AARC Authentication and Authorisation for Research and Collaboration

Developments in AAI Architecture and Policy

from community-first to community-driven

David Groep
AARC ARGIS Policy Area Coordinator
Nikhef Physical Data Processing group

Nikhef

IGTF and Security Workshop, Taipei
March 10, 2020

with material kindly contributed by Christos Kanellopoulos (GEANT) and Andrea Ceccanti (INFN)

AARC – leverage federated identity to facilitate research collaboration

Identity Federation & eduGAIN

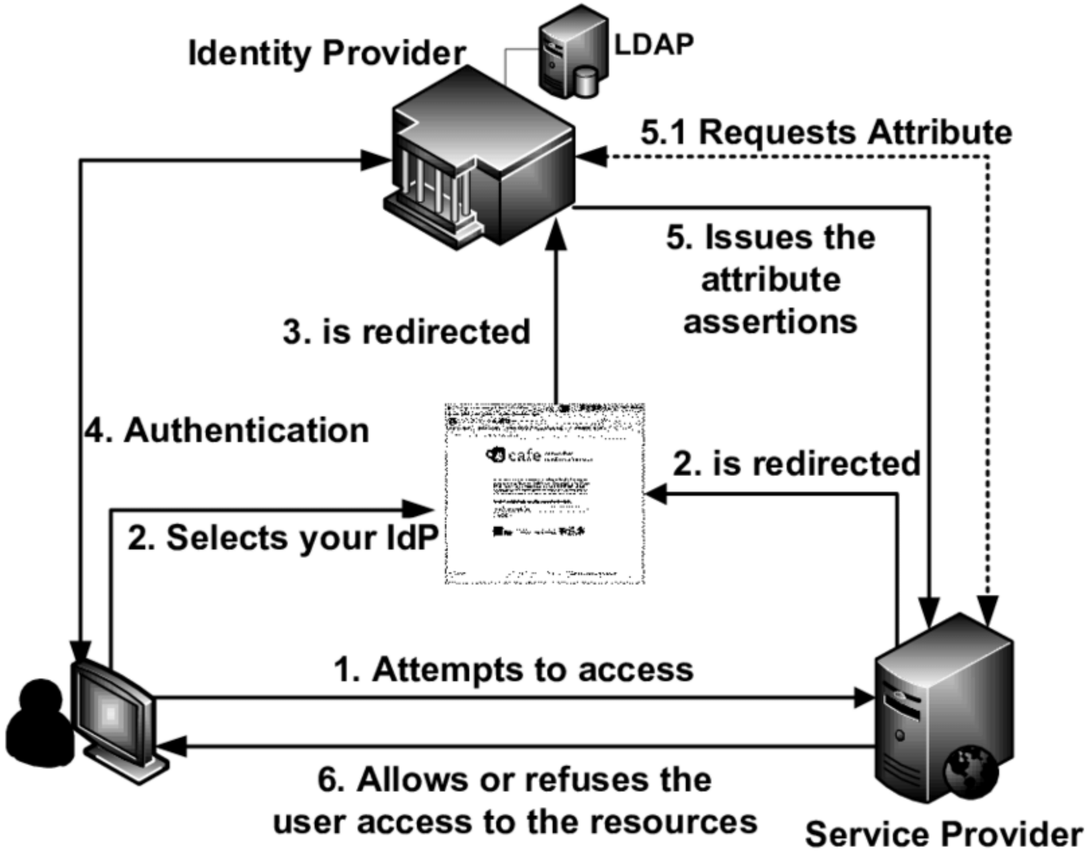
Research collaborations

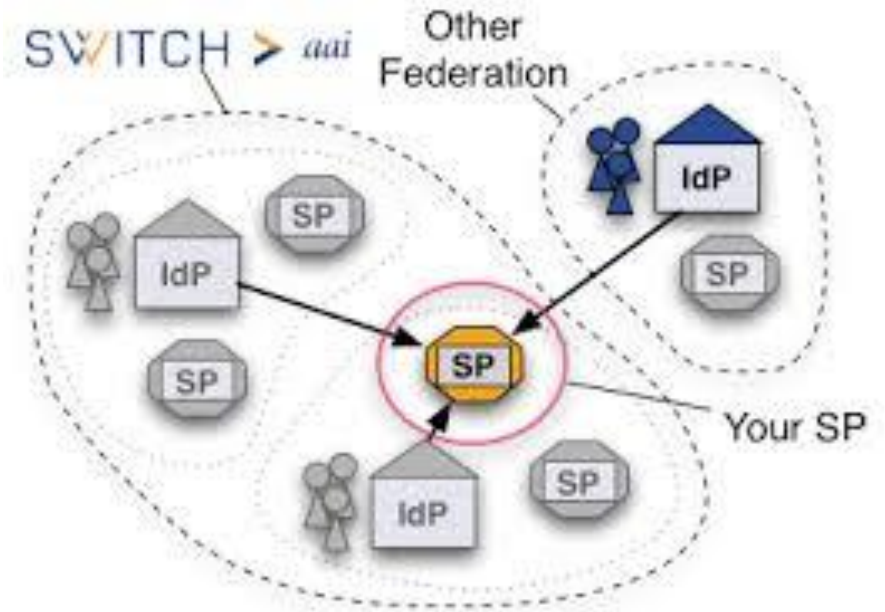
Our AARC Community

GÉANT
CESNET
Consortium GARR
JÜLICH
CERN
Science & Technology Facilities Council
instruct Integrating Biology
EMBL
MORAVIAN LIBRARY
PSNC
Nikhef
KIT
LIBER
Reti
egi
SURFNET
grnet
CYFRONET
UC
CARDIFF UNIVERSITY PRIFYSGOL CAERDYDD
INAF
INFRAFRONTIER
BBMRI-ERIC
DAASI International

… open to all …

Identity federation for research … and enterprise



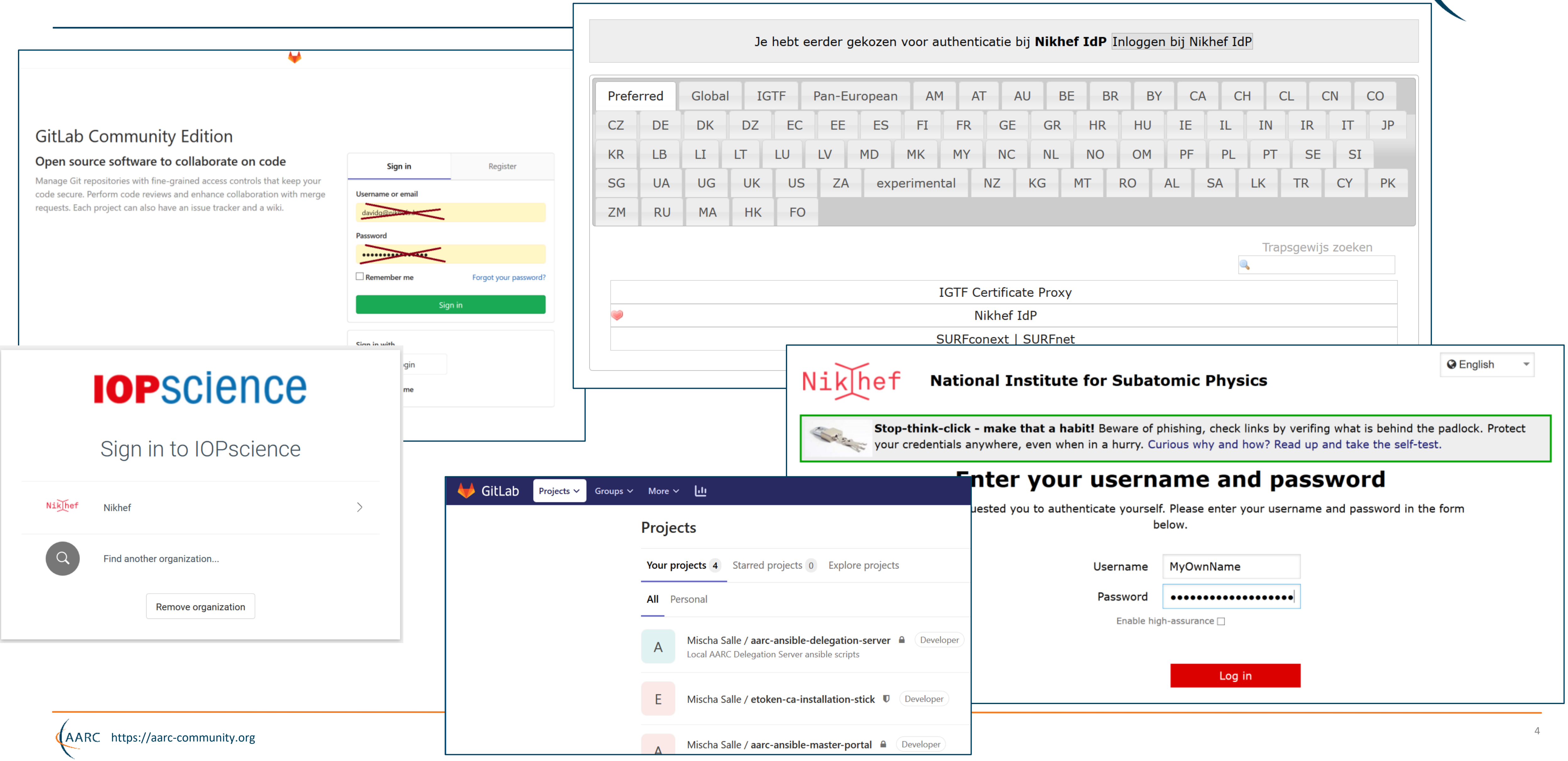


Bring federated access to eResearch

Avoid a future in which new research collaborations develop independent AAIs

Build on existing tools and framework

Service Provider Examples



GitLab Community Edition

Open source software to collaborate on code

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Sign in | Register

Username or email: [redacted]

Password: [redacted]

□ Remember me — Forgot your password?

Sign in

Sign in with ... gin ... me

Je hebt eerder gekozen voor authenticatie bij **Nikhef IdP** Inloggen bij Nikhef IdP

Preferred	Global	IGTF	Pan-European	AM	AT	AU	BE	BR	BY	CA	CH	CL	CN	CO			
CZ	DE	DK	DZ	EC	EE	ES	FI	FR	GE	GR	HR	HU	IE	IL	IN	IR	IT	JP
KR	LB	LI	LT	LU	LV	MD	MK	MY	NC	NL	NO	OM	PF	PL	PT	SE	SI
SG	UA	UG	UK	US	ZA	experimental	NZ	KG	MT	RO	AL	SA	LK	TR	CY	PK	
ZM	RU	MA	HK	FO													

Trapsgewijs zoeken

IGTF Certificate Proxy

Nikhef IdP

SURFconext | SURFnet

IOPscience

Sign in to IOPscience

Nikhef

Find another organization...

Remove organization

GitLab — Projects — Groups — More

Projects

Your projects 4 — Starred projects 0 — Explore projects

All — Personal

A — Mischa Salle / aarc-ansible-delegation-server — Developer
Local AARC Delegation Server ansible scripts

E — Mischa Salle / etoken-ca-installation-stick — Developer

A — Mischa Salle / aarc-ansible-master-portal — Developer

Nikhef — **National Institute for Subatomic Physics** — English

Stop-think-click - make that a habit! Beware of phishing, check links by verifing what is behind the padlock. Protect your credentials anywhere, even when in a hurry. Curious why and how? Read up and take the self-test.

nter your username and password

uested you to authenticate yourself. Please enter your username and password in the form below.

Username: MyOwnName

Password: ••••••••••••••••••

Enable high-assurance □

Log in

Where did we come from & where should we go …

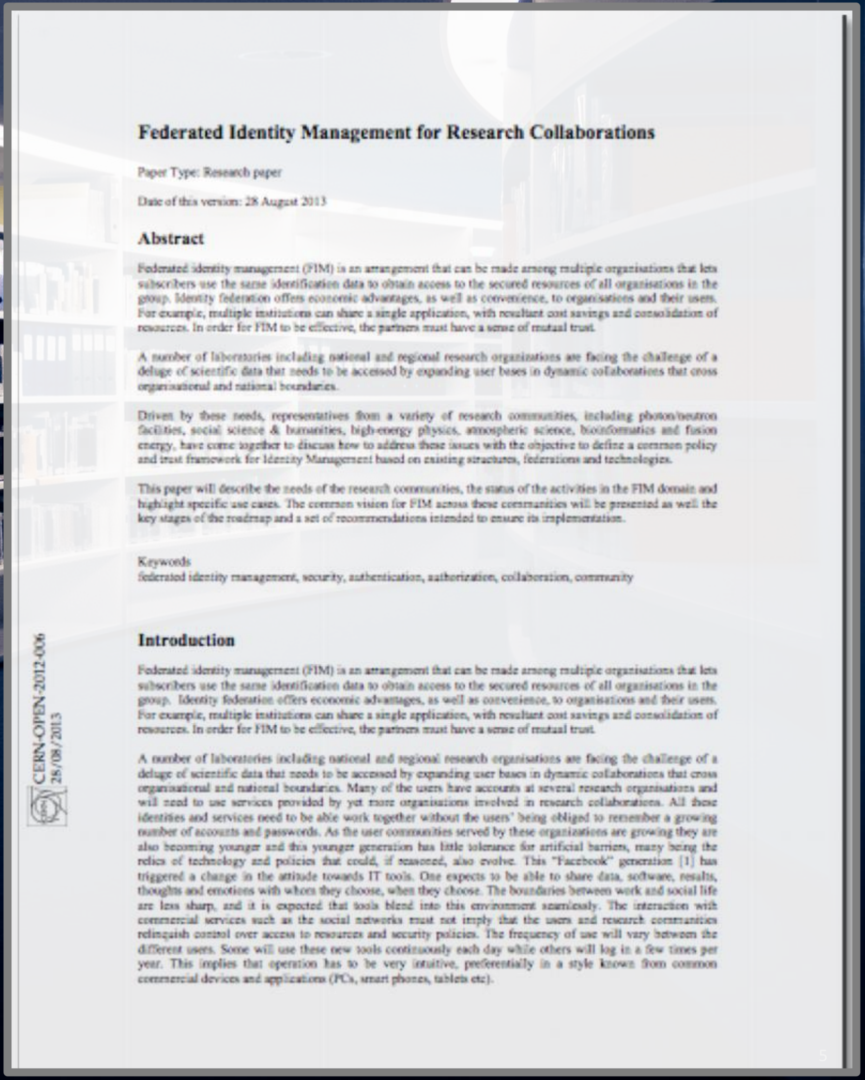
European Commission

Advancing Technologies and Federating Communities

A Study
on Authentication
and Authorisation Platforms
For Scientific Resources
in Europe

FINAL REPORT
A study prepared for the European Commission
DG Communications Networks, Content & Technology

Digital Agenda for Europe



Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

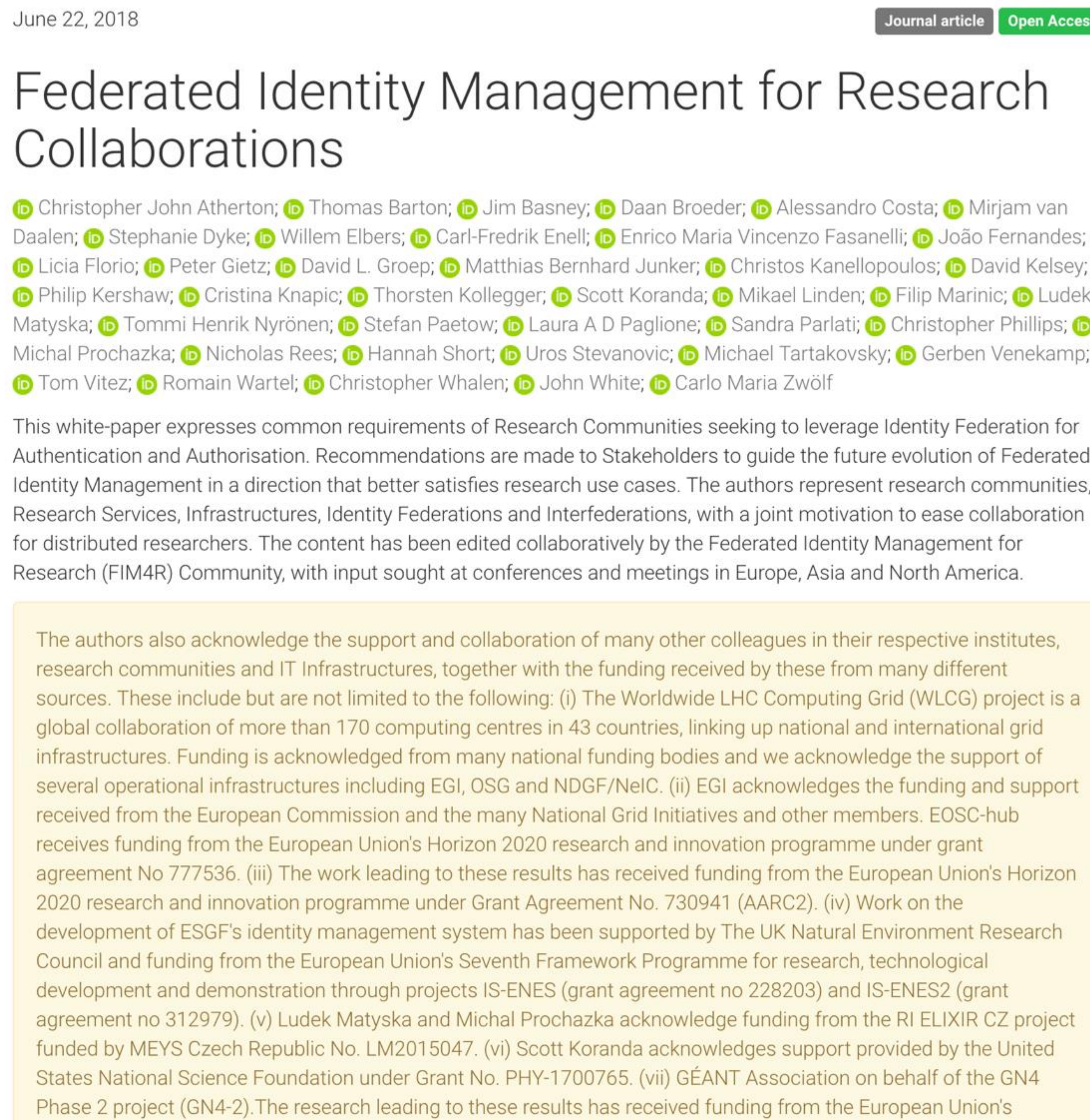
Keywords
federated identity management, security, authentication, authorization, collaboration, community

CERN-OPEN-2012-006
28/08/2013

Introduction

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in research collaborations. All these identities and services need to be able work together without the users' being obliged to remember a growing number of accounts and passwords. As the user communities served by these organizations are growing they are also becoming younger and this younger generation has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This "Facebook" generation [1] has triggered a change in the attitude towards IT tools. One expects to be able to share data, software, results, thoughts and emotions with whom they choose, when they choose. The boundaries between work and social life are less sharp, and it is expected that tools blend into this environment seamlessly. The interaction with commercial services such as the social networks must not imply that the users and research communities relinquish control over access to resources and security policies. The frequency of use will vary between the different users. Some will use these new tools continuously each day while others will log in a few times per year. This implies that operation has to be very intuitive, preferentially in a style known from common commercial devices and applications (PCs, smart phones, tablets etc).



June 22, 2018

Journal article Open Acces

Federated Identity Management for Research Collaborations

Christopher John Atherton; Thomas Barton; Jim Basney; Daan Broeder; Alessandro Costa; Mirjam van Daalen; Stephanie Dyke; Willem Elbers; Carl-Fredrik Enell; Enrico Maria Vincenzo Fasanelli; João Fernandes; Licia Florio; Peter Gietz; David L. Groep; Matthias Bernhard Junker; Christos Kanellopoulos; David Kelsey; Philip Kershaw; Cristina Knapic; Thorsten Kollegger; Scott Koranda; Mikael Linden; Filip Marinic; Ludek Matyska; Tommi Henrik Nyrönen; Stefan Paetow; Laura A D Paglione; Sandra Parlati; Christopher Phillips; Michal Prochazka; Nicholas Rees; Hannah Short; Uros Stevanovic; Michael Tartakovsky; Gerben Venekamp; Tom Vitez; Romain Wartel; Christopher Whalen; John White; Carlo Maria Zwölf

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

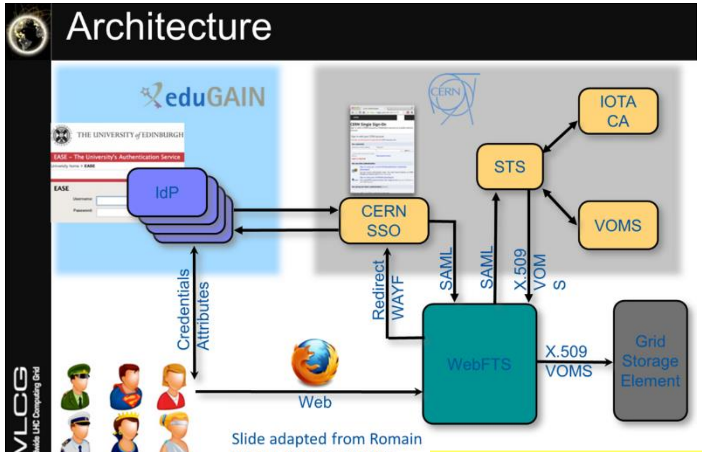
The authors also acknowledge the support and collaboration of many other colleagues in their respective institutes, research communities and IT Infrastructures, together with the funding received by these from many different sources. These include but are not limited to the following: (i) The Worldwide LHC Computing Grid (WLCG) project is a global collaboration of more than 170 computing centres in 43 countries, linking up national and international grid infrastructures. Funding is acknowledged from many national funding bodies and we acknowledge the support of several operational infrastructures including EGI, OSG and NDGF/NeIC. (ii) EGI acknowledges the funding and support received from the European Commission and the many National Grid Initiatives and other members. EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777536. (iii) The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2). (iv) Work on the development of ESGF's identity management system has been supported by The UK Natural Environment Research Council and funding from the European Union's Seventh Framework Programme for research, technological development and demonstration through projects IS-ENES (grant agreement no 228203) and IS-ENES2 (grant agreement no 312979). (v) Ludek Matyska and Michal Prochazka acknowledge funding from the RI ELIXIR CZ project funded by MEYS Czech Republic No. LM2015047. (vi) Scott Koranda acknowledges support provided by the United States National Science Foundation under Grant No. PHY-1700765. (vii) GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).The research leading to these results has received funding from the European Union's

Access services **based on role(s)**

One **persistent** identifier across community's services

Easy way to **connect to eduGAIN**

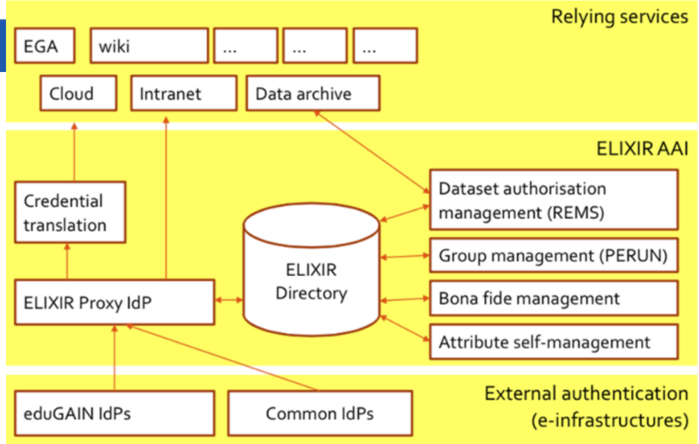
Whence we came – collaborative research AAIs predating AARC


Architecture

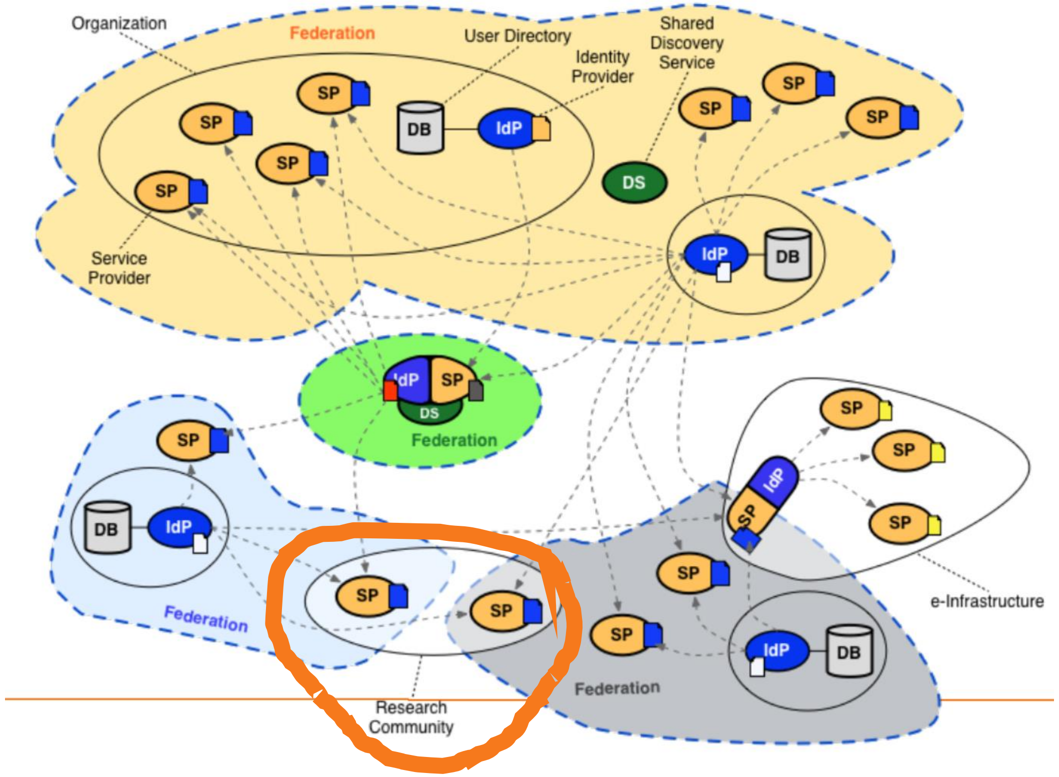
Slide adapted from Romain Wartel, GDB Sept 2014

WebFTS 'FIM4R' in wLCG
Romain Wartel

ELIXIR reference architecture
Mikael Linden et al.



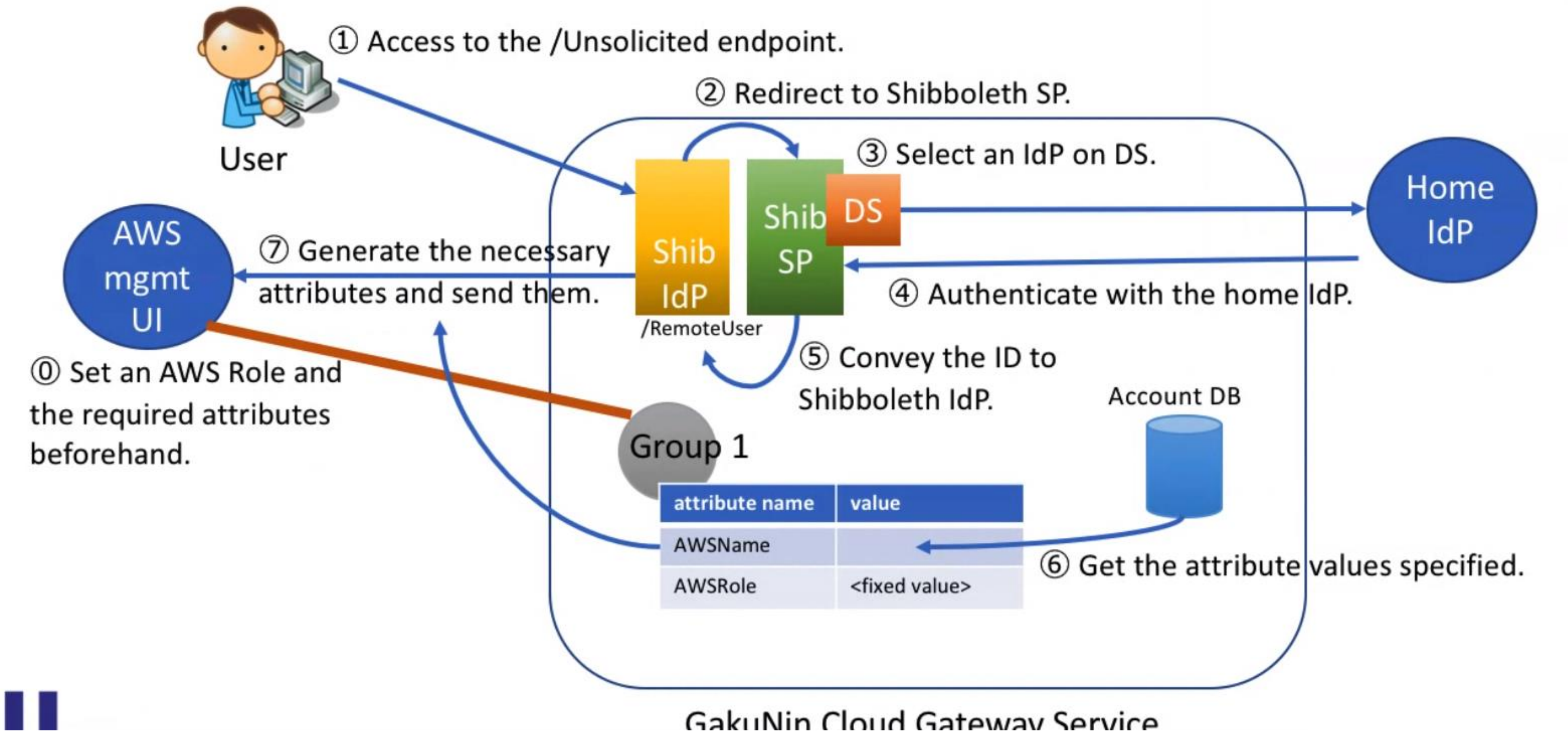
communities had either invented
their own 'proxy' model to abstract complexity



or they were composed of many services
each of which had to manage federation complexity

Images: Romain Wartel, CERN; Mikael Linden, CSC; Lukas Hammerle, SWITCH

… and from Eisaku-san’s talk yesterday …



User

① Access to the /Unsolicited endpoint.

② Redirect to Shibboleth SP.

③ Select an IdP on DS.

④ Authenticate with the home IdP.

⑤ Convey the ID to Shibboleth IdP.

⑥ Get the attribute values specified.

⑦ Generate the necessary attributes and send them.

⓪ Set an AWS Role and the required attributes beforehand.

AWS mgmt UI

Shib IdP

/RemoteUser

Shib SP

DS

Home IdP

Account DB

Group 1

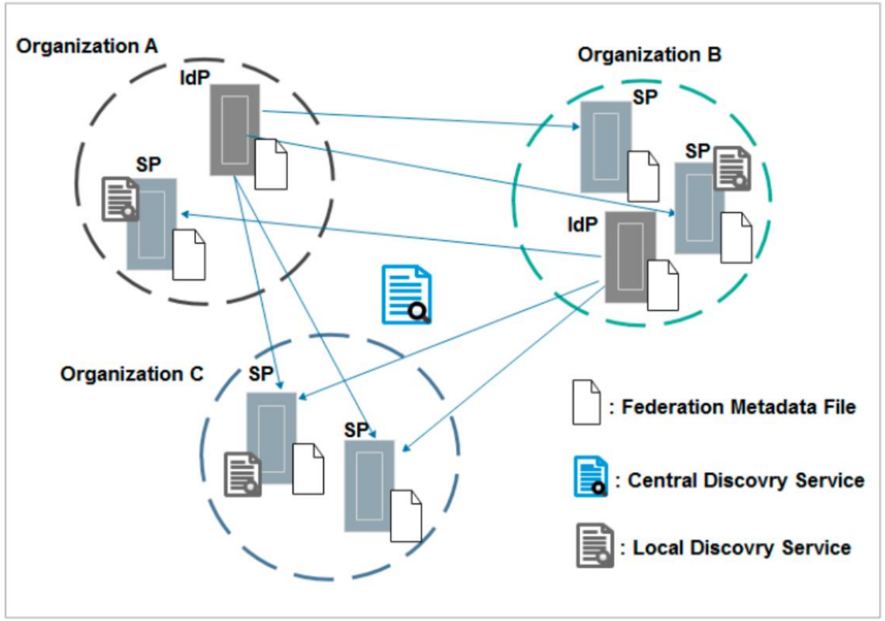
attribute name	value
AWSName	
AWSRole	<fixed value>

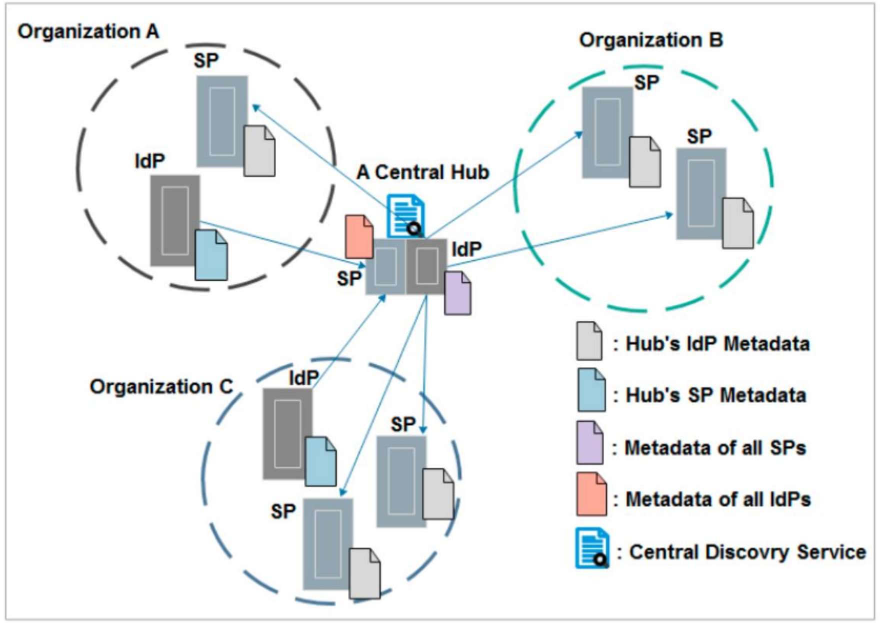
GakuNin Cloud Gateway Service

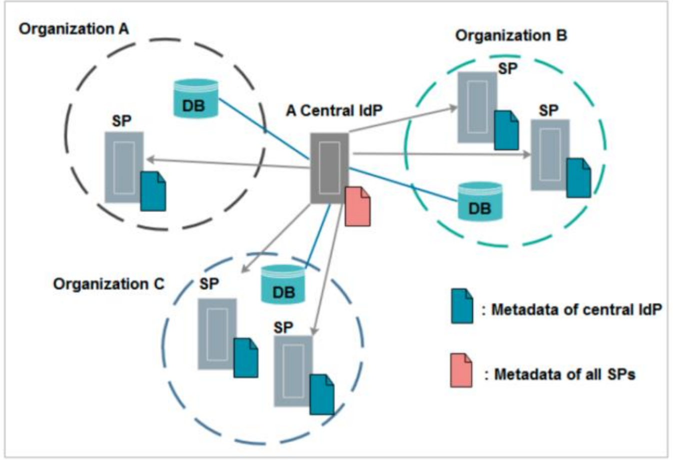
integrates a portal (“/Unsolicited”) with the IdP-SP proxy, so looks a bit more complex …

source: Eisaku Sakane, NII (http://indico3.twgrid.org/indico/contributionDisplay.py?contribId=4&confId=926)

