Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios

Publication Date	2019-02-27
Authors:	H. Short;R. Wartel;D. Groep;I. Nielson;U. Stevanovic;D. Kelsey
Document Code:	AARC2-DNA3.2 (D3.1)
DOI:	*n/a*
Contractual Date:	28-02-2019
Actual Date:	27-02-2019
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.1
Lead Partner:	CERN

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

Abstract

This report provides an overview of the current state of security incident response and cybersecurity in Federated Authentication Scenarios, focusing particularly on efforts that have taken place in the past two years related to input from the AARC2 project.

Table of Contents

Table of Contents 2

1. Introduction 3

2. Incident Response 4

2.1. Sirtfi 4

2.2. Sirtfi Registry 5

2.3. Incident Response Test Model 6

2.3.1. Simulation 1 6

2.3.2. Simulation 2 7

2.3.3. Future Coordination 7

2.4. Procedures and suggested improvements 8

3. Operational Security for Attribute Authorities 9

4. Trust Groups 10

4.1. Addressing the needs of the Federated R&E Community 11

5. Conclusions and next steps 13

References 14

1. Introduction

This report provides an overview of the state of Incident Response and Cybersecurity in Federated environments, focusing on particular areas in which the AARC project has dedicated effort over the past two years.

The AARC project in its second phase has benefitted from the Blueprint Architecture (BPA) and the increased engagement with user communities to strengthen the collective security posture of the community. The extension of the Sirtfi [Sirtfi] concept to areas where, for various reasons, organisations cannot join the scheme through their Identity Federation meta-data services has been addressed through the *Sirtfi Registry* concept. This is supported by the REFEDS [REFEDS] Sirtfi working group with support from research communities and infrastructures in joint discussions with eduGAIN [eduGAIN] and federation operators. Incident response model tests based on Sirtfi, and increasingly able to involve the eduGAIN security capability, have also been conducted.

The increased deployment of community-operated and community-managed BPA compliant proxies has also resulted in an increased deployment of attribute authorities, sources of trusted information that merit a protection level comparable to identity providers. The operational security activity has therefore also provided guidelines [G048] on how such attribute authorities are appropriately protected from common operational security risks.

Lastly, in an ever-more interconnected system, the timely exchange of sensitive information regarding security incidents is essential. Models to ease such information flow through trust groups involving many stakeholders are discussed in the context of federated infrastructures.

2. Incident Response

2.1. Sirtfi

As of December 2018, over 450 entities in eduGAIN support Sirfti, the Security Incident Response Trust Framework for Federated Identity. Sirtfi specifies a baseline of best practices that demonstrate the ability of an organisation to adequately participate in Incident Response in an Identity Federation. Since the core competency of many Federated Entity Operators is not Operational Security, an important mission of the REFEDS Sirtfi Working Group is to raise awareness of the framework and of the importance of incident response. In 2016 the Group defined a mechanism for asserting compliance with the Sirtfi framework in federation metadata. A significant proportion of Federations (numbering 27 out of 60 in December 2018) support their members in making the necessary declaration of an assurance profile and security contact.

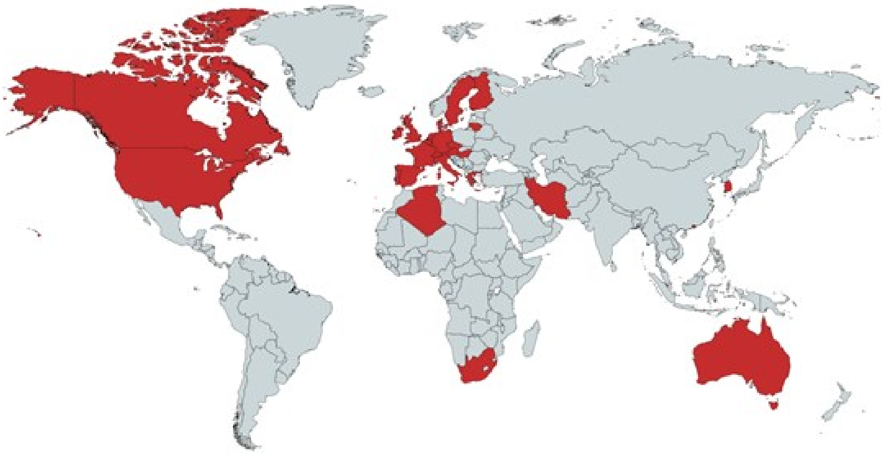

Figure 1: the national federations that contain at least one Sirtfi-compliant entity.

