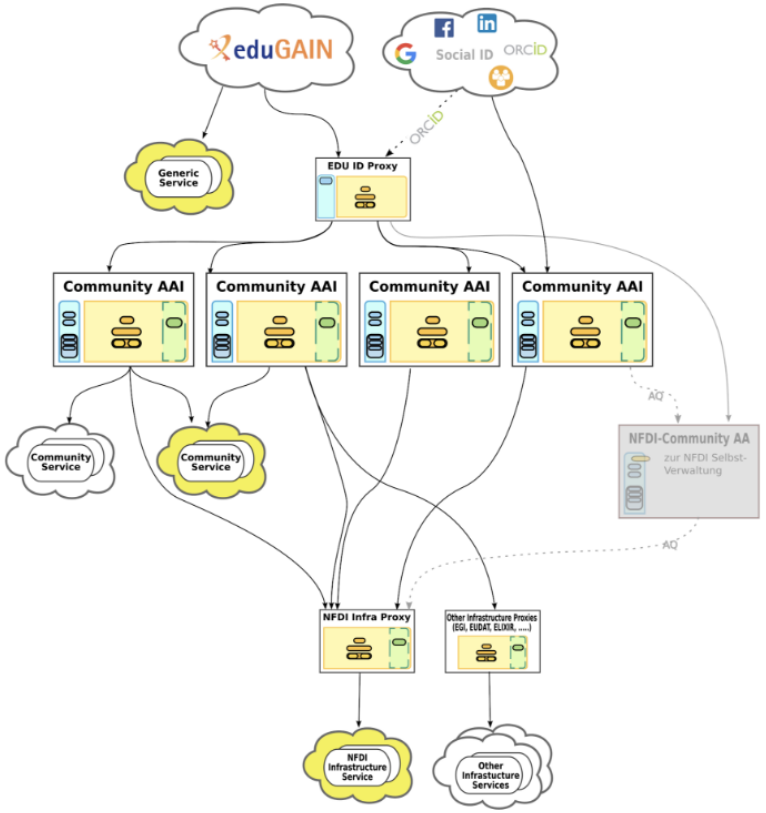
Proxies in Federations (Snctfi)

David Kelsey (UKRI-STFC)

FIM4R workshop
CERN
16 February 2023

Overview

- AARC BPA is used in many places
- Not a single Proxy – can be many federated Proxies
  - Community, Infrastructure, Site, edu-ID
- How to Trust SPs?
- How “open” should Proxy be?
- Does Snctfi V1 need
  - Guidance
  - Update to V2



Sncfti

Start with a reminder – (some) slides shown at FIM4R in Montreal, Canada in September 2017