Federation models – the meshy world that AARC needs to leverage

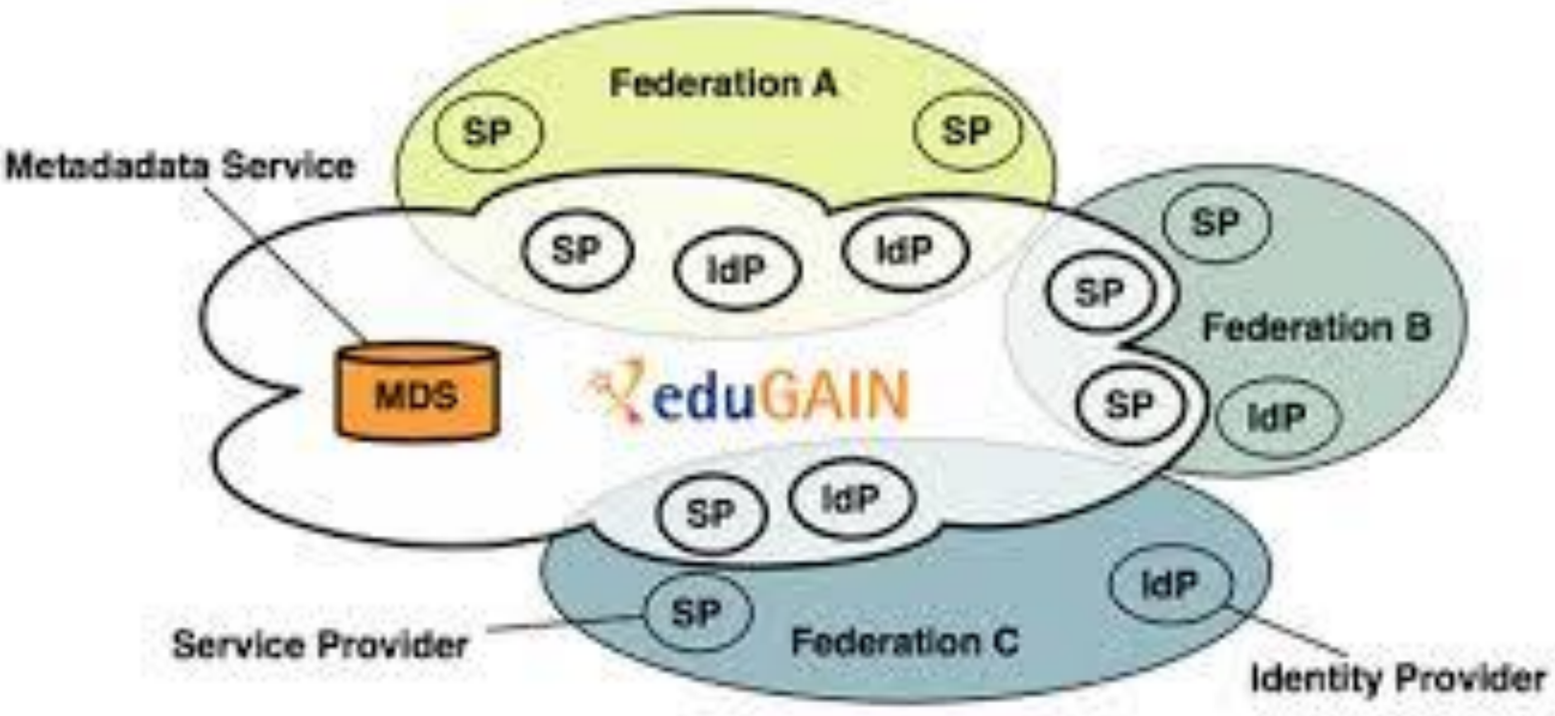






imagery from: A Hybrid Scheme for an Interoperable Identity Federation System El Hadouti and El Kettani 2019

eduGAIN – global interfederation



Identified common challenges

Communities / e-infrastructures surveyed in AARC

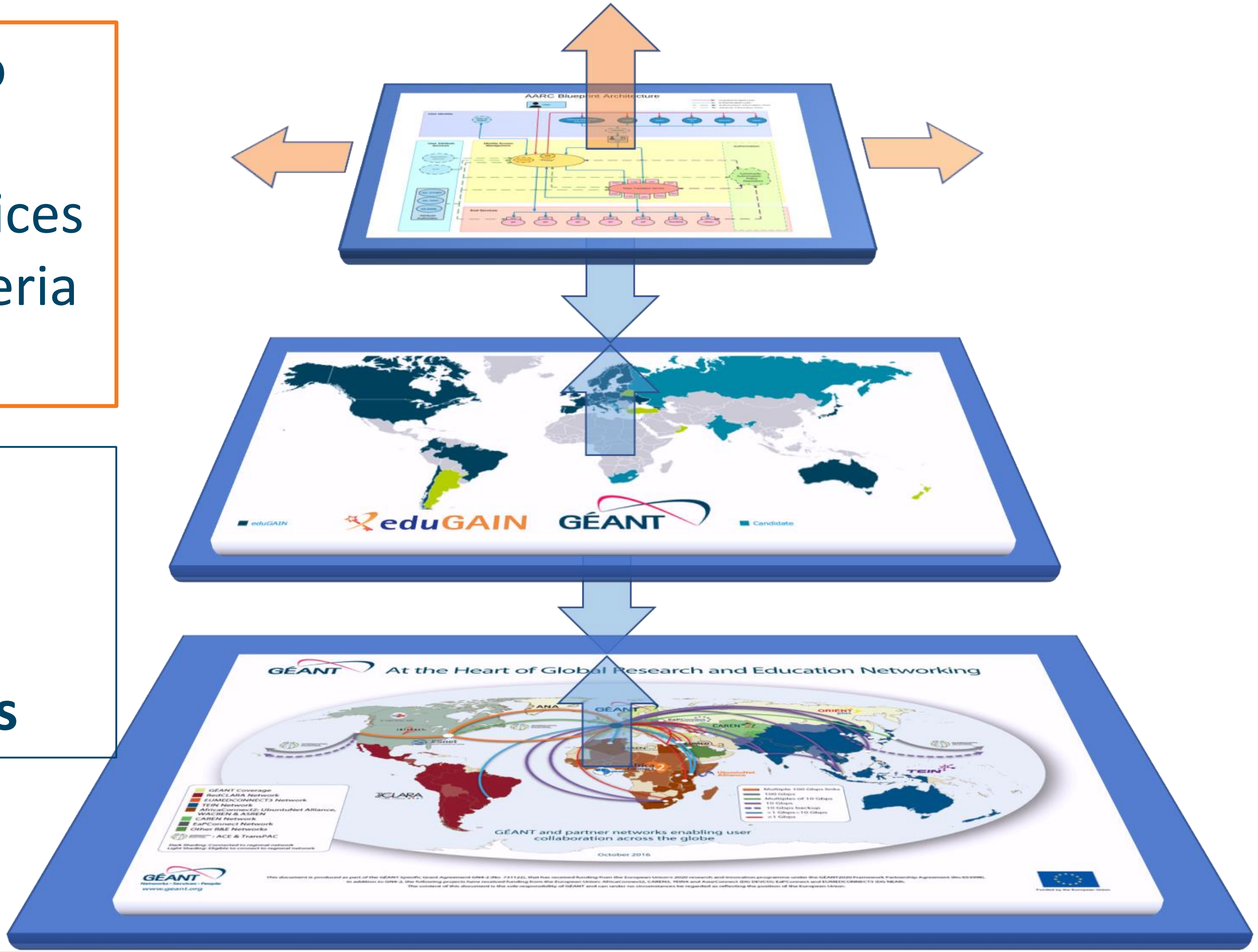
BBMRI
Biobanking and Biomolecular Resources Research Infrastructure
CORBEL
instruct
Integrating Biology
LIGO PROJECT
elixir
EPOS
EUROPEANPLATEOBSERVINGSYSTEM
CLARIN
LifeWatch
INFRAFRONTIER
umbrella
BioVeL
cta
cherenkov telescope array
WLCG
Worldwide LHC Computing Grid
DARIAH-EU
HP
ARIADNE
EISCAT 3D
PRACE
EUDAT
egi
GÉANT
CERN
HELIX NEBULA
THESCIENCECLOUD

- Homeless users
- User friendliness
- PII Data Protection
- Community based AuthZ
- SP friendliness
- Credential translation
- Bridging Communities
- Engaging SPs

The AARC Blueprint Architecture to bring everyone together

Defines a **model** and **building blocks** to address researcher needs
Cross-domain interoperation and services based on community and provider criteria expressed using **common guidelines**

Allows researchers to use **ONE** digital identity to access **MANY** services and resources available through **eduGAIN** and **in collaborative r/e-Infrastructures**

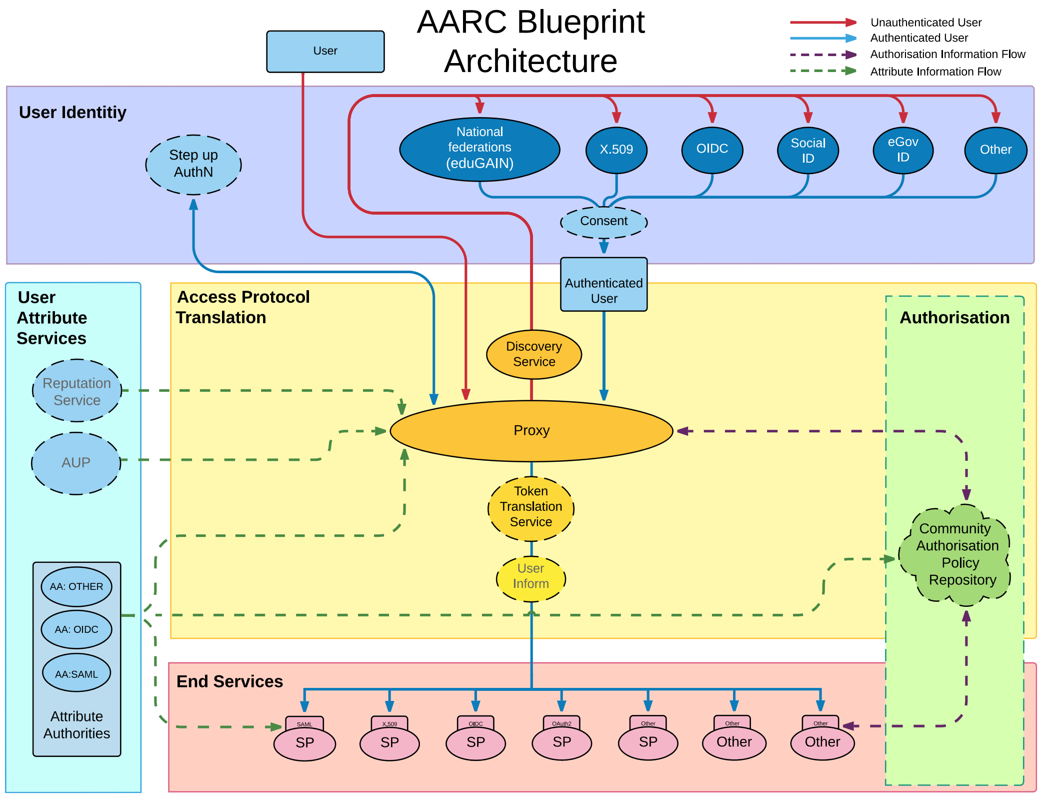


AARC Blueprint Architecture
eduGAIN
eduGAIN
GÉANT
Candidate
GÉANT
At the Heart of Global Research and Education Networking
GÉANT and partner networks enabling user collaboration across the globe
October 2016

Key int

AARC Blueprint Process

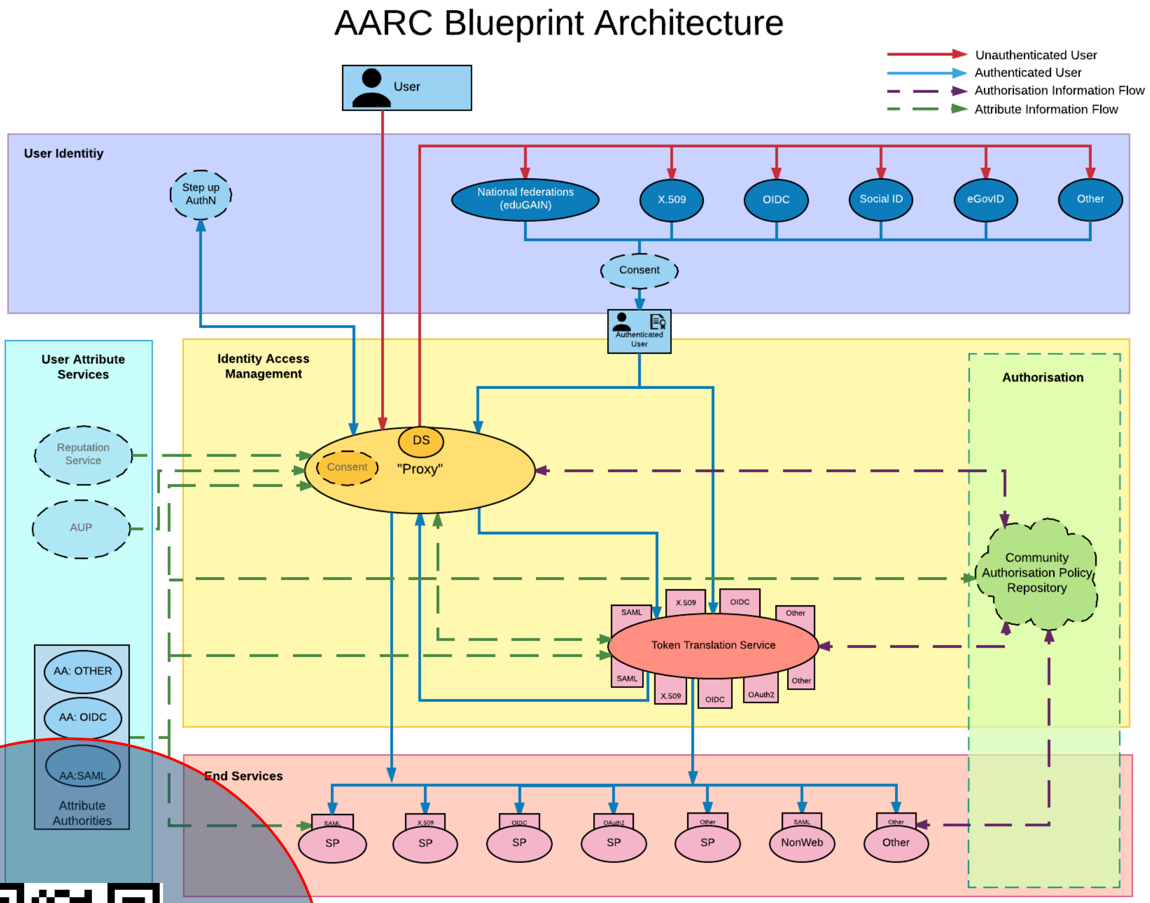
https://aarc-project.eu/architecture/

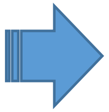


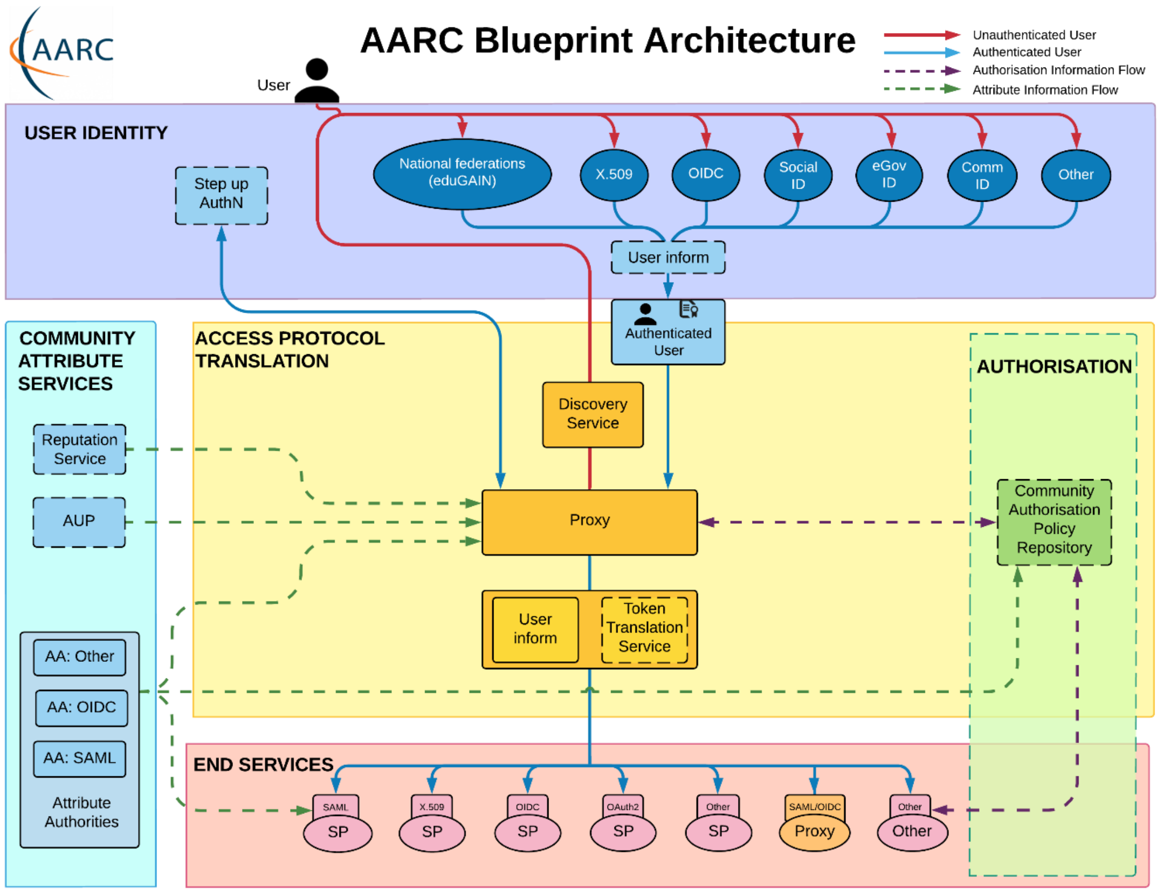
Guidelines and supporting documents

- *reference architecture*
- *conventions and community standards*
- *best policy practices*
- *implementation hints*
- *training for ‘FIM’ communities*

Evolution of the Blueprint Architecture



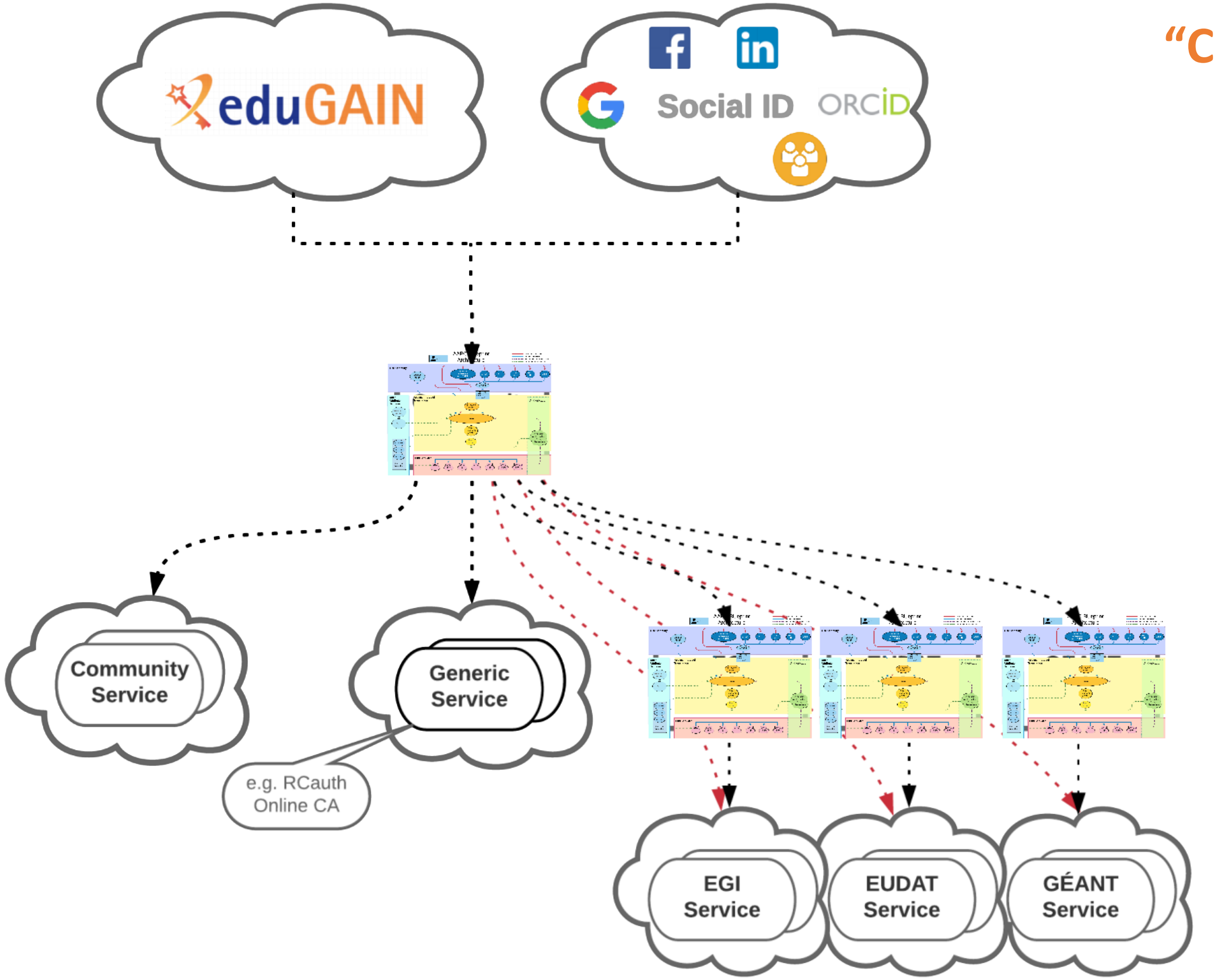




AARC-BPA-2017

AARC-BPA-2019

Evolution of the Blueprint Architecture

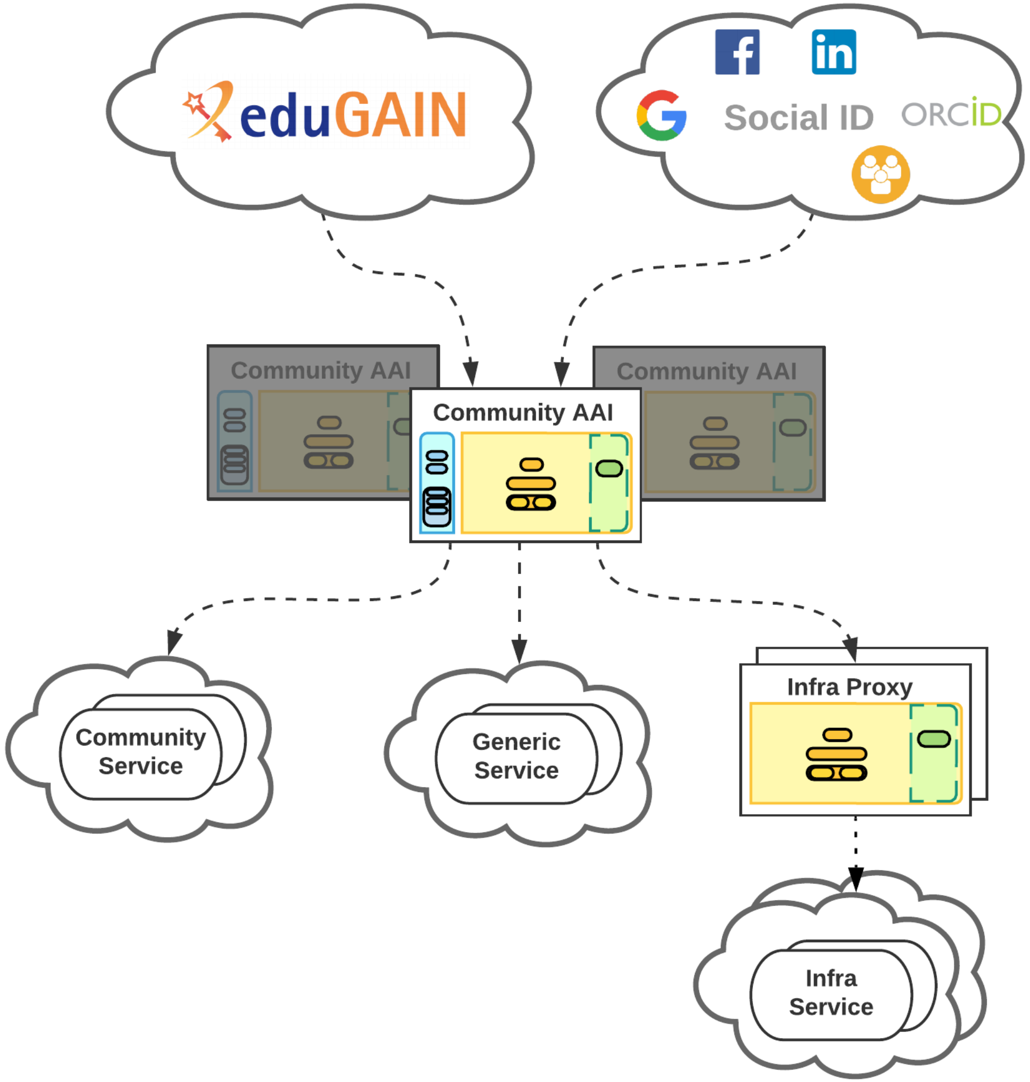


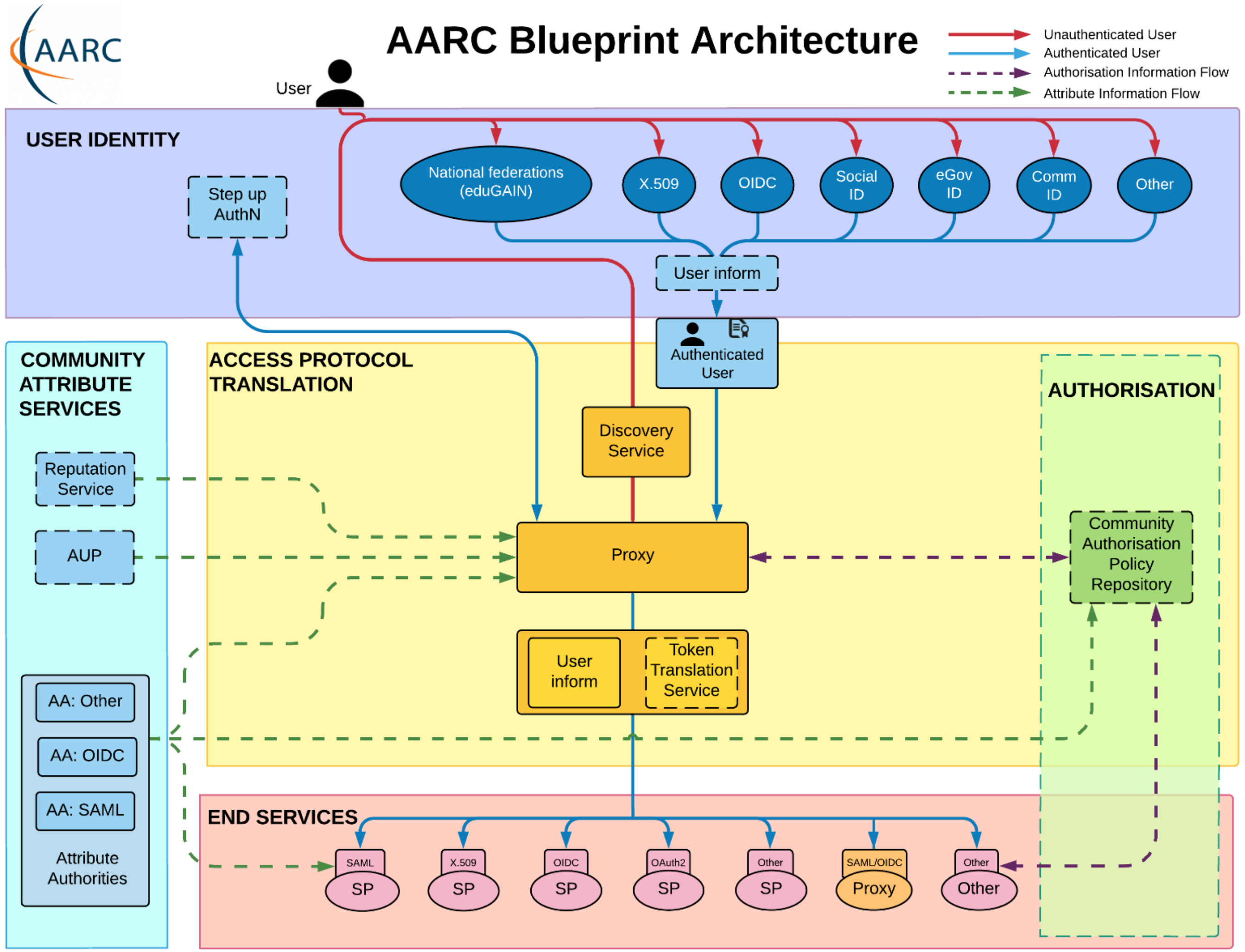
“Community-first” BPA approach

- Researchers sign in using their institutional (eduGAIN), social or community-managed IdP via their Research Community AAI
- Community-specific services are connected to a single Community AAI
- Generic services (e.g. RCauth.eu Online CA) can be connected to more than one Community AAI proxies
- e-Infra services are connected to a single e-infra SP proxy service gateway, e.g. B2ACCESS, Check-in, Identity Hub, etc

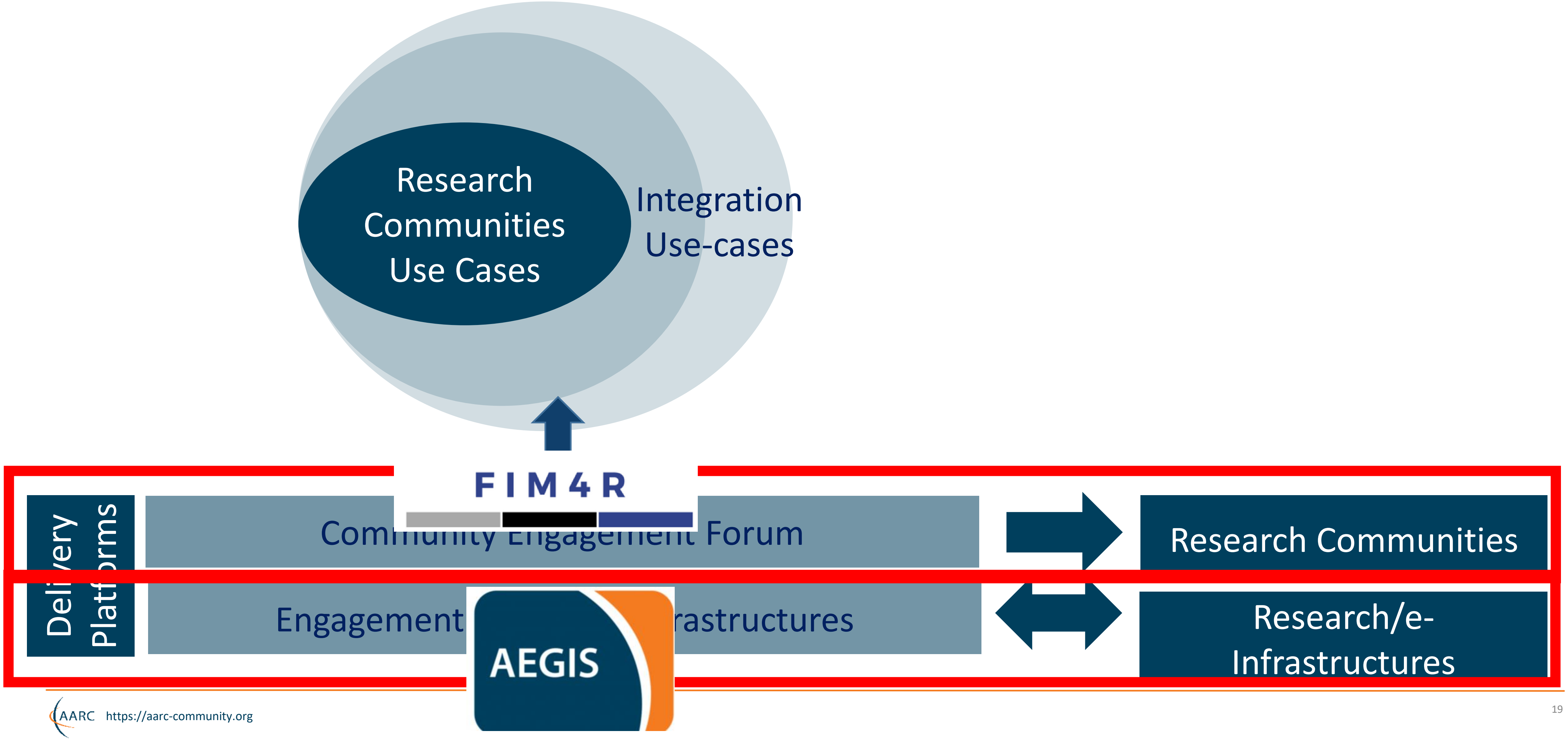
https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf

Evolution of the Blueprint Architecture





Engaging with the AARC Community



Research Communities Use Cases

Integration Use-cases

Delivery Platforms

Community Engagement Forum

Engagement

rastructures

Research Communities

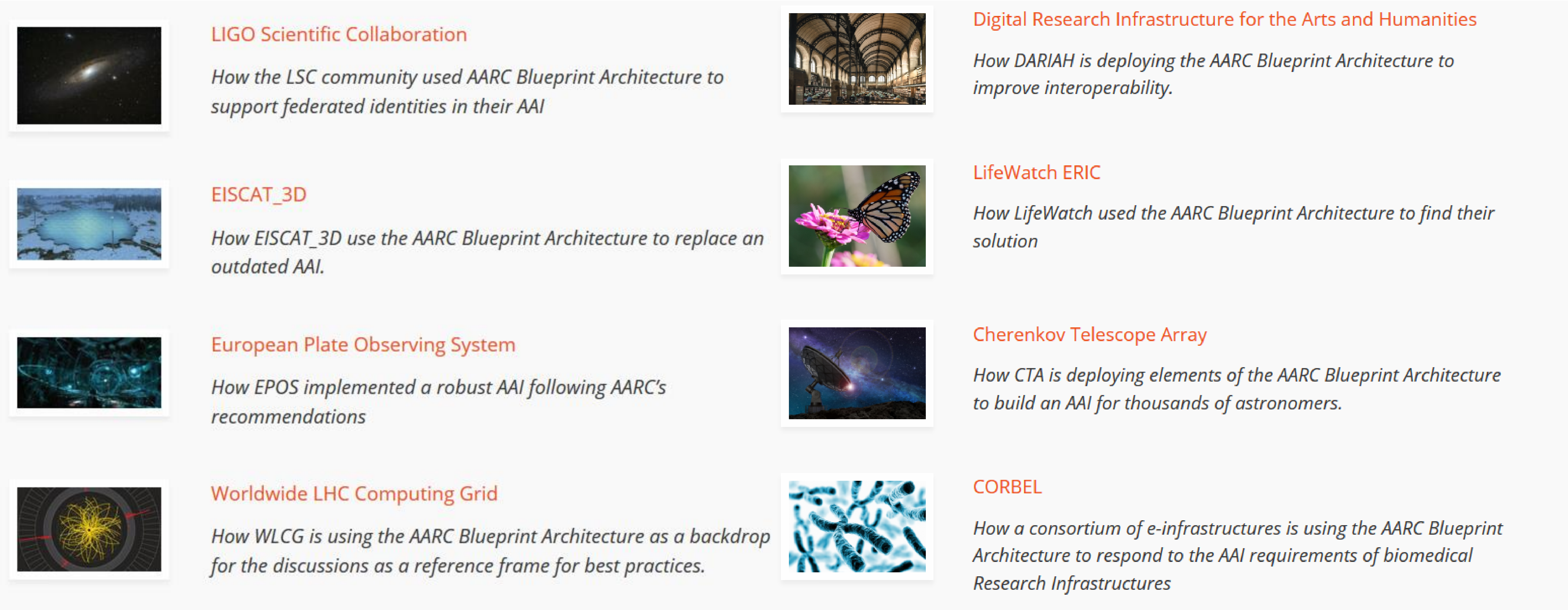
Research/e-Infrastructures

Implementation in the generic e-Infrastructures and AAI offerings

	EUDAT B2ACCESS	EGI Check-in	GEANT eduTEAMS	INDIGO IAM
Alignment of user attribute/claim names	✓	✓	✓	Sept 2019
Alignment of VO/group membership and role information	✓	✓	✓	Sept 2019
Alignment of resource capabilities information	July 2019	Jun 2019	✓	Sept 2019
Alignment of affiliation information	TBC	Sep 2019	Sep 2019	Sept 2019
Alignment of assurance information	TBD	TBD	TBD	TBD
Alignment of privacy statements	✓	✓	✓	✓
Alignment of operational security and incident response policies	✓	✓	✓	✓
Alignment of Acceptable Use Policies (AUPs)	July 2019	✓	✓	Sept 2019

Guidelines on expressing group membership and role information (201710)

AARC In Action – https://aarc-community.org/aarc-in-action/



LIGO Scientific Collaboration

How the LSC community used AARC Blueprint Architecture to support federated identities in their AAI

EISCAT_3D

How EISCAT_3D use the AARC Blueprint Architecture to replace an outdated AAI.

European Plate Observing System

How EPOS implemented a robust AAI following AARC's recommendations

Worldwide LHC Computing Grid

How WLCG is using the AARC Blueprint Architecture as a backdrop for the discussions as a reference frame for best practices.

Digital Research Infrastructure for the Arts and Humanities

How DARIAH is deploying the AARC Blueprint Architecture to improve interoperability.