The individuals responsible for the Federated Entity (SP or IdP) may choose to nominate a separate entity to provide Security Incident Response support (i.e. the Sirtfi contact). An estimative study, performed in May 2018, demonstrates the breadth of types of contacts chosen. The high number of National Research and Educational Network (NREN) contacts primarily reflects the decision of SURFnet [SURF] to act as Sirtfi contact for all SURFconext[1] entities, since they are a hub and spoke federation. There is, however, an overall trend for Federated Entities to select a contact that is dedicated to security, rather than a generic IT contact or an individual.

[1] SURFconext is the brandname of the Dutch identity federation

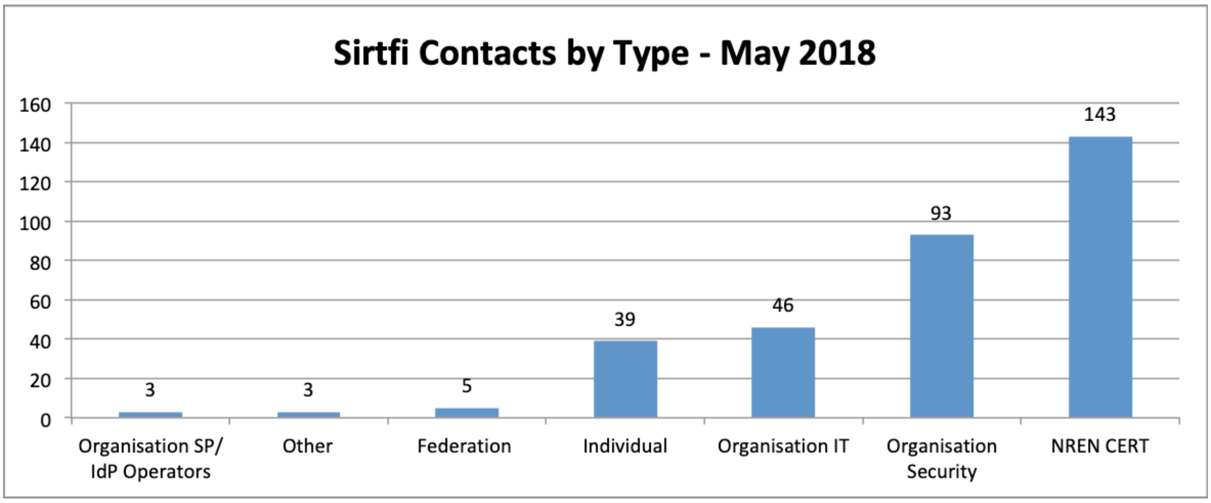

Figure 2: Sirtfi contacts as listed in the eduGAIN federation meta-data classified by contact type.

2.2. Sirtfi Registry

Although many active Federations allow their members to assert Sirtfi, others do not. This creates a problem for Research Communities whose policies require Sirtfi from all authenticating Identity Providers. Researchers from organisations in Federations that do not allow them to declare their compliance with the framework are consequently unable to access the Research Community, regardless of the security standing of their organisation. Similar situations may arise for Service Providers, though it is the Identity Provider scenario that provided the original use case for the Sirtfi Registry discussed here.

The Sirtfi Registry is proposed as a source of trusted information, outside Federation metadata, where organisations unable to assert compliance with Sirtfi through their Federations are able to do so. For example, this could be either a metadata feed that is injected into eduGAIN, or a layer that sits on top of eduGAIN to which interested parties could subscribe.

Work on the Sirtfi Registry is being coordinated by the REFEDS Sirtfi Working Group, in which several AARC NA3 participants are active, and has raised interest from the wider community. A concern of many is to avoid disrupting the Federation Trust Model. To this end Federation Operators, eduGAIN and Research Community representatives are holding joint discussions (including at Internet2's Technology Exchange[2] 2018 to foster global interoperation) to identify a solution that is of wide applicability and benefit.

More information can be found on the REFEDS Sirtfi Working Group page [SIRTFI-WIKI]. A pilot of this tool will be developed through the GN4-3 [GN43] Incubator Task.

[2] Internet2 is one of the research and academic network operators in the USA, whose technology exchange forum includes wide participation from both the US and the Canadian research identity federation community.

2.3. Incident Response Test Model

AARC2 MNA3.3 [MNA33] proposes simulations to test the capability of Federation Participants to respond to security incidents. Two scenarios were designed; a data breach where an SP must inform multiple IdPs, and an incident where a single compromised identity has accessed multiple SPs. The second proved to be the more interesting test as a higher level of active participation was required of participants.

