WISE, SCI & policy templates

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

FIM4R & TIIME, Vienna, 11 February 2019

Contents

- The WISE community
- Security for Collaborating Infrastructures (SCI)
- AARC2 Policy Development Kit
- AARC2/WISE Baseline AUP

Note: WISE has several different activities – not just SCI
For example Risk Assessment working group has published draft risk assessment spreadsheets for use by others, see
https://wise-community.org/risk-assessment-template/

The WISE Community & Security for Collaborating Infrastructures (SCI)

The SCI activity was a co-founder, together with TERENA/GEANT SIG-ISM (2015)

More details on SCI: Trusted CI Webinar – D Kelsey (24 Sep 2018)
https://trustedci.org/webinars/

Next WISE Community meeting – Kaunas, Lithuania, 16-18 April 2019 – all welcome! https://wise-community.org/events/

WISE meetings (Oct 2015, Feb & Aug 2018) – others not shown!

Barcelona, Spain

Abingdon, UK

Alexandria, VA, USA

Security for Collaborating Infrastructures (SCI)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, …
- Grew out of JSPG(EGEE/EGI/WLCG) and IGTF – from the ground up (2011-13)
- 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

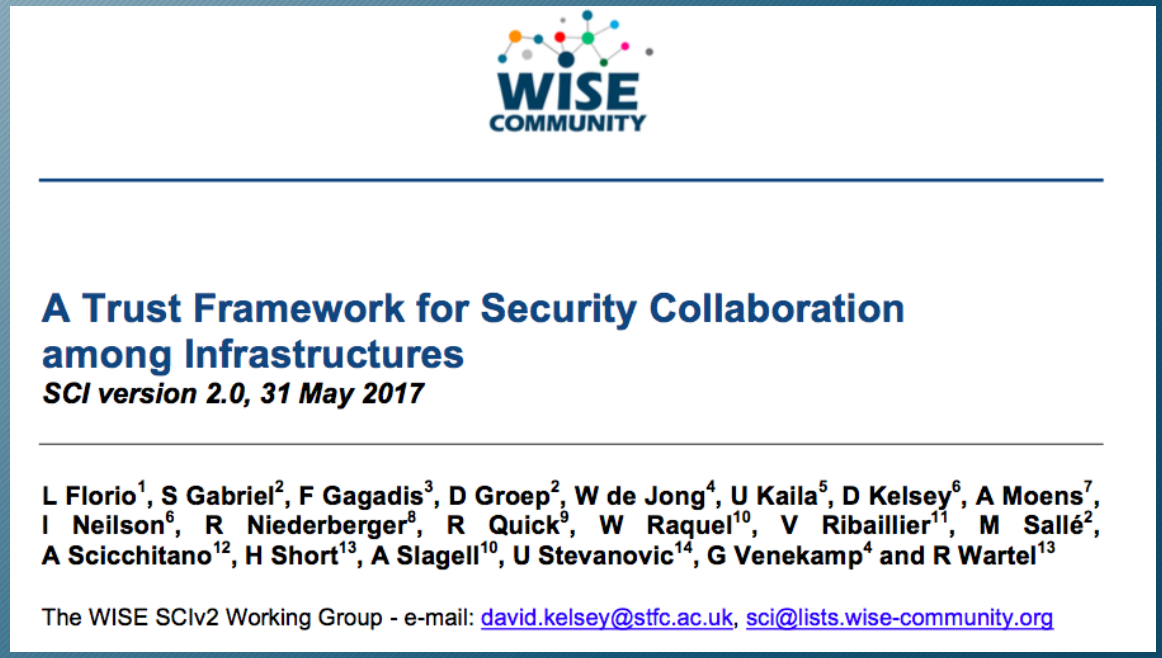
SCI version 1 (2013) - children

- 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/

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

SCI-WG in 2018/19

(Nearly) complete

- Joint work AARC2/EOSC-hub on Policy Development Kit
- Produce WISE Baseline AUP v1.0 (Prepared by AARC2)

Work in progress

- Maturity (self) Assessments against SCI v2
- Assessment spreadsheet/FAQ/Guidelines – how to satisfy SCI V2?

