

European IGTF+ update

*Enabling Communities, Trust, Identity,
and Security from the EUGridPMA+*

Meanwhile in the EUGridPMA+ ...

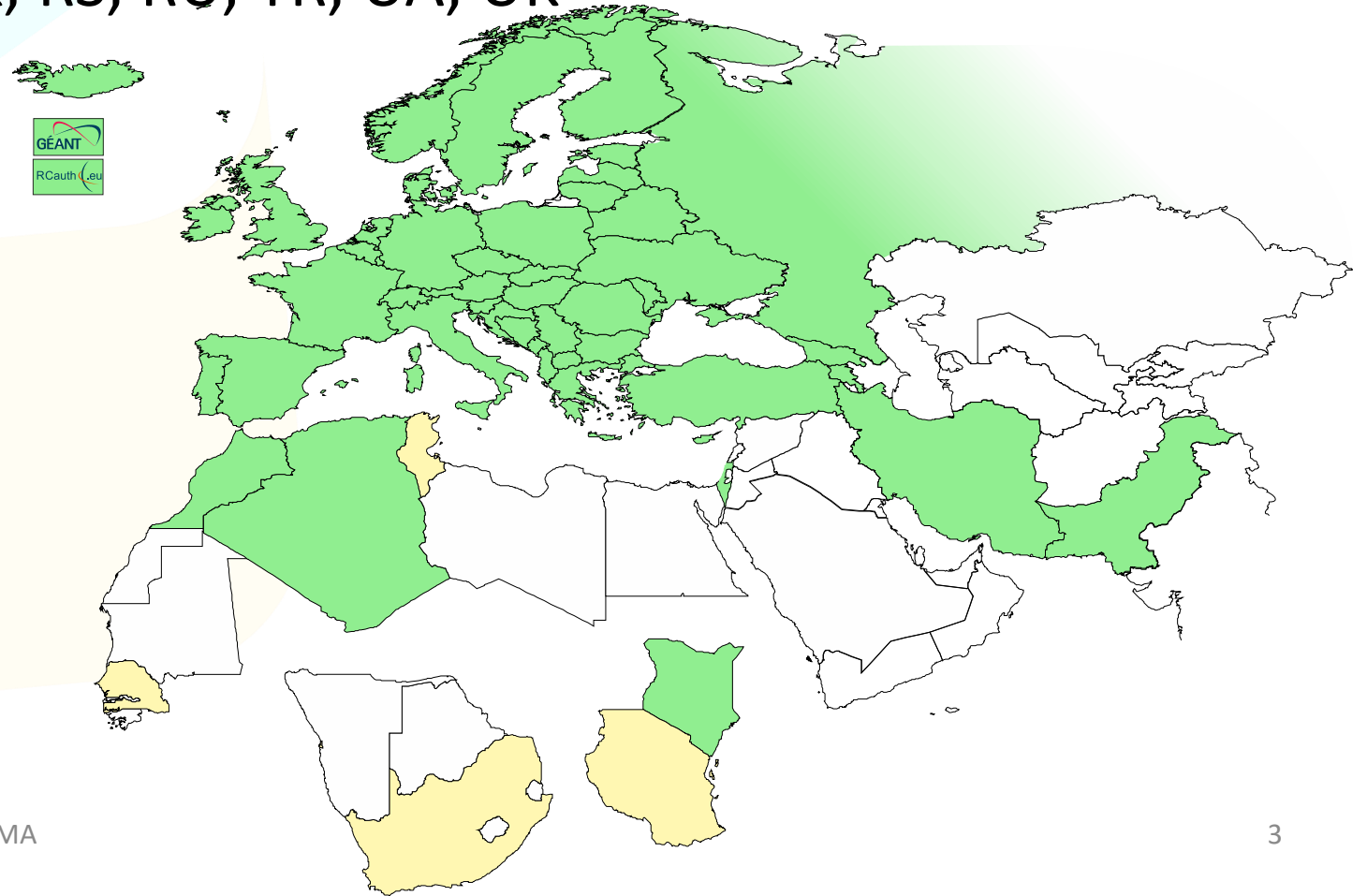
- EUGridPMA State of the Fabric
 - constituency and developments
 - IGTF distribution updates and packaging
 - S/MIME baseline in CABF: separating authentication and email in TCS
- AARC (Authentication and Authorisation for Research Collaboration) *and its* Technical Revision for Enhanced Effectiveness (AARC TREE)
 - Evolving AARC and the AARC Blueprint Architecture “BPA 2025”
 - Attribute Authority Operations self-assessment for secure and trusted BPA proxies
 - Policy Development Kit: supporting community structuring and a secure baseline
 - Notice management for AUP and data protection
 - novel (OpenID) federation models – disambiguating trust and technical translations

<https://www.eugridpma.org/> for all details and meeting minutes!



EMEA area membership evolution

- Europe⁺: GEANT TCS, and CZ, DE, DK(+FI+IS+NO+SE), FR, GR, HR, NL, PL, RO, SI, SK; AM, MD, ME, MK, RS, RU, TR, UA, UK
- Middle East: IR, PK
- Africa: DZ, KE, MA
- CERN, RCauth.eu



Membership and other changes

- Identity providers: both reduction and growth
 - migration to GEANT TCS continues
<https://wiki.geant.org/display/TCSNT/TCS+Participants+Sectigo>
 - CERN joining TCS via Renater (FR)
 - Discontinued: -GE, -BY, -PT, -AE
 - Suspended: -KE
- Self-audit review
 - Cosmin Nistor will update us in a moment
 - real-time interaction between authority and reviewers helps, but ...
- .ch is now served by eMudhra – confirmed since September 2024



RedHat's and Firefox's idea of what trust means for self-signed objects in an explicit trust store ...

The Challenge of Self-Signed Roots in RedHat

Although it conceptually makes no sense ...

While all intermediate and end-entity certificate now use secure hash algorithms, some operating system distros are deprecating sha1 *also for self-signed root certs*

- FF103+
- RHEL9+ (and its rebuilds)

Impacts both joint-trust and igtf-only trust, but for web-trust clients it is taken care of by specific bespoke software configuration (RHEL's OpenSSL trust flags, or the Firefox built-ins)

For other cases, there is – for now – a policy override:

```
update-crypto-policies --set DEFAULT:SHA1  
update-crypto-policies --set LEGACY
```

A blunt mitigation for the actual issue, as it allows for other sha1 purposes

- which is 'fine' for the IGTF fabric, but not in general



The OSG experiment

- OSG shipped the dual-blob mode that mimicks the bespoke OS config
 - using equivalent of <https://www.nikhef.nl/~davidg/tmp/make-trusted.sh>
 - first a “BEGIN TRUSTED CERTIFICATE”,
then in the same file “BEGIN CERTIFICATE”
- However, it broke 😞
 - CANL-Java, extending BouncyCastle, cannot process this blob and will balk *even if* it does not recognise it and should just ignore it (<https://stackoverflow.com/questions/55550299/java-can-not-load-begin-trusted-certificate-format-certificate>)
 - open as a dCache Feature Enhancement on CANL Java (by Paul Millar)
- will not be fixed overnight, of course ... and we may find other issues thereafter



Yet maybe ...

