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.

Revision #1
Created 15 February 2023 07:25:26 by Wout Slakhorst
Updated 24 March 2023 10:41:13 by Wout Slakhorst