SCI Version 2

David Kelsey (STFC-RAL, UK)

WISE Workshop, NSF Cybersecurity Summit, Arlington VA, 15 Aug 2017

Agenda

- SCI history
- SCI version 2 paper
- Maturity assessment
  - Walkthrough

SCI Version 2 – co-authors

- Thanks to all my colleagues
- Especially Adam Slagell (co-chair of WISE SCI working group)

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

SCI History

- “Security for Collaborating Infrastructures” (SCI)
- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, …
- Developed a *Trust framework (published in 2013)*
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies
- Joined with GEANT SIG-ISM to become “WISE” (Oct 2015)

SCI Version 1 paper (2013)

- Proceedings of the ISGC 2013 conference

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

- The document defines 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

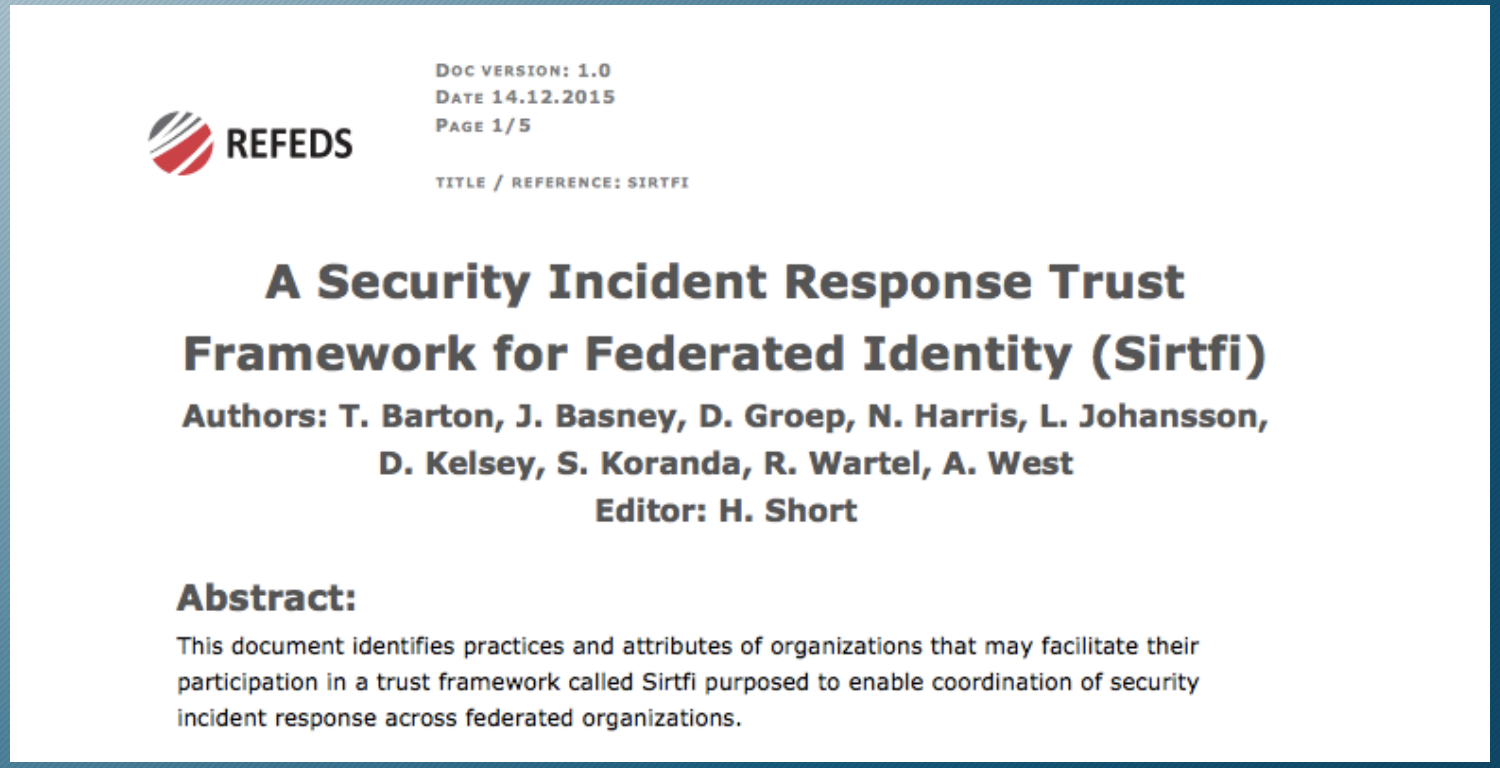
http://pos.sissa.it

PoS(ISGC 2013)011

SCI version 1 - children

- Both separate derivatives of SCI version 1
- REFEDS Sirtfi - The Security Incident Response Trust Framework for Federated Identity
  - https://refeds.org/sirtfi
- AARC/IGTF Snctfi – The Scalable Negotiator for a Community Trust Framework in Federated Infrastructures
  - https://www.igtf.net/snctfi/

