OID4VCI issuing IdPs

Janne Lauros
Marko Ivančić
Febri Kazazi
Mihály Héder

Motivation

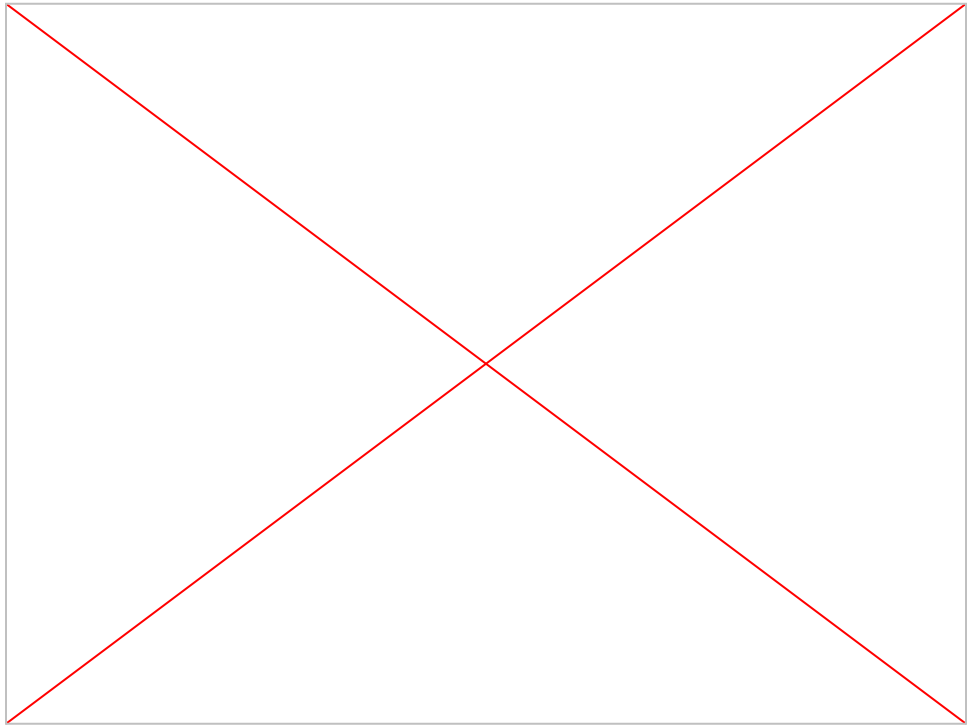
- **simpleSAMLphp** and **Shibboleth** power the *vast majority* of identity providers at academic institutions
  - these institutions manage a wealth of verified user data
    - assured personal attributes,
    - official documentation to academic records and affiliations
  - they ideal Verifiable Credential sources
  - attribute sources (**ssp** processing filters, **shib** resolvers, filters, transcoders and manipulation)
- idea: make them **OID4VCI issuers**!
- Idea: use the profile page (previous Incubator deliverable)

Work Done

- Initial work: Proof-of-concept with Sphereon Issuer
  - both Shib and SSP - see in the incubator wiki
  - Using the sphereon API to issue credentials, Proof-of-Concept/Inspiration
  - WP9 code review
- Wallet overview (OID4VCI versions…)
  - FUNKE
    - wwwallet

Work done

- Native implementations: **Shibboleth**
  - 3rd party plugin for OpenID VCI Pre-authorized code flow
    - Only partial and crude implementation exists
  - Can handle (saying ‘supports’ would be too much):
    - SD-JWT VC credentials
    - “did:jwk” and “jwk” binding methods, proof of possession
  - Test and demo instance (not always available):
    - https://geant-vci.2.rahtiapp.fi/.well-known/openid-credential-issuer
    - https://geant-vci.2.rahtiapp.fi/idp/profile/userprofile (to test with your wallet)
  - TODO for alpha release
    - Pick minimum set of features, implement.
    - Conformance tests - no such yet available, moving target
    - I’d say we are 20% done, not 80% :-)

