REFEDS Assurance Suite

FIM4R, 11 Feb 2019
Mikael Linden, REFEDS assurance wg chair
mikael.linden@csc.fi
Challenge

How was the registration/Identity Proofing done?
Is that even a shared account (libraryuser1@university.org)?
Can this user ID be later reassigned to some other person?
How fresh is that affiliation information?
How was the user authentication done?
Short history of REFEDS Assurance Suite

- 11/2015 AARC publishes minimum requirements on assurance
- 6/2016 REFEDS establishes Assurance working group
- 4-6/2017 First public consultation on RAF
- 2-5/2018 Pilot on RAF, SFA and MFA
- 4-6/2018 Second public consultation on RAF and SFA
- 10/2018 RAF and SFA ver 1.0 published
REFEDS Assurance Suite

- REFEDS Assurance Framework (RAF) ver 1.0
  - Approved and published
  - [https://refeds.org/assurance](https://refeds.org/assurance)

- REFEDS Single-factor authentication profile (SFA) ver 1.0
  - Approved and published
  - [https://refeds.org/profile/sfa](https://refeds.org/profile/sfa)

- REFEDS Multi-factor authentication profile (MFA) ver 1.0
  - approved in June 2017
  - [https://refeds.org/profile/sfa](https://refeds.org/profile/sfa)

You can use them together or separately
The big picture of assurance in REFEDS

Identifiers
- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

ID proofing
- Low (self-asserted)
- Medium (e.g. postal credential delivery)
- High (e.g. F2F)

Attributes
- Affiliation freshness
  - 1 month
- Affiliation freshness
  - 1 day

Authentication
- Single-factor authentication
- Multi-factor authentication
Split of responsibility between REFEDS specs

REFEDS Assurance framework (RAF)

Identifiers
- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

ID proofing
- Low (self-asserted)
- Medium (e.g. postal credential delivery)
- High (e.g. F2F)

Separate specification:
- REFEDS Single-Factor Authentication (SFA)
- REFEDS Multi-Factor Authentication (MFA)

Attributes

Authentication
- Single-factor authentication
- Multi-factor authentication

AuthN profiles
Test your IdP’s conformance:
https://attribute-viewer.aai.switch.ch/aai/

RAF values released by your IdP

You can ask the test SP to request particular authentication context and display IdP’s response
Outreach to federations

• Presentations REFEDS 38th in Trondheim
• Presentations REFEDS 39th meeting in Orlando
• TechEx 2018 session in Orlando
• Webinar December 2018
  • https://www.youtube.com/channel/UCussxbcR_OxG1e_kRp0pjpA
Start supporting it!
Start requiring it!

Otherwise the IdPs are not going to deploy it.
Questions?

The work has been funded by AARC, AARC2 and GN4 projects.
Backup slides
Assurance Framework assertions and profiles

To be expressed by the CSP in the eduPersonAssurance attribute:

$PREFIX$=https://refeds.org/assurance
RAF values for properties of identifiers

**Identifiers**

ID is unique, personal and traceable

- **eduPersonAssurance=${PREFIX}$/ID/unique**
  1. The user identifier represents a **single** natural person
  2. The CSP **can contact** the person to whom the identifier is issued
  3. The user identifier is **never re-assigned**
  4. The **user identifier** is `eduPersonUniqueID`, SAML 2.0 persistent
     nameId, subject-id or pairwise-id or OIDC sub (public or pairwise)

ePPN is unique, personal and traceable

- **eduPersonAssurance=${PREFIX}$/ID/no-eppn-reassign**
  - `eduPersonPrincipalName` value has properties 1-3 (see above).

- **eduPersonAssurance=${PREFIX}$/ID/eppn-reassign-1y**
  - `eduPersonPrincipalName` value has properties 1-2 (see above) but
    may be re-assigned after a hiatus period of 1 year or longer.

(e.g. F2F)
RAF values for identity proofing

Identifiers
- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

ID proofing
- Low (self-asserted)
  - eduPersonAssurance=$PREFIX$/IAP/low
  - sections 5.1.2-5.1.2.9 & 5.1.3 of Kantara AL1
  - IGTF level DOGWOOD or ASPEN

- Medium (e.g. postal credential delivery)
  - eduPersonAssurance=$PREFIX$/IAP/medium
  - sections 5.2.2-5.2.2.9, 5.2.2.12&5.2.3 of Kantara AL2
  - IGTF level BIRCH or CEDAR
  - section 2.1.2, 2.2.2 and 2.2.4 of eIDAS low

- High (e.g. F2F)
  - eduPersonAssurance=$PREFIX$/IAP/high
  - section 5.3.2-5.3.2.9, 5.3.2.12&5.3.3 of Kantara AL3
  - section 2.1.2, 2.2.2 and 2.2.4 of eIDAS substantial

Identity proofing and credential issuance, renewal, and replacement qualify to any of…
RAF values for attribute freshness

**Identifiers**

- **edupersonassurance=*/PREFIX$/*/ATP/*/ePA-1m
  - edupersonaffiliation, edupersonscopedaffiliation and edupersonprimaryaffiliation attributes (if populated and released to the RP) reflect user's departure within **31 days** time

