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.

Table of Contents

1 Executive Summary

This document proposes homogeneous, scalable security incident response procedures to ease collaboration in the event of a security incident impacting multiple organisations in a federated infrastructure. By its very nature, coordinated incident response requires collaboration between many independent entities, and this AARC work is done in close partnership with and in the context of the wider global effort, including research infrastructures, institutions, and identity federation operators. The REFEDS Sirtfi working group ("Security Incident Response Trust Framework for Federated Identity") provides the mechanism to achieve consensus and gain adoption by the communities outside of the AARC project.

The Sirtfi "version 1" specification, which achieved endorsement in 2016, provides the basic structure to communicate incident response capabilities – its scope is briefly presented in this document. The requirements identified and new operational experience extend upon Sirtfi v1 and the procedures presented here are the first attempt to produce recommendations from the AARC project that address more complex cases. It is expected also that work will continue within the REFEDS Sirtfi Working Group to refine the proposal and gain agreement and support from the community at large. Procedures are provided for the key actors in federated security incident response; Federation Participants, Federation Operators and Interfederation Operators. The goal is not to replace internal procedures that a participating organisation has already established, but to provide a shared framework to be used when a coordinated response is required between several of these actors. Such a capability was identified by Research Communities as a prerequisite for the widespread adoption of federated identity management [FIM4R].

Procedures to effectively manage response to a security incident will typically encompass handling of confidential information. Hence criteria are also defined that must be met in order that a federation actor is entitled to play one of the roles defined below. In particular, Federation Participants must comply with Sirtfi (defined below) in order to participate in security incident response processes.
To support the procedures, this document contains background information on the concepts and processes required for security incident response in a federated environment. Effective security incident response is an ongoing challenge for federations and is, as yet, only partially solved. The AARC Project recommends that further analysis be completed to identify the full set of capabilities required for achieving a sustainable security incident response capability across federations.

2 Introduction

The expanding suite of services run by Research Communities and available through identity federations exposes an inviting attack surface for malicious activity. A single compromised account provides an entry point to this global network of resources linking thousands of organisations.

The interfederation landscape, as it stands at the end of 2016, has not comprehensively defined and documented security incident response processes or designated coordinators. Currently there is no visibility into the maturity of operational security of each participant and no guarantee that they will willingly collaborate. This deliverable proposes both the necessary procedures and operational support capabilities required for effective security incident response. Although these procedures are primarily framed to support the needs of Research Communities, they are generally applicable to all federation participants.

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) is an essential foundation on which a coordinated response to security incidents can be built [SIRTFI]. This is achieved via a series of statements relating to an organisation's ability to participate effectively in security incident response. An organisation asserts compliance by agreeing to honour these statements. Sirtfi forms the guiding principles of these security incident response procedures.

The AARC Project aims to develop an authentication and authorisation framework [AARC] to guide the evolution of federated infrastructures and communities. Scalable, homogeneous procedures for security incident response are included in the project's objective to define a reusable policy package. These procedures, however, are only the starting point for a mature security incident response coverage for interfederation. The final part of this document highlights the range of capabilities required for security incident response within a distributed environment and analyses the current coverage of such capabilities. A conclusion is drawn that additional work is required to ensure that such capabilities exist and are being used within the environment.

3 Definitions

Federated Security Incident
A suspected or confirmed violation of an explicit or implied security policy involving multiple entities making use of federated identity management.

Federation
Identity federation. An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions. [EDUGAIN]

Federation Operator
The organization managing a Federation, operating the central components. [EDUGAIN]
Federation Participant
Any federation member including, but not limited to, identity providers, service providers and attribute authorities. This may include Research Community service providers, identity and service provider proxies, or e-Infrastructures that are registered as service providers in a Federation.

Interfederation
Interfederation takes place if a user authenticated by an IdP registered in one federation accesses a service that is registered in another federation.

Interfederation Operator
The organization managing an Interfederation, operating the central components

Security Incident Response Coordinator
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. 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 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.

4 Scope

The scope of this document relates to the procedures and concepts relevant to responding to Federated Security Incidents in Identity Federations and Interfederation. This document does not address security vulnerability management or processes relating to non-security incidents.

The proposed procedures should be applied during Security Incidents in which federation participants including, but not limited to, Service Providers (SPs) and Identity Providers (IdPs), from separate organisational domains are involved as a consequence of their participation in identity federations.

5 Trust Frameworks and Communication

When multiple organisations are involved in a single security incident, managed communication is needed to share information, gain a full understanding of the security incident and work towards recovery. Such communication may contain sensitive information. It is essential that recipients are trusted to maintain confidentiality and preserve the reputations of all involved.

Individual organisations traditionally are oriented to support their own users or computing resources but, in the case of distributed systems, each will rely on others for input when it is their own systems that are affected by a security incident. In the case of federations, user authentication and service information are owned by separate organisations but both will be required to fully understand the timeline of a security incident. Organisations must act beyond their immediate mandate and collaboration is paramount to gain a complete understanding of a federated security incident.