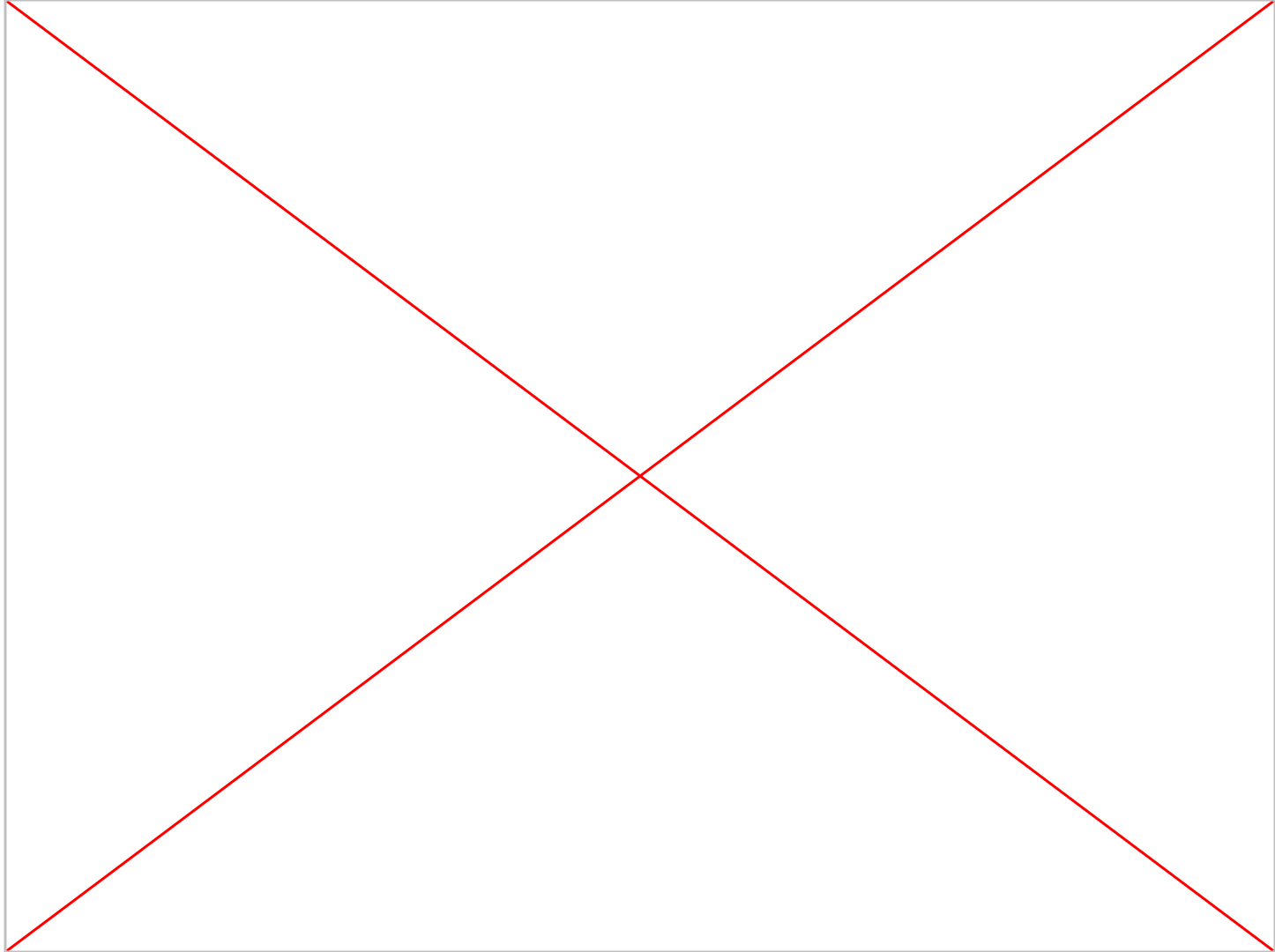


Shibboleth user profile page + VCI plugin acting in tandem as OpenID VCI Issuer

Work done

- Native implementations: **SimpleSAMLphp**
  - Pre-authorized code flow
    - new flow defined by the VCI spec
    - works, with some hard-coded parts - WIP
  - Credential format:
    - jwt_vc_json, using VCDM v1.1 (v2.0 published in May)
  - OID4VCI draft 14 (15 not supported by wallet)
  - Ability to test credential issuance in module admin area
  - Configuration Endpoint URL: https://idp.mivanci.incubator.hexaa.eu/.well-known/openid-credential-issuer
  - Git branch: https://github.com/simplesamlphp/simplesamlphp-module-oidc/tree/wip-vci
  - TODO
    - Implement SD-JWT credential format
    - API for credential offer fetching
    - Implementation in Profile Page module, using API
    - Proof binding (binding credential to public key of the holder)