Sirtfi



REFEDS

DOC VERSION: 1.0
DATE 14.12.2015
PAGE 1/5

TITLE / REFERENCE: SIRTFI

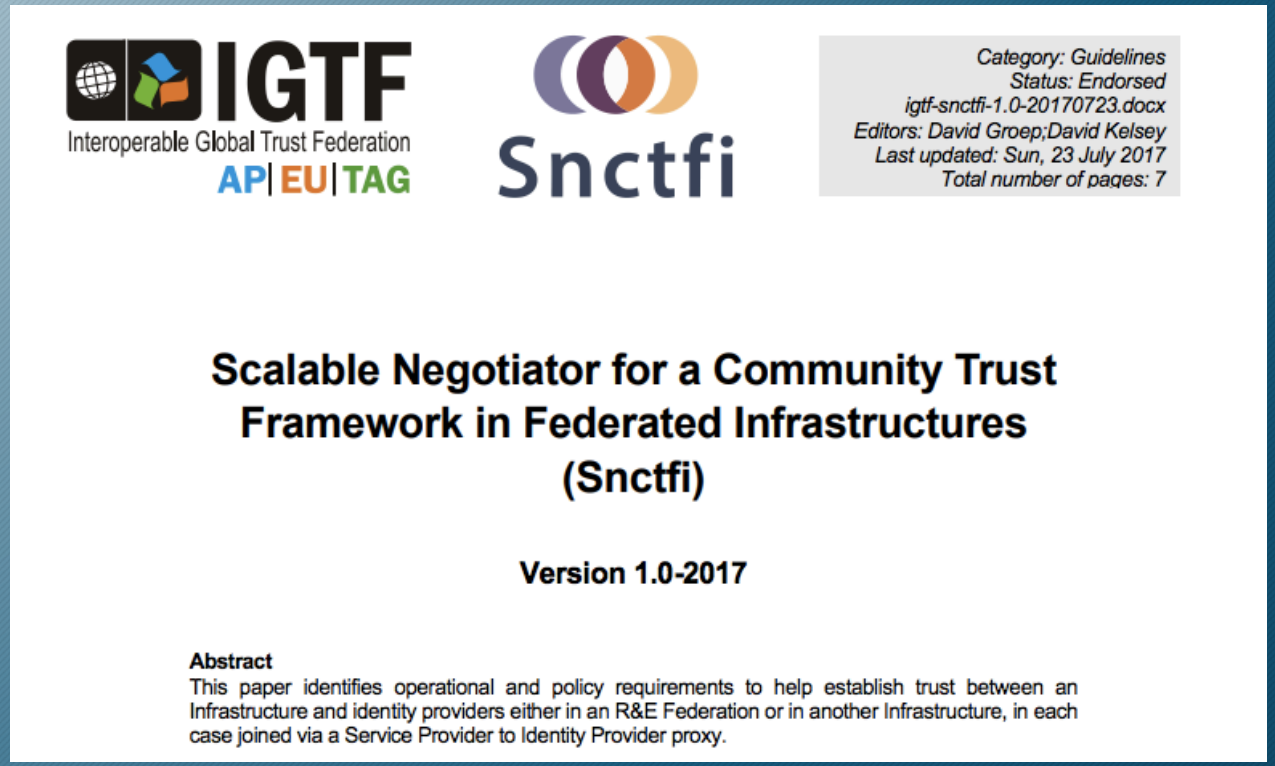
A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

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.

WISE SCI Version 2

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

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.
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

