Security for Collaboration among Infrastructures - SCI version 2

David Kelsey (STFC-RAL, UK Research and Innovation)
David Groep (Nikhef)

WISE/SIGISM Kaunas April 2019

In collaboration with and co-supported by EU H2020 EOSC-HUB

In collaboration with and co-supported by EU H2020 AARC2

Shared threats & shared users

- Infrastructures are subject to many of the same threats
  - Shared technology, middleware, applications and users
- User communities use multiple e-Infrastructures
  - Often using same federated identity credentials
- Security incidents often spread by following the user
  - E.g. compromised credentials
- Several e-Infrastructure security teams decided “we should collaborate”

Security for Collaborating Infrastructures (SCI-WG)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, HBP…
- Grew out of EGEE/WLCG JSPG and IGTF – from the ground up
- We developed a *Trust framework*
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies

SCI Document – version 1

- Proceedings of the ISGC 2013 conference

http://pos.sissa.it/archive/conferences/179/011/ISGC%2020 2013_011.pdf

- The document defined a series of numbered requirements in 6 areas

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

SCI Version 1 “children”

SCI version 1 (2013) - children

- Both separate derivatives of SCI version 1
- REFEDS Sirtfi - The Security Incident Response Trust Framework for Federated Identity
  - requirement in FIM4R version 1 paper
  - https://refeds.org/sirtfi
- AARC/IGTF Snctfi – The Scalable Negotiator for a Community Trust Framework in Federated Infrastructures
  - For scalable policy – Research Services behind a SP/IdP proxy
  - https://www.igtf.net/snctfi/

Sirtfi

REFEDS

DOC VERSION: 1.0
DATE 14.12.2015
PAGE 1/5

TITLE / REFERENCE: SIRTFI

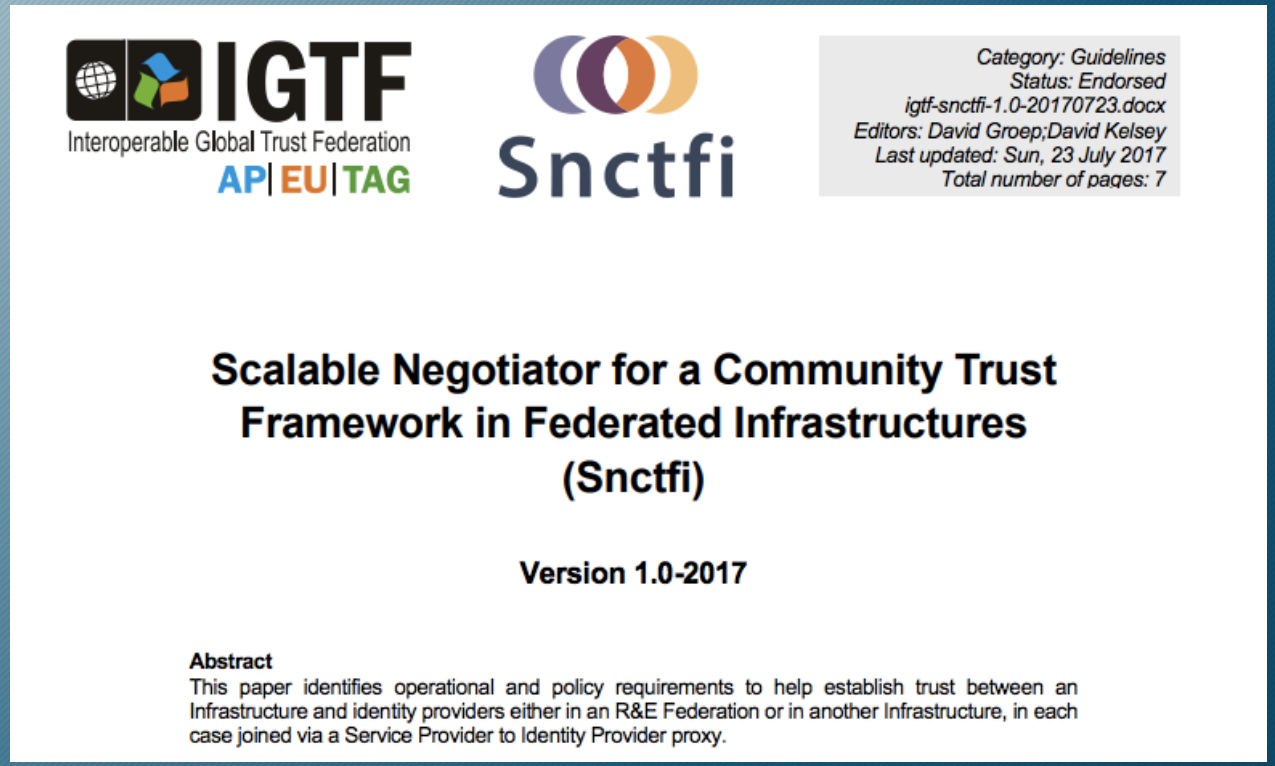
A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

