Guide to Federated Security Incident Response for Research Collaboration

Publication Date	2019-03-22
Authors:	Hannah Short;David Groep;AARC NA3
Document Code:	AARC-I051
DOI:	
Grant Agreement No.:	730941
Lead Partner:	CERN, Nikhef

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

This guide collects the experience from the controlled, or 'mock', security incident response exercises performed as part of the AARC project. These exercises built on the prepared base of Sirtfi-compliance entities registered with eduGAIN and within research and collaborative Infrastructures, and used a – still evolving – set of notification and communications procedures to mitigate and resolve the (mock) incident. By documenting the steps needed to prepare for federated response, the evolving recommendations on how to act during the resolution of an incident, and how to report about an incident, we aim to capture the experience from the mock exercises and provide a basis for continued evolution of these procedures in the REFEDS Sirtfi working group.

Table of Contents

1. Introduction

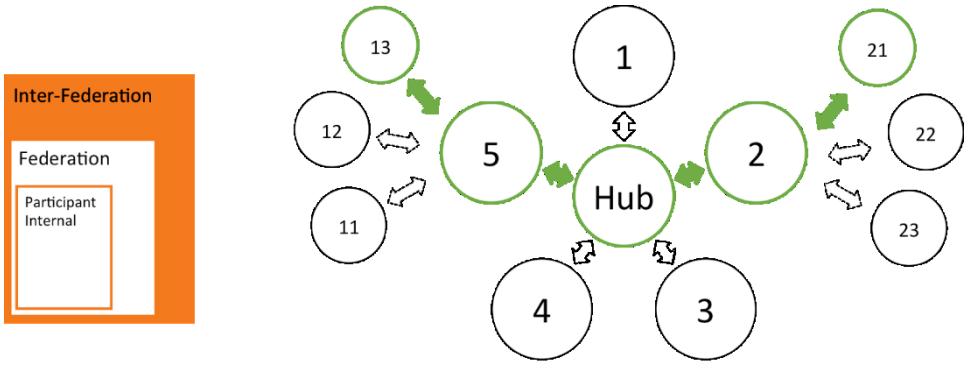
Unlike traditional distributed infrastructures, interfederation with eduGAIN was intended to only offer the appropriate levels of support required of a metadata distribution service. The need for a central security incident response coordination capability has become apparent with the wider participation of high-usage service providers. As the “eduGAIN” brand has become identified with interfederation in the eyes of international service providers, identity providers and users, there is an expectation that eduGAIN themselves will address security incidents at the interfederation level. If this is not the case, service providers may lose faith in eduGAIN as a whole. A subset of the federations interconnected by eduGAIN have developed mature support offerings in this area, whilst others have not, leading to highly heterogeneous coverage in terms of the level of incident response.

The interfederation of national federations is, by definition, international. European and international data protection laws carry significant liability for the data controller, which could discourage federation operators and participants from releasing personal data during authentication or service use. To allow security incident response communication to contain personal data, a clause is typically added into an organisation’s data protection policy to make its approval explicit [AARC-G016]. Ensuring that each federation participant has an equivalent clause is a further challenge for security incident response in federations. Finding a scalable solution to enable data sharing for security incident response requires further research.

This guide collects the experience from the controlled, or ‘mock’, security incident response exercises performed as part of the AARC project. These exercises built on the prepared base of Sirtfi-compliance entities registered with eduGAIN and within research and collaborative Infrastructures, and used a – still evolving – set of notification and communications procedures to mitigate and resolve the (mock) incident.

By documenting the steps needed to prepare for federated response, the evolving recommendations on how to act during the resolution of an incident, and how to report about an incident, we aim to capture the experience from the mock exercises and provide a basis for continued evolution of these procedures in the REFEDS Sirtfi working group.

2. Be prepared



Inter-Federation Incident Response Communication

2.1. Federated Entities Should Support Sirtfi

The need for a Security Incident Response Trust Framework for Federated Identity (Sirtfi) was identified in the 2013 paper "A Trust Framework for Security Collaboration among Infrastructures" [SCI]. The Sirtfi Working Group was subsequently established within REFEDS to consolidate the framework requirements. With the support of AARC, version 1.0 of Sirtfi was published via REFEDS in January 2016 after successful community consultation [SIRTFI]. Sirtfi has been accepted by the Internet Assigned Numbers Authority [IANA] as a recognised assurance profile. Following the approval of a normative description in November 2016 [DESC], REFEDS recommends Sirtfi for deployment use in production environments. As of March 2019, 28 national federations support Sirtfi [TECH-EDUGAIN].