- On 2023-12-20 13:25, Guido Pineda (SURF NL) wrote:
 - > I am using fetch-crl version 3.0.22.
 - > We have a total of 89 trust anchors configured on our /etc/grid-security directory.
 - > I have tested fetch-crl with different versions of OpenSSL and here are the
 - > outcomes:
 - > For versions 1.1.1k and versions 3.2.0, the amount of errors when trying to verify
 - > the CRL's is only one [which was explainable]
 - > However, when using OpenSSL version 3.0.7, we get 10 errors
- Due to self-compiling OpenSSL? And does that then ignore the RH crypt-policies?



It cannot be solved without changes to RP software

- asking for ‘a SHA-1 free IGTF distribution’ is not helpful
 - unless you at the same time also remove all SHA-1 from the public web trust stores
- dual-blob solution might be the best option, but it needs CANL-Java fixes
 - for the large authorities, e.g. DigiCert Assured ID Root from 2006, re-issuing with the same key and different digest will cause unfathomable confusion in browsers
 - migrating to another (SHA-2 rooted) signing hierarchy will take at least 395 days, may be a lot of engineering on the RP and CA side, or require new contracts
- root cause is RH and FF not understanding what a self-signed trust anchor is, but that will not help us in the short term 😞



Reissuance of roots – state and progress

Just to make the problem appear smaller, some issuers are migrating anyway

Current list of SHA-1 self-signed trust anchors:

ASGCCA-2007

DZeScience

IHEP-2013 (to change <1yr)

KEK

MARGI

RomanianGRID

SiGNET-CA

seegrid-ca-2013

ArmeSFo

DigiCertAssuredIDRootCA-Root

CESNET-CA-Root

RDIG

SRCE

TRGrid

Changed by now:

GridCanada, CILogon basic/silver/OpenID, UKeScienceRoot-2007

Removed:

DigiCertGridCA-*, DFN-GridGermany, CNIC, BYGCA , LIPCA

Pending withdrawal:





Authentication and Authorisation for Research Collaboration (AARC) & Enabling Communities (EnCo)

FEDERATED T&I AND AARC

Federated T&I and AARC

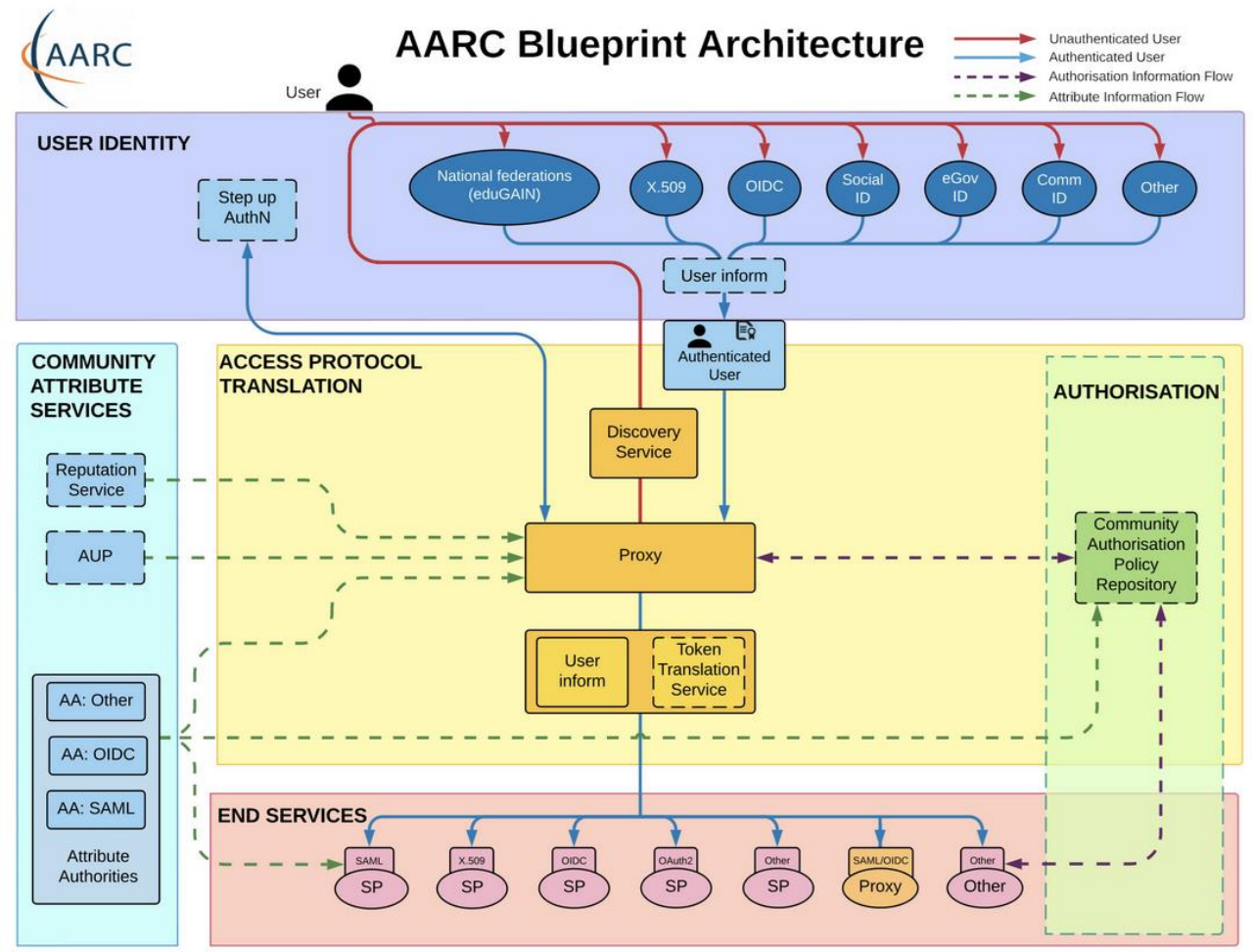
EUGridPMA+ is also the place for the AARC Policy Community & EnCo:

- AARC Policy Development Kit:
supporting community structuring, security baseline, trust proxies
- notice management for AUP and data protection in proxies
- novel (OpenID) federation models – disambiguating trust and translation
- but also federated access to ‘SSH’ non-web services, and ssh-ca

<https://www.eugridpma.org/meetings/2024-09/The-Copenhagen-60th-EUGridPMA+-Meeting-Summary.pdf>



Interoperability – more than just the nice colours



Not sure how to begin with the AARC Blueprint Architecture? There are plenty of guidelines available but it can be a minefield at first. You probably want to start by designing the high level approach of your infrastructure based on the AARC Blueprint Architecture. There are several general topics you should consider, such as Data Protection (AARC-G042) and Federated Security Incident Response (AARC-I051). Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

User Identity:

- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? AARC-G029

Assurance:

- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

Community Attribute Services:

- How should attributes from multiple sources be aggregated? AARC-G003
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user? AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G071
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

Access Protocol Translation:

- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

Authorisation:

- How should I manage authorisation information from multiple sources? AARC-G006
- How should group and role information be expressed to facilitate interoperability? AARC-G002
- How should resource capabilities be expressed? AARC-G027

Proxies:

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user? AARC-G026
- How should I express assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061
- How can my proxy route the user to the correct discovery service? AARC-G062

End Services:

- My service needs to act on behalf of the user – how should I handle credential delegation and impersonation? AARC-G005
- My services are not web based, how can I use identities from the proxy? AARC-G007
- How should Services hint which IDP they would like users to use? AARC-G049
- Which Security practices should I follow? AARC-G014

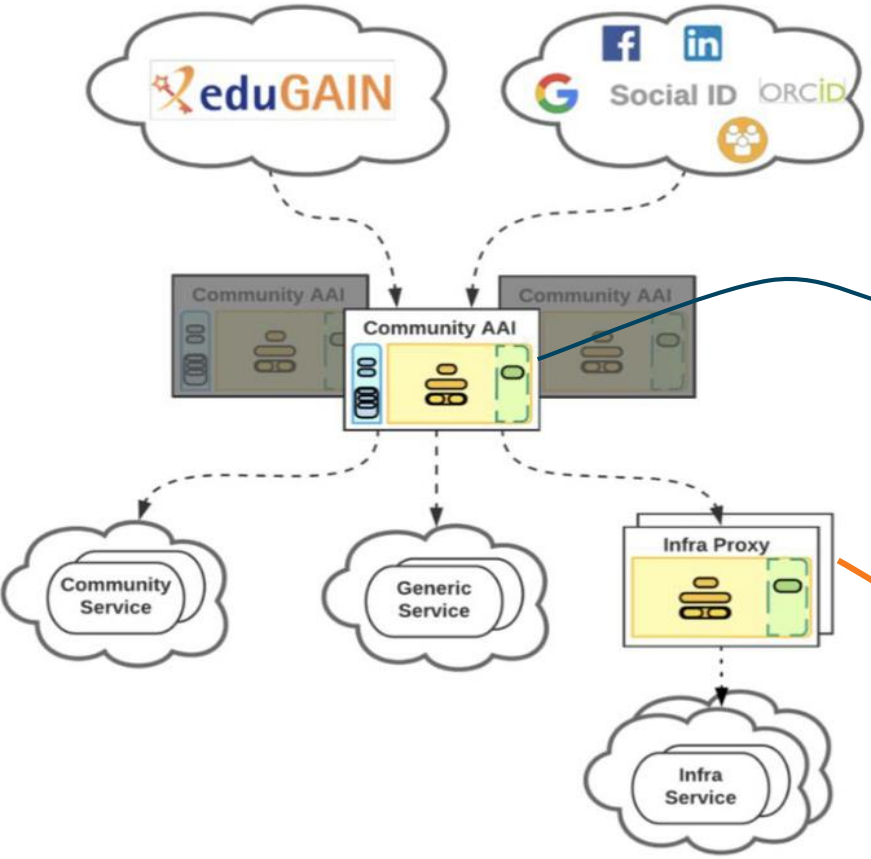
What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.

Personal Data	Protection Contact	Services (abide by)	Services (abide by) processing personal data.
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.
		Services (abide by)	This policy defines requirements for running a service within the infrastructure.
		Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.

PDK

Showing 1 to 9 of 9 entries

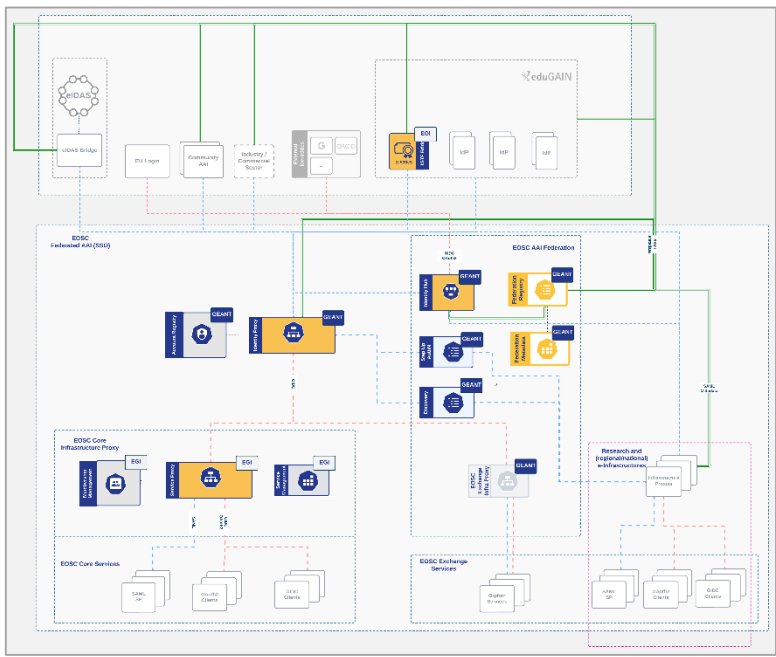
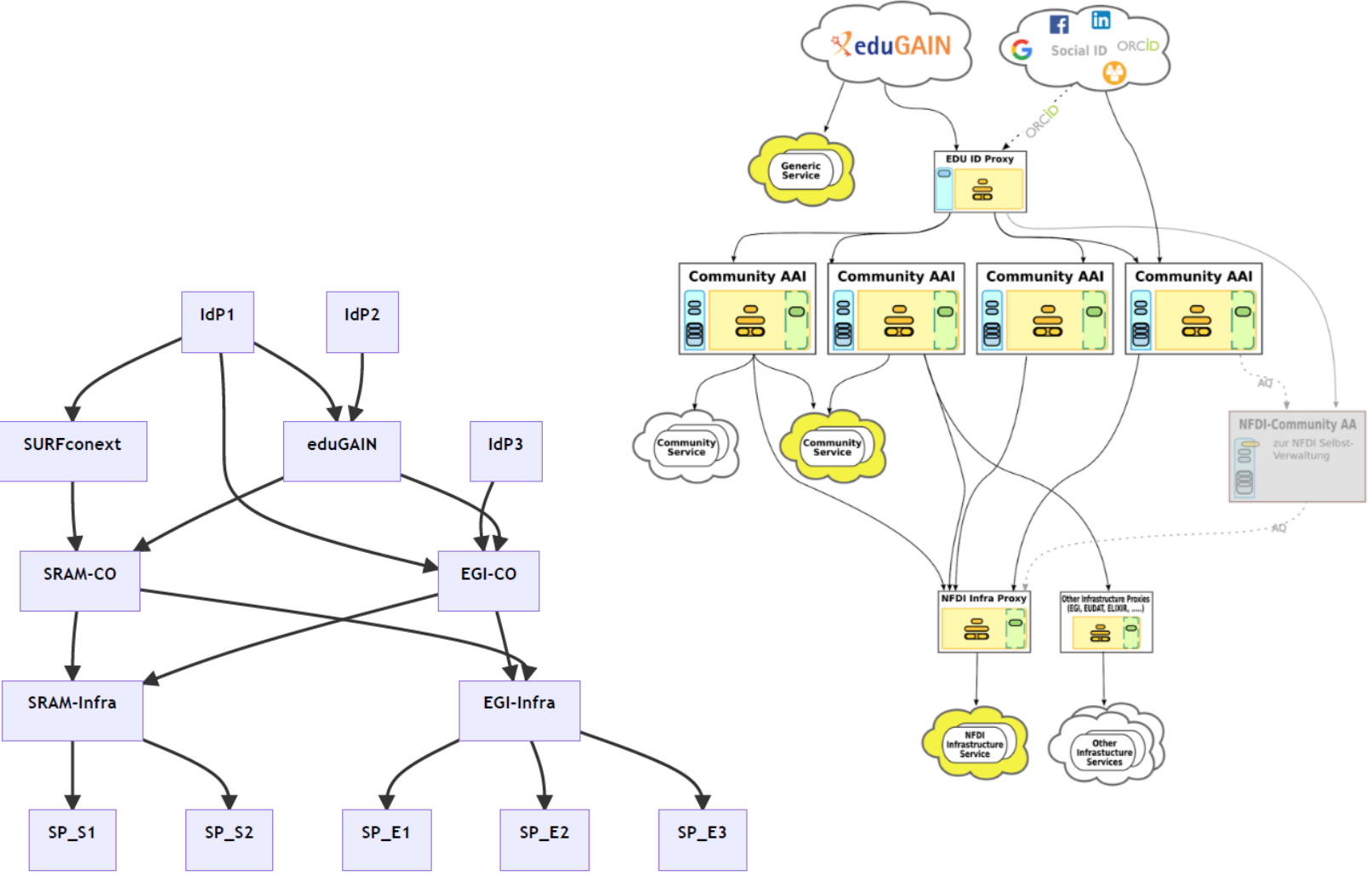
The Community AAI and the Infrastructure Proxy – structuring elements