SSP demo video



Shibboleth UI (Before)

- Personal Data
- Connected Services
- Activity Page

Personal Data

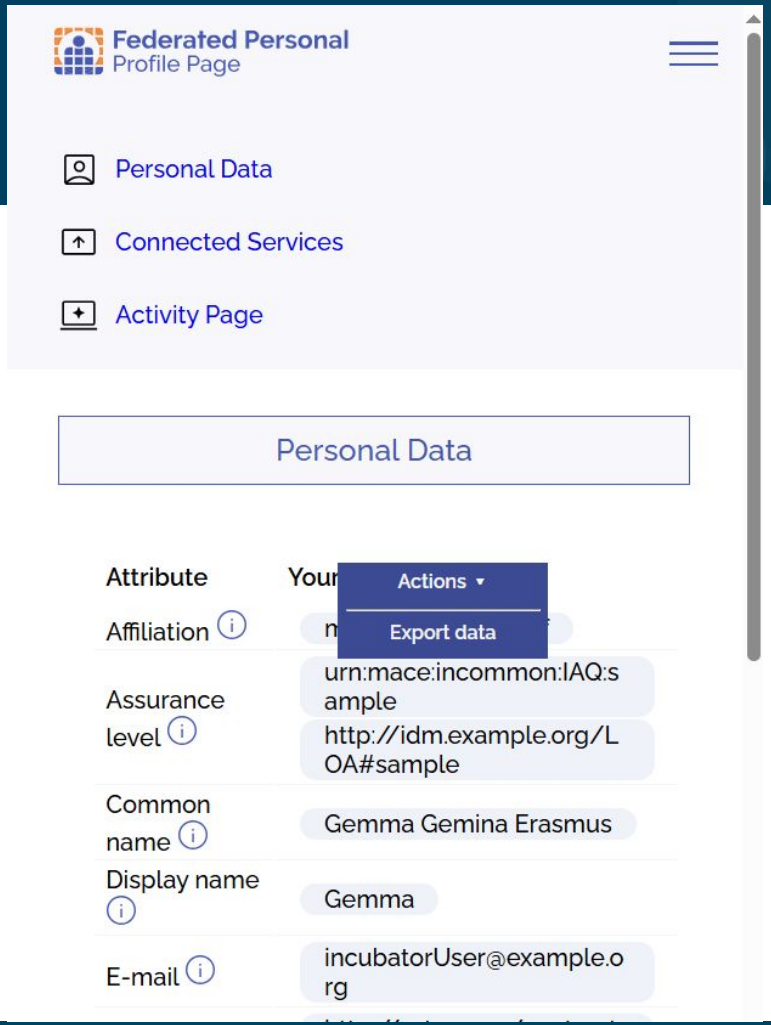
Actions ▾

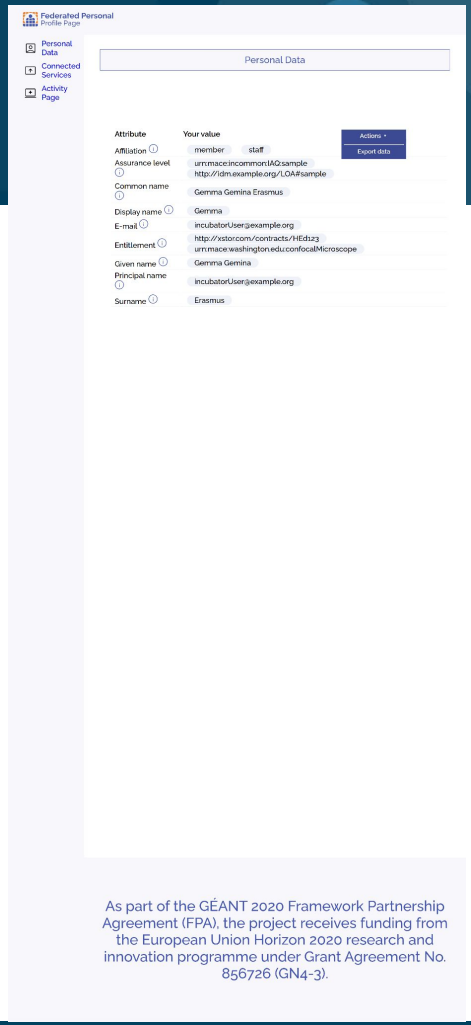
Export data

Attribute	Your value
Affiliation	member staff
Assurance level	urn:mace:incommon:IAQ:sample http://idm.example.org/LOA#sample
Common name	Gemma Gemina Erasmus
Display name	Gemma
E-mail	incubatorUser@example.org
Entitlement	http://xstor.com/contracts/HEd123 urn:mace:washington.edu:confocalMicroscope
Given name	Gemma Gemina
Principal name	incubatorUser@example.org
Surname	Erasmus

