AARC Policy and Best Practice

supporting the FIM and e-Infra communities

David Groep
AARC AEGIS policy area coordinator
Nikhef

FIM4R Vienna
February 2020

Making the proxy behave: infrastructure and community policy support

aarc-community.org/guidelines

Trust and global policy

A single policy cannot apply

- different risk scenarios for participants,
- different risk appreciation,
- distinct legal contexts, …

But one can 'map' policies and align policy structures

"enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks."

which is the role of SCI - Security for Collaboration among Infrastructures
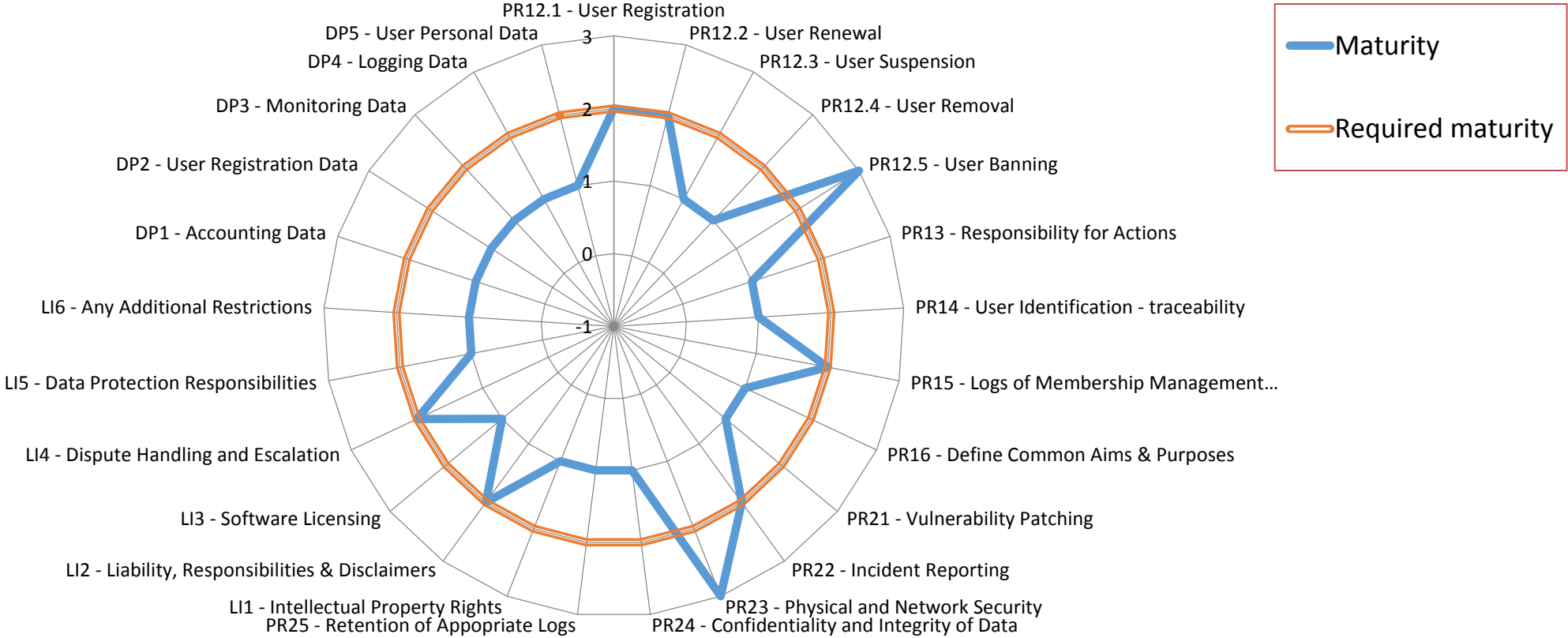
Determining interoperable risk profiles
for collaborating infrastructures and services

concept in SCI context: Urpo Kaila

Baseline AUP at WISE SCI

The WISE Baseline Acceptable Use Policy and Conditions of Use
Version 1.0.1 (draft), 25 Feb 2019

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

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/

Other Sources / Attribution / Acknowledgements: "EGI Acceptable Use Policy and Conditions of Use", used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

DRAFT WISE Baseline AUP template v1.0.1

When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text

- **shown only once** to user during registration

- information on *expected behaviour* and restrictions

- **can *optionally* be augmented** with
  additional community or infrastructure specific clauses

- registration point may be operated directly by research community or by third party on community's behalf

Other information shown to user during registration

- *Privacy Notice* – information about processing & user rights

- *Service Level Agreements* – information about what user
  can expect from the service in terms of 'quality'

