

EFWG 2022-10-13 Meeting - Trinsic

Meeting Schedule

- Bi-Weekly at 8:00-9:00 am PST / 11:00-12:00 am EDT / 15:00 – 16:00 UTC / 17:00 - 18:00 CET
- <https://zoom.us/j/95389236256?pwd=RFErMm9SS0tBenA1Q0dSYlpXK3Bqdz09>

Attendees

- [Steve Magennis](#)
- [Eric Drury](#)
- [Carly Huitema](#)
- [P A Subrahmanyam](#)
- Fireflies.ai Noetaker Mark
- Richard Zbinden (new)
- Vlad Zubenko
- Anita Rao
- Callum Haslam
- Charles Macpherson (new)
- Jason (new)
- Chi Hwa Tang
- dhoffman
- Gary de Beer
- Jacques Bikoundou
- Jorge Flores
- Ken Garner
- Neil Thomson
- Phil Wolff
- Richard Zbinden
- Savita
- Scott Perry
- [Sumabala Nair](#)
- Thomas
- Tomislav Markovski
- Trinh

Presentation Files

- [Presentation slides](#)
- [Example VCs showcased during the Demo](#)
- [Trinsic's open source implementation of Trust Registry with eSSIF Lab](#)

Recording

- [Meeting Recording](#)

Notes

Agenda Items & Meeting Notes


- Welcome & Introductions
 - EFWG Community Topics & Announcements
 - Presentation from Trinsic: "Solving Governance in SSI Ecosystems with Trust Registries"
 - Q&A / Discussion
-
- Ecosystem white paper passed by all members present with no dissent
-
- Tomislav Markovski presenting Ecosystem Governance and SSI - Trust Registries



Ecosystem Governance & SSI


Trust Registries

Tomislav Markovski
Trinsic



Importance of Governance in Identity

To provide a layer of trust in an open ecosystem



- Importance of Governance in Identity - to provide a layer of trust in an open ecosystem
 - need to protect authentic data

Examples of Technical Approach to Governance

- Single authority
- Multiple authorities (enterprise network, consortium, etc)
- Authority Delegation
- Reputation based
- Voting based



Multiple approaches to Governance - who provides the root of trust

- First three - are fairly decentralized methods
- last two more decentralized model

Trust Registry

Governance problem to solve:

- Can Acme act as an issuer of Driver's License under the authorized license issuers act?
- Is this verifier authorized to verify this credential type under the given ecosystem governance framework?



Trust Registry

Practical problems to solve

- It is infeasible for all verifiers to maintain lists of all authorized members in a given ecosystem governance framework
- Cross ecosystem trust establishment



- Trust Registry
 - answers if an ecosystem participant has authority to act according to governance framework
 - practical problem - how for all verifiers maintain lists of all authorized members in a given ecosystem
 - cross ecosystem trust establishment - different ecosystems can identify other ecosystem's trust registries that they also trust
- Participants don't have to trust ecosystem itself, but that data providence is trusted

Types of Trust Registries

- Collection based
 - Databases
 - ACL (access control lists)
- Privacy-preserving
 - Cryptographic Accumulators
 - Merkle Trees



Types of trust registries

- Thinking about them in term of technical solutions
- Not just a list of members, can be other types as well

- Trinsic has done work with centralized trust registries

ToIP Trust Registry Protocol Specification

- Governing Authority
- Ecosystem Governance Framework
- Authoritative Member
- Authorized Action (Issue, verify)
 - Authorized Data Type (Credential, Presentation, Schema)
- Trust Registry



ToIP trust registry protocol specification

Related Efforts

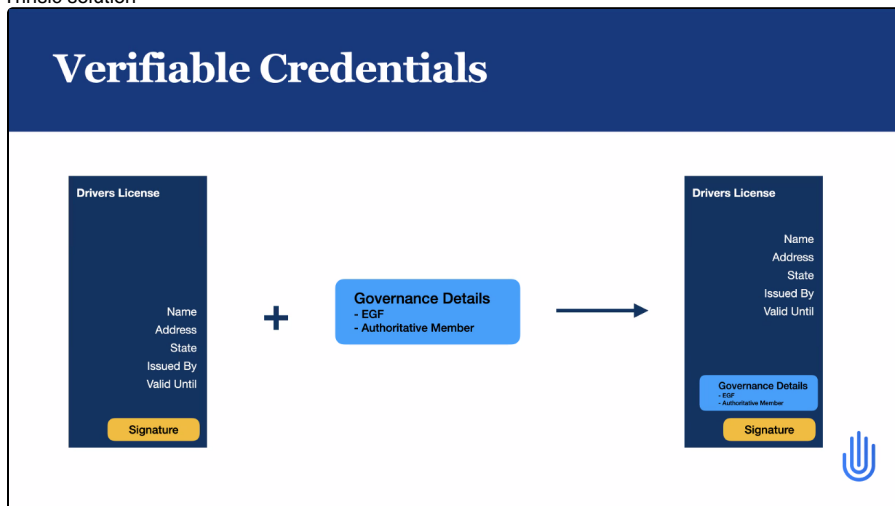
- Trust Establishment (status: Strawman) - incubated at DIF
<https://identity.foundation/trust-establishment/>
- TRAIN project (TRust mAnagement INfrastructure) -
incubated at eSSIF Lab
<https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/>



