eduGAIN SG-2018 June

eduGAIN Steering Group Meeting

Tuesday 19th June 2017, 12:00 - 13:30 UTC (in your timezone)

Please Note that the above time is **CONFIRMED**.

11:45 UTC 13:45 CEST	Arrival & "Can you hear me now?" (see Connection Details) ○ Chat via https://edugain.org/slack
12:00 UTC 14:00 CEST	**Welcome, Introductions & Agenda Agreement** • Open Actions & Previous Meeting.

12:15 UTC 14:15 CEST	**Membership Updates and Joining**
	
	   ○ Pipeline and process for new members.
	   ○ Malaysia and CAFMoz are currently in the membership pipeline.

12:30 UTC 14:30 CEST	**Revision of the eduGAIN Policy Framework**
	
	   ○ SAML Profile impact of enforcement
	   ○ Changes to implement
	   ○ Acceptable grace period for current participants?

12:45 UTC 14:45 CEST	**Best/Current Practices within eduGAIN**
	
	   • Best & Current Practices
	   • What to add? How to validate?

13:00 UTC 15:00 CEST	**Future Voting?** • What to do in a Post-Foodle world (1 July 2018)

13:15 UTC 15:15 CEST	**Future SG Meetings**
	
	   • Conflict/Changes to 2018 meeting dates/times?
	   • Next meeting @ 6-9 August 2018 at APAN46 & via VC

13:20 UTC 15:20 CEST	Any other business, Summary, Actions and Close (or we're running over time).
13:30 UTC 15:30 CEST	Meeting Close.

Connection Details

- WebRTC: https://call.lifesizecloud.com/call/2410313
- H323: https://call.lifesizecloud.com/otherways/2410313 H323:169.57.7.200##2410313
- SIP: 2410313@lifesizecloud.com
- Phone: tel:+31858884440,2410313# or https://call.lifesizecloud.com/numbers

Attendance

Federations in Attendance (19)

1. TAAT/EENet
2. eduID.lu/RESTENA
3. IDEM/GARR
4. FÉR/RENATER
5. COFRe/REUNA
6. SAFIRE
7. DFN-aai
8. SWAMID/SUNET
9. UK Federation/Jisc
10. LEAF/RENAM/Moldova
11. IIF/IUCC
12. AAI@EduHR
13. RIF
14. ACOnet-AAI
15. CAFe
16. ARNaai
17. HKAF
18. FEIDE
19. *safeID

*Not a member.

Attendees (23)

1. Brook Schofield, GÉANT
2. Casper Dreef, GÉANT
3. Nicole Harris, GÉANT
4. Sten Aus, EENet
5. Stefan Winter, RESTENA
6. Barbara Monticini, IDEM GARR
7. Anass Chabli , RENATER
8. Alejandro Lara, REUNA
9. Donald Coetzee, SAFIRE
10. Guy Halse, SAFIRE
11. Wolfgang Pempe, DFN
12. Pàl Axelsson, SWAMID
13. Rhys Smith, Jisc
14. Valentino P, LEAF
15. Zivan Yoash, IIF
16. Miroslav Milinovic, AAI@EduHR
17. Nicholas Mbonimpa, RIF
18. Peter Schober, ACOnet
19. Rui Riberio, CAFe
20. Aouaouche El-Maouhab, ARNaai
21. Jonathan Cheng, HKAF
22. Jaime Perez, FEIDE
23. *Martin Stanislav, safeID

Apologies (7)

1. Arnout Terpstra, SURFnet
2. Pascal Panneels, Belnet
3. Terry Smith, AAF
4. José-Manuel Macías, RedIRIS
5. Chris Phillips, CAF
6. Simon Green, SGAF
7. Zenon Mousmoulas, GRNET

Notes

Welcome, Introductions & Agenda Agreement

The Chair welcomed everyone to the 4th meeting of 2018.

Membership Updates and Joining

For details on new members and candidates see https://technical.edugain.org/status and work on progressing new members is underway.

Membership assessment continues on track but tracking votes will soon be an issue.

