Leveraging REFEDs specifications in OpenID Federation federation and OpenID Fed based wallet ecosystem (WIP!)

1.

- 1. Introduction
- 3. REFEDs specifications
- 4. Specification types
  - 4.1. OpenID Federation implementation of specification types
- 5. Overview of findings
- 6. Detailed discussion
  - 6.1. Personalized Access v.2

2. Introduction

The research and education sector has over the past decades developed a global identity federation ecosystem which has simplified access to content, services and resources for their community. The eduGAIN interfederation comprises over 80 national federations connecting more than 8,000 Identity and Service Providers. On a national level even more services and institutions are connected. The sector has been able to achieve this by creating a highly interoperable ecosystem, where both a high level of technical, as well as policy and trust interoperability has been accomplished, through the joined implementation of various specifications. The joined journey of establishing this ecosystem has enabled the emergence of a global research and education trust and identity community with strong bonds and decades of experience in deploying and operating identity federation at scale.

REFEDs, the Research and Education FEDerations group, has been instrumental in providing an open meeting place for articulating the mutual needs of research and education identity federations worldwide. Over the years, REFEDS has addressed issues and topics based on the interests and requirements of its participants. This includes mostly policy, but also some technical and outreach topics in areas such as interfederation, privacy, assurance, relationships with partner communities, marketing, and support of emerging federations.

While REFEDs as such has no bias towards a specific technical implementation, the fact that the SAML 2.0 specification is currently the dominant protocol in identity federation in R&E has had some impact on various specifications created by REFEDs. This ranges for protocol specific sections, to assumption on how a specification would be implemented operationally. The rise of protocols like OpenID Connect, OpenID Federation and the emergence of decentralized, wallet based ecosystems requires a revisit of the specifications. Not only should it be investigated in what way the specifications may be implemented in these protocols, in addition we must assume a multi-protocol ecosystem will emerge and exist for several years to come. This means the specifications may also need to take into account how to go between protocols as it may be required to translate between not just technical credentials, but also policy and trust frames.

This document provides a first assessment on how the current REFEDs specifications (Nov 2023) may be leveraged in an OpenID Federation (Draft 31) based federation and in a wallet ecosystem based on OpenID Federation and the OpenID4VC specifications. For the latter it should be noted that as this ecosystem and its standards are still being developed, the statements and assumptions on how REFEDs specification may be relevant should be considered speculative.

3. REFEDs specifications

source: https://refeds.org/specifications (Nov 2023)

<table>
<thead>
<tr>
<th>specification name</th>
<th>type</th>
<th>URI</th>
<th>doi</th>
<th>supporting material</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research and Scholarship (R&amp;S) v1.3</td>
<td>Entity Category</td>
<td><a href="http://refeds.org/category/research-and-scholarship">http://refeds.org/category/research-and-scholarship</a></td>
<td>blocked URL</td>
<td><a href="https://wiki.refeds.org/display/ENT/Research+and+Scholarship">https://wiki.refeds.org/display/ENT/Research+and+Scholarship</a></td>
</tr>
<tr>
<td>Hide From Discovery v.1</td>
<td>Entity Category</td>
<td><a href="http://refeds.org/category/hide-from-discovery">http://refeds.org/category/hide-from-discovery</a></td>
<td>blocked URL</td>
<td><a href="https://wiki.refeds.org/display/ENT/Hide+From+Discovery">https://wiki.refeds.org/display/ENT/Hide+From+Discovery</a></td>
</tr>
<tr>
<td>MFA Profile v.1</td>
<td>Profile</td>
<td><a href="https://refeds.org/profile/mfa">https://refeds.org/profile/mfa</a></td>
<td>blocked URL</td>
<td><a href="https://wiki.refeds.org/display/PRO/MFA">https://wiki.refeds.org/display/PRO/MFA</a></td>
</tr>
<tr>
<td>SFA Profile v.1</td>
<td>Profile</td>
<td><a href="https://refeds.org/profile/sfa">https://refeds.org/profile/sfa</a></td>
<td>blocked URL</td>
<td><a href="https://wiki.refeds.org/display/PRO/SFA">https://wiki.refeds.org/display/PRO/SFA</a></td>
</tr>
</tbody>
</table>
4. Specification types