Maturity assessment

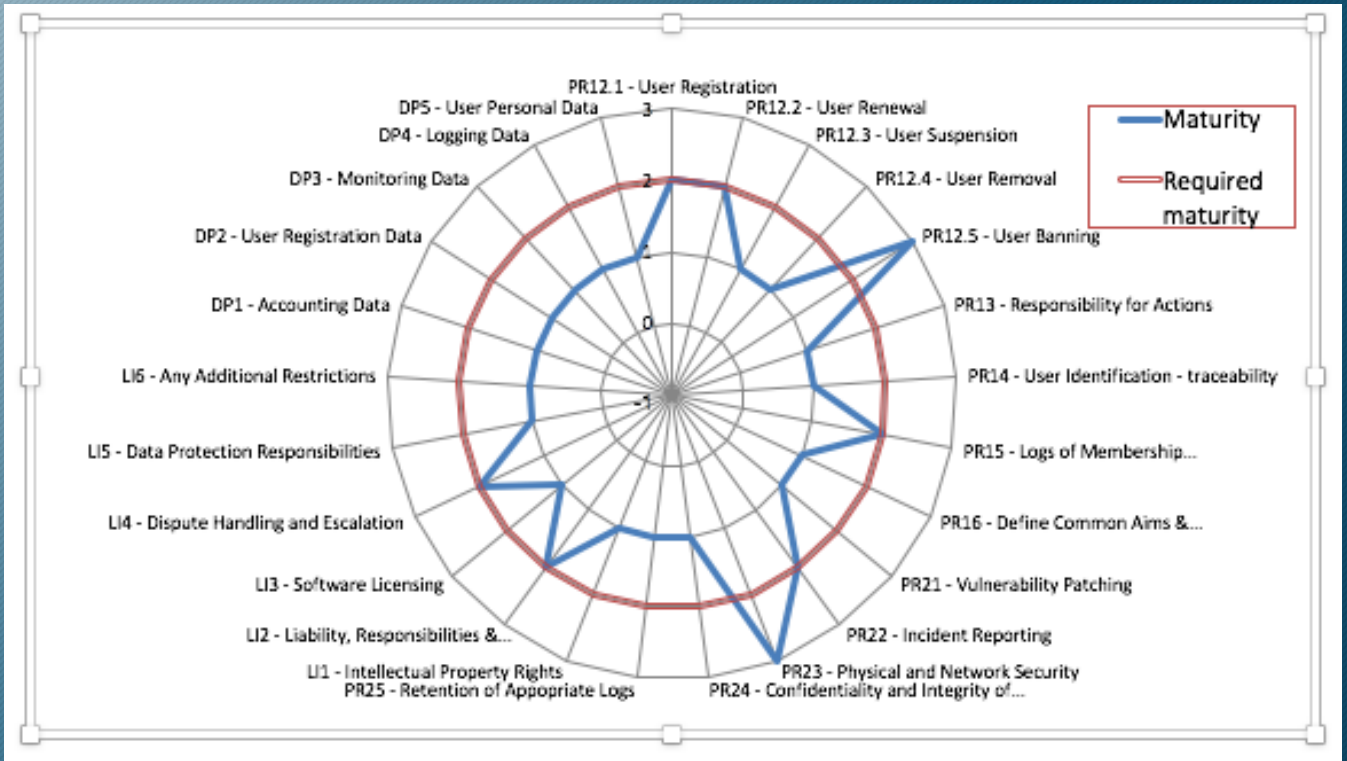
To evaluate the extent to which the requirements described in this document are met, we recommend that each Infrastructure assess the maturity of its implementation of each function or feature according to the following levels:

- Level 0: Not implemented for critical services;
- Level 1: Implemented for all critical services, but not documented;
- Level 2: Implemented and documented for all critical services;
- Level 3: Implemented, documented, and reviewed by a collaborating Infrastructure or by an independent external body;
- "Justifiable exclusion": In the unlikely case that the function or feature is not relevant for the infrastructure.

Maturity assessment - spreadsheet

	A	B	C	D	E	F	
1	**Infrastructure Name:**	<insert Infrastructure name>					**SCI Version 2.0**
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 (Document Name and/or URL)**	**Version Number**	**Document Date**	**Document Page or Section Number**	**Comments**
6	**OS1 - Security Officer/security team**						
7	**OS2 - Security risk management**						
8	**OS3 - Security plan**						
9	**OS4 - Security patching**						
10	**OS5 - Security vulnerability handling**						
11	**OS6 - Intrusion detection**						
12	**OS7 - Access control and emergency suspension**						
13	**OS8 - Contact users and SPs**						
14	**OS9 - Policy enforcement**						
15	**OS10 - Security input to service design and deployment**						
16	**Incident Response [IR]**						
17	**IR1 - Contact Information**						
18	**IR2 - Incident Response Procedure**						
19	**IR3 - IR Collaboration**						
20	**IR4 - information Sharing Restrictions**						
21	**Traceability [TR]**						

A fictitious maturity assessment (SCI v1)



SCI walkthrough - aims

- Show the SCI Version 2 paper
- Maturity Assessments from a number of volunteer Infrastructures
- Gather feedback:
  - problems experienced in completing the assessment spreadsheet
    - paper not clear
    - multiple concepts lumped together
    - maturity levels not clear
- To improve the spreadsheet
- To produce an SCI version 2 FAQ guidance document
- For input into SCI version 3 (merge SCI v2, Sirtfi and Snctfi?)

Questions?