To achieve the required level of communication, i.e. communication that contains the necessary information and is responded to by the appropriate people, we define here a trust framework to establish a common set of roles and procedures to which participants appropriately adhere [ISGC-2016-030]. Such a framework provides a basis for cooperation between organisations and its consistent implementation helps establish and reinforce trust among participating individuals.

5.1 The Impact of Trust on Communication

As an example of the need for trustworthy communication, consider the situation below:

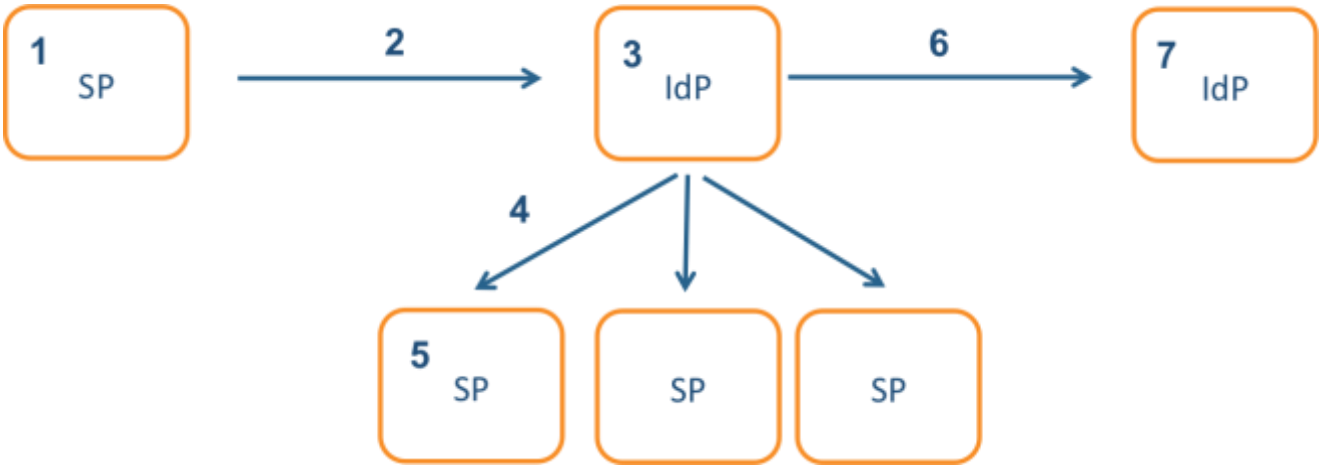


Figure 1, Incident Response Communication, expected flow

Figure 1 shows an expected workflow of a compromised Identity Provider (IdP) being identified following suspicious activity detected at a Service Provider (SP) and the subsequent security incident response communication:

1. Intrusion involving a federated identity is suspected at an SP
2. SP notifies the IdP associated with the identity

3. IdP discovers that they are fully compromised due to a software vulnerability, contains the security incident and begins recovery process
4. IdP notifies any SPs contacted by compromised identities
5. SPs begin investigation of activity performed by compromised identities
6. IdP distributes information on the security incident appropriately, alerting an additional IdP using the software that led to the compromise
7. IdP begins their own investigation

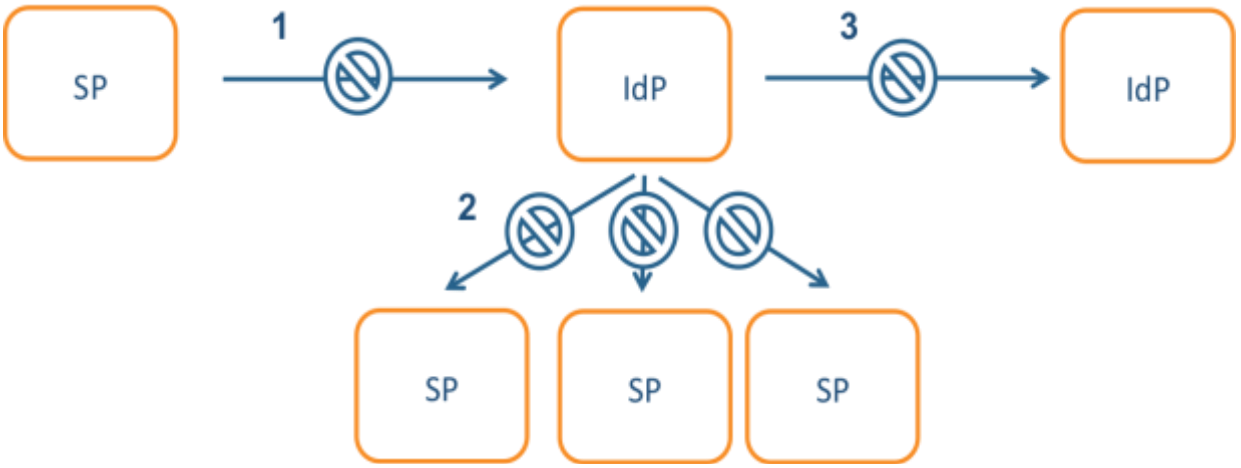


Figure 2, Incident Response Communication, communication blocks

In current practice this workflow may be broken for multiple reasons as visualised by the examples in Figure 2:

