OID4VCI issuing IdPs

Janne Lauros
Marko Ivančić
Febri Kazazi
Mihály Héder

Motivation

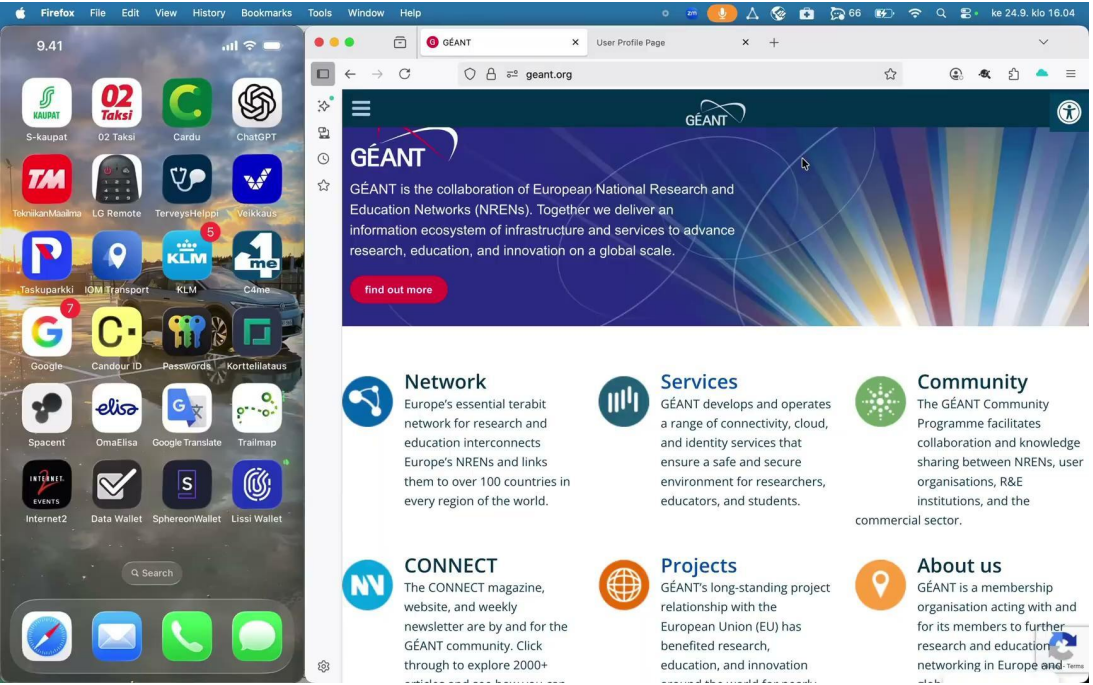
- **simpleSAMLphp** and **Shibboleth** power the *vast majority* of identity providers at academic institutions
  - these institutions manage a wealth of verified user data
    - assured personal attributes,
    - official documentation to academic records and affiliations
  - they ideal Verifiable Credential 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**
- Last demo was running happy case with **Pre-Authorized** flow. Since that..
  - Support for **TX Code** in **Pre-Authorized** flow
  - "**Stateless**" mode, ie, having Storage is optional.
  - Moved from then v14 wallet (Sphereon) to v15 wallet Lissi (https://www.lissi.id/) as counterpart for our issuer.
  - Main target was to execute **Code** flow successfully transferring credentials resolved by Shibboleth IdP to Lissi wallet. Checked.
  - No new credential formats implemented so still supporting only **SD-JWT VC**.
  - 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
  - Plugin is still only a **poc** running happy path. It does show already that Production grade plugin can be done with sane amount of work.



Shibboleth VCI Plugin running Code flow With Lissi Wallet

Work done

- Native implementations: **SimpleSAMLphp**
  - **Grant types:**
    - Pre-authorized Code flow (new flow defined by the VCI spec)
    - Authorization Code flow
  - **Credential formats**:
    - jwt_vc_json, using VCDM v1.1 (v2.0 published in May)
    - dc+sd-jwt (previously vc+sd-jwt) (SD-JWT)
  - **Proof types**:
    - jwt
  - API for credential offer fetching
  - Implementation in Profile Page module, using API
  - 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

