EOSC Technical Specification

Security

Technical Area:	Security
Version:	1.0
Status:	Final
Document Link:	https://wiki.eosc-hub.eu/display/EOSCDOC/Security

EOSC-HUB RECEIVES FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO. 777536.

DELIVERY SLIP

Date	*Name*	*Partner/Activity*
From:	Jens Jensen	UKRI-STFC
Moderated by:		
Reviewed by:	Michal Prochazka	Masarykova Univerzita
Approved by:		

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
1.0	15/04/2020	Reformatted to template	J Jensen

TERMINOLOGY

https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+Glossary

Terminology/Acronym	*Definition*
AARC	Authentication and Authorisation for Research Communities
AUP	Acceptable Use Policy
BPA	Blueprint Architecture (AARC)
CERT	Computer Emergency Readiness Team
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity (enisa.europa.eu)
IdP	Identity Provider
IGTF	Interoperable Global Trust Federation (www.igtf.net)
NIST	National Institute for Standards and Technology (www.nist.gov)
NREN	National Research and Education Network
REFEDS	Research and Education FEDerationS
SCI	Security for Collaborating Infrastructures trust framework
SIRTFI	Security Incident Response Trust Framework for Federated Identity
SNCTFI	Scalable Negotiator for a Community Trust Framework in Federated Infrastructures
SP	Service Provider
SVG	Software Vulnerability Group
WISE	wise-community.org

Table of Contents

Introduction

As a TCOM area, this specification describes Security, i.e. the standards and specifications for *operational security*, or "cybersecurity." Ultimately, the purpose of security, in this sense, is to ensure that the infrastructure is trustworthy, and participants are able to carry out their legitimate work and collaborations, while protecting the infrastructure and data from unauthorised parties.

In order to ensure that participants in e-infrastructures, research infrastructures, and identity federations (such as those operated by NRENs) can reduce the risk of security incidents, and collaborate on investigating, managing, and resolving security incidents, it is necessary to have a shared security operations framework. Specifically, this will cover

- best practices,
- security contacts,
- processes for assessing severity (and hence urgency),
- traceability of users,
- defining, updating, and tracking users' acceptance of acceptable use policies.

In addition, the standards cover how the compliance is asserted in a machine readable way. There are also constraints on human readable information but the specification on how to implement these constraints is left to the federation operator and/or participants.

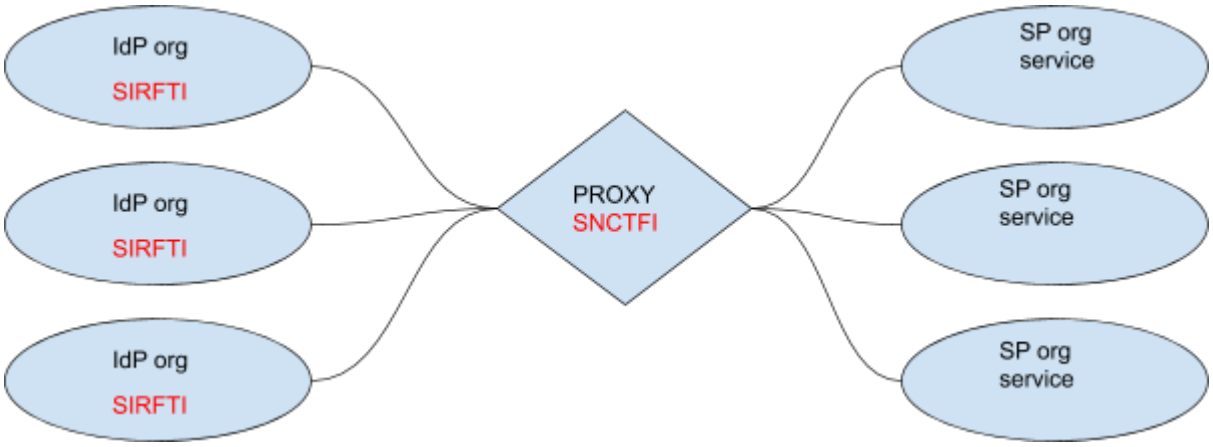
It should also be noted that the wider issue of establishing, maintaining, and restoring trust – between organisations, communities, and infrastructures – is not covered here.

Adopted standards

The standards listed below are formally issued by REFEDS [2] (Research and Education FEDerationS) and IGTF (Interoperable Global Trust Federation), respectively. However, both have come out of AARC2 [1] NA3 work (policies and harmonisation), and are established on the basis of wide consultation, not just in Europe.

Standard	Short Description	References
Security Incident Response Trust Framework for Federated Identity (SIRTFI – pronounced "certify")	Best practices for ensuring that federation participants are capable of minimising the risk of security incidents, and collaborate on handling them. The standard applies to both organisations running IdPs and SPs.	https://refeds.org/sirtfi
Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (SNCTFI – pronounced "sanctify")	Practices for handling and communicating SIRTFI compliance of federation participants in proxy-based federations. Includes SIRTFI as a requirement on IdPs and SPs.	https://www.igtf.net/snctfi/
A Trust Framework for Security Collaboration among Infrastructures	Operational security requirements on the infrastructure as a whole, published by the WISE community [7]. Overlap with SIRTFI (which covers IdPs and SPs).	[8]

High-level Service Architecture



The diagram above references the proxy [**2**] which adheres to SNCTFI in order to establish trust in the IdPs – the problem being that the proxy itself cannot assert SIRTFI for the IdP's domain as it is not authoritative for this domain.

Interoperability guidelines

The standards specify how SIRFTI compliance should be asserted in SAML-based federation in the metadata. SNCTFI is specified to enable proxy-based federations [1] to communicate the relevant attributes (SIRTFI compliance, traceable user identities) in a trustworthy way across proxies [2].

