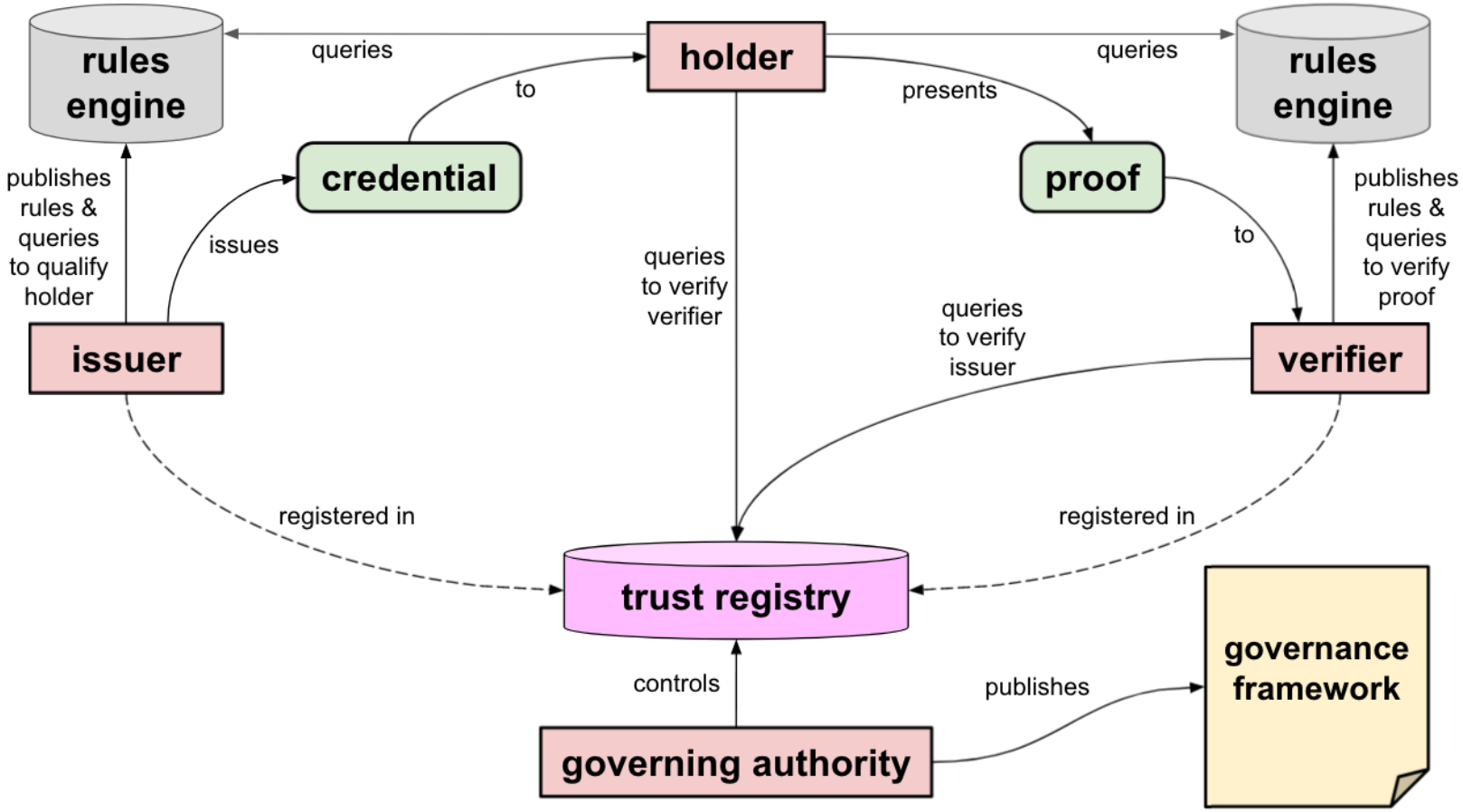





émettre
Titulaire
présenter
Émetteur
Vérificateur
poser et vérifier
des ancrages de
confiance
Registre de base
R. de confiance
poser et vérifier
des ancrages de
confiance