1. SP does not inform the IdP since federated identities are outside the scope of the SP's security mandate
2. IdP does not inform the affected SPs either due to fear of a leak of sensitive information and damage to their reputation or to being out of scope of their mandate
3. IdP does not alert additional IdP since there is no established channel of communication between participants

The most fundamental reason for this workflow to breakdown at any stage is the absence of a valid and up-to-date security contact for each participant. This is addressed by Sirtfi, discussed below, which also establishes basic expectations of security operations for federation participants. The trust framework defined further below extends Sirtfi by specifying analogous expectations and procedures to be followed by all federation actors, thus enabling the expected workflow in Figure 1 to occur in a consistent manner.

5.2 The Security Incident Response Trust Framework for Federated Identity

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. Sirtfi is supported by 5 national federations to date [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

6 Security Incident Response for Distributed Infrastructures

6.1 Existing Security Incident Response Structures

Although identity federations differ from the classical idea of distributed infrastructures, operational practices of such infrastructures can be used to inform procedures and draw comparisons. Traditional distributed infrastructures, such as grid infrastructures, typically recognise the importance of a unit mandated to coordinate security across the infrastructure [EGI]. It is critical that this unit is trusted and has the required skills and authority to manage the full lifecycle of a security incident. There are two primary models for establishing such a unit.

6.1.1 Fully Distributed

In the first set of infrastructures, such as PRACE [PRACE] (the Partnership for Advanced Computing in Europe) and XSEDE (the Extreme Science and Engineering Discovery Environment), each participant is represented within the security incident response unit. The participants form a ring of trust within which security incident response communication and post-incident reports are shared. This approach is well suited to infrastructures with a small number of highly skilled participants.

Assigning responsibility for resolving a particular security incident is important in a fully distributed model. At XSEDE, the initial responder (i.e. the participant at which the security incident occurs) drives the security incident response process unless the impact is widespread or could have critical impact on the infrastructure or trust fabric, in which case an XSEDE Lead is assigned [XSEDE-PLAYBOOK]. The designated individual or group plays the role of security incident response coordinator.

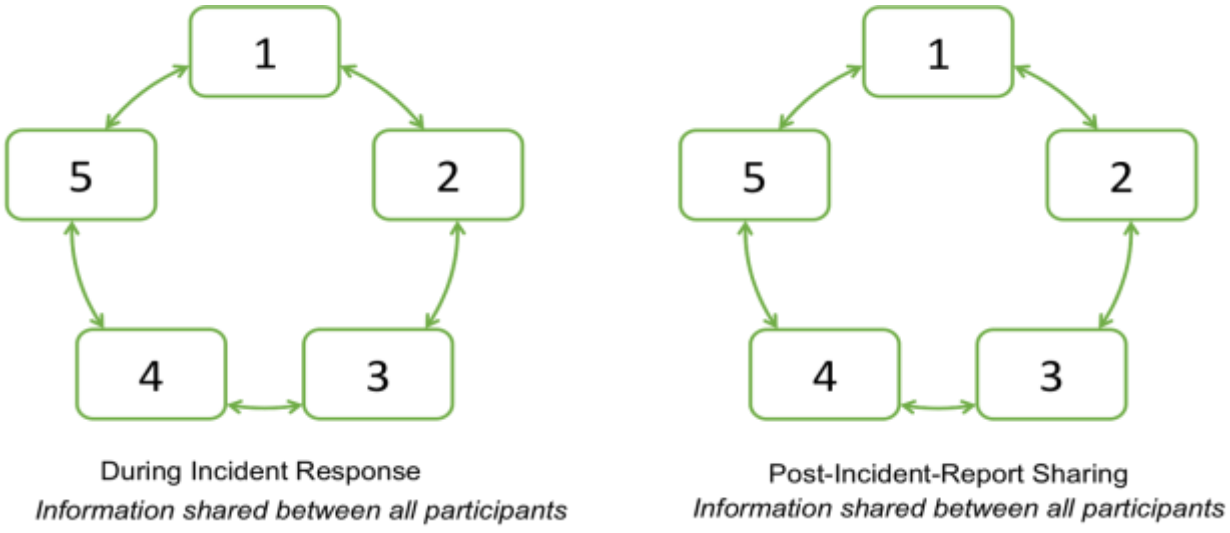


Figure 3, Information exchange for Fully Distributed Model

6.1.2 Hub & Spoke

In the second set of infrastructures, such as EGI (the European Grid Infrastructure) and OSG (the Open Science Grid), an authoritative unit is established that centralises tasks pertaining to security incident response. An individual within this unit would play the role of security incident response coordinator. Participants sponsor this unit to perform security incident response duties on their behalf. This approach is more appropriate for large infrastructures where common decisions are difficult to achieve and sharing detailed security incident response information with all participants may have less value. Targeted communication is typically sent to only the relevant parties during the security incident. A followup report of the security incident will be shared widely.