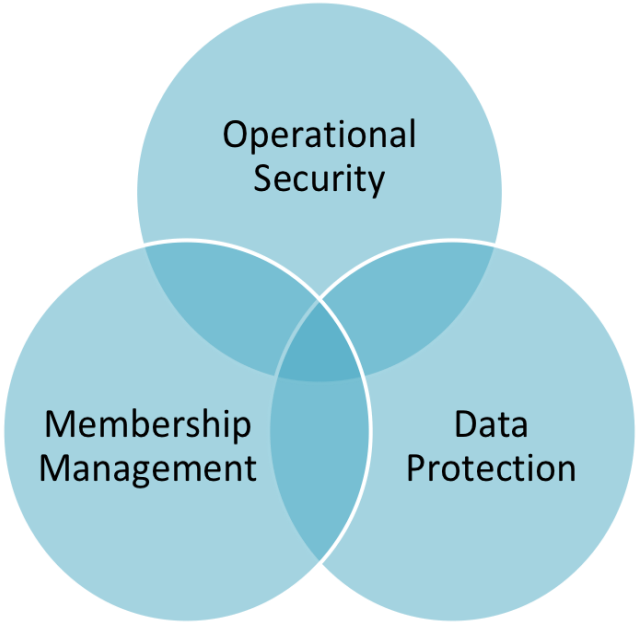
AARC2 (Uros Stevanovic & NA3 policy team) Policy development kit

- Establishing an Infrastructure (or Community) requires clear rules for security, membership management, data protection, etc.
- Rules → Policies
- Policies provide:
  - Trust
  - Manage and govern Infrastructure
  - Legal compliance
- AARC (and WISE) providing templates, instructions, trainings

- https://aarc-project.eu/policies/policy-development-kit/

Which policies?

- SCI paper (*A Trust Framework for Security Collaboration among Infrastructures)*
- SNCTFI (*Scalable Negotiator for a Community Trust Framework in Federated Infrastructures)*
  - Top level policy
    - Operational Security
    - Membership management
    - Data protection
- Consider current best practices (EGI, CERN, ELIXIR, TrustedCI, etc.)
- Policies start from EGI versions
- Some other policies (Infrastructure-related) will need to be handled by WISE/EOSC-hub



Slides of Ian Neilson - A common AUP - motivation

To make a recommendation for the content of an Acceptable Use Policy (AUP) to act as a baseline policy (or template) for adoption by research communities

- To facilitate -
  a) a more rapid community infrastructure ‘bootstrap’
  b) ease the trust of users across infrastructures
  c) provide a consistent and more understandable enrolment for users.
- Adoption of a policy preferred to template

2018 study of existing AUPs

- AARC2 NA3 policy (Ian Neilson)
- For details see: https://wiki.geant.org/pages/viewpage.action?pageId=86736956
- Looked at AUPs from 11 infrastructures
- Then considered clause by clause in a spreadsheet:
- https://docs.google.com/spreadsheets/d/1bg5I9n_DM7QcXdnja_7r0OEpTfjrb72ftq7-xHQxfxM/edit#gid=822235717

How will this Baseline AUP used?

- Forms part of the information shown to a user during registration with his/her community
- AUP provides information on expected behaviour and restrictions
- "baseline" text can, optionally, be augmented with additional, community or infrastructure specific, clauses as required, but the numbered clauses should not be changed
- The registration point where the user is presented with the AUP may be operated directly by the user's research community or by a third party on the community's behalf
- Other information shown to user during registration
- Privacy Notice - information about the processing of their personal data together with their rights under law regarding this processing
- Service Level Agreements - information about what the user can expect from the service in terms of quality such as reliability and availability
- (Optional) Terms of Service

WISE Baseline Acceptable Use Policy & Conditions of Use

Has been sent to WISE steering committee for approval (n.b. consultation has ended)

The 10 AUP policy statements are:

- *You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.*
- *You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.*
- *You shall respect intellectual property and confidentiality agreements.*
- *You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.*
- *You shall keep your registered information correct and up to date.*
- *You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.*
- *Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.*
- *Your personal data will be processed in accordance with the privacy statements referenced below.*
- *Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.*
- *If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.*

Questions?

- And discussion ….