22-01-2024

# Deliverable D5.1
# Report on Trust and Identity Services, Enabling Communities and Incubator

| | |
|---|---|
| Contractual Date: | 31-12-2023 |
| Actual Date: | 22-01-2024 |
| Grant Agreement No.: | 101100680 |
| Work Package: | WP5 |
| Task Item: | Task 1, Task 2, Task 3, Task 4, Task 5 and Task 6 |
| Nature of Deliverable: | R (Report) |
| Dissemination Level: | PU (Public) |
| Lead Partner: | SUNET, SURF |
| Document ID: | GN5-1-23-843894 |
| Authors: | Maarten Kremers (SURF); Marina Adomeit (SUNET); Paul Dekkers (SURF); Davide Vaghetti (GARR); Christos Kanellopoulos (GÉANT Association); Michelle Williams (GÉANT Association); Niels van Dijk (SURF); Michael Schmidt (LRZ/DFN) |


## Abstract

This document reports on the Trust and Identity service families operated in GN5-1 by WP5 Tasks 1, 2, 3 and 4: eduroam, eduGAIN, Core AAI Platform and InAcademia; and on activities in Task 5 Incubator and Task 6 Enabling Communities. It covers uptake and usage, KPIs, activities, issues and outreach from the beginning of January 2023 to the end of October 2023.

# Table of Contents

# Table of Figures



# Table of Tables

# Executive Summary

This document reports on the services delivered by Work Package 5 Trust and Identity Services Evolution and Delivery (WP5) and related Incubator and outreach activities. WP5 is responsible for managing the Trust and Identity (T&I) services portfolio, which encompasses development of new services (if new use cases emerge), and enhancement and operation of existing services with the aim to drive them towards the anticipated maturity levels. This is the first service report of GN5-1, and it covers the activities and status of the services from the beginning of January 2023 until October 2023.

The T&I service portfolio comprises four service families: eduroam, eduGAIN, the Core AAI Platform and InAcademia. eduroam and eduGAIN are established hierarchical infrastructures, where GÉANT manages the top-level service and the National Research and Education Networks (NRENs) worldwide manage the national nodes. The other services are more centrally run, being the Core AAI platform, which evolved from the eduTEAMS services in 2023, and InAcademia, the affiliation validator service.

Each service has an appointed service owner who is responsible for service delivery and who manages and organises the work of the service teams in order to ensure effective, efficient, secure services operation, development and support.

During the reporting period, all services met or exceeded their key performance indicators on service availability and uptake. Highlights include:

- The eduroam team further developed and enhanced supporting software for the service, including new versions of the Configuration Assistant Tool (CAT) with support for OpenRoaming and geteduroam. New geteduroam clients, for a more secure way of getting access to eduroam, were also released (the Linux client was developed together with the T&I Incubator Task).
- eduGAIN Task members worked on strengthening its service delivery by initiating the creation of a more robust architecture for the service based on multiple delivery sites. The Task worked extensively with the community to update the eduGAIN Constitution in order to implement the first part of the recommendation of the eduGAIN Futures Working Group.
- The eduTEAMS service evolved to the Core AAI Platform. Initially delivered as an Identity and Access Management (IAM) solution, it experienced significant growth, leading to the creation of various AAI service implementations. This expansion prompted a transformation into the Core AAI Platform during the GN5-1 project's initial phase. This shift allows a separate focus on platform evolution and service development, providing flexibility for customisation and ensuring a streamlined user experience built on top of the globally recognised identity federation infrastructure eduGAIN.
- The InAcademia service keeps growing in terms of both availability in different federations and number of student validations. InAcademia welcomed its tenth federation (where it is supported by the national R&E federations).

Developing new ideas in T&I takes place in the Incubator (successfully launched in GN4-3), with the results of one iteration during the reporting period. A number of outreach activities have taken place, in coordination with the relevant outreach Work Packages, and specialised T&I business development and stakeholder engagement were undertaken by a dedicated outreach Task (Enabling Communities) in WP5.

Work Package 5 is mindful of its responsibilities as custodian of the flagship Trust and Identity services that are crucial to the research and education community. Therefore, while the results achieved in the project to date confirm the services' success, WP5 will continue its programme of development and innovation, of both existing and new services, to ensure the level of achievement is maintained and the community's needs are met.

# 1 Introduction

Trust and Identity (T&I) services underpin and enable research and education (R&E) collaboration across Europe and worldwide. The R&E community relies on a trustworthy and secure global authentication infrastructure, where resources can authorise users based on the information received from the user's home organisation (typically university or National Research and Education Network (NREN)) and on the resource policy.

GN5-1 Work Package 5 Trust and Identity Services Evolution and Delivery (WP5) is responsible for the innovation and development of both existing and new GÉANT T&I services and their operation, as well as driving them towards achieving the expected maturity levels. WP5 ensures that T&I services are operated efficiently and securely, with relevant procedures and processes in place, and that their operational health and usage are monitored and reported to the stakeholders, as appropriate.