Sample SimpleSAMLphp Config

```
// Enable or disable verifiable credentials capabilities. Default is disabled (false).
ModuleConfig::OPTION_VERIFIABLE_CREDENTIAL_ENABLED => true,

// Allow or disallow non-registered clients to request verifiable credentials. Default is
disallowed (false).
ModuleConfig::OPTION_ALLOW_NON_REGISTERED_CLIENTS_FOR_VCI => true,

// Allowed redirect URI prefixes for non-registered clients. By default, this is set to
// 'openid-credential-offer://' to allow only redirect URIs with this prefix.
//
// Example:
// [
//     'https://example.org/redirect',
//     'https://example.org/redirect2',
// ]
//
ModuleConfig::OPTION_ALLOWED_REDIRECT_URI_PREFIXES_FOR_NON_REGISTERED_CLIENTS_FOR_VCI => [
    'openid-credential-offer://',
    'https://oob.lissi.io',
    'datawallet://callback',
    'https://idp.mivanci.incubator.hexaa.eu',
],
```

```
// Mapping of user attributes to a credential claim path, per credential configuration ID.
ModuleConfig::OPTION_USER_ATTRIBUTE_TO_CREDENTIAL_CLAIM_PATH_MAP => [
    'ResearchAndScholarshipCredentialDcSdJwt' => [
        ['eduPersonPrincipalName' => ['eduPersonPrincipalName']],
        ['eduPersonTargetedID' => ['eduPersonTargetedID']],
        ['displayName' => ['displayName']],
        ['givenName' => ['givenName']],
        ['sn' => ['sn']],
        ['mail' => ['mail']],
        ['eduPersonScopedAffiliation' => ['eduPersonScopedAffiliation']],
    ],
],
```

```
// (optional) Credential configuration statements, as per `credential_configurations_supported`
claim definition in
//
https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html#credential-issuer-para
meters.
ModuleConfig::OPTION_CREDENTIAL_CONFIGURATIONS_SUPPORTED => [

// Sample for 'dc+sd-jwt' format without notes about required and optional fields.
'ResearchAndScholarshipCredentialDcSdJwt' => [
    ClaimsEnum::Format->value => CredentialFormatIdentifiersEnum::VcSdJwt->value,
    ClaimsEnum::Scope->value => 'ResearchAndScholarshipCredentialDcSdJwt',
    ClaimsEnum::Display->value => [
        [
            ClaimsEnum::Name->value => 'ResearchAndScholarshipCredentialDcSdJwt',
            ClaimsEnum::Locale->value => 'en-US',
            ClaimsEnum::Description->value => 'Research and Scholarship Credential',
        ],
    ],
    ClaimsEnum::Claims->value => [
        [
            ClaimsEnum::Path->value => ['eduPersonPrincipalName'],
            ClaimsEnum::Mandatory->value => true,
            ClaimsEnum::Display->value => [
                [
                    ClaimsEnum::Name->value => 'Principal Name',
                    ClaimsEnum::Locale->value => LanguageTagsEnum::EnUs->value,
                ],
            ],
        ],

        // …

        [
            ClaimsEnum::Path->value => ['eduPersonScopedAffiliation'],
            ClaimsEnum::Display->value => [
                [
                    ClaimsEnum::Name->value => 'Scoped Affiliation',
                    ClaimsEnum::Locale->value => LanguageTagsEnum::EnUs->value,
                ],
            ],
        ],
    ],

    // REQUIRED
    ClaimsEnum::Vct->value => 'ResearchAndScholarshipCredentialDcSdJwt',
],
],
```