The practical solution

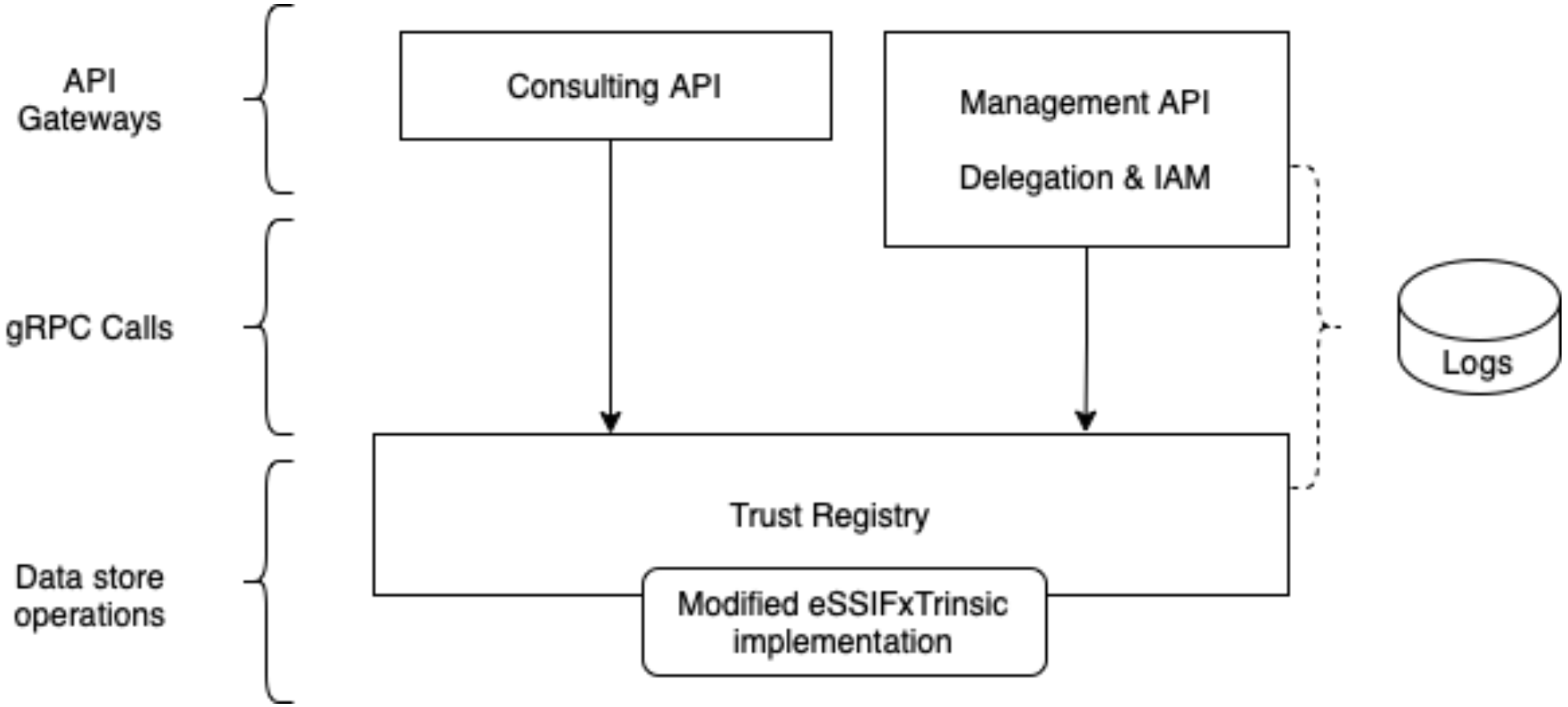
ToIP Trust Registry Protocol



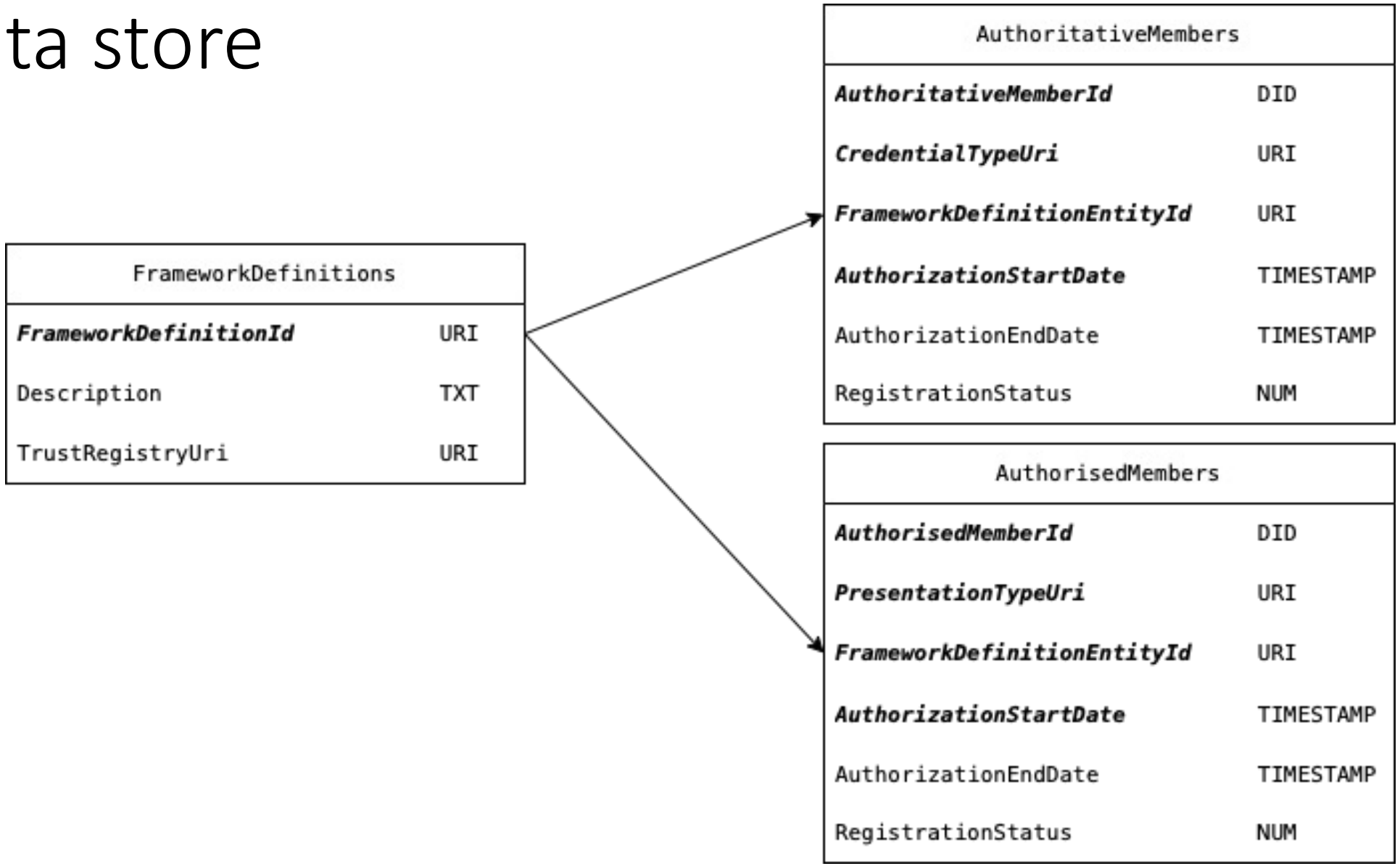
Implementation

- Follows the ToIP specification
- Main functionalities
  - Multiple ecosystem governance framework
  - Register and revoke authorized issuer
  - Register and revoke authorized verifier
- Keep history of authorization

Architecture



Data store


FrameworkDefinitions
FrameworkDefinitionId URI
Description TXT
TrustRegistryUri URI
AuthoritativeMembers
AuthoritativeMemberId DID
CredentialTypeUri URI
FrameworkDefinitionEntityId URI
AuthorizationStartDate TIMESTAMP
AuthorizationEndDate TIMESTAMP
RegistrationStatus NUM
AuthorisedMembers
AuthorisedMemberId DID
PresentationTypeUri URI
FrameworkDefinitionEntityId URI
AuthorizationStartDate TIMESTAMP
AuthorizationEndDate TIMESTAMP
RegistrationStatus NUM