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Shibboleth mobile view (Before)





GÉANT
Networks • Services • People

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

UX/UI Revamp

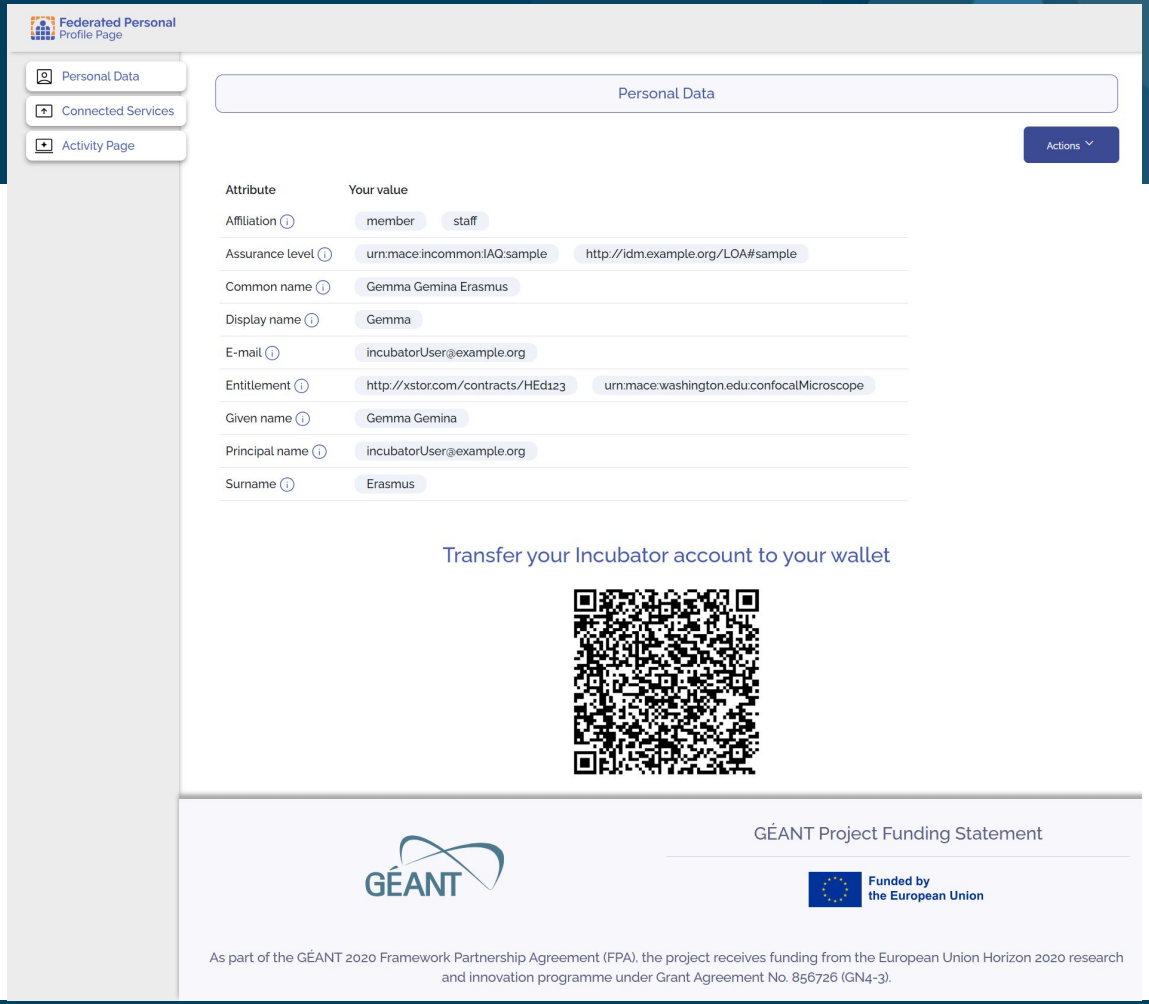
WEAKNESSES

- Clustered code reducing readability and maintainability.
- Buggy behavior on mobile view.
- Very minimalistic design with minimalistic intuitivity.