Related efforts

- Trust Establishment currently under early development <https://identity.foundation/trust-establishment/>
- TRAIN- registering definitions of credential schemas <https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/>

- Trinsic solution



- the ToIP trust registry specification merged with verifiable credentials
- No information coded in credential how valid is the credential
 - in an open ecosystem can have anyone issuing credentials
 - add the governance information to the credential for referencing.
 - Can validate the issuer ID but also the governance associated with it.
- Demo - no yet in production, CLI demo,

Demo

Trust Registries with Verifiable Credentials in the Trinsic Ecosystems platform



```

credential-1.json > {} credentialStatus
1 {
2   "context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://w3id.org/bbs/v1",
5     "https://schema.trinsic.cloud/tm/iso18013-drivers-license/context"
6   ],
7   "credentialSchema": [
8     {
9       "id": "https://schema.trinsic.cloud/tm/iso18013-drivers-license",
10      "type": "JsonSchemaValidator2018"
11    }
12  ],
13  "credentialStatus": {
14    "id": "urn:revocation-registry:tm:T96PMDpPulDvBwMjKcZ3M2",
15    "revocationListCredential": "urn:revocation-registry:tm:T96PMDpPulDvBwMjKcZ3M2",
16    "revocationListIndex": "2",
17    "type": "RevocationList2020Status"
18  },
19  "credentialSubject": {
20    "birthdate": "1998-08-28",
21    "documentNumber": "542426814",
22    "expiryDate": "2025-01-01T00:00:00Z",
23    "givenName": "John",
24    "id": "urn:uuid:7c855b6437084fee8888b0870a48478",
25    "issuanceDate": "2022-09-29T12:42:11.120824Z",
26    "issuingAuthority": "CO",
27    "issuingCountry": "US",
28    "lastName": "Doe"
29  },
30  "id": "urn:uuid:7c855b6437084fee8888b0870a48478",
31  "issuanceDate": "2022-09-29T12:42:11.120824Z",
32  "issuer": {
33    "did:ion:test:EiCqUlyywaDQZLhSb0_R-hTnaMEVYq4ben5Q7wa1Q",
34    "proof": {
35      "created": "2022-09-29T12:42:11Z",
36      "proofPurpose": "assertionMethod",
37      "proofValue": "scM@pkmzmgZ25PPGK9ccq/ge2htcn8sl/pYIXG1ZtZ2kavLfoEKUV"
38    }
39  }
40 }

credential-2.json > {} @context > 2
1 {
2   "context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://w3id.org/bbs/v1",
5     "https://schema.trinsic.cloud/tm/iso18013-drivers-license/context"
6   ],
7   "credentialSchema": [
8     {
9       "id": "https://schema.trinsic.cloud/tm/iso18013-drivers-license",
10      "type": "JsonSchemaValidator2018"
11    }
12  ],
13  "credentialStatus": {
14    "id": "urn:revocation-registry:tm:F2h6qwohG2DhbyJfLWl#3",
15    "revocationListCredential": "urn:revocation-registry:tm:F2h6qwohG2DhbyJfLWl",
16    "revocationListIndex": "3",
17    "type": "RevocationList2020Status"
18  },
19  "credentialSubject": {
20    "birthdate": "1998-08-28",
21    "documentNumber": "542426814",
22    "expiryDate": "2025-01-01T00:00:00Z",
23    "givenName": "John",
24    "id": "urn:uuid:c8834a1257df44a6bdf796fb07e2cf01",
25    "issuanceDate": "2022-09-29T12:43:07.6591340Z",
26    "issuingAuthority": "CO",
27    "issuingCountry": "US",
28    "lastName": "Doe"
29  },
30  "id": "urn:uuid:c8834a1257df44a6bdf796fb07e2cf01",
31  "issuanceDate": "2022-09-29T12:43:07.6591340Z",
32  "issuer": {
33    "did:ion:test:EiB267e1hMFFFe3YEus3PM7316TygAqQ2G8Y6Wm1g",
34    "proof": {
35      "created": "2022-09-29T12:43:07Z",
36      "proofPurpose": "assertionMethod",
37      "proofValue": "pVJw/LLzWry08UrtK5a3n261AbJcn9Y14DM/4z7PR00p0wFpruyLj1B5qfx01JNK"
38    }
39  }
40 }
  
```

- two VC demos, good and bad actor issuers and with and without governance for verification

The first screenshot shows two JSON files: `credential-1.json` and `credential-2.json`. `credential-1.json` contains a `credentialSubject` and a `credentialSchema` pointing to a schema. `credential-2.json` contains a `credentialStatus` and a `credentialSubject` with a `birthDate`.