Community AAI
 The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy
 The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant Policies and business logic for making available these resources to multiple communities

Our federated world is growing more complex



Images: SURF SSRAM and EGI by Maarten Kremers, NDFI AAI (Marcus Hardt), EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023 version)

AARC-TREE: Evolved BPA for more complex (and the simpler) worlds

Guidelines for **expression of community user attributes**

- **reduce inconsistencies** between implementations
- improve **interoperability & end-user usability** across research community communities and infrastructures

Extend AARC BPA

- improve **scalability**
- leverage emerging standards like **OpenID Federation**

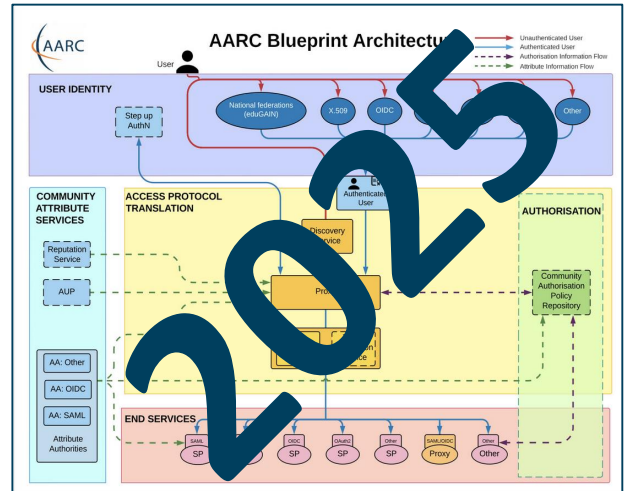
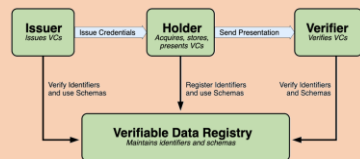
Authorisation guidelines

- best practises to enable efficient & effective **sharing of federated resources**



Decentralised identities

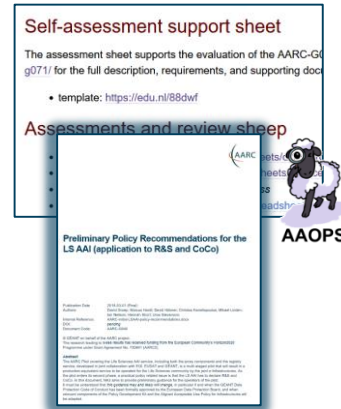
- guidance for **digital wallets** linked to BPA



Policy and good practice underpinning the AARC Blueprint BPA

Infrastructure alignment and policy harmonisation: helping out the proxy

- **Operational Trust** for Community and Infrastructure BPA Proxies
- Increase acceptance of research proxies by identity providers through **common baselines**
- Review infrastructure models for **coordinated AUP, T&C, and privacy notices**, improving cross-infrastructure user experience (users need to click only once)



User-centric trust alignment and policy harmonization: helping out the community

- Lightweight community management policy template
- Guideline on cross-sectoral trust in novel federated access models
- Assurance in research services through (eIDAS) public identity assertion



Anchored in the researcher user communities by **co-creation with FIM4R**



AARC-G071

IGTF AAOPS (<https://www.eugridpma.org/guidelines/aaops/>)

ATTRIBUTE AUTHORITY OPERATIONAL SECURITY

Taking proper care of trust sources

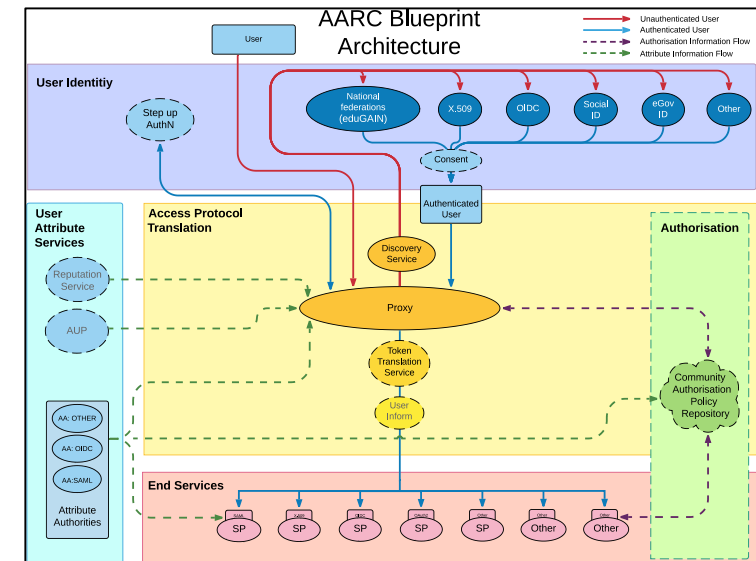
Protections for (IGTF) identity providers are known and documented