In addition, there is guidance on activities and practices that are relevant to the implementation of SIRTFI and SNCTFI. Guidance on a specific topic may be published by different projects or organisations – sometimes by national cybersecurity organisations – and should not vary substantially, although some might be more thorough than others. Although these are technically not standards, most of the guidance listed here is, like standards, based on state of the art and wide consultations.

In our guidance table, we have endeavoured to find examples of guidance likely to be accepted across a wide range of infrastructures.

Guideline	Short Description	Reference
Computer Security Incident Handling Guide	Principally focuses on handling a single incident but also includes sharing information with a	NIST SP800-61 rev 2 (DOI:10.6028/NIST.SP.800-61r2)

	Computer Emergency Readiness Team (CERT)	
Common Vulnerabilities and Exposures	The current list of known vulnerabilities can help organisations prevent incidents	https://cve.mitre.org/

Most countries would have national cybersecurity organisations. Organisations would also have their own policies and processes. There are also cybersecurity professional organisations, both nationally and internationally (see also [12] for an overview). An example of the latter is $(ISC)^2$, which publishes a code of ethics for cybersecurity professionals, as well as a certification scheme, CISSP. Also ENISA has cybersecurity training [10].

It should be added that there are many commercial "solutions" for (usually organisational) cybersecurity. The state of the art comprises:

- Cybersecurity awareness training for employees;
- Ransomware protection;
- Endpoint protection and security testing; penetration testing ("pentesting");
- Assistance with security incident handling from mitigation (phishing exercises, code analysis), through forensics to reactive (intrusion detection, SIEM, etc.) and to proactive handling (threat hunting);
- Virtual Private Networks for access to corporate resources;
- Tools to detect unusual or suspicious activities, e.g. login from an unusual location which might require multi-factor authentication, or detection of insider threats ("compromised" employees who access data they shouldn't).

Note that a security evaluation should include a threat model which should also cover any additional resources used by the community. These can include, but are not limited to, connecting users to infrastructures with mobile phones (e.g. for second factor authentication), community-specific edge devices such as sensor networks that provide data to the community's research infrastructure, and external clouds used by the community.

Technical interoperability guidelines

Based on the standards defined above, the minimal technical requirements for interoperability can be summarised as:

- Publish correct metadata in federations (which provides machine readable assertions on compliance with standards).
- Have established infrastructure (email contacts, ticket trackers, etc.) for handling security incidents. It may be necessary to secure these, in order to be able to discuss vulnerabilities without revealing vulnerabilities to would-be attackers.
- Have basic technical and physical security protecting their resources (firewalls, access controls, etc.), at a level suitable for the type and use of the resource.
- There must be means of communicating AUP to users and recording their acceptance.

Some of these requirements may apply to infrastructures, and some to the organisations participating in infrastructures, and some to both.

Policy interoperability guidelines

- Organisations should adhere to the practices above, i.e. collaborate on the resolution of security incidents, and have defined AUPs and data protection policies.
- In order to promote the interoperation at the policy level, it is recommended that organisations and infrastructures use resources from AARC [1], such as the Policy Toolkit.

Examples of solutions implementing this specification

EGI

EGI references guidance on SIRTFI to its IdPs: https://wiki.egi.eu/wiki/AAI_guide_for_IdPs
Notably, EGI also runs a Security Vulnerability assessment Group (SVG, https://wiki.egi.eu/wiki/SVG which handles the vulnerabilities related to software. Led by Dr Linda Cornwall from UKRI-STFC, the group is currently (Jan. 2020) in the process of establishing a deployment vulnerability group for EOSC.

EUDAT

During the lifetime of the EUDAT2 project, the project's WP6 specified that participants should adhere to SIRTFI (the reference does not seem to be publicly available). In particular, the project

maintained a link of security contacts for each organisation, although there was an issue with keeping the page up to date.

GEANT

From Terena/GEANT, it is worth noting:

- TF-CSIRT working group [5]
- The Information Security Management Special Interest Group (SIG-ISM) [6]
- The WISE community [7] which includes SCI which published [8].
- The CSIRT-KIT project [9]

ENISA

The European Union Agency for Cybersecurity provides guidance on incident reporting [11], and extensive guidance on operating CSIRT services [13], and a lot of other relevant information on cybersecurity.

NRENs

Currently (Q1 2020) NRENs do not require SIRTFI for their participants, but they support it for organisations that wish to assert it.

It was noted that when CERN's eduGain authentication started rejecting IdPs that did not assert SIRTFI, the uptake of SIRTFI improved.

Procedure to integrate a service with the EOSC Hub

As mentioned under technical requirements, little is required beyond email and ticket trackers. However, the need to secure the information against would-be attackers requires integration with an authentication and authorisation system. It would make sense for interoperating infrastructures to use the same but there is currently no single system in use, other than basic email.

References

[1] Authentication and Authorisation for Research Communities (AARC) https://aarc-project.eu/
[2] AARC Blueprint Architecture (BPA) https://aarc-project.eu/architecture/
[2] REFEDS www.refeds.org

[3] IGTF www.igtf.net
[4] ISC2 code of ethics https://www.isc2.org/about
[5] https://wiki.geant.org/display/TTC/Report+on+TF-CSIRT+Membership
[6] https://wiki.geant.org/display/SIGISM/SIG-ISM+Home
[7] https://wise-community.org/
[8] https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf
[9] http://www.csirt-kit.org/
[10] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists
[11] https://www.enisa.europa.eu/topics/incident-reporting
[12] https://www.enisa.europa.eu/topics/national-cyber-security-strategies
[13] https://www.enisa.europa.eu/topics/csirt-cert-services