

Sirtfi WG google folder:

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDalbqju40hOhUR

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.
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.
3. There have been many questions about which systems are covered by the Operational specs.
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).
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?

9. Important to specify clearly when we speak as 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. 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.
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.
13. Specific point to be clarified among the responses we got " *Some additional IdP elements are incompatible with ADFS*" : needs clarification
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.
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.
16. Most respondents see favourably requiring an organization to proactively notify other orgs - in case they have evidence of a security incident involving/impacting them too.

June 3, 2021

Attending: Dave K, Shannon, Tom, Sven, Daniel K, Mario R

Regrets: Hannah, Romain, Uros, Alan, Pål, Daniela, David C

Agenda:

1. Review & discuss 101 [survey responses](#)
2. AUP acceptance [PR2] for out-sourced providers of enterprise services
3. AOB

The smaller-than-usual group spent the hour reviewing survey responses, noting many items added to the list above.