


Security Trust and Policies - for WLCG and other Research Infrastructures

David Kelsey (UKRI-STFC)
HEPiX workshop, Victoria, BC, Canada
18 Oct 2023

Cybersecurity for Research?

- *Aim: to maintain the Availability, Integrity and Confidentiality of services and data*
- Standards-based best practice
  - Identify threats and manage risks
  - Security controls are used to mitigate risks
  - Controls can be technical, operational and managerial
- Trust is required to enable interoperation between Research Infrastructures
  - And to allow operational security teams to collaborate and share information
- Managerial security controls:
  Security Policies and Trust Frameworks

Science and Technology Facilities Council

Outline of talk

- History - Joint (WLCG/EGEE/OSG) Security Policy Group
- WISE/Security for Collaborating Infrastructures Trust Framework (SCI)
- AARC Policy Development Kit (PDK)
- Updating the AARC PDK
  - New policy templates
- AARC TREE
- FIM4R
- Other WLCG related activities
- Updating Security Policies for WLCG

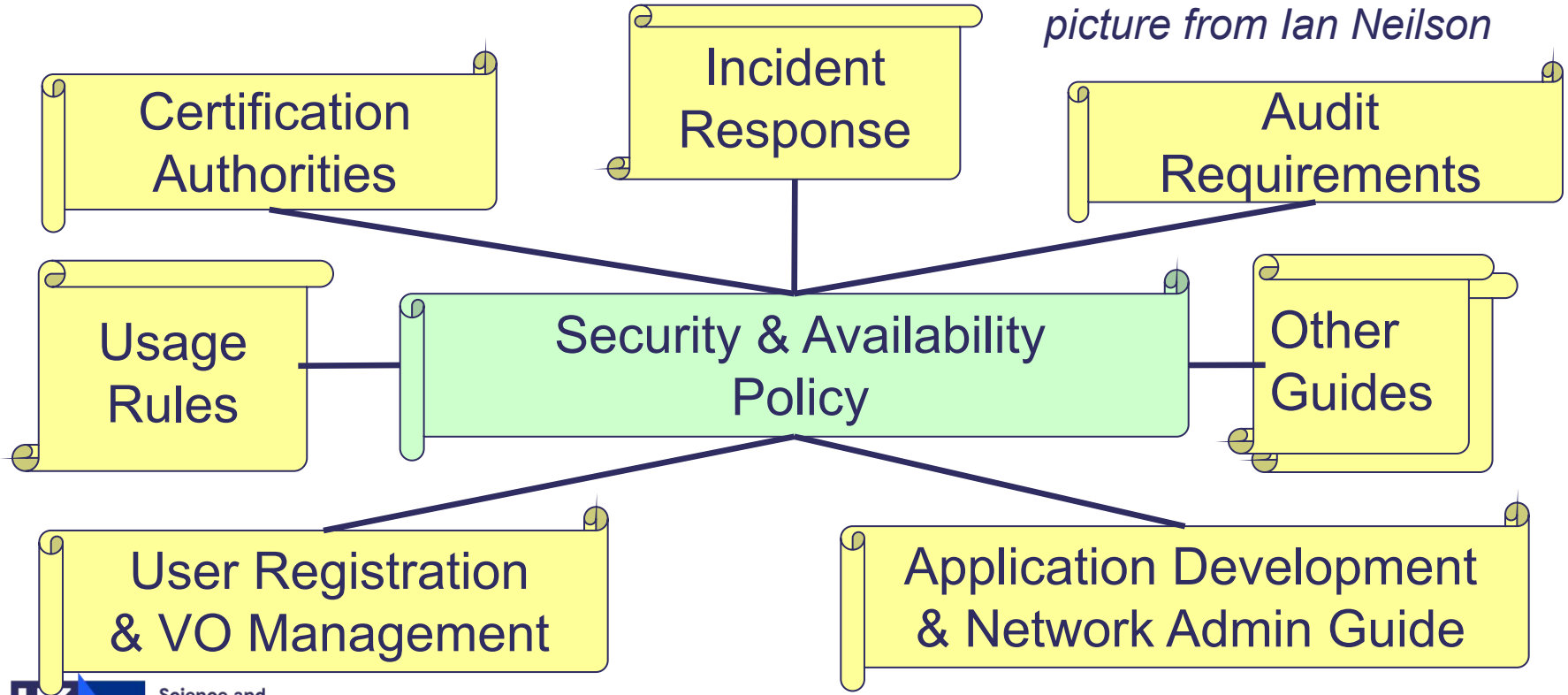
Science and Technology Facilities Council

