



Authentication and Authorisation for Research and Collaboration

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

Guidelines

The **AARC Guidelines** complement the **AARC Blueprint Architecture (BPA)** and the **policy best practices** recommended by the AARC project. The guidelines can apply to any topic that helps to advance Federated Identity Management for research and collaboration.

The AARC Guidelines help communities and infrastructures to implement and operate an AAI for research and collaboration more effectively and in an interoperable way.



aarc-community.org/guidelines

Architecture Guidelines

Policy Guidelines

Targeted Guidelines

Upcoming Guidance

AARC-G014 Security Incident Response Trust Framework for Federated Identity

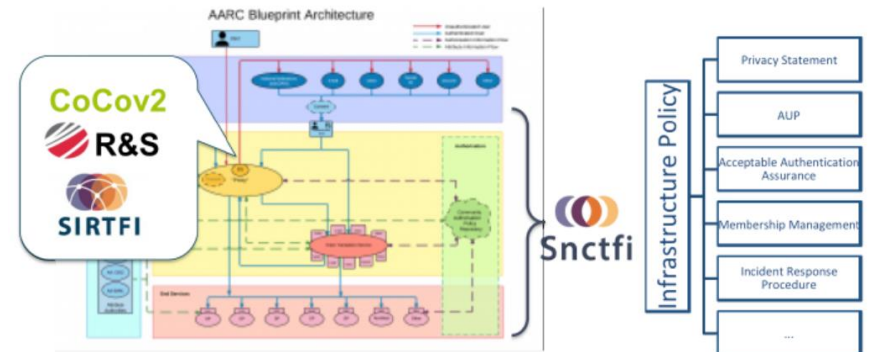
Sirtfi provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration. [more information](#)

AARC-G015 Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

The Snctfi framework identifies operational and policy requirements to help establish trust between Federations or in another infrastructure, in each case joined via a Service Provider to Identity Provider. [more information](#)

AARC-G021 Exchange of specific assurance information between

infrastructures and generic e-infrastructures comprise an 'effective' assurance profile derived by resulting assurance assertion obtained between infrastructures so that it need not be re-computed by the provider. This document describes the assurance profiles recommended to be used by the infrastructures. [more information](#)



Architecture Guidelines

Policy Guidelines

Targeted Guidelines

Upcoming Guidance

AARC-G040 Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

The Life Sciences AAI Service (LS AAI), developed in joint collaboration with EDI, EUDAT and GÉANT, 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 the LS AAI has to declare compliance to R&S and CoCo towards the R&E federations. This document provides preliminary guidance for the operators of the pilot LS AAI. [more information](#)