SimpleSAMLphp Credential API Endpoint - Sample Requests

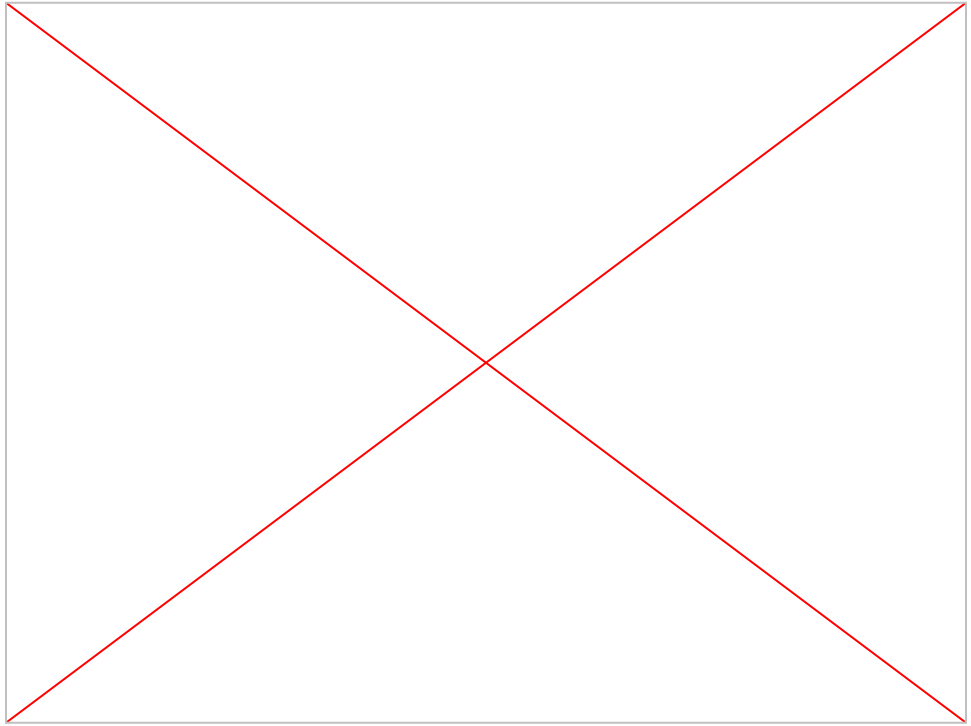
```
curl --location 'https://idp.mivanci.incubator.hexaa.eu/ssp/module.php/oidc/api/vci/credential-offer' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer ***' \
--data-raw '{
    "grant_type": "authorization_code",
    "credential_configuration_id": "ResearchAndScholarshipCredentialDcSdJwt"
}'
```


```
{
    "credential_offer_uri":
"openid-credential-offer://?credential_offer={\"credential_issuer\":\"https:\\/\\/idp.mivanci.incubator.hexaa.eu\",\"credential_configuration_ids\":[\"ResearchAndScholarshipCredentialDcSdJwt\"],\"grants\":{\"authorization_code\":{\"issuer_state\":\"30616b68fa26b00c5a6391ffac02e4e4fd9b0023fd6a3aa29ec754e2f5e2871\"}}}"
}
```


```
curl --location 'https://idp.mivanci.incubator.hexaa.eu/ssp/module.php/oidc/api/vci/credential-offer' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer ***' \
--data-raw '{
    "grant_type": "urn:ietf:params:oauth:grant-type:pre-authorized_code",
    "credential_configuration_id": "ResearchAndScholarshipCredentialDcSdJwt",
    "use_tx_code": true,
    "users_email_attribute_name": "mail",
    "authentication_source_id": "example-userpass",
    "user_attributes": {
        "uid": [“testuseruid"],
        "...": ["..."]
    }
}'
```


```
{
    "credential_offer_uri":
"openid-credential-offer://?credential_offer={\"credential_issuer\":\"https:\\/\\/idp.mivanci.incubator.hexaa.eu\",\"credential_configuration_ids\":[\"ResearchAndScholarshipCredentialDcSdJwt\"],\"grants\":{\"urn:ietf:params:oauth:grant-type:pre-authorized_code\":{\"pre-authorized_code\":\"_ffcdf6d86cd564c300346351dce0b4ccb2fde304e2\",\"tx_code\":{\"input_mode\":\"numeric\",\"length\":4,\"description\":\"Please provide the one-time code that was sent to e-mail testuser@example.com\"}}}}"
}
```