- RFC3647
- IGTF Guidelines
- Technical profiles

Table of Contents	
1	INTRODUCTION 7
1.1	OVERVIEW 7
1.2	IDENTIFICATION 7
1.3	COMMUNITY AND APPLICABILITY 7
1.3.1	Certification authorities 7
1.3.2	Registration authorities 8
1.3.3	End entities 8
1.3.4	Applicability 8
1.4	CONTACT DETAILS 9
1.4.1	Specification administration organization 9
1.4.2	Contact person 9
1.4.3	Person determining CPS suitability for the policy 9
2	GENERAL PROVISIONS 10
2.1	OBLIGATIONS 10
2.1.1	C4 obligations 10
2.1.2	RA obligations 10
2.1.3	Subscriber obligations 12
2.1.4	Relying party obligations 12
2.1.5	Repository obligations 13
2.2	LIABILITY 14
2.2.1	C4 liability 14
2.2.2	RA liability 14
2.3	FINANCIAL RESPONSIBILITY 15
2.3.1	Indemnification by relying parties 15
2.3.2	Fiduciary relationships 15
2.3.3	Administrative processes 15
2.4	INTERPRETATION AND ENFORCEMENT 15
2.4.1	Governing law 15
2.4.2	Severability, survival, merger, notice 15
2.4.3	Dispute resolution procedures 15
2.5	FEES 16
2.5.1	Certificate issuance or renewal fees 16
2.5.2	Certificate access fees 16
2.5.3	Revocation or status information access fees 16
2.5.4	Fees for other services such as policy information 16
2.5.5	Refund policy 16
2.6	PUBLICATION AND REPOSITORY 16
2.6.1	Publication of C4 information 16
2.6.2	Frequency of publication 16
2.6.3	Access controls 16
2.6.4	Repositories 17
2.7	COMPLIANCE AUDIT 17
2.7.1	Frequency of entity compliance audit 17
2.7.2	Identity/qualifications of auditor 17
2.7.3	Auditor's relationship to audited party 17
2.7.4	Topics covered by audit 17

The AAI relies also on other attribute sources, and on the hubs & AARC Proxies

- only generic guidance
- proxies fully hide ID source



Operational guideline landscape for - proxy or source

- AAI components

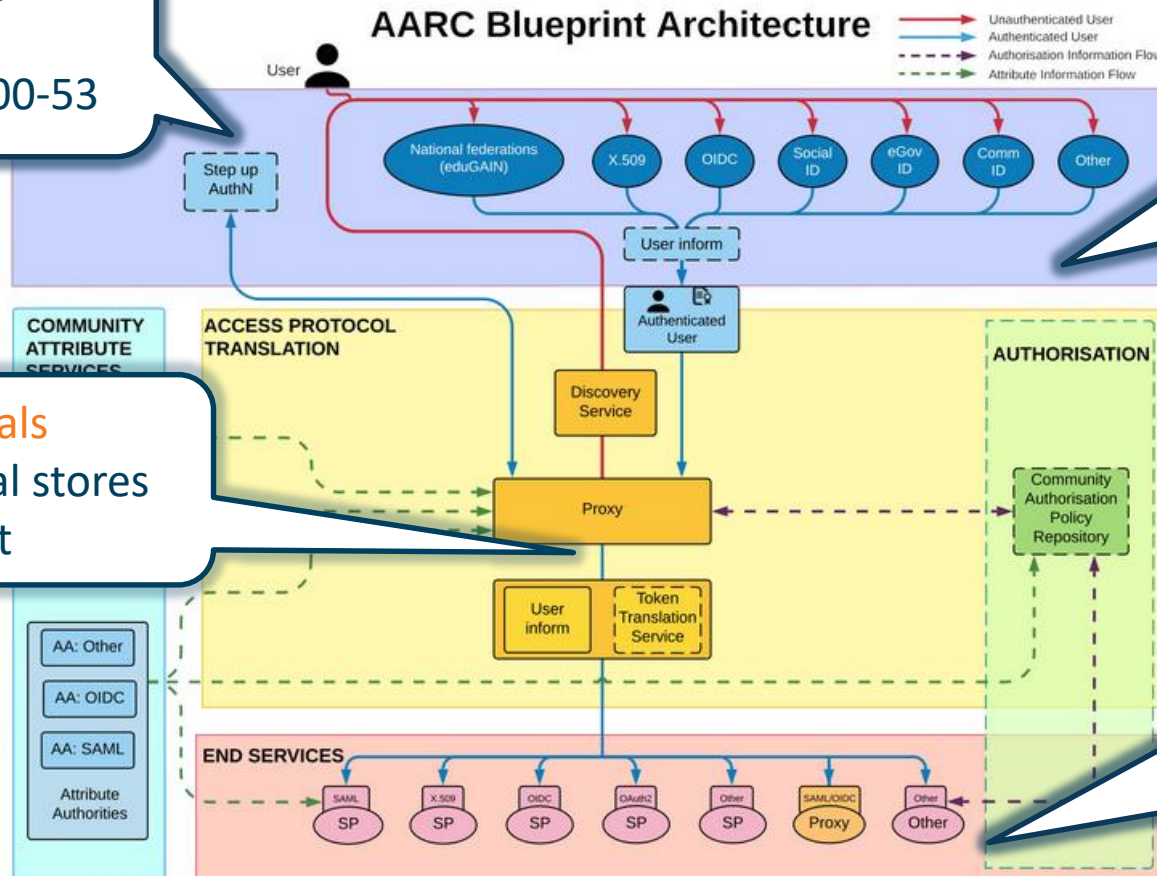
RFC6238/4226
FIPS140
NISTSP800-53

Authentication/identity sources
Sirtfi
(eduGAIN) baselining, RAF
IGTF AP Profiles
NIST SP800-63
eduGAIN sec. team workflow