Trust and global policy

A single policy cannot apply

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

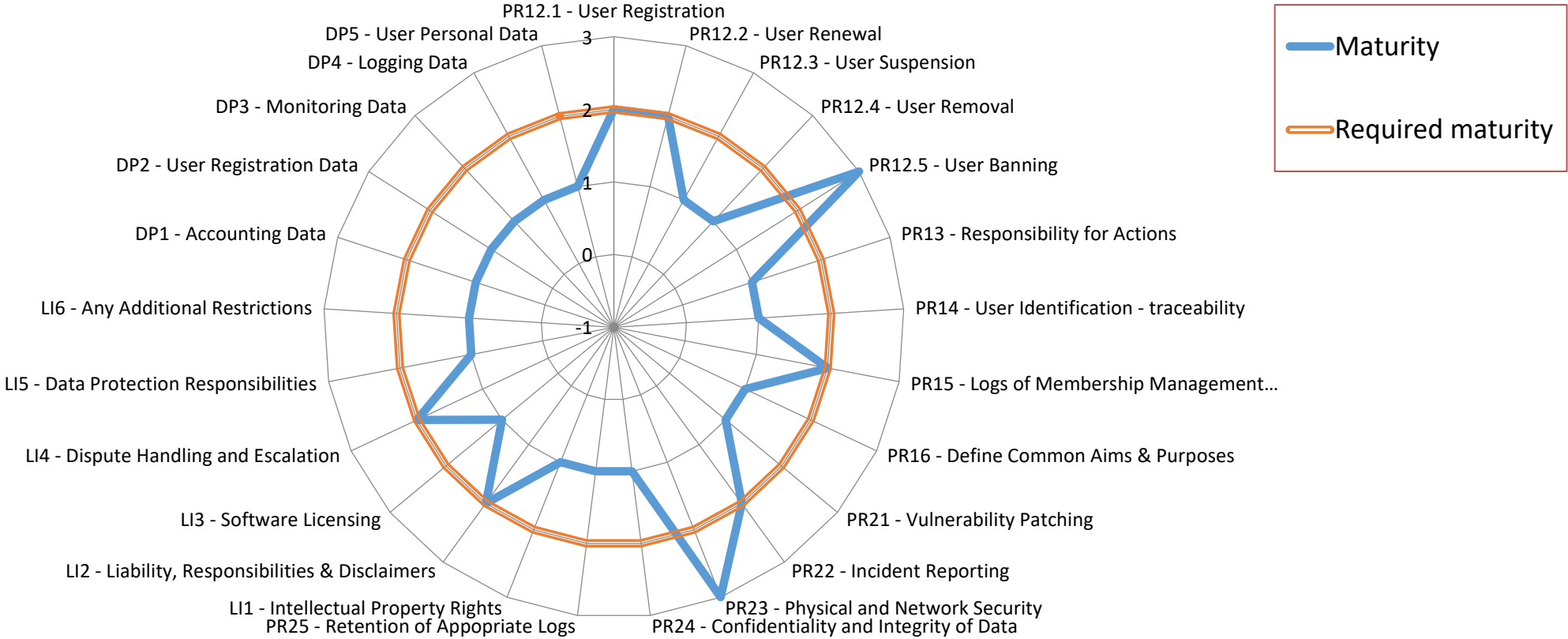
But one can 'map' policies and align policy structures



“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



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

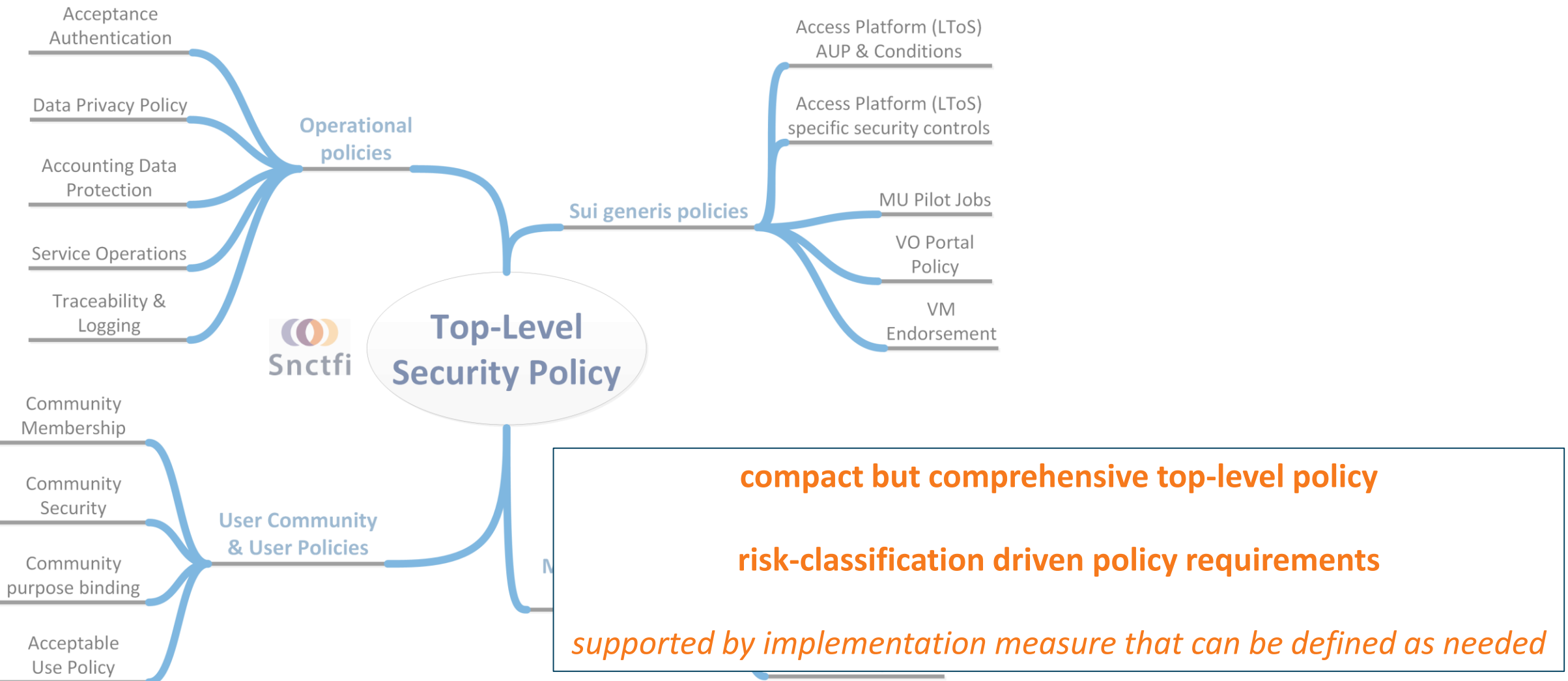
When using the baseline AUP text below, curly brackets "{}" (coloured blue) indicate text