- **edupersonassurance=*/PREFIX$/*/ATP/*/ePA-1d
  - edupersonaffiliation, edupersonscopedaffiliation and edupersonprimaryaffiliation attributes (if populated and released to the RP) reflect user's departure within **one days** time

**Attributes**

- **Affiliation freshness 1 month**
- **Affiliation freshness 1 day**

**Authentication**

- Single-factor authentication
- Multi-factor authentication
In all cases the CSP MUST (baseline expectations for Identity Providers):

1. The Identity Provider is operated with **organizational-level authority**
2. The Identity Provider is trusted enough that it is (or it could be) used **to access the organization’s own systems**
3. **Generally-accepted security practices** are applied to the Identity Provider
4. **Federation metadata is accurate, complete**, and includes at least one of the following: support, technical, admin, or security contacts

A CSP indicates its conformance to this profile by asserting $PREFIX$. 
"Cappuccino" for low-risk research use cases

REFEDS Assurance framework (RAF)

- **Identifiers**
  - ID is unique, personal and traceable
  - ePPN is unique, personal and traceable

- **ID proofing**
  - Low (self-asserted)
  - Medium (e.g. postal credential delivery)
  - High (e.g. F2F)

- **Attributes**
  - Affiliation freshness 1 month
  - Affiliation freshness 1 day

- **Authentication**
  - "Goes with" Single-factor authentication
  - Multi-factor authentication

AuthN profiles
“Espresso” for more demanding use cases

REFEDS Assurance framework (RAF)

Identifiers
- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

ID proofing
- Low (self-asserted)
- Medium (e.g. postal credential delivery)
- High (e.g. F2F)

Attributes
- Affiliation freshness 1 month
- Affiliation freshness 1 day

AuthN profiles
- Single-factor authentication
- Multi-factor authentication

"Goes with"
Single-factor authentication profile

https://refeds.org/profile/sfa
## SFA profile requirements

### Authentication

<table>
<thead>
<tr>
<th>Authenticator type</th>
<th>Secret basis</th>
<th>Min length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorized Secret</td>
<td>(\geq 52 \text{ characters (e.g. 52 letters)})</td>
<td>12 characters</td>
</tr>
<tr>
<td></td>
<td>(\geq 72 \text{ characters (e.g. 52 letters + 10 digits + 10 special characters)})</td>
<td>8 characters</td>
</tr>
<tr>
<td>Time based OTP-Device Out-of-Band Device</td>
<td>10-51 characters (e.g. 10 digits)</td>
<td>6 characters</td>
</tr>
<tr>
<td>Look-Up Secret Sequence based OTP-Device</td>
<td>10-51 characters (e.g. 10 digits)</td>
<td>10 characters</td>
</tr>
<tr>
<td></td>
<td>(\geq 52 \text{ characters (e.g. 52 letters)})</td>
<td>4 characters</td>
</tr>
<tr>
<td></td>
<td>(\geq 52 \text{ characters (e.g. 52 letters)})</td>
<td>6 characters</td>
</tr>
<tr>
<td>Cryptographic Software/Device</td>
<td>RSA/DSA</td>
<td>2048 bit</td>
</tr>
<tr>
<td></td>
<td>ECDSA</td>
<td>256 bit</td>
</tr>
</tbody>
</table>

---

*Identifiers*

- ID proofing
- Authentication

*Attributes*

- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

*Affiliation freshness*

- 1 month
- 1 day

*Authenticator type*

- Single-factor authentication
- Multi-factor authentication

*Secret basis*

- Secret basis
- Min length
Further SFA requirements

• Protection against online guessing (e.g. rate limiting).

• Secrets cryptographically protected online and in transit

<table>
<thead>
<tr>
<th>Way of delivery</th>
<th>Maximum life time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time based OTP Device</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Telephone network (e.g. SMS, phone)</td>
<td>10 minutes</td>
</tr>
<tr>
<td>E-mail (e.g. recovery link)</td>
<td>24 hours</td>
</tr>
<tr>
<td>Postal mail</td>
<td>1 month</td>
</tr>
</tbody>
</table>
SFA requirements:
Replacement for a lost authentication factor

• An **existing secret** must not be sent to the user (e.g. a stored password).
• The replacement procedure does not **solely rely on knowledge-based authentication** (e.g. answer a secret question).
• Human based procedures (e.g. service desk) ensure a **comparable level** of assurance of the requesting user identity as the initial identity vetting.
• In order to restore a lost authentication factor, an OTP may be sent to the users **address of record**.
• For authenticators which are provided to the user as a **backup**, all requirements of the corresponding authentication factor apply.
Multi-factor authentication profile

https://refeds.org/profile/mfa
The authentication of the user’s current session used a combination of at least two of the four distinct types of factors: something you know, something you have, something you are, something you do.

- The factors are independent (access to one factor does not by itself grant access to other factors).
- The combination of the factors mitigates single-factor only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.