Authentication and Authorisation for Research and Collaboration

Snctfi

SP/IdP Proxies and a new Policy Trust Framework

AARC NA3 Task 4 – Scalable Policy Negotiation

David Kelsey

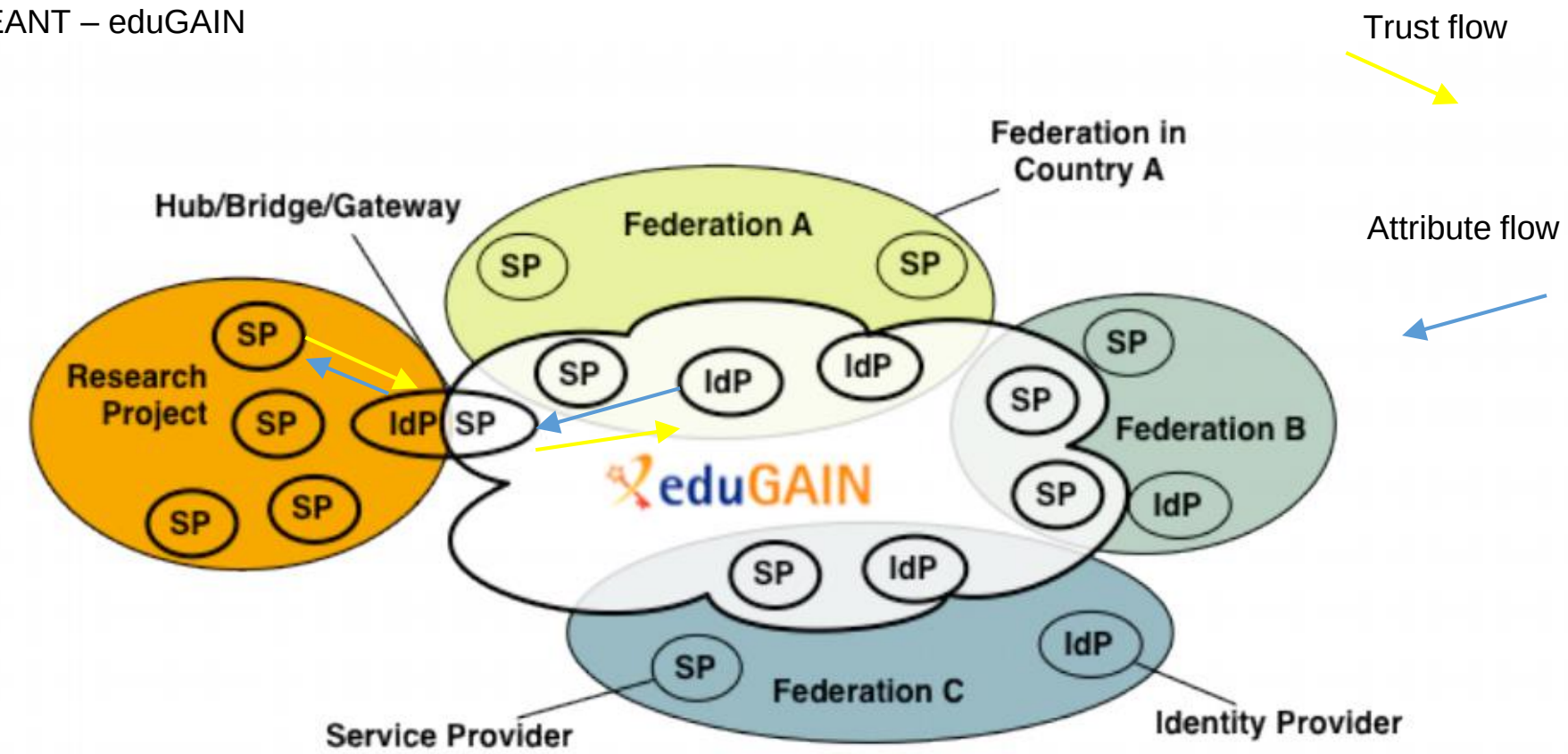
STFC-RAL

FIM4R meeting - Montreal

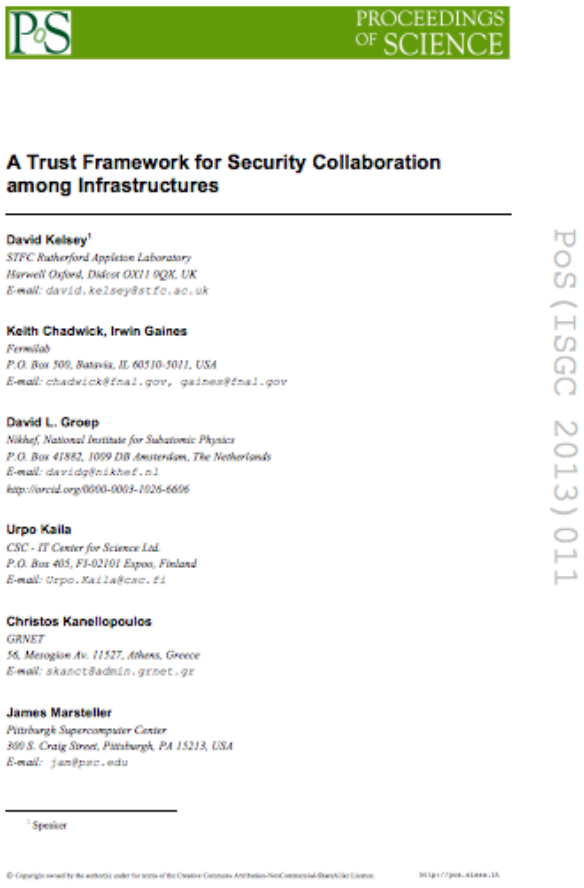
19 Sep 2017

Flow of attributes and trust – via SP/IdP Proxy

Picture from GEANT – eduGAIN



"Security Collaboration among Infrastructures" (SCI) – our starting point



PROCEEDINGS OF SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

David Kelsey[1]
STFC Rutherford Appleton Laboratory
Harwell Oxford, Didcot OX11 0QX, UK
E-mail: david.kelsey@stfc.ac.uk

