Beyond AARC

EnCo global engagement activities and the AARC-community.org

David Groep

EnCo *eScience Global Engagement*

Nikhef, PDP

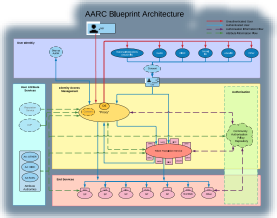
EUGridPMA46, EnCo, EOSCH-ISM, AARC

20-22 May, 2019

The AARC 'legacy' – the AARC community

Architecture

- Blueprint BPA and the Proxy gudelines
- Application Integration
- AEGIS and a lively FIM4R



Alignment with & between range of
policy development groups dedicated to interoperation

- WISE-community
- IGTF
- REFEDS
- FIM4R
- GN4 EnCo eSGE
- EOSCH-ISM

Policy Development Kit

Accessing, using, and operating services for research in today's world, as a rule, is inherently distributed, where users access resources outside their home organisations. In this complex environment, the question of trust for users, resource providers, and infrastructures, becomes paramount.

A set of policy documents is necessary to regulate and facilitate this trust. These policies outline the operational measures undertaken by the infrastructure to properly provide services. The policies principally cover security measures, user management and data protection.

What is the Policy Development Kit?

This material is provided to support Research Infrastructures in adopting or enhancing a policy set that regulates the operation and use of an authentication and authorisation infrastructure in line with the AARC Blueprint Architecture. The policies are there to provide a starting point, so that Research Infrastructures do not have to re-invent the wheel.

Start with AARC

More on AAI

WISE-community

IGTF

REFEDS

FIM4R

AEGIS

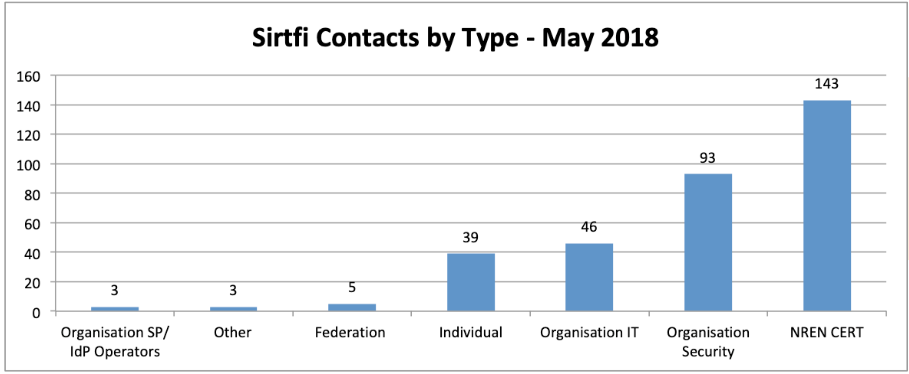
Collaboration EOSCH-GN4

national, domain and community groups

So much to do, so few people, …

- *Sirtfi & the Registry*
- *Communications Challenges*
- *Attribute Authority operations*
- *SCI evolution and its assessment to support trust*
- *Acceptable Use Policy*
- *Assurance profiles: adoption & suitability in high-risk cases*
- *Policy Development Kit evolution*
- *Data Protection guidance for global research collaboration*

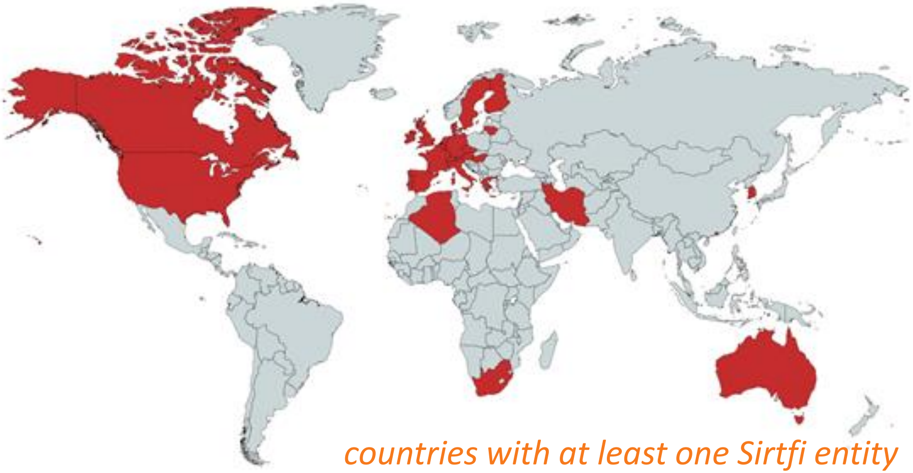
Sirtfi is there today – 561 parties (406 IdPs) joined, in 28 federations



SIRTFI
Security Incident Response Trust Framework for Federated Identity

Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration



countries with at least one Sirtfi entity

IAM Online Europe

IAM Online Europe webinars are broug

iamonlineEU 001 Sirtfi
IamOnline
38 views • 4 days ago

https://refeds.org/SIRTFI REFEDS > SIRTFI

Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response nisations. This assurance framework comprises a list of assertions which an organisation can attest in order mpliant. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response

Group has been active since 2014 and combines expertise in operational security and incident response pol- FEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC

Benefits
Why should I join? What are the Benefits?