This work is considered suitable for recommendation by the AARC project due to the wide approval for the framework gathered via multiple community consultations and forms the basis of the generic security incident response procedure.

Compliance with Sirtfi is expressed in federation metadata, which gives a transparent view of those organisations willing and able to engage in security incident response. Sirtfi provides the necessary trust framework for confidential communication between multiple participants involved during a federated security incident. This trusted communication, as we have seen in the previous section, is essential for information flow. The framework provides three key benefits for all participants:

1. Security contact information for each participant
2. Guarantee of a baseline of operational security capability
3. Guarantee of confidential, reciprocal collaboration during a security incident

Federated Entities should adopt Sirtfi, both by complying with the framework and by publishing their compliance and security contact.

2.2. Research Community Proxies Should Adopt Interoperable Security Policies and Procedures

Research Communities operating an AARC BPA compliant proxy should adopt the relevant Security Policies, as highlighted by the Policy Development Kit [PDK]. This is not only to aid governance within the Research Community, but also to facilitate interoperability.

2.3. Identity Federations and Interfederations Should Adopt Common Incident Response Procedures

Security Incident Response Procedures were developed for Federation Participants, Federation Operators and Interfederation Operators during the initial AARC project [AARC DNA3.2]. It is recommended that these procedures be verified, enhanced if necessary and adopted by Federations and Interfederations.

These procedures cannot be adopted in isolation by federations, SPs or IdPs, due to a reliance on support contacts at both the federation and interfederation level. Procedure adoption should be driven by eduGAIN (currently the only large scale Interfederation) agreeing to offer centralised security incident response support in line with these requirements. Following that, member federations should adopt the procedure.

Meanwhile, it should be noted that the following improvements should be made to the procedures, based on experience gathered during (mock) incident response:

- Receipt of incident notification by infrastructures and eduGAIN should be added
- Communications should add setting expectations on the timeline of future communications
- It should be clarified how a party can nominate itself as Incident Coordinator, and how this information can be shared

2.4. Leverage Templated Emails during Incident Response

Templated emails support Federation Participants in sharing the relevant information and asking the right questions. Although it is anticipated that work will continue within the REFEDS Sirtfi Working Group, the basic ‘heads-up report’ template is included here as a basis for at least the essential communications and key elements that should be included in incident response reports for federation partners.

Additional templates will be developed and teams doing incident response are encouraged to review the latest information made available through the Sirtfi pages.

2.5. Establish Secure Communication Channels in Advance

A key finding during Incident Response Simulations [AARC2-DNA3.2/DNA3.1] carried out in 2018 was the need for established, secure communication channels in the event of a security incident. Such channels should allow Federation and Interfederation Operators, Federation Participants and any potential third parties to easily communicate and safely share information. Significant work is required to understand the needs for the community, and to identify and provide a solution.

3. Act: incident response processes[1]

This section contains procedures for Federation Participants, Federation Operators and Interfederation Operators during security incident response. It is assumed that Sirtfi has the support of all Federations and the compliance of all Federation Participants. Interfederation will be referred to as eduGAIN for the purposes of this document; currently eduGAIN is the only global scale, production Interfederation and the procedure defined here could be ported to other Interfederation models.

This is a proposal produced by the AARC project and it is expected that work will continue within the REFEDS Sirtfi Working Group to define sustainable incident response capabilities for interfederation.

3.1. Scope

Nothing in these procedures is meant to restrict the flow of information from a participant to other participants, or within the federations, or with external parties. If the security incident is suspected to affect parties outside the federation, the eduGAIN security contact point must be notified.

A Federation should deliver the roles and responsibilities outlined in a manner that is the most effective for their particular federation environment. This may include defining their own procedures and policies in line with those below. If the federation has not provided a Federation Security Incident Response Coordinator it is considered that they are not supporting the Incident Response [IR] assertions of Sirtfi as required by their roles and responsibilities.

Failure to comply with these procedures, including references to Sirtfi assertions, may result in the removal of the Sirtfi Identity Assurance Certification attribute from a federation participant [SIRTFI-TAG]. Each federation, or inter-federation, is expected to manage their own membership exclusion policies in line with security risks

3.2. Definitions

Federated Security Incident

A suspected or confirmed violation of an explicit or implied security policy involving multiple participants making use of federated identity management.

