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.
    a. Do we (Sirtfi WG) really want to give guidance on this?
    b. *Maybe point out that English isn't required as the only language used in IR communications*.
    c. Incident responders will figure this out when it arises without Sirtfi needing to identify a solution in advance. More important is to actually communicate in some language.
    d. Consider enhancing the IR Handbook accordingly?
6. In some countries TLP may be uncommon, leading to difficulty in actually understanding and using it. 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).
    a. Give a brief recitation of what it means within the spec (informative section), in addition to a link to the FIRST definition (in a normative section). Is there a TLP tutorial somewhere in the world that we might mention in informative material?
    b. https://www.first.org/tlp/
7. 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?
    a. Should FOs be required to assure accuracy of security contacts of their entities?
    b. Should FOs be required to have a process by which anyone's concerns about the Sirtfi status of one of their entities can be investigated and resolved?
    c. Don't force FOs to play the bad cop.
    d. Consider a best practice encouraging FOs to be supportive of their members' uptake of Sirtfi in some specific ways.
    e. *Let's wait for an actual issue to arise rather than overly prepare for one ("procrastination for the win!").*
    f. *This is really a Baseline Expectations issue for FOs.*
    g. *Revisit this one next time.*

8. Important to specify clearly when we speak as a standardization body or we are suggesting: SIRTFI adopters should be able to clearly tell what is a mandatory point and what is only highly recommended.
    a. *Agree, understood, will do.*
9. 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?
    a. IR Handbook says “1 local working day”. A simple acknowledgement suffices.
    b. Consider incorporating the IR Handbook into the v2 spec.
    c. OTOH, we want v2 to be stable and IR procedures to evolve in response to circumstances.
    d. *We want v2 to complement existing procedures, not supersede any. So no statement on response time limits.*
10. 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?
    a. *Consider adding informative material to v2 either before the normative stuff or after (or both), that steps back and informs what this is all intended to accomplish. Cf. #18 below.*
11. 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.
    a. *Yes, that’s what is intended, so amend normative text to say so.*
12. 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.
    a. *Federations embody trust as their main value. Entities trust each other based on federation and federation member policies and procedures.*
    b. Sirtfi objectives (cf #18) are served best by self-attestation. External audit is a significant impediment.
    c. *Should fed ops be asked to do something when an entity is given the sirtfi attribute? Eg: send a confirmation message to security and other contacts for the entity/org as a check against the entity operator “checking the sirtfi box” out of convenience, without regard to meeting the specs.*
13. Specific point to be clarified among the responses we got “*Some additional IdP elements are incompatible with ADFS”* : needs clarification.
    a. Might the commenter mean that ADFS can’t digest metadata that has a security contact or a Sirtfi entity attribute?
    b. *Check with Pal or Chris about the ADFS Toolkit - does it massage metadata to make it palatable to ADFS? Revisit after we learn the answer.*
    c. Depending on answer to (b), consider adding informative text suggesting that IdP’s implemented using ADFS use the ADFS Toolkit to pre-process federation metadata.

14. 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. #7 above.
    a. Does BE require this? Of FOs or of Members? Only Members know the contact.
    b. Feds might be responsible for dealing with an issue if it comes to light that a particular security contact might not be accurate.
    c. How about Feds having a process to address any concern expressed about the accuracy of a member's security contact? Prerequisite is for Fed to have a policy requiring members maintain accurate metadata, or similar.
    d. This seems more of a Baseline matter, or better approached in that way.
15. 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.
    a. Be explicit in v2 that you're still responsible even when you hire someone else to operate it.
    b. Or leave things alone in v2 itself because it is already clear enough.
    c. Add an FAQ item about this.
16. 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.
    a. Indeed the current spec presumes users are adults at an organisation that can enforce its policies on them. SPs can because they control user access. IdPs might have a problem with users who are minors or when there is no contractual relationship between users and themselves, eg, library or museum.
    b. *Change the Sirtfi specs [PR1] and [PR2] to focus on what the attesting org must be able to do, ie, manage something about a user's account, rather than specifying how they do so, ie, by having an ability to enforce a policy on the user. Put the other way around, if they believe they cannot manage the user account, then they can't attest to Sirtfi. Possible [PR1'] text: "Org can take administrative unilateral steps in managing a user's account in connection with responding to a security incident."*
17. Related to 16, 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 #16, at issue is AUP acknowledgement.
    a. The change suggested in 16.b will work here too.

The following questions arose during WG discussion of the above and are captured here to avoid having to rummage around in meeting minutes to find them:

18. Should we enumerate the Sirtfi trust framework's objectives in v2, and if so, are these the right ones?
    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
19. Should we address concerns with legal liability for Sirtfi attestation some readers may have?
20. Should we create an implementation guide or checklist? This might help to address questions of scope.
21. Should the WG assemble a focus group to work through some of these questions?

August 12, 2021

Attending: Tom, Daniela, Shannon, Alan B

Regrets: Dave K, Romain, Sven, Mario

Agenda:

1. Aug 26 meeting logistics
2. Continue refining List of things to consider for Sirtfi v2 (see above), deciding what to actually address in v2, starting with #14.
3. AOB

We got through question #17, with consensus positions in italics.