


David Groep
davidg@nikhef.nl

Nikhef

 Maastricht University

 eu gridpma

*part of the work programme of
GEANT 5-1 EnCo, EGI-ACE, and EOSC-Future*

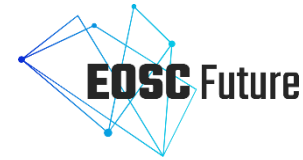
*the work has received co-funding from the
Horizon programme of the European Union* 

*co-supported by Nikhef and the Dutch
National e-Infrastructure coordinated by SURF* 

Building Trust and Security with AARC, IGTF, EOSC, & EnCo

*Enabling Communities through Trust, Identity,
and Security in our Open Science era*

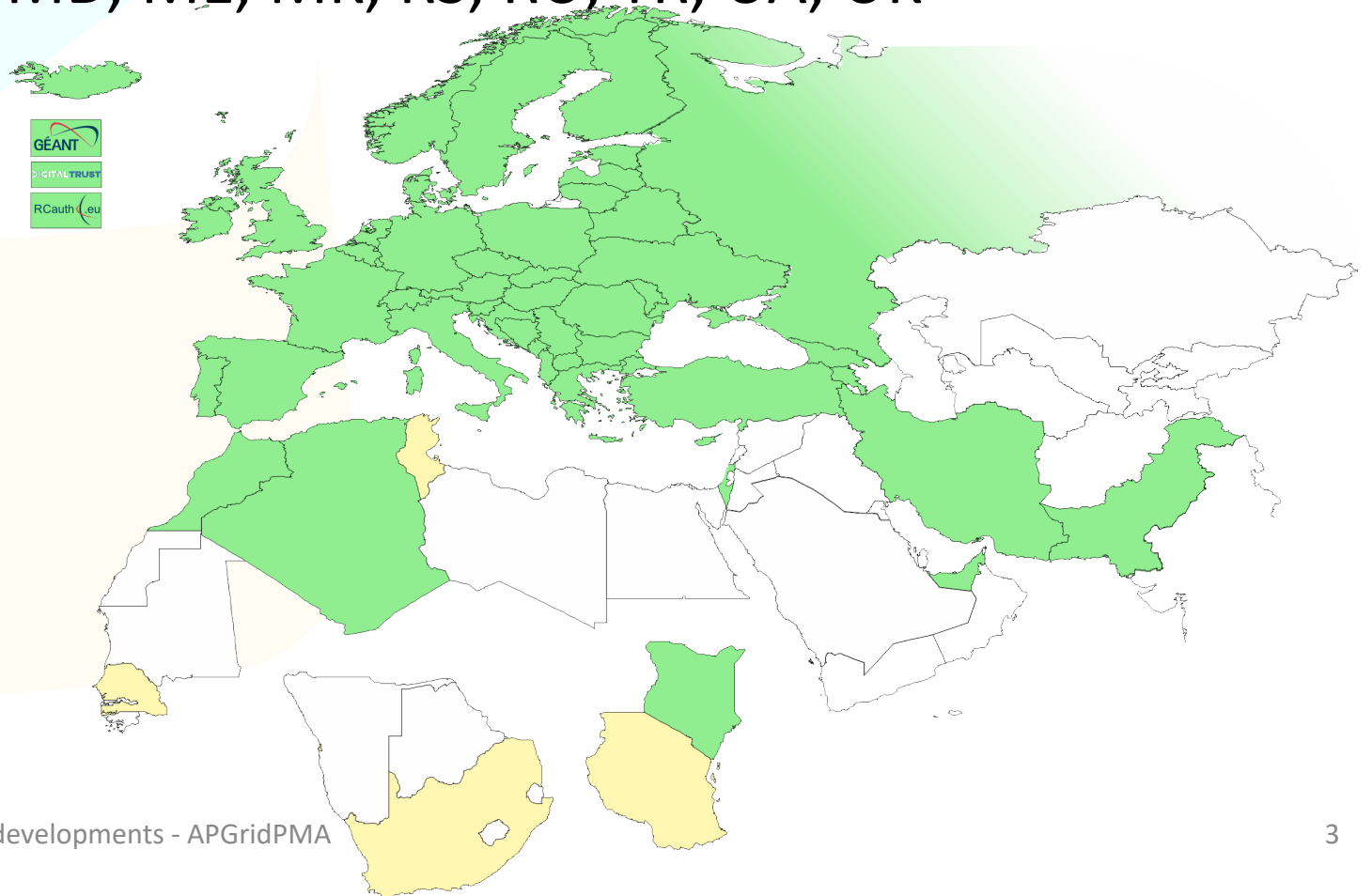
Meanwhile in the EUGridPMA+ ...



- EUGridPMA - constituency and developments
- S/MIME BR – separating authentication and email signing
- European Open Science – Security in the EOSC Interoperability Framework
- Attribute Authority Operations guideline
- Enabling Communities with GÉANT in GN5-1
- AARC's Technical Revision for Enhanced Effectiveness

EMEA area membership evolution

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



**Emphasis on collaboration
across the whole T&I space**

Membership and other changes

- Identity providers: both reduction and growth
 - migration to GEANT TCS is still ongoing
<https://wiki.geant.org/display/TCSNT/TCS+Participants+Sectigo>
 - CERN joining TCS via Renater (FR)
- Self-audit review
 - Cosmin Nistor as review coordinator
 - new self-audit model: real-time interaction between authority and reviewers helps!

Digital Trust <i>(Authority member)</i>	Scott Rea	Generic CP and CPS statements CA DigitalTrustAssuredCAG3-runbytheissuer (accruited:classic): CERT CRL concerns: ca-admins@digitaltrust.ae 9D:54:E9:A0:DE:59:80:4F:1A:41:01:E8:77:A2:08:0E:C2:BB:88:7D	2016-05-09	2022-01-27	2019-05-22 (2.Yr)
		CA DigitalTrustIGTFCA (accruited:classic): CERT CRL concerns: ca-admins@digitaltrust.ae 5F:27:FB:D9:B4:EA:82:66:71:59:CE:52:A3:7B:64:D5:65:6B:9E:18			
DutchGrid and NIKHEF CA <i>(Authority member)</i>	David Groep (6F298418) Dennis van Dok (7617EF19)	Generic CP and CPS statements CA NIKHEF (accruited:classic): CERT CRL concerns: ca@dutchgrid.nl F8:4D:ED:9B:42:34:58:F4:3B:AF:BF:0A:6E:1A:84:5C:18:34:5A:A3 Specific Policies and Practices	2001-03-01	2022-01-27	2020-09-08 (1.5yr)
		CA RCauth-Pilot-ICA-G1 (accruited:iota): CERT CRL concerns: ca@rcauth.eu 8B:E3:1E:7D:46:57:B1:19:E5:D7:CB:A8:17:4E:E6:F9:C9:18:29:4D			