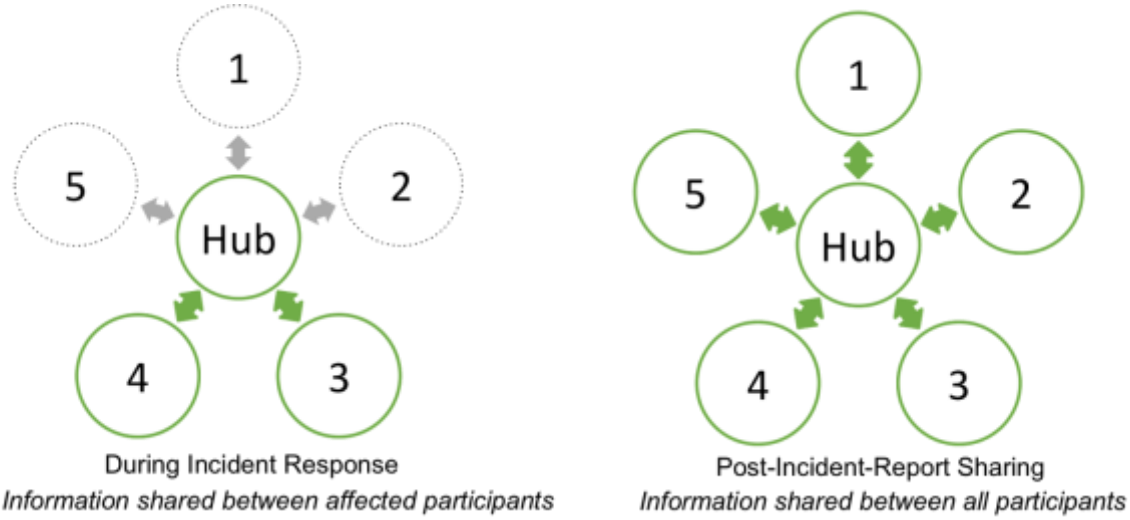


Figure 4, Information exchange for Hub & Spoke Model

6.2 Commonalities

In both models, a security incident response coordinator is identified early in the security incident response process. Likewise, a summary report of a security incident is shared with all participants. The reports are typically required within 30 days and contain a full description of the cause of the security incident, timeline of response and details of resolution. Trusted channels of communication are established and participants are held to a standard framework or policy dictating behaviour. This creates incentive for participants to act responsibly since failure to comply may result in exclusion from the infrastructure. A body exists with the authority to impose such sanctions, whether this be the security incident response coordinator or otherwise.

Much of this can be carried into federated security incident response. However, common policy and authority to hold all parties accountable does not pertain to global interfederation. This is addressed in the following sections.

7 Security Incident Response in an Identity Federation Landscape

7.1 Challenges

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, 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, despite security incidents having been contained to a limited number of entities. The trust framework defined below assigns a role and associated procedures to eduGAIN.

Some of the federations interconnected by eduGAIN likewise have not established a central security incident response capability. They too are assigned a role and associated procedures below.

The interfederation of national federations is, by definition, international. European and international data protection laws carry significant financial liability for the data controller, which discourages 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 inserted into an organisation's data protection policy to make its approval explicit [AARC-DNA3.5]. 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.

7.2 Community Consultation

Defining a procedure to be adopted by each member of the federated landscape requires buy-in from all entities affected, as well as the funding and support necessary to create sustainable processes. REFEDS provides the link between eduGAIN, national identity federations and those research communities actively involved in federated identity management. Each of these stakeholders has their own priorities when approaching security incident response but, for a procedure to be effective, they should all agree to a common framework. It is essential that a critical mass of the community demonstrate support for a shared procedure.

Sirtfi, which forms the base for the procedures defined here, has undergone several REFEDS community consultations since 2015. In December 2015, the framework itself underwent a consultation. In April 2016 a consultation was completed to define a REFEDS metadata schema for the security contact. In November 2016 a third consultation concluded on the usage of the Sirtfi Identity Assurance Certification Description, which allows entities to assert their Sirtfi compliance within their federation metadata. These three consultations afforded the opportunity for the community to become familiar with Sirtfi and agree on a common deployment method.

