Minutes VC-Subcommittee November 8th 2024

Niels presentation of VCs usage scenarios:

VCs definition approaches:

A) One VC including all eduPerson's attributes.

B) More target defined credentials: In SURF called "AcademicBaseCcredential". Roughly an equivalent to the attributes bundle in REFEDS person category (6 attributes).

Challenges:

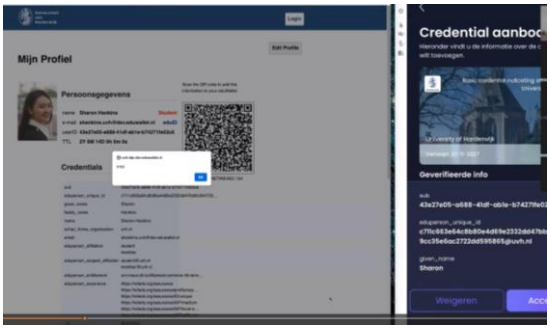
Verifiers decide which credentials they are going to request from the user

Attributes can have several meanings. For example, in the case of affiliations and entitlements. In the case of a service's request of an affiliation, the wallet could show all affiliations and the users (holder) could choose which affiliation to share. In the case of an entitlement request it would be more challenging for the user, because it is less transparent what it is needed for each situation.

Played personas' scenarios presented (created with SAML php):

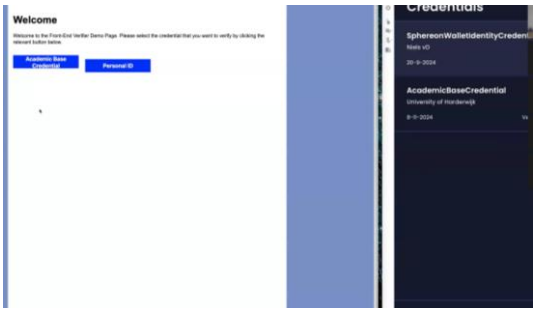
1. Sharon (student) AcademicBaseCredential

With a "pre-authorized" code flow, Sharon scans the QR code from the screen. From a security perspective risky if someone is behind Sharon being able to pick up the QR code. The flow should be protected with a PIN emailed to Sharon's institutional email address to avoid this risk.

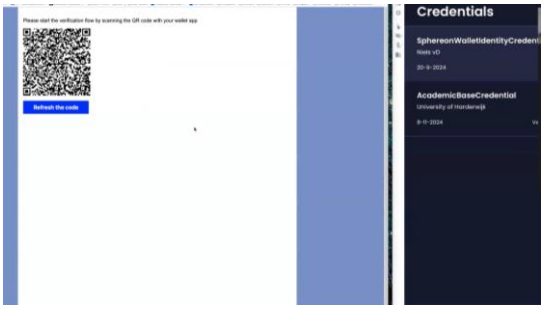


The visual representation of the data, the expiration date, the technical data, and all the credentials listed in the left side are shown to Sharon. She accepts the inclusion of all the information into the wallet. She can then see the name of the wallet, the issuer, the date of inclusion into the wallet.

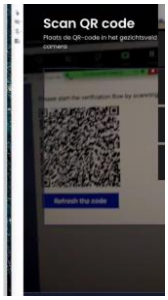
Verification flow:



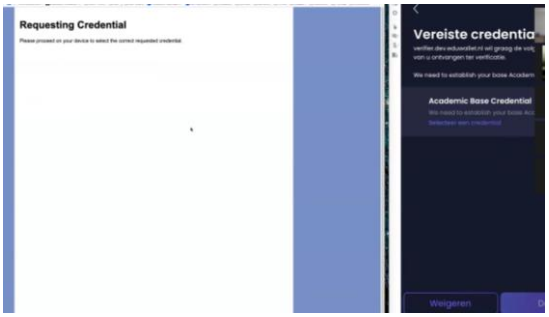
The verifier requests an AcademicBaseCredential