LifeWatch ERIC

How LifeWatch used the AARC Blueprint Architecture to find their solution

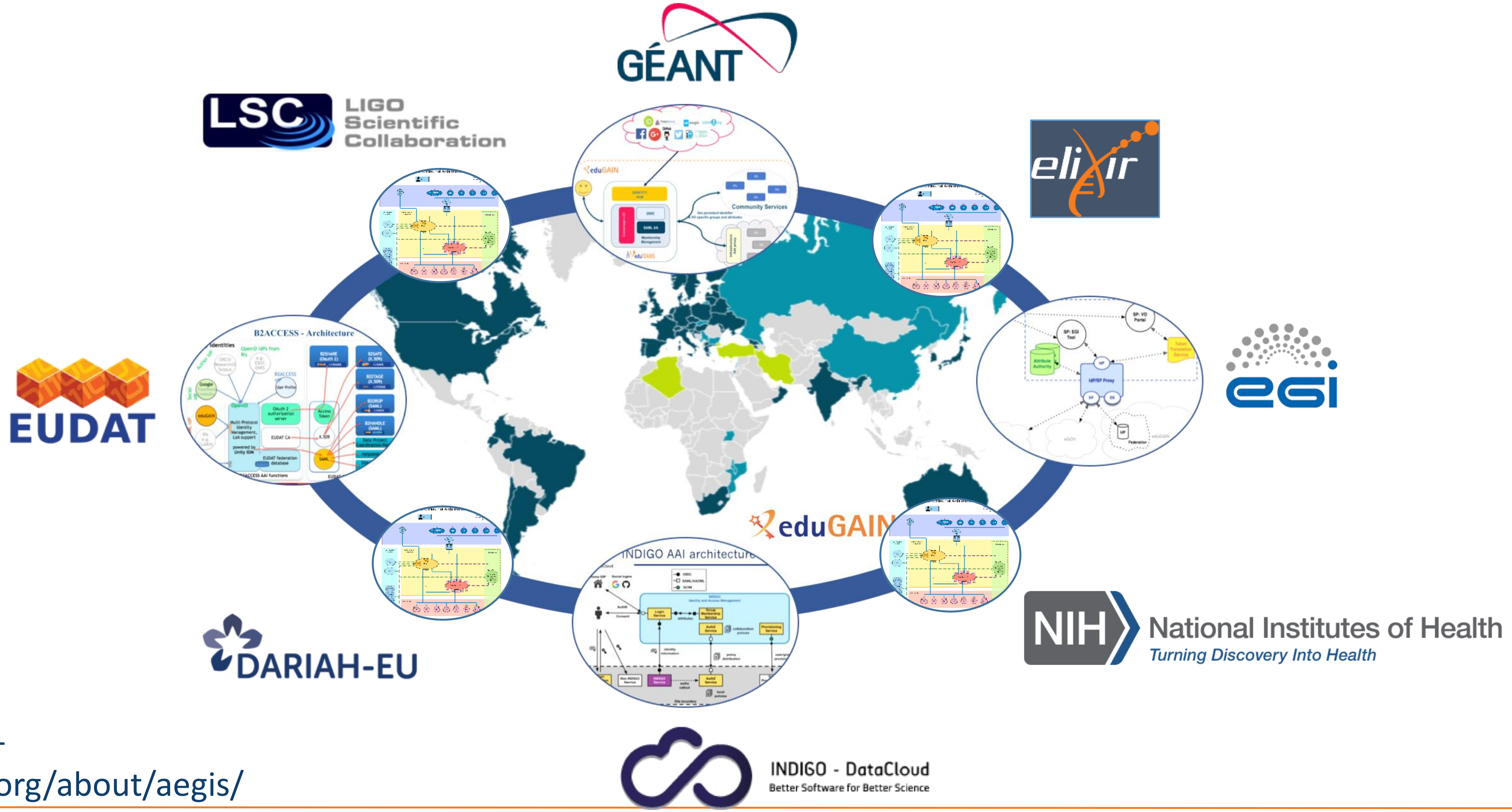
Cherenkov Telescope Array

How CTA is deploying elements of the AARC Blueprint Architecture to build an AAI for thousands of astronomers.

CORBEL

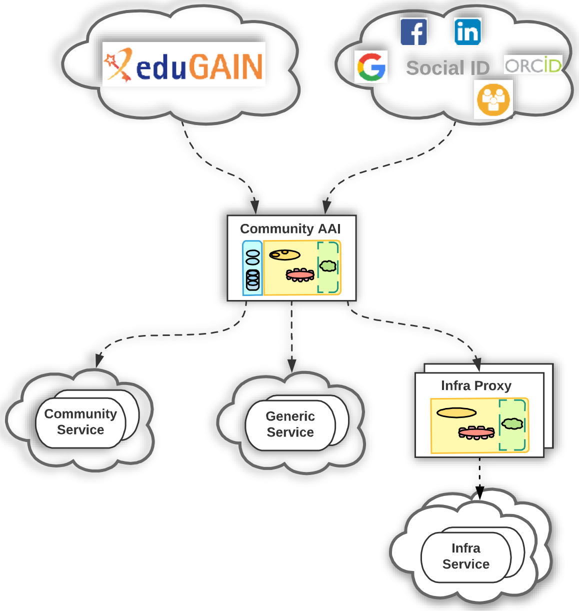
How a consortium of e-infrastructures is using the AARC Blueprint Architecture to respond to the AAI requirements of biomedical Research Infrastructures

AARC Blueprint Architecture Implementations


GÉANT
LSC LIGO Scientific Collaboration
elixir
EUDAT
B2ACCESS - Architecture
egi
eduGAIN
INDIGO AAI architecture
NIH National Institutes of Health
Turning Discovery Into Health
DARIAH-EU
INDIGO - DataCloud
Better Software for Better Science

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

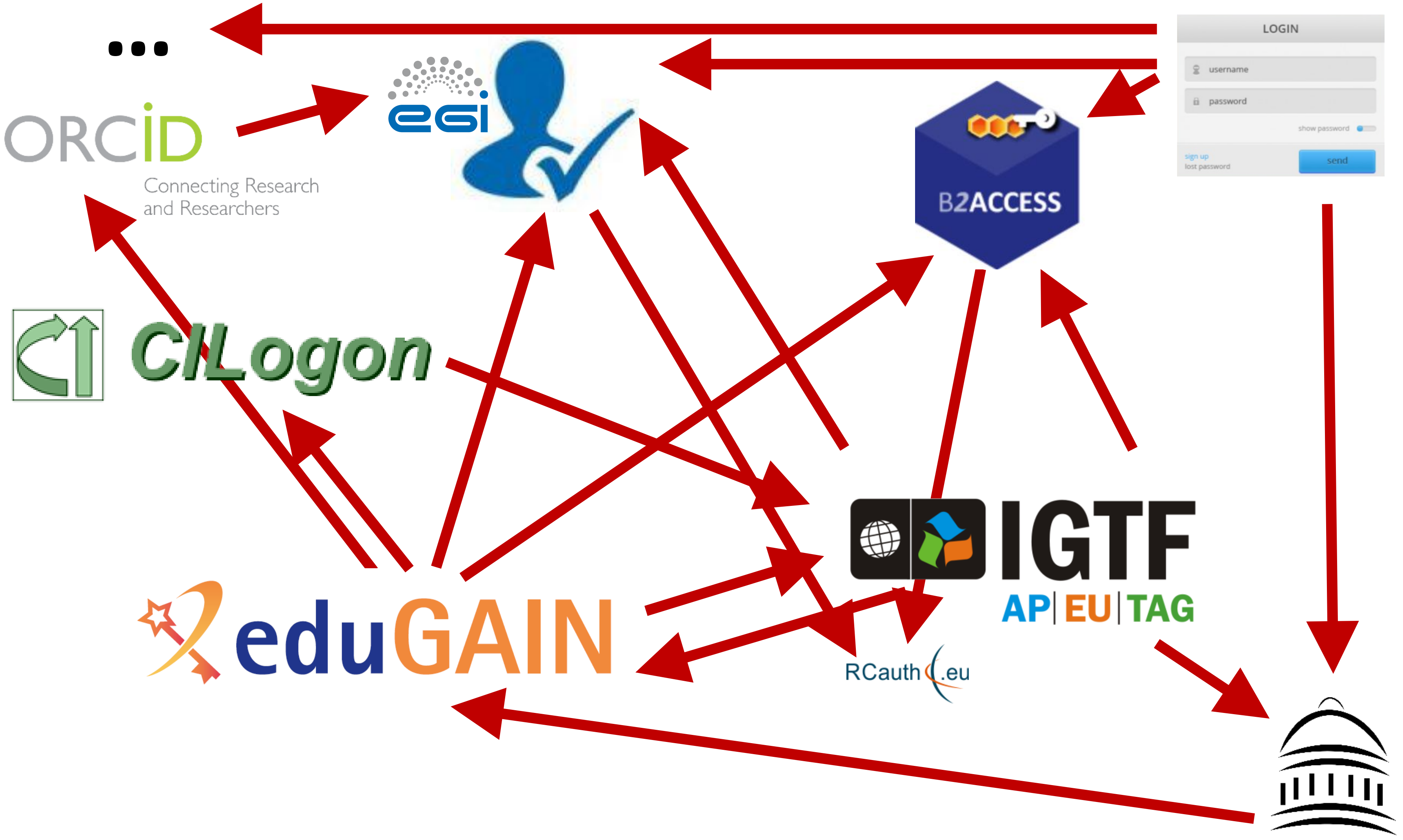
Deploying a federated AAI? You don't have to be on your own!



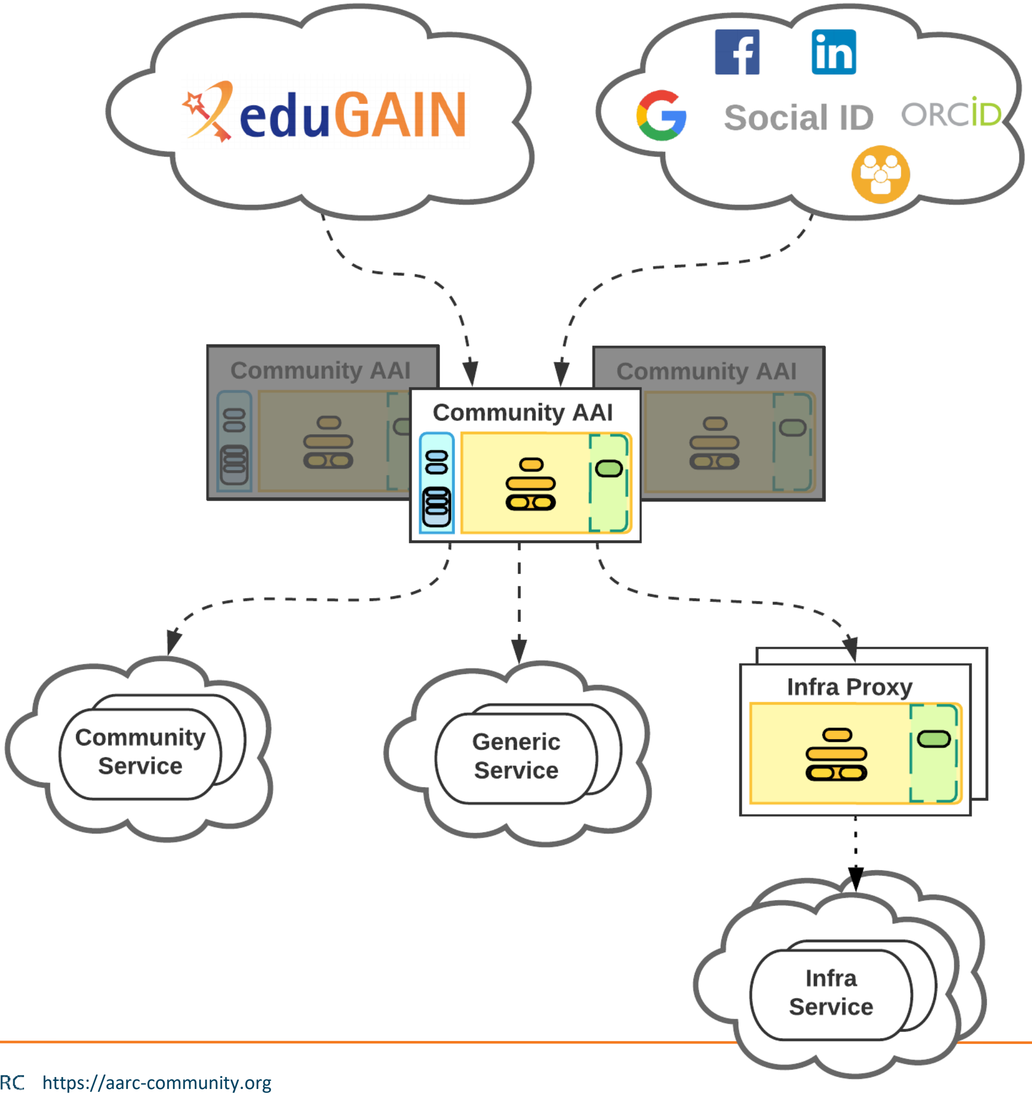
- Communities with **existing Community AAI** connect to e-Infra Proxies and access generic e-Infra services via 'community first' proxy-cascade
- They **increasingly outsource technical AAI – retaining content control**
  - using either dedicated or multi-tenant deployments of AAI services operated in EOSC
- Multi-tenant deployments
  - aimed at medium-to-small research communities/groups or individual researchers
  - community members, groups and authorisationattributes are still managed by community managers
- Dedicated deployments
  - customisation of user-facing elements: IdP discovery, enrolment, membership UI
  - customisation of AAI behaviour (attribute aggregation rules, service entitlements)
  - providers offer option of *bespoke* AAI Solutions, which might include individual components from the GÉANT eduTEAMS, EGI Check-in, INDIGO IAM, EUDAT B2ACCESS, and PERUN

for more information, ask Nicolas Liampotis, GRNET and EOSC-Hub AAI, on the AppInt list

As more infrastructures implement proxies and bridges …



Towards a mesh – research infrastructures as service providers



- Research Infrastructures offering services that both provide and consume offerings from e-Infras *as well as* peer Research Infras
- National and regional implementations of BPA
- Global - and the EOSC Exchange - ecosystem builds upon a largish number of proxies
- See e.g. the AAI section in the Security Whitepaper
- This will be the focus of the AARC BPA2020 and of the AAI Task Force of the EOSC Arch WG

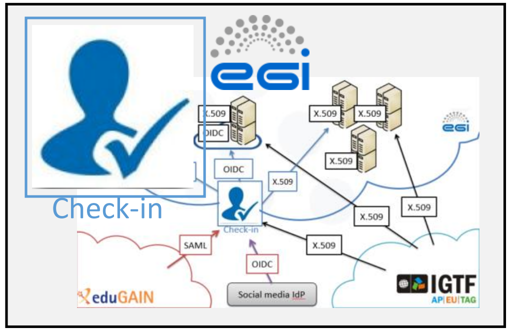
https://g.nikhef.nl/eosc-sec-wp

Blueprint Implementation Examples

One Blueprint, Many Implementations

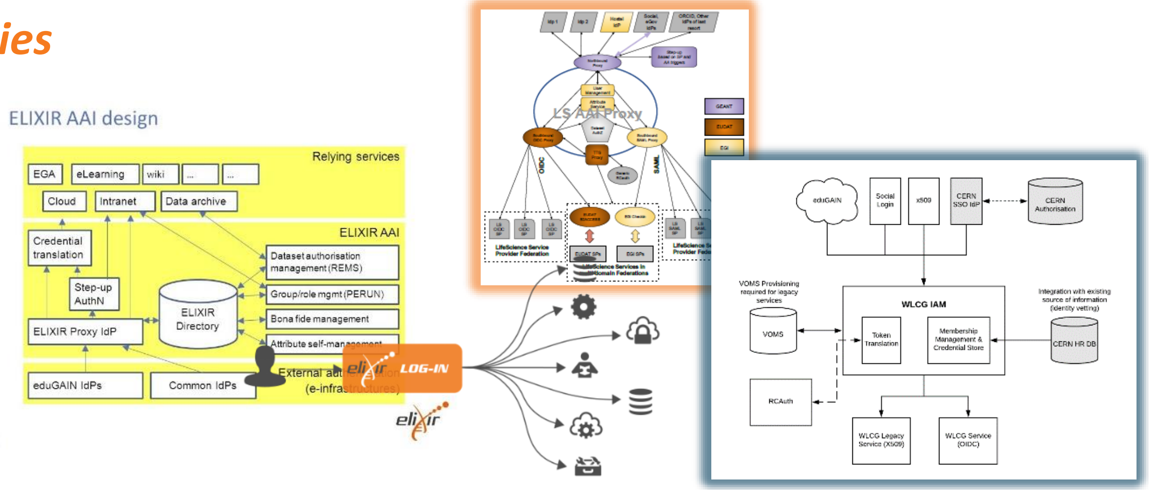
generic e-Infrastructures

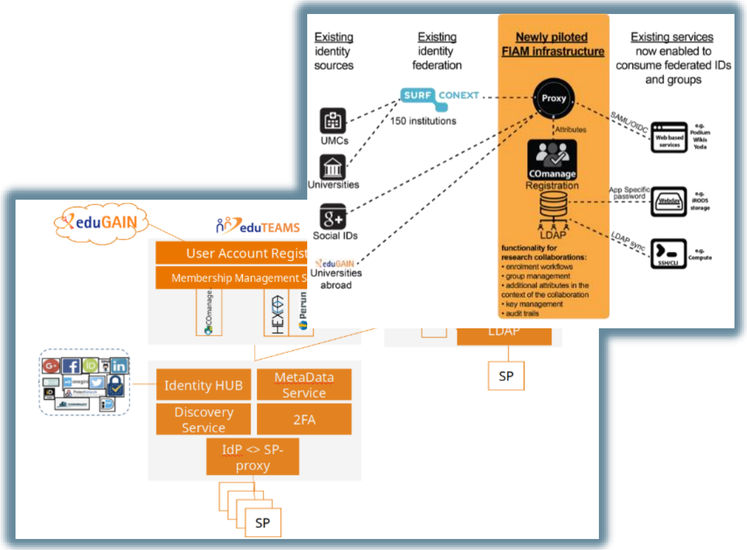
ESCAPE
European Science Cluster of Astronomy & Particle physics ESFRI research infrastructures
AAI
INDIGO - DataCloud
iam



eduTEAMS

domain-centred proxies

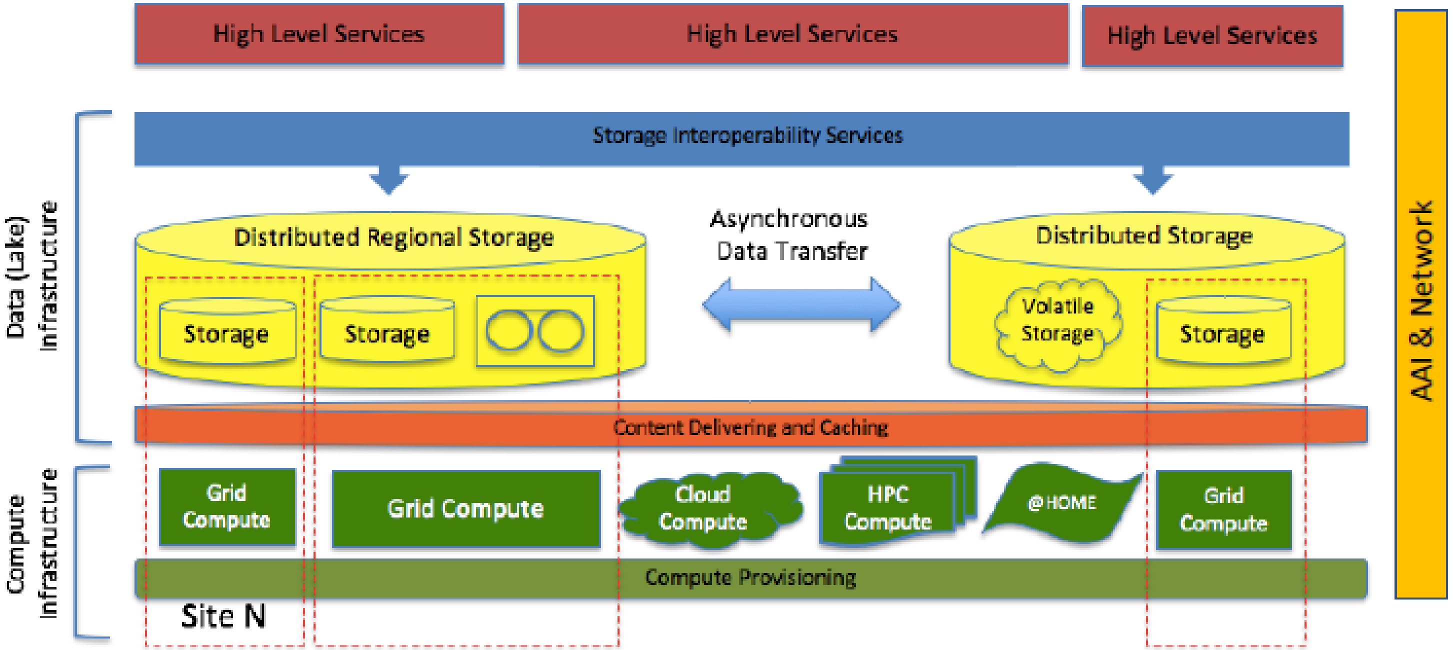




national infrastructure proxies

The ESCAPE data lake

Data Lake building blocks



Define, integrate and commission an ecosystem of tools and services to build a data lake

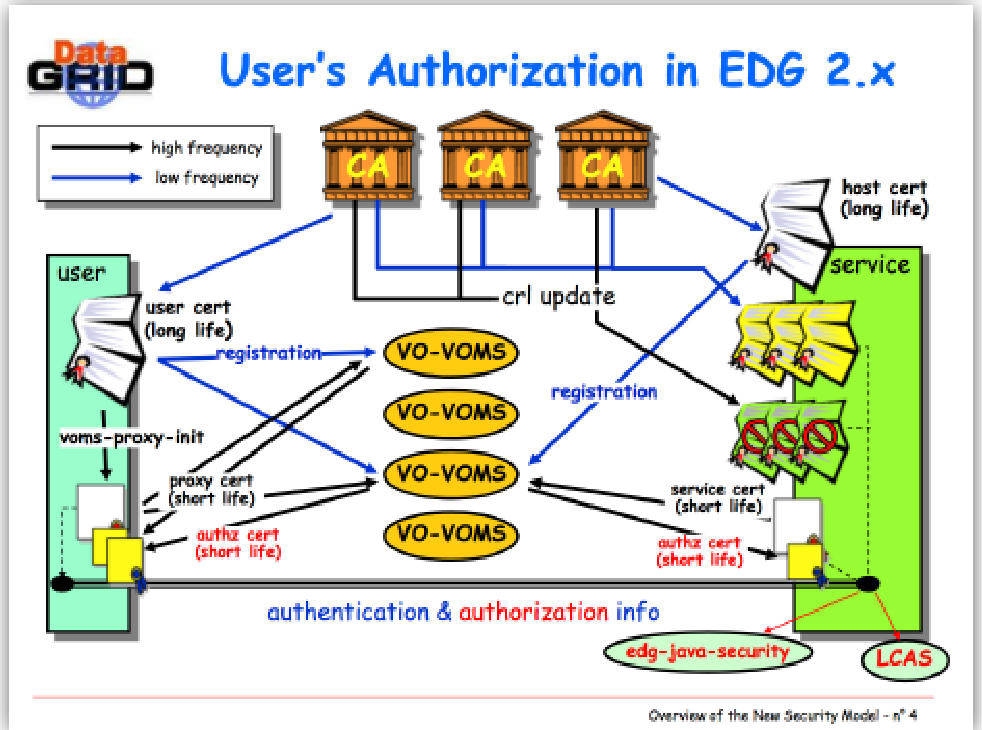
Leaves to the science projects the flexibility to choose the services and layout most suitable to their needs. Provides a reference implementation

Contributes to deliver Open Access and FAIR data services: relies on trustable data repositories; enables data management policies; hides the complexities of the underlying infrastructure providing a transparent data access layer

Funded by the European Union's Horizon 2020 - Grant N° 824064

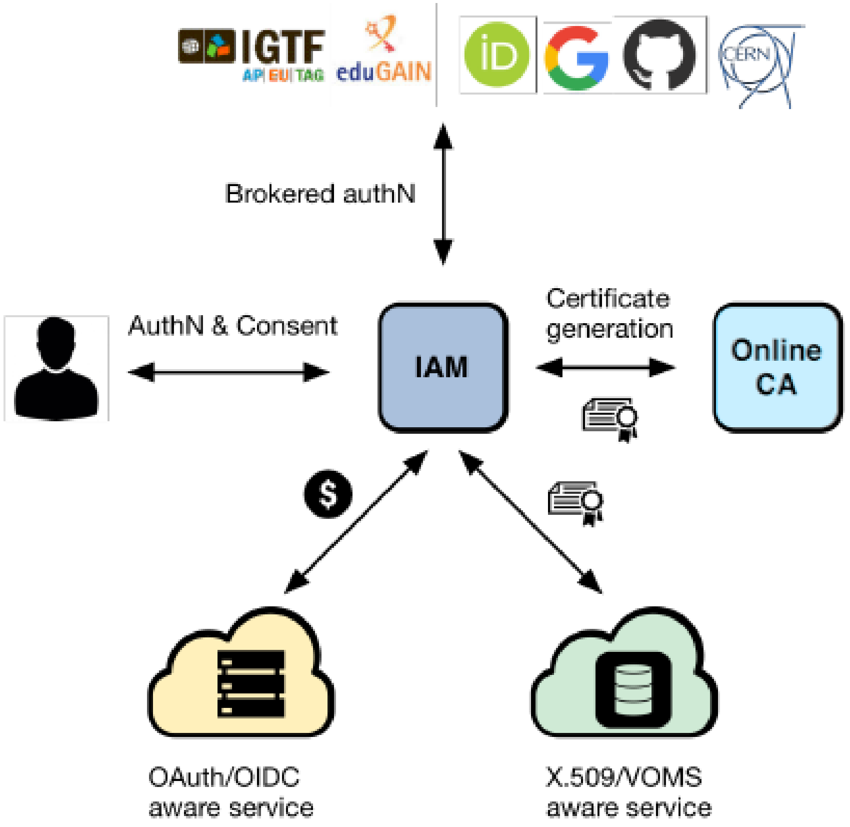
ESCAPE Data Lake AAI and WLCG

Current, X.509 based AAI



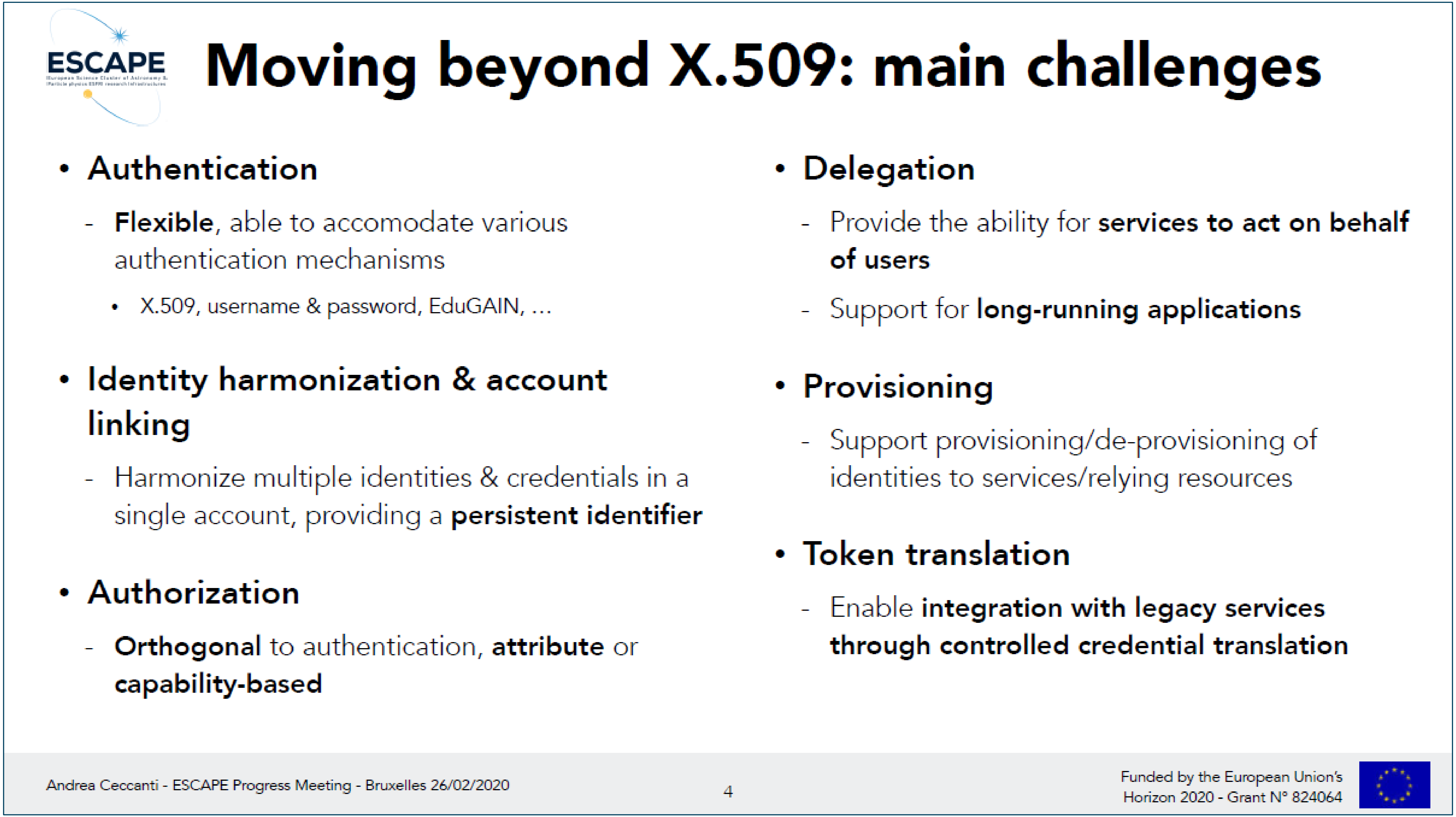
Move beyond X.509

Future, token-based AAI



Approach: leverage and build upon the WLCG experience

Funded by the European Union's Horizon 2020 - Grant N° 824064



Moving beyond X.509: main challenges

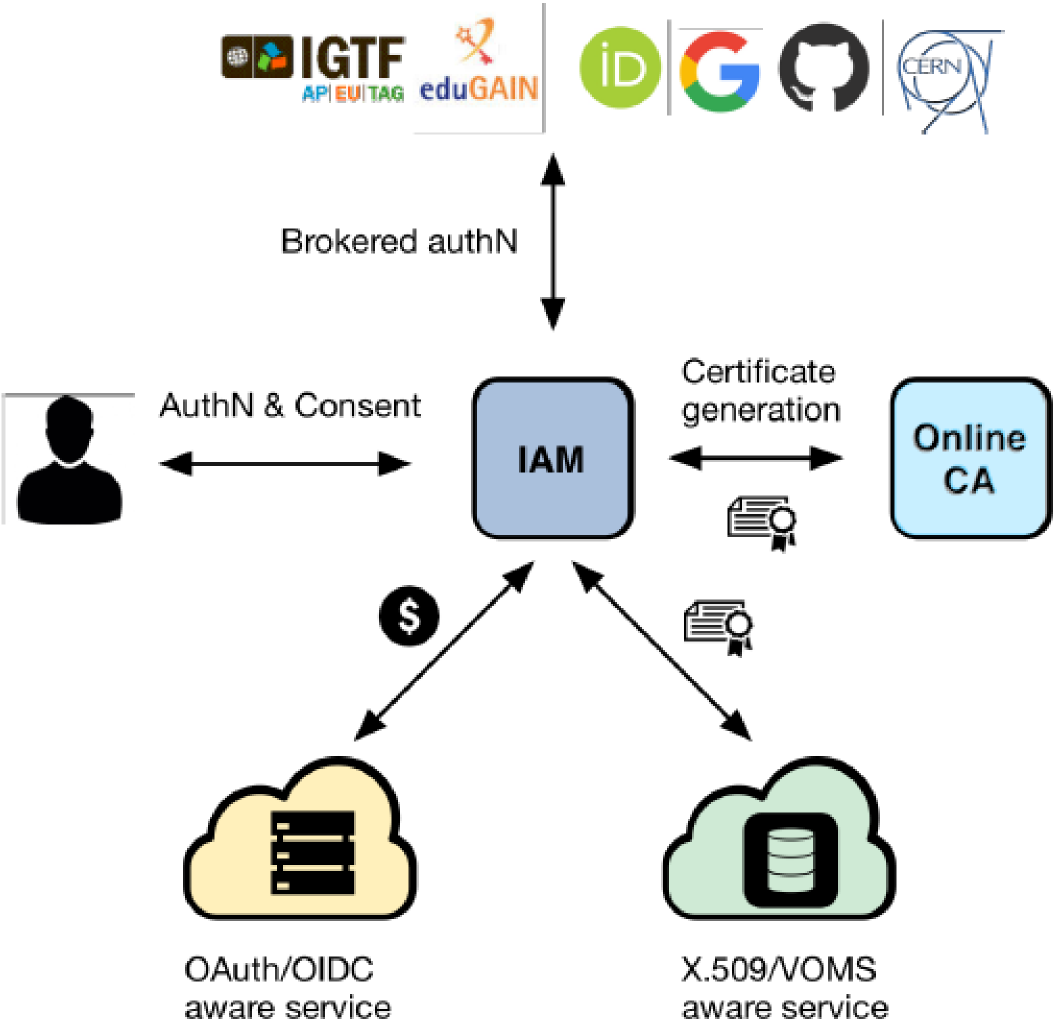
- **Authentication**
  - **Flexible**, able to accomodate various authentication mechanisms
    - X.509, username & password, EduGAIN, …
- **Identity harmonization & account linking**
  - Harmonize multiple identities & credentials in a single account, providing a **persistent identifier**
- **Authorization**
  - **Orthogonal** to authentication, **attribute** or **capability-based**
- **Delegation**
  - Provide the ability for **services to act on behalf of users**
  - Support for **long-running applications**
- **Provisioning**
  - Support provisioning/de-provisioning of identities to services/relying resources
- **Token translation**
  - Enable **integration with legacy services through controlled credential translation**

Funded by the European Union's Horizon 2020 - Grant N° 824064

INDIGO Identity and Access Management Service

- A **VO*-scoped** authentication and authorization service that
  - supports **multiple authentication mechanisms**
  - provides users with a **persistent, VO-scoped** identifier
  - exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
  - can integrate existing **VOMS**-aware services
  - supports **Web** and **non-Web access**, **delegation** and **token renewal**

*VO = Virtual Organization



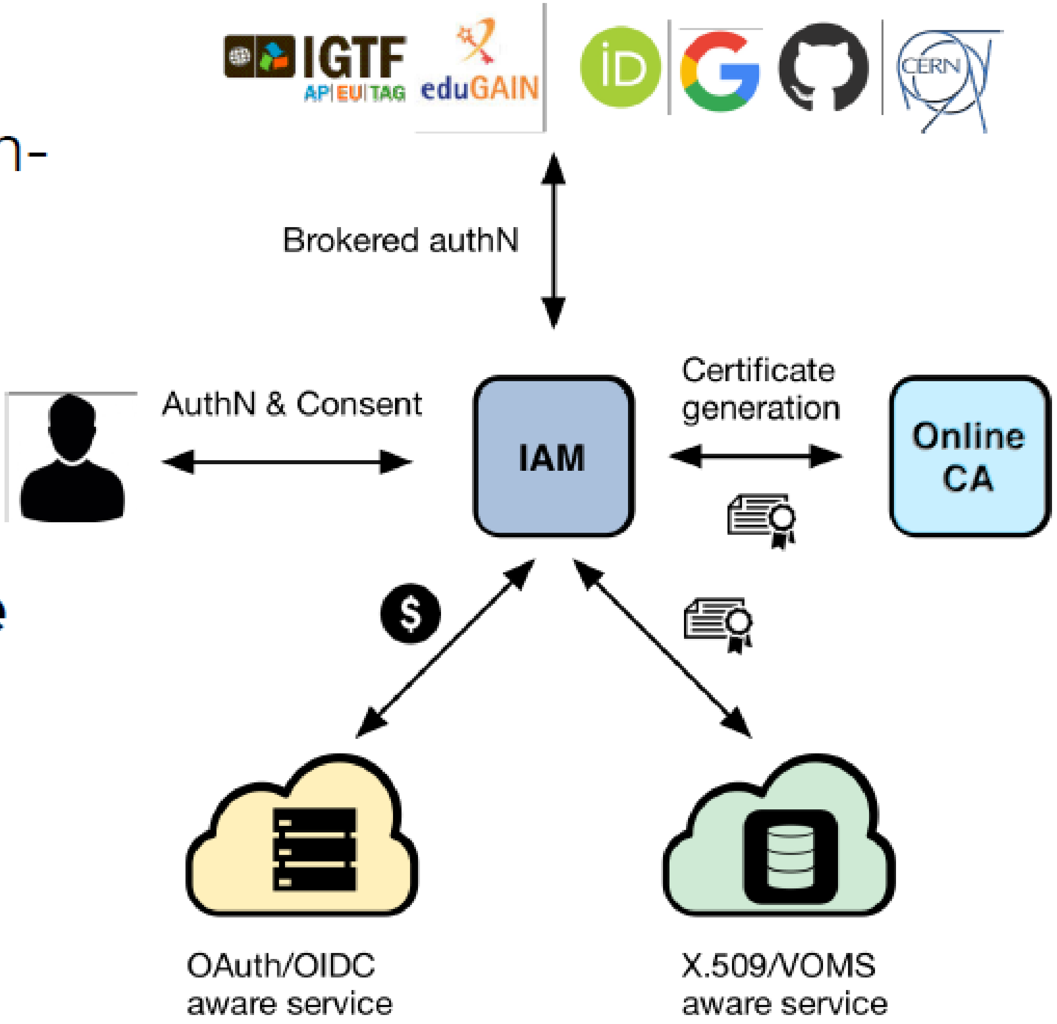
Funded by the European Union's Horizon 2020 - Grant N° 824064