To move beyond the requirements proposed in the Sirtfi framework and propose concrete procedures for security incident response, the AARC project gathered insight from existing infrastructures and pooled the experience of selected experts participating in REFEDS. At this stage, the procedures have not been exposed to wide-scale consultation outside the AARC project. This is a deliberate move to allow the research communities participating in federated identity management to define a draft proposal suiting their needs. It is expected that considerable work will be required within the REFEDS community to align the generic procedure with current practices and the priorities of federation operators, campuses and further stakeholders.

7.3 Proposal

To enable an effective response to a federated or interfederated security incident, this document proposes three procedures, one for each of the key players; Federation Participants, Federation Operators and Interfederation Operators. These procedures are intended to complement each other, and any existing internal security incident response procedures adopted by the federation participants. The appropriate procedure should be triggered according to the scope of the security incident in question. Internal security incident response procedures for federation participants are outside the scope of this deliverable.

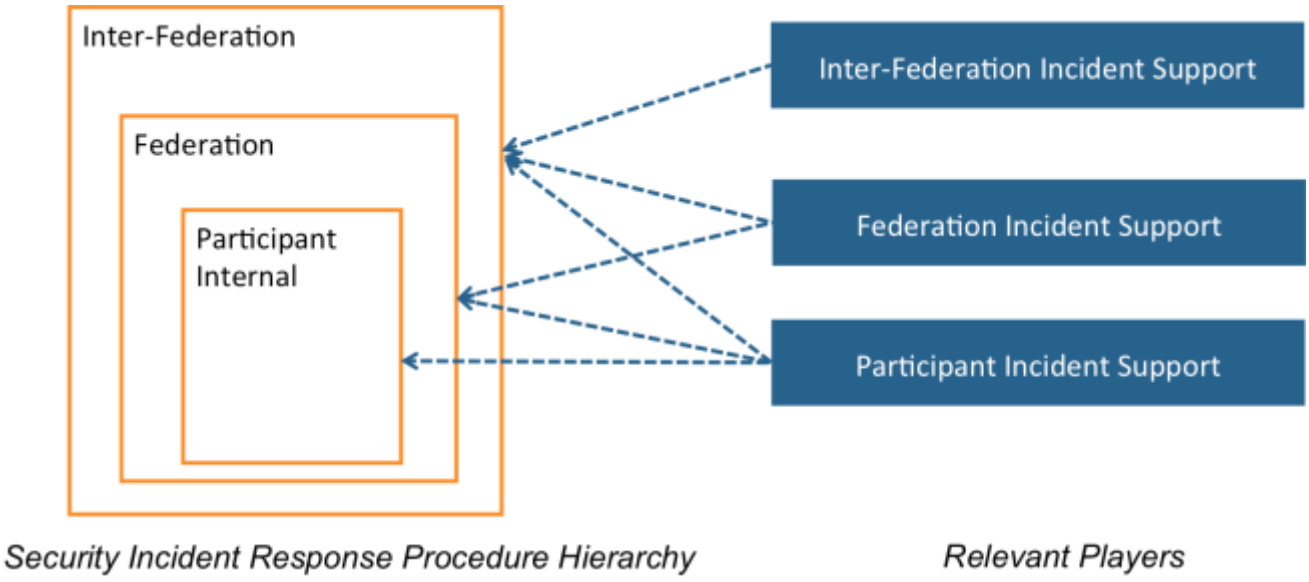
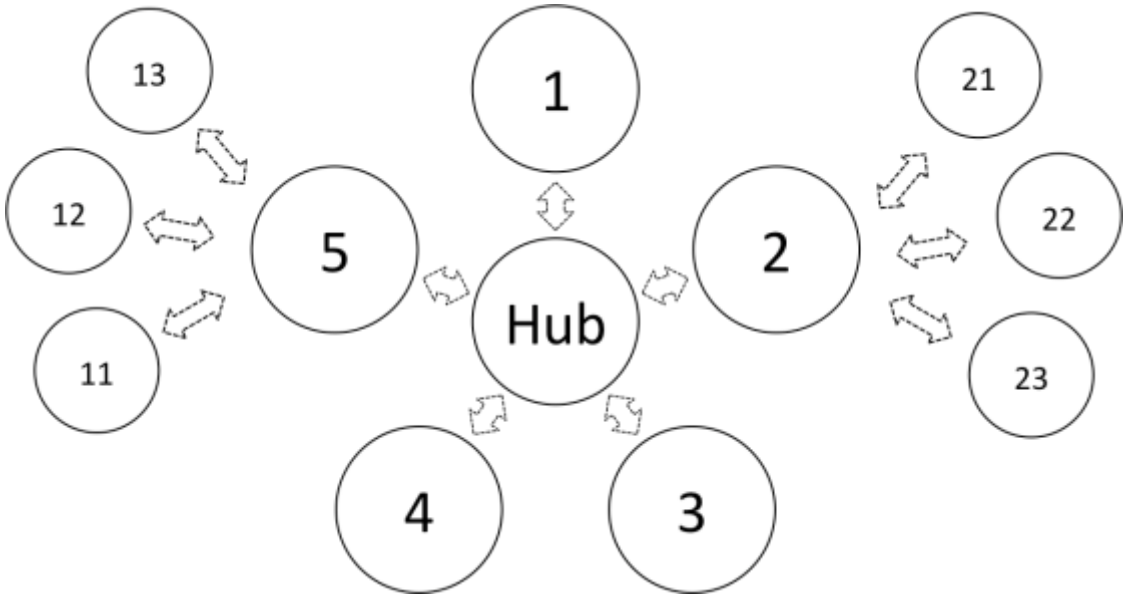