Sirtfi v 1.0
View the Sirtfi Framework

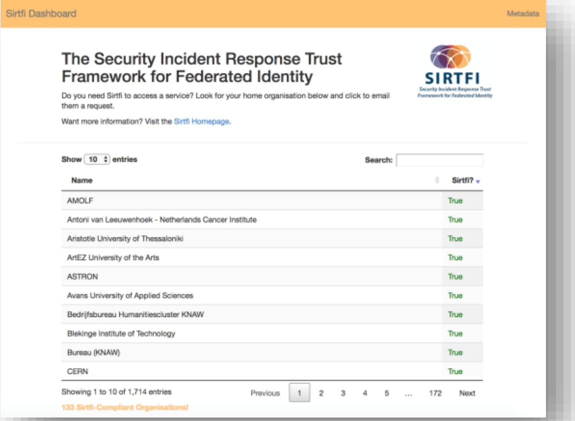
FAQs
Need help?

graphics source: AARC2 DNA3.2 Report on Incident Response in FIM; data: technical.edugain.org

Promoting Sirtfi: through REFEDS and communities

Sirtfi ‘encouragement’

- the tool certainly raises attention ☺
- lack-of-Sirtfi (and R&S) is non-trivial to diagnose – other causes may interfere



Sirtfi Dashboard
Metadata
SIRTFI
Security Incident Response Trust Framework for Federated Identity

The Security Incident Response Trust Framework for Federated Identity

Do you need Sirtfi to access a service? Look for your home organisation below and click to email them a request.

Want more information? Visit the Sirtfi Homepage.

Show 10 entries Search:

Name	Sirtfi?
AMOLF	True
Antoni van Leeuwenhoek - Netherlands Cancer Institute	True
Aristotle University of Thessaloniki	True
ArtEZ University of the Arts	True
ASTRON	True
Avans University of Applied Sciences	True
Bedrijfsbureau Humanitiescluster KNAW	True
Blekinge Institute of Technology	True
Bureau (KNAW)	True
CERN	True

Showing 1 to 10 of 1,714 entries

133 Sirtfi-Compliant Organisations!

https://sirtfi.cern.ch/

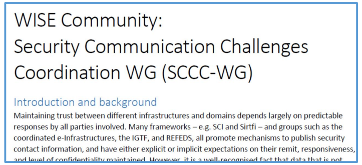
Sirtfi+ registry

- enabling more entities to express Sirtfi
- allow sharing of implicit trust between communities?
- tool requirements (lead by Laura et al.)

Incident Response procedures for R&E Fed

- AARC-I051 white paper guidance (based on challenges)
- Good resource: SANS Incident Handlers Handbook
  - Refer to SANS incident handling notes for a check on how our proposed preparations stack up against the SANS recommendation.
  - What should be added?
  - What should be removed?
  - What should be altered? Make comments/edits in the doc.
- handbook approach to the IR in R&E Feds

Testing incident response coordination

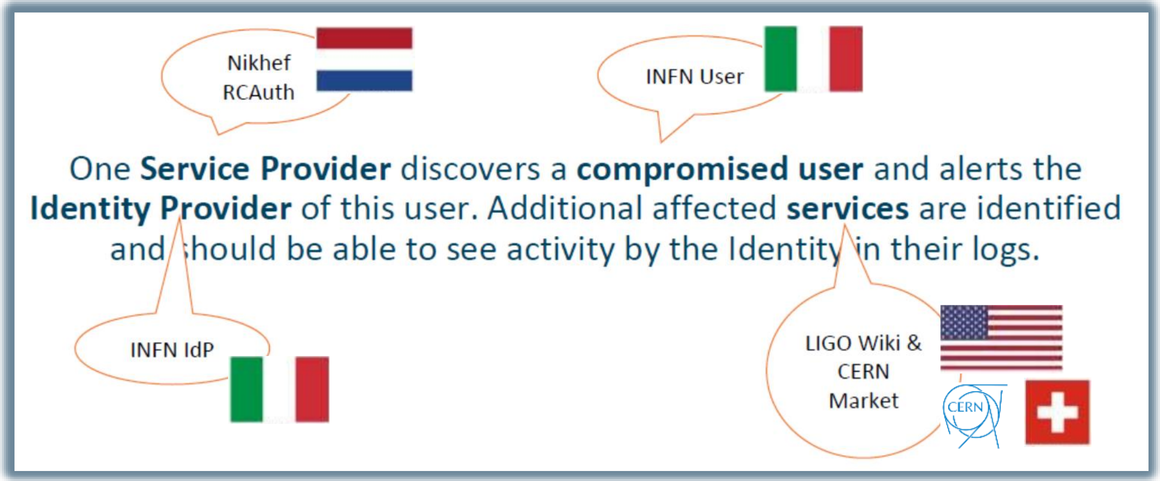


WISE Community:
Security Communication Challenges
Coordination WG (SCCC-WG)

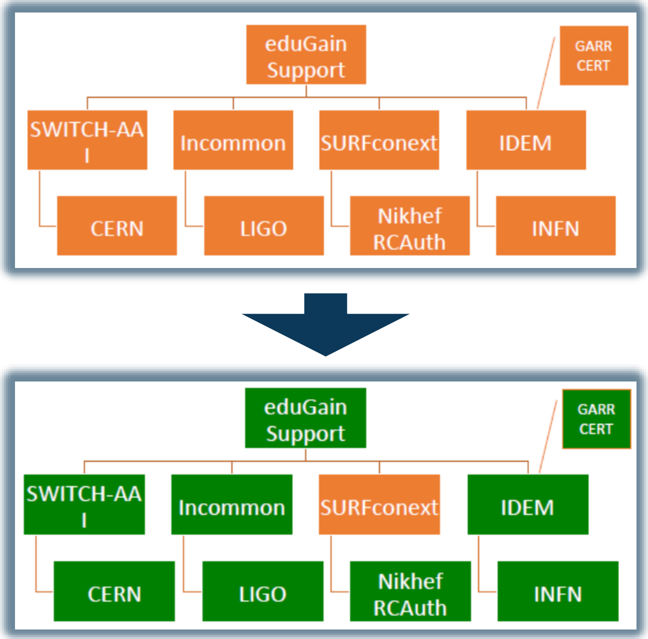
Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