SimpleSAMLphp VCI demo video

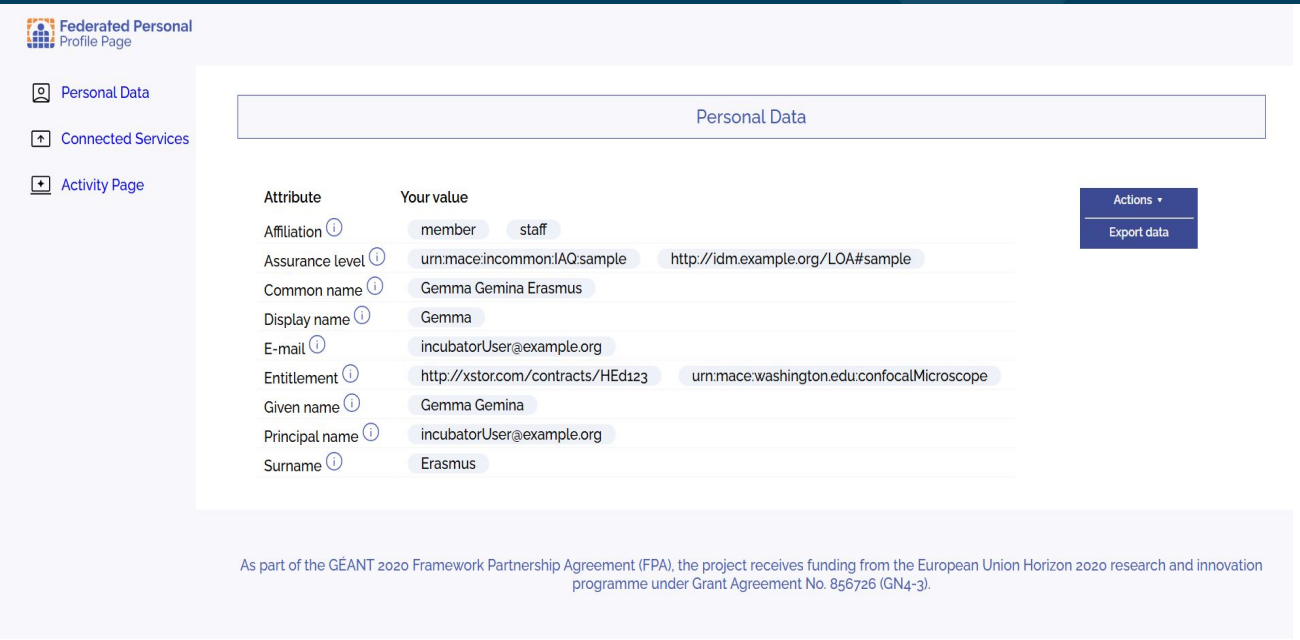


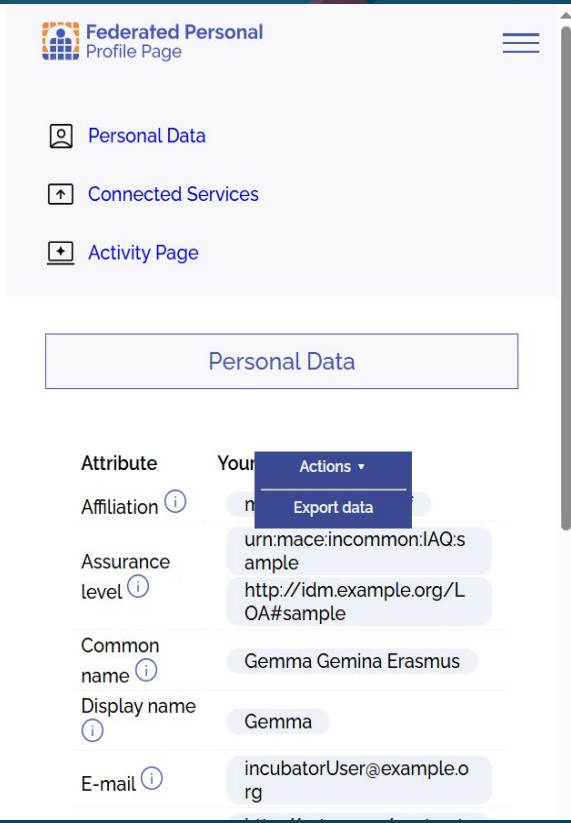
Tested wallets, grants and credential formats

	Pre-Authorized Code	Authorization Code
Sphereon	YES	NO (no client_id in authorization request)
Data	YES	NO (couldn't open system browser)
Lissi	YES	YES