Figure 5, Procedure hierarchy and the relevant players

It is proposed that a hybrid security incident response structure be established, based on the hub and spoke pattern described above. A central support unit provides security incident response coordination at the interfederation level and relies on federation support to perform the same duties within their constituents.

Figure 6,



Proposed Incident Response Structure for Inter-Federation (only participants from Federations 2 and 5 are shown.)

Following the adoption of security incident response procedures by interfederation and federation governance, it is expected that the appropriate process be invoked for a security incident. The subsequent figures illustrate the expected communication during a federation, and interfederation event. Additional information exchange outside the contents of these schematics, e.g. between two participants from separate federations or with external entities such as software vendors, is expected and should not be prohibited; the examples here depict the minimum expected communication.

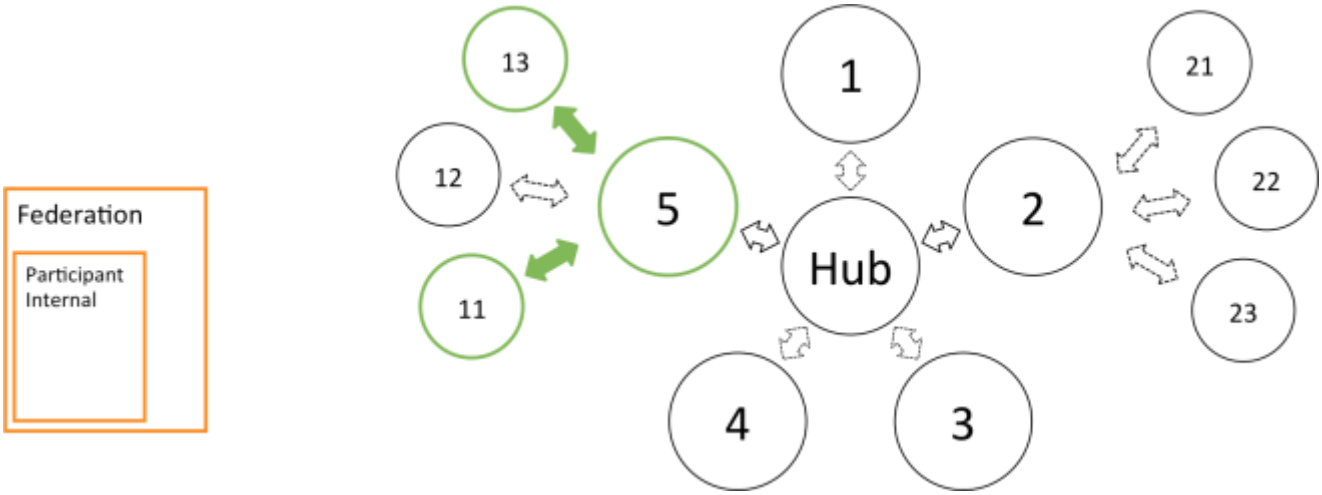


Figure 7, Federation Incident Response Communication

During a security incident contained within a single federation, communication is limited to the affected federation participants and federation itself. It is expected that the federation manage this communication.

