Link to 2024 ACAMP Wiki

Advance CAMP Thu. Dec 12, 2024

Room - III

Session Title: REFEDS Verifiable Credentials. How do we use VCs with; eduroam with VCs

CONVENER: Niels van Dijk, Gary Windham

MAIN SCRIBE(S): Mary McKee

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 33

Slides and video's demo'ed presented:
https://surfdrive.surf.nl/files/index.php/s/nDI2fu2oYxQ0MWA

DISCUSSION:

Verifiable Credentials subcommittee: we don't have well-defined credentials that align with our standards, results in wheel-reinventions.

You can use VCs in the context of wallets (hot topic right now); we should make sure that information contained within are aligned - this is the scope of the working group. ~20 participants, multi-stakeholder, meets biweekly (next one Dec 20).

You can read the charter online: wiki.refeds.org/display/STAN/VC+Subcommittee

What is a Verifiable Credential?

- Set of attributes or claims you can independently verify. In current SAML ecosystem, for example, the verification is implied by the IdP being trusted. In this case, the credential can be shipped independently of source and the information can be verified out of band.
- www.w3.org/TR/vc-data-model-2.0/
- VC != attributes
- We've done a lot as a community to standardize on eduPerson - some attributes in eduPerson are less used these days (pagerNumber, e.g.), there is a subset of these attributes that is used regularly.
- Thinking about VCs vs attributes - it isn't a single attribute, it is a bundle of attributes, and it would not be a good approach to treat as one attribute. Need to start thinking about attributes (=claims) and come up with some logical subsets of those claims
- Nothing stopping us from putting all of eduPerson into a verifiable credential; working group ran some technical demos: showing a sandbox issuer on left side issuing all eduPerson attributes as claims into wallet credential. (demo resulting in VC card that shows eduPerson claims associated with VC)
- If you combine this with *selective disclosure*, user can decide which of these attributes/claims to release, but this is a very large bundle of claims and could result in overasking for personal information.
- Niels would propose instead to have smaller bundles for more specific use cases. For example, eduPerson personalized entity category attributes (claims)
    - If you look at what identity federations are handing out, they are typically very close to this personalized entity category
    - We could create an academic base credential for this purpose
- Demo of an academic base credential: similar to previous, but generates a generic credential that includes things like name, email, affiliation, entitlements, assurance info
    - When we start issuing credentials in a wallet context, the branding of the credential itself can be done by the issuing party, so the wallet credential shows more of a sense of context; different orgs issuing credentials could, similar to passports looking somewhat different per country, mirror the branding of the issuing org
- It's also possible to combine sets from multiple schemas into one bundle or VC - e.g., combining eduPerson attributes and voPerson attributes. E.g., a membership statement that includes institutional context as well as personal context such as entitlements
- Another approach is to issue a verifiable credential with common claims + selective disclosure - so if the only thing we want to do is prove that someone is a student, we can

include eduPersonAffiliation and look at selectively disclosing the value of “student” in a multivalued context

Schema Definitions

- JSON schema is already in the specification
- Q: You’re pointing to the schema via a web URL, what about DNS attacks to pick up the wrong schema? How do you verify that you’re looking at the right source?
    - Not going to talk about federation right now, but the answer is federation. Need to put some of these schemas into our federation assets as an authoritative source/trust anchor within our ecosystem
    - Provide some sort of signature/publish a signed equivalent of metadata
- Issuer specific presentation
    - Display: name, description, text color, logo url, alt text, background colors, background images, etc
    - Credential definition (type)
    - Credential subject (name, locale, sub)
- The wallet has to interpret the above; looking at three different wallet interpretations of the same credential information, the credentials themselves can look very different - different color schemes (some ignored branding in some ways). We should probably have some standards for how the wallet should interpret these specs; on the other hand, users are unlikely to use 20 different wallet providers, so maybe it doesn’t matter - what any given user sees will be interpreted and presented consistently, if not the same as the next. Bad for institutional documentation if every wallet presents the credential differently.

Working Group Next Steps

1. Standardize claims (white paper for implementation of mappings between SAML 2.0 and OpenID Connect in Research and Education (2018) (link provided to google docs; likely this: https://wiki.refeds.org/display/CON/Consultation%3A+SAML2+and+OIDC+Mappings?preview=/38895621/38895643/20181011-OIDC-WP.pdf)
2. Standardized specific VCs based on common use cases - register JSON schema for these VCs. Interoperability with other sectors (healthcare, etc) is similar, so we should make it as standardized and understandable and global as possible (a reason to call it eduID, perhaps)

3. Describe best practices for presenting the VCs in the wallet - there's a fair chance that there will be a thousand wallets, but maybe we can support with guidance

Questions about crosswalking with current standards:

- You can imagine an entity that can be an IdP, an OP, and a verifiable credential issuer with the same dataset. Niels very convinced that VCs are not all we'll be using.
- Wallet scenario could potentially look like a second factor authentication scenario, could be that you log in with your wallet initially and then SAML or OIDC retains login - don't need to look for one technology to replace existing infrastructure, but rather find ways to take the best of each
- Suspension/revocation - one thing you can always do with VCs is give them a time to live (TTL) as the issuing party. You can also maintain a revocation list that a verifier could check back. No one loves revocation lists but it's the only thing that is currently standardized. Some of the folks working on this kind of stuff have less experience running this kind of infrastructure as many in this room, and solutions are being proposed that may not scale for reasons that are intuitive to R&E. In a scenario where you have 5 issuers, you are going to be able to do different things than us having 10,000, or other contexts where you could have millions
- Given the distributed development, where are the gaps? What about the authority to issue a credential? What is stopping people from issuing credentials they don't have the authority to issue? From the perspective of the VCs, it's brilliant that anyone can issue credentials, but the question is are you going to trust something that has been issued. What are the technologies you're going to use to help people make that determination? You need a way to make a statement that the university of Illinois is actually the real university with the authority to attest that someone is a UofI student? Current ways: a trust list (host file), or to stick into some sort of ledger or blockchain. Need to think about how distributed these systems are - sometimes entry point is very centralized. Should look at OIDC federation, GEANT T&I incubator is supporting development of these use cases, some ideas are emerging here.

Gary Demo

- Cirrus has been interested in how to use verifiable credentials to support the community
- Demo: using SimpleSAMLphp with Microsoft verifiable credentials as example
    - Microsoft Authenticator app with VC from fictional university (attributes like name, email, student ID)

    - Institutional sign on page - see discovery and choose the VC option, presented with a QR code
    - Scan QR code from Microsoft Authenticator which asks for verification to release the credential
    - Successful login at the SAML SP through the IdP delegating to the VC implementation
- Questions: are there use cases for this? What is the appetite to build on this kind of use case/POC/what do we need to be thinking about before this is practical from a university/org context?
    - Campus IAM models need to think about this in new way. In some ways you may not need single sign on. Is anyone aware of work being done to provide an accessible solution for this? Pointing phones at QR codes may not work for people with visual impairments
        - Using a pre-authorized codeflow can be the only way to kick off the flow (not accessible)
        - In an authorization codeflow, as long as you stay on the same device, you can have buttons (more accessible)