Sirtfi WG google folder:

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Current/Recent Tasks

Who	What	When	Status

Older tasks are at the bottom of running Sirtfi call notes document.

List of things to consider when producing Sirtfi v2

WG members, please add to this list whenever something comes to your attention that we should not fail to take into account when thinking about v2.

1. The word “immediate” in “[OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats” can be misconstrued to mean immediate reaction is required, rather than immediate, ie, current, threats are detected.
    a. Accept - we’ll see about sharpening the wording when we do editing work on the v2 spec.
2. There have been many questions about TLP. Clarify that it pertains only to communications with other federation members, not that an existing CSRT must change its practices categorically to using TLP if they don’t do so.
    a. Clarify that TLP must be followed in federation/Sirtfi contexts (and suggested as a best practice in all security communications)
3. There have been many questions about which systems are covered by the Operational specs.
    a. The most important thing about Sirtfi is that your security contact is published and that you appropriately share info and collaborate in managing the incident. The OS specs address how much information you may have available to bring to bear on the investigation (as well as embodying a level of security protection for your federated transactions). At a minimum, the IdP and SP system components must meet OS specs and any other system components that directly affect the integrity of the federated assertions sent or received (eg, user account self-service portal for accounts used in federated transactions). Beyond that it’s a matter of organisational risk management. Consider this an area for continuous improvement? Possibly modify normative language, but definitely add some informative material discussing the issue of Sirtfi’s scope. Maybe also address

that it's not precisely "all dependencies" of IdP and SP components. Perfection can be the enemy of the good.

4. There have been many questions that indicate that the statement at the top of the normative section has not achieved its purpose. People are used to "compliance" bringing external review, believing there's no room for the organization to exercise judgment in how it complies with a security spec. They really need reinforcement that judgment is what the Sirtfi spec expressly calls for (and that in fact all other security frameworks also require it).
    a. Might discussion of Sirtfi's objectives (see notes of July 1 meeting below) help?
5. Linguistic barriers can hinder communication between parties. One suggestion is to coordinate communication through federation operators.
6. In some countries TLP may be uncommon, leading to difficulty in actually understanding and using it.
7. Mention providing examples on how federations could involve NRENs CSIRT Teams to be appointed as their security contact (w.r.t. Mandatory security contacts in metadata..)
8. Should we address federation practices, such as removing contact information and sirtfi tag from metadata if an entity fails some test, or any other "value-add" they might do? Do we want to make federation practices around sirtfi more consistent, add any obligations to fed ops, or just leave them alone? Can we even obligate federation operators since their non-compliance would presumably result in their members being unable to assert sirtfi, and moreover, the fed op is the one who must implement this consequence? Who polices the fed ops?
9. Important to specify clearly when we speak as a standardization body or we are suggesting: SIRFI adopters should be able to clearly tell what is a mandatory point and what is only highly recommended.
10. In v2 do we want to introduce a time limit in responding to an incident response request coming from another organization or eduGAIN Ops/Sec teams?
11. Going in the opposite direction, should we emphasize that what we're after is first of all good security contact info, and secondly, a best effort to assist in an incident response?
12. Shall we address third parties on whom an entity's operation depends? Eg, tell the entity party that they need to ensure that their 3rd party meets Sirtfi specs as appropriate.
13. Consider inserting an initial disclaimer/statement about the usefulness of SIRTFI (*given many comments we got mentioning "why should I trust SIRTFI if it is not audited ?"*) specifying that our R&E community has a long-lasting tradition of being trustful and used to state the truth - and the decision was made on purpose and on good basis not to foresee an audit process. Informative docs might also refer to dispute resolution processes that some federations have.
14. Specific point to be clarified among the responses we got "*Some additional IdP elements are incompatible with ADFS"* : needs clarification.
15. Do we want to do something to promote or ensure that fed ops implement processes to maintain security contact info in their entities' metadata? Cf. #8 above.

16. Structured use case when SPs or IdPs are managed and provided for customers: the security management process in this case gets additional actors involved. Similar to #12 above.
17. Should Sirtfi v2 address organisations that are not higher ed? Eg, primary schools, museums, libraries might not subject their students/patrons to an AUP, or be prohibited from keeping track of who has acknowledged an AUP.
18. Related to 17, should Sirtfi v2 address commercial providers of enterprise services in a different manner, ie, those whose market extends well beyond the R&E sector and whose higher ed customers are like any other of their enterprise customers? These service providers are only tangentially interested in R&E federation and do not depend on it, so their motivation to change their service practices only for their higher ed customers is small, and their higher ed customers' points of contact are people representing their organisations in an enterprise context, not in a specifically academic context. Like #17, at issue is AUP acknowledgement.

July 1, 2021

Attending: Tom B, Dave K, David G, Alan B, Uros S, Shannon R

Regrets: Romain, Daniella, Mario, Hannah

Agenda:

1. Further review & discussion of 101 survey responses, as needed
2. Refine List of things to consider for Sirtfi v2 (see above), deciding what to actually address in v2
3. AUP acceptance [PR2] for out-sourced providers of enterprise services
4. AOB

The WG began to discuss items on the List above, capturing essential bits of the discussion in sub-bullets (we got through 1-4). Along the way we began to articulate a prioritized list of what the Sirtfi trust framework is trying to accomplish (immediately below), wondering whether the v2 spec should include a discussion of that in hopes that it helps readers to use appropriate judgement in assessing their compliance with the framework.

Sirtfi trust framework's objectives?

1. Communicate & coordinate in federated incidents
2. Protect integrity of federated transactions
3. Have a reasonable set of data that may be pertinent to share with collaborators

Should we address concerns with legal liability some readers for Sirtfi attestation may have?

Should we create an implementation guide or checklist? This might help to address questions of scope.

Should the WG assemble a focus group to work through some of these questions?