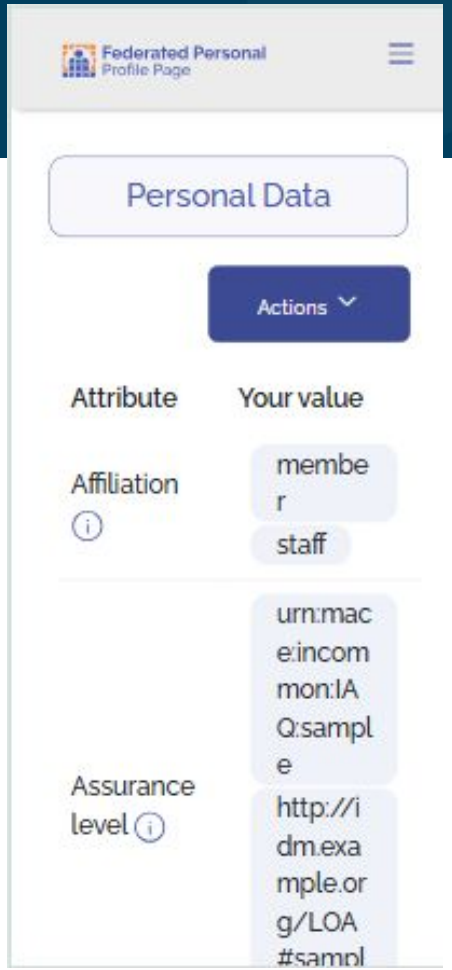
	jwt_vc_json	dc+sd-jwt
Sphereon	YES	YES
Data	YES	YES
Lissi	NO (errors out)	YES

Shibboleth UI (Before)