- Can we coordinate our collective R&E response?
- Communication guidelines to help timely resolution?
- Two ‘challenges’: **March 2018** and **December 2018**



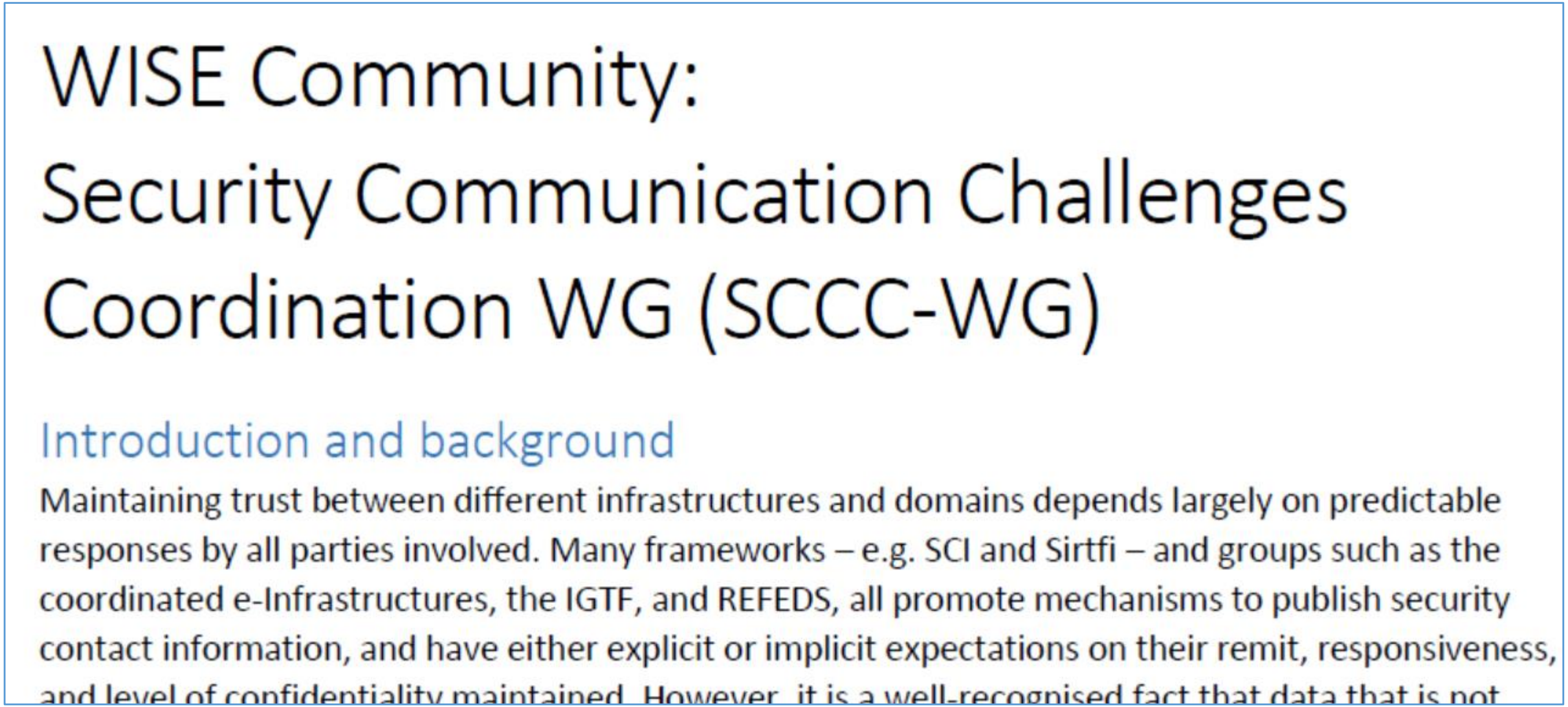
One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.



parties involved in response challenge

Report-outs see **https://wiki.geant.org/display/AARC/Sirtfi+Communications+Challenges%2C+AARC2-TNA3.1**

SCCC JWG



WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

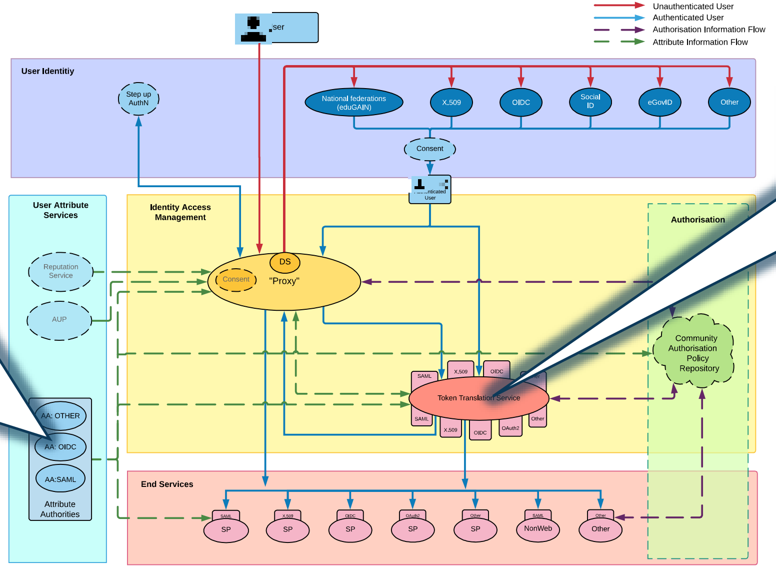
Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