Keith Chadwick, Irwin Gaines
Fermilab
P.O. Box 500, Batavia, IL 60510-5011, USA
E-mail: chadwick@fnal.gov, gaines@fnal.gov

David L. Groep
Nikhef, National Institute for Subatomic Physics
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands
E-mail: davidg@nikhef.nl
http://orcid.org/0000-0003-1026-6606

Urpo Kaila
CSC - IT Center for Science Ltd.
P.O. Box 405, FI-02101 Espoo, Finland
E-mail: Urpo.Kaila@csc.fi

Christos Kanellopoulos
GRNET
56, Mesogion Av. 11527, Athens, Greece
E-mail: skanct@admin.grnet.gr

James Marsteller
Pittsburgh Supercomputer Center
300 S. Craig Street, Pittsburgh, PA 15213, USA
E-mail: jam@psc.edu

[1] Speaker

PoS(ISGC 2013)011

Http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

- EGI, HBP, PRACE, EUDAT, CHAIN, WLCG, OSG and XSEDE
- Defined a policy trust framework
  - build trust and develop policy standards for collaboration on operational security
- SCI was used as the basis for ***Sirtfi***
  - ***A Security Incident Response Trust Framework for Federated Identity***
  - to enable coordination of security incident response across federated organizations
- Version 1

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

Snctfi

- As for “Sirtfi”
  - A meaningful acronym which is pronounceable
  - With no pre-existing hits in search engines

- “Sanctify” - meaning: make legitimate or binding
- Synonyms for sanctify: Approve, endorse, permit, allow, authorise, legitimise, “free from sin”

Snctfi - the new Trust and Policy Framework

- **Abstract**: identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy
- **The target audience**: intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness
- **Snctfi version 1**
  - An output of the EU H2020 AARC project
  - Published on 26 Apri 2017
  - https://aarc-project.eu/policies/snctfi/
- Peer-review and assessments – future work
  - Interoperable Global Trust Federation (IGTF)
  - https://www.igtf.net/snctfi/
- EGI Security Policy Group – together with AARC2
  - Working on two “Community” security policies – to implement requirements of Snctfi

Structure of the Snctfi document

- Background and Introduction
- Operational security [OS]
  - Aiming to prevent security incidents, or
  - Minimise the impact of those that occur
- User responsibilities [UR,RU,RC]
  - To establish trust between the *Infrastructure* and the R&E federations, and between *Infrastructures*, the *Infrastructure* relies on appropriate behaviour by its users and user communities.
  - Addresses issues related to user management, AUPs, security incident response, …
- Protection and processing of personal data [DP]
  - Bind the Infrastructure Constituents and Collections of users to either
    - A common *Infrastructure* Data Protection policy (framework)
    - Or GEANT Data Protection Code of Conduct

Discussion topics

- Policy for/ trust of SP/IdP Proxy (AARC BPA)
  - Does Snctfi help build Trust in Federations?
- What do Identity Federations need?
- Do we need a Snctfi entity attribute?
- Should we update Snctfi to version 2?
- Need for Snctfi FAQ and Guidance?
- Other issues?

Discussion – what do Identity Federations need?

- Is a AARC BPA Proxy a different Federation participant?
- And should it be registered as such?
- IdP, SP, attribute authorities, AARC BPA proxies, other “middle things”
- Or do we leave the Proxy as a simple “SP” in the federation but with appropriate entity attributes (Sirtfi, Snctfi, etc.)?

Discussion – update Snctfi V1 to V2?

- Snctfi V1 published in 2017
  - Was derivative of SCI trust framework V1
- Sirtfi is also a child of SCI V1
- SCI was updated to V2 in 2017
- Sirtfi V2 has just been published
- Surely we need a Snctfi V2?
- And perhaps, by the way, an SCI Version 3?
- Thoughts?

