20220209 - Futures Working Group (baseline)

Meeting Date: 9th February 2022, 14:00 CET.

Attendees: Steve Glover, Casper Dreef, Nicole Harris, Terry Smith, Davide Vaghetti, Alex Stuart, Guy Halse, Kevin Hickey, Pal Axelsson, Meshna Koren, Alan Buxey, Maarten Kremers, Daniel Muscat, Dean Flanders

Agenda:

1. Discuss Goal 1 of the Charter
2. Review recommendation summaries from each meeting.

After this meeting we will have reviewed all the goals. At this point I would propose the secretariat makes the first attempt at drafting a recommendations document and shares with the group for comment. Lets take a 4 week cycle for this Working doc

Recommendations so far:

<table>
<thead>
<tr>
<th>Recommendations (governance discussion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address the low attendance and low input at eduGAIN meetings by creating an eduGAIN Steering Committee (elected) and hold an annual assembly with all of the current SG</td>
</tr>
<tr>
<td>Improve participation in leadership from non-federation members</td>
</tr>
<tr>
<td>Have a consistent approach to how federations are expected to publish metadata downstream</td>
</tr>
<tr>
<td>Improve consistency of federation policies</td>
</tr>
<tr>
<td>Consider levels (max 3) that apply to all IdPs</td>
</tr>
<tr>
<td>Improve joining process for new entities</td>
</tr>
<tr>
<td>Support implementation of baseline expectations (see goal 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendations (service model discussion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have a consistent approach to how federations are expected to publish metadata upstream and downstream</td>
</tr>
<tr>
<td>Improve positioning of Seamless Access in relation to eduGAIN</td>
</tr>
<tr>
<td>Review eduGAIN mission statement</td>
</tr>
<tr>
<td>Consider levels (max 3) that apply to all IdPs (Anon, Pseudon, Personalised) plus CoCo, Sirtfi, Assurance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Baseline Requirement</th>
<th>Potential eduGAIN Improvements</th>
</tr>
</thead>
</table>
| [FO1] You focus on trustworthiness of Federation as a primary objective and are transparent about such efforts | • Inability to filter out an entity  
• Lack of updates regarding FO changes (solved by health check? / audit)  
• Inability to take action over CoCo, Sirtfi, R&S violations  
• Governance structure not fit for purpose |
| [FO2] You publish contact information and respond in a timely fashion to operational issues | • Enforce FO security contact  
• Enforce use of non-personal address for "contact"  
• We don't have management contacts  
• Poor response / participation from federations?  
• Do we want to create aliases for each federation? e.g. caf@support.edugain.org?  
• Regular testing of technical contacts as well as security contacts |
| [FO3] You apply security practices to federation operations and ensure timely incident response | • Inability to take actions centrally (in particular any complaint about a Member shall be made to the operator of its Participating Federation and dealt with between that Member and that operator according to the rules of that Participating Federation and subject only to that Participating Federation’s governing law and jurisdiction)  
• Lack of ability of eduGAIN to enact emergency changes and sanctions on entities  
• Suspension correlation to eduGAIN “rules”  
• Security of core eduGAIN infrastructure (MDS, websites etc)  
• Ensure that we define timely for eduGAIN |
### [FO4] You follow good practices to ensure authentic, accurate and interoperable metadata to enable secure and trustworthy federated transactions

- Inability to offer SPs a guaranteed response from specific IdPs - experience of trying to connect is too varied.
- Some technical checks are informal (e.g. checking the UK import issues list) and not formalised.
- Too many different tools, lack of one process for checking metadata issues.
- What is “accurate” what is “interoperable”? is “consistent” part of this?
- Is it just about metadata? about the protocol messages?
- Overview of the tools and description of what each does (landing page).
- Metadata propagation and how we improve

### [FO5] You implement and support frameworks that improve trustworthy and scalable use of Federation and promote their adoption by members and other participants

- Governance structure not fit for purpose
- Need to enforce standards like CoCo, R&S, Sirtfi, assurance, MFA and more
- Assurance?
- Adoption and promotion mandate

### [FO6] You collaborate with other organisations to promote realization of baseline expectations nationally and internationally

- Need to implement the baseline first.
- Continuous work to ensure that compliance is met.

**Notes:**

FO1: comments and additions
Davide: some of the potential improvements are linked. Violations & filtering and the decision making (governance structure).
Guy: +1. Not an agile governance model.
Meshna: Where lies the difficulty? Technical or policy?
Davide: The constitutions doesn't allow us to filter entities on the eduGAIN level.
Nico: The potential impact when taking an IdP down.
Davide: Process driven.
Alan: Rules aren't clearly written. It is the FO responsibility to provide clean MD. First step: agreement between FO and eduGAIN to allow filtering.
Guy: Wide range of technical and support abilities. We could do this differently for different federations.
Nico: Different service models for different types of federations.
Pal: FO still need to take/stay responsible for their MD. Be careful with wording.

Meshna: A need for an entity in Federation X to address changes with other federations?
Nico: Testing security and technical

FO2:
Guy: eG obligation that ...
Alex: Scrap enforcing non-personal accounts
Daniel: Could cause GDPR issues
Terry: Self-service.
Alex: EntitiesDiscriminator has an element. URI, URL and contact address.
Meshna: Self-service is great, but you need a central contact.
Terry: Use a token fee?

FO3:
Pal: We have stuff to utilise. Handbook, WG, Sec Team.
Nico: SIRTFI wasn't mentioned. Should this be considered?
Meshna: The environment is not ready for SIRTFI yet. Make SIRTFI approachable for non-techs. Describe scenarios. Determine smallest minimum requirement in certain situation more helpful than mandating.
Guy: Unlink security contact from SIRTFI. Upping the bar over time.
Maarten: Here also FO1 come into place. Governance model to get this done.
Terry: Using tiers rather than bars. Encourage to take the next step.
Davide: 1. currently over 30% SIRTFI entities, concentrated in limited number of federations. Agree with gradual progress
Pal: REFEDS is working on a new version, easier to understand. Adoption by key services is required. We need to talk about eduGAIN baseline level.

FO4:
Pal: We have a SAML profile, but may want to rework that.
Alex: Tune up the existing tools.
Pal: Should we a propagation time limit?
Davide: SAML2int? Not a minimal requirement.
Alan: Point back to FO1

FO5:
Pal: To make eG work seamlessly this needs to be promoted, rather than enforced.
Davide: How to implement them in your federation? No agreement on this. eG may fill the gap here.

FO6:
Pal: actively track if federations are also implanting baseline.
Skip next meeting (23 Feb).