Operational security focus in the BPA: beyond just the IdPs

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity

AARC Blueprint Architecture



Store and manage ephemeral user credentials

- trusted credential stores
- protection at rest

IGTF Guidelines on Trusted Credential Stores *(pre-existing)*

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements *(AARC-I048, in collaboration with IGTF AAOPS)*

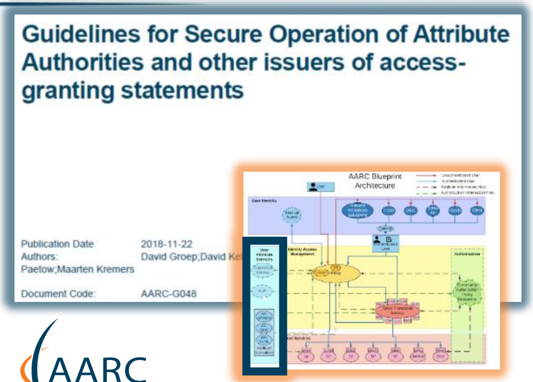
AARC-G048: keeping users & communities protected, moving across models

trusted delegation of response from communities to operators, and from services to communities in recognizing their assertions

Structured around concept of “**AA Operators**”,

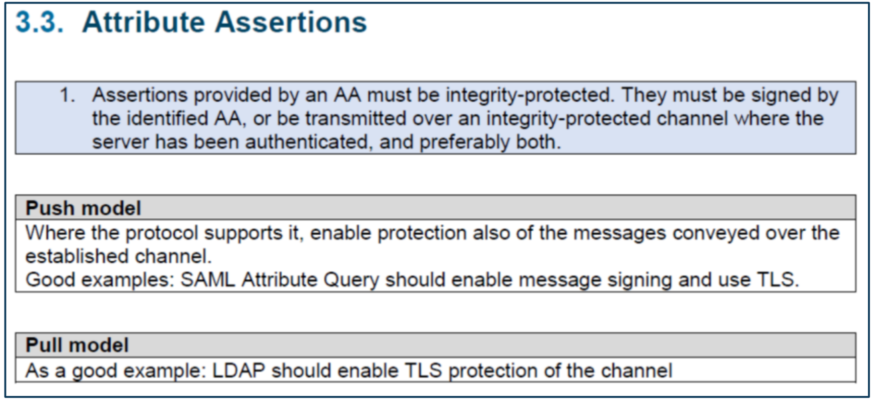
operating “**Attribute Authorities**” (technological entities),

on behalf of, one or more, **Communities**



Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements

Publication Date 2018-11-22
Authors: David Groep;David Ke
Paetow;Maarten Kremers
Document Code: AARC-G048

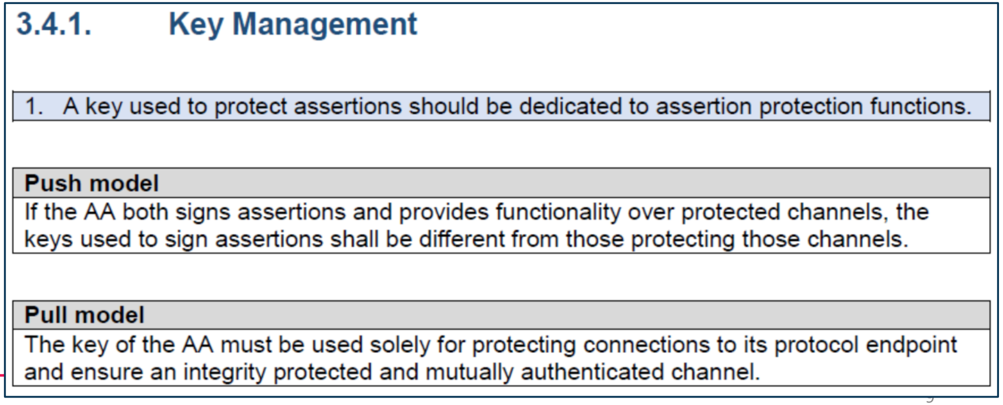


3.3. Attribute Assertions

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model
Where the protocol supports it, enable protection also of the messages conveyed over the established channel. Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model
As a good example: LDAP should enable TLS protection of the channel



3.4.1. Key Management

1. A key used to protect assertions should be dedicated to assertion protection functions.

Push model
If the AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting those channels.

Pull model
The key of the AA must be used solely for protecting connections to its protocol endpoint and ensure an integrity protected and mutually authenticated channel.