- **shown only once** to user during registration
- information on *expected behaviour* and restrictions
- **can optionally be augmented** with additional community or infrastructure specific clauses *but numbered clauses should not be changed*
- 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

Evolving the policy development kit >>> Smplfy the structure



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)	

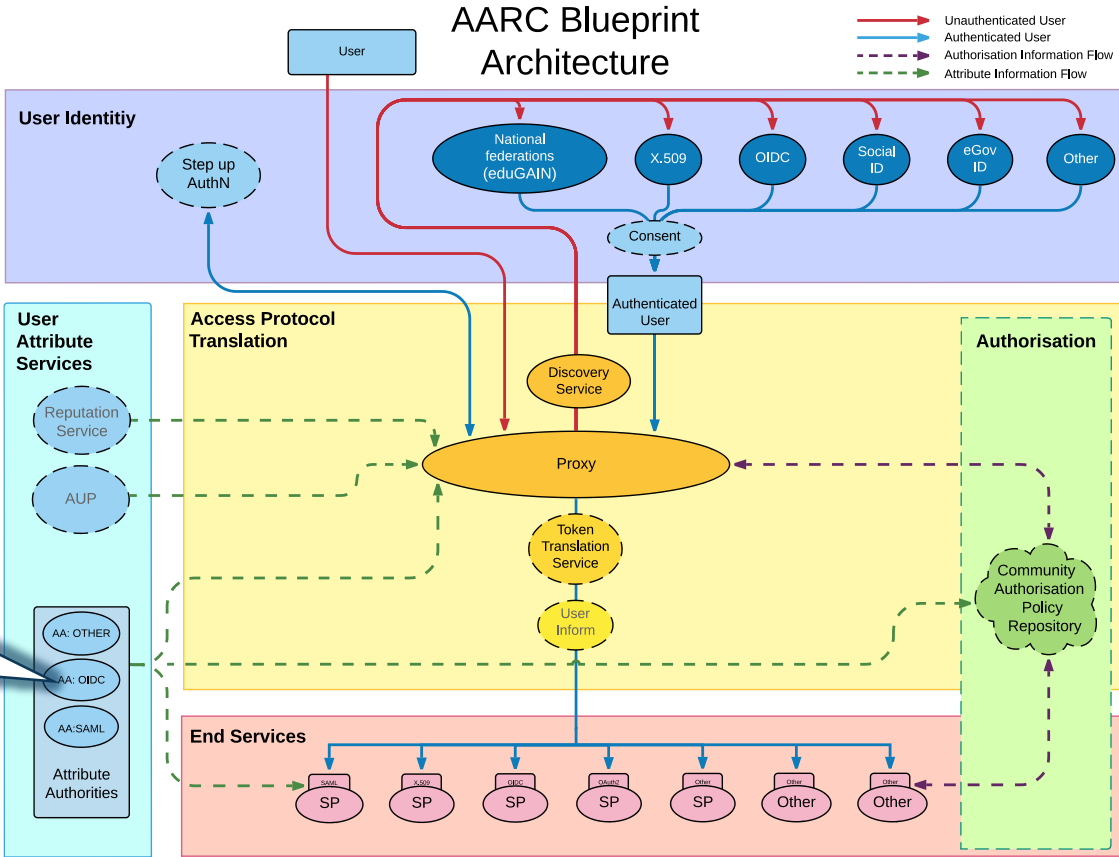
AARC Assam
 IGTF Dogwood
 RAF Cappuccino
 IGTF Birch
 RAF Espresso