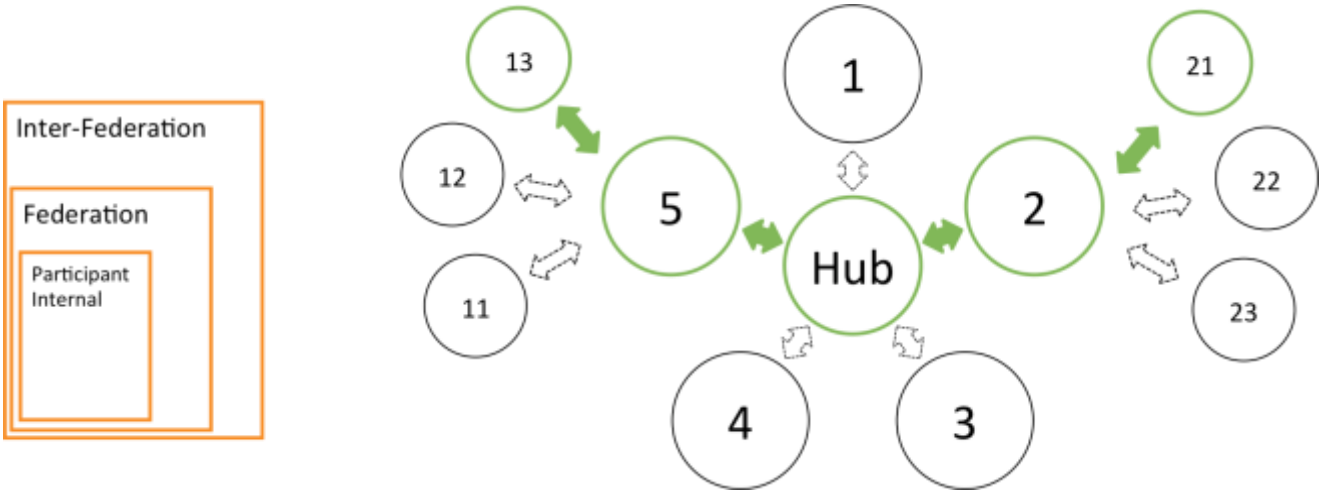


Figure 8, Inter-Federation Incident Response Communication

During a security incident impacting multiple federations, communication is extended to include interfederation, and all affected federations plus their participants. It is expected that communication is managed at the interfederation level.

These procedures have been developed to distribute responsibility for resolving a security incident across multiple federation actors. Responsibility should not rest wholly with the party that first identifies a security incident; one aim of this work is to encourage the adoption of federated identity management by more risk-averse service or identity providers.

7.4 Role of Research Communities

Distributed infrastructures, such as WLCG, EGI, OSG, PRACE, XSEDE or similar Research Infrastructures, will typically register with a federation as a service provider proxy when enabling federated identity management. From the perspective of the federation they appear as a single service provider masking the complexity of the infrastructure. The mature security incident response capabilities of these infrastructures must be leveraged during federated security incidents in order to enable them to operate and make use of federated identity management. Incident response experts from these communities may be best placed to coordinate federated security incident response and should be involved as appropriate. In addition, they may, following the principles of the Sirtfi framework, engage directly on security incident response with multiple federation participants, federations or interfederation management, operations team and security experts as commensurate with the severity of the security incident.

E-Infrastructures and Research Infrastructures should involve their own and external federations during incident response in order to leverage the pre-existing relationships established with federation participants. The procedures proposed in this document require interaction with federation and interfederation operators as a means of preserving the trust fabric of identity federations.

