Sirtfi and SURFconext

Summary

SURFconext's contact points regarding security incidents (per the Security Incident Response Trust Framework for Federated Identity (Sirtfi)):

- For all our **IdPs**, SURFnet's incident response team **SURFcert** is willing to function at the first point of contact.
    - If you have an incident involving a SURFconext IdP, please refer to https://cert.surfnet.nl for contact details, including the 24/7 phone number for emergencies.
- For SPs, we will republish the Sirtfi information they supply in their metadata (if any).
    - If you have an incident with a SURFconext SP that does not publish Sirtfi information and no other usable information is available, the SURFconext team (support@surfconext.nl) may be of assistance.
    - For services offered by SURFnet or one of its constituents, also SURFcert can be of assistance.

You may also want to review SURF's Responsible Disclosure policy.

Background

The Security Incident Response Trust Framework for Federated Identity (Sirtfi - spreek uit "cert'fy") is a REFEDS project which aims to publish incident response contact information for entities and have entities assert compliance with some basic incident response norms.

Technically, Sirtfi specifies two metadata elements:

- A new ContactPerson type "security" which lists the point of contact for incidents;
- A new EntityAttribute that asserts compliance with the Sirtfi framework norms.

General considerations

Incident response is of course nothing new to SURFnet and SURFconext is in this regard largely "yet another service". SURFcert deals with a large volume of incidents daily which include incidents very comparable to those that could affect SURFconext, e.g. "mail account x has been compromised and is sending phishing emails" or "eduroam account y sends suspicious traffic, please investigate". SURFcert has experience, procedures, contacts and systems in place to receive and handle incidents 24x7, register and follow up on them, and escalate when there are problems. We seek to re-use as much of that as possible. When specific knowledge of SURFconext is needed, SURFcert will liase with the SURFconext team.

SURFconext as a hub-and-spoke federation has centralised knowledge of who logged into what when (audit log). Normally IdP's will also log this. However, based on the incident, SURFconext's exclusive knowledge may be required to resolve an incident: if an opaque nameid is used, or if the reported incident refers to EngineBlock as the IdP.

Of course all incident handling and disclosure of information to other parties (if any) will be handled in accordance to SURFnet policy.

Sirtfi for IdPs

From the view of SP's, all logins for IdP's in our federation run through SURFconext; also SURFconext may filter or augment the outgoing data. Therefore it makes sense to make SURFnet the primary point of contact for questions about logins originating from SURFconext on an SP. SURFcert is SURFnet's 24/7 incident response team. Therefore we will publish SURFcert as the security contact for all our IdP's in the (eduGAIN) metadata we produce.

SURFcert can register the incident and follow up with surfconext-beheer and/or affected IdPs via their registered Security Entry Point (SEP). We assume that an institution's existing SEP will be or should be made able to handle/appropriate redirect IdP related incidents. This will be communicated explicitly upon adoption of this Sirtfi policy. SURFcert will have documentation about basic workings of the federations and contact- and escalation points for surfconext-beheer. Actually received incidents will be used as input on whether additional procedures or tools are needed for federation specific incidents.

As for the compliance assertion: SURFconext in combination with SURFcert complies with the points in the framework. Individual IdPs are already required to comply with those or equal rules through the SURFnet Aansluitovereenkomst and/or the SURFconext Addendum IX. Institutions that do not provide adequate incident response are routinely escalated to account advisers to resolve this problem. In our constellation we feel confident that we can publish compliance with Sirtfi for each of our IdPs.

Given the above there's no need for IdPs in SURFconext to add Sirtfi information to their metadata themselves if they only interface with SURFconext. If an IdP does so regardless, we should probably check with them what the expectations are and how to handle this: is it only for other connections this IdP has, or if they want to override SURFconext's info for some reason.

Sirtfi for SPs

For "incoming" SPs that our IdPs use via eduGAIN we can look up the relevant Sirtfi information in eduGAIN metadata when we need it. It will be made available though the SURFconext Dashboard to IdP administrators in the future. It does not currently seem opportune for us to reject SPs without Sirtfi.

"Outgoing" SPs that SURFnet publishes (in eduGAIN) should be handled individually. A commercial SP like Edugroepen should probably list its own direct contact information and check compliance with the framework. SPs that are run by SURFnet itself may similarly decide on what the most appropriate contact point is. We can republish such information from the SPs metadata feed.