Security Incident Response Coordinator

The main obligation of this role is to ensure the security incident resolution process does not stall. They are responsible for understanding and resolving the ongoing security incident by

[1] This basic procedure has been taken from AARC DNA3.2 and used as the basis for the final mock exercise performed within the context of AARC.

ensuring it is contained, coordinating the response from participants, tracking the progress of the process, coordinating action, disseminating information and providing expertise and guidance. They are expected to marshal concerned federated actors to participate in the response to a security incident.
This role should be played by the entity most appropriate for the task, such as a Research Community or e-Infrastructure CSIRT, or an individual or group appointed by the federation or interfederation.

3.3. Goals

The objective of this procedure is to ensure that all security incidents are investigated as fully as possible and that participants promptly report intrusions. Security incidents must be treated as serious matters and their investigation must be resourced appropriately.

3.4. Roles and Responsibilities

3.4.1. Federation Participants

- Follow the [OS], [IR], [TR], and [PR] requirements described by Sirtfi [1]
- Publish valid security contact information in federation metadata as defined by the REFEDS Security Contact Schema [2]
- Report all security incidents posing a risk to any other federation participant within or outside their own federation, to the federation security contact point at their own federation

3.4.2. Federations

- Follow the [IR] requirements described by Sirtfi, and [OS], [TR] and [PR] as applicable [1]
- Provide a security contact point (e.g. security@federation.org) available to all federation participants, federation operators, other federations and external organisations
- Define communication channels to be used for security incident response by federation participants
- Appoint a Federation Security Incident Response Coordinator when notified about a suspected security incident. This role may be played by a federation participant or external entity, such as a Research Community or e-Infrastructure CSIRT, as appropriate.
- Ensure a unique identifier is assigned for each security incident
- Provide or source technical expertise necessary to assist federation participants (forensics, technical investigation, log analysis, etc.)

The Federation Security Incident Response Coordinator is responsible for following the Incident Response Procedure for Federation.

3.4.3. eduGAIN

Caveat: this document is written at the time when there is only one global scale, production interfederation, eduGAIN, but the procedure could be ported to similar interfederation models.

- Follow the [IR] requirements described by Sirtfi, and [OS], [TR] and [PR] as applicable [1]
- Provide a security contact point (e.g. security@edugain.org) available to all federation participants, federation operators, other federations and external organisations
- Define communication channels to be used for security incident response by federation participants and Federation Security Incident Response Coordinators.
- Appoint an eduGAIN Security Incident Response Coordinator when notified about a suspected security incident. This role may be played by a federation, federation participant or external entity as appropriate.
- Ensure a unique identifier is assigned for each security incident
- Provide or source technical expertise necessary to assist federation participants and Federation Security Incident Response Coordinators (forensics, technical investigation, log analysis, etc.)

The eduGAIN Security Incident Response Coordinator is responsible for following the "Security Incident Response Procedure for the eduGAIN Security Incident Response Coordinator".

3.5. Security Incident Response Procedures

3.5.1. Federation Participants

1. Follow security incident response procedures established for the organisation.
2. Contain the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
3. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.
4. In collaboration with the Federation Security Incident Response Coordinator, ensure all affected participants in the federation (and, if applicable, in other federations), are notified with a "heads-up" and can take action.
5. Announce suspension of service (if applicable) in accordance with federation and interfederation practices.
6. Perform appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
7. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.

8. Respond to requests for assistance from other participants involved in the security incident within one working day.
9. Take corrective action, restore access to service (if applicable) and legitimate user access.
10. In collaboration with the Federation Security Incident Response Coordinator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
11. Update documentation and procedures as necessary.

3.5.2. Federation Security Incident Response Coordinators

1. Assist federation participants in performing appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
2. Ensure all affected participants in the federation (and, if applicable, in other federations) are notified with a “heads-up” within one local working day. If other federations are affected, the eduGAIN security contact point must be notified, even if affected participants in all other federations have been contacted directly.
3. Coordinate the security incident resolution process and communication with affected participants until the security incident is resolved.
4. Ensure suspension of service (if applicable) are announced in accordance with federation and interfederation practices.
5. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
6. Assist and advise participants in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
7. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
8. Update documentation and procedures as necessary.

3.5.3. eduGAIN Security Incident Response Coordinator

1. Assist federation participants and Federation Security Incident Response Coordinator in performing appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
2. In collaboration with Federation Security Incident Response Coordinators, ensure all affected participants in all federations are notified with a “heads-up” within one local working day.
3. Coordinate the security incident resolution process and communication with affected participants until the security incident is resolved.