- **Next meeting in Amsterdam, NL (SURF offices) May 22-23, 2023!**

RCauth.eu – a ubiquitous federated IOTA

- RCauth is an IGTF accredited IOTA (DOGWOOD class) CA
 - Online credential conversion
 - Connected to eduGAIN (R&S+Sirtfi) plus direct, e.g. EGI Check-in and eduTEAMS
- Inspired by and leveraging the delegation service from CILogon
- EOSC Future implemented High Availability setup across 3 sites



WLCG and server credentials study WG

- Increased use of automatic public cloud deployment (and at times lack of documentation) highlight the fact that in ‘conventional’ grid middleware server-trust and client-trust cannot be distinguished
- Similarly, while combined-assurance (DOGWOOD) is available for client-auth, there is no equivalent for server trust
- Although issues will change on introduction of ‘token-based’ access (which does distinguish client & channel trust), of limited help now

WLCG, with participants from the IGTF, set up a WG to study the issues

https://docs.google.com/document/d/1Sl0C_q-lGMCifChmFARHjsGzdnd-RM7O7jbpsGa8XRw





CA/B Forum developments

S/MIME BASELINE REQUIREMENTS

CA/BROWSER Forum

S/MIME BASELINE REQUIREMENTS

Table of Contents



Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

Current Version

Previous Versions

BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED S/MIME CERTIFICATES

CURRENT VERSION

[S/MIME Baseline Requirements v1.0.0](#) – adopted by Ballot [SMC01](#)

PREVIOUS VERSIONS

NA



Public Trust S/MIME (personal) is getting regulated

- It was basically a ‘free-for-all’, as long as the email address worked
- most ‘useful use’ for the general public signing was in bespoke certificates types (Adobe) or in Qualified Certificates (EC regulated)
- until now, the IETF personal requirements were much stricter than ‘public’ email signing, in that we did insist on a reasonable name and a ‘sponsor’ (organization) that was validated
- Now CA/BF is putting requirements on S/MIME for the first time

<https://cabforum.org/wp-content/uploads/CA-Browser-Forum-SMIMEBR-1.0.0.pdf>



Different 'profiles' and validations

- **Strict**
 - 825-days (2yr), limited RDN attributes allowed
 - intended only for S/MIME
- **Multi-purpose**
 - 825 days (2yr), slightly more eKUs allowed
 - crossover use cases between document signing and secure crossover use cases between document signing and secure email
- **Legacy**
 - 1185 days (3yr)
 - transitional profile (likely to be phased out in the end)
 - bit more freedom in subject, still allows DC naming, but otherwise not much more than MP
- **mailbox-validated**
 - just the rfc822name (only!)
- **organization-validated**
 - includes only Organizational (Legal Entity) attributes in the Subject
- **sponsor-validated**
 - Combines Individual (Natural Person) attributes and organizationName (associated Legal Entity) attribute
- **individual-validated**
 - Includes only Individual (Natural Person) attributes in the Subject

Sponsor validated

Sponsor-validated:

‘Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the subject:organizationName is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization.’

Certificate Type	Description
Mailbox-validated	Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.
Organization-validated	Includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated	Combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA.

Validation requirements

1. If the Certificate Request is for an Organization-validated or Sponsor-validated profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with [Section 3.2.2.1](#) or [Section 3.2.2.3](#). The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name “XYZ Co.” on the authority of Enterprise RA “ABC Co.”, unless the two companies are Affiliated as defined in [Section 3.2](#) or “ABC Co.” is the agent of “XYZ Co”. This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.’s Registered Domain Name.

commonName

7.1.4.2.2 Subject distinguished name fields

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)

Contents: If present, this attribute SHALL contain one of the following values verified in accordance with [Section 3.2](#).

Certificate Type	Contents
Mailbox-validated	Mailbox Address
Organization-validated	<code>subject:organizationName</code> or Mailbox Address
Sponsor-validated	Personal Name, <code>subject:pseudonym</code> , or Mailbox Address
Individual-validated	Personal Name, <code>subject:pseudonym</code> , or Mailbox Address

If present, the Personal Name SHALL contain a name of the Subject. The Personal Name SHOULD be presented as `subject:givenName` and/or `subject:surname`. The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but SHALL be a meaningful representation of the Subject's name as verified under [Section 3.2.4](#).

Where does that leave us?

- The 'Legacy' profile (still) allowed 'other' attributes, so for the moment e.g. DC prefixing would be OK
- However the commonName is regulated, which
 - impacts uniqueness identifiers (like ePPN as used in TCS)
 - does not allow for 'Robot's in the commonName these would go to Pseudonym, which is an ill-supported attribute, and anyway inflicts a subjectDN change
- who knows when the legacy profile will be deprecated! Will not be long 😞

However ...

... contrary to the host-cert issue, there is no joint-trust needed for email signing and client authentication!

- separating these should always have been done:
using TCS Personal certs for authentication is bad (since they are not unique), and
using TCS IGTF MICS client certs for S/MIME email is bad (since it's 7-bit ASCII only)
- this just formalizes that move beyond restricting keyUsage & eKU

Anticipated moves

- Have the S/MIME personal certs move to sponsor-validated (multi-purpose) BR-compliant certificates
- Move the *client authentication* trust to a 'private CA' (non-public trust anchor), retaining *exactly the same subject DNs*, just a different ICA issuerDN
- Add some additional ICAs and non-public Roots to the IGTF distribution and for IGTF RPs the change is minimal and transparent
- Inform relying parties, *also outside of the IGTF*, that client trust will become a specific decision. This is probably good, also for OpenVPN services, web access (.htpasswd), &c. The IGTF RPs are not impacted, others likely will be.

User awareness

- This is a change in communications and documentation as well, not only a set of technical changes
- In request systems, have to clearly distinguish for users *which product to order*. For example:
 - “Personal” == only for EMAIL and NOT for authentication
 - renaming “IGTF MICS Personal” to “Personal Authentication” and explain
 - renaming “IGTF MICS Robot Personal” to “Personal Automated Authentication”?
 - forking “IGTF Classic Robot Email”
 - Authentication-only (IGTF) profile “Classic Robot Email”
 - Email signing profile “Organisation-validated S/MIME signing” (i.e. team-based or role-based)

Other CABF things to keep in mind

- Server SSL BR has already been updated
 - the provision for using DC prefixing has been retained
- But expect shorter validity periods in the future
 - start preparing for 90-day max in your service deployment automation systems
 - increased use of automation (ACME OV using client ID+secret)

```
[root@hekel ~]# certbot certonly \  
  --standalone --non-interactive --agree-tos --email davidg@nikhef.nl \  
  --server https://acme.sectigo.com/v2/GEANTOV \  
  --eab-kid DUniqueID_forthisclient --eab-hmac-key mv_v3ryl0n9s3cr3tK3y \  
  --domain hekel.nikhef.nl --cert-name OVGEANTcert
```



