Securing Research and Education

A Security Incident Response Procedure for Identity Interfederation

2017 International Symposium on Grids and Clouds
5-10 March 2017
Academia Sinica, Taipei, Taiwan

Trusted Communication

- [IR1] Provide security incident response contact information

```
<md:ContactPerson xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      contactType="other"
      remd:contactType="http://refeds.org/metadata/contactType/security"
      xmlns:remd="http://refeds.org/metadata">
  <md:GivenName>Security Response Team</md:GivenName>
  <md:EmailAddress>mailto:security@xxxxxxxxxxxxxx</md:EmailAddress>
</md:ContactPerson>
```

- [IR5] Respect user privacy
- [IR6] Use the Traffic Light Protocol information disclosure policy

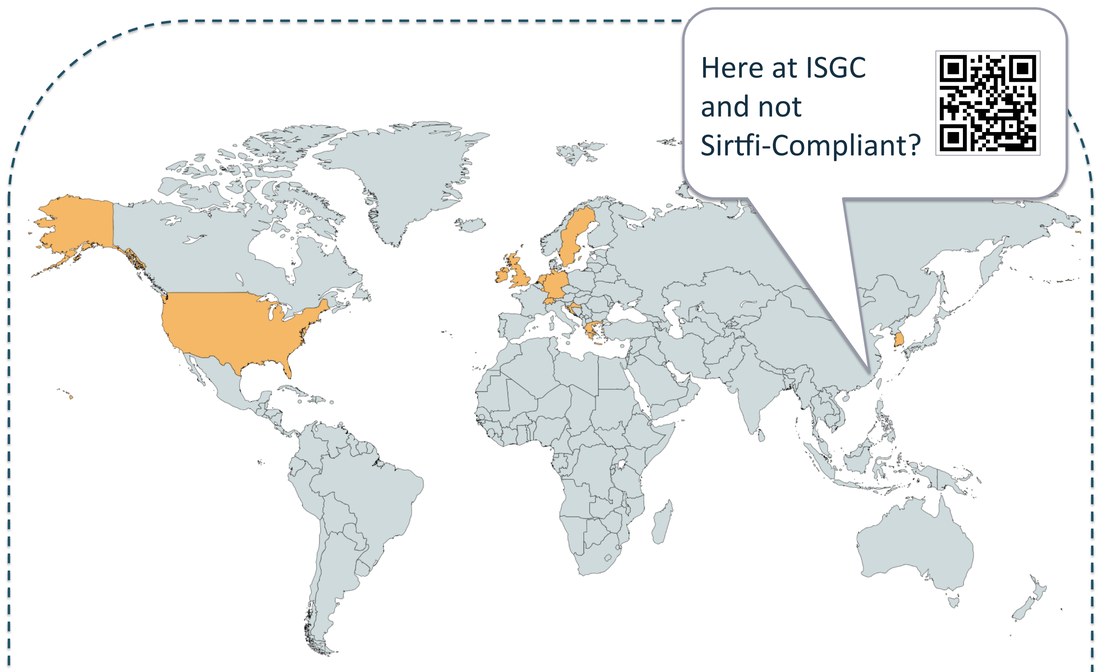
Guaranteed Collaboration

- [IR2] Respond to requests for assistance in a timely manner
- [IR3] Be able and willing to collaborate in the management of a security incident

Operational Security

- [OS1] Apply security patches
- [OS2] Manage software vulnerabilities [OS4] Be able to suspend access rights

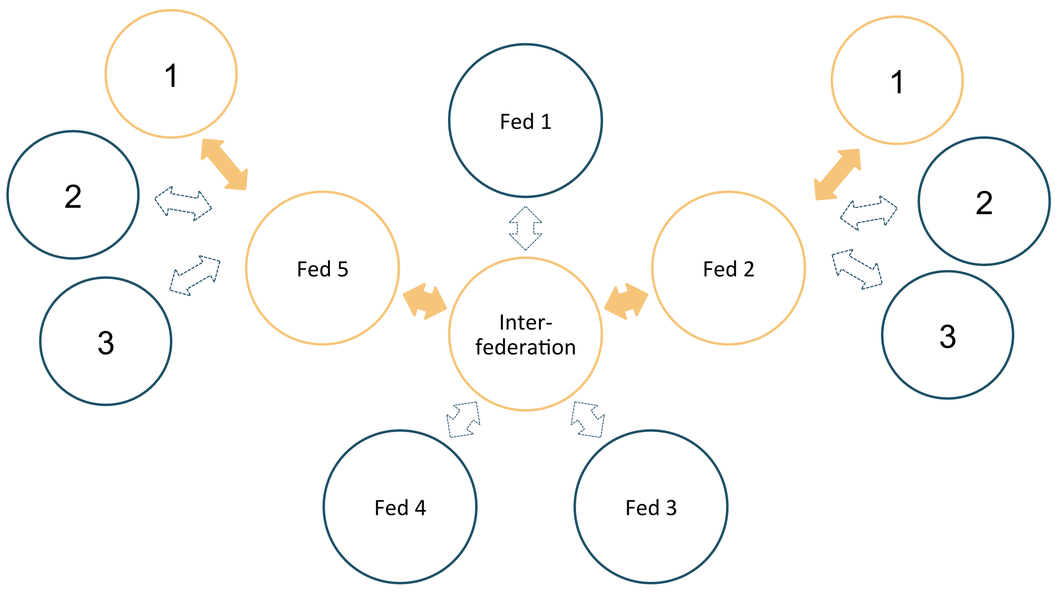
SIRTFI
Security Incident Response Trust Framework for Federated Identity