Discussion – FAQ and guidance

- WISE SCI-WG has recently completed
  - Guidance to maturity assessment against SCI V2
- Sirtfi (v2) has FAQ and guidance
- We need Snctfi guidance
- Will research communities do their own maturity assessment?
  - And help develop the Guidance

Thank you

David Kelsey or
policy@aarc-community.org

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Backup slides

Engage!

- https://fim4r.org
- https://refeds.org
- https://wise-community.org
- https://www.igtf.net
- https://aarc-community.org

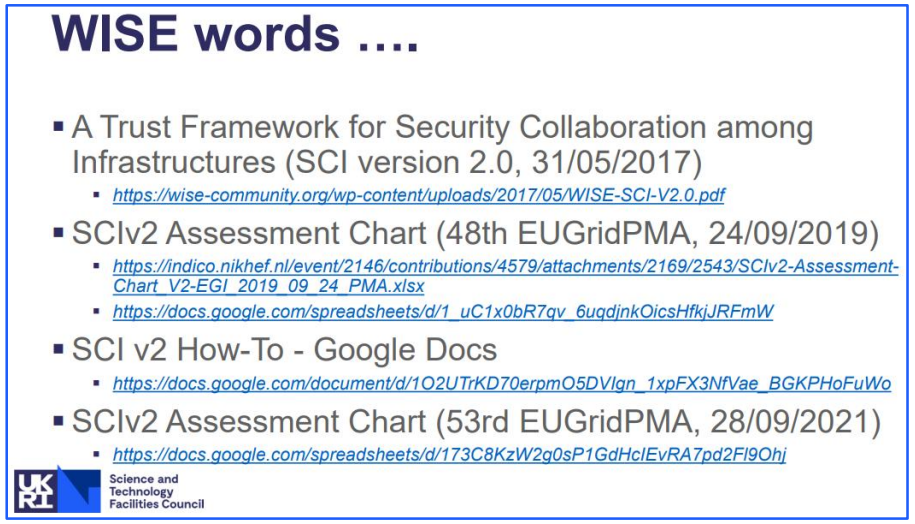
- Contact us: policy@aarc-community.org

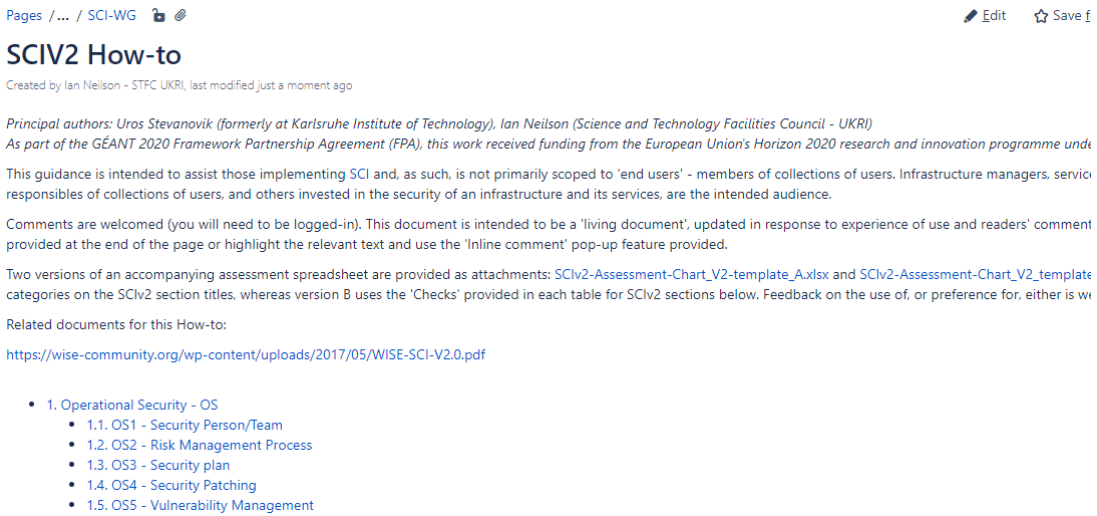
WISE SCI v2 ‘how-to’ guide update

Ian Neilson (UKRI-STFC)
SIG-ISM - WISE Workshop, Virtual 21/04/2022

By people from GN4-3 EnCo (Uros Stevanovic and Ian Neilson)

WISE words ….