Their full reports can be found on the AARC website [TESTREPS], and only key information is included here for brevity.

The Incident Response Simulation was run twice during 2018, once providing little guidance and once providing the AARC procedure in advance. The scenario consisted of a user accessing three SPs, each in a different federation, with the incident being triggered by an informant notifying one of the SPs that the identity used has been compromised. The objective was for all affected parties to be identified and for them to collaborate, fully explore, contain and resolve the incident.

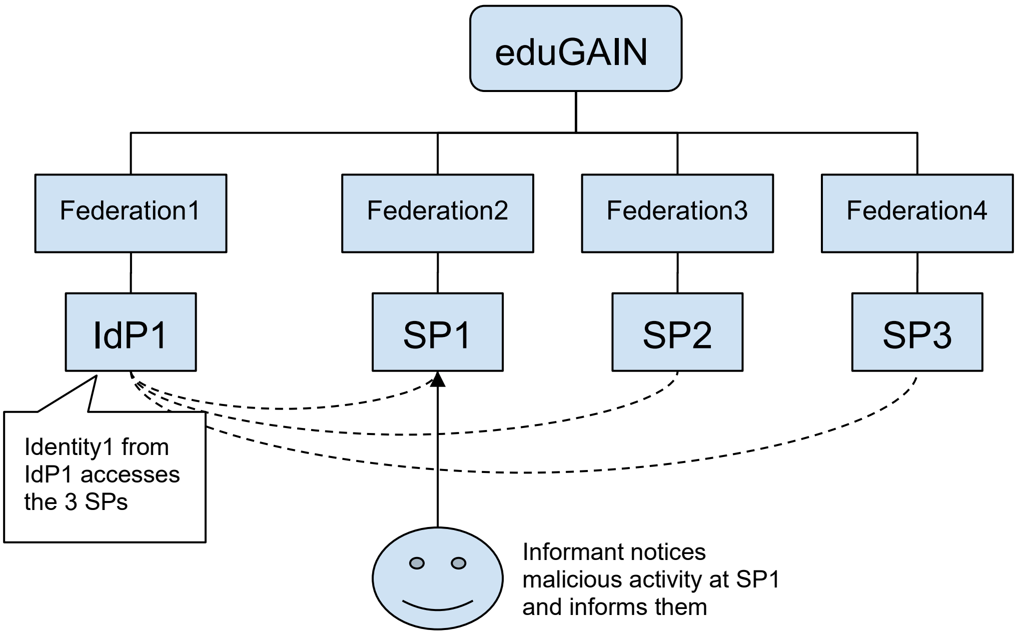
eduGAIN
Federation1
Federation2
Federation3
Federation4
IdP1
SP1
SP2
SP3
Identity1 from IdP1 accesses the 3 SPs
Informant notices malicious activity at SP1 and informs them

Figure 3: demonstration of the simulated scenario where a compromised user accesses three services, one of which is notified about an incident by a third party.

2.3.1. Simulation 1

When the simulation was run without a procedure, significant blocks in communication during incident response were experienced. The key findings indicated needs in the following areas:

1. An incident coordinator to be identified early in the incident, with a well defined set of responsibilities
2. Federation operators to be included in the incident response procedure to facilitate communication with IdPs and SP
3. A secure messaging system, set up in advance
4. A well known source of security contacts for federation participants, federation operators and eduGAIN
5. Clarity over the use of Sirtfi contacts when multiple are provided
6. Improved security knowledge at federation participants, federations and interfederation, or access to expertise freely available to the community
7. An incident response procedure for all participants to ensure that expectations are clear, behaviour is consistent and that the incident is fully investigated. Procedures should also contain template emails and suggested questions to be asked during investigation.

2.3.2. Simulation 2

Communication flows were significantly improved when the simulation was ran with the AARC procedure. Notwithstanding, several areas were identified for focus:

1. The availability of Federation and Interfederation security contact details should be addressed as a priority
2. Identifying the correct Sirtfi contact for Federated Entities is non trivial due to federation overlap and misleading tools
3. Further thought is required into how and where the Incident Reports should be made available, both to those affected directly and to the wider community
4. Regarding the proposed Incident Response Procedures:
   - Involving Federation Operators and Interfederation appears to be the correct approach
   - Guidance is required on how to identify, or nominate yourself as, the Incident Coordinator
   - A procedural step to “acknowledge” incident response communication should be considered
5. The community’s capability to send encrypted or authenticated (signed) messages should be understood and provision made for secure exchange of information

2.3.3. Future Coordination

Participants found the simulations to be useful for testing internal procedures, as well as for preparing for federated incidents. There was a strong request for future simulations to be coordinated. WISE, the Wise Information Security for collaborating E-Infrastructure Community [WISE], has a newly formed Working Group for this purpose. It aims to coordinate simulations and navigate the balance between desensitisation due to too many tests, and insufficient preparation.