Entity statuses

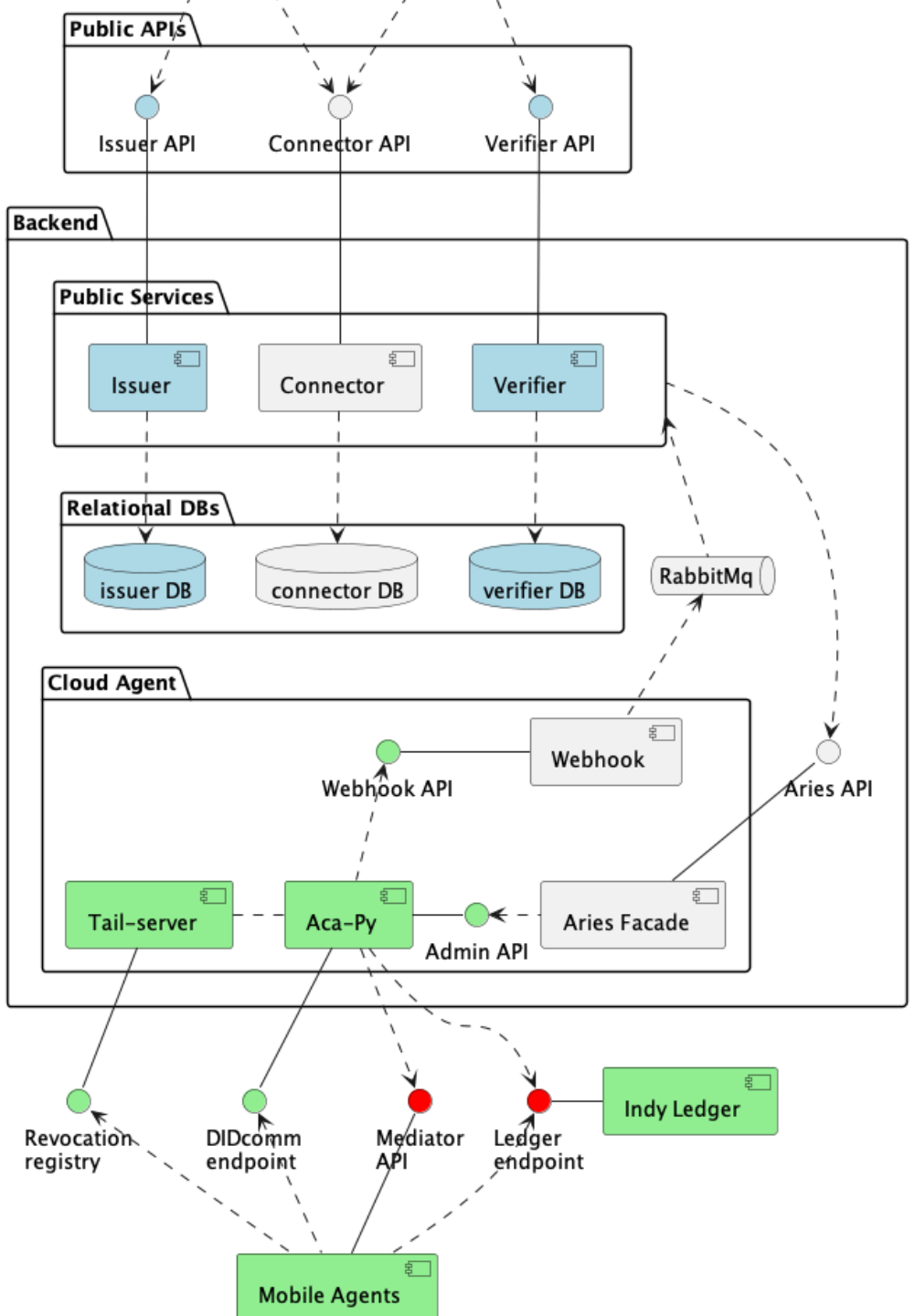
CURRENT	The entity is currently authorized, as of time of the query.
EXPIRED	Entity rights have expired.
TERMINATED	Entity has voluntarily ceased Issuer role under the specific EGF.
REVOKED	Entity authority under specific EGF was terminated by the governing authority.
NOT_FOUND	The entity was not found for the given EGF and credential type.