INDIGO Identity and Access Management Service

- **Selected by the WLCG Management Board** to be the core of the future, token-based WLCG AAI
  - while ensuring backward compatibility with the existing infrastructure
- **Sustained by INFN for the foreseeable future**, with current support from:

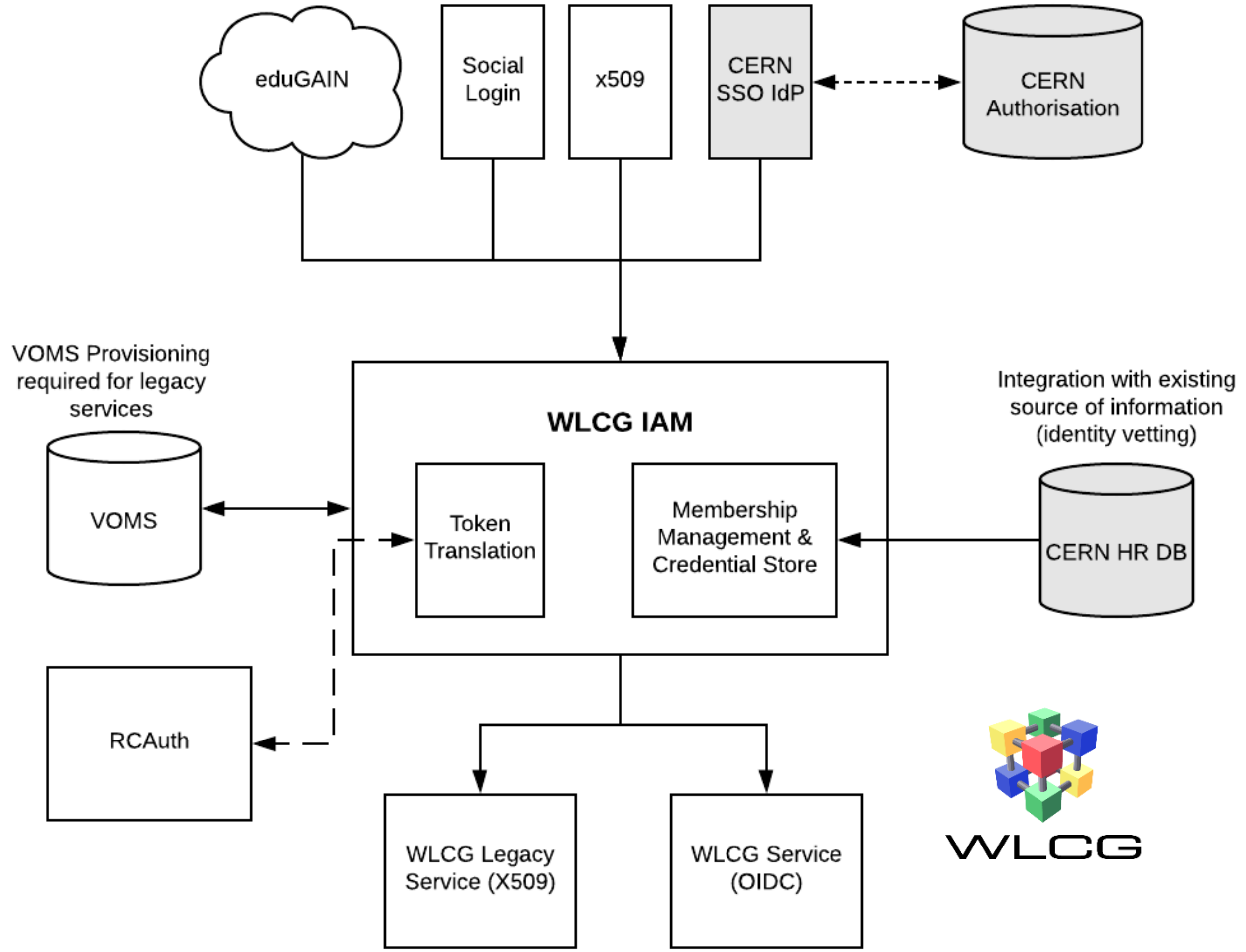
EOSC-hub

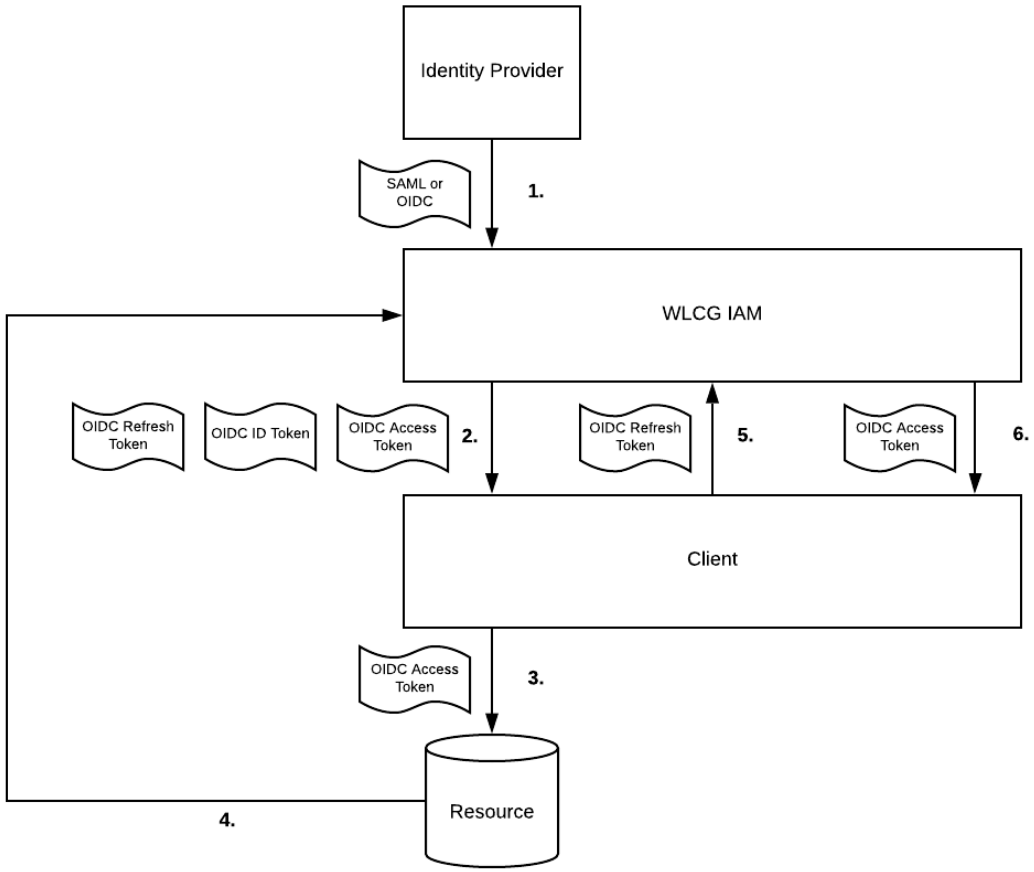
ESCAPE



Funded by the European Union's Horizon 2020 - Grant N° 824064

WLCG AuthZ working group


eduGAIN
Social Login
x509
CERN SSO IdP
CERN Authorisation
VOMS Provisioning required for legacy services
VOMS
WLCG IAM
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
RCAuth
WLCG Legacy Service (X509)
WLCG Service (OIDC)
WLCG



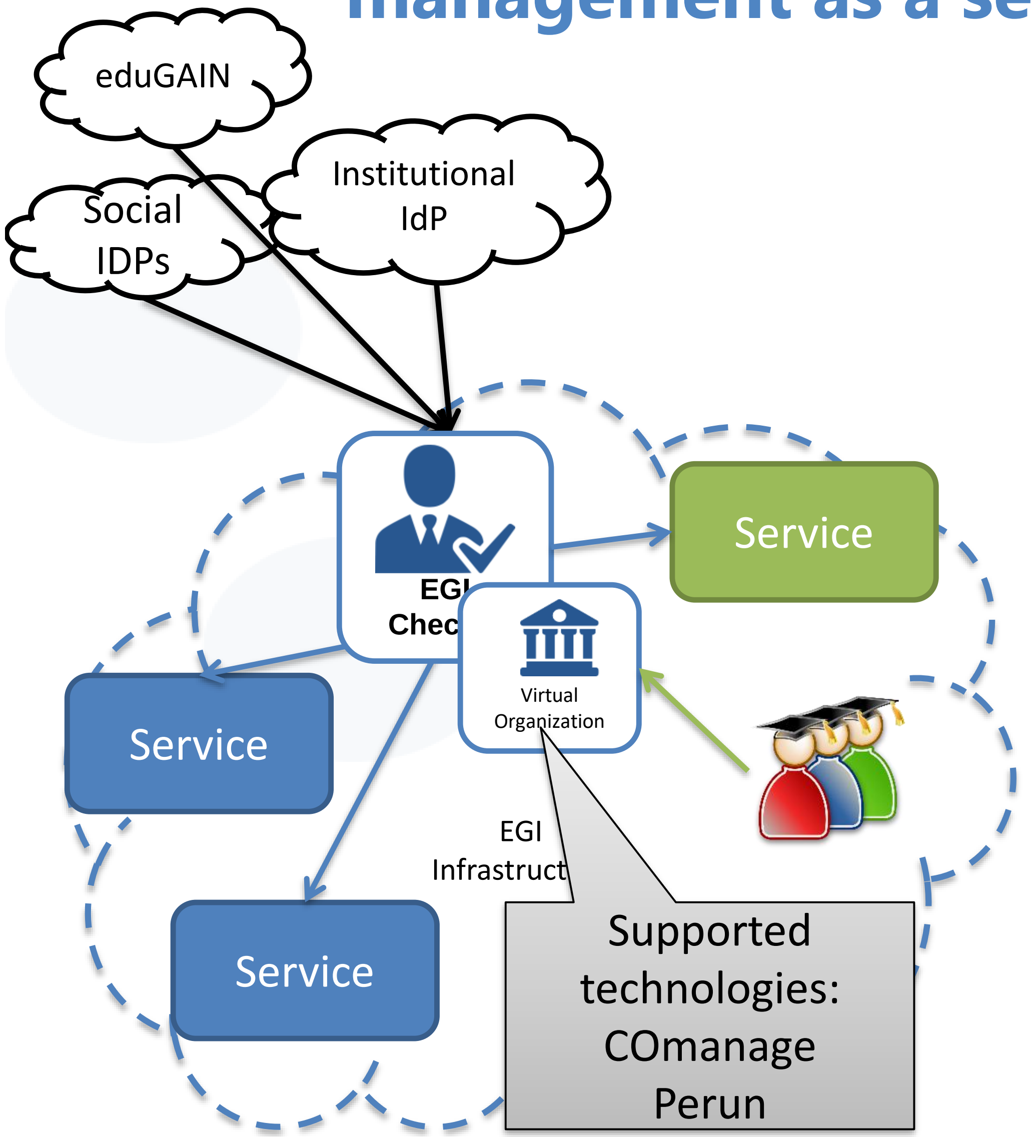
see Hannah Short et al.’s CHEP2019 paper (https://www.overleaf.com/project/5df7421204ffec00016f25c5)

WLCG JWT profile: http://doi.org/10.5281/zenodo.3460258

For the communities: full AAI platform with group management as a service

Communities that do not operate their own group management service can leverage the group management capabilities of the CheckIn platform

- ✓ Ready-to-use solution
- ✓ Avoid overhead of deploying a dedicated group management service
- ✓ Support for multi-tenancy to allow authorised VO admins to manage the information about their users independently
- ✓ Easy connect to both EGI and non-EGI services

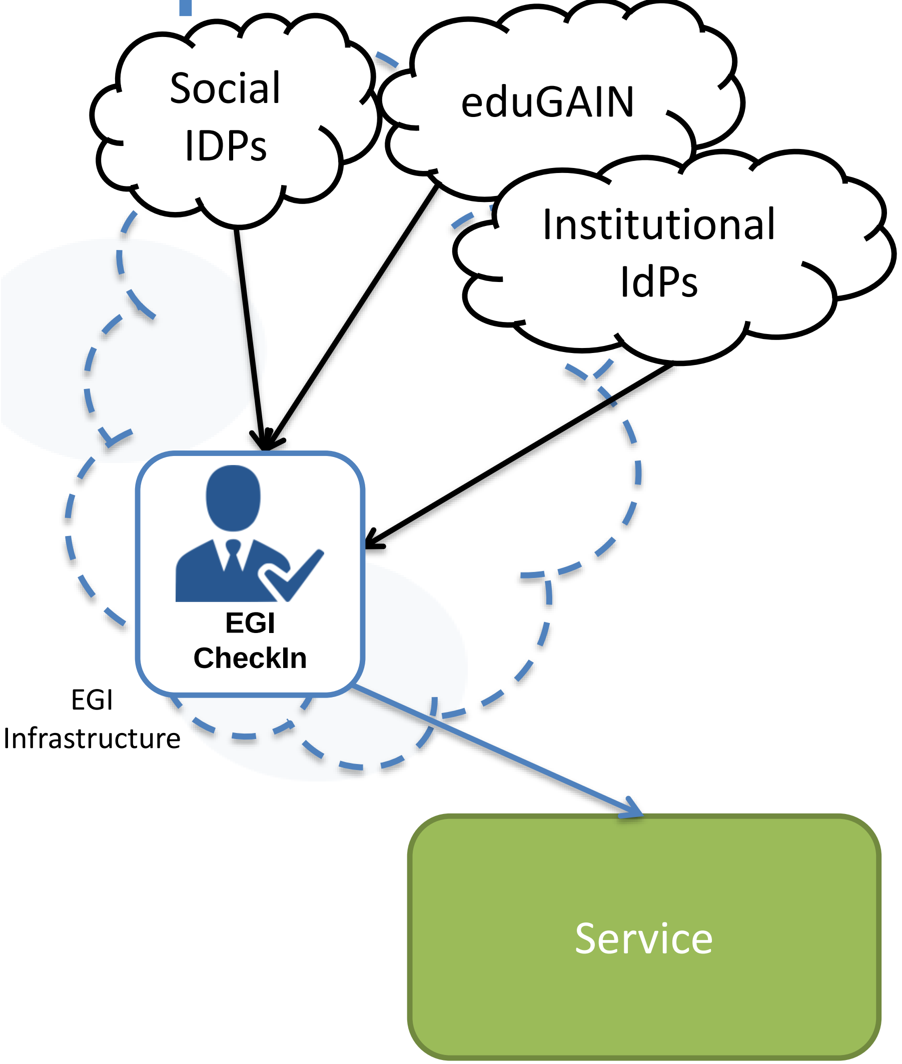


Supported technologies: COmanage Perun

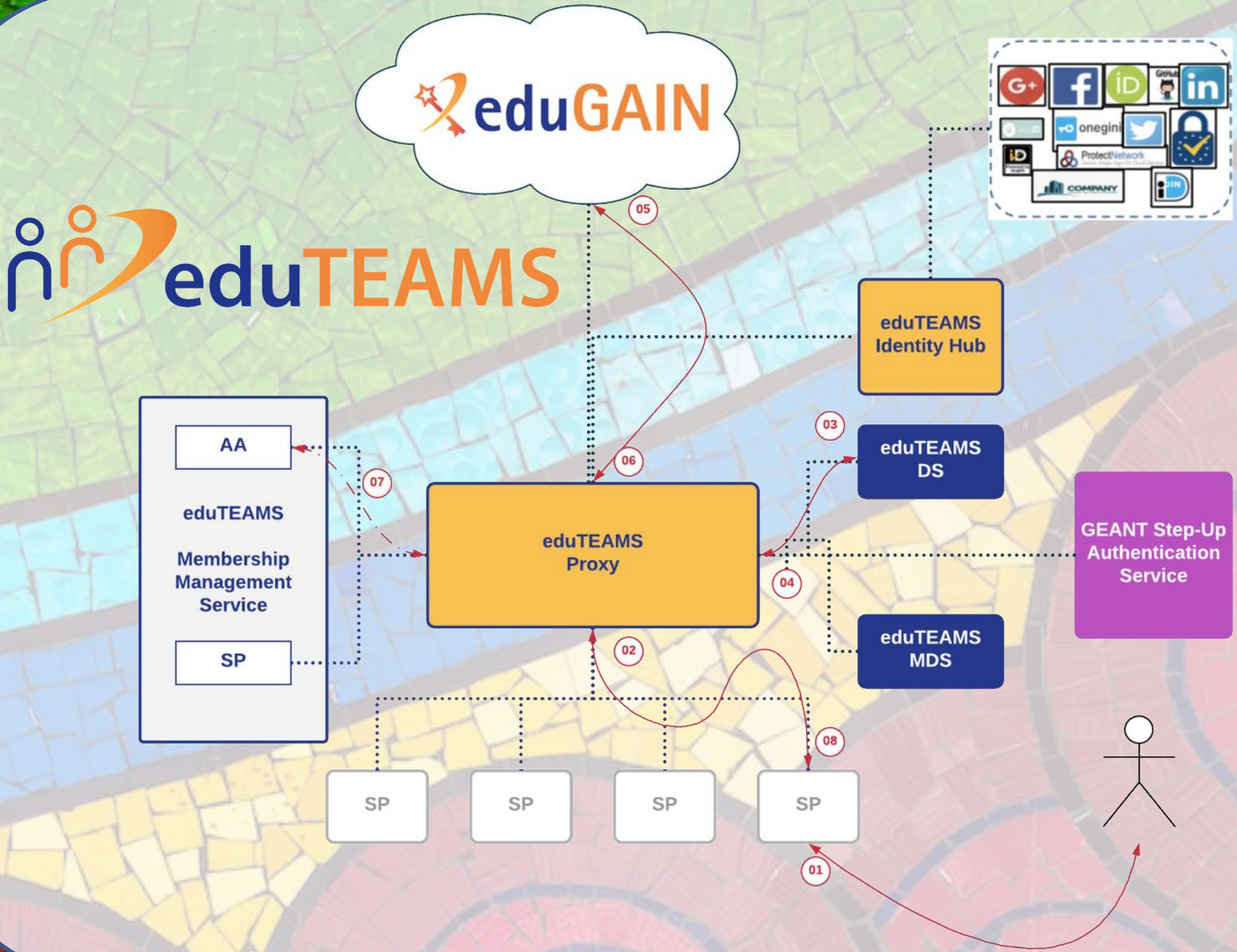
For service providers: AAI as a service

Check-in as an authentication proxy

- ✓ Enable login from institutional IdPs in eduGAIN and social media
- ✓ Minimal overhead for the service development
- ✓ All the other CheckIn features are available for the SP: account linking, attribute aggregation, ..
- Prerequisites:
  - ✓ Service provider must accept EGI policies on data protection



GÉANT
Networks • Services • People



eduTEAMS Offerings

eduTEAMS Service

Provided by GÉANT to small and medium sized communities who want to get started with their virtual collaborations and take full advantage of the federated access without having to deal with the complexity of operating and supporting their own AAI. Supports multiple communities on the same platform. Provides everything required in order to securely collaborate and use services available to the GÉANT community and European Open Science Cloud.

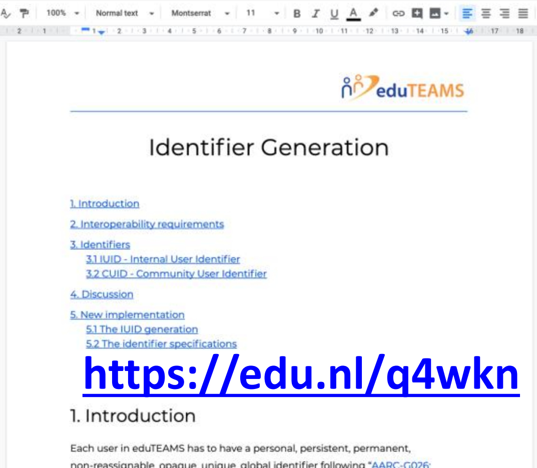
eduTEAMS Dedicated

For communities requiring full control of their AAI, GÉANT can host and operate their own, dedicated AAI Service powered by the eduTEAMS technology. Communities can rely on the operational capabilities and expertise of GÉANT, while they are in full control of the policies, configuration and branding of their AAI.

eduTEAMS Bespoke

For those communities who require tailor-made functionality, such as integration with custom back-office and front-office systems, new features or enhancing their existing AAIs with new functionality available in eduTEAMS, GÉANT can provide bespoke solutions based on the eduTEAMS technology, which can include a combination of consultancy, development and hosting of the service.

ID Generator -> IUIDs



eduTEAMS

Identifier Generation

https://edu.nl/q4wkn

1. Introduction

Each user in eduTEAMS has to have a personal, persistent, permanent, non-reassignable, opaque, unique, global identifier following "AARC-G026:

ID Generator -> IUIDs

Attribute Checker

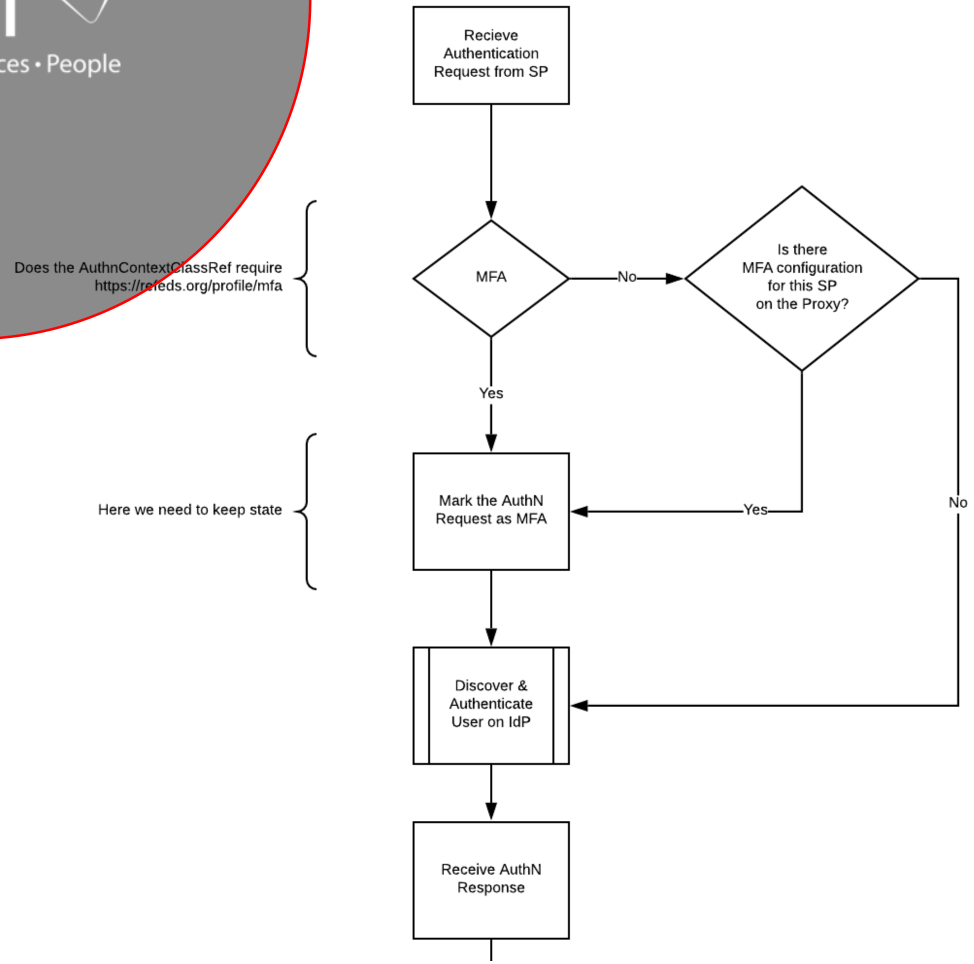
ID Generator -> IUIDs

Attribute Checker

Step Up

Step-Up Authentication Flow

Authentication Request from SP



Recieve Authentication Request from SP

Does the AuthnContextClassRef require https://refeds.org/profile/mfa

MFA

No

Is there MFA configuration for this SP on the Proxy?

Yes

Here we need to keep state

Mark the AuthN Request as MFA

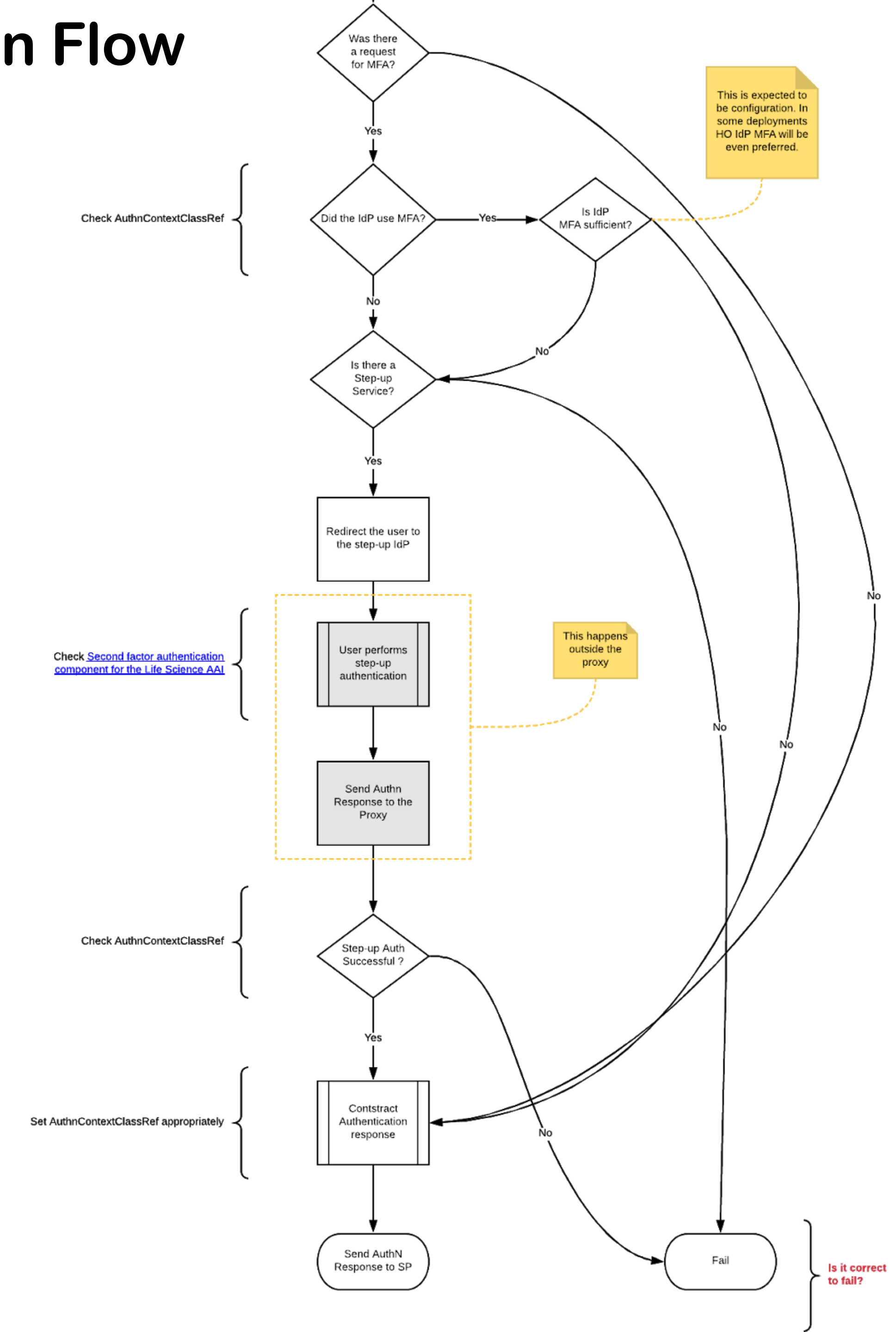
Yes

No

Discover & Authenticate User on IdP

Receive AuthN Response

Authentication Response from IdP



Was there a request for MFA?

Yes

Check AuthnContextClassRef

Did the IdP use MFA?

Yes

Is IdP MFA sufficient?

This is expected to be configuration. In some deployments HO IdP MFA will be even preferred.

No

No

Is there a Step-up Service?

Yes

Redirect the user to the step-up IdP

Check Second factor authentication component for the Life Science AAI

User performs step-up authentication

This happens outside the proxy

Send Authn Response to the Proxy

Check AuthnContextClassRef

Step-up Auth Successful ?

Yes

Set AuthnContextClassRef appropriately

Contstract Authentication response

Send AuthN Response to SP

No

No

No

No

Fail

Is it correct to fail?

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Return user record
including CUID

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Query MMS

Return user record
including CUID

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Query MMS

Process Attributes

Return user record
including CUID

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Query MMS

Process Attributes

SP Check

Return user record
including CUID

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Query MMS

Return user record
including CUID

Process Attributes

SP Check

Active Attribute
Selection

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Query MMS

Process Attributes

SP Check

Active Attribute Selection

Consent

Return user record including CUID

ID Generator -> IUIDs

Attribute Checker

Step Up

Query Account Registry

Query MMS

Return user record
including CUID

CUID
email
name
affiliation

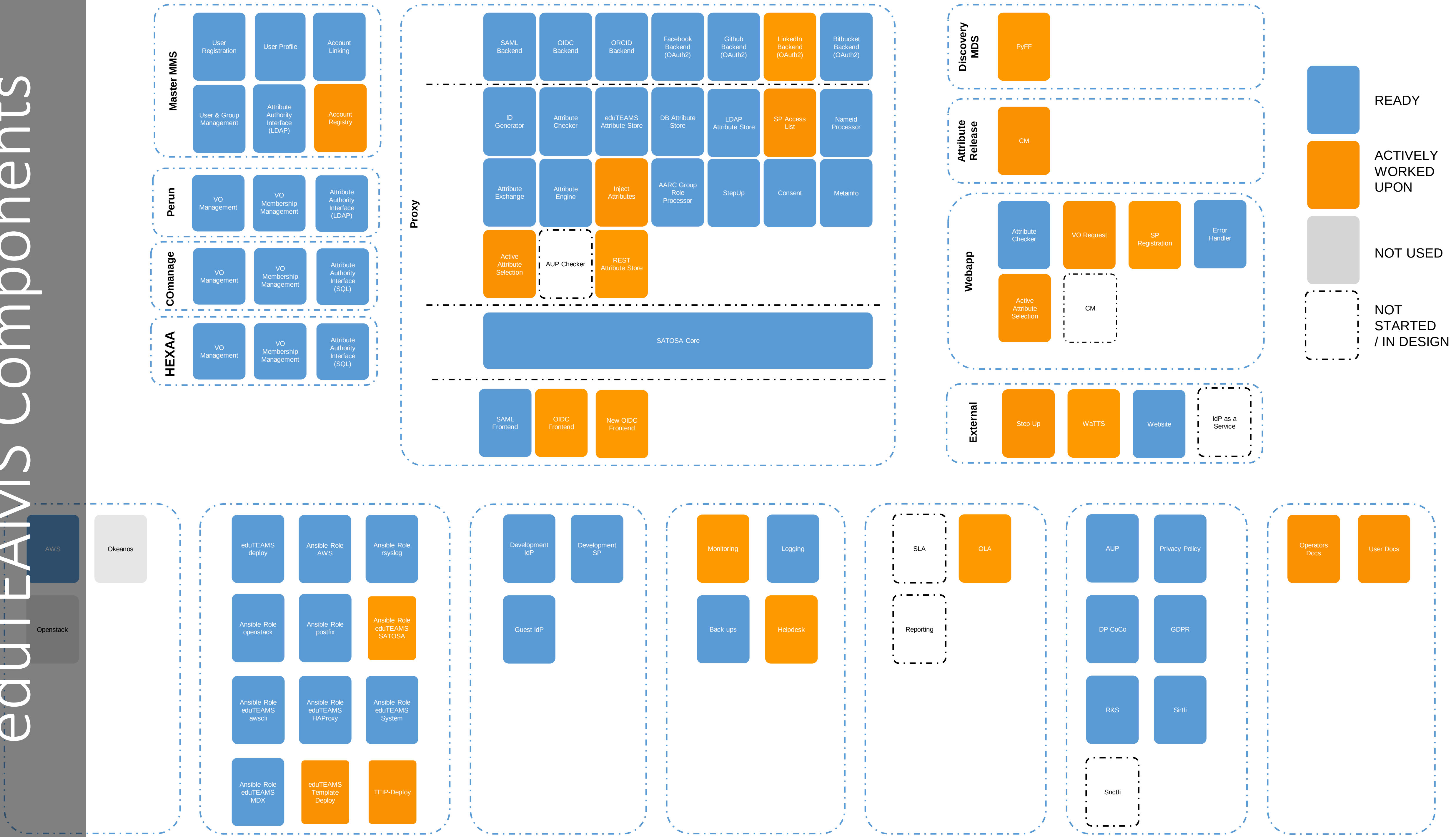
Process Attributes

SP Check

Active Attribute
Selection

Consent

eduTEAMS Components



- 🟦 READY
- 🟧 ACTIVELY WORKED UPON
- ▨ NOT USED
- ⬚ NOT STARTED / IN DESIGN

Master MMS
- 🟦 User Registration
- 🟦 User Profile
- 🟦 Account Linking
- 🟦 User & Group Management
- 🟦 Attribute Authority Interface (LDAP)
- 🟧 Account Registry

Perun
- 🟦 VO Management
- 🟦 VO Membership Management
- 🟦 Attribute Authority Interface (LDAP)

COmanage
- 🟦 VO Management
- 🟦 VO Membership Management
- 🟦 Attribute Authority Interface (SQL)

HEXAA
- 🟦 VO Management
- 🟦 VO Membership Management
- 🟦 Attribute Authority Interface (SQL)

Proxy
- 🟦 SAML Backend
- 🟦 OIDC Backend
- 🟦 ORCID Backend
- 🟦 Facebook Backend (OAuth2)
- 🟦 Github Backend (OAuth2)
- 🟧 LinkedIn Backend (OAuth2)
- 🟦 Bitbucket Backend (OAuth2)
- 🟦 ID Generator
- 🟦 Attribute Checker
- 🟦 eduTEAMS Attribute Store
- 🟦 DB Attribute Store
- 🟦 LDAP Attribute Store
- 🟧 SP Access List
- 🟦 Nameid Processor
- 🟦 Attribute Exchange
- 🟦 Attribute Engine
- 🟧 Inject Attributes
- 🟦 AARC Group Role Processor
- 🟦 StepUp
- 🟦 Consent
- 🟦 Metainfo
- 🟧 Active Attribute Selection
- ⬚ AUP Checker
- 🟧 REST Attribute Store
- 🟦 SATOSA Core
- 🟦 SAML Frontend
- 🟧 OIDC Frontend
- 🟧 New OIDC Frontend

Discovery MDS
- 🟧 PyFF

Attribute Release
- 🟧 CM

Webapp
- 🟦 Attribute Checker
- 🟧 VO Request
- 🟧 SP Registration
- 🟦 Error Handler
- 🟧 Active Attribute Selection
- ⬚ CM

External
- 🟧 Step Up
- 🟧 WaTTS
- 🟦 Website
- ⬚ IdP as a Service

- AWS
- ▨ Okeanos
- Openstack

- 🟦 eduTEAMS deploy
- 🟦 Ansible Role AWS
- 🟦 Ansible Role rsyslog
- 🟦 Ansible Role openstack
- 🟦 Ansible Role postfix
- 🟧 Ansible Role eduTEAMS SATOSA
- 🟦 Ansible Role eduTEAMS awscli
- 🟦 Ansible Role eduTEAMS HAProxy
- 🟦 Ansible Role eduTEAMS System
- 🟦 Ansible Role eduTEAMS MDX
- 🟧 eduTEAMS Template Deploy
- 🟧 TEIP-Deploy