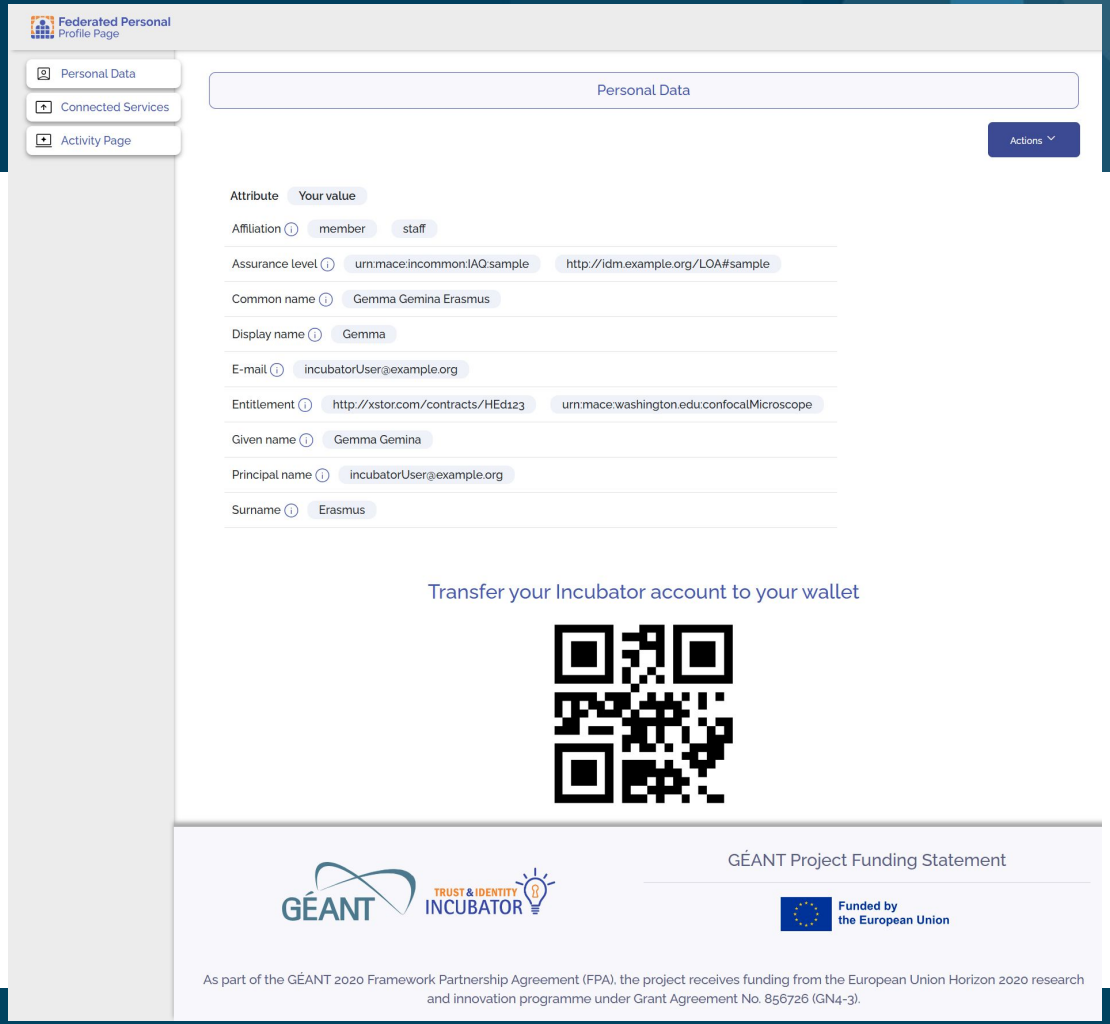




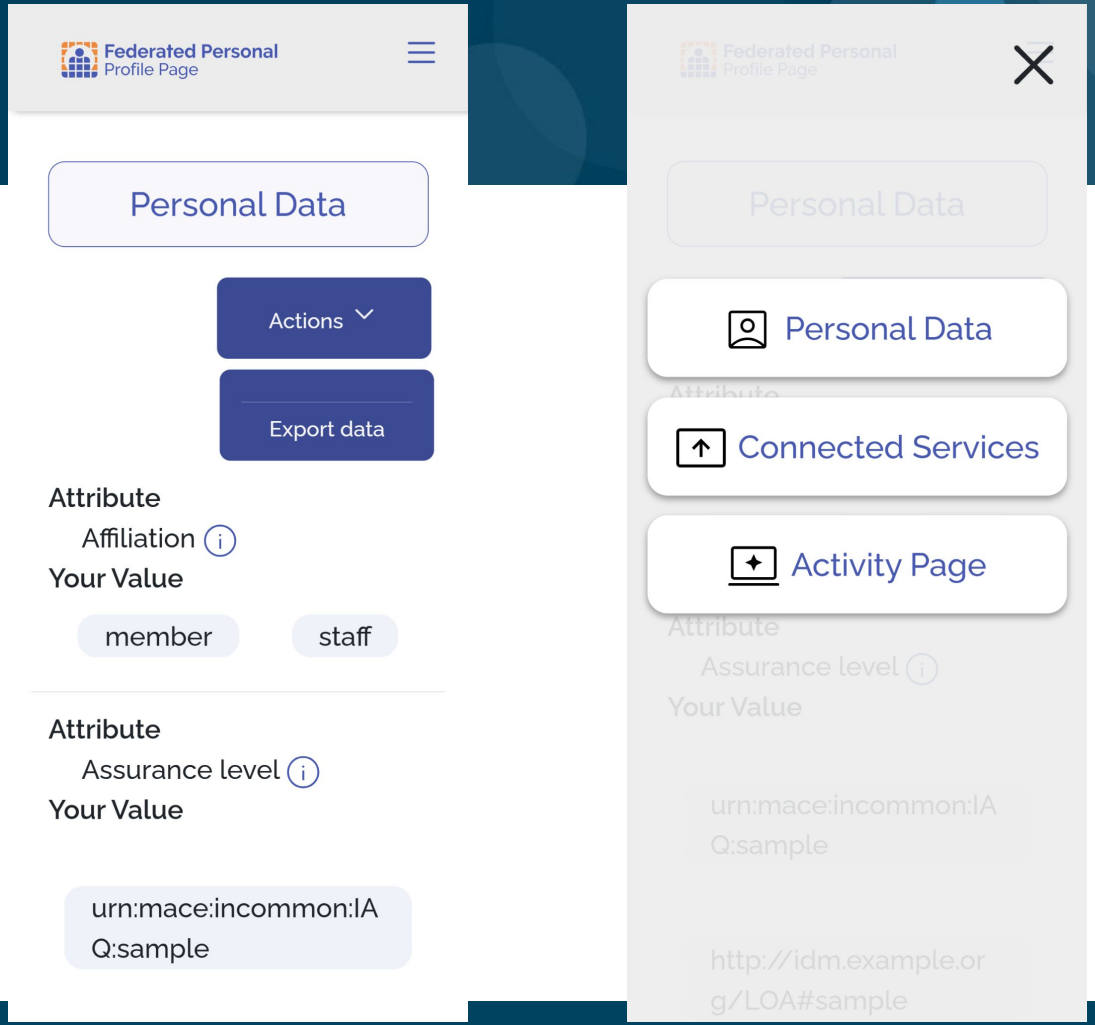
Shibboleth UI (Before)