AAOPS – engaging with the community AAIs and AASPs

usual targets to assess feasibility of the framework

- WLCG
- CheckIn
- eduTEAMS

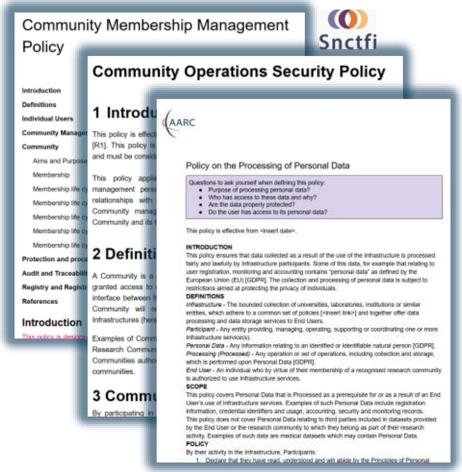
then evolve, expand, or explain and give as guidance to all communities?

SCI – assessment, policy development, AUP, PDK

SCIv2 paper itself discussed assessment – start it!

Level 0 ..3 or "Justifiable exclusion"

Policy Development Kit



Community Membership Management Policy

Introduction
Definitions
Individual Users
Community Manager
Community
Aims and Purpose
Membership
Membership life cy
Membership life cy
Membership life cy
Membership life cy
Membership life cy
Protection and proce
Audit and Traceabilit
Registry and Registr
References

Introduction

This policy is design

Community Operations Security Policy

1 Introdu

This policy is effecti
[R1]. This policy is
and must be conside

This policy applie
management perso
relationships with
Community manag
Community and its U

2 Definiti

A Community is a
granted access to
interface between t
Community will n
Infrastructures (here

Examples of Comm
Research Commun
Communities autho
communities.

3 Commu

By participating in

Policy on the Processing of Personal Data

Questions to ask yourself when defining this policy:

- Purpose of processing personal data?
- Who has access to these data and why?
- Are the data properly protected?
- Do the user has access to its personal data?

This policy is effective from <insert date>.

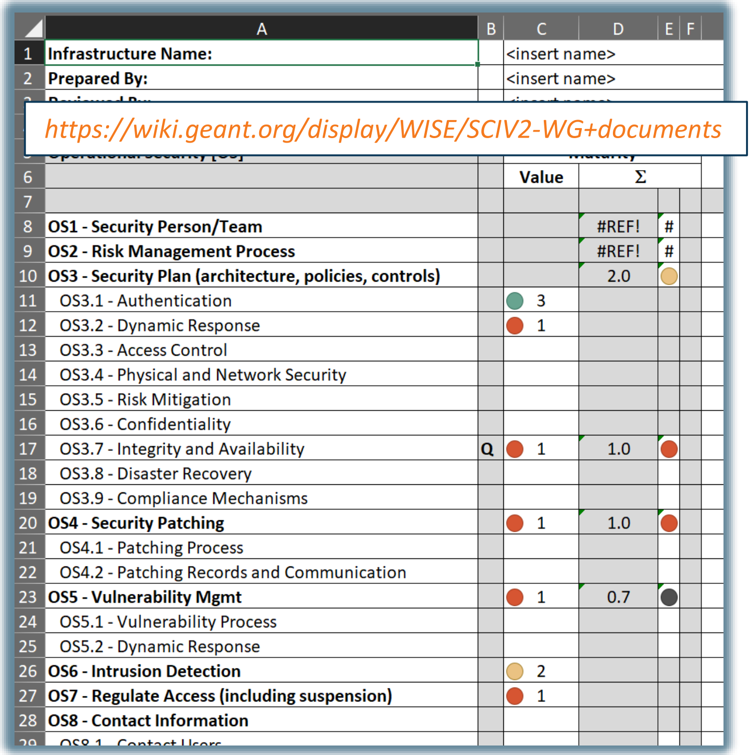
INTRODUCTION
This policy ensures that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of this data, for example that relating to user registration, monitoring and accounting contains "personal data" as defined by the European Union (EU) [GDPR]. The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

DEFINITIONS
Infrastructure - The bounded collection of universities, laboratories, institutions or similar entities, which adhere to a common set of policies [<insert link>] and together offer data processing and data storage services to End Users.
Participant - Any entity providing, managing, operating, supporting or coordinating one or more Infrastructure service(s).
Personal Data - Any information relating to an identified or identifiable natural person [GDPR].
Processing (Processed) - Any operation or set of operations, including collection and storage, which is performed upon Personal Data [GDPR].
End User - An individual who by virtue of their membership of a recognised research community is authorized to use Infrastructure services.

SCOPE
This policy covers Personal Data that is Processed as a prerequisite for or as a result of an End User's use of Infrastructure services. Examples of such Personal Data include registration information, credential identifiers and usage, accounting, security and monitoring records. This policy does not cover Personal Data relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.

POLICY
By their activity in the Infrastructure, Participants:

1. Declare that they have read, understood and will abide by the Principles of Personal

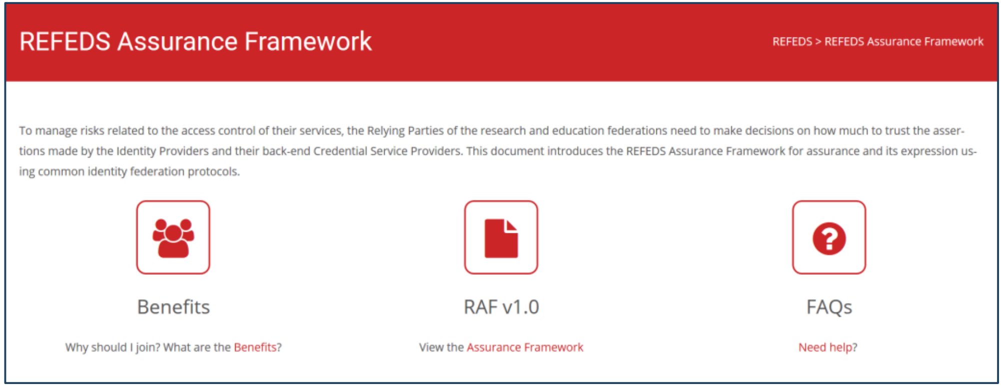


	A	B	C	D	E	F
1	**Infrastructure Name:**		<insert name>			
2	**Prepared By:**		<insert name>			
3	**Reviewed By:**		<insert name>			
4						
5	**Operational Security [OS]**			**Maturity**		
6			**Value**	Σ		
7						
8	**OS1 - Security Person/Team**			#REF!	#	
9	**OS2 - Risk Management Process**			#REF!	#	
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					
25	OS5.2 - Dynamic Response					
26	**OS6 - Intrusion Detection**		🟡 2			
27	**OS7 - Regulate Access (including suspension)**		🔴 1			
28	**OS8 - Contact Information**					
29	OS8.1 - Contact Users					

https://wiki.geant.org/display/WISE/SCIV2-WG+documents

http://wise-community.org/sci/

Assurance: REFEDS RAF, RAF adoption, …



REFEDS Assurance Framework

REFEDS > REFEDS Assurance Framework

To manage risks related to the access control of their services, the Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers and their back-end Credential Service Providers. This document introduces the REFEDS Assurance Framework for assurance and its expression using common identity federation protocols.

Benefits

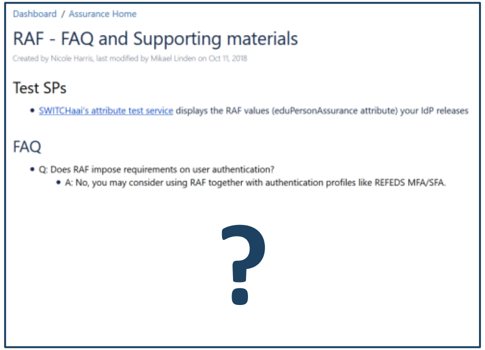
Why should I join? What are the Benefits?

RAF v1.0

View the Assurance Framework

FAQs

Need help?



Dashboard / Assurance Home

RAF - FAQ and Supporting materials

Created by Nicole Harris, last modified by Mikael Linden on Oct 11, 2018

Test SPs

- SWITCHaai's attribute test service displays the RAF values (eduPersonAssurance attribute) your IdP releases

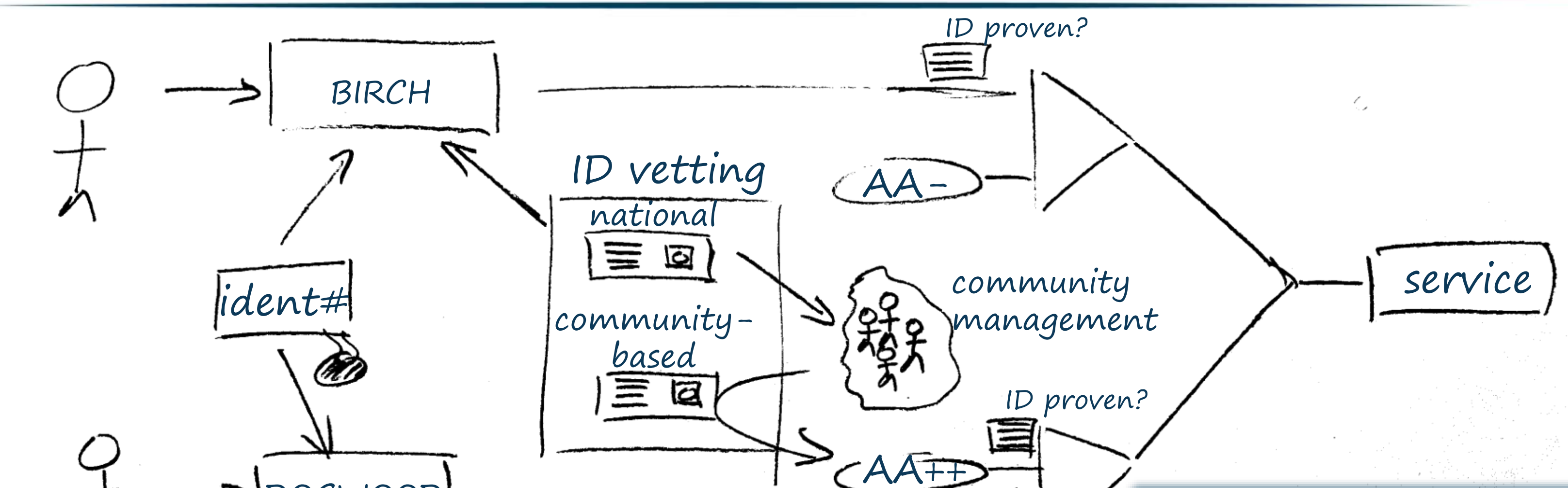
FAQ

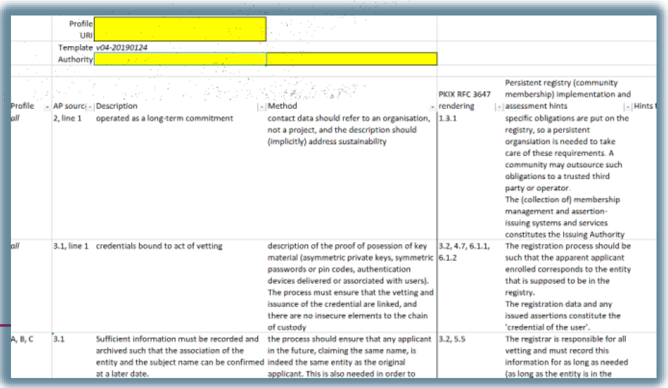
- Q: Does RAF impose requirements on user authentication?
  - A: No, you may consider using RAF together with authentication profiles like REFEDS MFA/SFA.

