


Consultation: Sirtfi v2

 This consultation is now closed (5 April 2022 at 17:00 UTC and closes on 3 May 2022 at 17:00 UTC).


Background

Sirtfi is the Security Incident Response Trust Framework for Federated Identity. For background information on Sirtfi please visit the [Sirtfi Homepage](#).

Overview

The Sirtfi working group has developed a new version of the SIRTFI framework. Sirtfi v2 incorporates editorial clarifications that result in renumbering some of the v1 assertions as well as a new assertion that requires security contacts of entities participating in Sirtfi to be notified when a security incident investigation suggests that those entities are involved in the incident.

Included as supporting material is a [document](#) that clarifies the co-existence of Sirtfi v1 and v2.

 The [PDF](#) for the consultation is available. All comments should be made on: consultations@lists.refeds.org or added to the changelog below. Comments posted to other channels will not be included in the consultation review.

Change Log

comment #	Line /Reference #	Proposed Change or Query	Proposer / Affiliation	Action / Decision (please leave blank)
1	233-241	Since SIRTFI v2 is a superset of v1, listing an attestation of compliance with v1 as part of the requirements is superfluous and these lines should be removed	Nicole Roy	To avoid some metadata processing complexity by relying parties and to ease migration between versions, the working group decided to explicitly ensure the presence of the Sirtfi (v1) Attribute in an entity's metadata whenever the Sirtfi v2 Attribute is present, reflecting the fact that v2 is a superset of v1. Text was added to the Syntax section explaining why this is the specified practice.
2	0-n	Is a diff between the v1 and v2 specifications available? Not only useful for the consultation but probably also later for existing implementers of v1.	Thijs Kinkhorst	Great suggestion, and also a version history is a new requirement of the REFEDS approach to specification versioning . A complete version history was added to the specification.
3	285	The reference to the REFEDS metadata extension appears to be wrong per the XML Schema Definition (Metadata Extension Schema): the namespace URI in the example is "https://refeds.org/metadata" instead of "http://refeds.org/metadata".	Davide Vaghetti	Good catch! This was fixed in the spec and will also be reflected in updated guidance documents being prepared for publication along with v2.
4	129 - 135	<p>The coordinating CSIRT needs to be aware of incidents affecting/involving eduGAIN entities, otherwise it will get very difficult to coordinate any concerted response.</p> <p>[IR3] Notify security contacts of the eduGAIN CSIRT and entities participating in Sirtfi when a security incident investigation suggests that those entities are involved in the incident. Notification should also follow the security procedures of any federations to which your organisation belongs.</p>	Sven Gabriel	The working group discussed this with Sven. We agreed that this concern is better addressed as guidance rather than normative text because not all federated entities belong to eduGAIN, and some will have other coordinating CSIRTs they are obligated to notify. A better place to do this is at eduGAIN, and the eduGAIN Futures WG has this in their draft report already.