Making Identity Assurance and Authentication Strength Work for Federated Infrastructures

ISGC 2021, 25 March 2021
Motivation

Assurance: Quality/degree of trust of identity and authentication information
Assurance Challenge

• Identity Provider Challenge: How to implement assurance requirements?
• Service Provider Challenge: Which values should be requested? Risk exposure?

→ Both will be discussed with use of the REFEDS Assurance Suite
## Common Assurance Frameworks and Risk Management

<table>
<thead>
<tr>
<th>Frameworks with R&amp;E Scope</th>
<th>Assurance Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGTF assurance profiles</td>
<td>NIST SP 800-63</td>
</tr>
<tr>
<td><strong>REFEDS Assurance Suite</strong></td>
<td>eIDAS</td>
</tr>
<tr>
<td></td>
<td>Kantara IAF</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Graphical Comparison of Assurance Frameworks (AARC-I050)
REFEDS Assurance Suite in a nutshell

- Consisting of three individual specifications:
  - REFEDS Assurance Framework (RAF), ver 1.0, published 2018
  - REFEDS Single Factor Authentication Profile (SFA), ver 1.0, 2018
  - REFEDS Multi Factor Authentication Profile (MFA), ver 1.0, 2017
- component-based approach
- Two identity assurance profiles: Espresso (high assurance) and Cappuccino (moderate assurance)
REFEDS Assurance Suite Big Picture

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 Profiles
- Single-factor authentication
- Multi-factor authentication

Cappuccino
- Single-factor authentication
- Multi-factor authentication

Espresso
- Single-factor authentication
- Multi-factor authentication
IDP-side: Implement REFEDS Assurance Components

Campus Use Case

• Consider different roles (e.g. student versus employee)

• ID uniqueness:
  • may be seen as the core criteria as it is affecting other components
  • identifier is bound to single natural person who can be contacted
  • special care needs to be taken on reassignment practices

• ID Proofing:
  • universities seem to meet/exceed Cappuccino requirements
  • How does enrollment for foreign students look like?
• Affiliation freshness:
  • check offboarding process and other top level policies

• Authentication Strength (SFA):
  • no requirement on periodic password changes, but for good quality passwords
  • threat protection
  • care is needed for secrets which are transmitted (e.g. initial password) and replacement processes
SP-side: Select REFEDS Assurance Values

• Determining the appropriate assurance level is all about risk management
• In an ideal world: three-fold approach
SP-side: Select REFEDS Assurance Values (cont.)

• In case formal asset & risk management processes are not in place:
  • Start self-assessing service(s) which rely on external assurance
  • If applicable, consider grouping of services
  • Focus on services in production
  • For R&E services, use medium as reference level for both identity and authentication assurance, increase or decrease if needed
Open Science Cyber Risk Profile¹
- Data Assets
- Facilities Assets
- System and Hardware Assets
- Software Assets
- Instruments
- Intangible and Human Assets

Categories of harm derived from NIST²
- Reputational damage & inconvenience
- Financial loss & liability
- Harm to assets & operations
- Unauthorized release of sensitive information
- Legal violations
- Personal Safety

1: http://trustedci.github.io/OSCRP/OSCRP.html
General Recommendations for adopting REFEDS Assurance Suite

• Identity Provider side:
  • It may make sense to introduce assurance components gradually (e.g. role based, starting with affiliation=staff)
  • Don’t use/introduce authentication factors considered as insecure (e.g. SMS)

• Service Provider side:
  • Don’t ask for more assurance than you need, consider how much you really need to control your users
  • OSCRSP assets & NIST categories of harm may serve as starting point
Conclusion

• We will submit a paper for more detailed information
• Work in progress, we plan to share further use cases, experiences and guidance
• Concept of ‘families of related services’

Any Questions?