Securing Research and Education

A Security Incident Response Procedure for Identity Interfederation

Recent work by AARC proposes security incident response procedures for identity federations and interfederation. They are based upon the Sirtfi framework, the research and education federations' response to the need for coordinated security incident response. The procedures recognise the necessity of establishing a central unit to provide security incident support at the interfederation level, and leveraging existing intrafederation relationships to address security incidents local to a single federation.

Sirtfi, the Security Incident Response Trust Framework for Federated Identity, lists 16 statements that must be asserted by an entity to become Sirtfi-Compliant. Sirtfi enables trusted communication between security-conscious federation participants.

Compliance is expressed in federation metadata. In May 2017, 14 national identity federations are publishing Sirtfi-compliant entities.