Ephemeral credentials

- trusted credential stores
- protection at rest

Service provider operations
ISO27k
Sirtfi
Infrastructure response plans

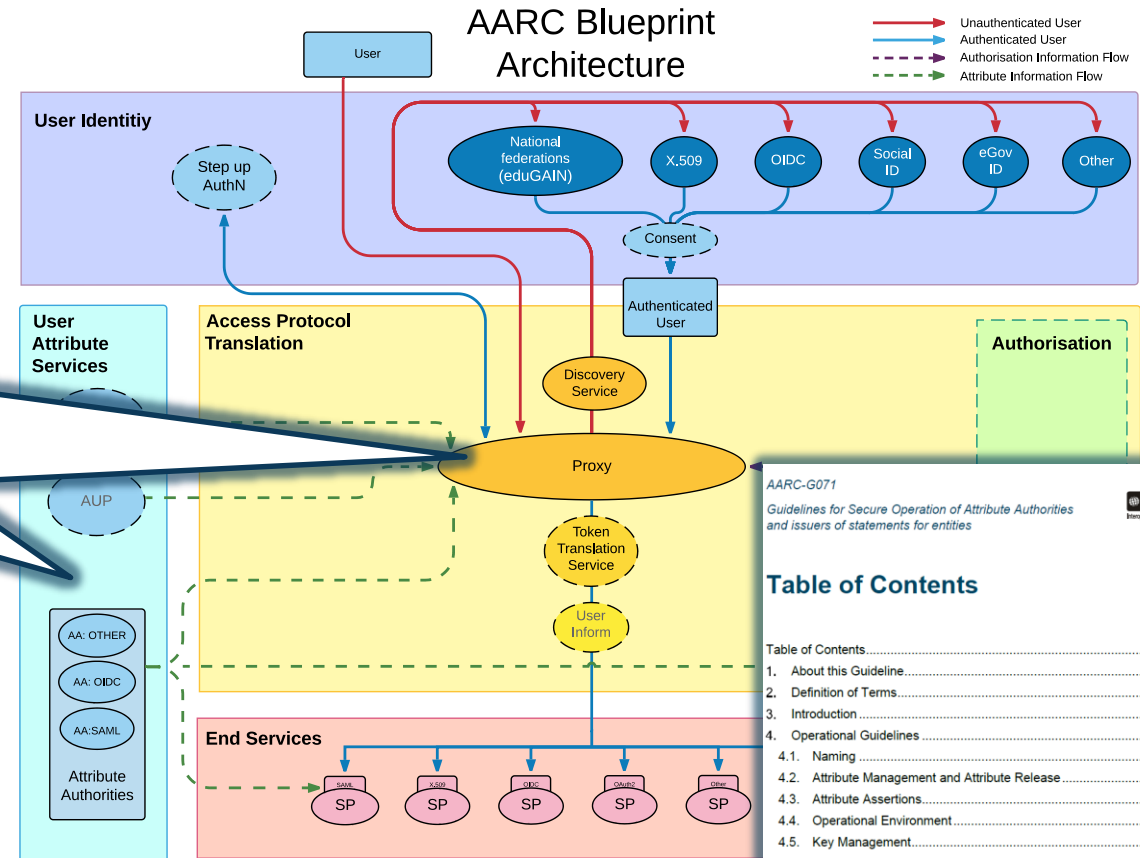


Trust and security in the BPA beyond IdPs and SPs

Community management and attribute authorities

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

AARC-G071: Structured around concept of “AA Operators” operating “Attribute Authorities” (technological entities or proxies), on behalf of, one or more, **Communities**, that are trusted by **Relying Parties**



AARC-G071
Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

IGTF
Interoperable Global Trust Federation
API/EU/TAG

AARC

Table of Contents

Table of Contents.....	2
1. About this Guideline.....	3
2. Definition of Terms.....	4
3. Introduction.....	5
4. Operational Guidelines.....	5
4.1. Naming.....	5
4.2. Attribute Management and Attribute Release.....	7
4.3. Attribute Assertions.....	8
4.4. Operational Environment.....	9
4.5. Key Management.....	9
4.6. Network Configuration.....	10
4.7. Site Security.....	11
4.8. Metadata Publication.....	11
4.9. Assessment and Review.....	12
4.10. Privacy and Confidentiality.....	13
4.11. Business Continuity and Disaster Recovery.....	14
5. Relying Party Obligations.....	14
References.....	15
Acknowledgements.....	16



Implementing the AA Operations Security guidelines

1. Major RPs and Infrastructures reviewed it based on current use cases and models
2. Guideline aimed at both Infrastructure and Community use cases
3. Useful input to e.g. 'EOSC' connected proxies as a good practice guideline
4. Assessment or review process is separate – could be IGTF or an RP consortium, but does state what needs to be logged and saved to do a (self) assessment

<https://aarc-community.org/guidelines/aarc-g071/>

AARC-G071 Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

These guidelines describe the minimum requirements and recommendations for the secure operation of attribute authorities and similar services that make statements about an entity based on well-defined attributes. Adherence to these guidelines may help to establish trust between communities, operators of attribute authorities and issuers, and Relying Parties, infrastructures, and service providers. This document does not define an accreditation process.

Document URL: <https://wiki.geant.org/download/attachments/123766269/AARC-G071-Secure-Operation-of-Attribute-Authorities-rev2.pdf>

Development information: <https://wiki.geant.org/display/AARC/Attribute+Authority+and+Proxy+operational+security>

Status: under AEGIS review

DOI: <https://doi.org/10.5281/zenodo.5927799> (reserved)

IGTF reference: <https://www.igtf.net/guidelines/aaops/>

Errata: none

Supersedes: AARC-G048

October 2024



G071 self-assessment process

<https://edu.nl/88dwf>



- Self-assessment by WLCG, UK-IRIS, eduTEAMS, EGI CheckIn, SURF SRAM
- mutual review also improves G071 guideline itself

The screenshot shows an Excel spreadsheet with the following content:

- Header: Review-sheet-G071-template .XLSX
- Menu: File Edit View Insert Format Data Tools Help
- Toolbar: 100%, Calibri, 11, Bold, Italic, Underline, Text Color, Fill Color, Borders, Styles, Print, Save, Undo, Redo, Zoom, Window, Help, Sum.
- Row 2: AARC-G071 Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities review sheet
- Row 3: Operator
- Row 4: AA scope
- Row 5: Model
- Row 6: Product(s)
- Row 7: Interop
- Row 8: Date of last update:
- Row 9: This assessment sheet supports the evaluation of the AARC-G071 "AAOPS" guidelines. Please refer to the Guidelines document <https://aarc-community.org/guidelines/aarc-g071/> for the full description, requirements, and supporting documentation. Please clone this sheet for your own assessment.
- Table with 5 columns: Item, Description, Status, References, Review comments

Self-assessment support sheet

The assessment sheet supports the evaluation of the AARC-G071 "AAOPS" [g071/](https://edu.nl/88dwf) for the full description, requirements, and supporting documentation. P

- template: <https://edu.nl/88dwf>

Assessments and review sheep

- WLCG - <https://docs.google.com/spreadsheets/d/1zyHrgdhUo9IA8Yis>
- UK-IRIS - <https://docs.google.com/spreadsheets/d/1lvce7TXXzzP4hi8>
- eduTEAMS (Core AAI platform) - *in progress*
- SURF SRAM - <https://docs.google.com/spreadsheets/d/1P4Up8JpIW>





AARC-G083

NOTICE MANAGEMENT BY PROXIES

With fewer clicks to more resources: AARC-G083


Users should not click the same policy at many different places

Services should not require the user clicking (policy) acceptance, since this will interrupt workflows

Target audience for this guideline

- both community and infra proxies and hybrids
- notices *for the proxies themselves*: so privacy notes personal data related to *use of the infrastructure*
- for the notices by *services that are mediated by the proxy*, and thereby also allow for specific protection on (personal) research data

<https://wiki.geant.org/display/AARC/AARC-G083++Guidance+for+Notice+Management+by+Proxies>



Guidance for Notice Management by Proxies

Publication Date: [Publish Date]
Authors: Arnout Terpstra, Catharina Vaendel, David Groep, David Kelsey, Maarten Kremers, et al.

Document Code: AARC-G083
Supported by:
Publishing Organisation: AARC Community
DOI:

© Members of the AARC community.
This work is licensed under a Creative Commons Attribution 3.0 License.

Abstract
Use of GDPR privacy notices and AUP acceptance practices in the current research infrastructures, and provide sectoral recommendations on aligning their presentation by AARC BPA proxies. Since different research infrastructures deal with data of varying sensitivity levels, the model shall allow for a scalable level of control and verifiability.