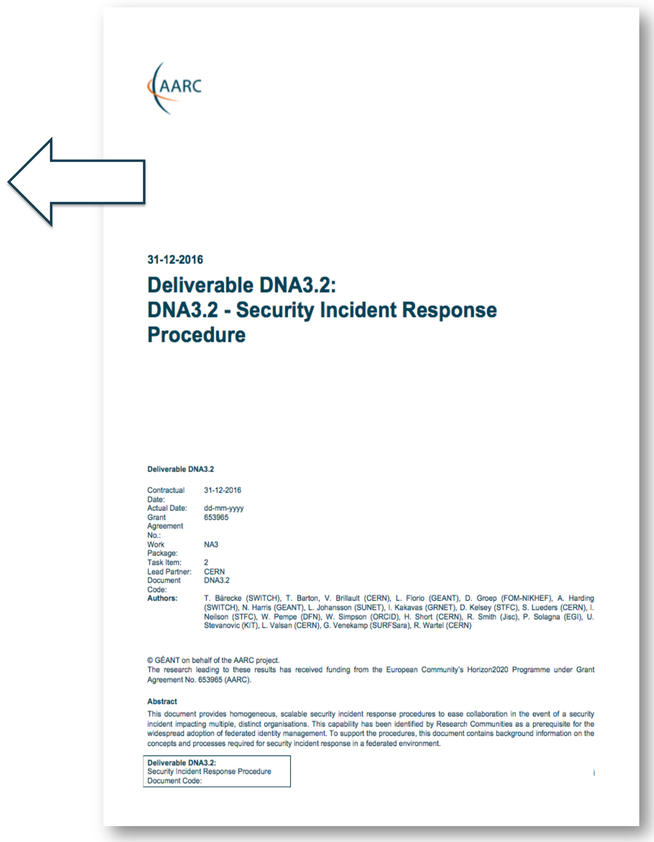
Sirtfi, the Security Incident Response Trust Framework for Federated Identity, lists 16 statements that must be asserted by an entity to become Sirtfi-Compliant. Sirtfi enables trusted communication between security-conscious federation participants.

Compliance is expressed in federation metadata. In February 2017, 12 national identity federations are publishing Sirtfi-compliant entities.

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.



During an interfederation security incident, it is expected that communication will include federation and interfederation operators. This preserves the trust fabric of identity federations and leverages the existing relationships within their constituencies.



AARC

31-12-2016

Deliverable DNA3.2:
DNA3.2 - Security Incident Response Procedure

Deliverable DNA3.2

Contractual Date:	31-12-2016
Actual Date:	dd-mm-yyyy
Grant Agreement No.:	653965
Work Package:	NA3
Task Item:	2
Lead Partner:	CERN
Document Code:	DNA3.2
Authors:	T. Bärecke (SWITCH), T. Barton, V. Brillault (CERN), L. Florio (GEANT), D. Groep (FOM-NIKHEF), A. Harding (SWITCH), N. Harris (GEANT), L. Johansson (SUNET), I. Kakavas (GRNET), D. Kelsey (STFC), S. Lueders (CERN), I. Neilson (STFC), W. Pempe (DFN), W. Simpson (ORCID), H. Short (CERN), R. Smith (Jisc), P. Solagna (EGI), U. Stevanovic (KIT), L. Valsan (CERN), G. Venekamp (SURFSara), R. Wartel (CERN)

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document provides homogeneous, scalable security incident response procedures to ease collaboration in the event of a security incident impacting multiple, distinct organisations. This capability has been identified by Research Communities as a prerequisite for the widespread adoption of federated identity management. To support the procedures, this document contains background information on the concepts and processes required for security incident response in a federated environment.

Deliverable DNA3.2:
Security Incident Response Procedure
Document Code:

Report

- Report the incident to the federation security contact
- Ensure affected participants receive a heads-up

Resolve

- Appoint Incident Response Coordinators
- Retain evidence
- Share information as often as necessary
- Investigate and resolve

Reflect

- Share incident reports with all Sirtfi Compliant participants
- Update procedures and policy

View the AARC proposal

SIRTFI Security Incident Response Trust Framework for Federated Identity

AARC

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965, **AARC** (Authentication and Authorisation for Research and Collaboration). Credit is due to members of the REFEDS Sirtfi Working Group in addition to the AARC NA3.2 task contributors.

REFEDS

CERN

Authors: H Short (CERN), R Wartel (CERN), *T. Bärecke (SWITCH), T. Barton (U. Chicago), V. Brillault (CERN), L. Florio (GEANT), D. Groep (FOM-NIKHEF), A. Harding (SWITCH), N. Harris (GEANT), L. Johansson (SUNET), I. Kakavas (GRNET), D. Kelsey (STFC), S. Lueders (CERN), I. Neilson (STFC), W. Pempe (DFN), W. Simpson (ORCID), H. Short (CERN), R. Smith (Jisc), P. Solagna (EGI), U. Stevanovic (KIT), L. Valsan (CERN), G. Venekamp (SURFSara)*