2020-02-18 Baseline Expectations meeting

Attendees:

- Casper Dreef
- Pål Axelsson
- Jon Agland
- Miroslav Milinovi
- Anass CHABLI
- Alex Stuart
- Derrick Ssemanda
- Alan Buxey
- Hellen Kabuubi

Discussion items

Time	Item
5 min	Review previous meeting, open actions
15 min	'Homework' submission, view of federations of implementation of Baseline likeness
15 min	Next steps, timeline Focus areas: ■ Identity Providers ■ Service Providers ■ Federation Operators
15 min	AOB

Draft minutes

Review previous meeting, open actions

homework - Identity Providers

Alex and Jon from UKAMF have looked at the IdP requirements in Baseline. For the homework, we've looked at InCommon's IdP requirements. There are differences between InCommon and UKfed metadata requirements so it would be difficult to lift requirements directly.

Alex: IdP-04: PrivacyStatementURL only in place for 1 IdP in UKfed.
Jon: Privacy policy sometimes not publicly available.

Miro stated that the baseline should be the basis of collaboration. The eduGAIN baseline should be less strict than federation baselines.

Alan - the baseline should be no looser than the lowest federation 'tightness'

Pal: lowest level we do now is technical contacts, MDUI, etc. Might already be definded in the SAML profile.

Point 2 for IdPs "The IdP is operated with organizational-level authority": Would you trust your own systems to be used by IdPs. Is it trusted?

"The IdP is operated with organizational-level authority" - will need to work on the wording here. what about

IdPs operated by a service/3rd party - okay if it's with the authority of the organisation. SWAMID covers

this with their policy - maybe polices can be used. what about the federation federation metadata? - doesn't

yet exist but vetting could be shown in the form of flags/enums for processes followed institutions with multiple IdPs - someone of a senior enough level can get it into the federation. how to check or confirm its authorised?

"The IdP is trusted enough to be used to access the organization's own systems" - Alex - 'what about smaller colleges who have an IdP to access external SPs but not an SP of their own to use with the IdP' . perhaps re-wording or phrasing such that 'IF you had a service, would you trust/use this IdP for access? '

"Generally-accepted security practices are applied to the IdP" - still have someway to go to define federated security practices but this statement didn't have any noted contention

"Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL"

SAML2Int only requires SPs to have privacy policy URL. most were okay with SPs in this way right now

UK does not have privacy policy URL for their IdPs (well, they have for 2. so thats pretty much none) - other federation particpants think this is okay and doable...buut maybe other things like CoCoV2 etc will sort this out ?

as for other elements
'admin' - the UK treats this as the admin user who has the authority to request/change federation data and does not publish this.
technical/support contacts - looks do-able but may need to adjust the requirements to not be a single indiviuidual persons address but an address that can be receoved by one or more people or a service desk solution etc (to ensure contactability.
security contact - pre SIRTFI this could be filled but if its filled its not a statement of SIRTFI compliance (that requires the entity category too) - but most federation operators said manny of their institutions havent got their services tightly intergrated into IT security process/involvement. whats about 3rd parties who manage the service?

discussion of MDUI information - logo requirement not too bad but other fields need looking at.
only a few entities in eduGAIN appeared to not have a DisplayName - so thats a pretty solid possibility
(but in eduGAIN SAML profile its only a SHOULD - we can maybe get that to a MUST to go with this baseline?
Description etc - what about language? we can currently only recommend language of the region and English(?) as a secondary ?
URLs - problematic and will need efforts.

discussion stopped just before going into SP requirements in the baseline due to time restraints.

Next steps, timeline

AOB