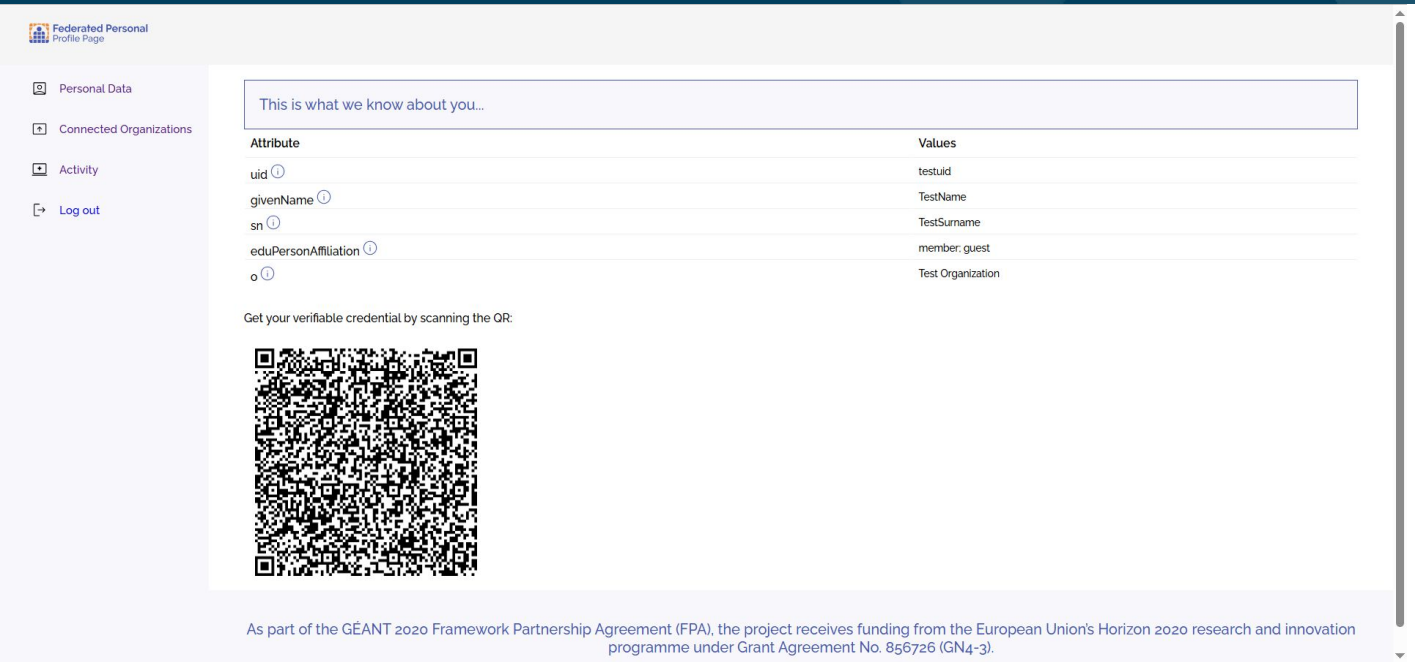
Shibboleth UI (After)

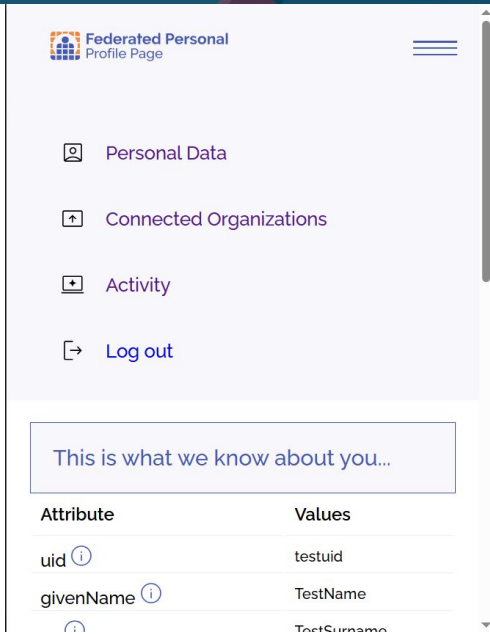


Shibboleth UI (After)