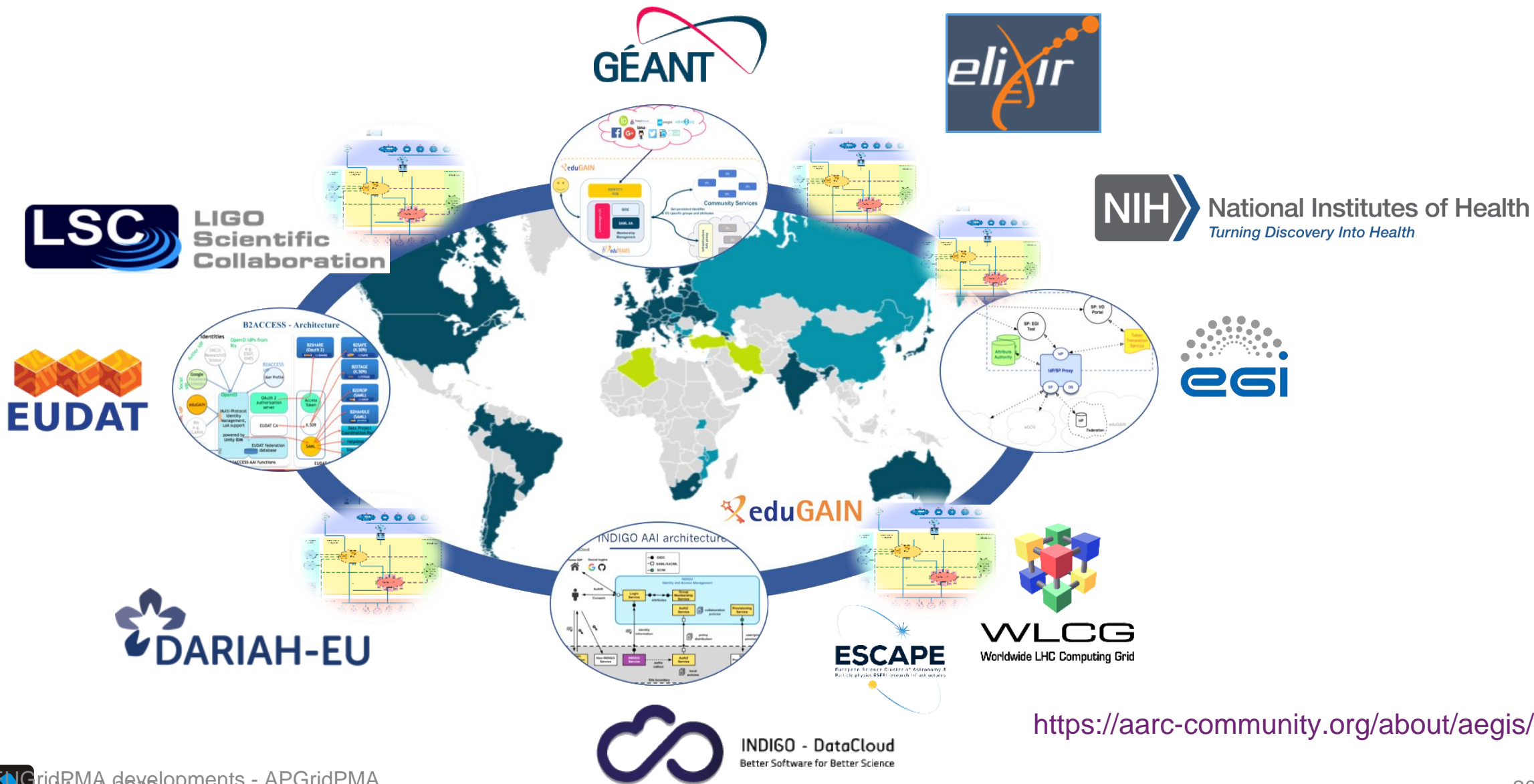
European Open Science Cloud

EOSC Security Baseline

Evolving the Policy Development Kit in WISE SCI

A SECURITY BASELINE FOR DIVERSE INFRASTRUCTURES AND THE EOSC

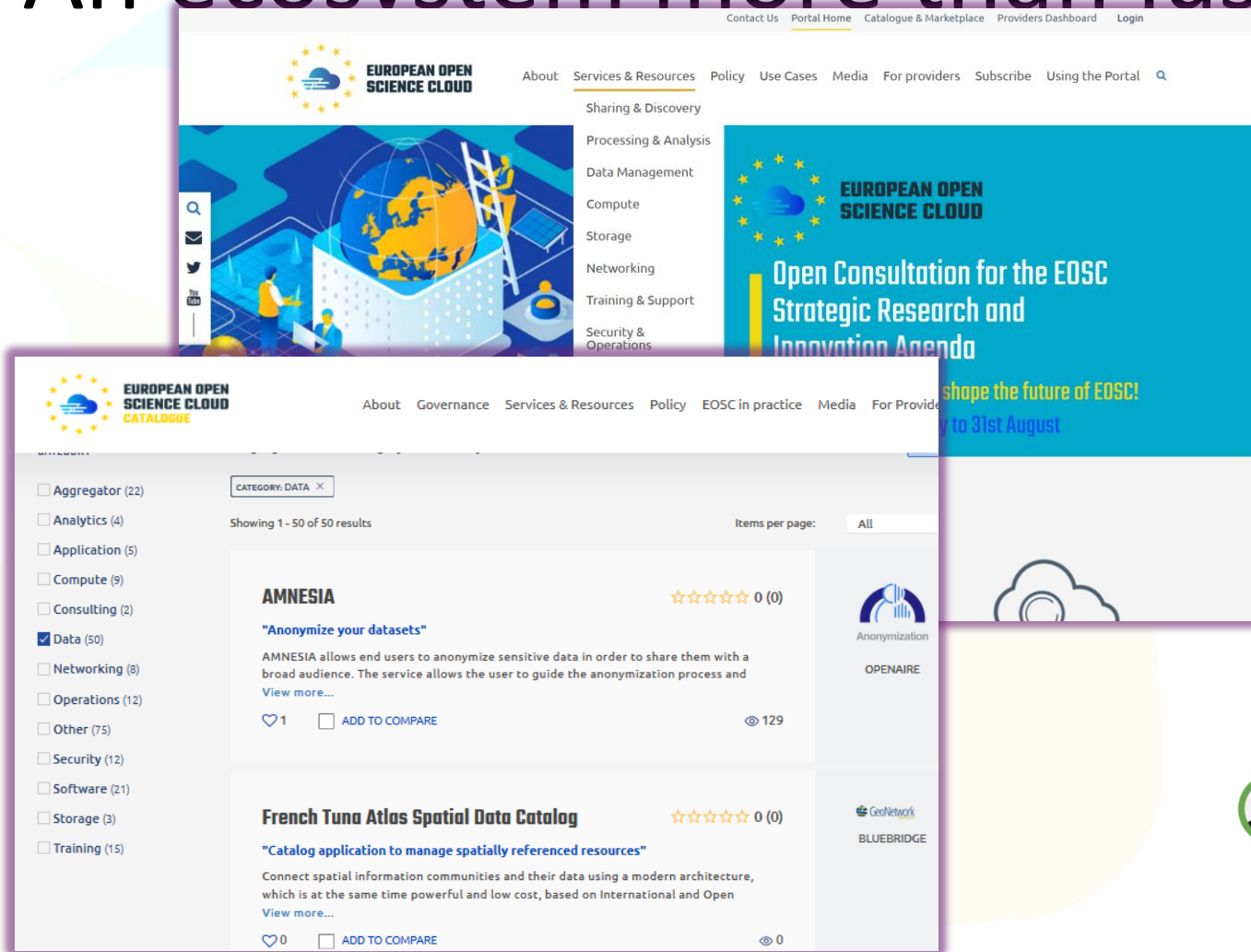
European Open Science Cloud - Interconnecting communities



