20220112 - Futures WG meeting (service model)

Attendees: Terry Smith, Guy Halse, Alex Stuart, Casper Dreef, Kevin Hicky, Nicole Harris, Davide Vaghetti, Pal Axelsson, Mario Reale, Dean Flanders, Daniel Muscat, Alan Buxey, Chris Phillips

Agenda:

- Goal 2
- Goal 3

Notes

Four goals of the working group were finalised on the 20211208 - Planning meeting for Futures WG.

Goal 2: fundamental changes on the eduGAIN service model. Currently only SAML.

Proposals: explicitly commit to certain profiles like CoCo and SIRTFI.

Alex: Import and export policies. Should standardising be a goal?
Guy: Observation. No coherence in the different services (eG, SeamlessAccess). Make it easier to understand for new SPs and IdPs.
Nicole: What changes could we propose?
Guy: Better documentation.
Pål: Should this be part of an eduGAIN mission statement.
Nicole: Improve the quality of IdPs.
Guy: Tagging and filter 'bad' MD. Set quality requirements.
Terry: We focused on supporting research first. Making it easy to collaborate and share.
Guy: Libraries can also drive adoption.
Pål: For libraries we have OpenAthens to compete with.
Alex: OA are now managing UK Federation. Different attitude than NREN based federations.
Is it that the researches have a more permanent relationships with their universities? Or are they more related to the topic.
Terry: We work with the (topic) community rather than the NREN. Similar to eduTEAMS.
Dean: We have to develop our own methodologies. The big limitation is that we can't get the research group information. eduGAIN has limitations.
Grouping is key to open science.

Davide: Common problem. Uni IT not able to cope with grouping thousands of users. What we've learned is the solution is creating virtual organisations with some who is assigned to look after entitlements.

Nicole: Budget / Resource limitations. How do we address this issue?
Dean: Minimum standards. Authenticate someone from a specific organisation is already useful, but additional information would be very useful. AuthZero is good solution.
Alan: To be sure we're not comparing apples to oranges would have to take into account the size of the federation when looking at FTE/funding - number of IdPs etc. (and full mesh versus hub and spoke have different scale/mgmt issues). Though would be concerned about > 1 FTE values - if its that low...is that at least some backup/succession person available should the current single person leave. Authorisation (group membership) needs a mature identity and access management platform - but you still have the issue of how to educate staff to request particular access for a relying party....and even then who is the authority to confirm that person should have that right given to them.... How does the IT dept know that Dr XYZ at LHC is the one to vouch that Dr ABC should have that entitlement (after Dr ABC has requested access to the service....)
Pål: The question is where you put the costs.

Dean: Integrate to more that SAML.
Chris: It seems that data is more important than authentication. Authentication methods support the exchange of data.
Nicole: Is not a group management services. It wants to integrate with group management solutions.
Pål: Release data and information in a safe and secure way.
Chris: eG as an electricity grid.
Nicole: True, but were are using different plugs.

Nicole: How to make this more practical?
Pål: We don't have the ability to force our members.
Chris: Provide Standard eG and eG+? Indeed, it is already there, but it is on voluntary basis.
Guy: Older federations are facing this problem. It's easier for the newer federations. But in the services drive this.
Kevin: If MFA, which is a form of assurance, is on the table, it does open the conversation to the infrastructure (Azure AD) organizations utilize. Few organization will choose to operate their own MFA solution.
Chris: interesting observation: *ALL* inCommon is SIRTFI enabled — and CIlogon considers it so.. so others have to specifically step up to tagging SIRTFI to get access to CIlogon

Nicole: Can eG be the catalyst?

<table>
<thead>
<tr>
<th>Recommendations</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>