The image shows two screenshots of spreadsheets used for identity assurance. The top screenshot is the 'REFEDS Assurance Framework Checklist: XSEDE', version 1.0 (Nov 26 2019). It lists various assertions such as 'The Identity Provider is operated with organizational-level authority' and 'The user identifier represents a single natural person'. It includes columns for 'Required for Cappuccino', 'Required for Espresso', and 'Meets Requirement?'. The bottom screenshot is the 'REFEDS MFA Checklist', version 1.0 (Nov 26 2019), which details multi-factor authentication requirements, such as 'The XSEDE IdP uses Kerberos passwords (something you know) and Duo MFA (something you have) for authentication.'

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



Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements (AARC-1048, 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 protection over the channel

Pull model
As a good example...

3.4.1. Key Management

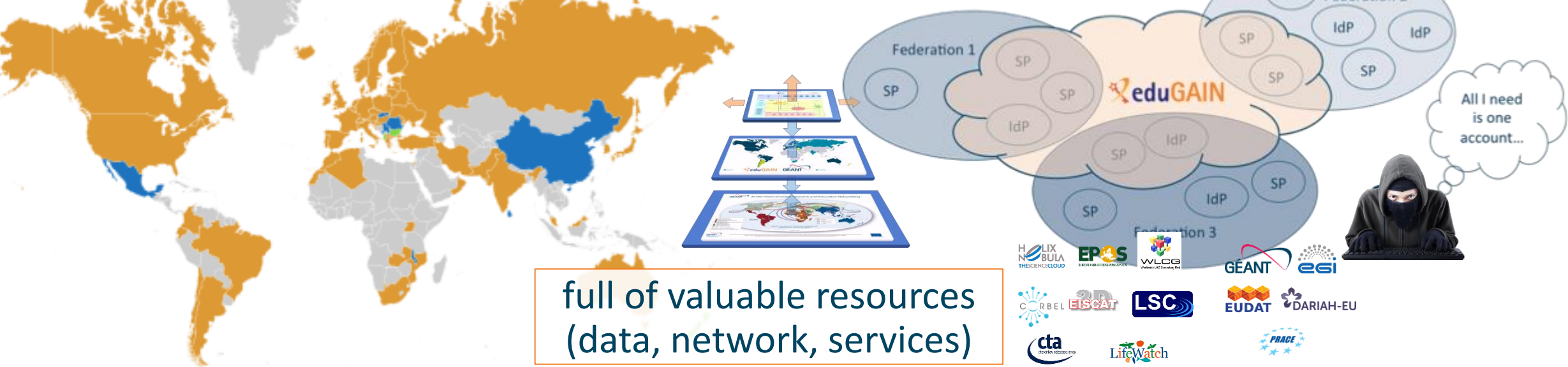
1. A key used to sign assertions must be different from those used to protect channels. If an AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting those channels.