The second screenshot shows the terminal output of the command `trinsic vc verify-proof --proof-document ./tr-credential-2.json`. The output indicates that the credential is valid, with no messages from the status, issuer, or schema checks.

The third screenshot shows the terminal output of the command `trinsic vc issue`. The output shows a new credential being issued, including fields like `issuingCountry`, `lastName`, `id`, `issuanceDate`, `issuer`, `proof`, and `proofPurpose`.

- Demo on good actor first confirms credentials are valid, not revoked, schema conforms, valid issuer, and signature verified for both good and bad actors.
- All the checks pass because there is nothing wrong with both credentials.
- How do you know? Trust Registry solves this.
- Issue a credential with governance information encoded.
- There is an issuer field extension to the VC, in the credential - not just the issuer DID. It includes claims of which governance framework and trust registry it belongs to.

The top screenshot shows two JSON files in a VS Code editor. The left file, 'tr-credential-1.json', contains a credential object with fields like 'expiryDate', 'givenName', 'id', 'issueDate', 'issuingAuthority', 'issuingCountry', 'lastName', 'id', 'issuanceDate', 'issuer', 'governanceFramework', 'trustRegistry', 'proof', 'proofPurpose', 'proofValue', 'type', 'verificationMethod', and 'type'. The right file, 'tr-credential-2.json', contains a similar object with additional fields like 'credentialSchema', 'credentialStatus', 'credentialSubject', and 'documentNumber'.

The bottom screenshot shows the same files with a terminal window open at the bottom. The terminal displays the output of a verification command, showing that the credential is valid and the issuer is authorized.

- Now verification doesn't work for the bad actor because the trust registry membership fails (an additional check)

```

~/tm → trinsic trust-registry get-membership-status `
>> -s https://schema.trinsic.cloud/tm/iso18013-drivers-license `
>> -f https://example.com/authorized-issuers `
>> -d did:ion:test:EiC0qiV_y1waDQZL0h5bQ_R--hTmaWEYvIq4ben5Q7WaiQ
ok
status → "Current"
~/tm → trinsic trust-registry get-membership-status `
>> -s https://schema.trinsic.cloud/tm/iso18013-drivers-license `
>> -f https://example.com/authorized-issuers `
>> -d did:ion:test:EiBZG7eihMFPFFFFe3YEuS9JPNT516TygAq2690Y6MnR1g
ok
status → "NotFound"
~/tm → trinsic trust-registry get-membership-status `
>> -s https://schema.trinsic.cloud/tm/iso18013-drivers-license `
>> -f https://example.com/authorized-issuers `
>> -d did:ion:test:EiBZG7eihMFPFFFFe3YEuS9

```

- Is there a list of EFGs and how do you discover them?
 - No list of Ecosystem Governance Frameworks that exist that someone maintains
 - Presumably it would be published on the website
- What controls are required to prevent bad actors from adding records to trust registries?
 - Depends on security and design of trust registries -it depends on who manages the registry.
- How will a standard schema be adopted for a given verifiable credential? Who drives it?
 - Community, adoption, large corporations, open standards e.g. mDL

- Schemas - will be interesting how communities adopt schemas. Centralizing and standardizing will develop
- Q. What's next for your project? Where is it going in the next six months or so?
 - Better management tools.
 - Adding privacy preserving trust registries, especially based on accumulators (useful also for revocation)
- Q. What do you hope to learn early in deployment?
 - How customers use the product
- Q. How much do various credential ecosystem parties have to do to extend what they do to include the registry?
 - minimal - current trust registry is membership based, just add and remove members
 - extensions possible
 - e.g. can be member of multiple governance frameworks/trust registries
- Concerns - correlation attacks, e.g. info leaks from the issuer identity

Admin Reminder : remember to re-subscribe to new meeting calendar

If you want your name on the invite, reach out to [Elisa Trevino](#) (on slack), she will put your name in the calendar invite to make sure that the invite is sent out each time.

Coming up

- Resuming regular schedule Sept 15
- Next presenter, Sept 29: Trinsic Trust Registry solution