History - WLCG Security Policy

- An agreed Security Policy
  - Written by Joint(WLCG/EGEE/OSG) Security Policy Group
  - Approved by the Grid Deployment Board/MB
- A single common policy for the whole project
  - *Augments* local site policies
- The policy
  - Defines *Attitude* of the project towards security and availability
  - Gives *Authority* for defined actions
  - Puts *Responsibilities* on individuals

Science and Technology Facilities Council

WLCG Policy - snapshot - years ago



picture from Ian Neilson

Science and Technology Facilities Council

Wise Information Security for collaborating e-Infrastructures

WISE Security for Collaborating Infrastructures (SCI) working group

In collaboration with and co-supported by
EU H2020 EOSC Future, GN4-3 & GN5-1

https://wise-community.org

The WISE Community

- Started in October 2015 – Joint - GEANT SIG-ISM & IGTF SCI
- Community members come from e-Infrastructures across the world
- *The WISE community enhances best practice in information security for IT infrastructures for research.*
- *WISE fosters a collaborative community of security experts and builds trust between IT infrastructures*

Security for Collaborating Infrastructures - The WISE SCI working group (SCI-WG)

SCI-WG - 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
- e-Infrastructure security teams need to collaborate
  - Trust is required

SCI Version 2 – published 31 May 2017 (TNC17) (version 1 was published at ISGC2013)

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

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?

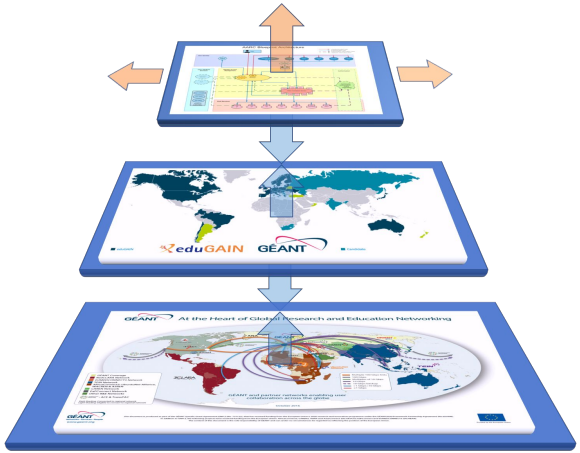
Science and Technology Facilities Council

Authentication and Authorisation for Research Collaboration

- EC-funded projects
  - AARC (2015-2017)
  - AARC2 (2017-2019)
- 25 Partners: NRENs, research and e-Infrastructure providers as equal partners
  - Focus on enabling FIM for eScience
- https://aarc-project.eu/

Watch the AARC video to find out more:
https://tinyurl.com/What-is-AARC

“Authentication and Authorisation for Research Collaboration” Results



Blueprint Architecture

Guidelines & Recommendations

SIRTFI

Snctfi

Policy Frameworks & Policy Development Kit (PDK)

Children of SCI - Sirtfi (now updated to V2)