- 🟦 Development IdP
- 🟦 Development SP
- 🟦 Guest IdP

- 🟧 Monitoring
- 🟦 Logging
- 🟦 Back ups
- 🟧 Helpdesk

- ⬚ SLA
- 🟧 OLA
- ⬚ Reporting

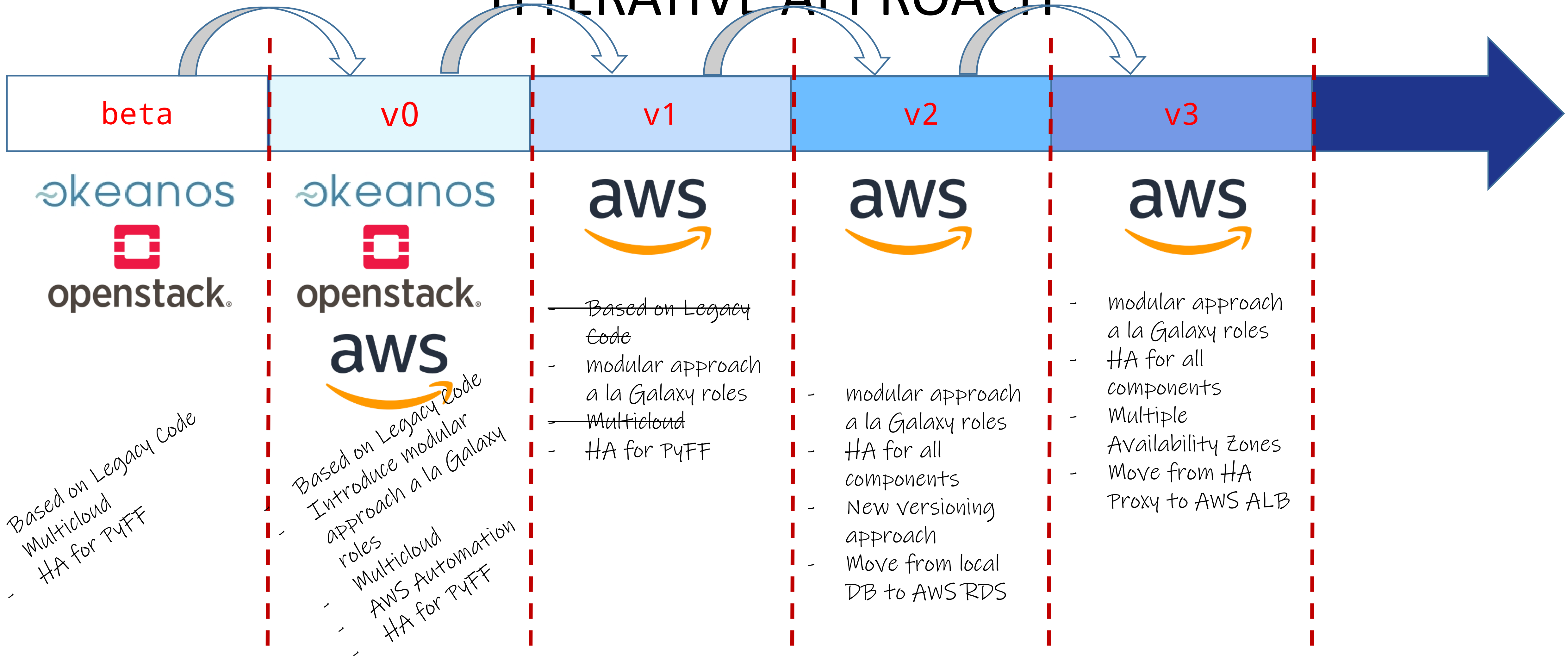
- 🟦 AUP
- 🟦 Privacy Policy
- 🟦 DP CoCo
- 🟦 GDPR
- 🟦 R&S
- 🟦 Sirtfi
- ⬚ Snctfi

- 🟧 Operators Docs
- 🟧 User Docs

INFRASTRUCTURE AS CODE

eduTEAMS

ITTERATIVE APPROACH



beta:

- Based on Legacy Code
- Multicloud
- HA for PyFF

v0:

- Based on Legacy Code
- Introduce modular approach a la Galaxy roles
- Multicloud
- AWS Automation
- HA for PyFF

v1:

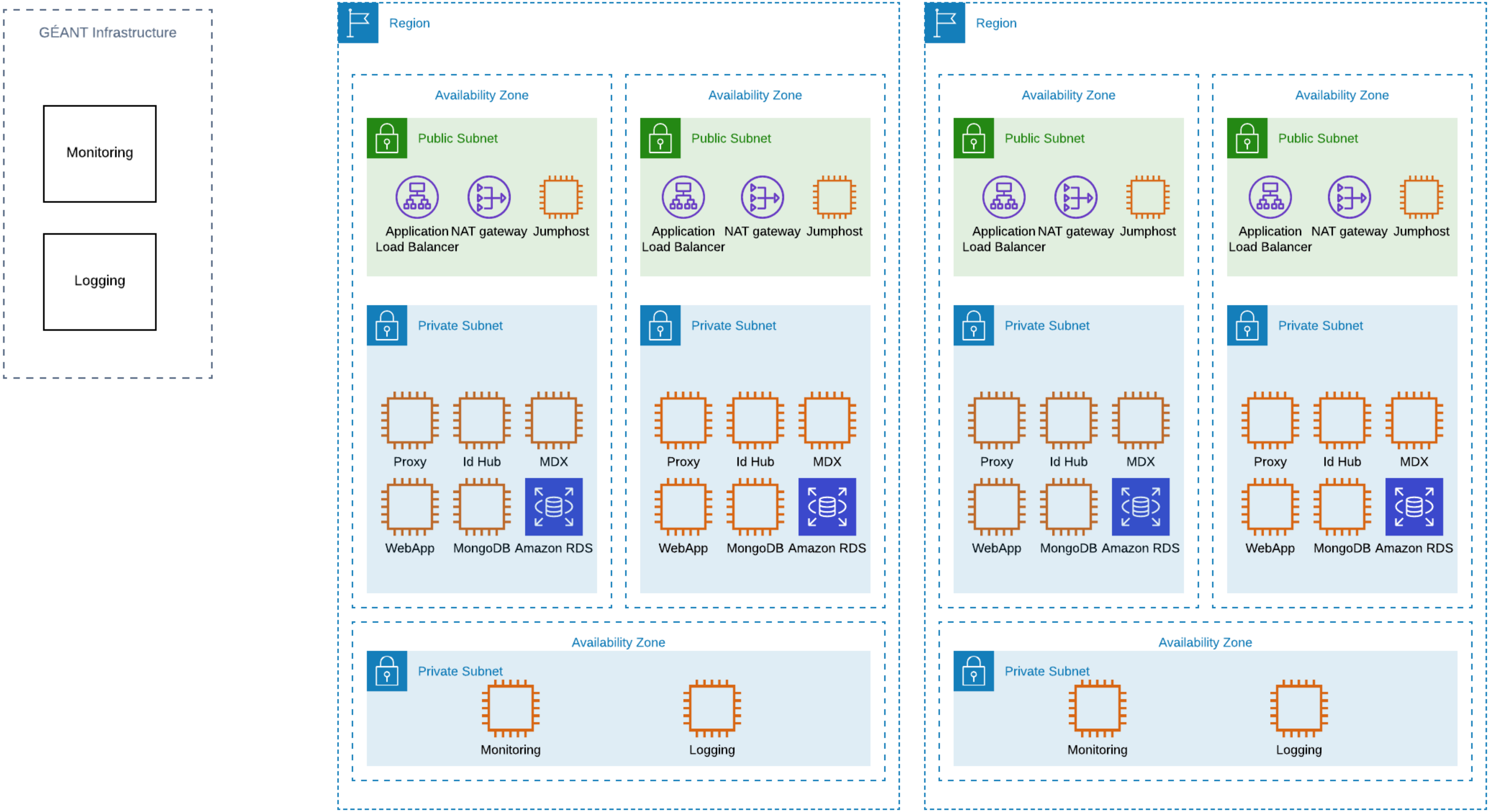
- ~~Based on Legacy Code~~
- modular approach a la Galaxy roles
- ~~Multicloud~~
- HA for PyFF

v2:

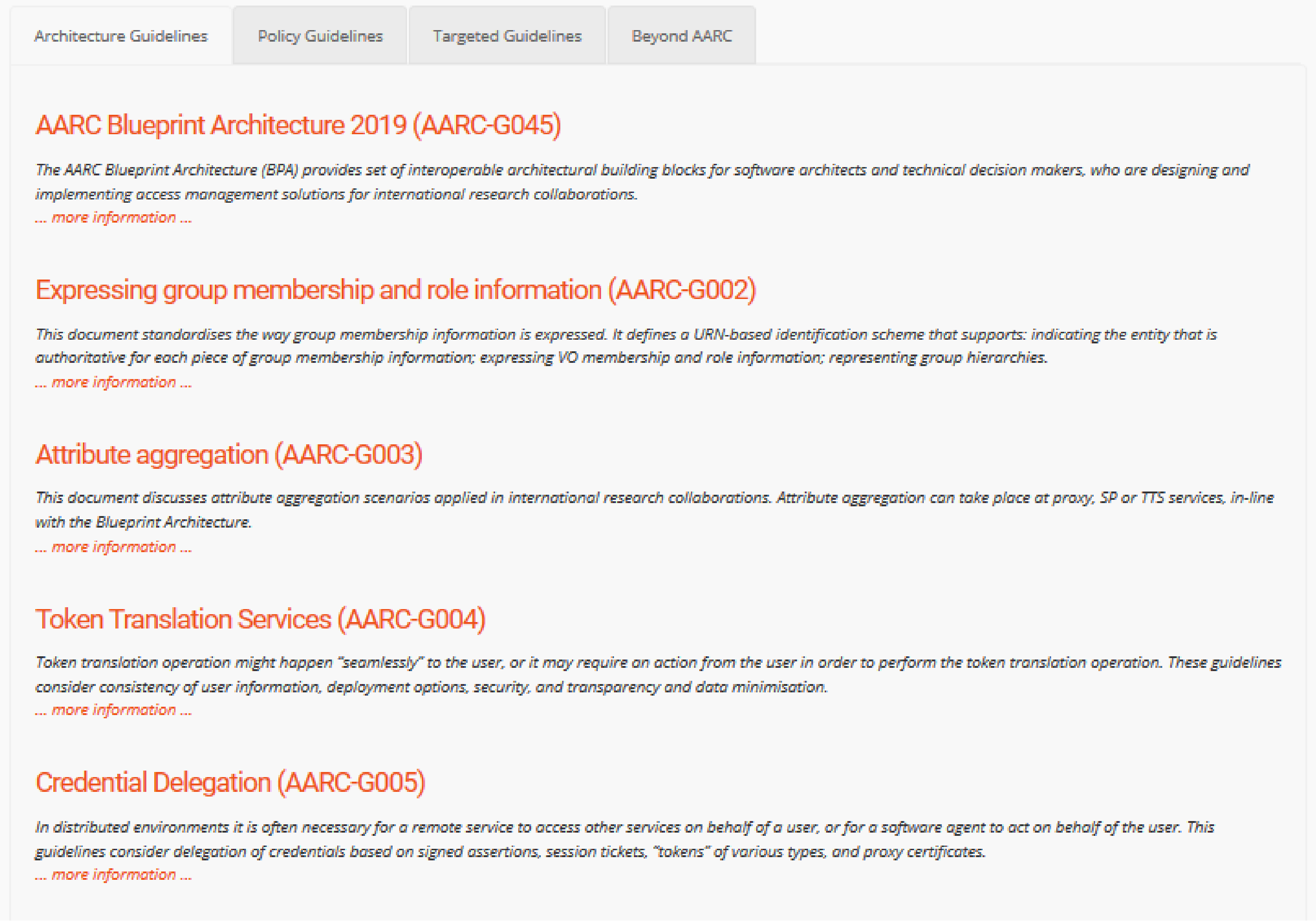
- modular approach a la Galaxy roles
- HA for all components
- New versioning approach
- Move from local DB to AWS RDS

v3:

- modular approach a la Galaxy roles
- HA for all components
- Multiple Availability Zones
- Move from HA Proxy to AWS ALB


GÉANT Infrastructure
Monitoring
Logging
Region
Availability Zone
Public Subnet
Application Load Balancer
NAT gateway
Jumphost
Private Subnet
Proxy
Id Hub
MDX
WebApp
MongoDB
Amazon RDS
Availability Zone
Public Subnet
Application Load Balancer
NAT gateway
Jumphost
Private Subnet
Proxy
Id Hub
MDX
WebApp
MongoDB
Amazon RDS
Availability Zone
Private Subnet
Monitoring
Logging
Region
Availability Zone
Public Subnet
Application Load Balancer
NAT gateway
Jumphost
Private Subnet
Proxy
Id Hub
MDX
WebApp
MongoDB
Amazon RDS
Availability Zone
Public Subnet
Application Load Balancer
NAT gateway
Jumphost
Private Subnet
Proxy
Id Hub
MDX
WebApp
MongoDB
Amazon RDS
Availability Zone
Private Subnet
Monitoring
Logging

Interoperation and guidelines



AARC Blueprint Architecture 2019 (AARC-G045)

The AARC Blueprint Architecture (BPA) provides set of interoperable architectural building blocks for software architects and technical decision makers, who are designing and implementing access management solutions for international research collaborations.

... more information ...

Expressing group membership and role information (AARC-G002)

This document standardises the way group membership information is expressed. It defines a URN-based identification scheme that supports: indicating the entity that is authoritative for each piece of group membership information; expressing VO membership and role information; representing group hierarchies.

... more information ...

Attribute aggregation (AARC-G003)

This document discusses attribute aggregation scenarios applied in international research collaborations. Attribute aggregation can take place at proxy, SP or TTS services, in-line with the Blueprint Architecture.

... more information ...

Token Translation Services (AARC-G004)

Token translation operation might happen "seamlessly" to the user, or it may require an action from the user in order to perform the token translation operation. These guidelines consider consistency of user information, deployment options, security, and transparency and data minimisation.

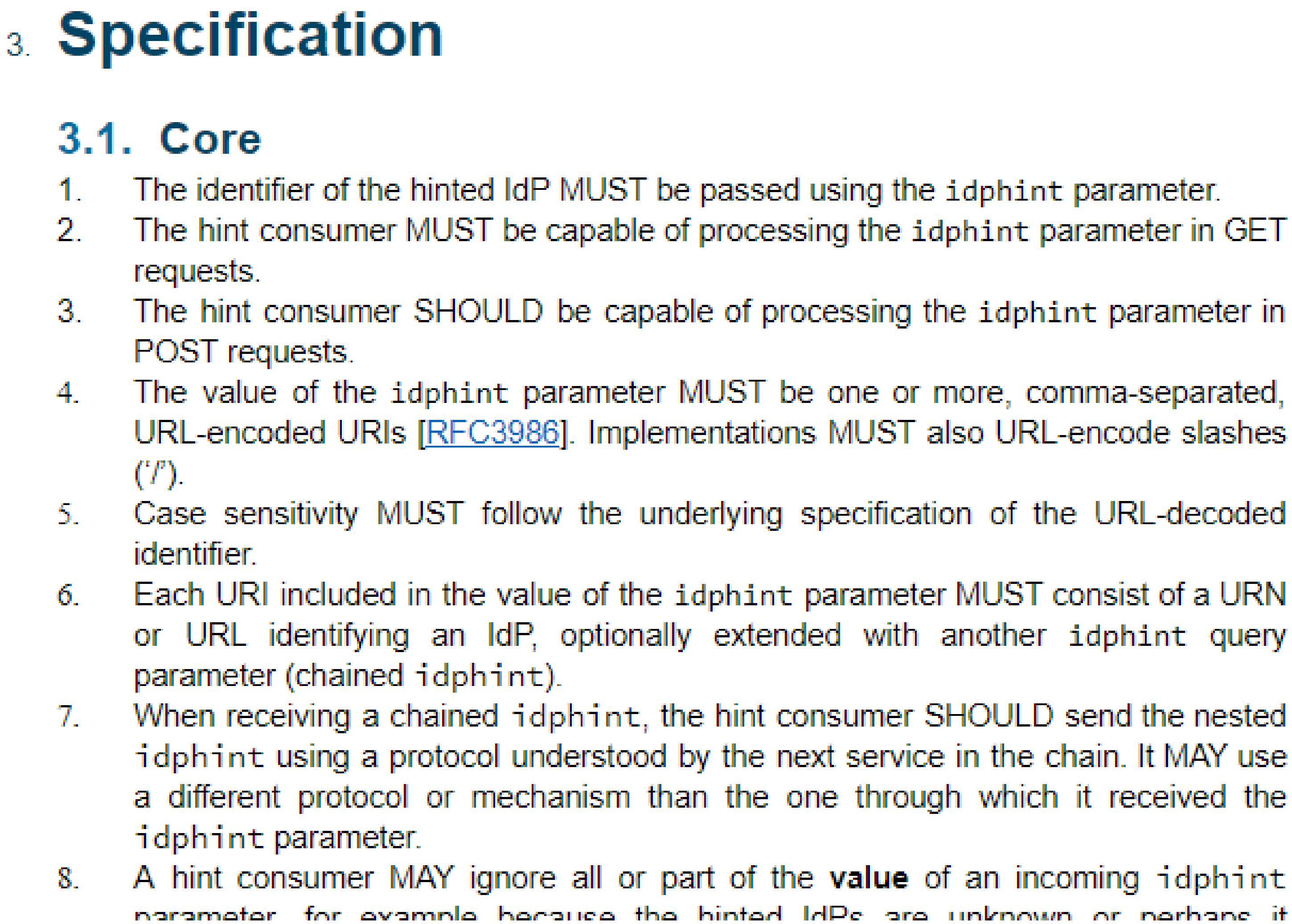
... more information ...

Credential Delegation (AARC-G005)

In distributed environments it is often necessary for a remote service to access other services on behalf of a user, or for a software agent to act on behalf of the user. This guidelines consider delegation of credentials based on signed assertions, session tickets, "tokens" of various types, and proxy certificates.

... more information ...

Example: IdP hinting specification in hierarchical proxy scenarios



3. Specification

3.1. Core

1. The identifier of the hinted IdP MUST be passed using the `idphint` parameter.
2. The hint consumer MUST be capable of processing the `idphint` parameter in GET requests.
3. The hint consumer SHOULD be capable of processing the `idphint` parameter in POST requests.
4. The value of the `idphint` parameter MUST be one or more, comma-separated, URL-encoded URIs [RFC3986]. Implementations MUST also URL-encode slashes ('/').
5. Case sensitivity MUST follow the underlying specification of the URL-decoded identifier.
6. Each URI included in the value of the `idphint` parameter MUST consist of a URN or URL identifying an IdP, optionally extended with another `idphint` query parameter (chained `idphint`).
7. When receiving a chained `idphint`, the hint consumer SHOULD send the nested `idphint` using a protocol understood by the next service in the chain. It MAY use a different protocol or mechanism than the one through which it received the `idphint` parameter.
8. A hint consumer MAY ignore all or part of the **value** of an incoming `idphint` parameter, for example because the hinted IdPs are unknown or perhaps it

Evolution of the BPA

The AARC Community, with and alongside European and global efforts, evolves the BPA

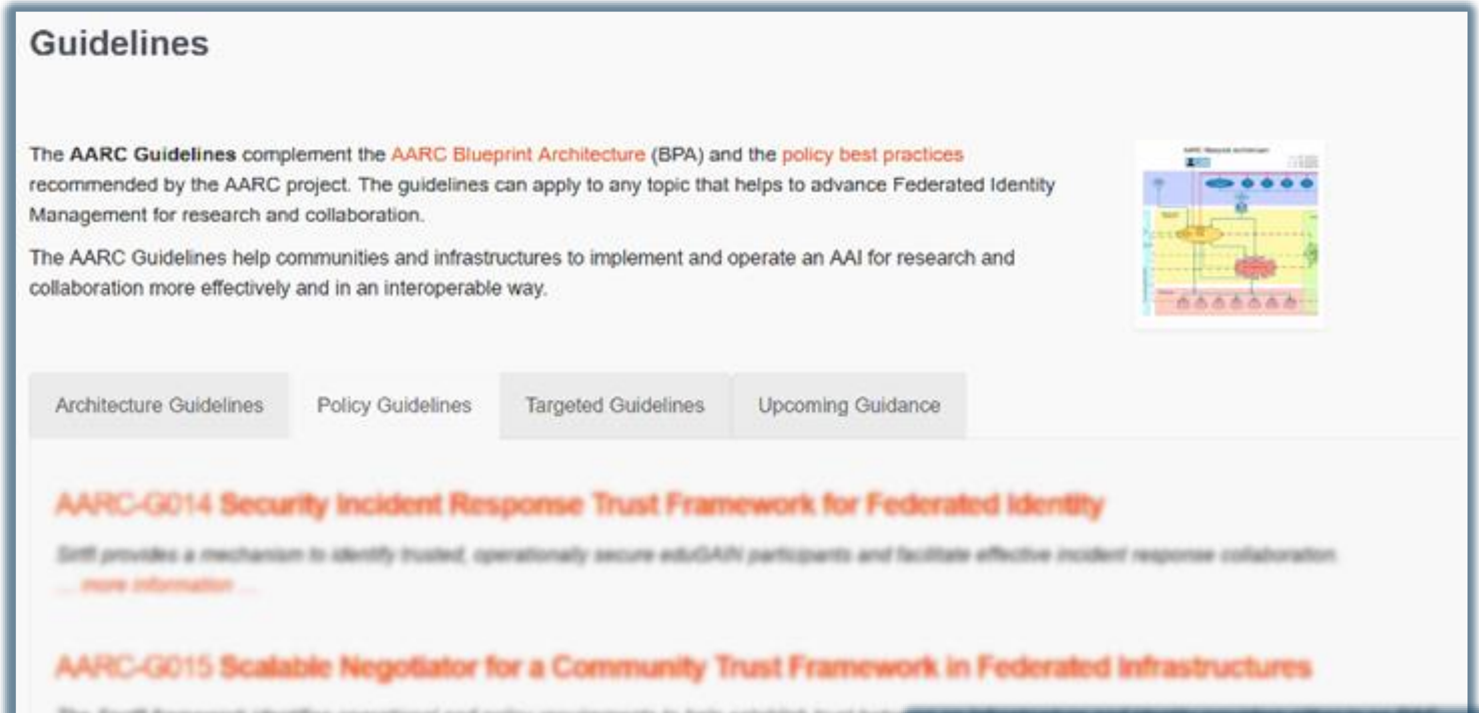
- https://aarc-community.org/architecture (the result thereof is /guidelines)
- AppInt – the “Application Integration” mailing list
  https://lists.geant.org/sympa/info/appint
- AppInt also the public discussion forum for the EOSC AAI Task Force of the Architecture WG
- AppInt keybase team: https://keybase.io/team/appint

https://g.nikhef.nl/eosc-sec-wp section 3 (AAI)

Policy recommendations and good practices for the BPA and AAI systems

Taming the Proxy

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-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 betw

Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Pr

... more information ...

AARC-G021 Exchange of specific assurance information betwee

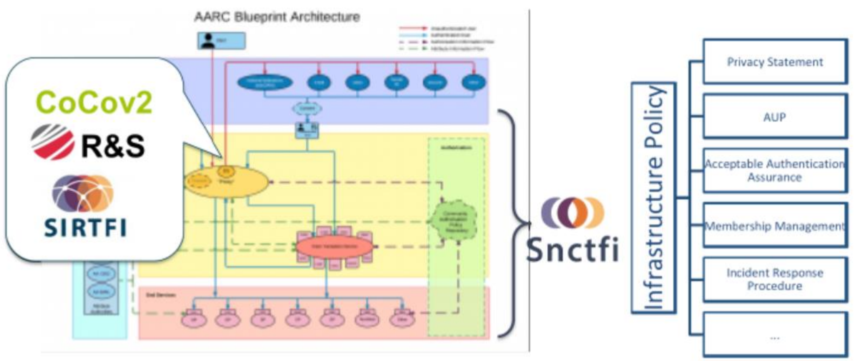
Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived fr

resulting assurance assertion obtained between Infrastructures so that it need not be re-compu

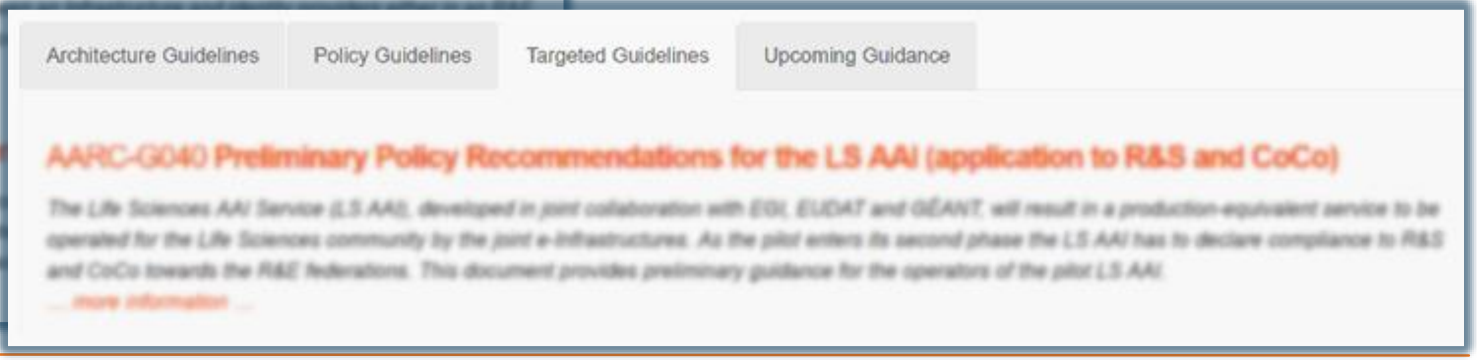
provider. This document describes the assurance profiles recommended to be used by the Infra

... more information ...

aarc-community.org/guidelines



AARC Blueprint Architecture
CoCov2
R&S
SIRTFI
Snctfi
Infrastructure Policy
Privacy Statement
AUP
Acceptable Authentication Assurance
Membership Management
Incident Response Procedure
...



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 EGI, 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 ...

The evolved role for policy and best practices for the AARC Community

Policy Guidelines for the Proxy and Infrastructure Consultancy role for *communities* & *infrastructures*

- work items address policy aspects of the architecture & implementation, *e.g.*,

  AARC-G041 *Assurance derived from social media*
  AARC-G048 *Secure Operation of Attribute Authorities …*

- address 'pilots' from the AARC communities, or Infrastructures, *e.g.*

  AARC-G040 *Policy Recommendations for the LS AAI (application to R&S and CoCo)*
  AARC-I044 *Implementers Guide to the WISE Baseline Acceptable Use Policy*

You see the policy work 'homed' in your favourite forums: WISE, IGTF, REFEDS, FIM4R

joint work
with peers in

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

E-INFRASTRUCTURES:
MAKING EUROPE THE BEST PLACE
FOR RESEARCH AND INNOVATION
EUDAT
GÉANT
OpenAIRE
PRACE
SECURITY FOR COLLABORATING INFRASTRUCTURES
security

WISE COMMUNITY

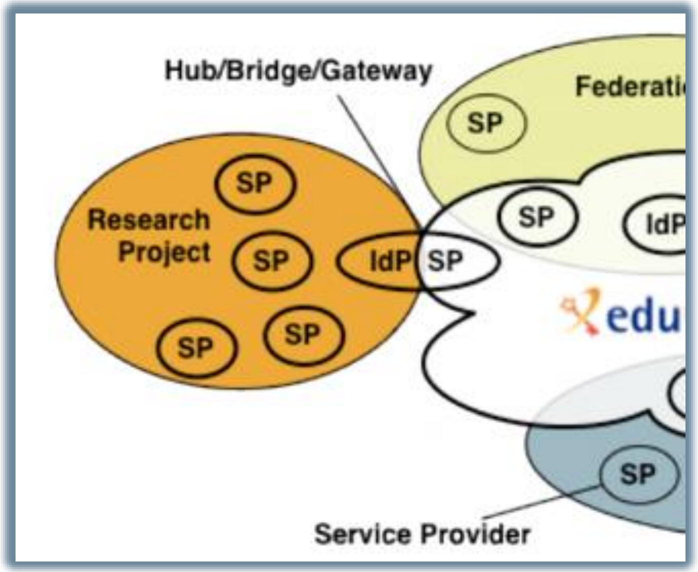
“enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks.”

which is the role of SCI - Security for Collaboration among Infrastructures

A policy framework for service providers groups and proxies in the BPA

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures



Sncffi v1.0 AARC

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsara)

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

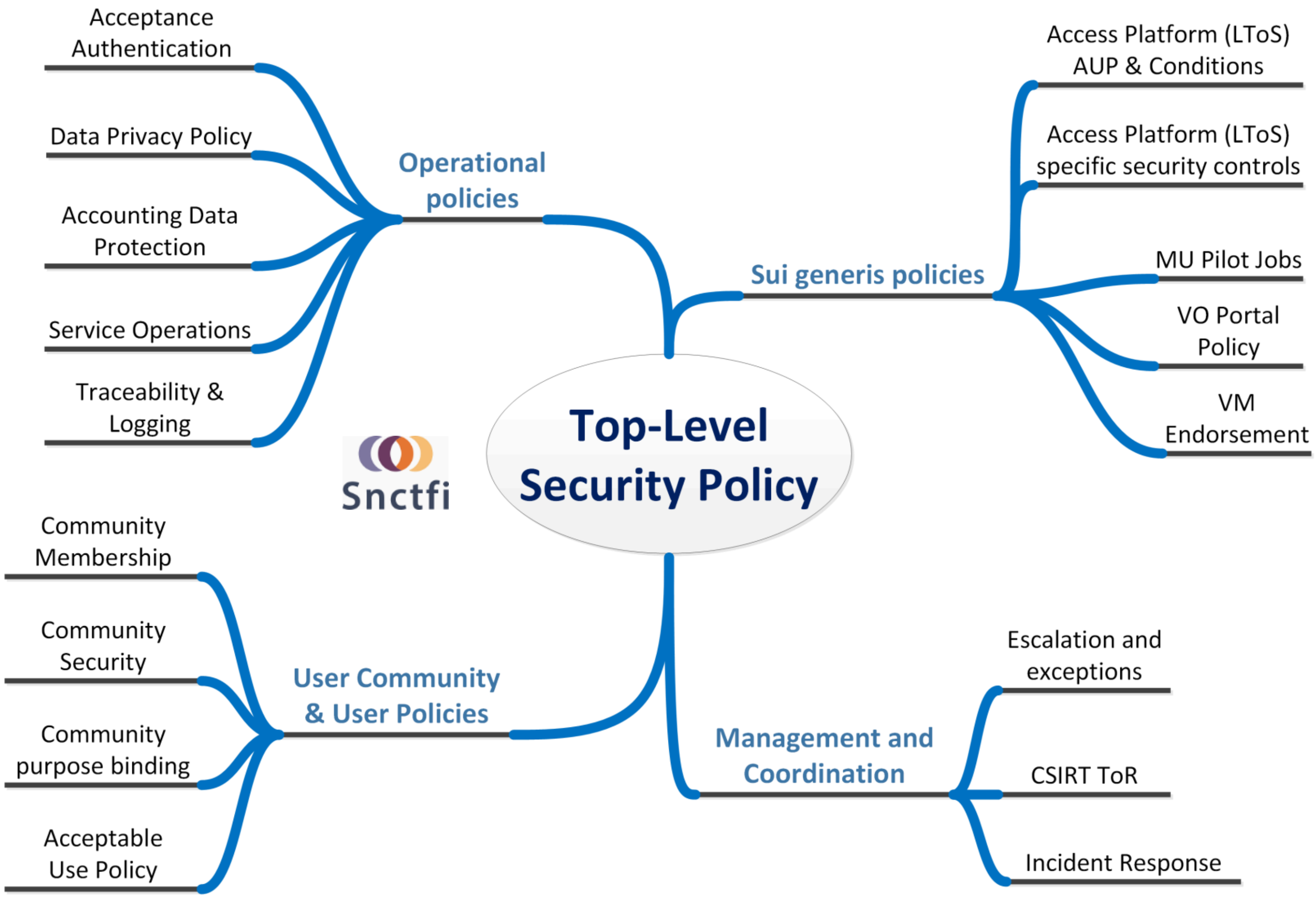
Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

derived from **SCIv2**: framework on *Security for Collaboration in Infrastructures* via **WISE**

reference policies supporting *Snctfi* fulfilment in the Policy Development Kit

graphic IdP-SP bridge: Lukas Hammerle and Ann Harding, SWITCH

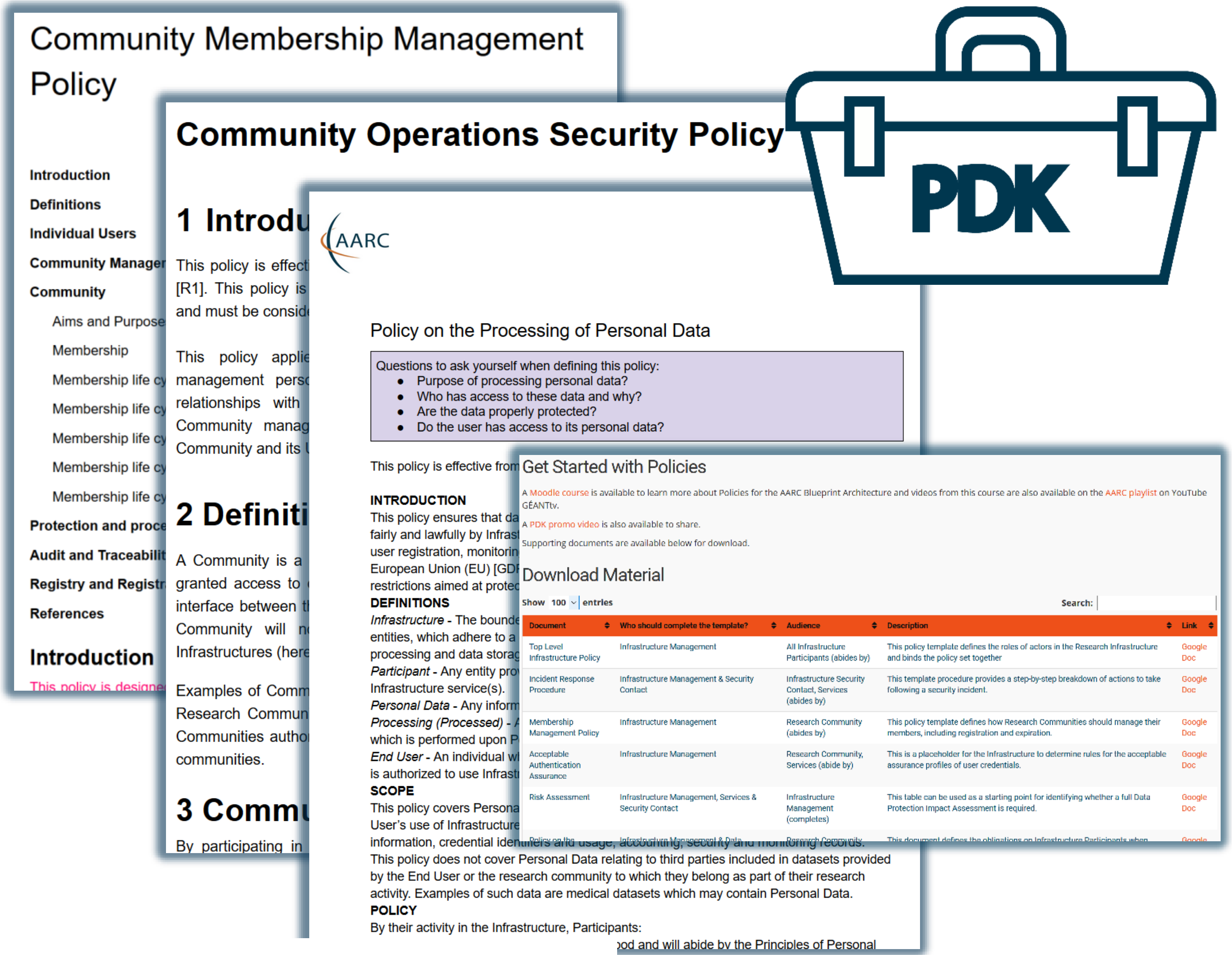
Mapping the trust and availability landscape areas


Top-Level Security Policy
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
Snctfi
User Community & User Policies
Community Membership
Community Security
Community purpose binding
Acceptable Use Policy
Management and Coordination
Escalation and exceptions
CSIRT ToR
Incident Response

Implementing Snctfi in community policies

Relevant to communities and e-Infrastructures both

- what are the requisite policy elements and processes you need to define to manage a structured community?
- which of these are required to access general-purpose e-Infrastructures?
- which roles and responsibilities lie with the community 'management' so that the BPA proxy model will scale out?



Community Membership Management Policy

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

Introduction

This policy is designe

Community Operations Security Policy

1 Introdu

This policy is effect
[R1]. This policy is
and must be consid

This policy applie
management pers
relationships with
Community manag
Community and its

2 Definiti

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

Examples of Comm
Research Commun
Communities autho
communities.

3 Commu

By participating in

AARC

Policy on the Processing of Personal Data

Questions to ask yourself when defining this policy:
- Purpose of processing personal data?
- Who has access to these data and why?
- Are the data properly protected?
- Do the user has access to its personal data?

This policy is effective from

INTRODUCTION
This policy ensures that da
fairly and lawfully by Infras
user registration, monitorin
European Union (EU) [GD
restrictions aimed at protec
DEFINITIONS
Infrastructure - The bounde
entities, which adhere to a
processing and data storag
Participant - Any entity pro
Infrastructure service(s).
Personal Data - Any inform
Processing (Processed) - A
which is performed upon P
End User - An individual w
is authorized to use Infrast
SCOPE
This policy covers Persona
User's use of Infrastructure
information, credential identifiers and usage, accounting, security and monitoring records.
This policy does not cover Personal Data relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.
POLICY
By their activity in the Infrastructure, Participants:
od and will abide by the Principles of Personal

Get Started with Policies

A Moodle course is available to learn more about Policies for the AARC Blueprint Architecture and videos from this course are also available on the AARC playlist on YouTube GÉANTtv.

A PDK promo video is also available to share.

Supporting documents are available below for download.