- All information now in one place (hopefully): on the WISE Wiki -
  - https://wiki.geant.org/display/WISE/SCIV2+How-to

Science and Technology Facilities Council

A Trust Framework for Security Collaboration among Infrastructures

- https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

3. Operational Security [OS]

Each of the collaborating *infrastructures* has the following:

- [OS1] A person or team mandated to represent the interests of security for the *infrastructure*.
- [OS2] A process to identify and manage security risks on a regular basis.
- [OS3] A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation.
- [OS4] A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts.

- ❑ 29 Assertions across 5 Categories.
- ❑ How to assess the level of compliance?

Science and Technology Facilities Council

SCIv2 Assessment Chart (A)

- https://wiki.geant.org/download/attachments/440303650/SCIv2-Assessment-Chart_V2-template_A.xlsx?api=v2

fx | Infrastructure Name:

	A	B	C	D	E	F	G	H
1	**Infrastructure Name:**		<insert name>					
2	**Prepared By:**		<insert name>					
3	**Reviewed By:**		<insert name>					
4								
5	**Operational Security [OS]**		**Maturity**				**Methods of enforcement**	**Evidence (Document Name and/or URL)**
6			**Value**	**S**				
7								
8	**OS1 - Security Person/Team**		3	#REF!	REF!			
9	**OS2 - Risk Management Process**		2	#REF!	REF!			
10	**OS3 - Security Plan (architecture, policies, controls)**			2.0	2.0			
11	OS3.1 - Authentication		2					
12	OS3.2 - Dynamic Response		2					

	OS3.8 - Disaster Recovery		2		
	OS3.9 - Compliance Mechanisms		2		
	OS4 - Security Patching		2	2.0	2.0
	OS4.1 - Patching Process		2		
	OS4.2 - Patching Records and Communication		2		
	OS5 - Vulnerability Mgmt		2	0.0	0.0
	OS5.1 - Vulnerability Process		2		

Science and Technology Facilities Council

SCI v2 How-To

- To provide guidance on interpreting the SCIv2 text
- *https://wiki.geant.org/display/WISE/SCIV2+How-to*

OS4 - Security Patching

Each of the collaborating infrastructures has:

What:	*"A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts."*
Why:	In order to maintain the security of a system to the fullest extent possible. Failure to apply security patches in a timely manner is one of the major causes of system compromise.
How:	Patching procedures should address the question of how the state of a system (e.g. has a security patch been applied?) is monitored and when and how required patches are applied. Procedures should also document the responsible persons and which actions must be taken. The investment of time in the deployment of software configuration management systems (https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software) is highly recommended.
Checks:	- A system is in place to track the installed state of all systems - Subscription or other means is available to receive update notices - A process or frequent review is in place to correlate and act on the above

SCIv2 Assessment Chart (B)

- https://wiki.geant.org/download/attachments/440303650/SCIv2-Assessment-Chart_V2_template_B.xlsx?api=v2

		Maturity			Evidence (Document Name and/or URL)
		Value	S		
Operational Security [OS]					
OS1 - Security Person/Team			**0.0**	0.0	
The person or team is appointed with clear responsibility and authority.	0	0			
Contact details for the above are published internally and externally.	0	0			
OS2 - Risk Management Process			**0.0**	0.0	
Risks and mitigations have been identified and documented.	0	0			
Reviews of the risks and mitigations take place on a regular basis.	0	0			
Actions resulting from the review are given appropriate priority and resources.	0	0			
OS3 - Security Plan (architecture, policies, controls)			**0.0**	0.0	
Documents exist defining the security requirements of the Infrastructure	0	0			

Score	Definition
Blank	Not yet assessed
0	Assessed and no implementation
1	Low implementation
2	Partial implementation
3	Full implementation
4	Full implementation with peer review

OS4 - Security Patching			**0.0**	0
A system is in place to track the installed state of all systems	0	0		
Subscription or other means is available to receive update notices	0	0		
A process or frequent review is in place to correlate and act on the above	0	0		
OS5 - Vulnerability Management			**0.0**	0