REFEDS

DOC VERSION: 1.0
DATE 14.12.2015
PAGE 1/5

TITLE / REFERENCE: SIRTFI

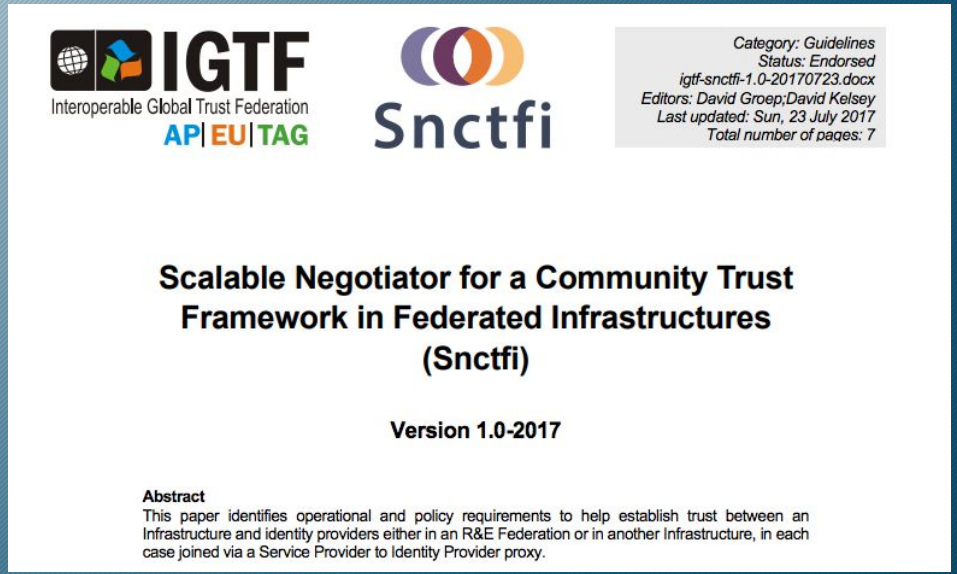
A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

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

Sctfi

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)

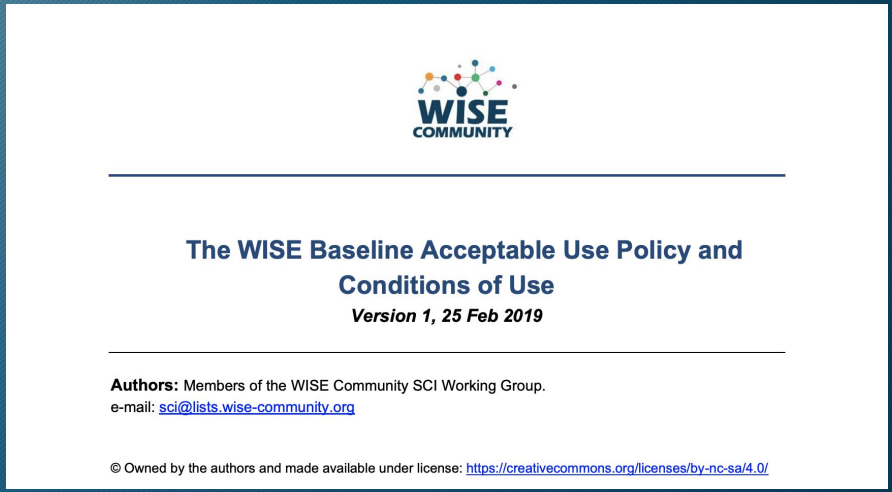
Version 1.0-2017

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 Baseline AUP
https://wise-community.org/wise-baseline-aup/

- a common baseline
- ease trust of users across infrastructures
- community and infrastructure-specific augmentation



WISE COMMUNITY

The WISE Baseline Acceptable Use Policy and Conditions of Use

Version 1, 25 Feb 2019

Authors: Members of the WISE Community SCI Working Group.
e-mail: sci@lists.wise-community.org

Developing the AARC Policy Development Kit

- WISE SCI-WG - updating policy templates

Development of AARC PDK by WISE SCI-WG

- Policy templates are useful to new Infrastructures and help build trust and interoperability (as compliant with SCI Trust Framework)
- Involve experience from many Infrastructures and policy groups (including AEGIS) *https://aarc-project.eu/about/aegis/*
- WISE SCI-wg collects feedback from Infrastructures
  - And use this if/when a new version of a template is required
- Unlike AUP, new templates may contain optional components
  - Infrastructures just use the components that work for them