REFEDs identify 5 types of specifications:

- **Entity Category**, defined in RFC8409, is a metadata label applied to identity providers or services which signal that they belong to the category which is described in the Entity Category specification. Metadata consumers which understand the Entity Category can alter their behaviour depending on the categories that the entity belongs to. Entity Categories may be used to signal to conform to the requirements of an identity assurance framework. The Assurance Certification can be self-asserted, or require validation by the registration authority (federation). An entity may conform to more than one Assurance Certification.

- **Profiles**, which define a standard to signal certain behaviour as part of a transaction, is generally covered in the underlying standards like OpenID Connect and OAuth.

- **Frameworks**, provide an extension to existing metadata profiles.

- **Metadata Extension**, defined in SAML V2.0 Identity Assurance Profiles Version 1.0, is a metadata label which can be applied to identity providers or services to signal that the entity conforms to the requirements of an identity assurance framework. The Assurance Certification can be self-asserted, or require validation by the registration authority (federation). An entity may conform to more than one Assurance Certification.

- **Security Contact**, defined in the Metadata Extension http://refeds.org/metadata/contactType/security, onforms to the requirements of an identity assurance framework. The Assurance Certification can be self-asserted, or require validation by the registration authority (federation). An entity may conform to more than one Assurance Certification.

- **Error Handling**, defined in https://refeds.org/specifications/errorurl-v1, which define a standard to signal certain behaviour in a federated authentication transaction, and how to respond to such a request.

Generally speaking, the information from the specifications is distributed in two ways:

- Entity metadata and/or
- As part of the transaction (e.g. in specific attribute values)

When a specification defines specific metadata elements to be be present, if is often required to have a protocol specific section in the specification. Not only is the technical format different (XML vs JSON), but there is also a difference in the way certain capabilities are expressed, e.g. Entity Categories vs Trustmarks, see later). When the specification only deals with 'on the wire' information, which is transmitted as part of the transaction, like e.g. attribute assurance, it is often much easier to adopt the specification to use in OIDC and OpenID federation, as often it suffices to just use the equivalent OIDC claim to transport the same values that were defined in the SAML based specification.

4.1. OpenID Federation implementation of specification types

OpenID Federation shares many concepts with the existing SAML based federations as currently deployed in R&E. The basic entities (OP, RP and trusted third parties like TA or IA) and the interactions between these can all be represented in OpenID Federation in a similar fashion as these exist in a SAML R&E federation.

- **Entity Category**: In OpenID federation, a Trustmark is defined as the way to signal certain behaviour of entities. A Trustmark is issued by a Trustmark Issuer, which in turn must be acknowledged in the Trust Anchor (metadata) to signal the Trustmark is part of the federation. A TA may set rules to enforce a Trustmark must be present in the entity metadata, which in turn leads to the mandatory requirement for entities to have the Trustmark before a trust chain can be established. The presence of a Trustmark may also be used to filter OPs in support of the discovery process.

- **Profiles**, which deal with 'on the wire' information, which is transmitted as part of the transaction, like e.g. attribute assurance, it if often much easier to adopt the specification to use in OIDC and OpenID federation, as often it suffices to just use the equivalent OIDC claim to transport the same values that were defined in the SAML based specification.

- **Assurance Certification** Signalling assurance certifications may be done using so called Trustmarks.

- **Metadata Extension**, defined in SAML V2.0 Identity Assurance Profiles Version 1.0, is a metadata label which can be applied to identity providers or services to signal that the entity conforms to the requirements of an identity assurance framework. The Assurance Certification can be self-asserted, or require validation by the registration authority (federation). An entity may conform to more than one Assurance Certification.

