Meeting notes

- 2023-01-16 Scope
- 2023-02-08 Trust & functional brainstorm
- 2023-02-14 Technical team discussion
- 2023-03-16 Working group periodic update

2023-01-16 Scope

This meeting was scheduled to determine the scope of the challenge and to make sure it was covered from multiple angles. 4 different vendors attended the meeting.

Resources

Video available @ youtube

Presentation available

Conclusion

The following points were concluded from the meeting:

- An authorization must be usable by any node/app from the organization which is authorized.
- Any node/app of an organization must accept this authorization
- Authorizations must only be issued to nodes that support the use-case
- Nodes/apps that issue authorizations must be authorized by the organization to do so for a use-case
- Authorizations must be automatically issued/revoked/sent when the topology changes (new nodes, nodes removed)
- The trust between the authorization issuer and authorization verifier within an organization requires extra care

Addtional notes

Currently the Nictiz qualification process can only qualify a pair of vendors/applications where each party covers the entire side of a use-case. Eg 1 side covers sending and the other receiving. It was concluded that to support multiple vendors properly, a combination of vendors at one side must be able to qualify as well.

2023-02-08 Trust & functional brainstorm

This live meeting was scheduled to get a first sense of direction. 2 subjects were on the agenda: how can one vendor trust the authorizations of another vendor within the same organisation context? And, what feature would allow authorizations to be used by multiple vendors.

Trust

The general direction that was decided on is to have a default level of trust between vendors. Vendors qualify their application and the care organisation only uses qualified applications. If a care organisation uses two vendors for a use case and both are qualified then those vendors automatically trust eachother within the context of that use case. Vendors will not require additional configuration or trust regarding that use case. This does mean that the care organisation has to authorize a vendor for a certain use case.

Functional solution

The main direction of the discussion is towards adding a functional identifier to an organisation credential and then use that identifier in the credential subject of a verifiable credential.

This changes the flow for requesting an access token. The requester will have to send both the authorization credentials and the organisation credential in the request. The combination of both credentials would satisfy the security constraints.

The issuer of the authorization credential will also have to monitor the network for any new organisation identifiers that match. When noticed, the DID that has received that functional identifier as subject will also have to receive an authorization credential.

Using a combination of organisation credential and authorization credential would allow the credential holder to use the authorization credential at a different verifier than the issuer. The verifier can validate the given credentials. How the verifier can check that one of its customers has the same functional identifier as the issuer is to be researched.

2023-02-14 Technical team discussion

With the Nuts technical team, consisting of the highest nuts-node code contributors, we discussed on how this feature could be supported. The following points have become clear from the discussion:

- AuthorizationCredentials will still be issued from and to a DID.
- `iss` and `sub` in the OAuth access token (request) will also remain a DID. This might be subject to change when the final design is being made.
- The result from the above two points is that the access token request will not need to contain any additional VCs/VPs.
- An issuer will have to respond to new DIDs that have the same logical identifier as DIDs that have already received an AuthorizatoionCredentials.
- A verifier will have to do a lookup on the issuer of the AuthorizationCredential and match it to a DID it controls via the logical identifier. The final design might also include the logical identifier in the access token request to prevent finding dupicates.

The points above require the following specification changes:

- Introduce the concept of a logical identifier.
- Implementations will need to be able to extract a logical identifier from a specific VC/VP. This probably needs to be configurable.
- Implementations will need to have a authorization registry where logical identifiers are mapped to AuthorizationCredential templates.
- Implementations will need to respond to new logical identifiers detected on the network and issue new AuthorizationCredentials to a DID
- Implementations will need to respond to revocations of identifiers revoke any AuthorizationCredential that has been issued using logical identifiers.
- Introduce the concept of scoping/purpose of use. Possibly enforced by a credential.

Additional implications for the network as a whole:

The working group already agreed on intra-vendor trust if the care organization approves both vendors for a particular use-case. This also means that both vendors are qualified to service that use-case. When looking at the Trust over IP model, this means that a use-case authority could perform the role of issueing a *scopeCredential* (needs better name). The combination of logical identifier and scope would allow nodes to automatically issue and trust AuthorizationCredentials.

Possible roadmap:

1. Place an IRMA signature on a contract using kvk credentials that link the vendor and scope to a logical identifier (kvk number)
2. Create and host *authority* software that issues a credential containing the scope. Care organizations can login on that software using the IRMA kvk credential. Administrators on

the software can approve specific vendors for a use-case.
3. LRZA also issues VCs. From the vendor, a care organization official jumps to the *authority* software (with a VP) and logs in using the kvk IRMA credential. It approves the scope and the *authority* software issues a VC to the care organization wallet. This slightly more complicated step is needed so the LRZA can revoke credentials for care organizations that are no longer a care organization.

Different time paths can be assigned to each step.

2023-03-16 Working group periodic update

Agenda

- Access token request
- templating
- filtering

Access token request

Currently RFC014 had a line in §4.2:

The credential issuer equals the sub field of the JWT in the access token request.

This will probably have to change to *the issuer must be trusted for the use-case*?

Templating

Because VCs ar not directly constructed but are to be constructed in response to *events* we'll need some sort of templating to create the right VCs. This has to be coordinated with efforts on implementing OIDC4VCI.

Filtering

To select the right *events* for VC generation, some sort of filtering language would be required. DIF presentation exchange seems the right candidate.