Download Material

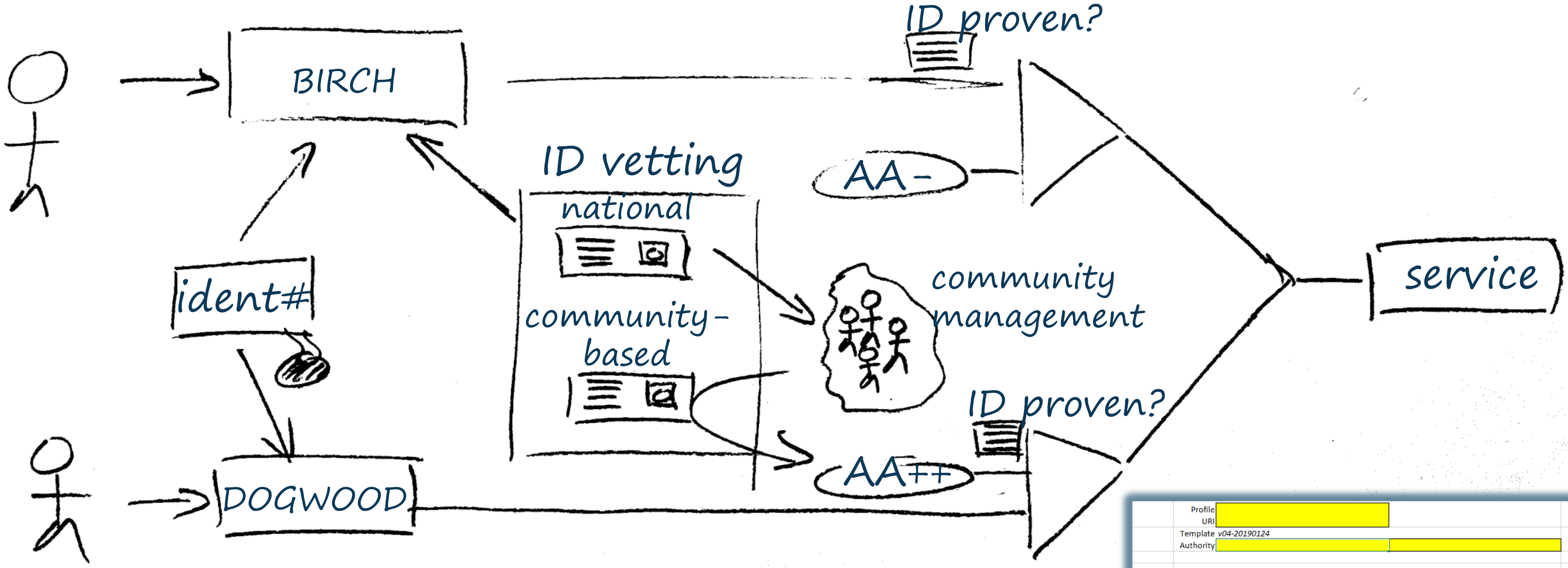
Show 100 entries Search:

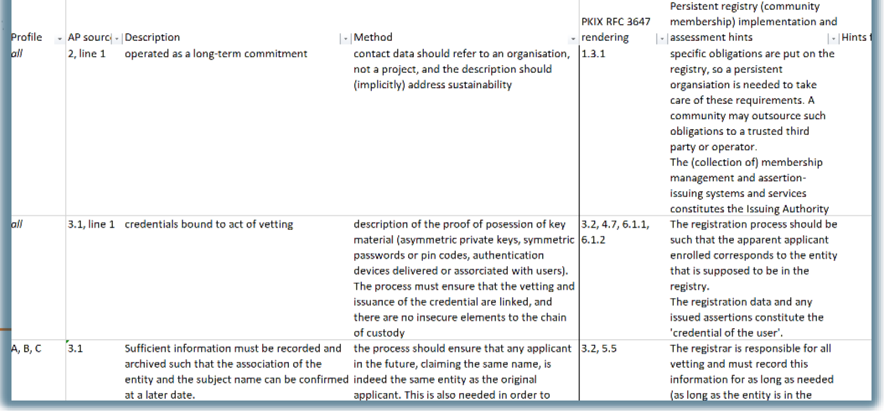
Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the	Infrastructure Management & Data	Research Community	This document defines the obligations on Infrastructure Participants when	Google

https://aarc-community.org/policies/policy-development-kit/

in collaboration with EGI, GEANT, EOSC-Hub, EUDAT, WLCG, PRACE, HBP, and SURF

A (too) Complex Example: Acceptable Authentication Assurance – enabling flexible user communities by mapping assurance elements





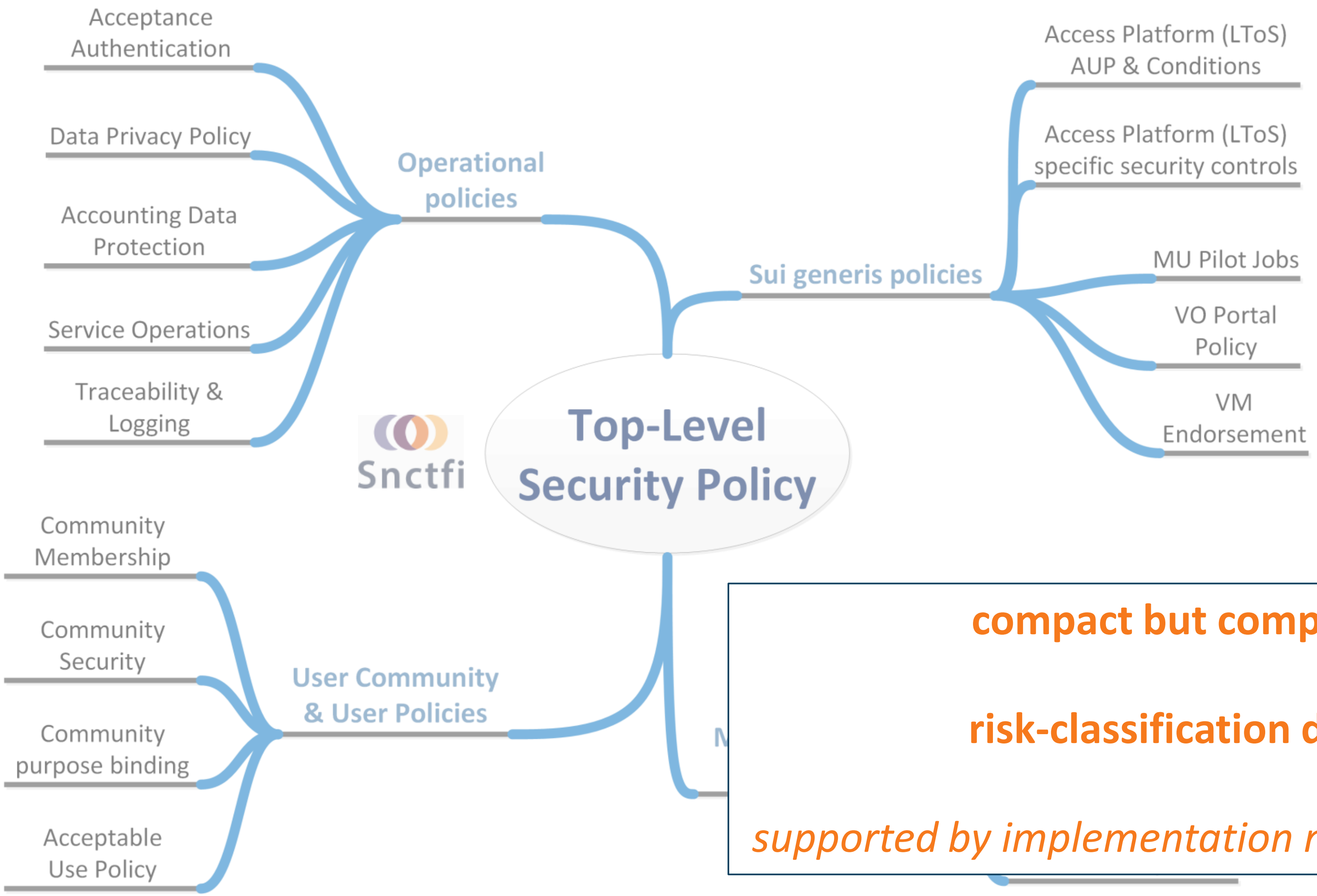
	Profile URI					
	Template	*v04-20190124*				
	Authority					
Profile	AP sourc	Description	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints f
all	2, line 1	operated as a long-term commitment	contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organisation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. The (collection of) membership management and assertion-issuing systems and services constitutes the Issuing Authority	
all	3.1, line 1	credentials bound to act of vetting	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or assorciated with users). The process must ensure that the vetting and issuance of the credential are linked, and there are no insecure elements to the chain of custody	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'credential of the user'.	
A, B, C	3.1	Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date.	the process should ensure that any applicant in the future, claiming the same name, is indeed the same entity as the original applicant. This is also needed in order to	3.2, 5.5	The registrar is responsible for all vetting and must record this information for as long as needed (as long as the entity is in the	

Identity vetting can be done

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

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

Evolving the policy development kit >>> Smplfy the structure



Top-Level Security Policy

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

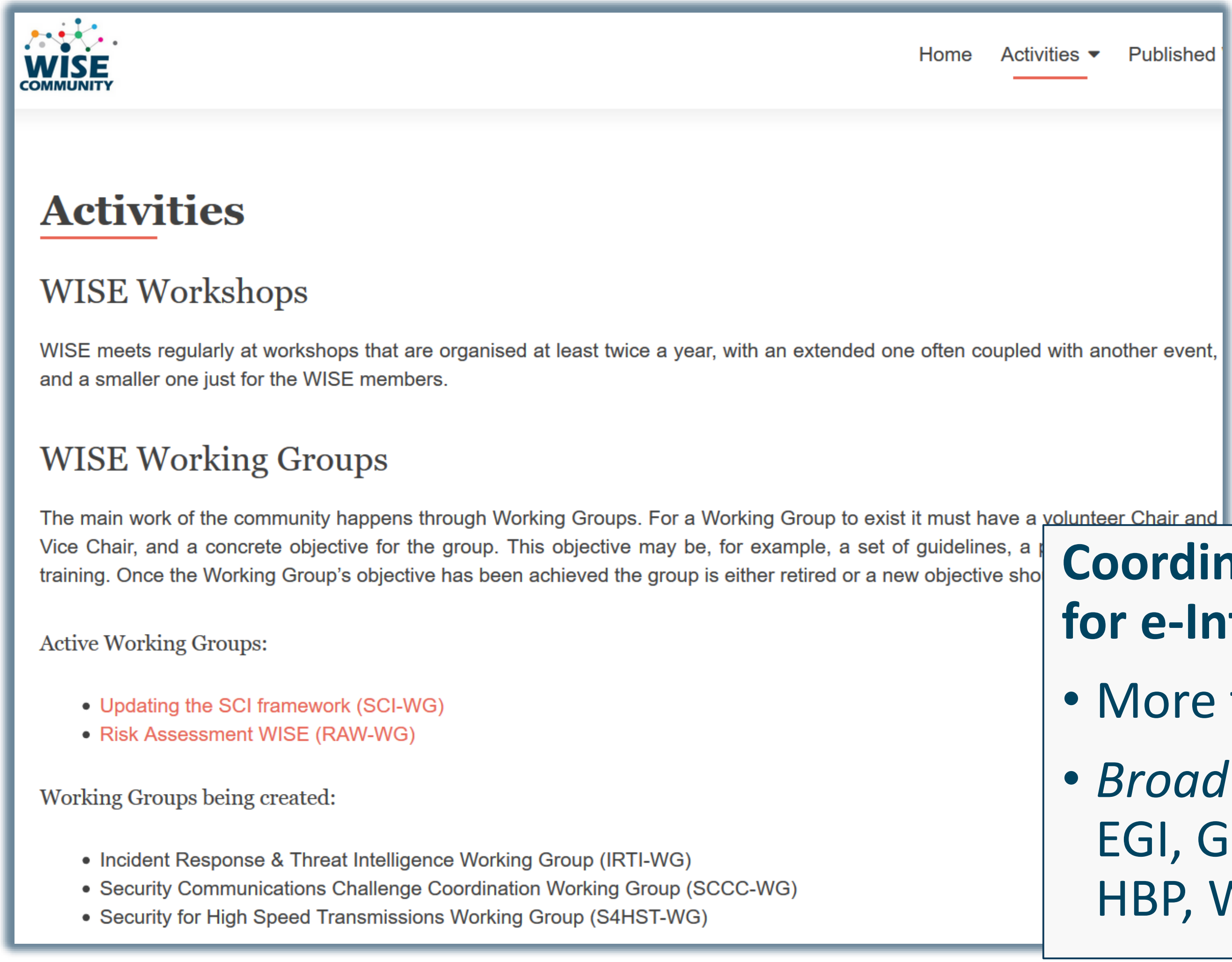
M

compact but comprehensive top-level policy

risk-classification driven policy requirements

supported by implementation measure that can be defined as needed

Bringing Infrastructures Together – the WISE road



Activities

WISE Workshops

WISE meets regularly at workshops that are organised at least twice a year, with an extended one often coupled with another event, and a smaller one just for the WISE members.

WISE Working Groups

The main work of the community happens through Working Groups. For a Working Group to exist it must have a volunteer Chair and Vice Chair, and a concrete objective for the group. This objective may be, for example, a set of guidelines, a training. Once the Working Group's objective has been achieved the group is either retired or a new objective sho

Active Working Groups:

- Updating the SCI framework (SCI-WG)
- Risk Assessment WISE (RAW-WG)

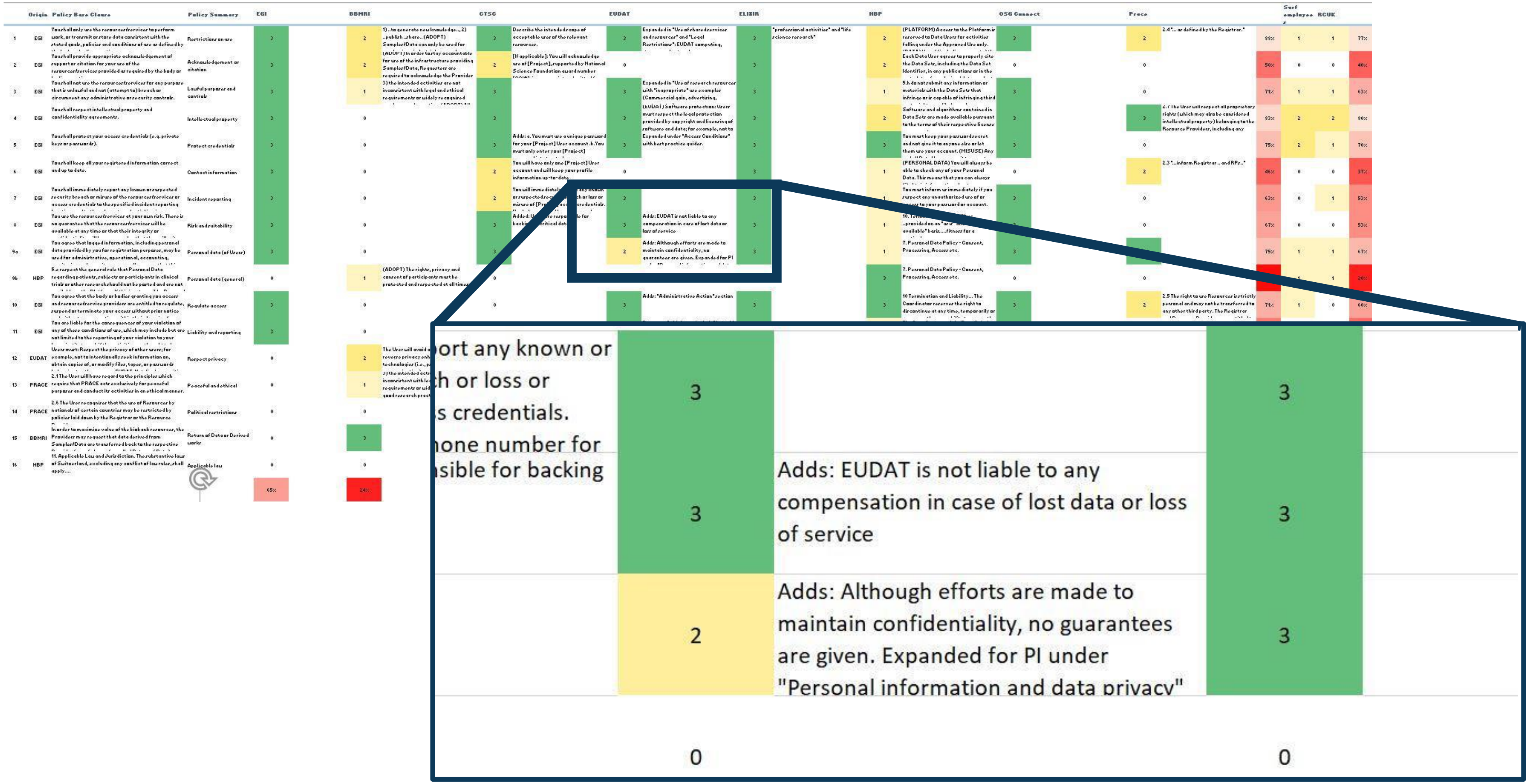
Working Groups being created:

- Incident Response & Threat Intelligence Working Group (IRTI-WG)
- Security Communications Challenge Coordination Working Group (SCCC-WG)
- Security for High Speed Transmissions Working Group (S4HST-WG)

Coordinating Information Security for e-Infrastructures

- More than just the home of SCI
- *Broad collaboration:* steering group with EGI, GEANT, EUDAT, PRACE, XSEDE, OSG, TrustedCI, HBP, WLCG, LIGO, SURF, CERN, CSC, JSC, & Nikhef.

Divergence and convergence – the AUP Alignment Study



Origin	Policy Base Clause	Policy Summary	EGI	BBMRI	CTSC	EUDAT	ELIXIR	HBP	OSG Connect	Prace	Surf employees	RCUK

…ort any known or …h or loss or …s credentials. …hone number for …sible for backing	3		3
	3	Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3
	2	Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"	3
	0		0

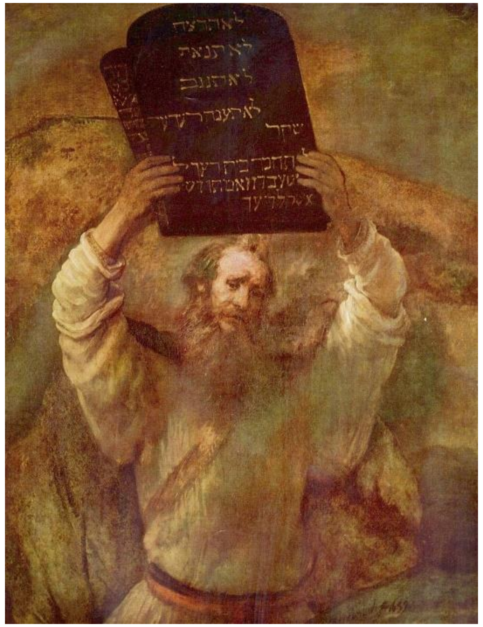
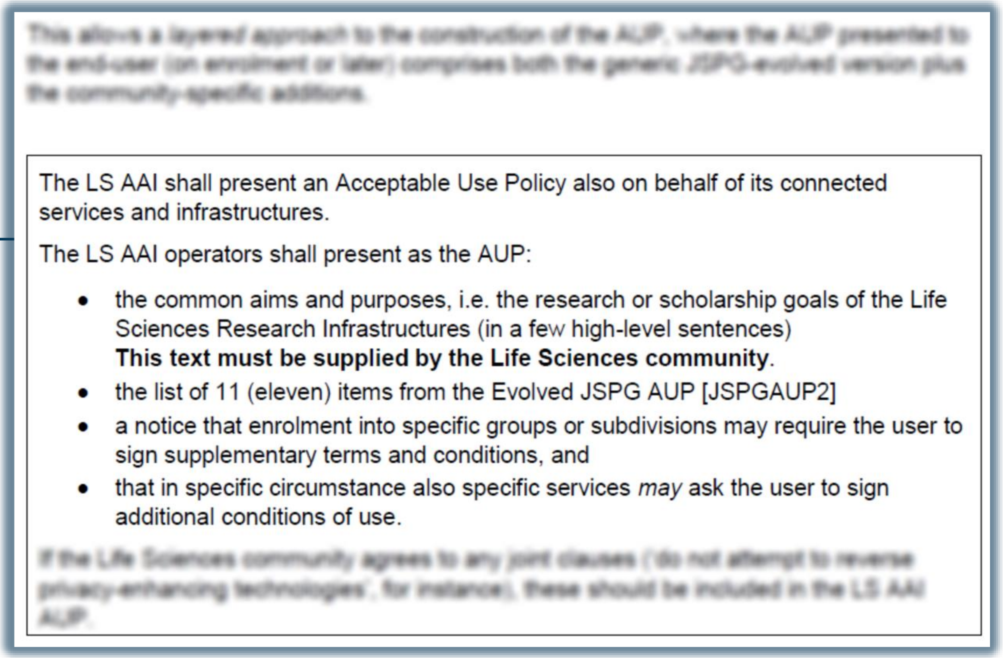


Image: Mozes en de tafelen der Wet, Rembrandt van Rijn, 1659

Scaling Acceptable Use Policy and data release

impractical to present user ‘click-through’ screens on each individual service



This allows a layered approach to the construction of the AUP, where the AUP presented to the end-user (on enrolment or later) comprises both the generic JSPG-evolved version plus the community-specific additions.

The LS AAI shall present an Acceptable Use Policy also on behalf of its connected services and infrastructures.

The LS AAI operators shall present as the AUP:

- the common aims and purposes, i.e. the research or scholarship goals of the Life Sciences Research Infrastructures (in a few high-level sentences)
  This text must be supplied by the Life Sciences community.
- the list of 11 (eleven) items from the Evolved JSPG AUP [JSPGAUP2]
- a notice that enrolment into specific groups or subdivisions may require the user to sign supplementary terms and conditions, and
- that in specific circumstance also specific services *may* ask the user to sign additional conditions of use.

If the Life Sciences community agrees to any joint clauses ('do not attempt to reverse privacy-enhancing technologies', for instance), these should be included in the LS AAI AUP.

Community conditions

Community specific terms & conditions

Community specific terms & conditions

RI Cluster-specific terms & conditions

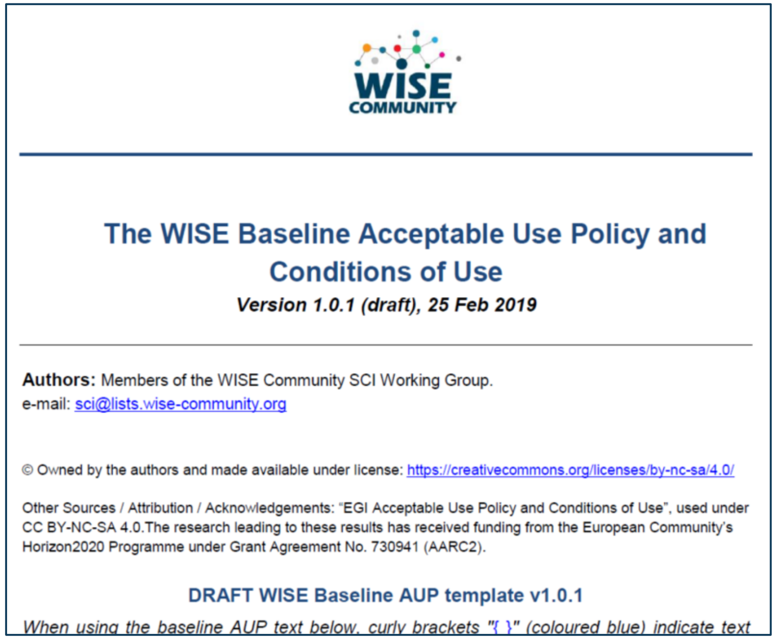
Common baseline AUP
for e-Infrastructures and Research Communities

WISE Baseline Acceptable Use Policy and Conditions of Use

Also picked up by e.g. SURF SCZ, eduTEAMS, CheckIn, Vorarlberg, …

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

Example – the WISE Baseline AUP *developed in WISE-SCI*



WISE COMMUNITY

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

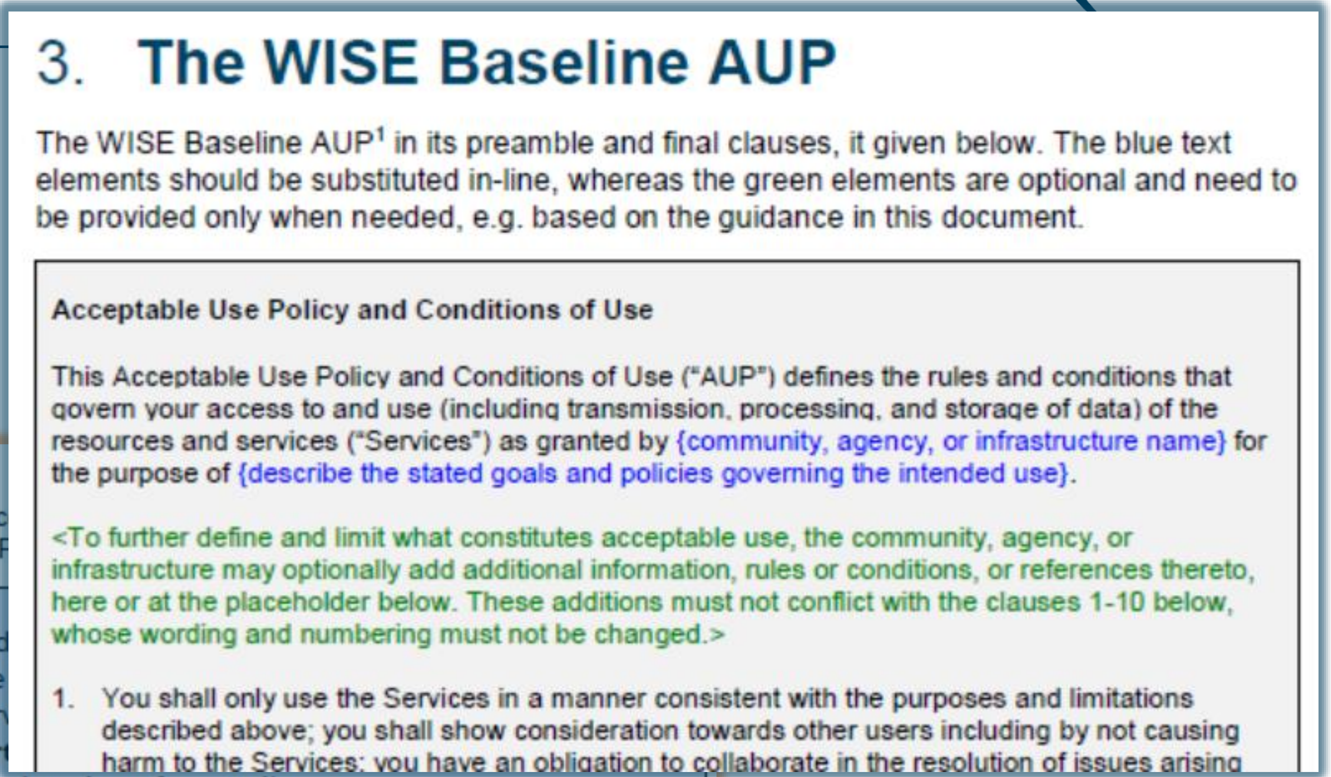
https://wiki.geant.org/display/WISE/Baseline+Acceptable+Use+Policy+and+Conditions+of+Use

WISE Baseline AUP – and how to apply it for your Infrastructure

AARC-I044

- Includes the final WISE Baseline AUP text
- for both ‘community-first’ and ‘user-first’ MMS services (attribute authorities)
- examples make it concrete

Quick take-up by e-Infras (both global and national)



3. The WISE Baseline AUP

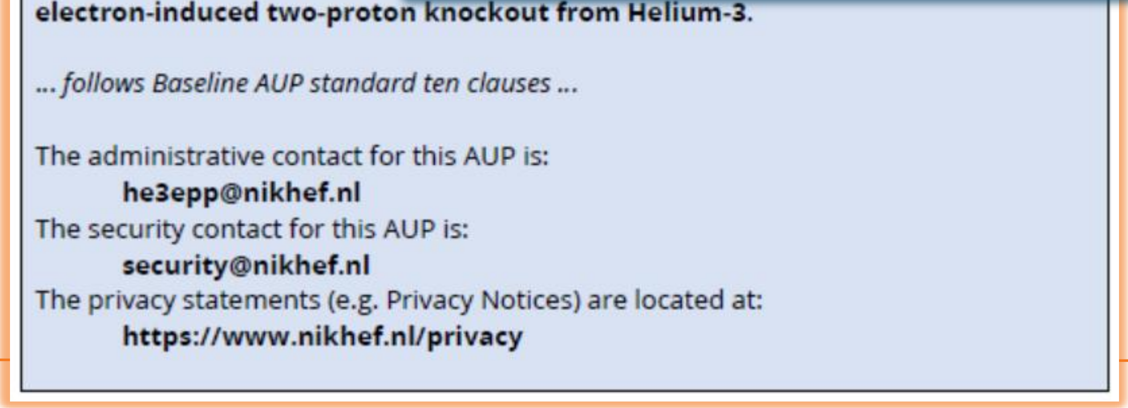
The WISE Baseline AUP[1] in its preamble and final clauses, it given below. The blue text elements should be substituted in-line, whereas the green elements are optional and need to be provided only when needed, e.g. based on the guidance in this document.

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use (“AUP”) defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services (“Services”) as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising



5.2. Example

The following example shows a c
the appropriate Acceptable Use F

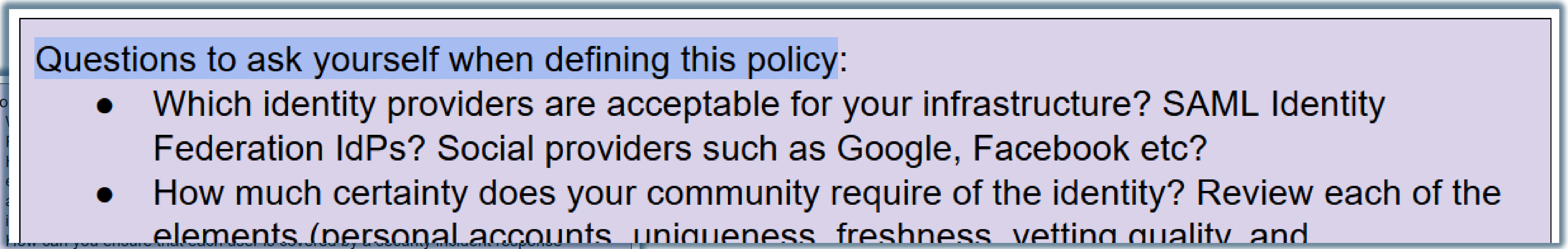
This Acceptable Use Policy and
govern your access to and use
data) of the resources and ser
the purpose of **studying short**
electron-induced two-proton knockout from Helium-3.

... follows Baseline AUP standard ten clauses ...

The administrative contact for this AUP is:
he3epp@nikhef.nl
The security contact for this AUP is:
security@nikhef.nl
The privacy statements (e.g. Privacy Notices) are located at:
https://www.nikhef.nl/privacy

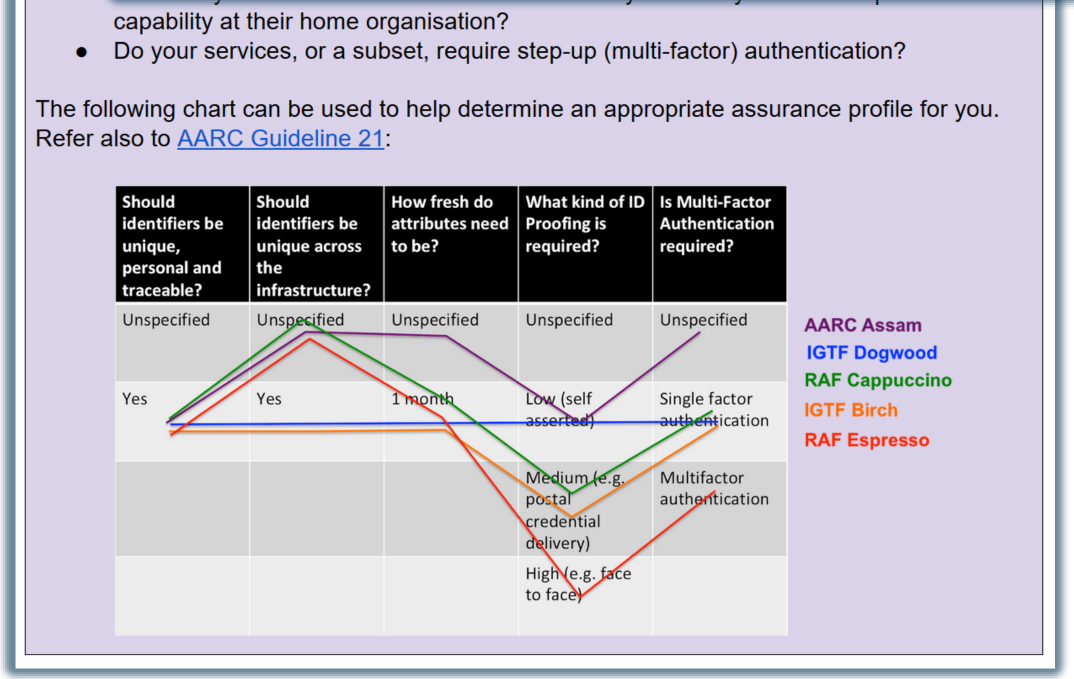
https://aarc-community.org/guidelines/aarc-i044/

Templates and guidance on how to implement



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



Questio

- 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)	

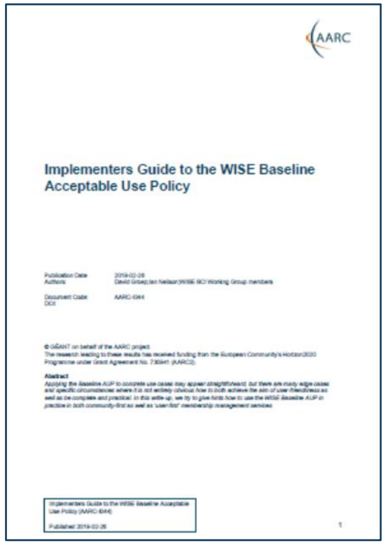
AARC Assam

IGTF Dogwood

RAF Cappuccino

IGTF Birch

RAF Espresso



Implementers Guide to the WISE Baseline Acceptable Use Policy

Publication Date 2019-02-28
Authors: David Groep; Ian Neilson; WISE SCI Working Group members

Document Code: AARC-I044
DOI:

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

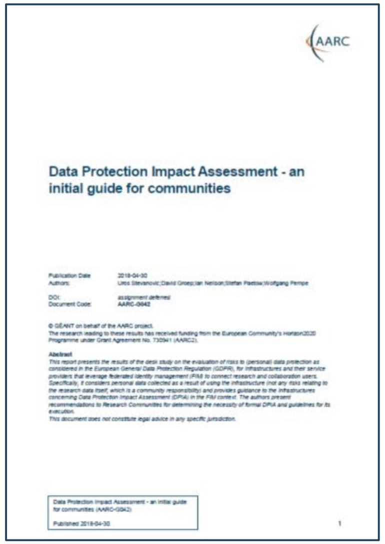
Abstract

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

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

Published 2019-02-28

1



Data Protection Impact Assessment - an initial guide for communities

Publication Date 2018-04-30
Authors: Uros Stevanovic; David Groep; Ian Neilson; Stefan Paetow; Wolfgang Pempe

DOI: assignment deferred
Document Code: AARC-G042

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

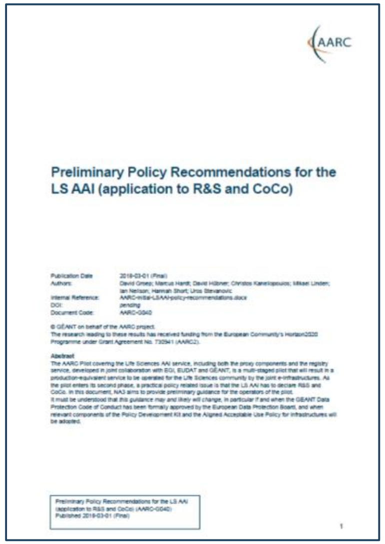
Abstract

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

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

Published 2018-04-30

1



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

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

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

Abstract

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

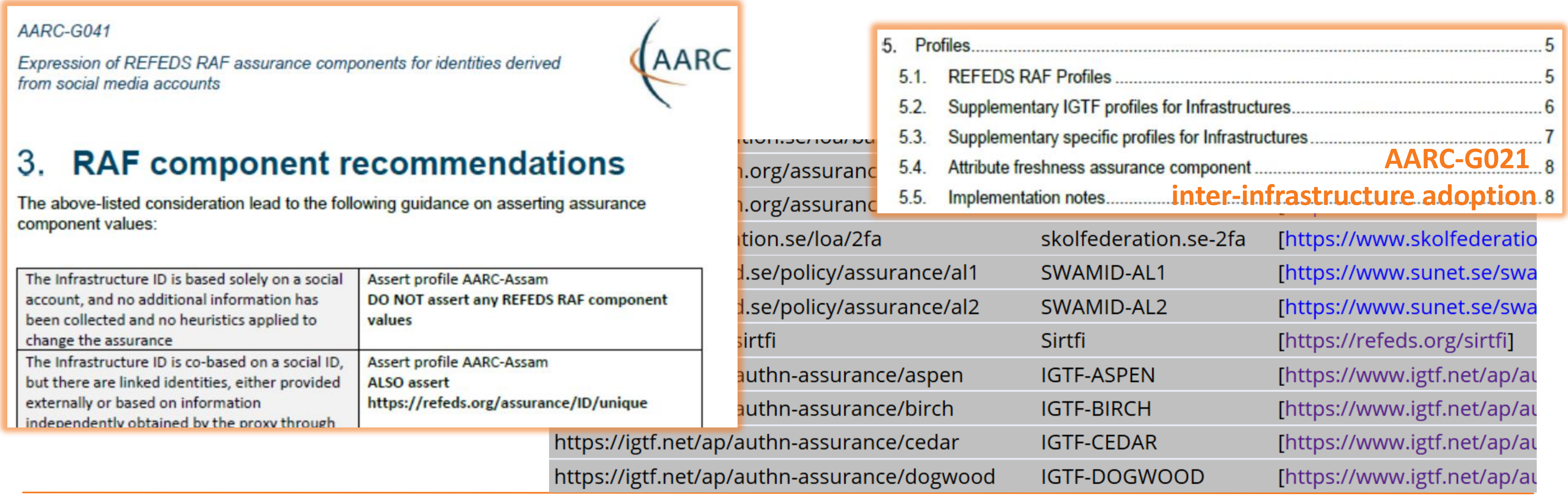
Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo) (AARC-G040)
Published 2018-03-01 (Final)

1

...