Building on AARC PDK in WISE SCI-WG

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

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	
Data Protection	Privacy Statement	Defines			Defines	Views
	Policy on the Processing of Personal Data	Defines	Abides by	Abides by	Abides by	
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

Policy Area	New Template	Lead Participants
Top Level	Infrastructure Policy	IRIS
Data Protection	Privacy Statement	WLCG, IRIS
Data Protection	Policy on the Processing of Personal Data	EGI, WLCG
Membership	Community Policy	IRIS, EOSC, GN5-1, IGTF
Membership	Acceptable Authentication Assurance	GN5-1, IGTF
Operational Security	Incident Response	eduGAIN, Sirtfi, GN5-1, EOSC & many opsec groups
Operational Security	Service Operations	EOSC, IRIS

Service Operations Security Policy

- Original AARC PDK Template: https://docs.google.com/document/d/1_cNMF3l3YVPqBBH0MPqx9DLAL1t3Z33_fJcjln8Xk48/edit#heading=h.1dp93lqbm8kt
- In the UK, the IRIS Infrastructure used the PDK template – but made many changes to simplify and improve its Service Operations Security Policy (approved May 2021)
- The SCI working group used the IRIS version together with input from EOSC-hub, EOSC Future, EGI, ELIXIR, HIFIS and worked from October 2021 to April 2022
- See https://wiki.geant.org/display/WISE/Policy+Development+Kit
- The EOSC Security Baseline (Sep 2022) may serve as a better option for loosely coupled federations
- https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline
- EOSC FAQ Guidance at: https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Security+Operational+Annotated+Baseline

Service Operations Security Policy

WISE PDK Template Version 2 See *WISE-SCI-PDK-ServiceOpsSecPol-V2.pdf*

The WISE AARC Policy Development Kit

Service Operations Security Policy Template

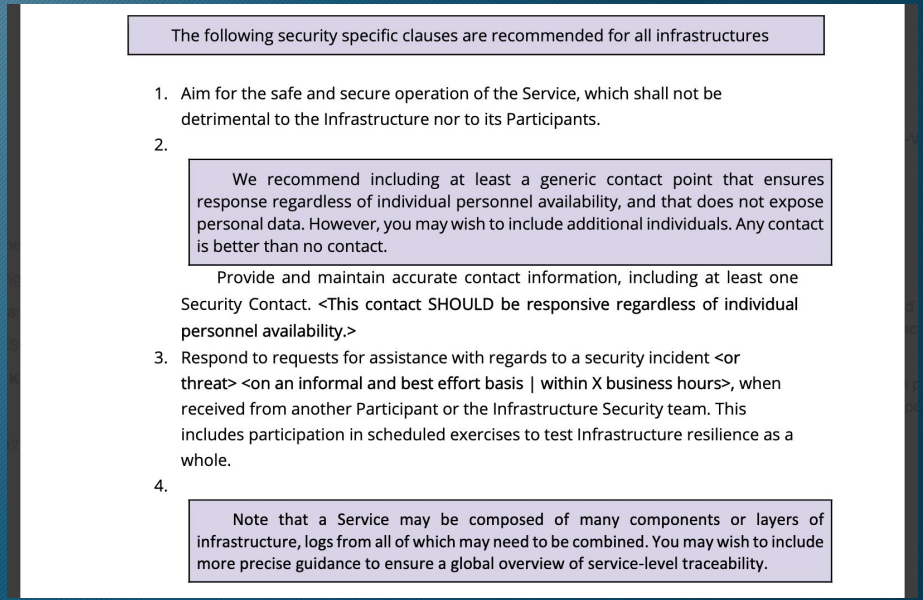
Part of the generic WISE-AARC Policy Development Kit

Version 2, 20 Apr 2022

Authors: Members of the WISE Community SCI Working Group, particularly:

Linda Cornwall (UKRI), David Crooks (UKRI), Thomas Dack (UKRI), Sven Gabriel (Nikhef), Baptiste Grenier (EGI Foundation), David Groep (Nikhef), David Kelsey (UKRI), Maarten Kremers (SURF), Alf Moens (GEANT), Ian Neilson (UKRI), Ralph Niederberger (FZJ), Hannah Short (CERN), Uros Stevanovic (KIT), Romain Wartel (CERN)

e-mail: sci-wg@lists.wise-community.org



The following security specific clauses are recommended for all infrastructures

1. Aim for the safe and secure operation of the Service, which shall not be detrimental to the Infrastructure nor to its Participants.
2.