<https://aarc-community.org/about/aegis/>



An ecosystem more than just the infrastructure

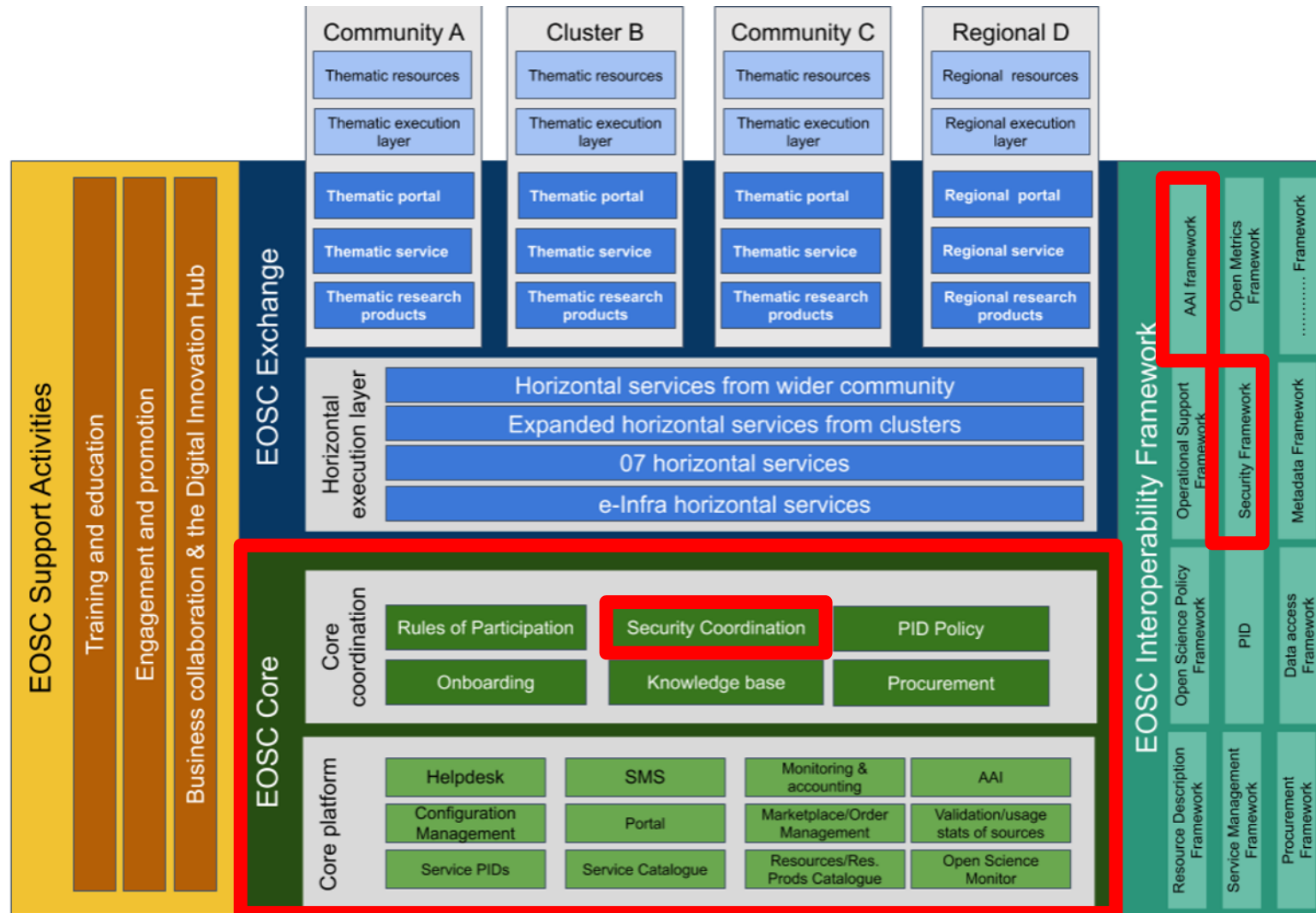


circle diagram: from Ignacio Blanquer's ISGC 2022 keynote Digital Skills for FAIR and open science doi.org/10.2777/59065

EOSC Portal (<https://www.eosc-portal.eu/>) – as built by EOSChub



The EOSC ecosystem – core and an ‘exchange’



Back to Basics: the few tenets for the ecosystem security



- **From promoting and monitoring capabilities to managing core risk**

A service provider should

- **do no harm** to interests & assets of users
- **not expose *other*** service providers in the EOSEC ecosystem to enlarged risk as a result of *their* participation in EOSEC
- **be transparent** about its infosec maturity and risk to its customers and suppliers

this will mean *some minimum requirements* in the Rules of Participation

Photo Hippocrates tomb: Melania Stubos, CC-BY-SA-3.0
<http://himetop.wikidot.com/hippocrates-funeral-monument>

Security: from infrastructure to ecosystem view

Original AARC PDK version of “Service Operations” was specific & prescriptive

- includes ‘service-internal’ operations and software
- embedded in the PDK document suite:
does not work well as a ‘stand-alone’ document
- has built-in assumption of coherent and coordinated single infrastructure

procedures [17], and must assist the Infrastructure in security incident response.

c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.

6. Provisioning of Services is at your own risk. Any software provided by the Infrastructure is provided <on an as-is basis | in accordance with service level agreements>, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure is correct or sufficient for any particular purpose. The Infrastructure and other Participants acting as service hosting providers are not liable for any loss or damage in connection with your participation in the IT Infrastructure.