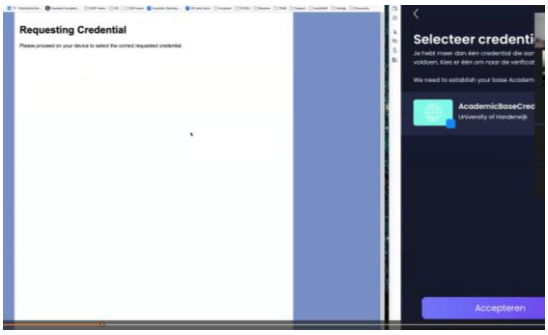
The QR code is scanned

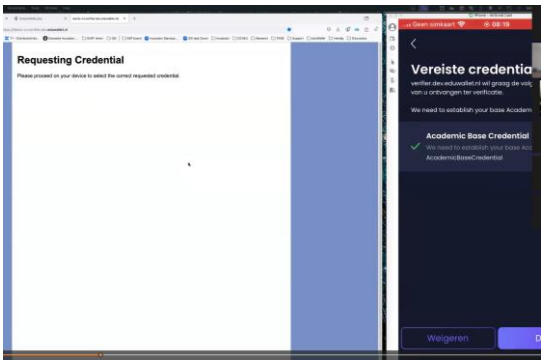


The request for the specific AcademicBaseCredential must be accepted

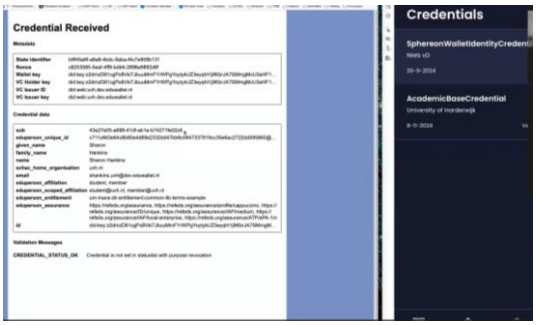


The credential including all attributes is shared once Sharon accepts the request and selects the credential.

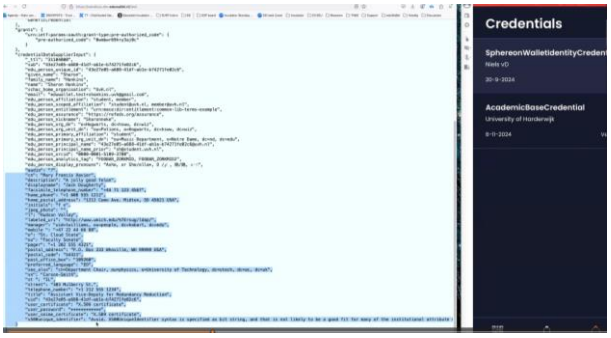




Once accepted, Sharon introduces the PIN to confirm the sharing of the data.

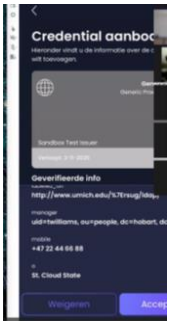


2. Scenario including in a VC all eduPerson attributes



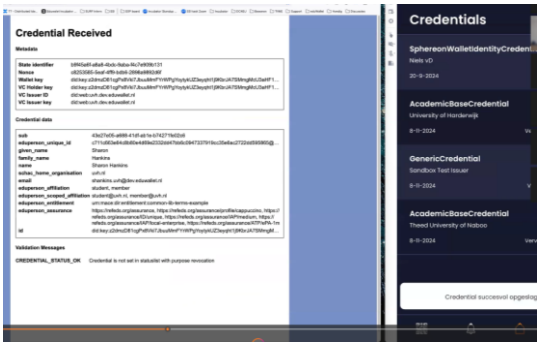
The data included after eduPerson-> audio… are data related to the past development of eduPerson coming from an LDAP schema, but no more useful.

Scanning this credential would mean to also include all the useless information:

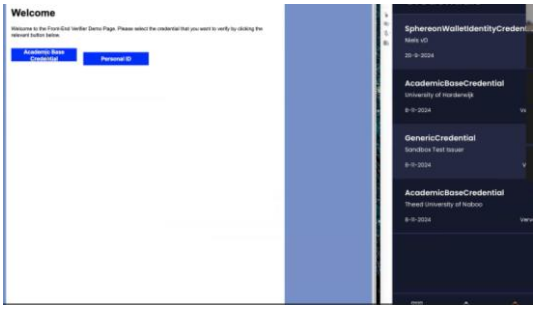


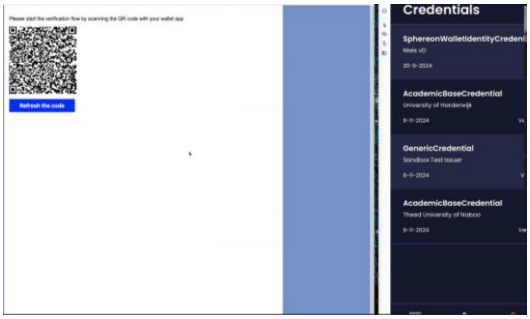
-> Does this make sense?

3. Scenario with attributes with different meanings -> Sharon has two student identities

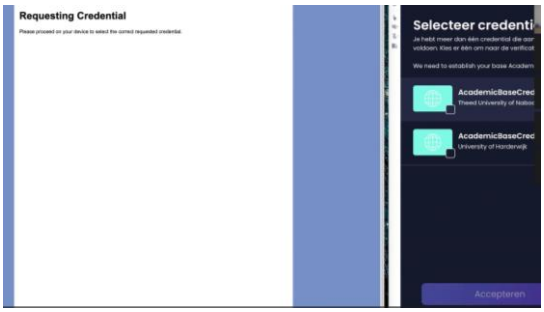


The verifier requests Sharon to share a credential:





If Sharon wants to share one of her two identity credentials, the wallet shows a list with her two credentials. Both are AcademicBaseCredentials, but from different universities:



In this case it is still not so complicated for Sharon to decide which credential to share. But in the case of belonging to several research groups organisations with several eduPerson entitlements, it would be difficult for Sharon to distinguish between the various values.