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



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.

SCI version 2

WISE SCI Version 2

- Aims
  - Involve wider range of stakeholders
    - GEANT, NRENS, Identity federations, …
  - Address any conflicts in version 1 for new stakeholders
  - Add new topics/areas if needed (and indeed remove topics)
  - Revise all wording of requirements
  - Simplify!
- SCI Version 2 was published on 31 May 2017
- https://wise-community.org/sci/

SCI Version 2 – published 31 May 2017

WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

Endorsement of SCI Version 2 at TNC17 (Linz)

- 1st June 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

Sections of V2 paper

- In this document, we lay out a series of numbered requirements in five areas (operational security, incident response, traceability, participant responsibilities and data protection) that each Infrastructure should address as part of promoting trust between Infrastructures

- Concise representation putting requirements, not specific wording *(see some text from SCI V2)*

4. Incident Response [IR]

Each *infrastructure* has the following:

- [IR1] A process to maintain security contact information for all *service providers* and communities.

- [IR2] A documented Incident Response procedure. This must address: roles and responsibilities of individuals and teams, identification and assessment of incidents, minimisation of damage to the *infrastructure*, response and recovery strategies to restore *services*, communication and tracking tools and procedures, and a post-mortem review to capture lessons learned.

- [IR3] The capability to collaborate in the handling of security incidents with affected *service providers*, communities, and *infrastructures*, together with processes to ensure the regular testing of this capability.

- [IR4] Policies and procedures to ensure compliance with information sharing restrictions on incident data exchanged during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with other security teams on a need to know basis, and will not be redistributed further without prior approval.