Assurance – standard profiles and 'untangling spaghetti'

- REFEDS RAF profiles (feasible assurance from all over R&E federations – as far as we can!)
- inter-infrastructure profiles and relying-party oriented profiles (IGTF BIRCH, DOGWOOD)
- how to express social media assurance, for citizen science and in support of account linking



AARC-G041

Expression of REFEDS RAF assurance components for identities derived from social media accounts

3. RAF component recommendations

The above-listed consideration lead to the following guidance on asserting assurance component values:

The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**

AARC-G021

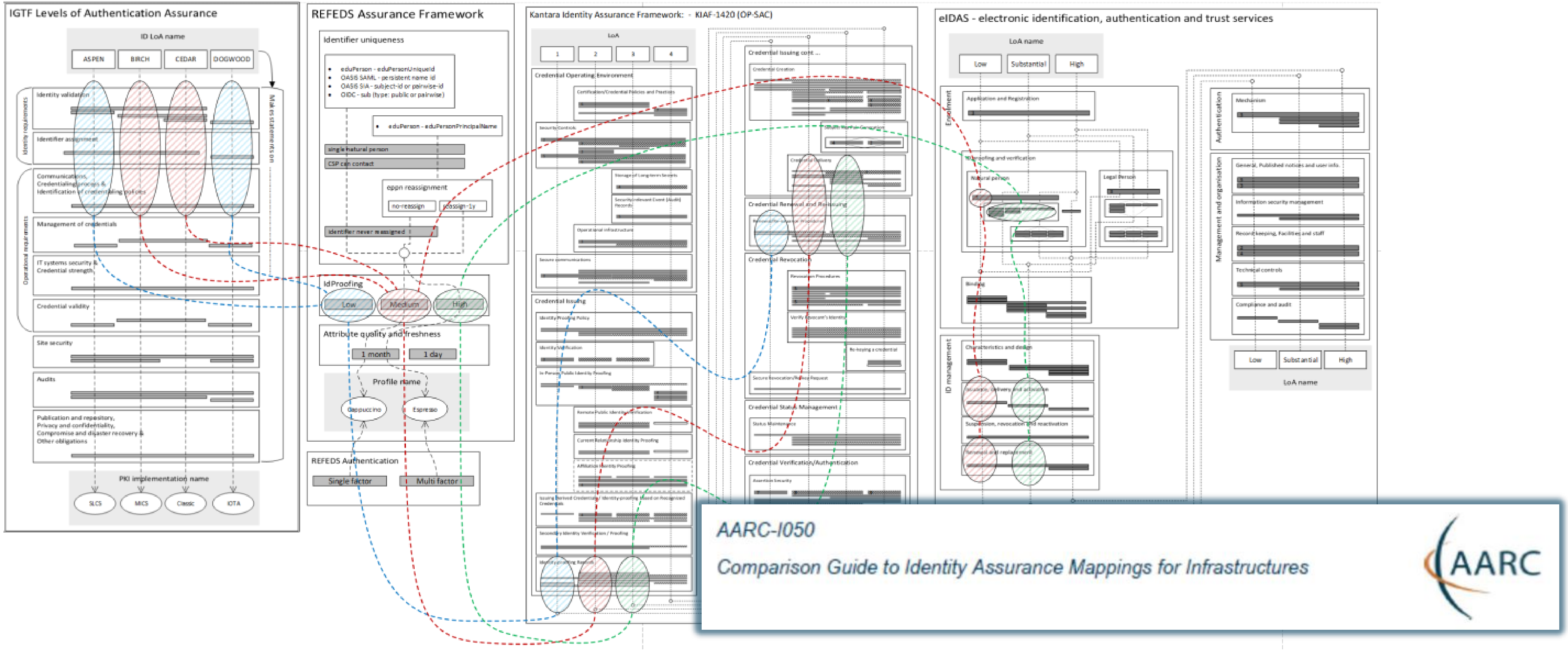
inter-infrastructure adoption

ıtion.se/loa/bu		
ı.org/assuranc		
ı.org/assuranc		
ıtion.se/loa/2fa	skolfederation.se-2fa	[https://www.skolfederatio
d.se/policy/assurance/al1	SWAMID-AL1	[https://www.sunet.se/swa
d.se/policy/assurance/al2	SWAMID-AL2	[https://www.sunet.se/swa
sirtfi	Sirtfi	[https://refeds.org/sirtfi]
authn-assurance/aspen	IGTF-ASPEN	[https://www.igtf.net/ap/au
authn-assurance/birch	IGTF-BIRCH	[https://www.igtf.net/ap/au
https://igtf.net/ap/authn-assurance/cedar	IGTF-CEDAR	[https://www.igtf.net/ap/au
https://igtf.net/ap/authn-assurance/dogwood	IGTF-DOGWOOD	[https://www.igtf.net/ap/au

https://www.iana.org/assignments/loa-profiles/

Untangling Assurance Spaghetti:
Comparison Guide to Identity Assurance Mappings for Infrastructures

Look forward to the ISGC2020 presentation on assurance to clarify this spaghetti!

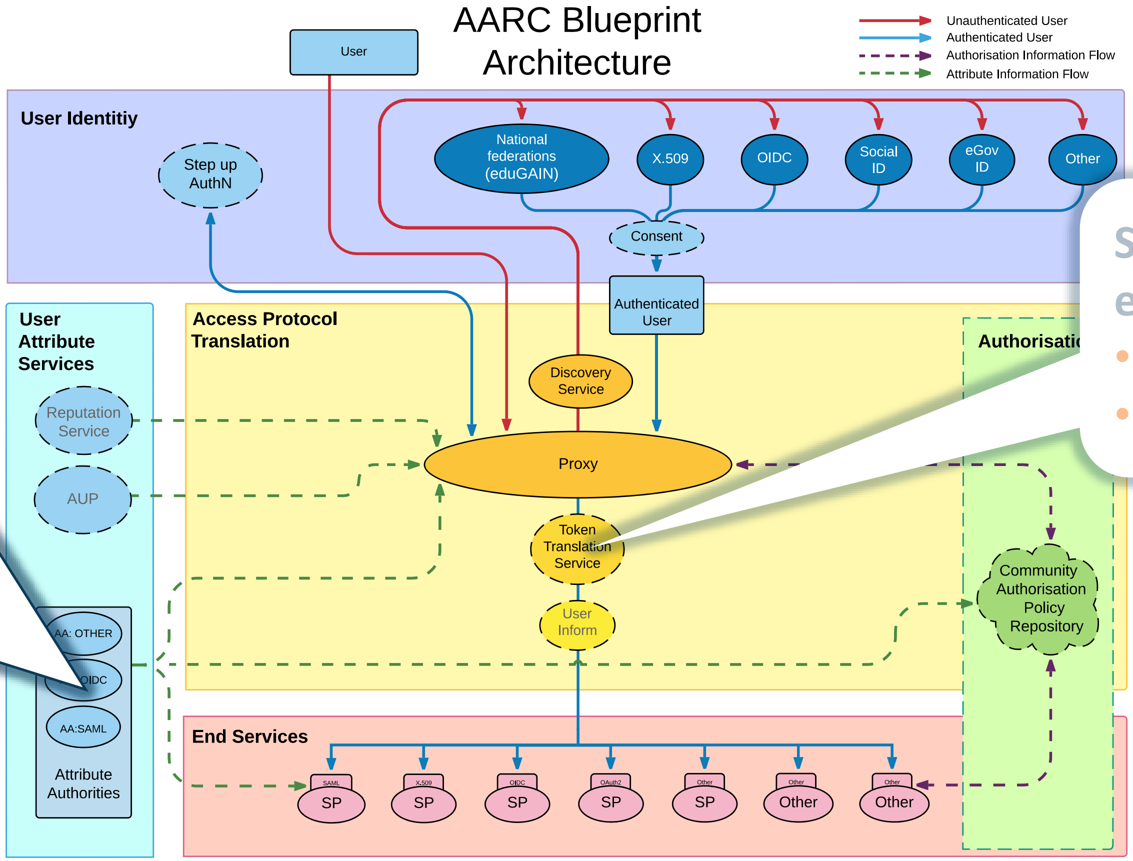

IGTF Levels of Authentication Assurance
ID LoA name
ASPEN
BIRCH
CEDAR
DOGWOOD
Identity validation
Identifier assignment
Communications, Credentialing process & Identification of credentialing policies
Management of credentials
IT systems security & Credential strength
Credential validity
Site security
Audits
Publication and repository, Privacy and confidentiality, Compromise and disaster recovery & Other obligations
Identity requirements
Operational requirements
Makes statements on
PKI implementation name
SLCS
MICS
Classic
IOTA
REFEDS Assurance Framework
Identifier uniqueness
eduPerson - eduPersonUniqueId
OASIS SAML - persistent name id
OASIS SIA - subject-id or pairwise-id
OIDC - sub (type: public or pairwise)
eduPerson - eduPersonPrincipalName
single natural person
CSP can contact
eppn reassignment
no-reassign
reassign-1y
identifier never re-assigned
IdProofing
Low
Medium
High
Attribute quality and freshness
1 month
1 day
Profile name
Cappuccino
Espresso
REFEDS Authentication
Single factor
Multi factor
Kantara Identity Assurance Framework: - KIAF-1420 (OP-SAC)
LoA
1
2
3
4
Credential Operating Environment
Credential Issuing
Credential Renewal and Re-issuing
Credential Revocation
Credential Status Management
Credential Verification/Authentication
eIDAS - electronic identification, authentication and trust services
LoA name
Low
Substantial
High
Enrolment
Application and Registration
ID proofing and verification
Natural person
Legal Person
Binding
ID management
Characteristics and design
Issuance, delivery and activation
Suspension, revocation and reactivation
Renewal and replacement
Authentication
Mechanism
Management and organisation
General, Published notices and user info.
Information security management
Record keeping, Facilities and staff
Technical controls
Compliance and audit

AARC-I050

Comparison Guide to Identity Assurance Mappings for Infrastructures

https://aarc-project.eu/guidelines/aarc-i050/

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

Store and manage ephemeral user credentials

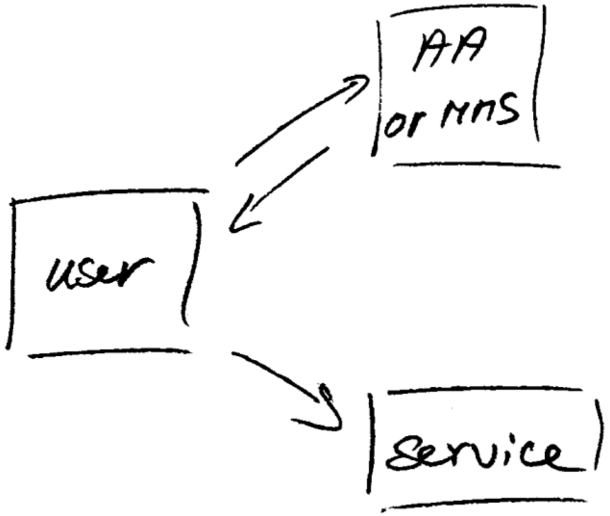
- trusted credential stores
- protection at rest

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

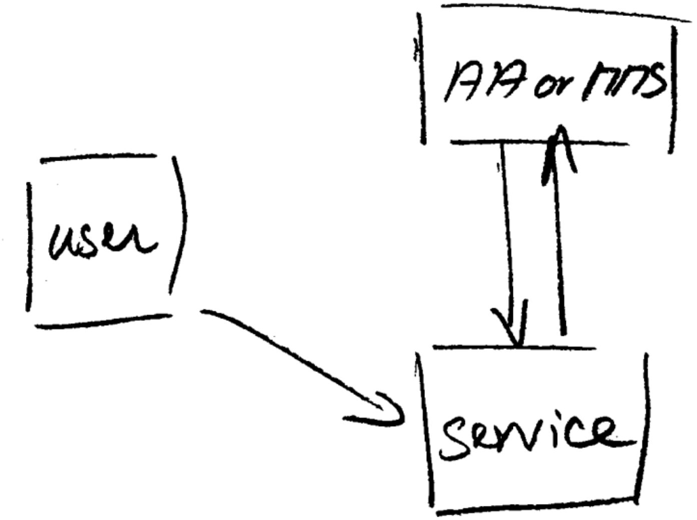
Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements *(**AARC-I048**, in collaboration with IGTF AAOPS)*

Protecting the community membership data and its proxy

- Intentionally targeted broader than just BPA-style communities, since operational security spans data centres and infrastructures using other forms of AA membership management
- PRACE: ‘pull model’ directory-based communities
- BPA: encourages ‘push model’ attribute-carrying service requests



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



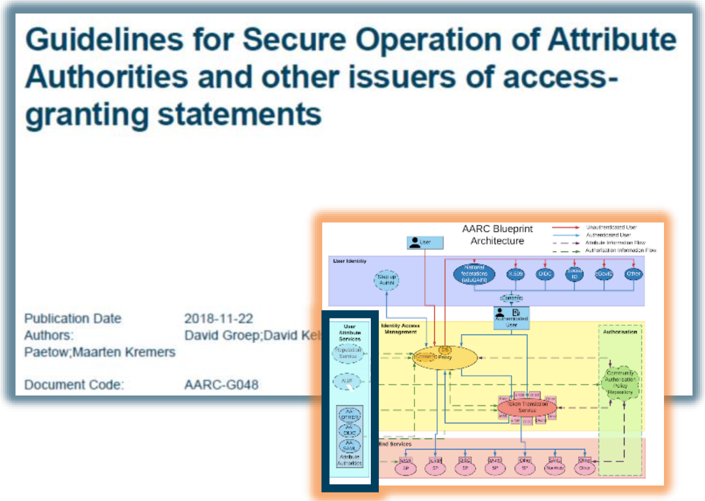
pull model – common when using directories
(e.g. LDAP in PRACE, GUMS in OSG)

push and pull model diagrams as per RFC2904 – the 3rd (agent) model is uncommon in research/collaboration scenarios except for provisioning

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

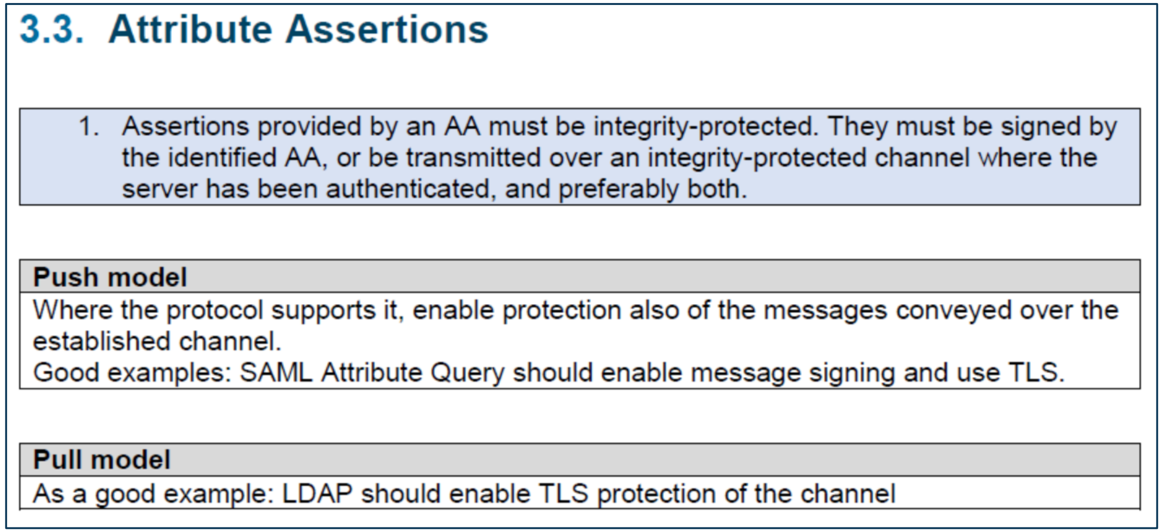
Structured around concept of "**AA Operators**",
operating "**Attribute Authorities**" (technological entities),
on behalf of, one or more, **Communities**



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

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

Document Code: AARC-G048

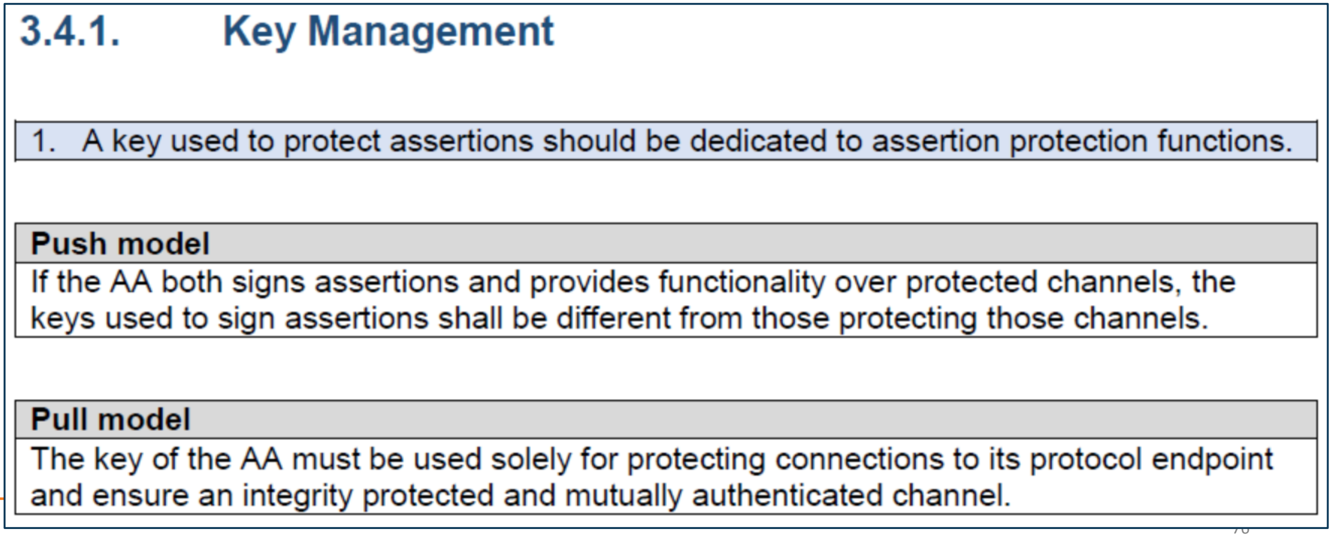


3.3. Attribute Assertions

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

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

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



3.4.1. Key Management

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

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

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

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

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

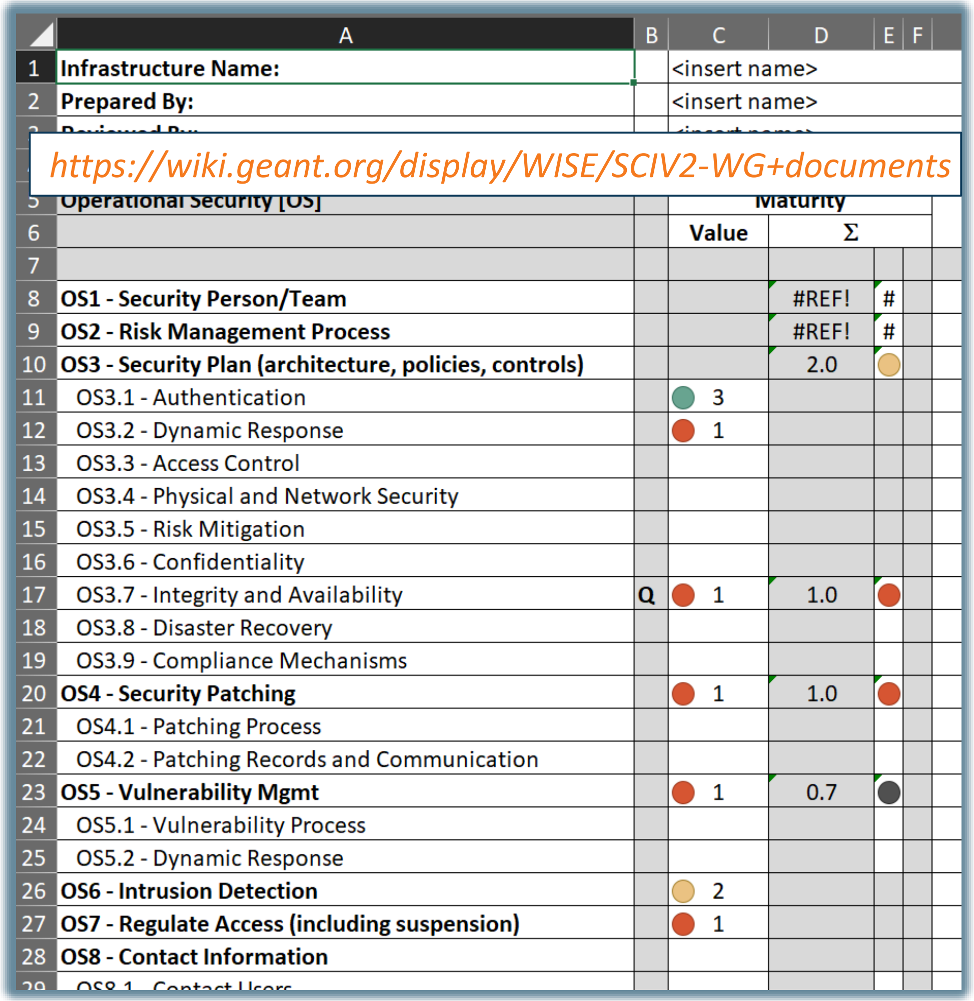
SCIv2 assessment and peer review – do you want to work with your peer?

SCIv2 proposed assessment model

Level 0: *Not implemented for critical services;*
Level 1: *Implemented for all critical services, but not documented;*
Level 2: *Implemented and documented for all critical services;*
Level 3: *Implemented, documented & reviewed by a collaborating Infrastructure or by an independent external body;*
"Justifiable exclusion": *feature not relevant for infrastructure.*

Conclusions

- self-assessment feasible, SCI model emphasises proper elements for *federated* access
- peer-review extends trust across similar organisations
- transparency needed:
  infrastructures weigh sub-elements differently!
  (no global consensus yet on any weighting method …)

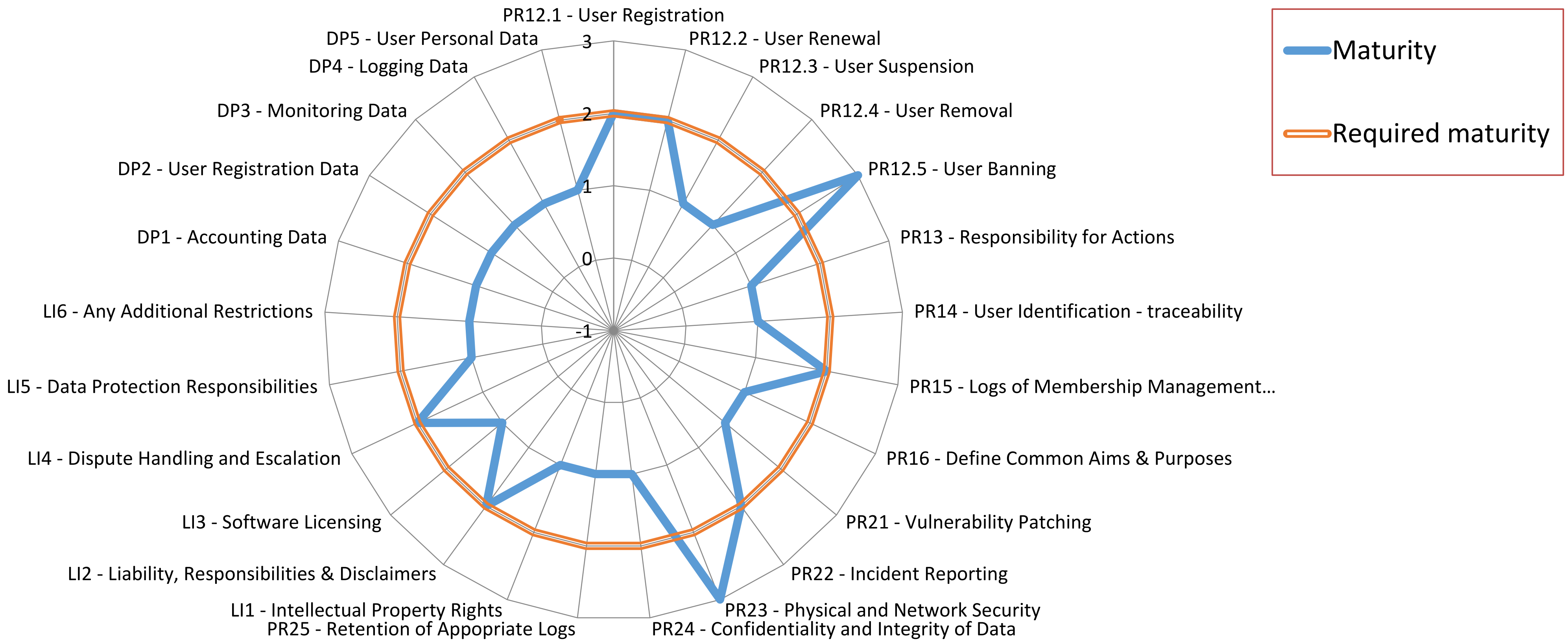


	A	B	C	D	E	F
1	**Infrastructure Name:**		<insert name>			
2	**Prepared By:**		<insert name>			
3	**Reviewed By:**		<insert name>			
5	**Operational Security [OS]**		**Maturity**			
6			**Value**	Σ		
7						
8	**OS1 - Security Person/Team**			#REF!	#	
9	**OS2 - Risk Management Process**			#REF!	#	
10	**OS3 - Security Plan (architecture, policies, controls)**			2.0	●	
11	OS3.1 - Authentication		● 3			
12	OS3.2 - Dynamic Response		● 1			
13	OS3.3 - Access Control					
14	OS3.4 - Physical and Network Security					
15	OS3.5 - Risk Mitigation					
16	OS3.6 - Confidentiality					
17	OS3.7 - Integrity and Availability	**Q**	● 1	1.0	●	
18	OS3.8 - Disaster Recovery					
19	OS3.9 - Compliance Mechanisms					
20	**OS4 - Security Patching**		● 1	1.0	●	
21	OS4.1 - Patching Process					
22	OS4.2 - Patching Records and Communication					
23	**OS5 - Vulnerability Mgmt**		● 1	0.7	●	
24	OS5.1 - Vulnerability Process					
25	OS5.2 - Dynamic Response					
26	**OS6 - Intrusion Detection**		● 2			
27	**OS7 - Regulate Access (including suspension)**		● 1			
28	**OS8 - Contact Information**					
29	OS8.1 - Contact Users					

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

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

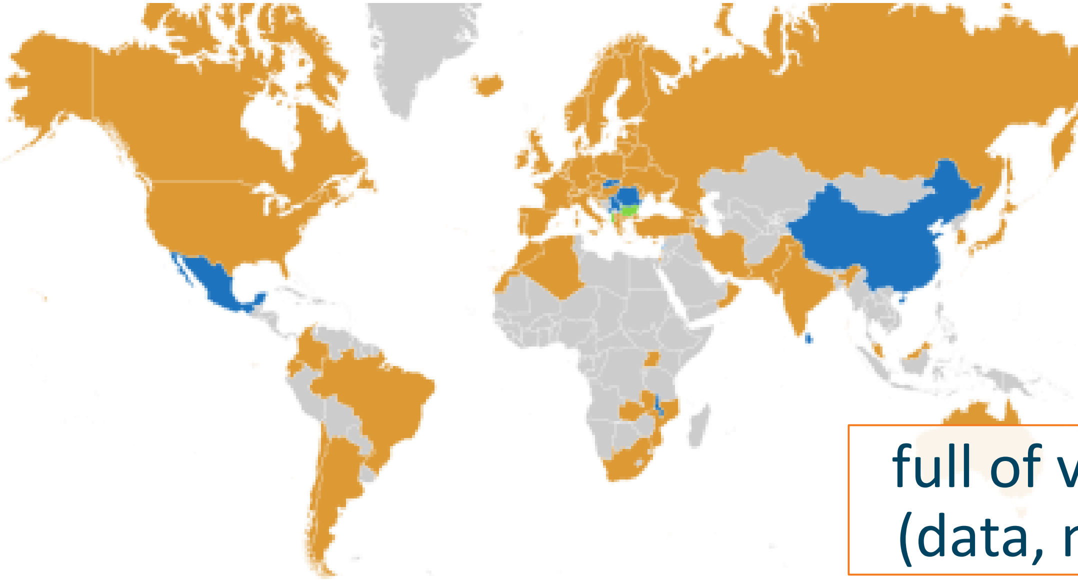
Determining interoperable risk profiles for collaborating infrastructures and services

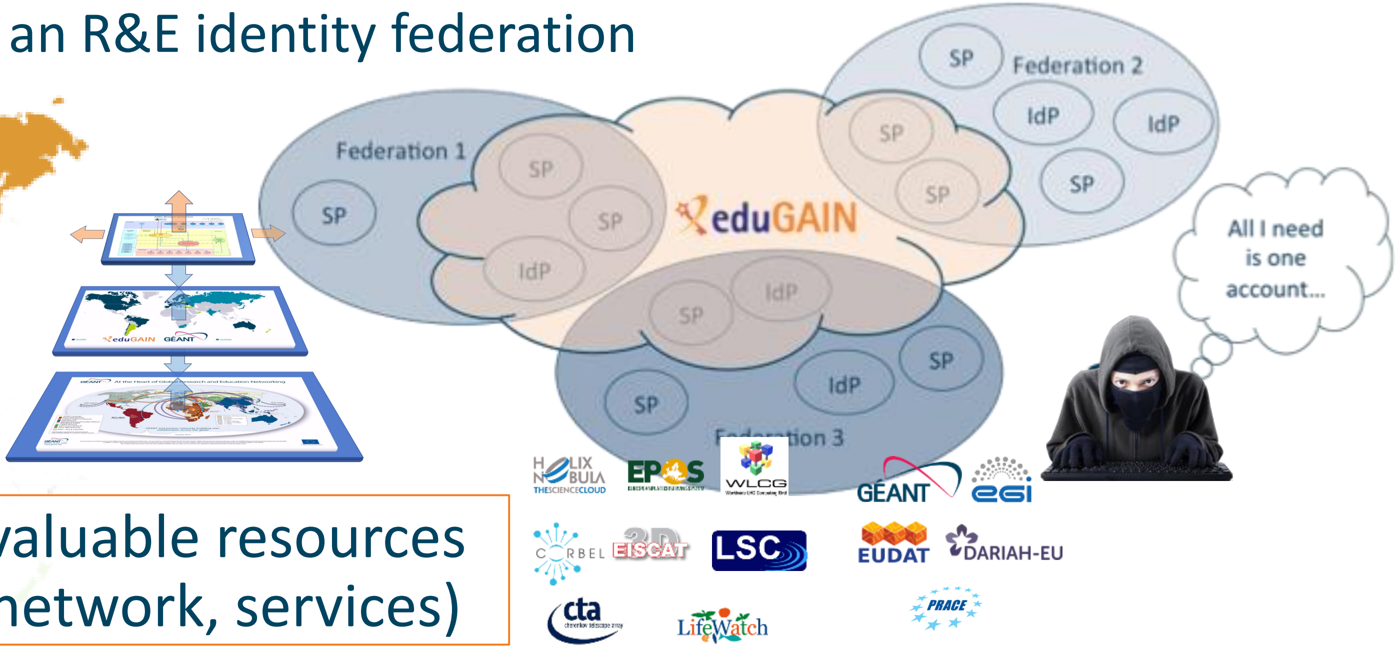


concept in SCI context: Urpo Kaila

Security Incident Response in the Federated World

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





full of valuable resources (data, network, services)

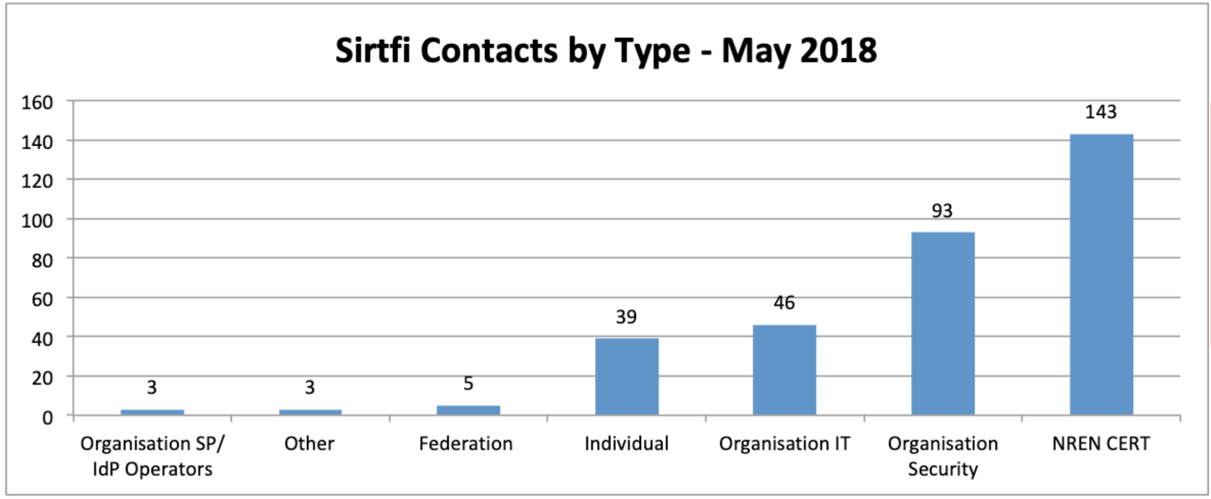
Could we ensure that information is shared confidentially, and reputations protected?