7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate

8. Your Service’s connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions

~~Upon retirement of a service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for~~

New EOSC Baseline Process

Co-development of EOSC Future & AARC Policy Community

- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

AARC Policy team consultation > AEGIS > EOSC

- just 12 itemised points:
<https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline>
- complemented by an 'FAQ' with guidance and refs (no new standards, there is enough good stuff out there)
- leverages *Sirtfi* framework
- connects to the Core Security Team

All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

1. comply with the [SIRTFI security incident response framework](#) for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the [confidentiality requirements](#) of information gained as a result of their Service's participation in the Infrastructure.
5. [respect the legal and contractual rights of Users](#) and others with regard to their personal data processed, and only use such data for administrative, operational, accounting, monitoring or security purposes.
6. [retain system generated information](#) (logs) in order to allow the reconstruction of a [coherent and complete view of activity](#) as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted [IT security best practices and governance](#), such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. [collaborate in a timely fashion](#) with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.



But an FAQ is almost mandatory

EOSC Security Operational Annotated Baseline

Created by David Groep, last modified on Jan 18, 2022

The EOSC Security Operational Baseline sets minimum expectations and puts requirements on the behaviour of those offering services to users, and on communities connected to the EOSC, when interacting with the EOSC infrastructure and peer services. Worded in an intentionally concise manner, the 12 key requirements may give rise to additional questions, or in general can benefit from concrete examples and guidance. In this "FAQ" document, each of the key baseline items is put in context with additional examples, best practices, and generally helpful ideas.

Development information

This FAQ is based on the dynamic source document that was [edited here](#). That version is no longer in active use, but retained during the endorsement process as background information.

- Can you elaborate on what is meant by item 3 (new: 9) and its incident response requirements?
- What are 'IT security best practices' in item 4 (new: 7)?
- What does "honour the confidentiality requirements of information" in item 6 (new: 4) mean?
- What are "the legal and contractual rights of Users and others with regard to their personal data processed as part of service delivery" in item 7 (new: 5)?
- "Retain system generated information (logs)" in item 8 (new: 6) sounds rather open-ended. What do I need to do? And why?
- "Aggregated centrally wherever possible, and protected from unauthorised access or modification" in item 8 (new: 6), how and why?
- Log aggregation in the layered and composite infrastructure of EOSC
- What about the 'reconstruction of a coherent and complete view of activity' when you have a 'layered technology stack' mentioned in item 12 (new: 6)?
- What are "Named persons"?

Can you elaborate on what is meant by item 3 (new: 9) and its incident response requirements?

Item 3 talks about security incident response. In an interwoven environment it is vital that data about incidents is shared and communicated to detect, analyse, contain and eradicate malicious actors while preserving the necessary evidence for analysis and post-processing. For EOSC, there is a dedicated team of incident response specialists to aid with this task. This team can also communicate between different service providers affected by the incident, help in getting necessary data from related services and disseminate data to help others.

For incident response, there is a documented process you can find from the EOSC Wiki. It acts as a recommendation and guideline to help different actors in case of computer security incidents. It is strongly recommended that all service providers implement the procedure as ably as possible, but in such a way that it serves the needs which are recognised by the service owners and operators. The starting point for all providers is to be aware of the process and from where they can get help in case of need, as well as understanding the need to share information to protect EOSC and other service providers.

You can find the procedure in EOSC Future ISM.

The EOSC incident response team can be contacted via abuse AT eos-security.eu.

What are 'IT security best practices' in item 4 (new: 7)?

On a global scale there are myriad different documents and sources defining best practices to secure different types of information systems and even the entire organisations. It is important to follow well known recommendations that fit your needs. This can depend on the scale of your service, organisation, technology choices and even your service's location.

and a way to both get the required information out of providers, gauge maturity, and raise awareness ...

Introduction

By responding to this questionnaire, you will get basic information about security requirements in the EOSC. The questions are based on the security baseline and other security activities provided by the EOSC to protect the infrastructure and ensure compliance.

Questions

Service name (provide)
Running since (provide)
Service dependencies within EOSC (provide)
Contact details (e.g. your email address)

Generic questions:

1. Security contact of the service: [insert email]
 - a. How many people are responsible to answer any contacts initiated via this contact point (0, 1, 2-5, 6 or more)
 - b. What are the expected operational hours of the security contact (low expectations, best effort, random, generic local office hours (8-16 +/- 2h), 24/7)
 - c. How much delay is to be expected after a contact during office hours (4 hours or less, 4 < delay <= 8, 8 < delay <= 24, days)
2. Is the service aware of a requirement to have an AUP or terms of use (yes, no, what's this)
How is it ensured that all users are aware of the AUP or terms of use (user has to





EOSC Interoperability Framework

EOSC Portal - A gateway to information and resources in EOSC

[Home](#)

EOSC Interoperability Framework


EOSC Interoperability Framework



About the EOSC Interoperability Framework (EOSC-IF)

Enabling interoperability across resources and services is essential for building a European Open Science Cloud that is federated and fit for purpose. In turn, interoperability guidelines are necessary to facilitate the cross-discipline collaboration of researchers, providers and research communities.


[LEARN MORE](#)



EIAB and EIAC Charter

The EOSC Interoperability Framework aims to provide a set of

LATEST NEWS



Science communication of RDA calls in the context of EOSC

The Research Data Alliance (RDA) and EOSC Future are unlocking a budget of 15000€ in their latest call for highly...





AARC-G071

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

ATTRIBUTE AUTHORITY OPERATIONAL SECURITY

Taking proper care of trust sources

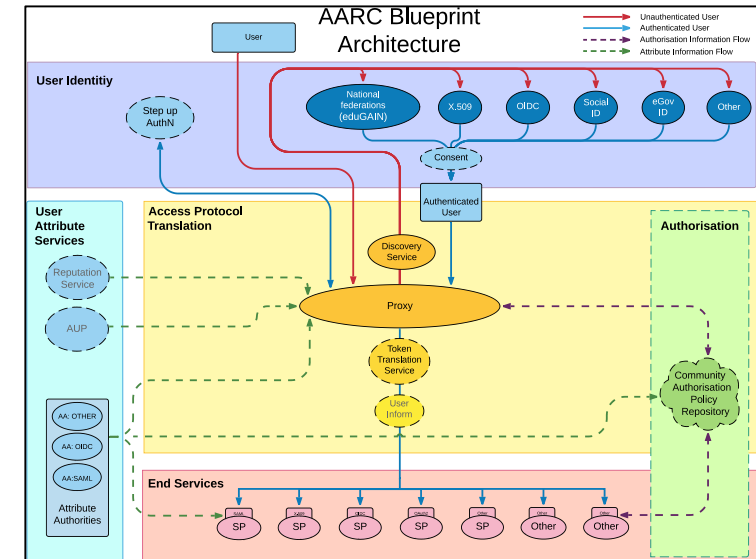
Protections for (IGTF) identity providers are known and documented

- 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	CA 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	CA 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	FEE'S 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 CA 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