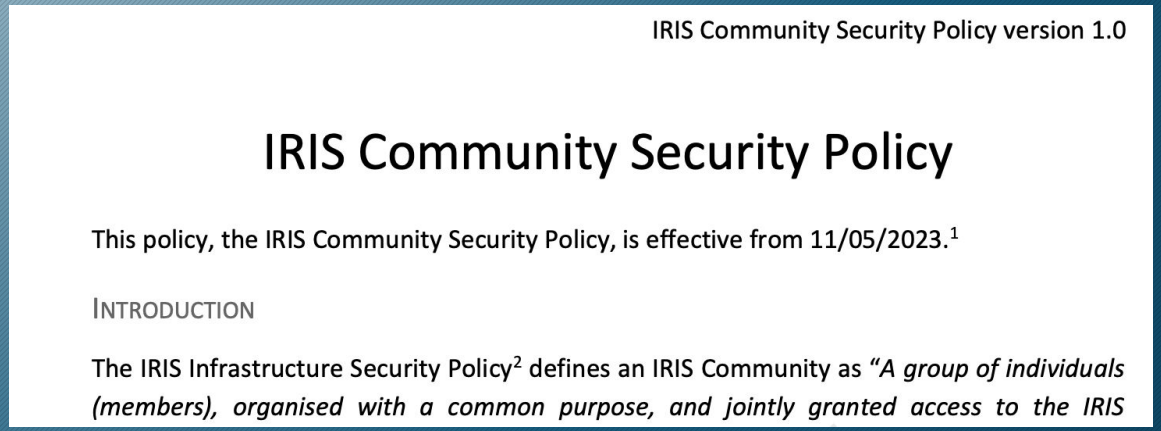
   We recommend including at least a generic contact point that ensures response regardless of individual personnel availability, and that does not expose personal data. However, you may wish to include additional individuals. Any contact is better than no contact.

   Provide and maintain accurate contact information, including at least one Security Contact. <This contact SHOULD be responsive regardless of individual personnel availability.>
3. Respond to requests for assistance with regards to a security incident <or threat> <on an informal and best effort basis | within X business hours>, when received from another Participant or the Infrastructure Security team. This includes participation in scheduled exercises to test Infrastructure resilience as a whole.
4.

   Note that a Service may be composed of many components or layers of infrastructure, logs from all of which may need to be combined. You may wish to include more precise guidance to ensure a global overview of service-level traceability.

Community Security Policy – new PDK template (work in progress)

- STFC IRIS (UK) has produced new policy (approved – May 2023)
- Based on combining two policies (AARC PDK & EGI security policy)
  - Community Membership Management Policy & VO Operations Policy
- To be used as input to WISE SCI work on an updated AARC template



IRIS Community Security Policy version 1.0

IRIS Community Security Policy

This policy, the IRIS Community Security Policy, is effective from 11/05/2023.[1]

INTRODUCTION

The IRIS Infrastructure Security Policy[2] defines an IRIS Community as *"A group of individuals (members), organised with a common purpose, and jointly granted access to the IRIS*

More information - PDK

The original AARC PDK: https://aarc-community.org/policies/policy-development-kit/

- AARC guidance documents on policy: https://aarc-project.eu/guidelines/#policy

WISE Community: https://wise-community.org/

- WISE SCI-WG – Wiki - https://wiki.geant.org/display/WISE/SCI-WG
- WISE SCI-WG PDK updates - https://wiki.geant.org/display/WISE/Policy+Development+Kit

