Sirtfi Consultation 3, Sirtfi Identity Assurance Certification Description

https://wiki.refeds.org/display/CON/Sirtfi+Consultation%3A+Sirtfi+Identity+Assurance+Certification+Description

Attendees: Rhys Smith, Romain Wartel, Nick Roy, Licia Florio, Hannah Short

Number	Current Text / Reference	Proposer
1	Line 32 Introduces the concept of a "registrar." I believe this is a Federation Registrar, and I would like to suggest the addition of the Federation adjective. Later, in Line 62, the document makes mention of an "entity's registrar"; however, I think the meaning is intended to be Federation Registrar here as well, not a different registrar that belongs to the entity. Short of defining the term, the addition of "Federation" before registrar would help the reader know to whom the registrar reports and is responsible. If there are others who might be registrars (attribute authorities, etc) perhaps a defined term is called for to explain further who this might be and what the role is/is not.	John Krienke
Action:		
2	Line 32. Related to Sirtfi v1.0 and the attribute named on Line 47. How will versioning be handled? I imagine the committee has already discussed this. Will the federation operator be required to support new attributes whenever the spec is versioned? It might be prudent to add a brief section to this document that discusses how versioning and updates will be handled in relation to the attribute namespace.	John Krienke
Action:		
3	Line 76. I'd like to recommend that the word "membership" be replaced by the word "certification" to remain consistent with Lines 1 and 47.	John Krienke
Action:		
4	Line 78. Related to the requirement that a security contact MUST be in metadata (line 40), I have a question to consider. If an entity that is successfully tagged then later removes its security contact	John Krienke Peter Schober

	from metadata, is it the responsibility of the Federation (MUST?) to remove the Sirtfi tag from the entity? Or, is it the responsibility of the entity to notify the Federation registrar that the entity no longer complies? If the responsibility is the Federation's, this will become a requirement that our systems will need to automate against. While any kind of business process could be mandated here the presence of entity attribute and security contact person element is something that's trivial to monitor for automatically, so not something one should lose sleep over. Cf. the CoCo (GEANT Data Protection Code of Conduct for Service Providers) monitor at http://monitor.edugain.org/coco/	
Action:		

Sirtfi Qs from e.g. Eric, consider whether these should form part of FAQ page https://wiki.refeds.org/display/SIRTFI/FAQs

1) Would we would need to assert these requirements for all our systems, or just the IdP and SP related ones? My colleagues' reading of the document is that the organization must apply these practices to our services as a whole (e.g., regular patching or comprehensive incident management practices) and not just in the specific area of IdP and SP management. This concern applied to all of the OS and TR requirements, and also to several of the IR requirements.

- Gist from WG, we should find some clever wording to leave this open to the interpretation of each organisation. Some organisations seem to need a clearer message

2) Are the federation incident interactions covered intended to be limited to SAML interactions? The particular concern here was eduroam access, and whether the Incident Response requirements mean we need the capability to track the detailed activity of anyone we allow onto our networks (who authenticated at a remote site) if that guest user does something malicious to some third party application while on site at our location.

- In [IR2] and [IR3] we scope this to "organisations participating in the Sirtfi trust framework." We say nothing about the nature of the incident motivating those organizations to contact others. As to which systems or activities are sufficiently instrumented to provide good traceability, the statement "determination can only be made within each organization" as in the above question is all we can say, and remains the right answer I think. If we give more definite answers, as in X is in but Y is not, we are making de facto normative statements. If we want to make them, let's queue them up for discussion on v2 of the spec.

3) There were concerns about managing privacy.

3a) In OS5, there's little context provided about "Users...can be contacted". It seemed to imply (again to other readers) that SIRTFI partners can ask for contact information to use to interact with our users.

- should be fine to have a FAQ that makes clear that the v1 spec does not confer a right for anyone to contact an org's users except the org.

3b) Similarly, it's not clear in the incident response and tracing requirements that the information granted to SIRTFI partners can be limited, even though information provided in, e.g., SAML assertions can be. For instance, if we have a service that receives (only) ePTID for privacy reasons, can these requirements be read to imply that the SP can ask for a real name and email address or other personally identifying information as part of an incident response request?

- Perhaps we can clarify that "respond" in [IR2] only implies reciprocal contact. It does not obligate doing whatever may be requested. Further [IR3] uses "collaborate" to suggest the manner in which response is conducted, and [IR4] and [IR5] specifically acknowledge constraints on what can be communicated in a response.