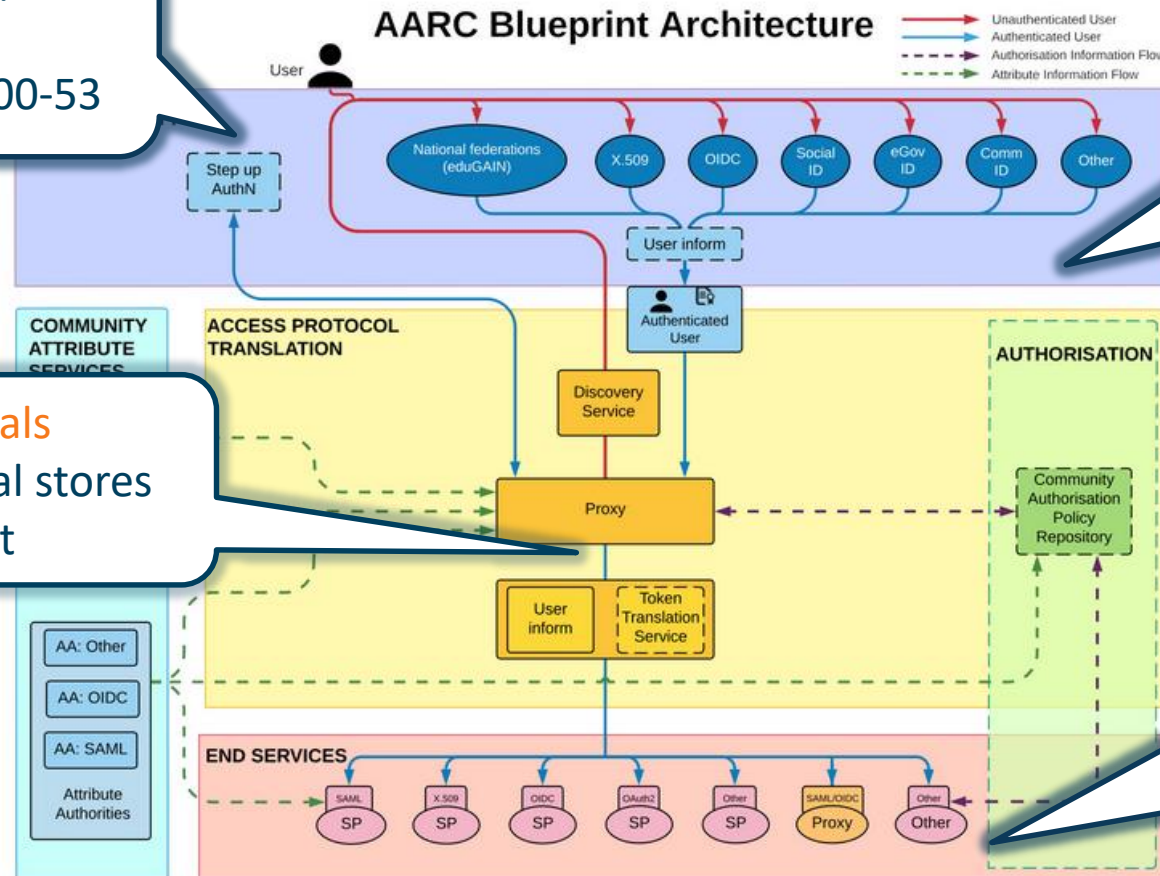
RFC6238/4226
FIPS140
NISTSP800-53

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

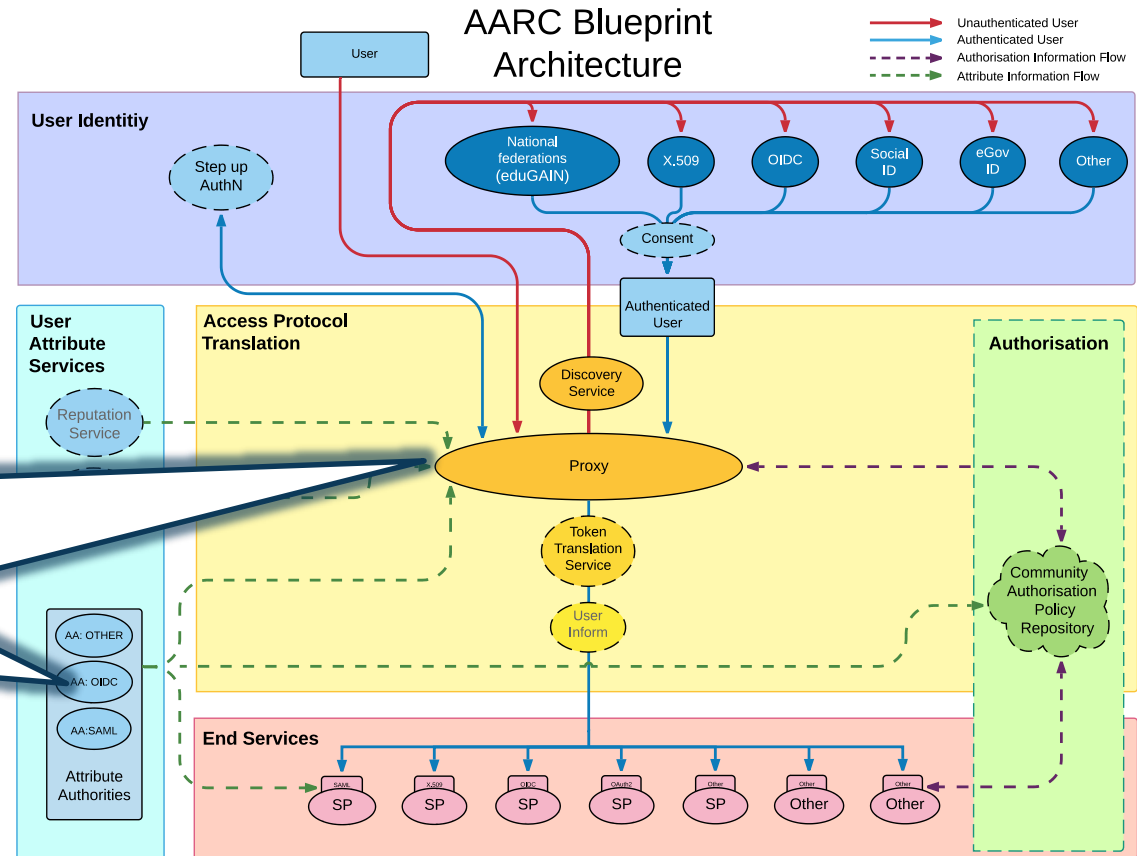
Service provider operations
ISO27k
Sirtfi
Infrastructure response plans



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-G071: keeping users & communities protected, moving across models

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**

formerly AARC-G048bis



March 2023

European and EUGridPMA developments - APGridPMA

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

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

AARC-G071

*Guidelines for Secure Operation of Attribute Authorities
and issuers of statements for entities*



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

Deployment guidance included ...