?

- We have the framework, we have a few good use cases (CILogon Silver, BBMRI)
- How to break the deadlock for adoption?
- More guidance, both on the IdP side (how) and SP side (why should I require,request it)?

Example: Acceptable Authentication Assurance – enabling flexible user communities by mapping assurance elements





Profile URI	
Template	*v04-20190124*
Authority	

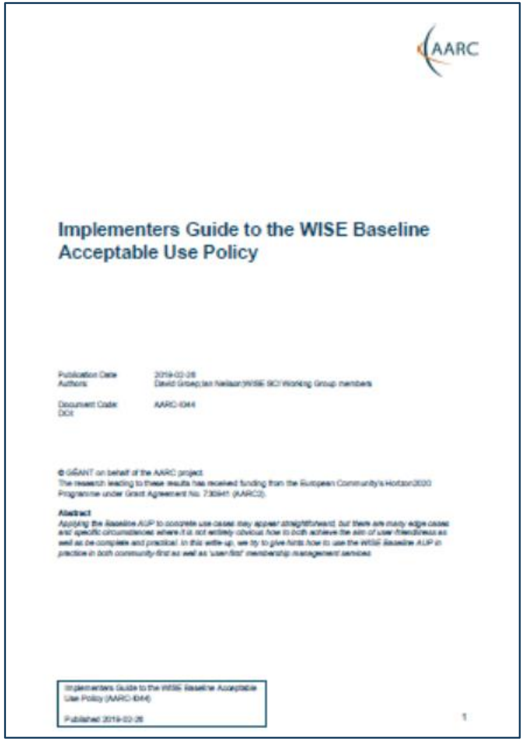
Profile	AP sourc	Description	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints
all	2, line 1	operated as a long-term commitment	contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organsiation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. The (collection of) membership management and assertion-issuing systems and services constitutes the Issuing Authority	
all	3.1, line 1	credentials bound to act of vetting	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or assorciated with users). The process must ensure that the vetting and issuance of the credential are linked, and there are no insecure elements to the chain of custody	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'credential of the user'.	
A, B, C	3.1	Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date.	the process should ensure that any applicant in the future, claiming the same name, is indeed the same entity as the original applicant. This is also needed in order to	3.2, 5.5	The registrar is responsible for all vetting and must record this information for as long as needed (as long as the entity is in the	

Identity vetting can be done

- when credentialing the user
- on enrolling the user in a community

e.g. *LIGO LSC* always does researcher vetting, and Assurance Policy accommodates linkage in either place – still meeting SP trust needs

Community guidance: GDPR, privacy notices, implementation guidance



Implementers Guide to the WISE Baseline Acceptable Use Policy

Publication Date	2019-02-26
Authors	David Groep;Ian Neilson;WISE SCI Working Group members
Document Code	AARC-I044
DOI	

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

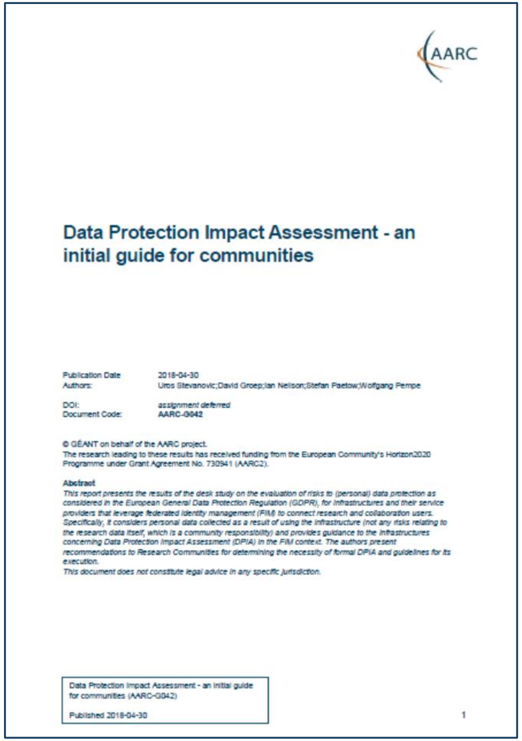
Abstract

Applying the Baseline AUP to concrete use cases may appear straightforward, but there are many edge cases and specific circumstances where it is not entirely obvious how to both achieve the aim of user friendliness as well as be complete and practical. In this write-up, we try to give hints how to use the WISE Baseline AUP in practice in both community-first as well as 'user-first' membership management services.