Science and Technology Facilities Council

SCI Version 1 (2013) “children”

Kelsey/Proxies

16 Feb 2023

Sirtfi (and now updated to Sirtfi V2)

REFEDS

DOC VERSION: 1.0
DATE 14.12.2015
PAGE 1/5

TITLE / REFERENCE: SIRTFI

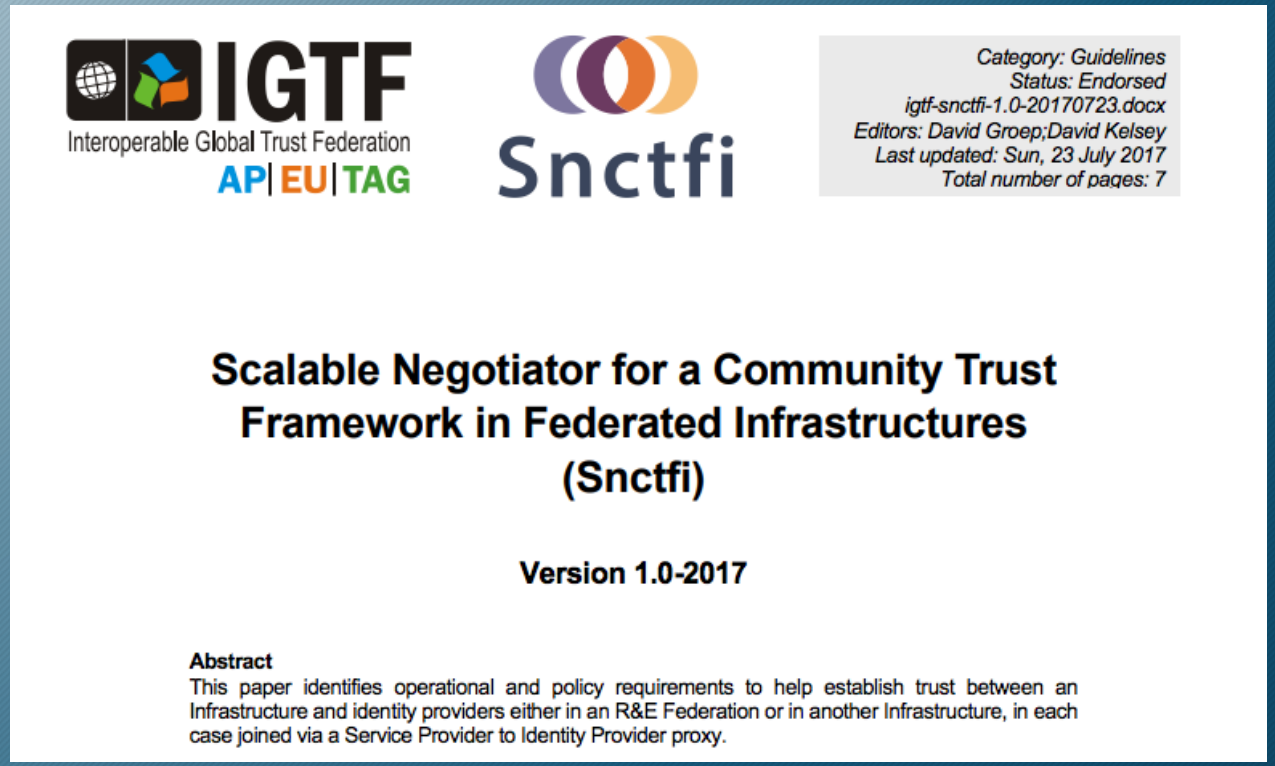
A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

Authors: T. Barton, J. Basney, D. Groep, N. Harris, L. Johansson, D. Kelsey, S. Koranda, R. Wartel, A. West
Editor: H. Short

Abstract:

This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to enable coordination of security incident response across federated organizations.

Snctfi (time for a version 2?)



IGTF
Interoperable Global Trust Federation
AP|EU|TAG

Snctfi

Category: Guidelines
Status: Endorsed
igtf-snctfi-1.0-20170723.docx
Editors: David Groep;David Kelsey
Last updated: Sun, 23 July 2017
Total number of pages: 7

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Version 1.0-2017

Abstract

This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.