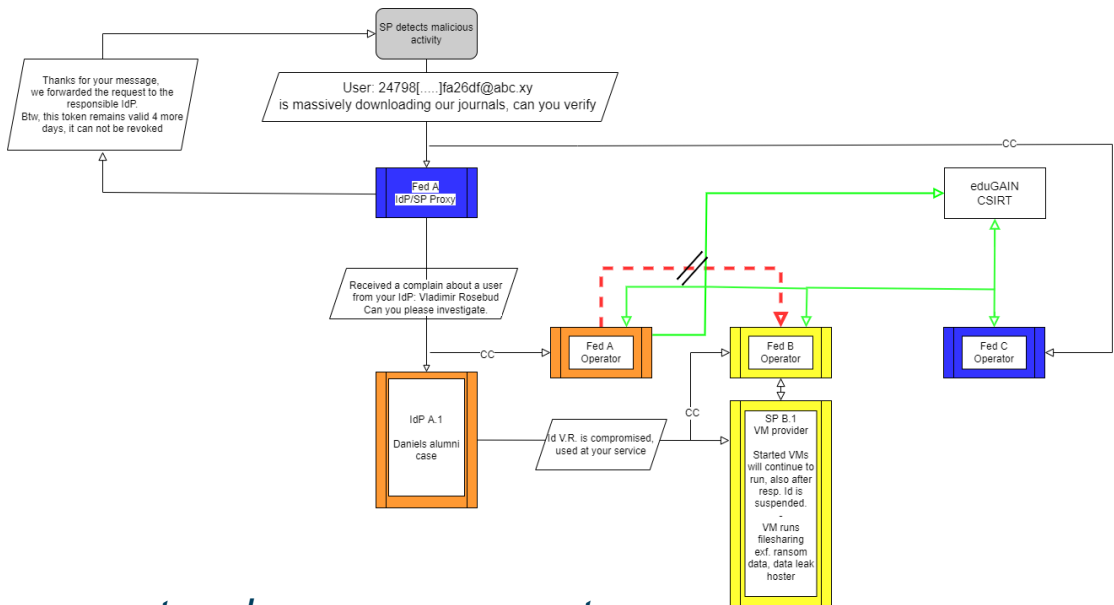
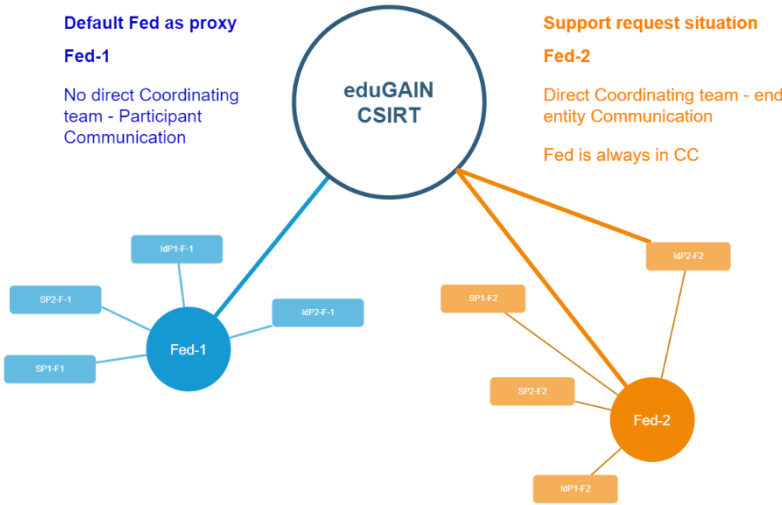
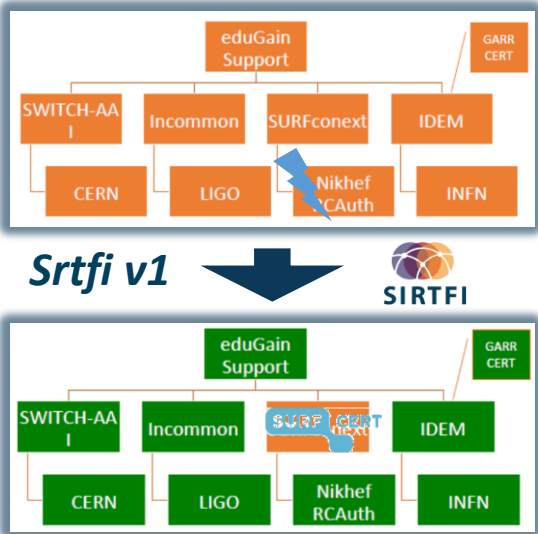




<https://wiki.geant.org/display/AARC/AARC+Policy+Harmonisation>

GROWING AARC POLICY HARMONISATION

Response and traceability across IdP-SP Proxies and the limits of Sirtfi



Guidelines for a joint **operational trust baseline** for membership management and proxy components, supplemented by policy guidance for sectoral federations with more specific policies where needed

- ‘How can we **convey the trust in what is in and behind the proxy?**’
- ‘How to provide **timely traceability** between services and identities through the proxy?’

Based on requirements from FIM4R, WISE, and the proxy operators in AEGIS.



joint work with GN5 EnCo and eduGAIN CSIRT



Can we build on a trusted baseline and expectations to increase acceptance of research infrastructure proxies with R&E identity providers

Even though affiliation is the most relevant attribute from home IdPs, ...

- still need assurance statements and REFEDS Assurance Framework attribute freshness
- unless 'well hidden', proxies are met with scepticism by IdPs to release personalised to R&S
- do Entity Categories 'traverse' proxies? and can proxy ops rely on their 'downstreams'?

a common **baseline** that proxies can endorse and manage for their connected services helps



review and enhance effectiveness of Snctfi 'revamped'

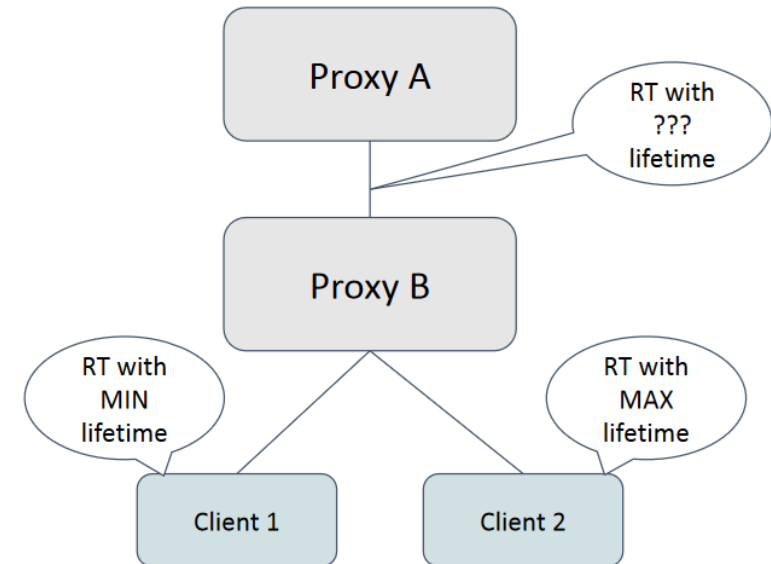
the set of guidelines that describe a (self-) accessible baseline for a set of service providers behind an AARC BPA Proxy

and thereby encourage trust in the proxies *and* their connected services

Token life times: both technical and policy elements in AARC G081

While for *Refresh Tokens* the validity period can be long ... a risk-based approach is needed

- Access and ID tokens may come in form that can be validated ‘off-line’
- For opsec, there should be no *long-lived* credentials that can’t be invalidated
- **But** *what* is ‘long-lived’?
If revocation is needed – what issues does that cause?
- What trust can proxies have in their downstream (or upstream)?
What about token change flows (even if less likely)?
- Limited differentiation of life times,
with SHOULD defaults and MUST upper *and lower* bounds



