REFEDS Assurance Framework

AARC AHM 11 Apr 2018 in Athens
Mikael Linden, REFEDS assurance wg chair
mikael.linden@csc.fi
Short history and future

• 11/2015 AARC publishes minimal LoA requirements for low-risk research
• 6/2016 REFEDS establishes the Assurance working group
  • To write a specification to meet the requirements
• 4-6/2017 Public consultation on the 1st draft of the REFEDS Assurance Framework (RAF)
• Going to expose RAF to second public consultation soon
  • Together with REFEDS Single-Factor Authentication (SFA) profile
• Currently having a pilot on RAF/SFA
  • SPs: ELIXIR, BBMRI, CILogon, EGI Check-in
  • IdPs: Chicago, XCEDE, Aalto, CSC
  • Missing more IdP products (SimpleSAMLphp, ADFS, ...)
The big picture of assurance

<table>
<thead>
<tr>
<th>Identifiers</th>
<th>ID proofing</th>
<th>Attributes</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID is unique, personal and traceable</td>
<td>Low (self-asserted)</td>
<td>Affiliation freshness 1 month</td>
<td>Single-factor authentication</td>
</tr>
<tr>
<td>ePPN is unique, personal and traceable</td>
<td>Medium (e.g. postal credential delivery)</td>
<td>Affiliation freshness 1 day</td>
<td>Multi-factor authentication</td>
</tr>
<tr>
<td></td>
<td>High (e.g. F2F)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Split of responsibility clarified

REFEDS Assurance framework

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
- Separate specification: REFEDS Single-Factor Authentication (SFA) DRAFT
- Separate specification: REFEDS Multi-Factor Authentication (MFA) ver 1.0 June 2017

Authentication
- Single-factor authentication
- Multi-factor authentication

AuthN profiles
“Cappuccino” for low-risk research use cases

REFEDS Assurance framework

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

AuthN profiles
“Espresso” for more demanding use cases

**REFEDS Assurance framework**

**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

**AuthN profiles**
More information

• REFEDS assurance wg: https://wiki.refeds.org/x/MgDI
• mikael.linden@csc.fi
REFEDS Single-Factor Authentication Profile

• New approach: SFA v0.2
• Basic structure/hierarchy (Profile–Minimum Requirements–Recipes) dropped

→ One generic document covering all types of authentication factors

• Risk-based approach (controls) dropped
REFEDS Single-Factor Authentication Profile

- SAML and OIDC authentication context
- Terminology used in this document based on NIST 800-63B
- Defines a security baseline for AuthN using a single factor
- Two main criteria:
  1) Requirements for authentication factors
     - Properties of the factor itself:
       Minimum secret length, Basis for secret generation
     - Threat protection:
       Prevent online guessing, Protect the secret cryptographically
  2) Requirements for replacement of a lost authentication factor