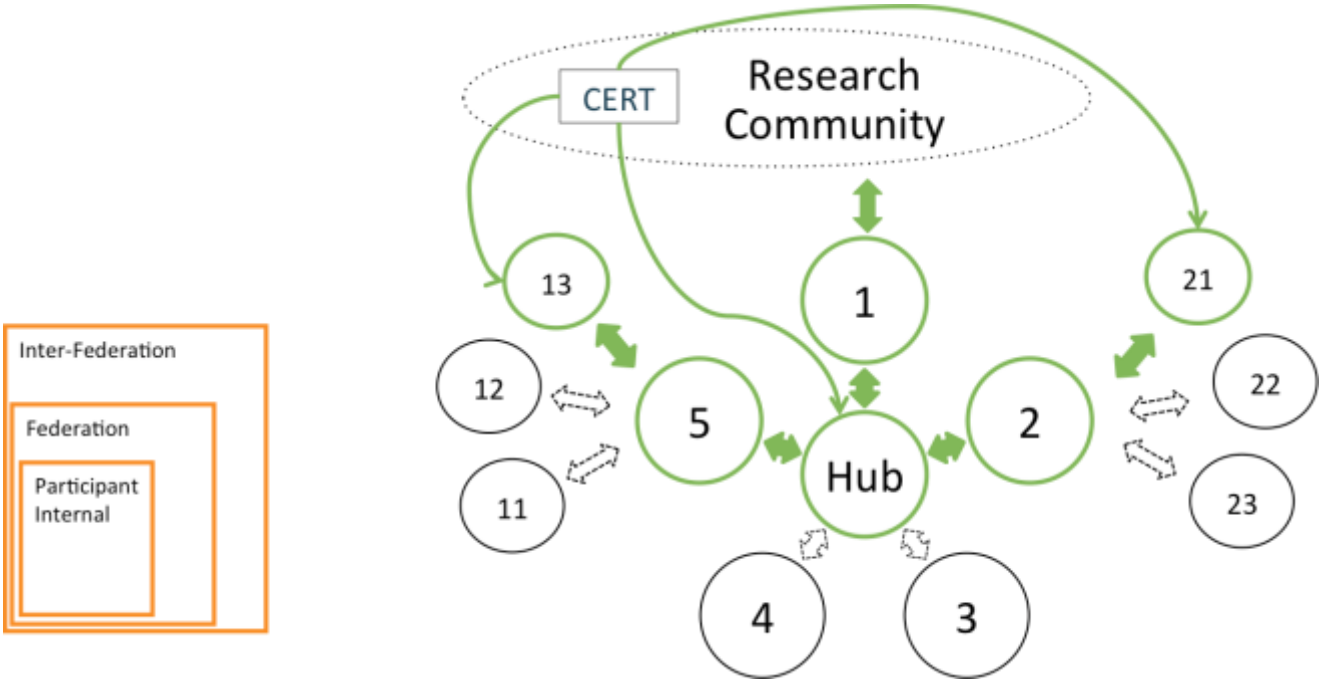


Figure 9, A Research Community (RC) Driven Incident in which the RC is registered as an SP in Federation 1. The security incident affects participants from multiple federations and external parties. The RC should follow the security incident response procedures defined in this document in parallel to their own to ensure that all necessary parties are informed. Communication with inter-federation and federation representatives is expected. RCs should be encouraged to fill the security incident response coordinator role where appropriate.

8 Conclusions and Next Steps

In Appendix A this AARC deliverable presents a description of the roles, responsibilities and proposed procedures required for security incident response in federations. The authors conclude that a layered approach to federated security incident response is necessary, requiring participants, federations and interfederation representatives to collaborate.

Until such time as a central unit has been established, and identity federations have formalised their internal procedures, it is anticipated that research communities and high usage service providers will drive security incident response as they are identified.

It is expected that this work will be continued by the REFEDS Sirtfi Working Group to extend and mature the procedures, concretely define the tools required to support security incident response and to aid individual federations in formulating their own incident response procedures in line with those proposed. An extended discussion is needed to agree on appropriate actions for the community to follow during the interim in which a federation does not have procedures in place. In parallel, AARC2 will complete further analysis into the capabilities required for managing the entire incident lifecycle and their current coverage within identity federations.

9 Summary

This document proposes security incident response procedures for identity federations and interfederation. The procedures are based upon the Sirtfi framework, the research and education federations' response to the need for coordinated security incident response. The procedures are based on a central unit being established to provide security incident support at the interfederation level, and leveraging existing intrafederation relationships to address security incidents local to a single federation.

Appendix A: Template Procedures

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.

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 must be driven by eduGAIN agreeing to offer centralised security incident response support in line with these requirements. Following that, the procedure could be adopted federation-by-federation.

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.

A.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

A.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 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.

A.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.

A.4 Roles and Responsibilities

Roles and Responsibilities of 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

Roles and Responsibilities of 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.

Role and responsibilities of 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".

A.5 Procedures

Security Incident Response Procedure for 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 via their security contact 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.

Federation Security Incident Response Procedure for 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 via their security contact 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.

Security Incident Response Procedure for the 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 via their security contact 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

Appendix B: Heads-up Notification Example

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-----
Comment: GPGTools - http://gpgtools.org

iQIcBAEBCAAGBQJYRYFMAAoJEKI4ZxEq8/Y2gZAP/2LMs2jqEeewyvRCE6h4jKDA
R6BXfvVBVETztg+zeYzUE+wzleHg8qrRL8pw219D6S/5x3NvvceO/pGI0Weg66AF
PtGOAdENyxnfQ53BvzLC17A4B490MWioSz10nk2ir50UH7b6+yVf/M9wP8r9F8Gb
K4XfCvKHYrFR5Ouoh3Ptbdz/MBeY10L7fpVYbPiEkWzFGnjVlqa7fudoOkCXO47e
bNzxgSJ6BfFOh2lCbB3IdL75/pqkvzps9+eNW5PZPCaSd0Kd9+m2B19oT/18ZJiU
OdYXKT4xJlrWv9SMTn6lH9EGt+MQoFkXwPmdyUCx13hL7xlqVn6yjkeAivmtwOaD
7b7Gv/80+1QnfEdfK8Yu8vsfPOkFaLAfuDpXLzvJ6fgPjLGhb9U3nGPDAkgmGb2+
vFo+HSpoMkLPwpMcCzBgE7+S4HyOSbCudF63MoWjxzjzWpxzSk9fnUSNHAwdcY3g
BG9HCn+SE8PC1ln9v1w6bGrNctIKxg9SxZlgdKyqCivFaeAF9SBl4UmSgIwd4i4d
Gg6d5iTQwvsPaPZw2eLVTUBssCpqKOOJmcEA38yhAojHox9Re5jinMJnneBULdSo
TX66HcSZ/k51iBjWN8u4351/3LxVUwgZAk8OgJIdPHPe1H2nBKV3fZYNOe/dwRCT
+empCRrFuUbUbpYLAsg3
=BYdx
-----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-DNA3.5] TBC

[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