Making Identity Assurance and Authentication Strength Work for Federated Infrastructures

EGI Conference 2020, 3 November 2020
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?

→ The former will be discussed with use of the REFEDS Assurance Suite
## Common Assurance Frameworks

<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>REFEDS Assurance Suite</td>
<td>eIDAS</td>
</tr>
<tr>
<td></td>
<td>Kantara IAF</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
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)
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?
Campus Use Case

• 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
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. Start from medium.
Conclusion

• Work in Progress, stay tuned!
• SP recommendations for helping decide which assurance value to ask will follow soon

Any Questions?