2.4. Procedures and suggested improvements

AARC proposed procedures for Federated Incident Response in (the first project's AARC-1) "*DNA3.2 Generic security incident response procedure for federations*" [IRPROC]. These procedures have been trialled through the second simulation described above. The procedures included not only AARC contributors as authors, but also Federation Operators, eduGAIN and a wide range of stakeholders from relevant groups and projects.

The REFEDS Sirtfi Working Group is planning to open a community wide consultation of the procedures, through which input will be gathered to produce a second version.

Based on the knowledge gathered during AARC2 we suggest the following improvements to the procedures:

- Include templates for incident notification and follow up, including relevant questions to ask
- Add a procedural step for acknowledging receipt of an incident notification
- Adding guidance for setting expectations on the timeline of future communication
- Clarify how a party can nominate itself as Incident Coordinator, and how this information can be shared

The following points should be taken into account to improve the practicalities of Federated Incident Response

- Federation Operator security contacts should be collected and published
- Tools to identify the federation operator of an entity should be reviewed and improved
- The procedures should be made easily available in the anticipated places (e.g. the Sirtfi web page, eduGAIN, by Federation Operators)
- A mechanism for securely exchanging confidential data should be established
- The federated community's access to the benefits of Security Trust Groups (see section below) should be understood and/or enabled to facilitate improved Incident Response and Operational Security

3. Operational Security for Attribute Authorities

Sirtfi covers the federation facing components of AAIs (Authentication and Authorisation Infrastructures), however in the context of the AARC BPA this is insufficient to address the needs of research communities. Moving towards shared infrastructures with AA operators chosen by communities, additional provisions should be made. An existing policy from EUGridPMA addressed the problem of security at attribute authorities, but required a significant update to address the current deployment models.

This update was completed during AARC2 and published as AARC Guideline G048 *Guidelines for Secure Operation of Attribute Authorities and other issuers of access statements* [G048].

4. Trust Groups

One outcome of the Security Incident Simulations described above was an increased awareness of the variation of federation participants' engagement in Trust Groups, and a recommendation to improve access to the benefits afforded by such groups.

The term "Trust Group" here is used to describe a collection of individuals who operate within a community with a degree of confidence between the members, to the extent that confidential or delicate information pertaining to security incidents can be shared. Such groups can be formed and operated in multiple ways, some examples of which are explored below. A secondary aspect of a group is the scope in which it operates; those spanning multiple sectors, (e.g. industry as well as academia) typically have access to a wider range of threat intelligence.

Group Description	Impact	Example
Organisational level membership, Open application	A low degree of trust allows organisations to make contact with one another when required and facilitates the exchange of best practice. These groups typically provide opportunities for additional face-to-face trust building.	REN-ISAC[3]
Organisational level membership, Open application with peer vetting	A moderate degree of trust may lead to threat intelligence and vulnerability sharing. These groups facilitate the exchange of best practices. These groups typically provide opportunities for additional face-to-face trust building.	Trusted Introducer[4], FIRST[5]
Individual membership, Invitation only	A high degree of trust leads to valuable threat intelligence sharing and collaboration on incident response. Individuals are expected to play an active role and have a strong security background. Trust is accrued as an individual meaning that if an employee chooses to leave their job, the benefits are typically lost to the employer.	*Due to its sensitivity, no examples can be given*
Infrastructure group, individuals nominated by participating organisations	These groups facilitate the protection of distributed infrastructures where there may not be a single organisation held responsible. Individuals are typically nominated due to their role as a security expert at a participating organisation.	EGI-CSIRT[6]

[3] https://www.ren-isac.net/membership/how-it-works.html

[4] https://www.trusted-introducer.org/processes/accreditation.html

[5] https://www.first.org/membership/process

[6] https://csirt.egi.eu

4.1. Addressing the needs of the Federated R&E Community

Existing Trust Groups do not fully cover the membership of R&E Federations, meaning that many federated organisations are not currently able to participate in key security activities. This can be due to organisations falling outside the geography or scope of the groups, or a lack of awareness. In addition, an organisation may not have the capacity to participate in such groups, either in terms of time or expertise. This is particularly relevant for small campuses where there may be no association with a CERT or CSIRT, which are usually the target audience of Security Groups.