Integration

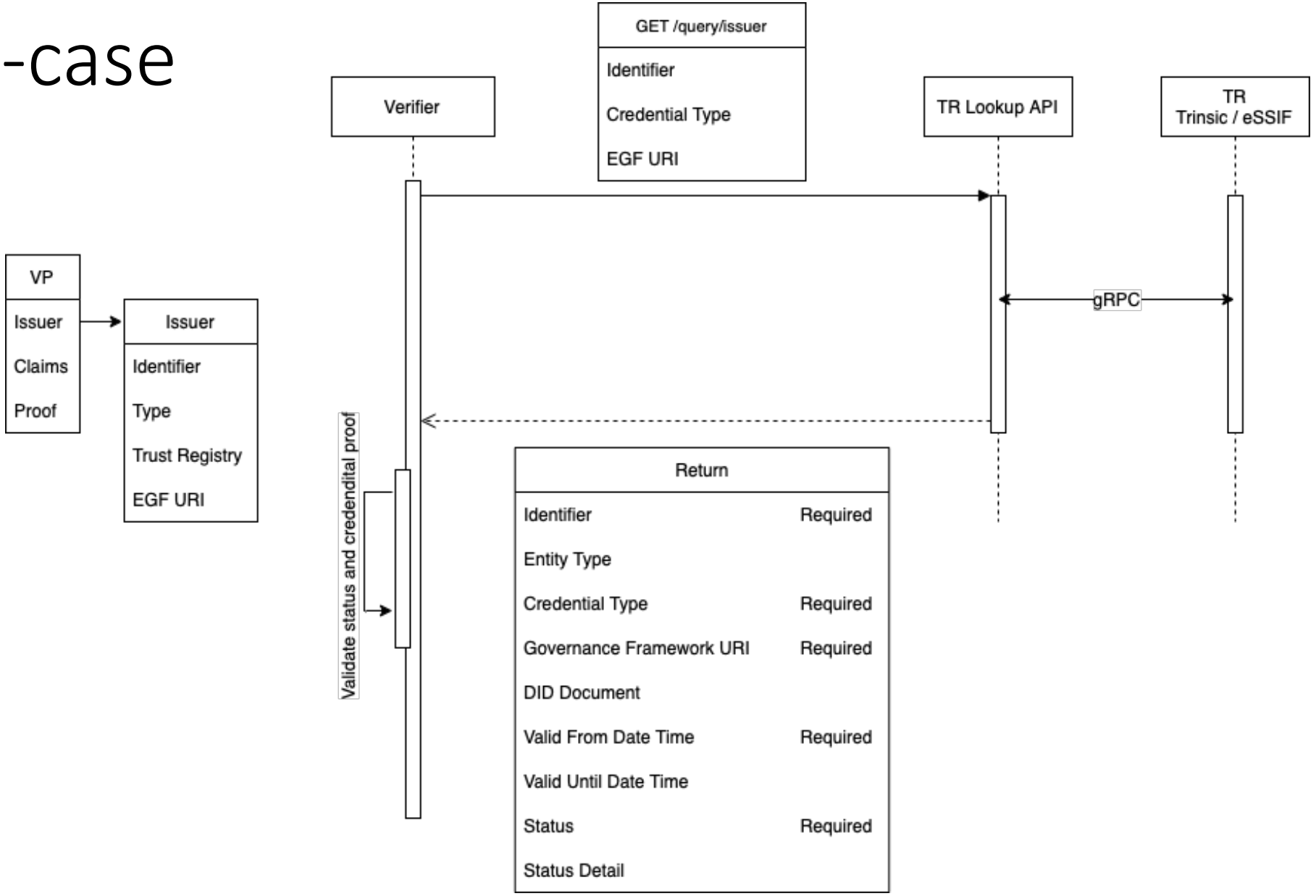
- ACA-Py Plugin

- Keeps the system consistent
- Can be used by other instances

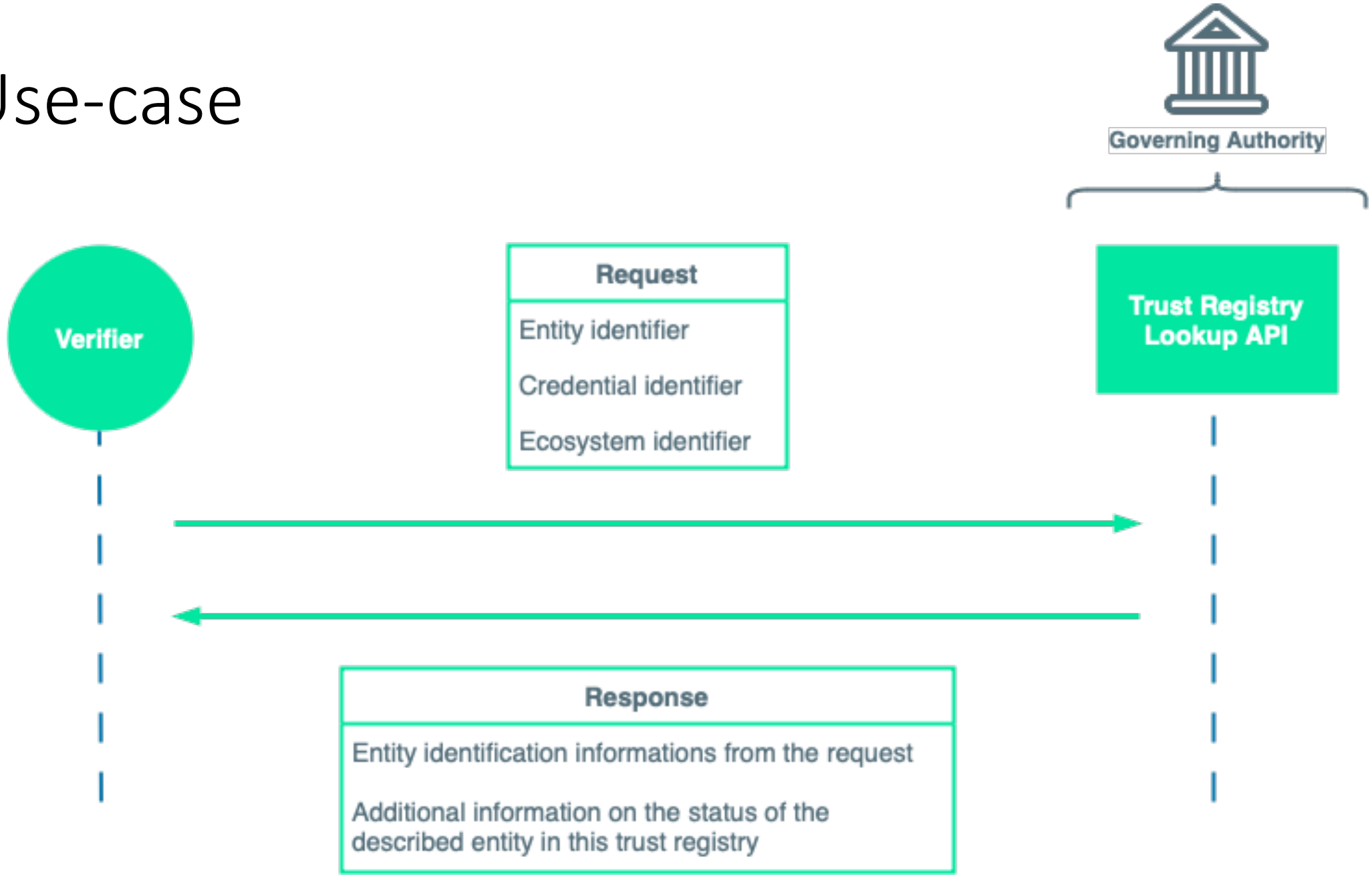
- Verifiable Credential Management System
- https://github.com/SSI-Solutions/vcms



Use-case


GET /query/issuer
Identifier
Credential Type
EGF URI
Verifier
TR Lookup API
TR
Trinsic / eSSIF
gRPC
VP
Issuer
Claims
Proof
Issuer
Identifier
Type
Trust Registry
EGF URI
Validate status and credendital proof
Return
Identifier Required
Entity Type
Credential Type Required
Governance Framework URI Required
DID Document
Valid From Date Time Required
Valid Until Date Time
Status Required
Status Detail

Use-case


Governing Authority
Verifier
Request
Entity identifier
Credential identifier
Ecosystem identifier
Trust Registry Lookup API
Response
Entity identification informations from the request
Additional information on the status of the described entity in this trust registry

Conclusion

Merci !

Sources

SlIde 3: ToIP Stack

https://trustoverip.org/toip-model/

Slide 3: Trust Diamond

Alex Preukschat. Self-sovereign identity: decentralized digital identity and verifiable credentials. Shelter Island, NY: Manning, 2021.

Slide 4: e-ID Components

The Federal Assembly of the Swiss Confederation. Avant-projet - Loi fédérale sur l'identité électronique et autres moyens de preuve électroniques.
https://www.eid.admin.ch/eid/fr/home/dokumentation/nsb-news_list.msg-id-89515.html

Slide 6: ToIP Trust Registry Protocol v1

https://github.com/trustoverip/tswg-trust-registry-tf/blob/main/docs/ToIP%20Trust%20Registry%20V1%20Specification.md

Slide 11: Adnovum VCMS components view

https://github.com/SSI-Solutions/vcms