Implementers Guide to the WISE Baseline Acceptable Use Policy (AARC-I044)

Published 2019-02-26

1



Data Protection Impact Assessment - an initial guide for communities

Publication Date	2018-04-30
Authors:	Uros Stevanovic;David Groep;Ian Neilson;Stefan Paetow;Wolfgang Pempe
DOI:	*assignment deferred*
Document Code:	**AARC-G042**

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

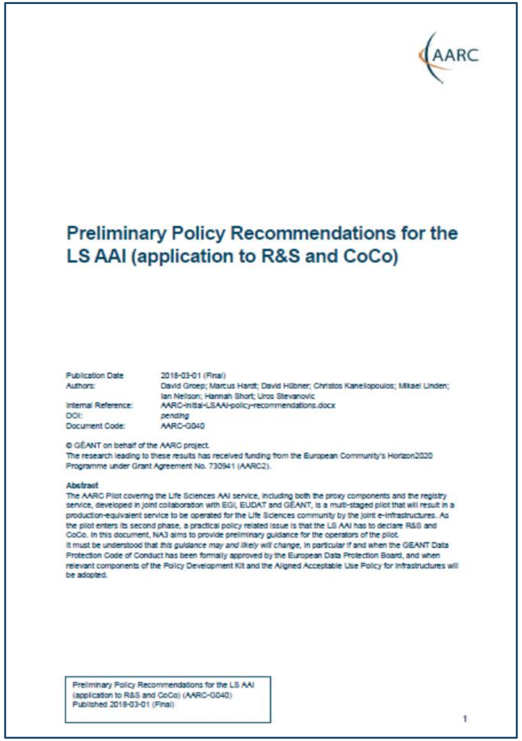
Abstract

This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European General Data Protection Regulation (GDPR), for infrastructures and their service providers that leverage federated identity management (FIM) to connect research and collaboration users. Specifically, it considers personal data collected as a result of using the infrastructure (not any risks relating to the research data itself, which is a community responsibility) and provides guidance to the infrastructures concerning Data Protection Impact Assessment (DPIA) in the FIM context. The authors present recommendations to Research Communities for determining the necessity of formal DPIA and guidelines for its execution.
This document does not constitute legal advice in any specific jurisdiction.

Data Protection Impact Assessment - an initial guide for communities (AARC-G042)

Published 2018-04-30

1



Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date	2018-03-01 (Final)
Authors:	David Groep; Marcus Hardt; David Hübner; Christos Kanellopoulos; Mikael Linden; Ian Neilson; Hannah Short; Uros Stevanovic
Internal Reference:	AARC-initial-LSAAI-policy-recommendations.docx
DOI:	*pending*
Document Code:	AARC-G040

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

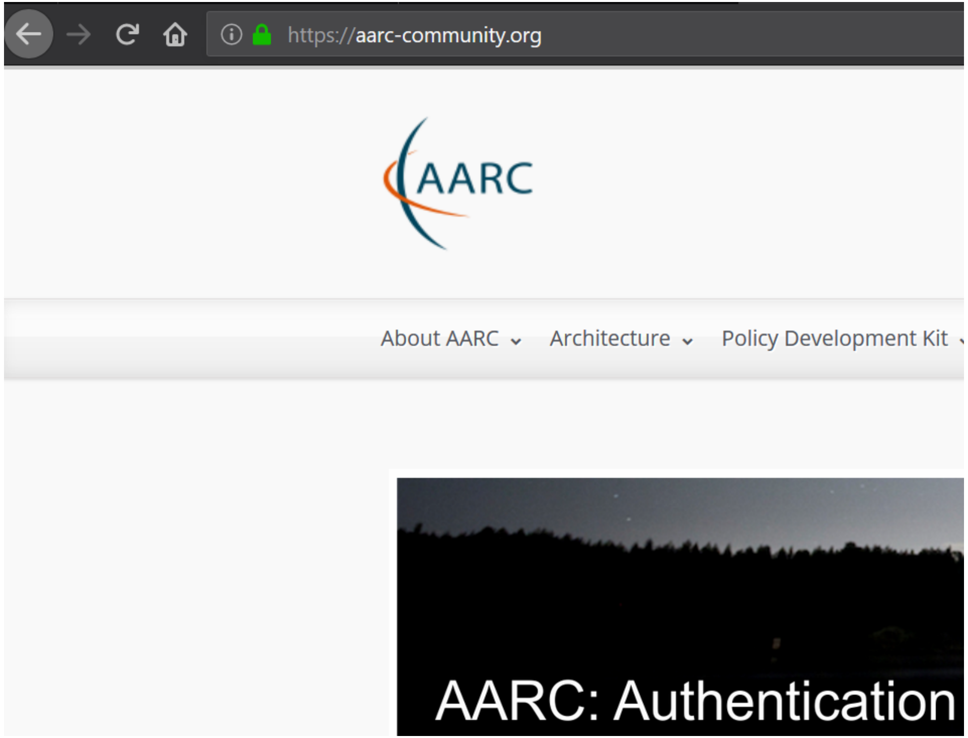
The AARC Pilot covering the Life Sciences AAI service, including both the proxy components and the registry service, developed in joint collaboration with EGI, EUDAT and GÉANT, is a multi-staged pilot that will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-infrastructures. As the pilot enters its second phase, a practical policy related issue is that the LS AAI has to declare R&S and CoCo. In this document, NA3 aims to provide preliminary guidance for the operators of the pilot.
It must be understood that *this guidance may and likely will change*, in particular if and when the GEANT Data Protection Code of Conduct has been formally approved by the European Data Protection Board, and when relevant components of the Policy Development Kit and the Aligned Acceptable Use Policy for Infrastructures will be adopted.

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo) (AARC-G040)
Published 2018-03-01 (Final)

1

...

AARC-community.org: AARC forever!



https://aarc-community.org

AARC

for now just a reverse proxy for aarc-project.eu …

Thank you

davidg@nikhef.nl

GÉANT

Networks · Services · People
www.geant.org

This work is part of a project that has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).