Authorized Issuer Lists

By Manu Sporny <msporny@digitalbazaar.com>

Trust can be more difficult to establish in decentralized systems than in centralized ones. For example, how do you know whether to trust a Verifiable Credential Issuer? As the Verifiable Credentials ecosystem grows, and the number of Issuers increases, it will become increasingly difficult for Verifiers to vet every Issuer of a Verifiable Credential. This paper explores mechanisms that could be used by Verifiers to bootstrap which Issuers they should trust to issue specific Verifiable Credentials.

The AuthorizedIssuerList Verifiable Credential

This paper proposes a new Verifiable Credential called an `AuthorizedIssuerList`, which could take the following form:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v2",
    "https://w3id.org/vc/ail/v1"
  ],
  "issuer": "did:web:authority.example",
  "issuanceDate": "2023-02-13T00:18:30.053Z",
  "type": ["VerifiableCredential", "AuthorizedIssuersCredential"],
  "credentialSubject": [{
    "id": "did:web:issuer.example",
    "type": "AuthorizedIssuer",
    "authorizedToIssueCredential": [{
      "type": "UniversityDegreeCredential",
      "credentialSchema": {
        "id": "https://issuer.example/degree.json",
        "type": "AuthorizedIssuerJsonSchema2022"
      }
    }, {
      "type": "StudentIdCredential",
      "credentialSchema": {
        "type": "AuthorizedIssuerJsonSchema2022",
        "schema": "{\"properties\":\{\"credentialSubject.state\":\"NV\"}}"
      }
    }]
  },
  "proof": { ... }
}
```

The format above would enable Verifiers to injest a list of authorized issuers for a particular set of credentials.

Authorized Issuer List Use Cases

What follows below is a preliminary set of use cases that an Authorized Issuer List credential might address:

Elena is an IT Administrator at a hiring department at a mid-size company that would like to vet job applicants as having received their degrees from an accredited college or university. Elena configures their hiring software to refer to multiple lists containing several hundred organizations that are curated by the various accreditation bodies that they trust.

Pietor is a hiring manager that is looking through a list of job applicants that have submitted their digital resumes. One of the resumes is flagged as containing a Verifiable Credential from an issuer that is not on any of the approved authorized issuer lists. Pietor performs a vetting process on the issuer and finds out that the organization is newly accredited but has not yet been added. Pietor adds the organization to their internal list of trusted issuers.

Corban works at an accreditation body and is responsible for constructing the list of authorized issuers. Corban sends an email requesting a Verifiable Credential from every authorized issuer that they know of stating which credentials they are interested in issuing. Once Corban vets each issuer, he places them in the authorized issuer list if they meet the accreditation body's vetting criteria.

Broni has noticed that DiplomaMill, Inc. has lost its accreditation status and, while the organization is included in an authorized issuer list that they use, that they no longer want to recognize DiplomaMill as a authorized issuer. Broni configures their software with an exception to reject DiplomaMill Verifiable Credentials that were issued after the current year.

John is reviewing suppliers for a food product they are bringing to market. The food company John works for desires to ensure that their suppliers not only meet organic certification for their country of origin, but also that they produce food in a manner that is free from forced labor. John checks the list of organic certifiers against a regulatory list of country of origin approved suppliers, filters his supplier list to only those that have VCs showing organic certification issued by a certifier that meets the regulatory requirements. He further checks that list against a list of company approved trusted issuers that certify labor practices.

Jan is a customs agent who needs to set policy regarding the import of goods into his country. He reviews various entities that issue Verifiable Credentials related to the identity of business and their subsidiaries. If their company review practices meet the rigor required by his state legislation, he adds the issuer to an approved list of issues related to company identity for importer of record status. He performs a similar review of product identification issuers, and adds those issuers to a product identification issuer list, provided that that issuer performs the significant inspection as required for certain products on a list maintaintained by his department to prevent tariff fraud.

Authorized Issuer List Requirements

The following is a list preliminary requirements from the use cases listed in the previous section:

- An Authorized Issuer List MUST be digitally signed such that it is clear which authority is providing the list.
- An Authorized Issuer List Entry MUST contain the type of Verifiable Credential that is authorized for issuance as well as the identifier for the issuer that is authorized to issue that credential.
- An Authorized Issuer List Entry MAY contain further contraints such as attribute values, geographic regions, times, or other limits on the properties of the issued credential.
- An Authorized Issuer List Entry MAY provide data format schema that MUST be used to detect if a Verifiable Credential is a match for the issuer.

It is expected that there are other requirements on an Authorized Issuer List data model; the list above is expected to grow during converastions at RWoT.

Relevant Work

The concept of Authorized Issuer Lists have been explored in at least the following venues:

- Trust Registries at ToIP Foundation
- Trust Establishment at DIF
- TRust mAnagement INfrastructure (TRAIN) at eSSIF-Lab
- Trust Registry at Trinsic

Collaboration at and Beyond RWoT 11

There are a number of open questions related to authorized issuer lists. These questions include:

- Should the `AuthorizedIssuer` digitally sign their list of credentials they are authorized to issue to ensure that an publisher doesn't include an issuer against their will?
- Should there be an API to define how these lists are managed such that issuers can update their own information in the list?
- Should the `authorizedToIssueCredential` property contain something more than a QueryByExample mechanism? What about JSON Schema?
- How many different data formats and proof formats should be supported?
- Should Verifiers be able to add to the list in their own configurations?
- How is trust in the list provider established?

The author of this paper seeks individuals that are interested in publishing lists of authorized issuers in a specific market vertical and would like to collect answers

to the questions above as well as other questions that ecosystem participants have.