Join WISE mail list: https://lists.wise-community.org/sympa/info/wise
Join WISE SCI-WG: https://lists.wise-community.org/sympa/subscribe/sci-wg

The Future – AARC TREE project (2024-2026) – subject to contract

- Authentication and Authorisation for Research Collaboration Technical Revision to Enhance Effectiveness
- Contract negotiation with the European Commission – likely to start early 2024 and run for two years
- Objectives include:
  - New Authentication and Authorisation interoperability requirements
    - provide a landscape analysis of AAIs services (including gaps)
  - Define and validate new technical and policy guidelines for the AARC BPA that address RIs use-cases
  - Expand the number of research communities that can implement the AARC BPA and/or the AARC guidelines, by providing a validation environment and toolkits
  - Bring RIs, e-Infrastructures and relevant stakeholders together to align strategies to integrate new technologies, better interoperate and share resources
    - produce a compendium and recommendations for different stakeholders
- Need to target small and medium research communities, simplify the AARC PDK, establish Trust and Interoperability where multiple proxies are connected (see next slide)
- FIM4R.org seen as an important place to discuss and establish requirements
  - Work will be done in an open environment – all are welcome!

Federated Identity Management for Research (FIM4R)

- *FIM4R is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research cyber infrastructures*
- FIM4R version 1 paper – 2012
- FIM4R version 2 paper – 2018
- *http://doi.org/10.5281/zenodo.1296031*
  - Published on 9 July 2018

Federated Identity Management for Research Collaborations

C J Atherton[1], T Barton[2], J Basney[3], D Broeder[4], A Costa[5], M van Daalen[6], S O M Dyke[7], W Elbers[8], C-F Enell[9], E M V Fasanelli[10], J Fernandes[11], L Florio[1], P Gietz[12], D L Groep[13], M Junker[10], C Kanellopoulos[1], D P Kelsey[14], P J Kershaw[14,15], C Knapic[5], T Kollegger[16], S Koranda[17], M Linden[18], F Marinic[19], L Matyska[20], T H Nyrönen[18], S Paetow[21], L Paglione[22], S Parlati[10], C Phillips[23], M Prochazka[20,24], N Rees[25], H Short[11], U Stevanovic[26], M Tartakovsky[27], G Venekamp[28], T Vitez[23], R Wartel[11], C Whalen[27], J White[29] and C Zwölf[30]

[1]GÉANT Association, Amsterdam, The Netherlands; [2]University of Chicago, Chicago, Illinois, USA; [3]National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign, USA; [4]Meertens Institute, Amsterdam, The Netherlands; [5]INAF- National Institute for Astrophysics - Italy; [6]Paul Scherrer Institute, 5232 Villigen PSI, Switzerland; [7]McGill University, Montreal, Canada; [8]CLARIN ERIC, Utrecht, The Netherlands; [9]EISCAT Scientific Association, Kiruna, Sweden; [10]INFN - National Institute for Nuclear Physics - Italy; [11]European Organization for Nuclear Research (CERN), Geneva, Switzerland; [12]DAASI International, Tübingen, Germany; [13]Nikhef, Amsterdam, The Netherlands; [14]STFC UK Research and Innovation, Rutherford Appleton Laboratory, Didcot, United Kingdom; [15]NCEO (National Centre for Earth Observation), NERC, United Kingdom; [16]GSI Helmholtzzentrum für Schwerionenforschung, Darmstadt, Germany; [17]University of Wisconsin-Milwaukee (UWM), Milwaukee, Wisconsin USA; [18]CSC – IT Center for Science, ESPOO, Finland; [19]European Space Agency (ESA/ESAC), Madrid, Spain; [20]Masaryk University (MU), Institute of Computer Science (ICS), Brno, Czech Republic; [21]Jisc, Harwell, United Kingdom; [22]ORCID Inc, Bethesda, Maryland USA; [23]CANARIE, Ottawa, Canada; [24]CESNET, Prague, Czech Republic; [25]SKA Organisation, Jodrell Bank, Lower Withington, Macclesfield, United Kingdom; [26]Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany; [27]National Institute of Allergy and Infectious Diseases, Rockville, Maryland USA; [28]SURFsara, Amsterdam, The Netherlands; [29]NeIC, Oslo, Norway; [30]Observatoire de Paris (Obspm), France

ABSTRACT

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

“Every researcher is entitled to focus on their work and not be impeded by needless obstacles nor required to understand anything about the FIM infrastructure enabling their access to research services.” **FIM4R version 2**

FIM4R - Who is represented?

