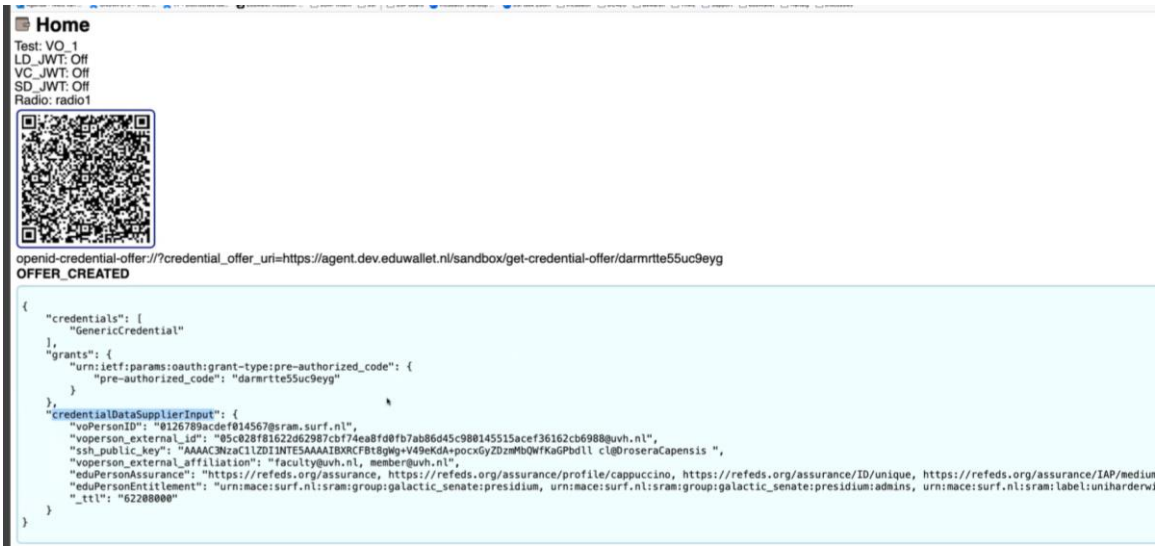
Minutes VC-Subcommittee November 22nd 2024

- Targeted model: In a targeted VC model, taking the **example of virtual organisations**, credentials would be scoped to the virtual organisation (in the screen-shot: "voPersonID": "… **@sram.surf.nl**") releasing the credential.

The "voperson_external_id" identifier value matches with the value of "eduperson_unique_id", so that there is a reference to the original university account. A set of values needed in the context of the research communities follow in "credentialDataSupplierInput": public key, external affiliation (very relevant because a specific affiliation to a particular organisation/institution is commonly the requirement to be a member of the virtual organisation: in the example the user should at least be a member@uvh.nl or a faculty@uvh.nl at the uvh), assurance and entitlement (most important part of the information being sent. It comprises some groups such as the presidium's group membership in the galactic senate or the group membership "admins" or the entitlement from the original institution "id_123456").



From the perspective of the verifier, in this model, requests are restricted to the VC type: basic academic VC for example.

- Requesting claim and applying selective disclosure (video min 00:21:00): In the wallet, if a verifier requests a generic VC "eduPersonEntitlement", any and all VCs stored in the wallet that satisfy this requirement would be presented to the user as a valid choice to respond to the verifier's request. To show this in the demo, the user's ("Linnaeus") virtual organisation credentials are intentionally created as incompatible (Galactic Senate and Rebel Alliance) – not desired by the user to be shown together. Users should be able/allowed to decide what claims to show from "Generic credentials".

An example to solve this, in the case that users do not want to show any "eduPersonEntitlement", but only a credential entitlement, "Elixir" for example, would be to request a specific "credential type" Elixir. That would help users. To facilitate the visualisation of VC types in the wallet the VC could be provided with their own display properties such as their own logos (colour schemes, etc.).

- Standardisation at the level of claims: The claims (attributes) definitions (for example multi-valued) are open. Useful for the definition would be to apply the suggested mapping from SAML to OIDC[1] (from

[1] Van Dijk, N. (2018) White Paper for implementation of mappings between SAML 2.0 and OpenID4 Connect in Research and Education. In: https://daasi.de/pub/20181011-OIDC-WP.pdf

attributes (SAML) towards claims (OIDC)). This could be proposed for consultation within the REFEDS community. At the moment, the mapping is only a recommendation and not an official document.

- Resource capability request (video min 00:28:00): In AARC, requests look up for capabilities instead of asking for values. It is like a translation process from the service. The person is a member of the virtual organisation, so that the resource access capability can be assigned.

There are two implications of these requests forms in the wallet:

1. If the verifier asks for an "eduPersonEntitlement" (in the example, from Galactic Senate, it could be all the Galactic Senate entitlements), the user selects one. If the user does not understand what to release (select among the different entitlement values), it could mean not to get the right one back.

2. The released value is negotiated between the research RI and the verifier. Technically speaking, the verifier could also be an issuer. In this case the research RI would not need to be there: the resource holder (i. e. computer facility) could act as the own issuer and release some specific credential (similar to an access token). The negative consequence is that too easily, too many credentials can be created:

    - How would the verifier know what to use? In a research context that would not be so difficult assuming that the research context is well enough organized.

    - How would you know that someone else is not going to request your research RI credential?-> phishing risk. There are already some examples of this scenario: universities alliances, European student cards).

- Role of RIs in the context of research: RIs aggregate credentials and transfer them to services. They also help to manage which roles and rights certain users must have. This RI's role would remain. They will probably become issuers as well. They are trust anchors too: the proxy must be trusted by all the services involved. In a model where the research RI would become a trust anchor as well in terms of OIDF, there is immediately a place for trustfully publishing the schema. This would create an ecosystem with federation properties, own schema or at least the capability to have it. It would be well established by all the participant parties in that federation.

- Trusting the proxy (video min 00:36:05): is there a schema for trusting what the proxy releases? In the SAML national education federations, the federation publishes the domain name part of the schac home organisation in SAML metadata. A service that receives an attribute (i. e. student@universityX..) can check in the SAML metadata as published by federation operator and see whether the university is an allowed domain name part for that university. This capability of writing the domain name of the university is not possible in the wallet.

There are other mechanisms with a similar effect: first, you assume in an issued VC that whatever is published by this issuer is consistent. Second, there are ways in OIDF to express federation membership and to have trust marks (i. e. one trust mark saying: this entity is allowed to issue a particular set of scopes).

Next steps:

- Define (Virtual Organisations') use cases.

- Apply the suggested mapping from SAML to OIDC[2]. Propose this for consultation within the REFEDS community.

[2] Van Dijk, N. (2018) White Paper for implementation of mappings between SAML 2.0 and OpenID4 Connect in Research and Education. In: https://daasi.de/pub/20181011-OIDC-WP.pdf