- **Security Contact**, defined in the Metadata Extension http://refeds.org/metadata/contactType/security, onforms to the requirements of an identity assurance framework. The Assurance Certification can be self-asserted, or require validation by the registration authority (federation). An entity may conform to more than one Assurance Certification.

Table 1 provides an overview of the specifications that were evaluated, and identifies the areas in the specification that would need modification to adopt OIDC and OpenID federation. Because of the commonalities in the structure of the Personalized Access, the Anonymous Access and the Pseudonymous Access Entity Category, only the first one was extensively evaluated, see Chapter 6. It was assumed similar modifications will be required for the Anonymous Access and Pseudonymous Access specification.

5. Overview of findings
<table>
<thead>
<tr>
<th>specification name</th>
<th>type</th>
<th>Applies to entity</th>
<th>Asserted by</th>
<th>Level of Modification needed?</th>
<th>In scope for OpenIDFed</th>
<th>In scope for wallets</th>
<th>Attribute profile</th>
<th>SAML Specific Protocol requirements</th>
</tr>
</thead>
</table>
| Personalized Access v.2 | Entity Category | IdP/OP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Personalized Access v.2 | Entity Category | SP/RP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Anonymous Access v.2 | Entity Category | IdP/OP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Anonymous Access v.2 | Entity Category | SP/RP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Pseudonymous Access v.2 | Entity Category | IdP/OP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Pseudonymous Access v.2 | Entity Category | SP/RP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Research and Scholarship (R&S) v1.3 | Entity Category | SP/RP | Registrar | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 4: RC3  
Section 5 (extension already possible)  
Section 7: SAML specific example, should probably move under 5.1.1  
Section 8: SAML specific example, should probably move under 5.1.1 |
| Research and Scholarship (R&S) v1.3 | Entity Category | IdP/OP | IdP/OP | anyak | ✓ (7) | ✓ | ✓ | RFC8409  
Section 4.3.1  
Section 4.3.3  
Section 6 (moving mention of <md:RequestedAttribute> mechanism to SAML 2.0 specific part of section 5 would already suffice)  
Section 6 (SAML specific example and identifier handling)  
Section 7 (SAML example) |
| Hide From Discovery v.1 | Entity Category | IdP/OP | IdP/OP | anyak | ✓ (7) | ✓ | ✓ | Use of SAML specific terms like IdP and SP  
Section 6: SAML specific example |
| Assurance v.1 | Framework | IdP/OP | IdP/OP | anyak | ✓ (7) | ✓ | ✓ | Section 7 already discusses the use of the "eduperson_assurance" claim as the mechanism to provide assurance information in OIDC |
| MFA Profile v.1 | Profile | IdP/OP | ✓ (7) | ✓ | ✓ | ✓ | No changes needed, however has dependency on Security Contact Metadata Extension  
For use with wallets more context is needed |
| SFA Profile v.1 | Profile | IdP/OP | ✓ (7) | ✓ | ✓ | ✓ | No changes needed, however has dependency on Security Contact Metadata Extension  
For use with wallets more context is needed |
| Sirtfi v1 & v2 | Assurance Certification | IdP/OP | Registrar | anyak | ✓ (7) | ✓ | ✓ | No OIDC or OpenID Federation specification present.  
Requires extension of OIDC Metadata model |
| Security Contact Metadata Extension | IdP/OP, SP/RP | IdP/OP, SP/RP | anyak | ✓ (7) | ✓ | ✓ | No changes needed, however has dependency on Security Contact Metadata Extension  
For use with wallets more context is needed |

Legenda for relevance column: 🤔 Under investigation; ❌ Not relevant; ✓ Relevant; (T) Trustmark required  
Indication of required changed: 😞 No changes required; 😩 Minor updates to wording required; 😞� Significant updates to wording required; 😞���, Significant updates to wording and/or implementation required

6. Detailed discussion

6.1. Personalized Access v.2