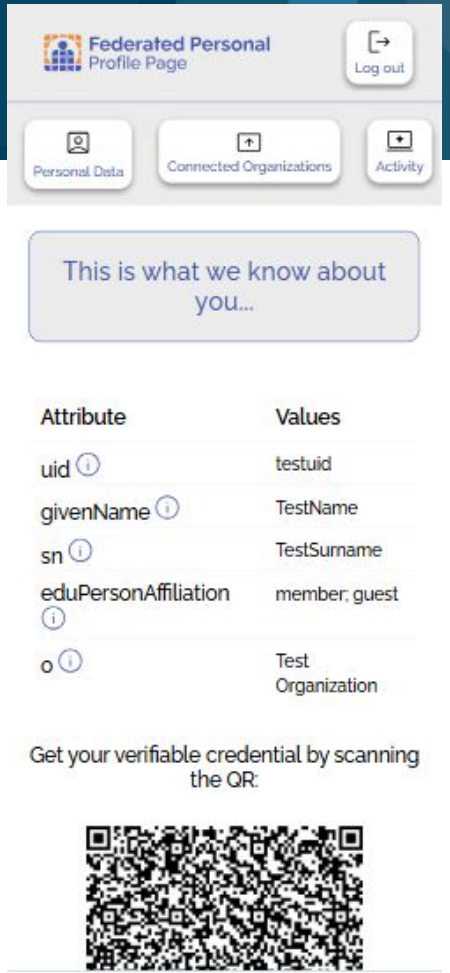


SimpleSAMLphp UI (Before)

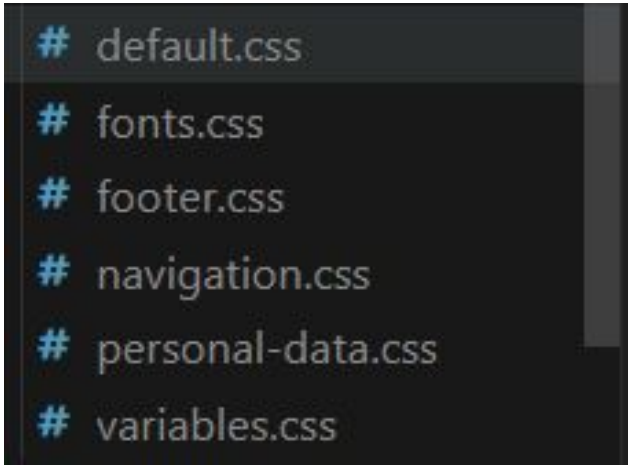


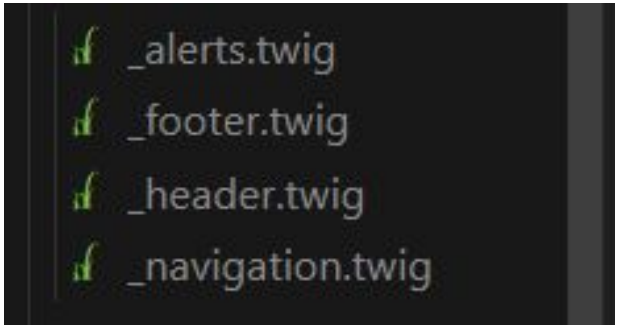


SimpleSAMLphp UI (After)



UX/UI Revamp






```
a:has(.navicon) {
    text-align: center;
}
```

Future plans

- code flow, not just pre-auth
- version 15, waiting for final draft?
  - multiple credential format(s), depending on interop needs - DIIP
- 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
  - Future plan: code review by WP9
    - Already some experience with shib user profile
  - Outreach and hand-over, wwWallet
- UX
  - Modular architecture.
  - Scalable CSS class structure (i.e., Block Element Modifier).
  - Focus on user feedback.

Thank you & please reach out to us!

mihaly.heder@sztaki.hu