Author: Paul den Hertog, Niels van Dijk | SURF
Version: v0.4 draft, request for comments
May 28, 2024

FASTER: a Federated Approach for Secure, Trustworthy Educational credentials and Registries

Research and Education stakeholders, led by the NREN community, have in the past decades collaborated continuously to build a well-established, global infrastructure for R&E identity. By defining interoperability, trust and shared governance, this work has led to an infrastructure that nowadays provides a solid foundation for national and international use cases for millions of R&E users on a daily basis.

With the emergence of the new wallet based ecosystems, opportunities exist to connect wallets to this existing identity infrastructure. This will provide wallets with readily usable, high quality identity credentials which are foundational to many decentralized identity use cases in the R&E sector and beyond. However, to allow for the (re)use of identity information in a wallet ecosystem some basic requirements need to be agreed upon and fulfilled.

This initiative aims to lay out concrete, commonly agreed upon requirements from the NREN identity community which can be used as input for wallet ecosystem implementers and pilot projects both nationally and internationally. Through the implementation of these requirements, it is envisioned the wallet ecosystem can be provided with a core layer of educational identity credentials. At the same time it will also help accommodate the uptake of wallet based credentials in the existing R&E ecosystem.

Background
As the new wallet ecosystem is emerging, there is a need to establish and test the proposed EUDI ecosystem, to demonstrably showcase it can work [PL4] in a technology-agnostic, interoperable manner in European tertiary education.

While DC4EU was envisioned to provide that capability, DC4EU and other LSPs are behind schedule and further delays are to be expected as the implementing acts still need to be concluded and the Architecture Reference Framework is (still) unclear on several key areas. Additionally, the current ISO/mDL focus of the NiScy Reference Wallet means it is not yet ready for testing with many use cases in Education.[PL5]
Furthermore, EU projects do currently not take into scope the global environment the R&E sector is operating in.

The above challenges however do not mean we as a community cannot try to leverage the opportunities the wallet ecosystem may bring. This is specifically true for cases where so-called non-Qualified (non-government issued) identity can play a role and a high level of assurance or a government issued PID is not required. The existing federated identities which are currently issued by institutions may fulfill the need for a base identity. It is therefore feasible to use the existing federated identities as authoritative for establishing an “eduPID”. By establishing an eduPID and defining its relationship with well understood schema and specifications already existing in the federated identity ecosystem, these credentials could become readily available.

Similar to describing requirements for the technical use of the federated identity credentials, it is required to define the trust and security requirements. By aligning these requirements with existing practices in the sector, a consistent ecosystem can be established where wallet based, and federation-based credentials may be used in accordance to the use case they fit best.

The FASTER initiative is not a standalone project, but rather an initiative taken by various stakeholders in the R&E identity community, who are active within national projects (eduWallet, SURF, ….) Pan European projects like GEANT project, and global collaborations with the aim of accelerating R&D, by sharing and combining knowledge, insights and available resources such as open source code.

Boundary conditions

The academic identity ecosystem has several core values that have driven the design choices. These values should also be reflected in any new ecosystem, and hence lead to a few boundary conditions should be included:

- Ensures the individual's privacy and protection of personal data
- Makes use of Open Standards, ensures interoperability and is technologically agnostic
- Complies with the current principles of the ARF (1.4) and makes well-substantiated recommendations on points that have not yet been elaborated in the ARF
- Supports (convergence of) emerging European interoperability profile initiatives (e.g. Netherlands, Sweden and Italy).
- Should consider the global scope of the R&E community
- Leverages the way *organizational trust* is established in the European tertiary educational community, while at the same time facilitating the decentralized character of that ecosystem.
- Makes use of existing educational identity federations as source for credentials
- Aligns with existing practices with respect to trust, security and data protection as commonly found in educational identity federations
- Must be fit for purpose and hence be able to meet technical requirements such as security and scalability.
- At least supports OpenID Federation standard protocol as an open standard for exchanging trust information
- At least supports W3C Verifiable Credentials and the OpenID4VC protocol
- Should be verified in a PoC incorporating at least two different implementations of each of the ecosystem components, while leverage existing Open Source based projects and products

Call to action

To accomplish the above the following is needed:

- Bring together existing interoperability profile initiatives, like DIIP v3 - NL, and EUWIF – SE & IT, incorporating (broadly):
    - W3C Verifiable Credentials and the OpenID4VC protocol
    - Selective Disclosure
    - OpenID Federation
- Incorporate eduGAIN and national federation as trusted parties
- Standardise VCs for eduPerson, SCHAC and voPerson via REFEDs
- Standardise a ‘Base Credential for Academic Wallet Identity’ inspired by the REFEDs personalized entity category:
    - Organization
    - User identifier
    - Person name
    - Email address
    - Affiliation
    - Assurance
- Nominate at least two different implementations of the ecosystem components, and validate interoperability between these, while leverage existing Open Source based projects and products