The following benefits are typically provided through trust groups, and are of interest to the Federated R&E Community. The following table makes proposals for bringing such benefits to the Federated R&E Community given that it is considered unlikely that all Federation Participants would participate in Trust Groups as described above.

Trust Group Benefit	Proposal for the Federated R&E Community
Access to security contacts	Work should continue to promote the Sirtfi framework and identify contacts for Federation Participants. In addition, contacts for Federations and Interfederations should be made easily available.
Access to threat intelligence	The exchange of threat intelligence is typically mutual, there may be an expectation for consumers to also contribute. This is unrealistic for all Federation participants and it remains to be seen whether a provision for threat intelligence sharing within the Federated R&E Community can be made. Further analysis is required in this area.
Access to vulnerability reports	In some cases, in particular for IdP and SP software, Federations already offer support for this. It is proposed that these capabilities also be considered in the eduGAIN Operational Security function that will be matured during GN4.
Access to expertise for advanced incident investigation, e.g. forensics	In some cases Federations already offer support for this. It is proposed that these capabilities also be considered in the eduGAIN Operational Security function that will be matured during GN4.
Fostering of trust between members	It remains to be seen whether an additional trust group is required, or even feasible given the size of R&E Federations. One option may be to leverage the WISE Community for this purpose, however this requires further analysis within a newly formed WISE Working Group on Incident Response.

A critical aspect to Trust Groups is the role that key individuals play by spanning groups. Through these people, information is able to flow (as far as allowed by confidentiality levels) and threat intelligence is not trapped in silos. It is expected that the eduGAIN Operational Security function may form a group similar to “Infrastructure wide” group described above; it should be highlighted that the individual members should form bridges between groups.

5. Conclusions and next steps

The AARC2 Project has made contributions in several areas that improve the capacity of Identity Federations to handle security incidents. In particular, the following items were produced - they are listed here along with a suggested path for ensuring that the work is taken into account in future.

Item	Sustainability Model
Defining and testing a model for Incident Response Simulation	• Using the results of such tests to identify improvements for the proposed Incident Response Procedures for Federated Identity, set to go through Community Consultation in 2019 • Testing will be coordinated by a newly formed Working Group in the WISE Community
Evolution of the “Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements”	• The guidelines will become part of the Policy Development Kit, extended under the WISE Community • The guidelines will be adopted by IGTF
Input into the Sirtfi Registry (AARC contribution but not responsible)	• The Sirtfi Registry discussion will continue in the REFEDS Sirtfi Working Group • The GN4 incubator task has volunteered effort to pilot a tool
Trust Group Analysis	• The topic will be further discussed under a newly formed Working Group in the WISE Community

References

AARCWEB *Authentication and Authorization for Research and Collaboration web site*; https://aarc-project.eu/about/documents/

BPA *The AARC Blueprint Architecture*; https://aarc-project.eu/architecture/

eduGAIN *The eduGAIN Interfederation Service*; https://edugain.org/

G048 *Guidelines for Secure Operation of Attribute Authorities and other issuers of access statements (AARC-G048),* D.L. Groep, D.P. Kelsey, H. Short, M. Sallé, U. Stevanovic, S. Paetow, M. Kremers, *et al.* (IGTF); https://aarc-project.eu/guidelines/aarc-g048/

GN43 *The GÉANT 4 Project phase 3*; https://www.geant.org/Projects/GEANT_Project_GN4-3

IRPROC Generic security incident response procedure for federations, H. Short et al. (the AARC1 consortium); https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf

MNA33 *Test model for organisations (IdPs) to share information related to account compromises,* H. Short et al.; https://aarc-project.eu/wp-content/uploads/2018/02/MNA3.3-IncidentResponseTestModelForOrganisations.pdf

REFEDS *The Research and Education FEDerations group*; https://refeds.org/

Sirtfi *Security Incident Response Trust Framework in Federated Identity (Sirtfi)*, REFEDS Sirtfi WG; https://refeds.org/sirtfi/

SIRTFI-WIKI *Sirtfi workspace*; https://wiki.refeds.org/display/GROUPS/SIRTFI

SURF Collaborative organisation for ICT in Dutch education and research; https://surf.nl/

TESTREPS *Incident Simulation Report #1 and Incident Simulation Report #2; https://aarc-project.eu/wp-content/uploads/2018/04/20180326-Incident-Simulation-Report.pdf and https://aarc-project.eu/wp-content/uploads/2018/11/Incident-Response-Test-Model-for-Organisations-Simulation-2.pdf*

WISE *Wise Information Security for E-infrastructures community*; https://wise-community.org/