- *Terms of Service* – optional, with the 'benefits' to the user

https://aarc-community.org/guidelines/aarc-i044/

https://wiki.geant.org/display/WISE/Baseline+Acceptable+Use+Policy+and+Conditions+of+Use

Evolving the policy development kit >>> Smplfy the structure

Operational policies
- Acceptance Authentication
- Data Privacy Policy
- Accounting Data Protection
- Service Operations
- Traceability & Logging

Sui generis policies
- Access Platform (LToS) AUP & Conditions
- Access Platform (LToS) specific security controls
- MU Pilot Jobs
- VO Portal Policy
- VM Endorsement

User Community & User Policies
- Community Membership
- Community Security
- Community purpose binding
- Acceptable Use Policy

Snctfi

Top-Level Security Policy

compact but comprehensive top-level policy

risk-classification driven policy requirements

supported by implementation measure that can be defined as needed

Conveying Assurance and Profiles in practice – at the IGTF: XSEDE & FNAL

Questions to ask yourself when defining this policy:
- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook etc?
- How much certainty does your community require of the identity? Review each of the elements (personal accounts, uniqueness, freshness, vetting quality, and authentication strength). How will you validate this for each source of (federated) identity?
- How can you ensure that each user is covered by a security incident response capability at their home organisation?
- Do your services, or a subset, require step-up (multi-factor) authentication?

The following chart can be used to help determine an appropriate assurance profile for you. Refer also to AARC Guideline 21:

| Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

AARC Assam
IGTF Dogwood
RAF Cappuccino
IGTF Birch
RAF Espresso

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
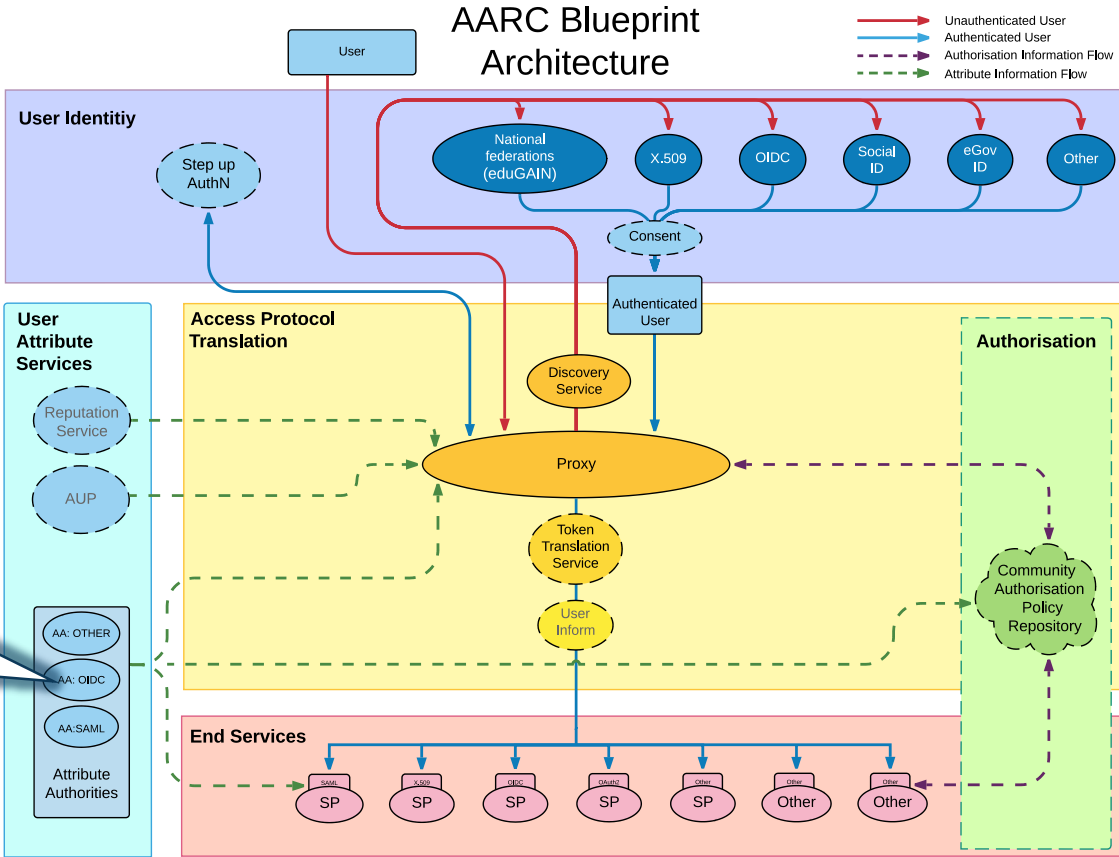
AARC Blueprint Architecture

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

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

Publication Date   2018-11-22
Authors: David Groep;David Kel...
Paetow;Maarten Kremers

Document Code: AARC-G048

Structured around concept of "**AA Operators**",

operating "**Attribute Authorities**" (technological entities),

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

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 ... established channel.
Good examples: SAML Attribute Query should enable me...