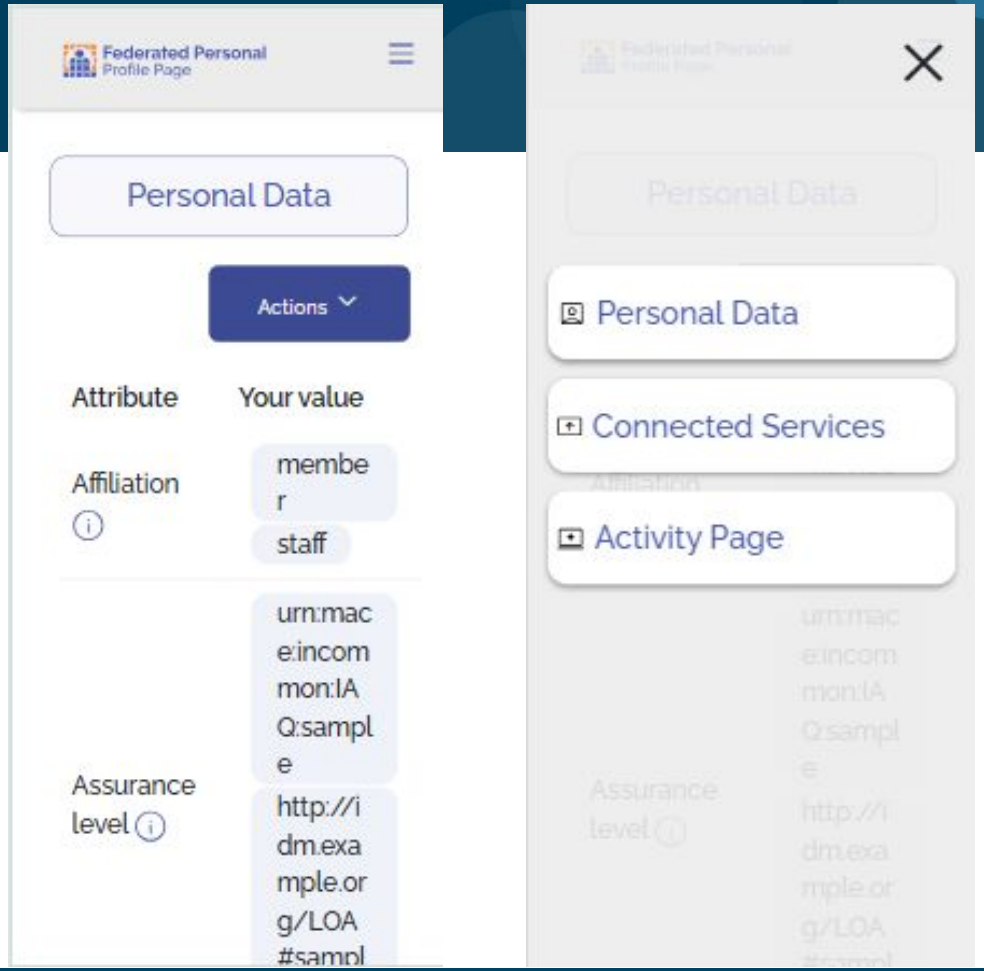
SOLUTIONS

- CSS stylesheet separated into different files using a component-based approach.
- Updated the meta tag and @media CSS rule. Restyled the entire layout. (A & B testing approach).
- Small yet big design changes performed.
  - Rounded edges.
  - Shadows.
  - Contrasting colors.
  - Hover animations and other dynamics.

Shibboleth UI (After)



Shibboleth mobile view (After)



SimpleSAMLphp UI (Before)

Federated Personal
Profile Page

- Personal Data
- Connected Organizations
- Activity
- Log out

This is what we know about you...