G081

Current approach to

Canonical GFD.32 guidance still appears appropriate

- 1Ms and ~1 year
- a capability to invalidate (off-line) tokens on an opsec incident should be < 6 hrs, the acceptable value for emergency suspension in e.g. the WLCG operational infrastructure

Token	Bounded	Rotation	Verified online	Revocable	Structured	Signed	Opaque*	Recommended lifetime		
								Default	Minimal	Maximal
Opaque Access Tokens	Yes	No	Yes	No	No	No	Yes			
JWT Access Tokens	Yes	No	No	No	Yes	Yes	No			
JWT Access Tokens	Yes	No	Yes	Yes	Yes	Yes	No			
OIDC ID Tokens	Yes	No	No	No	Yes	Yes	No			
OIDC Refresh Tokens	Yes	Yes	Yes	Yes	Yes	Yes	No			
OIDC Refresh Tokens	Yes	No	Yes	Yes	Yes	Yes	No			

https://docs.google.com/presentation/d/1P_ZDUWTX0py8kXTgWHMCCfO2f_9uzsE0/edit#

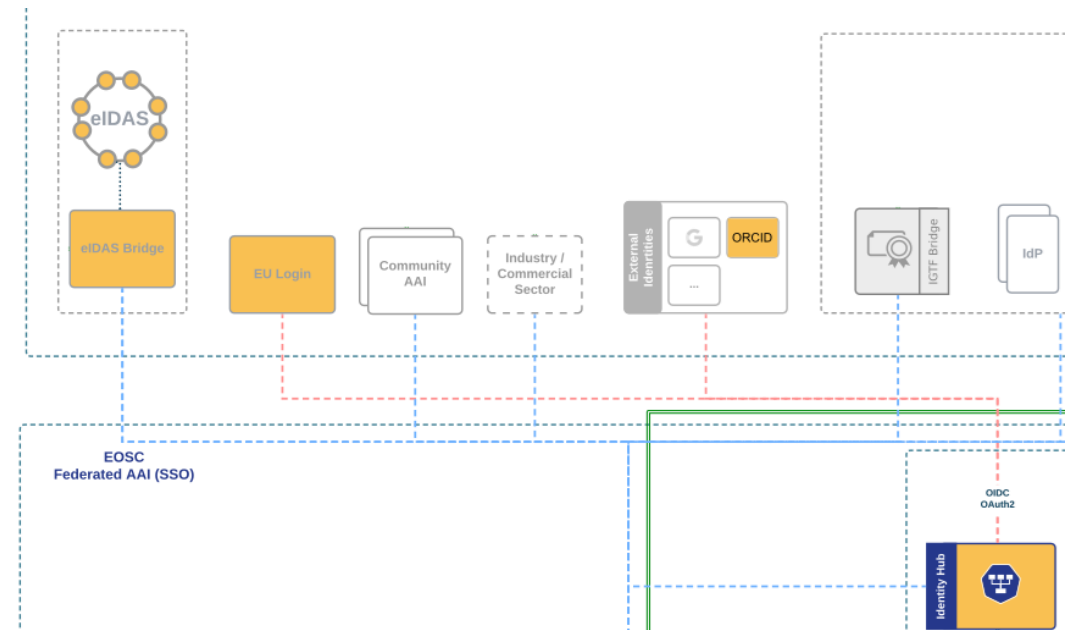
We'll see more diverse sources of identity & assurance anyway

Most reliable (and most 'available') source of assurance may be the European government identity ecosystem.

- Step-up to at least substantial level can now readily be done 'at home' by users through their national eID schemes
- Joint work on eIDAS, Erasmus Student Mobility, and more makes this more accessible
- Better attainable than relying on home institutions?

... but:

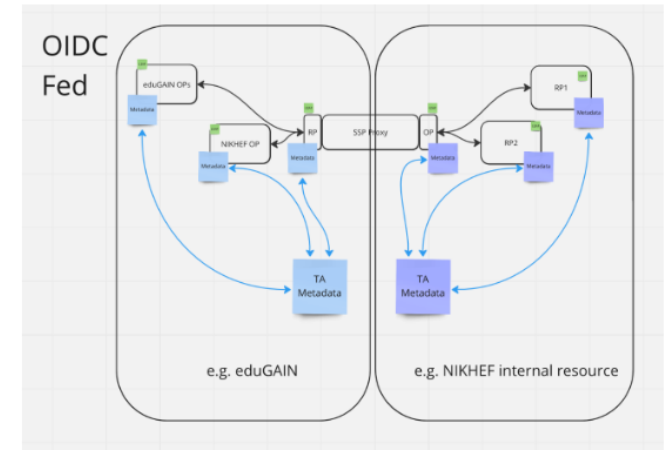
- what to do with non-European users?
- how to link the identities together



New trust models – what is the role of the proxy in OIDCFed? And Wallets?

In today's BPA proxy links both sides by being opaque, **both** for attributes **as well as** for trust

- does it *have* to be that way?
- separate claims/attribute transformation from trust bridging?
- can OIDCfed structure convey trust transparently? Should it?
- can we then be more flexible? or will it just confuse everyone?
- easier to bridge trust *across sectors* this way?
e.g. linking .edu, .gov, and private sector federations?
- how do wallets change the trust flow? Also with composite VCs?



David Groep:

Raise of hands

Who knows about

- Proxy: most in the room
- OIDC federation: few in the room
- Bridge PKI (public key infra): 1

What was the problem that triggered this session?

Proxies are wonderful, they can be opaque and expose things to the outside world..
Proxy into eduGAIN using SAML, token translation, attribute transformation, augmentation
Membership services?

OIDC world, to amalgamate a set of RPs

Essentially overloading the proxy with two roles, technical role of translating one for format to another (+ augment of claims), but also bridging trust between both "domains"
In OIDC federation, you can chain metadata statements not by publishing to a list, but building hierarchies, trust anchors who can sign intermediates . multiple signatures on the same

All about enabling research: FIM4R & communities are a key factor

Also in AARC-TREE we target a “co-creation process”

- support FIM4R to increase the reach of workshops in the next 2 years
- community review, ideas, and input on both policy and architecture
- start from the high-level requirements and broad community input

whatever we build must be *usable and available* by researcher communities first of all, and align to interoperability standard and open, collaborative research goals

Really a global activity: we want to engage everyone, in AARC TREE and beyond



Questions?

BUILDING OUR GLOBAL TRUST FABRIC

Nikhef

 Maastricht University



David Groep davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>

this work is co-supported by the Trust and Identity
work package of the GEANT project (GN5-1)

*in collaboration with many, many people
in the AARC+ Community, including
Christos Kanellopoulos, Nicolas Liampotis,
Licia Florio, Hannah Short, Maarten
Kremers, Niels van Dijk, David Crooks,
Dave Kelsey, Ian Neilson, Mischa Sallé,
Slavek Licehammer, Catharina Vaendel,
Liam Atherton, Arnout Terpstra, Jens
Jensen, and so many others!*

Thank you

Any Questions?

davidg@nikhef.nl



<https://aarc-community.org>

© members of the AARC Community and the AARC TREE consortium.
The work leading to these results has received funding from the
European Union and other sources.



Co-funded by
the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement No. 101131237 (AARC TREE).