4.2. Attribute Management and Attribute Release

AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

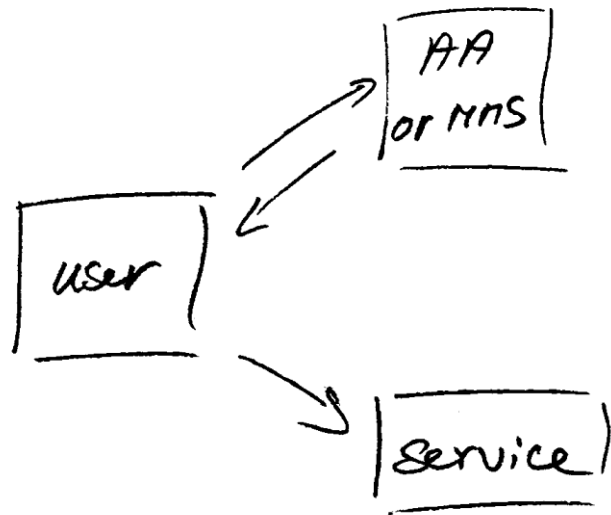
By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

AMR-3

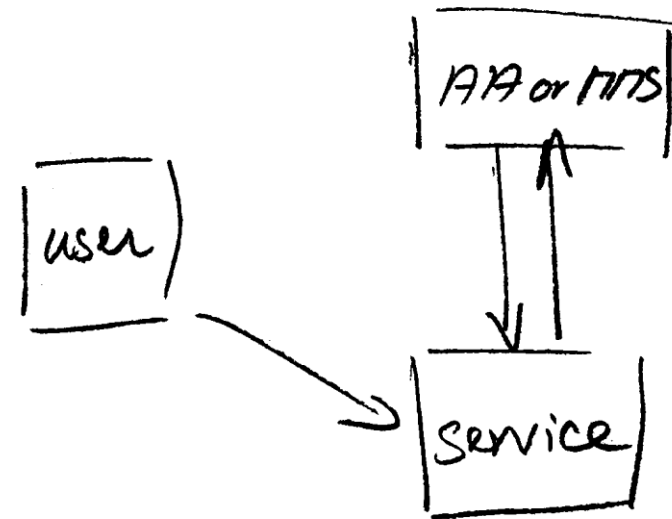
It is recommended that the AA Operator provide a capability for the community to

Protecting the community membership data and its proxy

Intentionally targeted broader than just the push model, since operational security spans data centres and infrastructures using other forms of AA membership management (SAML, OIDC, LDAP, ...)



push model – the common BPA method (e.g. SAML AttributeStatement, VOMS AC)



pull model – common when using directories (e.g. LDAP in PRACE, userinfo endpoint in OIDC)

When the AA is in a managed environment ...

Many of the recommendations are already implemented ‘implicitly’

- because common software implements it: e.g. signing SAML assertions and JWTs
- because a good data centre already has network monitoring and central logging in place
- because you signed up to Sirtfi (didn't you?) – so you collaborate in incident response
- because you have trained IT operations personnel looking after the service

And some are intuitive best practice

- like assigning a unique and lasting name to a group
- because implemented controls ought to be those that have been documented

Some items contain reminders about appropriate values and recommendations that are good practice - based on the relevant standards involved



Implementation of the AA Operations (“AAI proxy”) 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

March 2025



G071 self-assessment process

- Self-assessment by WLCG, UK-IRIS and eduTEAMS
- mutual review process also improves on the G071 guideline itself!

Review-sheet-G071-template .XLSX

File Edit View Insert Format Data Tools Help Last edit was on 14 February

100% E % .0_ .00 123 Calibri 11 B I S A

A1 fx

Item	Description	Status	References	Review comments
AN-1	Identifiers of the AA Operator and the AA must both be non-reassigned and globally unique.			
AN-1.2	In addition, the identifier of the Community should be unique.			
AN-1.3	Community User Identifiers for subjects and attributes should be chosen in accordance with the AARC Guidelines and the Community Membership Management policy [AARC-G003].			
AN-1.4	The AA must use a defined naming scheme for subjects and attributes.			
AN-1.5	Subject identifiers must be non-reassigned and unique within an AA.			
AMR-1	The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.			In a shared multi-tenancy setup where the AA Operator is the controller, this is actually defined by the operator, not the Community. The semantics must align with the AARC Guidelines, so is not only the community. So "The Controller must define ..." The "Owner" or "Service Owner" is better than AA operator in those fields, or Community
AMR-1.2	semantics			
AMR-1.3	lifecycle			

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





Federated Services









eduGAIN

T&I Incubator

and ... (ask Maarten Kremers!)

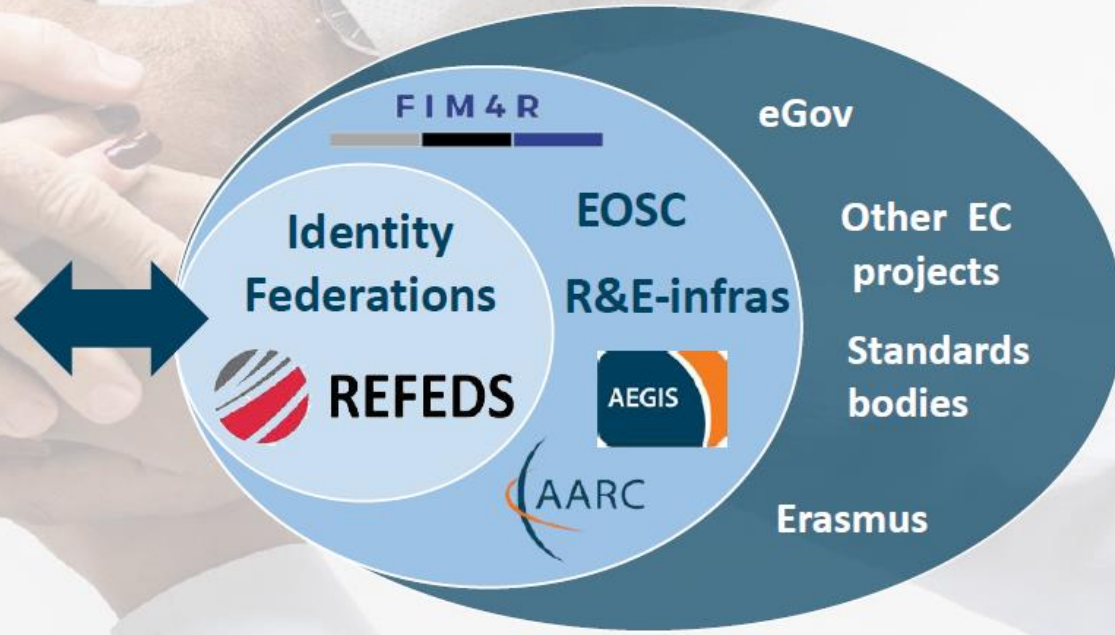
ENABLED COMMUNITIES IN GÉANT GN5-1

T&I Team and Key Collaborations

T1		Paul Dekkers SURF	
T2		Davide Vagheti GARR	
T3	Core AAI Platform	Christos Kanellopoulos GÉANT	
T4		Michelle Williams GÉANT	
T5		Niels van Dijk SURF Michael Schmidt LRZ	 
T6	Enabling Communities	Maarten Kremers SURF	
T7	Distributed Identities	Christoph Graph, SWITCH	