Research Fields (14)

- Arts and Humanities
- Climate Science
- Earth Observation
- European Neutron and Photon Facilities
- Gamma-Ray Astronomy
- Gravitational Wave Astronomy
- High Energy Physics
- Ionospheric and Atmospheric Science
- Infectious Disease Research
- Life Sciences
- Linguistics
- Nuclear Physics
- Radio Astronomy
- Virtual Atomic and Molecular Data Centre

Others

Research Driven Services

- HNSciCloud
- ORCID

Identity Federation Projects/Communities

- AARC(2)
- GÉANT-GN4
- InCommon/Internet2
- REFEDS

Related activities in WLCG - but not just for WLCG

- *AuthZ working group*
  - Implement use of tokens (move from X.509 certificates)
  - Some policy and trust but mainly delegated to TTT group
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG
- *Resource Trust Evolution task force*
  - Which CA's can be used in cloud storage?
  - https://twiki.cern.ch/twiki/bin/view/LCG/ResourceTrustEvolution
- *Token Trust and Traceability (TTT) working group*
  - Answer security questions in various kinds of documentation
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGTokenTrustTraceability

Science and Technology Facilities Council

WLCG Security Policy

https://wlcg.web.cern.ch/using-wlcg/computer-security

Policies

WLCG participants are bound by a set of security policies, that are approved by the Management Board:

Top-level Grid Security Policy:

- e-Infrastructure Security Policy (Updated 1 Feb 2017)

General policies:

- WLCG Privacy Notice (16 July 2019)
- Security Incident Response Policy (Updated 14 Nov 2016)
- Security Traceability and Logging Policy (Updated 14 Nov 2016)
- Policy on the Processing of Personal Data (Updated 1 Feb 2017)
- Policy on Acceptable Authentication Assurance (Updated 1 Feb 2017)
- Policy on e-Infrastructure Multi-User Pilot Jobs (Updated 14 Nov 2016)
- Grid Policy on the Handling of User-Level Job Accounting Data (Updated 19 Mar 2013)

For all Users:

- Acceptable Use Policy and Conditions of Use (Updated 10 Oct 2016)

Science and Technology Facilities Council

WLCG - too many policies & need updating

For all Sites:

- Service Operations Policy (Updated 1 Jun 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images (Updated 10 Oct 2016)

For all VOs:

- VO Operations Policy (Updated 13 Jul 2010)
- Virtual Organisation Registration Security Policy (Updated 13 Jul 2010)
- Virtual Organisation Membership Management Policy (Updated 13 Jul 2010)
- VO Portal Policy (Updated 14 Nov 2016)
- Service Operations Security Policy (Updated 1 June 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images (Updated 10 Oct 2016)

Glossary of terms used in JSPG policy documents:

- Security Policy Glossary of Terms (Update 08 Mar 2011)

Future plans

- AARC TREE starts (March 2024)
  - further develop PDK and Guidance and SCI/Snctfi trust frameworks
- FIM4R meeting to discuss Research Community requirements
  - Copenhagen - Tuesday 30 Jan 2024 (as part of TIIME meeting)
  - https://indico.cern.ch/event/1325302/
  - https://tiime-unconference.eu/
- EGI and EOSC have already used the new templates
- WLCG needs to do the same
  - Simplification and revision of the WLCG policy set
- As ever - the work will be useful for other Research Communities too
  - Not just for WLCG
- Volunteers very welcome to join the Policy group

Science and Technology Facilities Council

Questions?

Science and Technology Facilities Council