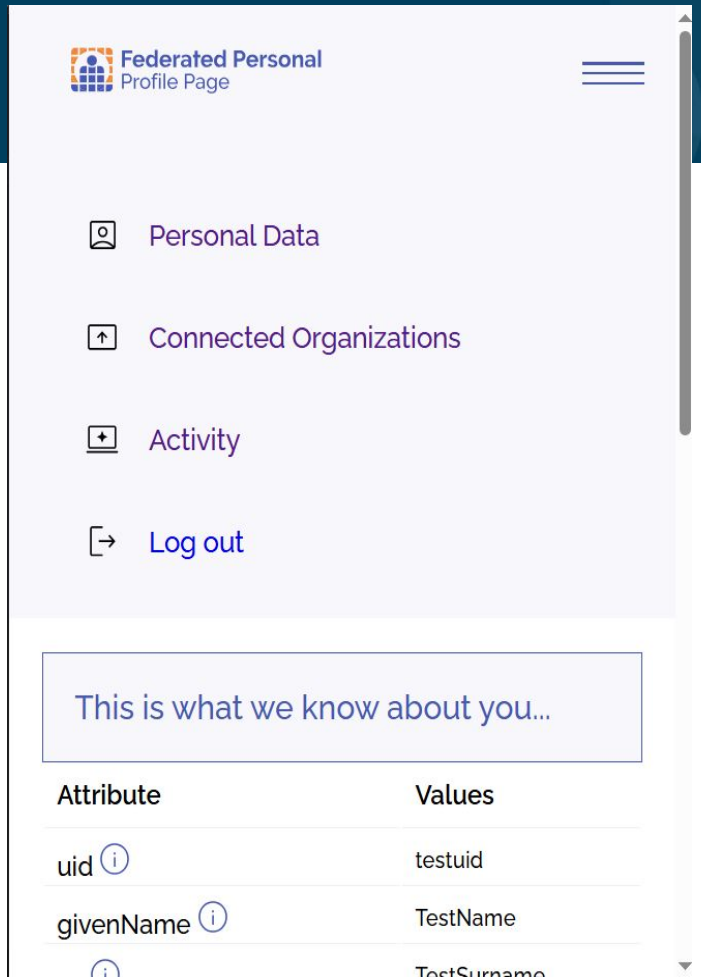
Attribute	Values
uid	testuid
givenName	TestName
sn	TestSurname
eduPersonAffiliation	member; guest
o	Test Organization

Get your verifiable credential by scanning the QR:

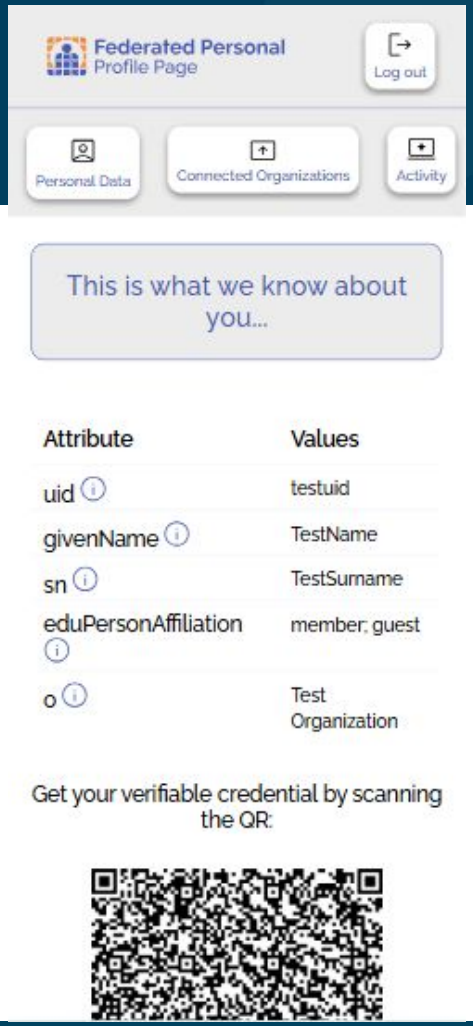
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

SimpleSAMLphp UI (After)

SimpleSAMLphp mobile view (Before)



SimpleSAMLphp mobile view (After)



CHALLENGES

Maintain code simplicity.

Account for legacy code.

Future plans

- code flow, not just pre-auth
- version 15, 16?, 17? - pause?
  - multiple credential format(s), depending on interop needs
- REFEDS eduperson VC schema interoperability
- source code release
  - shib: 3rd party module, there is already a repo from shib project
  - ssp - official openid connect module, just like
  - code review by WP9
- UX
  - Code refactoring ensuring robustness.
  - Coherent code development methods ensuring future proofing, and scalability, graceful degradation.
  - Focus on user feedback

Thank you & please reach out to us!

mihaly.heder@sztaki.hu