Security Incident Response Trust Framework for Federated Identity

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

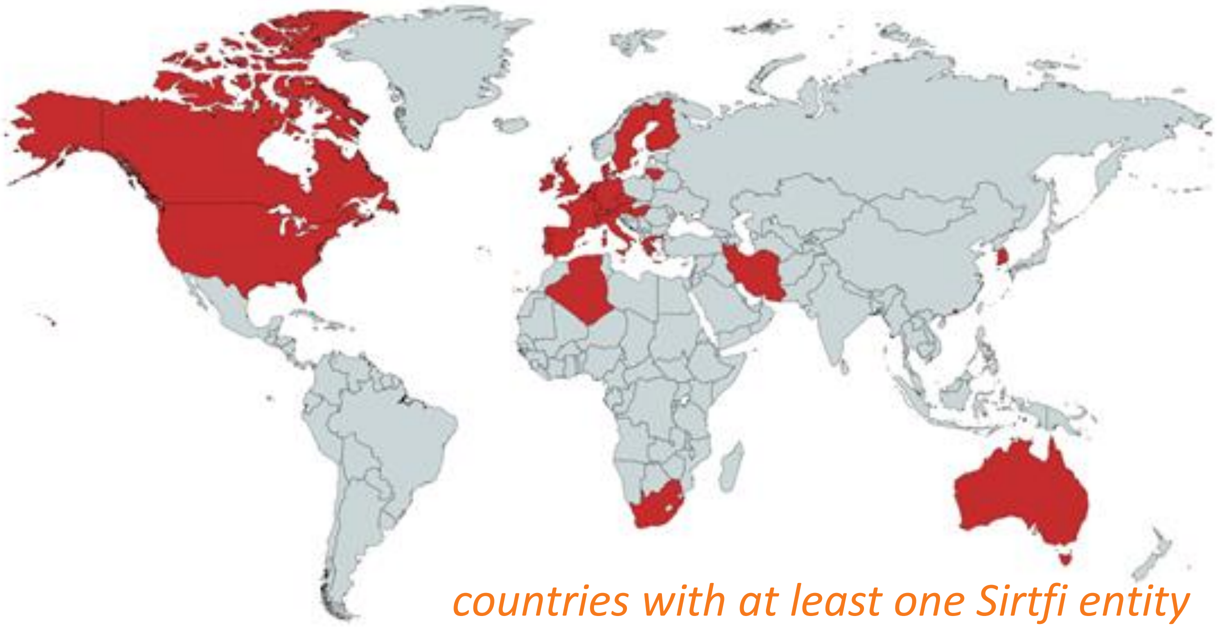
Sirtfi is there today – 575 parties (420 IdPs) joined, in 28 federations

SIRTFI
Security Incident Response Trust Framework for Federated Identity

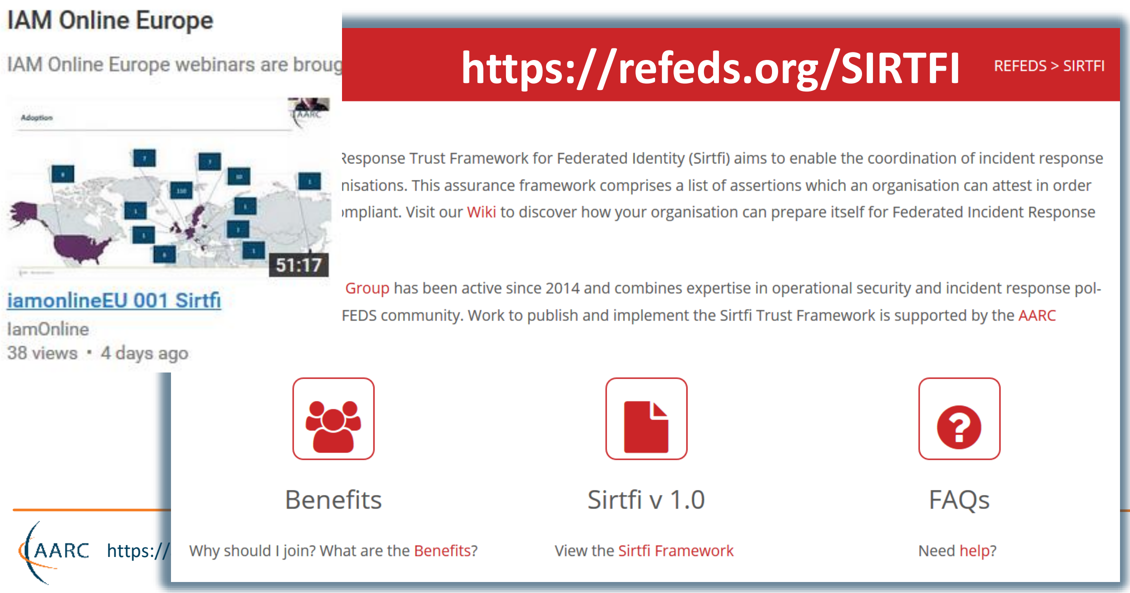


Incident Response

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



countries with at least one Sirtfi entity



IAM Online Europe

IAM Online Europe webinars are broug

iamonlineEU 001 Sirtfi

IamOnline

38 views • 4 days ago

https://refeds.org/SIRTFI

REFEDS > SIRTFI

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

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

Benefits

Why should I join? What are the Benefits?

Sirtfi v 1.0

View the Sirtfi Framework

FAQs

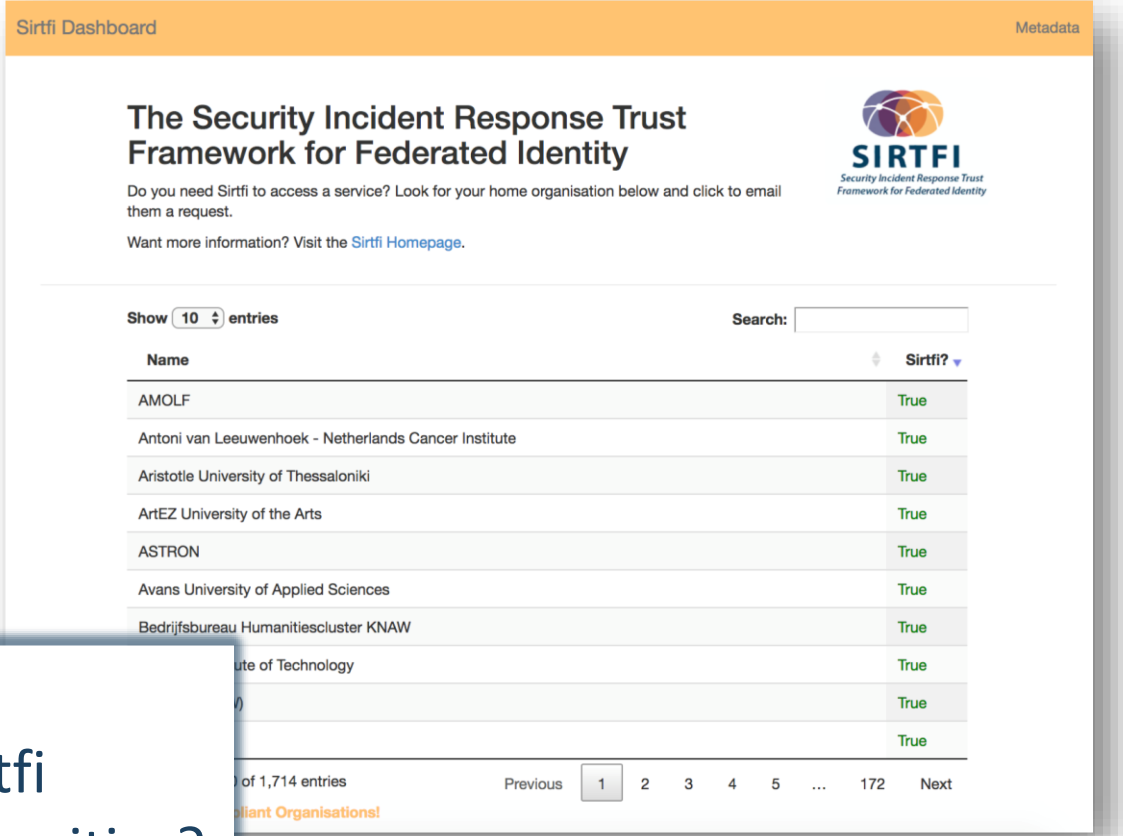
Need help?

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

The sociology of checking Sirtfi enablement …

Sirtfi ‘encouragement’

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



Sirtfi Dashboard

The Security Incident Response Trust Framework for Federated Identity

SIRTFI
Security Incident Response Trust Framework for Federated Identity

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

Want more information? Visit the Sirtfi Homepage.

Show 10 entries

Search:

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

) of 1,714 entries

pliant Organisations!

Sirtfi+ registry

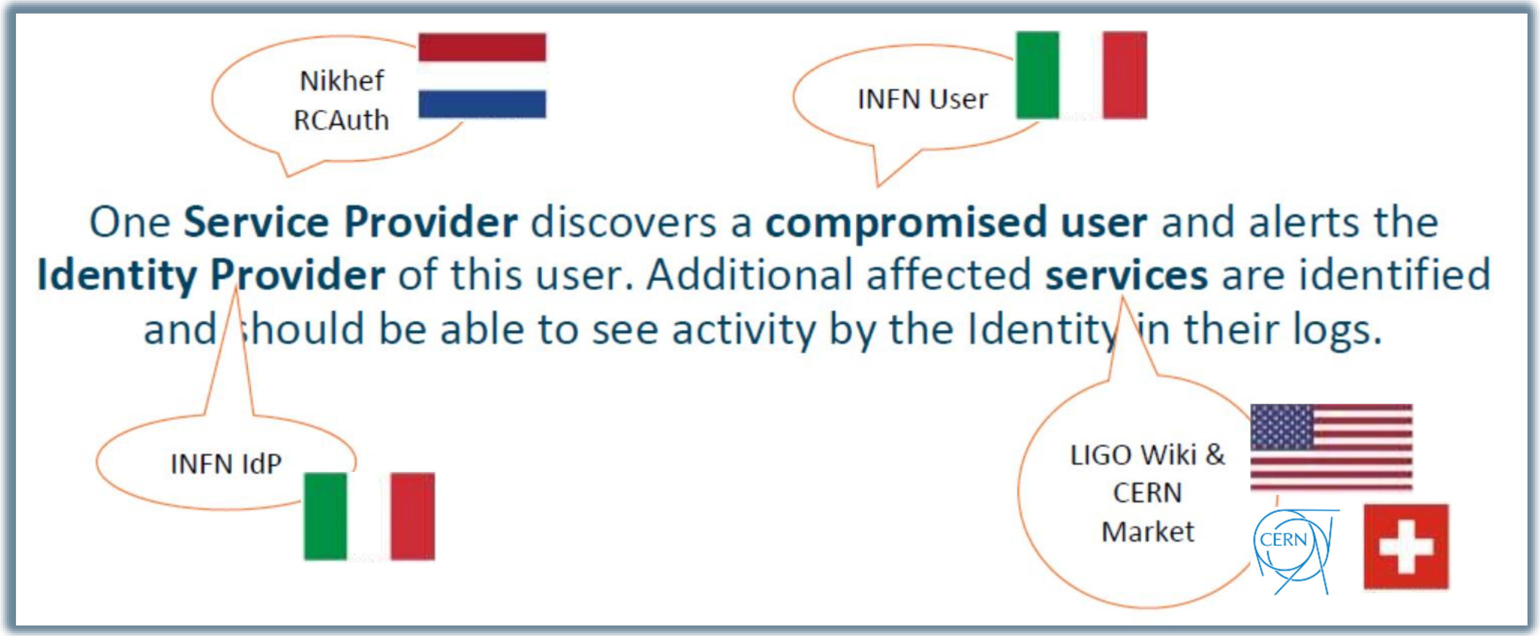
- enabling more entities to express Sirtfi
- sharing implicit trust between communities?
- tool requirement

http://sirtfi.cern.ch/

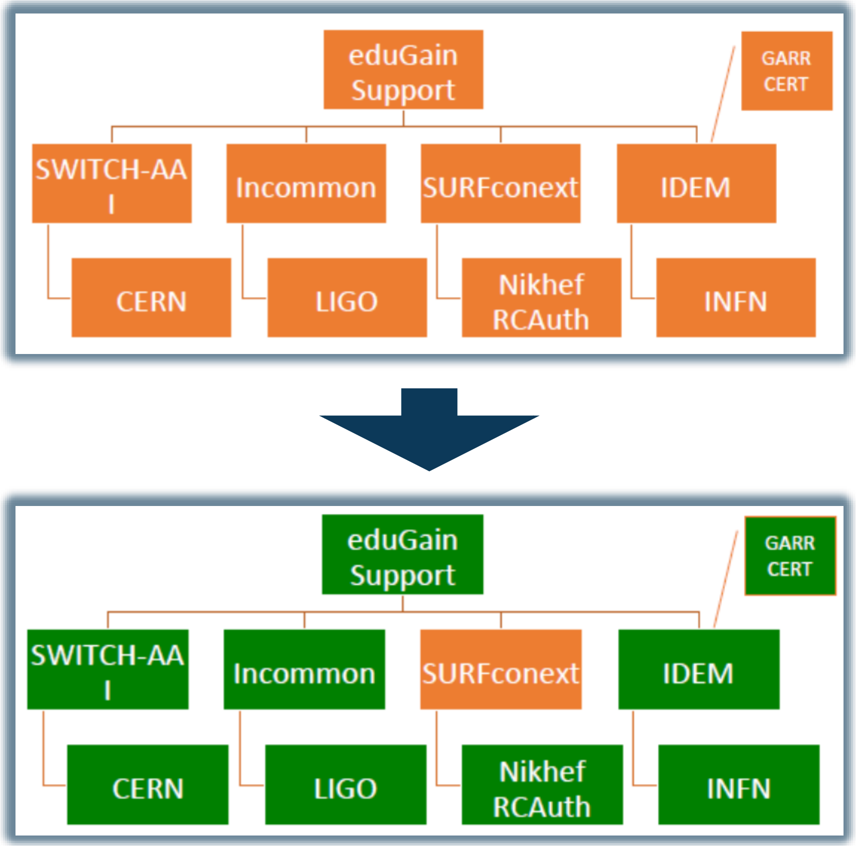
graphics source: Hannah Short, CERN

Testing incident response coordination

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



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

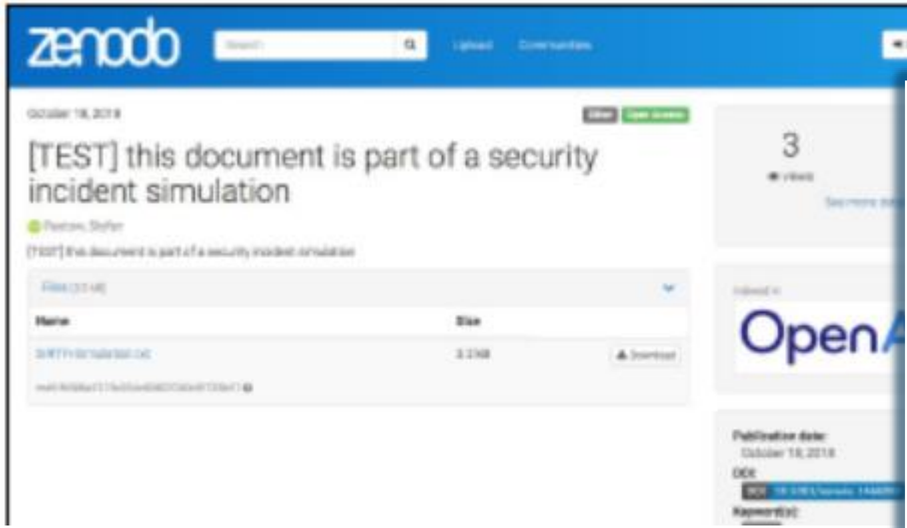


parties involved in response challenge

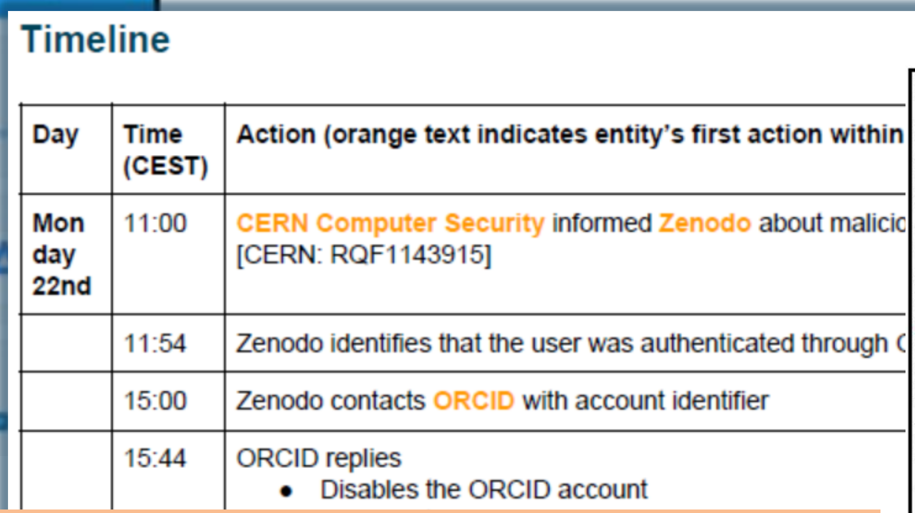
Report-outs see **https://wiki.geant.org/display/AARC/Sirtfi+Communications+Challenges%2C+AARC2-TNA3.1**

2nd challenge, December 2018: using the draft response templates

Malicious content hosted on Zenodo, uploaded with an ORCID account

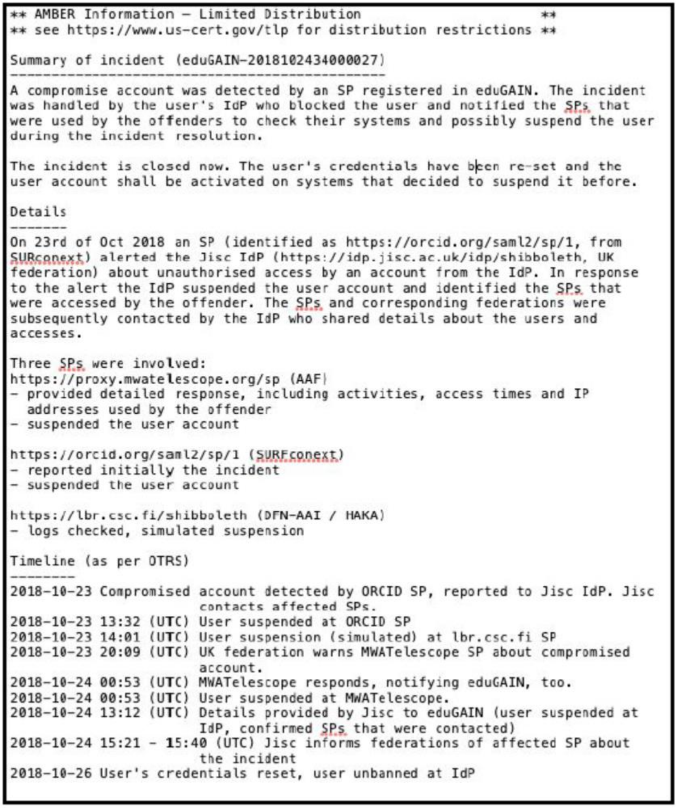


[TEST] this document is part of a security incident simulation



Timeline

Day	Time (CEST)	Action (orange text indicates entity's first action within
Mon day 22nd	11:00	CERN Computer Security informed Zenodo about malicio [CERN: RQF1143915]
	11:54	Zenodo identifies that the user was authenticated through O
	15:00	Zenodo contacts ORCID with account identifier
	15:44	ORCID replies ● Disables the ORCID account



```
** AMBER Information – Limited Distribution                    **
** see https://www.us-cert.gov/tlp for distribution restrictions **

Summary of incident (eduGAIN-201810243400027)
----------------------------------------------
A compromise account was detected by an SP registered in eduGAIN. The incident
was handled by the user's IdP who blocked the user and notified the SPs that
were used by the offenders to check their systems and possibly suspend the user
during the incident resolution.

The incident is closed now. The user's credentials have been re-set and the
user account shall be activated on systems that decided to suspend it before.

Details
--------
On 23rd of Oct 2018 an SP (identified as https://orcid.org/saml2/sp/1, from
SURconext) alerted the Jisc IdP (https://idp.jisc.ac.uk/idp/shibboleth, UK
federation) about unauthorised access by an account from the IdP. In response
to the alert the IdP suspended the user account and identified the SPs that
were accessed by the offender. The SPs and corresponding federations were
subsequently contacted by the IdP who shared details about the users and
accesses.

Three SPs were involved:
https://proxy.mwatelescope.org/sp (AAF)
- provided detailed response, including activities, access times and IP
  addresses used by the offender
- suspended the user account

https://orcid.org/saml2/sp/1 (SURFconext)
- reported initially the incident
- suspended the user account

https://lbr.csc.fi/shibboleth (DFN-AAI / HAKA)
- logs checked, simulated suspension

Timeline (as per OTRS)
---------
2018-10-23 Compromised account detected by ORCID SP, reported to Jisc IdP. Jisc
                       contacts affected SPs.
2018-10-23 13:32 (UTC) User suspended at ORCID SP
2018-10-23 14:01 (UTC) User suspension (simulated) at lbr.csc.fi SP
2018-10-23 20:09 (UTC) UK federation warns MWATelescope SP about compromised
                       account.
2018-10-24 00:53 (UTC) MWATelescope responds, notifying eduGAIN, too.
2018-10-24 00:53 (UTC) User suspended at MWATelescope.
2018-10-24 13:12 (UTC) Details provided by Jisc to eduGAIN (user suspended at
                       IdP, confirmed SPs that were contacted)
2018-10-24 15:21 - 15:40 (UTC) Jisc informs federations of affected SP about
                       the incident
2018-10-26 User's credentials reset, user unbanned at IdP
```

- time delay between 'malicious act' and request for investigation (+3 days)
- spread over all time zones (.au, .ch, .nl, .uk, .us,
- new set of participant IdPs and federations
- initial mitigation within 4 hrs, but eduGAIN support desk gets it only on the 3rd day …
- contact with affected user effective and appreciated
- TLP classification not used throughout, some entities initially missed

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

Preparing the ground for REFEDS Sirtfi procedures: AARC-I051

Acknowledging that only reviewers read deliverables, response process from DNA3.2 issued as …

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

Be Prepared

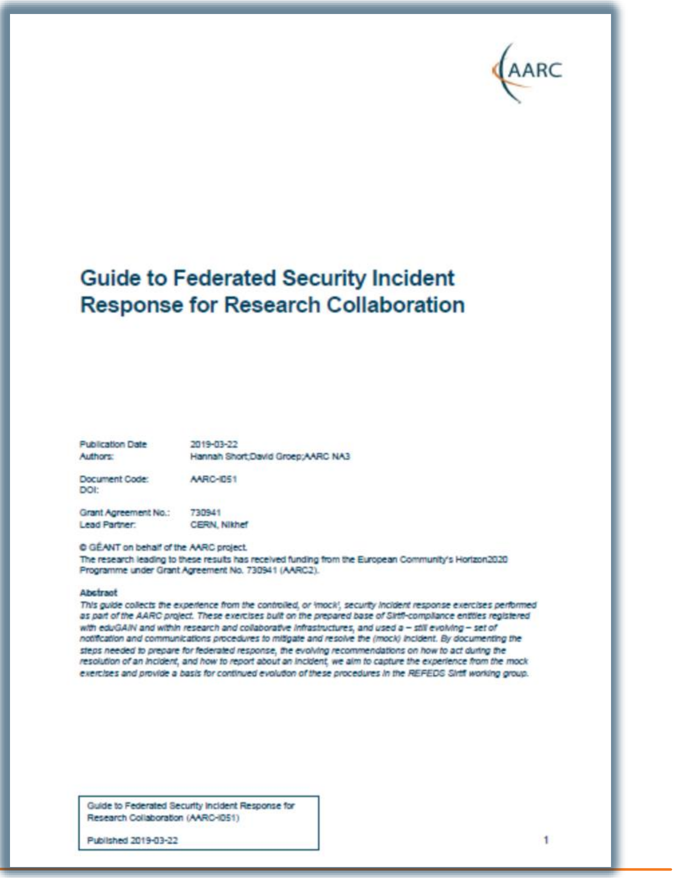
- Federated Entities Should Support Sirtfi
- Community Proxies Should Adopt Interoperable Policies & Procedures
- Federations and Interfederations Should Adopt Common Procedures
- Leverage Templated Emails
- Establish Secure Communication Channels in Advance

Act

- Scope
- Goals
- Responsibilities
- **Procedures**: for IdPs & SPs, for coordinators, for eduGAIN

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!



AARC

Guide to Federated Security Incident Response for Research Collaboration

Publication Date	2019-03-22
Authors:	Hannah Short;David Groep;AARC NA3
Document Code:	AARC-I051
DOI:	
Grant Agreement No.:	730941
Lead Partner:	CERN, Nikhef

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

Abstract

This guide collects the experience from the controlled, or 'mock', security incident response exercises performed as part of the AARC project. These exercises built on the prepared base of Sirtfi-compliance entities registered with eduGAIN and within research and collaborative infrastructures, and used a – still evolving – set of notification and communications procedures to mitigate and resolve the (mock) incident. By documenting the steps needed to prepare for federated response, the evolving recommendations on how to act during the resolution of an incident, and how to report about an incident, we aim to capture the experience from the mock exercises and provide a basis for continued evolution of these procedures in the REFEDS Sirtfi working group.

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

Published 2019-03-22

1

https://aarc-project.eu/guidelines/aarc-i051/

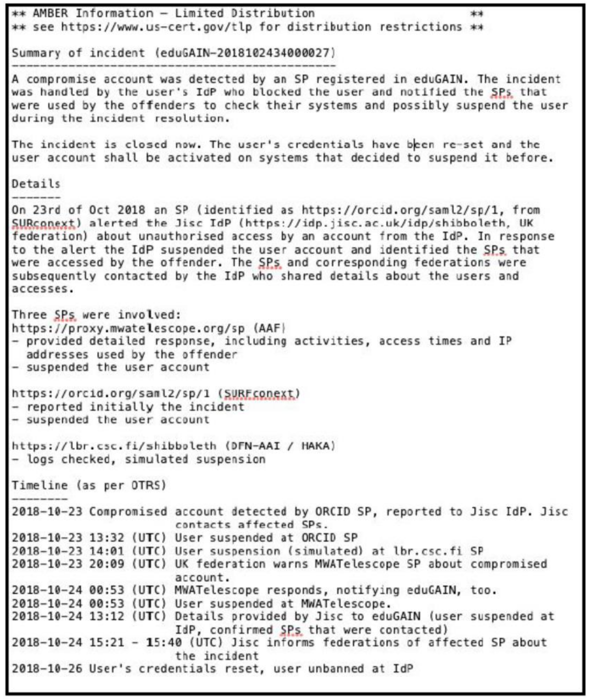
Example of WISE coordination – evolving the *Sirtfi* challenges

The first Sirtfi challenges were run ‘by AARC’ to establish the guidelines

But: many ‘logical’ candidates that could all run the test

… and all have an interest in knowing the result so to establish trust!

- eduGAIN
- GEANT.org
- any EOSC-HUB and e-Infrastructure CSIRT teams
- the IGTF (as it leverages federated identity in RCauth, TCS, CILogon)
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, OSG, HPCI, …
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, …



```
** AMBER Information - Limited Distribution                **
** see https://www.us-cert.gov/tlp for distribution restrictions **

Summary of incident (eduGAIN-2018102434000027)
----------------------------------------------
A compromise account was detected by an SP registered in eduGAIN. The incident
was handled by the user's IdP who blocked the user and notified the SPs that
were used by the offenders to check their systems and possibly suspend the user
during the incident resolution.

The incident is closed now. The user's credentials have been re-set and the
user account shall be activated on systems that decided to suspend it before.

Details
-------
On 23rd of Oct 2018 an SP (identified as https://orcid.org/saml2/sp/1, from
SURconext) alerted the Jisc IdP (https://idp.jisc.ac.uk/idp/shibboleth, UK
federation) about unauthorised access by an account from the IdP. In response
to the alert the IdP suspended the user account and identified the SPs that
were accessed by the offender. The SPs and corresponding federations were
subsequently contacted by the IdP who shared details about the users and
accesses.

Three SPs were involved:
https://proxy.mwatelescope.org/sp (AAF)
- provided detailed response, including activities, access times and IP
  addresses used by the offender
- suspended the user account

https://orcid.org/saml2/sp/1 (SURFconext)
- reported initially the incident
- suspended the user account

https://lbr.csc.fi/shibboleth (DFN-AAI / HAKA)
- logs checked, simulated suspension

Timeline (as per OTRS)
--------
2018-10-23 Compromised account detected by ORCID SP, reported to Jisc IdP. Jisc
                      contacts affected SPs.
2018-10-23 13:32 (UTC) User suspended at ORCID SP
2018-10-23 14:01 (UTC) User suspension (simulated) at lbr.csc.fi SP
2018-10-23 20:09 (UTC) UK federation warns MWATelescope SP about compromised
                      account.
2018-10-24 00:53 (UTC) MWATelescope responds, notifying eduGAIN, too.
2018-10-24 00:53 (UTC) User suspended at MWATelescope.
2018-10-24 13:12 (UTC) Details provided by Jisc to eduGAIN (user suspended at
                      IdP, confirmed SPs that were contacted)
2018-10-24 15:21 - 15:40 (UTC) Jisc informs federations of affected SP about
                      the incident
2018-10-26 User's credentials reset, user unbanned at IdP
```

and any institution (or person) with access to https://mds.edugain.org/ can run them, of course!

‘so in a short while, all the email in the world will be on Sirtfi Incident Response tests??’

Challenge elements – what is valued or expected might differ …

A single test and challenge can answer one **or more** of these questions

timeliness

ability to take action

confidentiality

investigative capability

- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

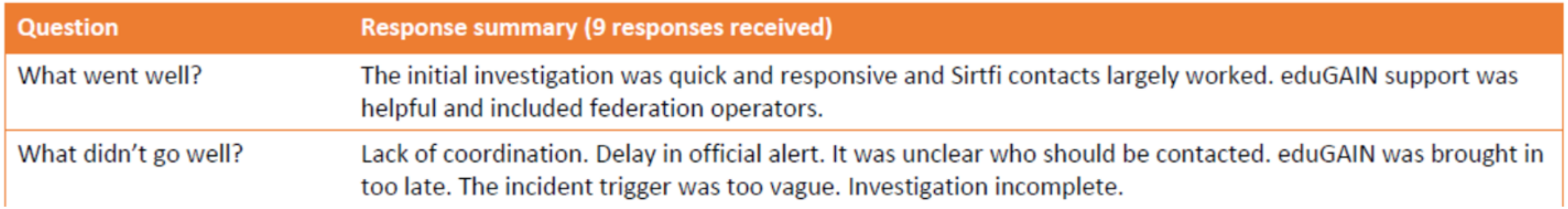
Communications challenges build ‘confidence’ and trust – an important social aspect!

- different tests bring complementary results: responsiveness vs. ability act , or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging …

Communications Challenges

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

testing communications channels identified as high-priority target

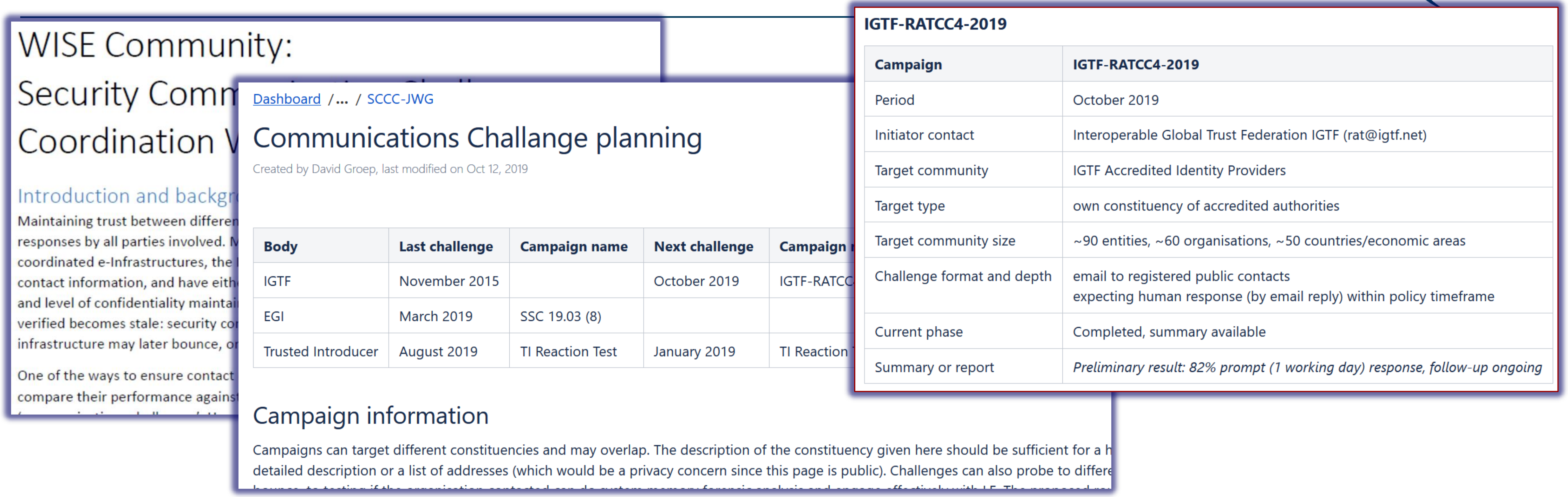


Question	Response summary (9 responses received)
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn't go well?	Lack of coordination. Delay in official alert. It was unclear who 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 W

Introduction and backgr

Maintaining trust between differen
responses by all parties involved. M
coordinated e-Infrastructures, the I
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 against

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

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://wise-community.org/sccc/

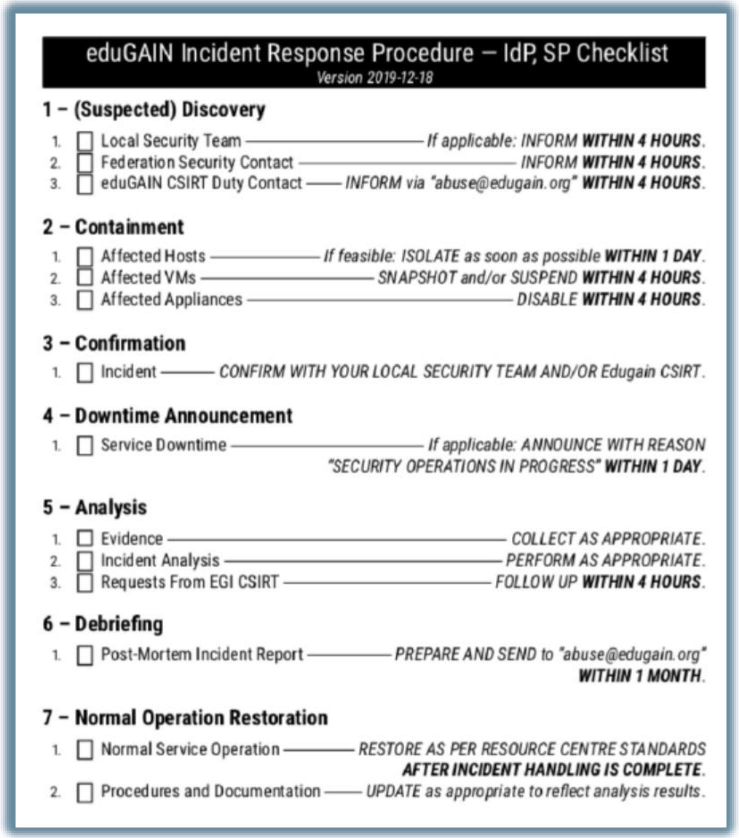
Evolving incident response: from I051 to eduGAIN Security

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**.*

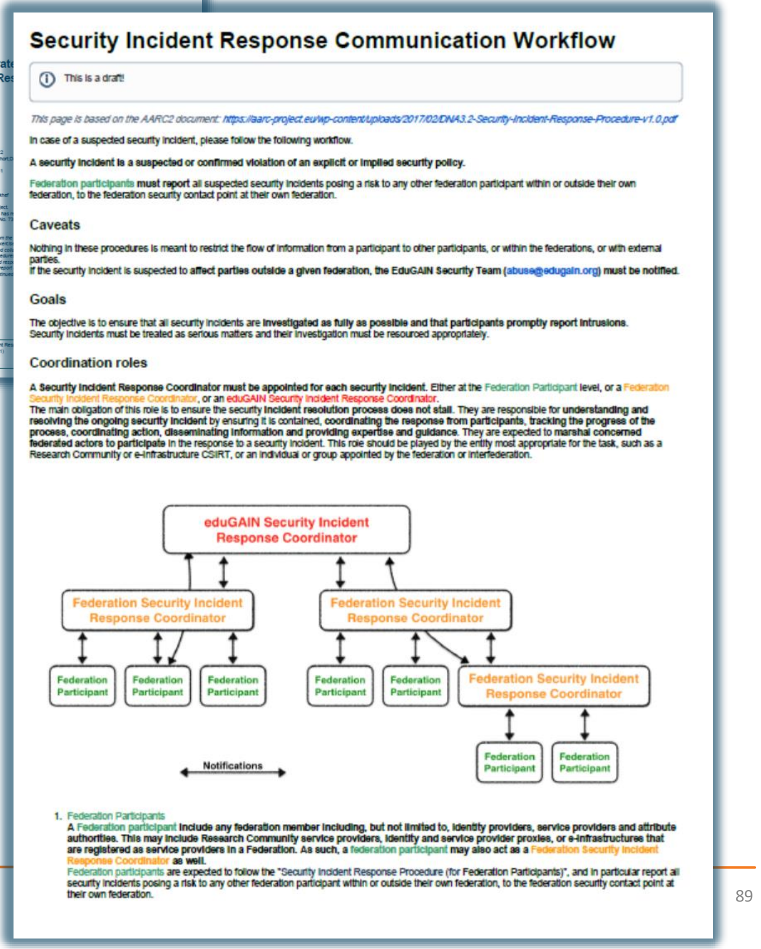
6 – Debriefing

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.*

Guide to Federat
Response for Res



Security Incident Response Communication Workflow

ⓘ This is a draft!

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

In case of a suspected security incident, please follow the following workflow.

A security incident is a suspected or confirmed violation of an explicit or implied security policy.

Federation participants **must report** all suspected 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.

Caveats

Nothing in these procedures is meant to restrict the flow of information from a participant to other participants, or within the federations, or with external parties.
If the security incident is suspected to **affect parties outside a given federation, the EduGAIN Security Team** (abuse@edugain.org) **must be notified.**

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 interfederation.

eduGAIN Security Incident Response Coordinator
Federation Security Incident Response Coordinator
Federation Security Incident Response Coordinator
Federation Participant
Federation Participant
Federation Participant
Federation Participant
Federation Participant
Federation Security Incident Response Coordinator
Federation Participant
Federation Participant
Notifications

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-infrastructures 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!

https://aarc-project.eu/guidelines/aarc-i051/

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

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

Co-supported by the Dutch National e-Infrastructure coordinated by SURF and by the EOSC-Hub and GEANT-4-3 RC Horizon 2020 projects