Pull model

As a good example ... ... or the channel

3.4.1.   Key Management

1. A key used ... ...icated to assertion protection functions.

... ... 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.

contribute: validate it with current implementations

https://aarc-community.org

https://www.igtf.net/guidelines/aaops/

https://aarc-community.org/guidelines/aarc-g048/

Security Incident Response in the Federated World

many countries & economic regions with an R&E identity federation

full of valuable resources
(data, network, services)
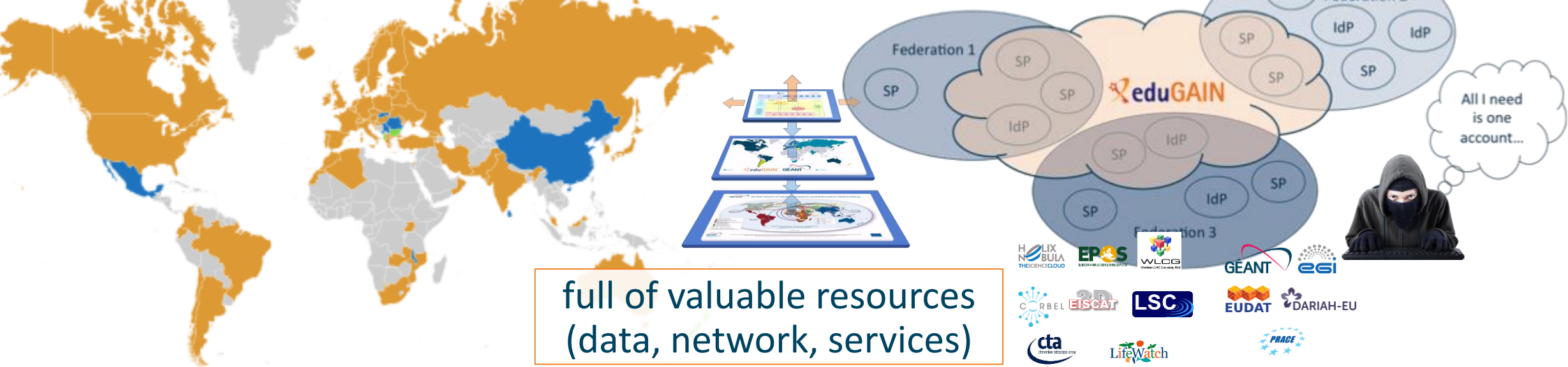
Could we ensure that information is shared confidentially, and reputations protected?

Security Incident Response Trust Framework for Federated Identity

Sirtfi – *based on Security for Collaborating Infrastructures (SCI) & FIM4R Recommendations*

Communications Challenges

Based on *Sirtfi* incident role play of AARC in eduGAIN …

testing communications channels identified as high-priority target

Question	Response summary (9 responses received)
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn't go well?	Lack of coordination. Delay in official alert. It was unclear who should be contacted. eduGAIN was brought in too late. The incident trigger was too vague. Investigation incomplete.

Planned progress
- More exercises, coordinated via WISE
- Improve available tooling
- Set defined roles, including a *coordinator*, and promote eduGAIN security capability GN4-*

WISE SCCC-WG – participate!

WISE Community:
Security Comm...
Coordination V...

Introduction and backgr...
Maintaining trust between differe...
responses by all parties involved. M...
coordinated e-Infrastructures, the ...
contact information, and have eith...
and level of confidentiality maintai...
verified becomes stale: security co...
infrastructure may later bounce, o...

One of the ways to ensure contact...
compare their performance agains...

Dashboard / ... / SCCC-JWG

Communications Challange planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign
IGTF	November 2015		October 2019	IGTF-RATCC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h...
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe...
bounce, to testing if the organisation contacted can do system memory forensic analysis and engage effectively with LE. The proposed n...

IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	*Preliminary result: 82% prompt (1 working day) response, follow-up ongoing*

WISE, SIGISM, REFEDS, TI joint working group
see wise-community.org and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

AARC-I051 *Guide to Federated Security Incident Response for Research Collaboration*

Be Prepared
Act
Report and Share

informational document and not a guideline since Sirtfi WG still needs to get global endorsement, yet we need practical guidance right now!

See also
https://aarc-community.org/policies/
https://g.nikhef.nl/pma48-summary

join policy@aarc-community.org
- this is the 'na3' list, you may already be there!

Thank you
Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org