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.

contribute: validate it with current implementations

Security Incident Response in the Federated World

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



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 differ
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, or

One of the ways to ensure contact
compare their performance agains

[Dashboard](#) / ... / [SCCC-JWG](#)

Communications Challenge 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
bounced to testing if the communication contacted people, custom messages for analysis and response effectiveness with I.E. The success level

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	<i>Preliminary result: 82% prompt (1 working day) response, follow-up ongoing</i>

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

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

Evolving incident response: from I051 to eduGAIN Security

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

Be Prepared Act Report and Share

eduGAIN Incident Response Procedure – IdP, SP Checklist
Version 2019-12-18

1 – (Suspected) Discovery

1. Local Security Team _____ *If applicable: INFORM WITHIN 4 HOURS.*
2. Federation Security Contact _____ *INFORM WITHIN 4 HOURS.*
3. eduGAIN CSIRT Duty Contact _____ *INFORM via "abuse@edugain.org" WITHIN 4 HOURS.*

2 – Containment

1. Affected Hosts _____ *If feasible: ISOLATE as soon as possible WITHIN 1 DAY.*
2. Affected VMs _____ *SNAPSHOT and/or SUSPEND WITHIN 4 HOURS.*
3. Affected Appliances _____ *DISABLE WITHIN 4 HOURS.*

3 – Confirmation

1. Incident _____ *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR Edugain CSIRT.*

4 – Downtime Announcement

1. Service Downtime _____ *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS" WITHIN 1 DAY.*

5 – Analysis

1. Evidence _____ *COLLECT AS APPROPRIATE.*
2. Incident Analysis _____ *PERFORM AS APPROPRIATE.*
3. Requests From EGI CSIRT _____ *FOLLOW UP WITHIN 4 HOURS.*

6 – Debriefing

1. Post-Mortem Incident Report _____ *PREPARE AND SEND to "abuse@edugain.org" WITHIN 1 MONTH.*

7 – Normal Operation Restoration

1. Normal Service Operation _____ *RESTORE AS PER RESOURCE CENTRE STANDARDS AFTER INCIDENT HANDLING IS COMPLETE.*
2. Procedures and Documentation _____ *UPDATE as appropriate to reflect analysis results.*

Security Incident Response Communication Workflow

This page is based on the AARC2 document: <https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf>

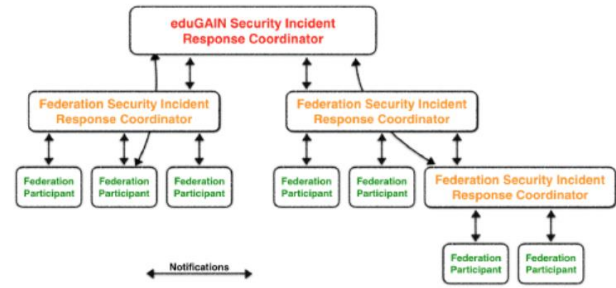
Goals

The objective is to ensure that all security incidents are investigated as fully as possible and that participants promptly report intrusions. Security incidents must be treated as serious matters and their investigation must be resourced appropriately.

Coordination roles

A Security Incident Response Coordinator must be appointed for each security incident. Either at the Federation Participant level, or a Federation Security Incident Response Coordinator, or an eduGAIN Security Incident Response Coordinator.

The main obligation of this role is to ensure the security incident resolution process does not stall. They are responsible for understanding and resolving the ongoing security incident by ensuring it is contained, coordinating the response from participants, tracking the progress of the process, coordinating action, disseminating information and providing expertise and guidance. They are expected to marshal concerned federated actors to participate in the response to a security incident. This role should be played by the entity most appropriate for the task, such as a Research Community or e-Infrastructure CSIRT, or an individual or group appointed by the federation or inter-federation.



1. Federation Participants

A Federation participant include any federation member including, but not limited to, identity providers, service providers and attribute authorities. This may include Research Community service providers, identity and service provider proxies, or e-Infrastructure that are registered as service providers in a Federation. As such, a Federation participant may also act as a Federation Security Incident Response Coordinator, as well.

Federation participants are expected to follow the "Security Incident Response Procedure (for Federation Participants)", and in particular report all security incidents posing a risk to any other federation participant within or outside their own federation, to the federation security contact point at their own federation.

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://g.nikhef.nl/pma48-summary>

Thank you Any Questions?

davidg@nikhef.nl



<https://aarc-community.org>



© members of the AARC Community.
The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

Project support by AARC2, GN4-3, and EOSChub