Questions

2nd scenario: Does keeping the useless "historical" eduPerson data make sense?

3rd scenario:

- How does the verifier know that the different credentials exist?

- From interoperability view: how can verifiers know what is the synonymous VCs content and its semantics? The semantics could be solved getting one by one the semantics of the eduPerson schema and similarly naming the attributes.

Grouping the credentials into a grouping claim is more difficult. -> what would be the best approach?

Discussion

- Doubts on the user experience dealing with selective disclosure in the 3rd scenario in terms of deciding about the best choice between credentials and the attributes to select.

Probably verifiers will ask for multiple subsets already standardised. For example, in the case of requesting the PID, which is an EU preferred credential, it would be very problematic due to the varieties of EU national PIDs. Preferably would be that the verifiers could accept different compatible credentials (i. e. any of: AcademicBasedCredential name or a post-office name, etc.).

For an international researcher could be a scary scenario to need dealing with lots of credentials.

Also, if the values are not in the spec there is the risk that the credential is not accepted.

The issuers publish a logo as part of the metadata, but not all wallets do publish this in the same way. It would be useful to demand the uniqueness and permanence of the entities' logos. The visual part of the credential will be very important for the users.

Looking from a verifier perspective: the education & research community should come up with a description of what to do. It would also be useful to provide the verifiers with a name of credential schema as well as guidance of what to do in different scenarios, what to ask for.

The users also need to easily know what they have to do. We should identify the use cases, tell the verifier what to do, and implemented in a way that is easy for the students to understand how to fulfil the verifiers requests.

Including all in one credential is probably not the best approach neither to include too many VCs in the wallet even if the users have free choice.

From a verifier view, if an attribute is used to give access to a service, how to know that the correct card is being used to validate? And if it is allowed to select two different cards, could one attribute from one card and another from the other card for different rights be used? Yes, that could be done using checks like it happens in the SAML-world. It could be checked whether different credentials information comes from the same wallet. It is needed to apply some scope into the credential, particularly in the research community, the name and the value would be very specific.

We should think how to use/not to use this information in order to avoid lots of potential problems. People do not see the result of they do.

Regarding the suggestion of having per use case specific directions for the verifiers (i. e. for checking the students' status check this or to provide access to an specific service, check the entitlement type):

A scenario could be to have particular entitlements for the research community, the suggestion could be to pick some basic identity such as the AcademicBaseCredential, but also the exact same claims with the attached semantics and put it i. e. in an ELIXIR VC or in a EOSC VC. We have the benefit of having a very well defined set of claims, so that we could also come up with an scenario where EOSC could have a subset of these claims in their VC and on top of that a layer of an identity credential meant more generally like an AcademicBaseCredential. This would facilitate the actions of the service providers who could explicitly request for example an EOSC and an AcademicBaseCredential and maybe some specific claims in case of providing selective disclosure.

EOSC VC could also have logos attached making them easily recognisable and hopefully understandable for users. At the same time if we could agree that the claims underneath that VC are from the well-known schemas like eduPerson and Schach schemas that would mean that we can apply reusable schemas that would also be compatible with SAML and OIDC. That would be useful for the verifier, the SP or whatever perspective. The VC would just be a transport of existing compatible schemas.

From the users' perspective that could also be used through scoping users.

- Regarding trust anchors: probably a definition of trust anchors will be needed for each use case specified in guidelines for verifiers. It is suggested that in the same guidelines for verifiers, in addition to VCs and elements to ask for, it should be demanded that those are issued by particular organisations entitled by the education and research community or "sector player" (trust anchors).

At the level of trust this is already existing in the definitions of the OIDF. But for some cases it might be a too restrictive approach.

- One of the most challenging things will be to ask users to decide what information to release to the verifier. More targeted VCs (s. B above) would be useful to deal with this challenge. Users in the research community for instance, could recognise a branded VC (i.e. ELIXIR).

It is suggested not to end up with an endless number of VCs.

In the research community a common scenario is to have a proxy that combines the research credentials in one assertion and shift that over to the service. It could be a tendency to repeat that process in the wallet ecosystem rather than having a base academic credential as the identity part of the profile and an ELIXIR credential to have the context relevant infos (roles & rights within the ELIXIR community). The other possibility would be to come up with a new VC, which would be the easiest way to operate in the research community: stick an issuer on the backend of the research proxy and release the entire set and aggregate. It is open whether this is good.

From the perspective of libraries having a large diversity of users: credentials can be stored at different places, but the owner of the credential is an institution. If a user has a wallet with credentials and these are deleted, these can be recovered from the institution. The governance is not at the users' side, but at the institutions (authorised issuers) side. This is not for all credentials the case. For example, in the case of diplomas, if the institutions loose the user attached to the diploma, how can they assure that the diploma issued by the institution corresponds to a specific person.

Next steps

Demo of "targeted VCs" using i.e. ELIXIR. (Niels) at the next meeting on the 22nd of November 8.00-9.00 *CEST