Revision of the eduGAIN Policy Framework

Impact of enforcement of the SAML Profile is described in the following table:

Issue	Federations	Count
No issues	DZ, AU, AT, BY, BR, CA, HR,CZ, EC, EE, GE, DE, IN, HU, KR, LV, LT, LU, MD, NO, RU, PL, SG, ZA, ES, UA, CH, NL	28
EntitiesDescriptor does not contain PublicationInfo	AR, FI, IE, PT	4
Missing an "English" value in Metadata	AM, FR, JP, UK	4
mdui:Logo has wrong value	BE	1
Signature using an Empty Reference	CO, FR, UG	3
validaUntil is less than 5 or greater than 28 from creationInstant	CO, IL, IT	3
creationInstant wrong / in the future	CL, FR, HK, IR, MK, SI	6
Signature Method/Digest Weak	CL	1
Organization block / ContactPerson not found or missing tech/support	DK, GR, JP, IE, MK, SE, US	7
Not Assessed	OM	1

Some refinement of the mdui:Logo assessment is still required for the validator where the SAML Profile requires Data URL or https:// URL and for https:// URLs to be publicly accessible.

The information in this table along with eduGAIN Compliance Issues will be collated and regularly assessed at steering group meetings. There is no immediate need to make a decision on a timeline for these issues and federations will be contacted regarding their issues. Once the problem has been reduced to a small handful of federation, particularly if those federations are non-responsive then a decision will be made**.**

Best/Current Practices within eduGAIN

The outline of a Guide for Joining eduGAIN as a Federation has been developed. Discussion centred on what should be added/included in this work.

There are many SHOULD requirements that were stripped from the eduGAIN SAML Profile that could be used as the basis for this work.

There is an increasing number of groups providing advice and guidance and this in an opportunity to provide clarity, especially for new/emerging federations in this space. The existance of R&S, CoCo, SIRTFI, FIM4R, SAML2Int, REFEDS MFA needs to be consolidated into useful guidance.

Whether this covers federation or entityt practices was raised but not concluded.

Peter stated that it should be a "Good Practice Guide for Decent Interoperability".

Specifically, Key Management Practices and Incident Response was raised. Some practices have evolved over time but there is "no good reason to keep doing it this way". There is a lot of legacy in documentation and it needs to be clear that some of these practices are no longer a good thing™.

Future Voting?

Since Foodle will shutdown from 1 July 2018 there is a need to find a replacement for voting on membership (and other) issues.

The Foodle codebase is available but there is likely to be significant effort in supporting this tool. Nicole to take eduGAIN Steering Group use of Foodle forward as one use-case to justify GÉANT taking on this work. She stated that the domain (in addition to the software) was also available for any suitable home. There have been discussions with some federations on this topic.

Peter Schober suggested a range of tools that could be used for e-Voting purposes.

- A couple of possible replacement code-bases (not touching on the larger issue of who would be willing to run something like this for all of eduGAIN):
    - https://framadate.org/ - https://framagit.org/framasoft/framadate/
    - https://www.loomio.org/ - https://github.com/loomio/loomio
- If eduGAIN want to use an actual e-voting system (as opposed to a lightweight polling service), maybe https://zeus.grnet.gr/zeus/ is worth trying out
    - provided as a service by GRNET, no EOL in sight
    - free service for elections involving a low number of voters, which don't require user support

- certainly more formal than a polling service: each election to be held requires an election committee to register list of voters and produce authenticated results at the end
- option to use a SAML asserted (SP published to eduGAIN) identifier as 2FA; the first factor always being a token sent to the voter via e-mail etc.

Anass suggessted Evento from RENATER as a possible solution. This service isn't published into eduGAIN currently.

Terry Smith highlighted the AAFs need for any such tool to support R&S to ensure it is available to its IdPs without going through a committee approval process.

Update: Evento has been succesfully used in the vote of Malaysia/SIFULAN and appears to be acceptable. Additionally, FÉR updated their federation metadata management tools to support R&S for the AAF use-case.

Future meetings

The next meeting will take place on 6-9 August 2018 at APAN46 in Auckland, New Zealand and since the APAN46 programme (and the Identity & Access Management programme that surrounds it is still in flux there might be an adjustment from the initially proposed time. It will be in the Asia/Pacific timezone so some pain will be felt by the Americas and Europe.

Time is now confirmed as per the annoucement of the next meeting.

AOB and Close

Peter Schober raised the issue of a DigiCert SSO key rollover. Their SSO entry is published by ACOnet for all TCS subscribers to use and the current signing certificate in SAML metadata is set to expire, while this won't affect saml2int compliant IdPs it will impact ADFS. The current SP setup doesn't allow multiple keys in simultaneous operation. The new certificate is generated from the existing private key material and as such won't cause a problem for simpleSAMLphp instances (but these are in the minority). Peter will be annoucing the rollover on the FOG mailing list and interested parties should follow along.

The meeting closed at 13:30