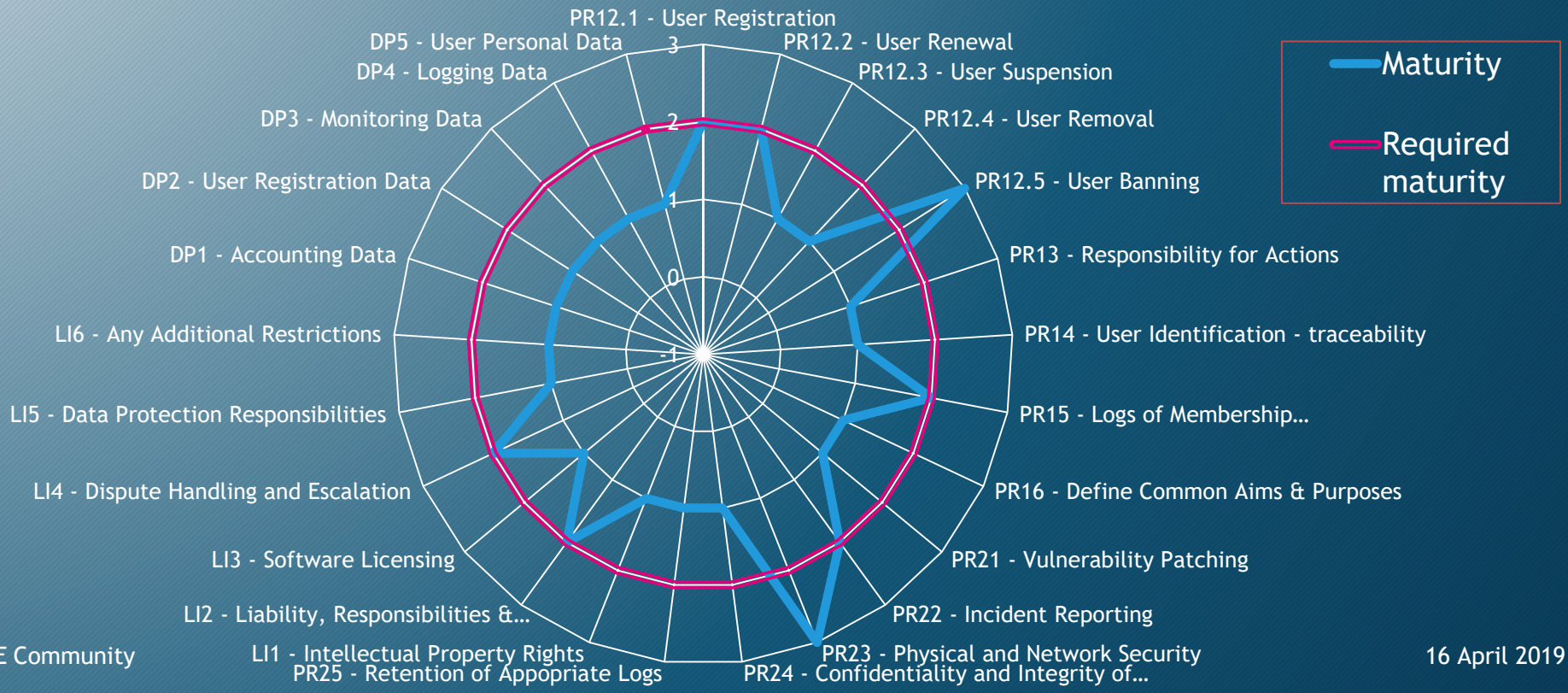
SCI Assessment of maturity

- To evaluate extent to which requirements are met, we recommend Infrastructures to assess the maturity of their implementations
- According to following levels
  - Level 0: Function/feature not implemented
  - Level 1: Function/feature exists, is operationally implemented but not documented
  - Level 2: … and comprehensively documented
  - Level 3: … and reviewed by independent external body

Assessment spreadsheet (AARC2 development)

	A	B	C	D	E	F	G	H	I	
1	**Infrastructure Name:**		<insert name>							
2	**Prepared By:**		<insert name>						**On Date:**	<insert date>
3	**Reviewed By:**		<insert name>						**On Date:**	<insert date>
4										
5	**Operational Security [OS]**		**Maturity**				**Evidence**	**Version Number**	**Document Date**	**Document Page**
6			**Value**	**Σ**			**(Document Name and/or URL)**			
7										
8	**OS1 - Security Person/Team**				●					
9	**OS2 - Risk Management Process**				●					
10	**OS3 - Security Plan (architecture, policies, controls)**			2.0	●					
11	OS3.1 - Authentication		3							
12	OS3.2 - Dynamic Response		1							
13	OS3.3 - Access Control									
14	OS3.4 - Physical and Network Security									
15	OS3.5 - Risk Mitigation									
16	OS3.6 - Confidentiality									
17	OS3.7 - Integrity and Availability	Q	1	1.0	●					
18	OS3.8 - Disaster Recovery									
19	OS3.9 - Compliance Mechanisms									
20	**OS4 - Security Patching**		1	1.0	●					
21	OS4.1 - Patching Process									
22	OS4.2 - Patching Records and Communication									
23	**OS5 - Vulnerability Mgmt**		1	0.7	●					
24	OS5.1 - Vulnerability Process									

Or present graphically



example, not an actual infrastructure

Current SCI activities

SCI-WG in 2019

Work in progress

- Joint work AARC2/EOSC-hub on Policy Development Kit
- WISE Baseline AUP v1.0 (from AARC PDK)

On the to-do list

- Produce FAQ/Guidelines & Training – how to satisfy SCI V2?
- Maturity Assessments from a number of Infrastructures

Next steps

- SCI assessment – infrastructure to self-assess and peer review (e.g. in conjunction with the IGTF)
- Guidance on AUP implementation beyond AARC
- Policy Development Kit evolution
- Coherency of security policy development for collaborating infras

- **ALL** welcome to the various mail lists and F2F meetings

Acknowledgements

- Many thanks to all colleagues in AARC2 policy team for slides
- Thanks to all colleagues in WISE & SCI-WG
  - and co-authors of SCI version 1 and version 2
- For funding received from EU H2020 projects, including
  - AARC2
  - EOSC-hub
- EGI, WLCG, GridPP, EUDAT, HBP, PRACE, …
- The Extreme Science and Engineering Discovery Environment (XSEDE) is supported by the National Science Foundation.

Questions?

- And discussion ….