4. Ensure suspension of service (if applicable) is announced in accordance with federation and interfederation practices.
5. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
6. Assist and advise participants in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
7. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
8. Update documentation and procedures as necessary.

[1] https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

[2] https://refeds.org/metadata/contactType/security

[3] https://www.us-cert.gov/tlp

4. Report and share

Sharing pertinent information with federation peers should be performed regularly in accordance with the procedures above, and each communication should preferably include a mention of when the next communications will be.

Besides the basic 'heads-up' notification template provided here, additional templates might be available within your federation or Infrastructure – refer to your federation incident response information pages or the Sirtfi web site. The names of the organisations used below are for example purposes only.

```
Subject: [CERNCERT-2016-12-24] HEADS-UP: Multiple identities compromised at
 Acme Corporation [TLP:AMBER]

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Dear affected eduGAIN participants,

TLP:AMBER

## SUMMARY ##

The CERN CERT has detected multiple identities being compromised at the
Acme Corporation IdP. CERN is investigating the case and has reported the
abuse to Acme Corporation (no reply yet).
Early forensics findings highlighted several eduGAIN participants (all
recipients of this email) are likely affected and should urgently check
their security status.

This is an ongoing investigation and more details will be shared as they
become available.

## INTRUSION TIMELINE ##

2016-12-24 06:01: Will. E sends an abuse complaint to the CERN CERT.
2016-12-24 08:31: CERN CERT confirms abuse and reports it to the
                  Acme Corporation.
2016-12-24 09:40: CERN CERT discovers other affected parties.
2016-12-24 10:50: SWITCH Federation Security contact is informed and its
                  is agreed CERN CERT will act as the incident coordinator
                  for now
2016-12-24 11:34: CERN CERT sends this heads-up is sent to all Sirtfi
                  affected parties in eduGAIN
2016-12-24 11:38: CERN CERT notifies affected third parties outside of eduGAIN

## INDICATORS OF COMPROMISE

Indicators of compromised are available on the eduGAIN Security Wiki
(https://edugain.org/security/operations/)

## REPORTING & SHARING

We would be grateful if affected parties report back on their findings
to their federation security coordinator or to CERN CERT directly.
-----BEGIN PGP SIGNATURE-----
...
-----END PGP SIGNATURE-----
```

References

SIRTFI	https://refeds.org/sirtfi
AARC	https://aarc-project.eu
ISGC-2016-030	"Raising Security and Trust in our Inter-Federated World", H. Short et al, in the Proceedings of the International Symposium of Grids and Clouds 2016 (ISGC 2016), Taipei, Taiwan, March 13-18, 2016, PoS (ISGC 2016) 030
SCI	"A Trust Framework for Security Collaboration among Infrastructures", D. Kelsey et al, in the Proceedings of the International Symposium of Grids and Clouds 2013 (ISGC 2013), Taipei, Taiwan, March 17-22, 2013, PoS (ISGC 2013) 011
FIM4R	"Federated Identity Management for Research Collaborations", D Broeder *et al.*, April 23 2012, CERN-OPEN-2012-006
AARC-G016	*Recommendations on the exchange of personal data in accounting data sharing* https://aarc-project.eu/guidelines/aarc-g016
IANA	https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml
TLP	https://www.us-cert.gov/tlp
PRACE	https://www.nsc.liu.se/joint-sec-training-media/PRACE%20security%20incident%20handling.pdf
TECH-EDUGAIN	https://technical.edugain.org/entities
XSEDE-PLAYBOOK	https://www.ideals.illinois.edu/bitstream/handle/2142/50104/XSEDE%20Security%20Playbook.pdf
CONTACT	https://refeds.org/metadata/contactType/security
SIRTFI-TAG	https://refeds.org/wp-content/uploads/2016/11/Sirtfi-certification-v1.0.pdf
EGI	https://documents.egi.eu/document/2935
EDUGAIN	https://technical.edugain.org/doc/GN3-10-326%20eduGAIN_constitution%20v2.0.pdf

Glossary

AARC	Authentication and Authorisation for Research and Collaboration
REFEDS	The Research and Education FEDerations group
SIRTFI	Security Incident Response Trust Framework for Federated Identity (Sirtfi)
AAI	Authentication and Authorisation Infrastructure
SP	Service Provider
IDP	Identity Provide
CSIRT	Computer Security Incident Response Team