WP 5

Marina Adomeit SUNET
Maarten Kremers SURF





Implementation of eduGAIN
Future WG recommendations



78

Identity Federations

5100+

Identity Providers

3600+

Service Providers

TRUST & IDENTITY INCUBATOR



Develop, foster & mature new ideas in T&I space

- Identity & Access Management
- Standards & Protocols
- Security & Privacy



TIM

TRUST & IDENTITY
MENTORSHIP PROGRAMME



Landing results is hard

Room in other activities
for uptake

Place to practice and learn
more



4 to 6 activities in parallel

Community consultations

7M cycle, 1M sprint

2 public sprint demos per cycle



Enabling Communities

Marketing and Communication

Partner Relations

Services Owners

Service's Business Development

eScience Global Engagement

Enabling Communities

International Relations

Embedded Business Developers





AARC Community – you can check in, but never leave!

TECHNICAL REVISION FOR ENHANCED EFFECTIVENESS



Collaboration and sharing is critical for research

“Authentication and Authorisation Infrastructures (AAls) play a key role in enabling federated interoperable access to resources.”

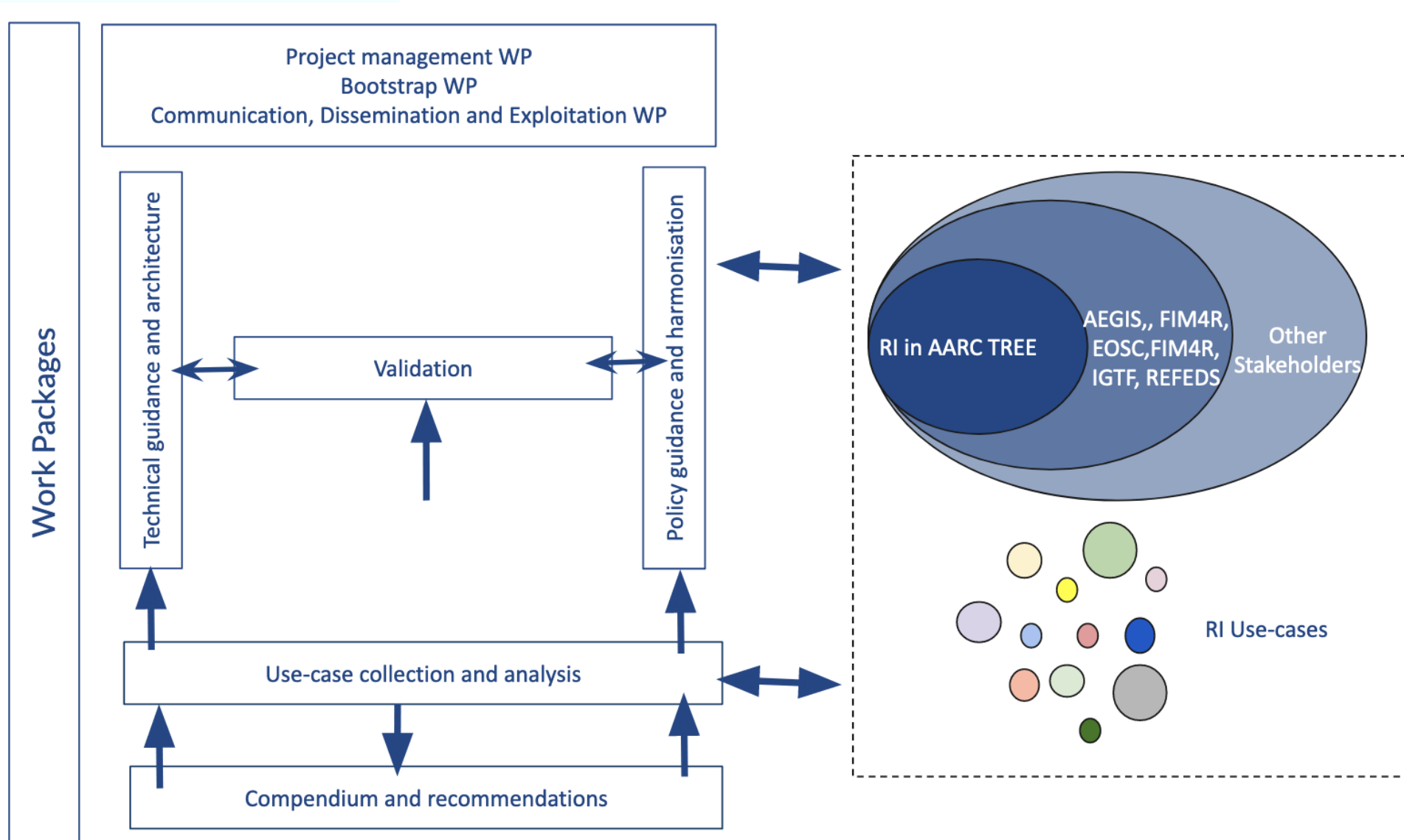
AARC Technical Revision to Enhance Effectiveness (AARC TREE) plans to

- define common strategies for the development and deployment of AAls in the pan European Research Infrastructures at large
- to improve access and sharing of scientific resources and
- to improve interoperability among research infrastructure communities across the thematic areas

Technical Revision objectives

1. **Capture and analyse** new **Authentication** and **Authorisation interoperability requirements** (as emerging that support integration use-cases across the thematic area) and provide a **landscape analysis** of AAls services (including gaps) in the RIs represented in AARC TREE
2. **Define and validate** new technical and policy guidelines for the AARC BPA that address RIs use-cases. This will **improve** the **integration** of RIs across thematic areas and increase the ability of RIs to support emerging needs
3. **Expand the number of research communities** that can implement the AARC BPA and/or the AARC guidelines, by providing a **validation environment and toolkits**. At the same time **support** existing AARC communities in adopting new guidelines
4. **Bring RIs**, e-Infrastructures and relevant stakeholders together to **align strategies** to integrate new technologies, better interoperate and share resources across thematic areas and produce a compendium and recommendations for different stakeholders

Leveraging our AARC community & structures





Questions?

BUILDING OUR GLOBAL TRUST FABRIC

Nikhef

 Maastricht University



<https://www.nikhef.nl/~davidg/presentations/>  <https://orcid.org/0000-0003-1026-6606>

David Groep *davidg@nikhef.nl*

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, Jens Jensen, and so many others!



Thank you

davidg@nikhef.nl



This work has been co-supported by projects that have received funding from the European Union's Horizon research and innovation programmes under Grant Agreement No. 101100680 (GN5-1), 856726 (GN4-3), and 730941 (AARC2).

EOSC Security work has received funding from the European Union's Horizon research and innovation programmes under Grant Agreement No. 101017536 (EOSC Future).