MICROSOFT ENTRA VERIFIED ID

Verifiable Credentials, Microsoft style
TF-DLT, Sept 19, 2022

Peter Clijsters, Martin van Es, Niels van Dijk
Use cases

• Credential exchange between institutions

• Company ID as Guest login

• Credential issuance towards services
Why investigate?

VC issuance & verification capabilities are now part of Azure/Entra

Many institutions have Azure in place already

Can we leverage existing (Federated) AAI?

Can we integrate incoming credentials?
Use your eduiD credential to prove your identity.
Issue credentials from eduID using Microsoft Entra verified ID
W3C verifiable Credentials
Verifying credentials issued by eduID using Microsoft Entra verified ID
Requirements

- Azure tenant both for Issuers as well as Verifier
- Activate various components in your tenant
- Issuer and/or verifier client lib (python/.net/java)
- Microsoft Authenticator
Configuration -2

[JSON]

```json
{
    "locale": "en-US",
    "card": {
        "title": "Verified Credential Expert",
        "issuedBy": "Microsoft",
        "backgroundColor": "#000000",
        "textColor": "#ffffff",
        "logo": {
            "url": "https://didcustomerplayground.blob.core.windows.net/public/VerifiedCredentialExpertLogo"
        },
        "description": "Use your verified credential to prove to anyone that you know all about",
        "consent": {
            "title": "Do you want to get your Verified Credential?",
            "instructions": "Sign in with your account to get your card."
        },
        "claims": [
            {
                "claim": "vc.credentialSubject.firstName",
                "label": "First name",
                "type": "String"
            },
            {
                "claim": "vc.credentialSubject.lastName",
                "label": "Last name",
                "type": "String"
            }
        ]
    }
}
```

Source: https://docs.microsoft.com/en-us/azure/active-directory/verifiable-credentials/credential-design
Attestation Types

• ID token hint
  → passes claim values after Issuer AuthN (demo’ed)
• ID tokens
  → issuance flow requires interactive sign-in to OIDC OP
todo: will this also work w/ SSP or Shib?
• Existing verifiable credential
  → ‘transfrom’ using another VC
• Self-asserted claims
  → let the user type
• Verifiable Credential for directory based claims
  → not test (yet)
Directory Based Claims
Standards: OIDC / SIOP, DID:WEB, DID:ION
In the DID:Web implementation trust is established based on DNS, domain ownership and publishing .well-known file.

Azure as well as MS authenticator validate the .well-know file.

For DID:ION, Azure (and hence Microsoft) interacts with the VDR. It is at this point unknown if one can independently validate transactions against the ION ledger.

Relation between Issuer/Verifier client and Azure backend API is based on client key/secret.

Additional trust beyond technical, e.g. federation membership, is not possible except via additional credential issuance.
Findings

Setup of Issuer or Verifier is super easy (< 1 hour)

VC implementation does not make direct use of backend AAI storage like Azure AD; all credentials must be presented to the API. *Azure is only used as a ‘token translation’ proxy.*

In DID:ION implementation Azure also interacts with the ledger (the wallet *does not*)

*No selective release of credentials* by user, only the entire credential can be presented

Each issuer *and verifier* must have its own Azure tenant, no none-Azure implementations are known at this time
Conclusions

Implementation is very tightly locked into the MS ecosystem, not only technically, but also from the trust perspective.

**Integration is lightweight**, AZURE takes care of heavy lifting.

**Privacy and scalability** of VC release looks challenging.

**No selective controle** over Credential usage by users.

Given that Azure already has federation capabilities, the only clear benefit of verifiedID seems to be that *it does not need upfront trust establishment*.

No integrated provisioning path for Verifier.

Verifier Azure tennant requirement is potential barrier.