The set of services delivered within the Work Package is:

- **eduroam**: provides a secure, worldwide roaming access service for the international research and education community. It includes the delivery of core eduroam European infrastructure (European Top-Level RADIUS (ETLR) servers), a set of supporting services (monitoring and diagnostics, eduroam database, Configuration Assistant Tool (CAT), eduroam Managed Identity Provider (IdP)) and as pilot, eduroam Managed Service Provider (SP).
- **eduGAIN**: interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. The service includes delivery of core global infrastructure (Metadata Aggregator (MDA)) and a set of supporting services (technical site with eduGAIN check-in tools, entities database, F-Ticks and eduGAIN Reporting).
- **Core AAI Platform**: is the platform to realise solutions for advanced federated identity, research and education use cases. The Core AAI Platform enables research and education communities to securely access and share resources using eduGAIN federated identities. It simplifies user authentication, identification, and role management while providing a unified integration point for services. This centralisation allows advanced solutions, while reducing complexity. The notable services built on top of the Core AAI Platform include MyAccessID, MyAcademicID, EOSC AAI, GÉANT AAI and the eduTEAMS services.
- **InAcademia**: provides service providers with a quick, reliable and secure way to verify academic affiliation (whether a user is a student, a member of staff or faculty) to determine whether a user is eligible for discounts or academic-only offers, provided the user is registered with a participating eduGAIN identity provider. The service is available in two editions: Commercial (service providers are charged for using InAcademia) and Community (selected not-for-profit service providers in the R&E sector may use InAcademia free of charge).

In addition to these four services, WP5 operates two more activities: the Incubator and the outreach activities.

The Incubator aims to develop, foster and mature new ideas in the Trust and Identity space in research and education. The outreach activities are the bi-directional channel with key T&I stakeholders to understand their needs and obtain feedback on the work done within Trust and Identity services as well as contribute to external T&I projects and initiatives.

The following sections provide information on the services and activities listed above from the start of January 2023 until the end of October 2023. For each service and activity the document presents a summary description; contact details; data on uptake, usage and key performance indicators (KPIs); and a summary of key activities and any issues encountered in the reporting period.

# 2 eduroam

Service Owner: Paul Dekkers (SURF)

eduroam (education roaming) [eduroam] provides a secure, worldwide roaming access service for the international research and education community. The eduroam service allows students, researchers and staff from participating institutions to obtain secure Internet connectivity on their mobile devices and laptops across their campuses and when visiting other participating institutions. Its architecture is based on a specific set of technologies and regulated by a number of agreements, which combined provide the essential eduroam user experience: 'open your laptop and be online'.

The contact details and information sources for eduroam are shown in Table 2.1, below:

| Aspect | Link |
|---|---|
| Website | https://www.eduroam.org/ |
| Wiki | https://wiki.geant.org/display/H2eduroam |
| Monitoring and statistics site | https://monitor.eduroam.org |
| Configuration Assistant Tool | https://cat.eduroam.org |
| eduroam Managed IdP | https://hosted.eduroam.org |
| geteduroam portal | https://get.eduroam.org |
| General support | help@eduroam.org |
| Support for National Roaming Operators | eduroam-ot@lists.geant.org |
| (European) eduroam Steering Group | eduroam@lists.geant.org |

Table 2.1: Contact details and information sources for eduroam

In the reporting period, the eduroam service recorded a high level of availability in terms of the performance of its core operations and supporting infrastructure and services, achieving 100% against its European Top-Level RADIUS (ETLR) availability key performance indicator.

## 2.1 Service Description

The basic principle underpinning the security of eduroam is that the authentication of a user is carried out at their home institution using the institution's specific authentication method. The authorisation to access local network resources is granted by the visited network. This allows the users to work as if they were at their own home institution, even when they are at another location where eduroam is available.

GÉANT operates the confederation-level service for members of the European eduroam Confederation, which is formed of autonomous roaming services who agree to a set of defined organisational and technical requirements by signing and following the eduroam Policy Declaration [eduroam_PolDecl], which is based on

the eduroam Service Definition [eduroam_ServDef]. The Confederation's goal is to provide a secure, consistent and uniform network access service to its users.

The European service is governed by the eduroam Steering Group (SG), while day-to-day operations and support are carried out by the eduroam Operations Team (OT).

In addition to operating the service's basic technical infrastructure (European Top-Level RADIUS (ETLR) servers), the GÉANT eduroam team also delivers a supporting services suite to facilitate the widespread, global deployment of eduroam. This suite includes:

- A central database (**eduroam db**) [eduroam_db] with information about and provided by participating National Roaming Operators (NROs) and institutions.
- Monitoring and metering tools (**F-Ticks**) [eduroam_Monitor], which are used for monitoring the availability of NRO eduroam infrastructure and collecting and processing eduroam authentication statistics. Note such collection and process are undertaken in line with eduroam's privacy-preserving approach.
- A Configuration Assistant Tool (**CAT**) [eduroam_CAT], which enables institution administrators to create eduroam installers configured with their local (home institution) setup, and end users to download the installers to configure devices they wish to use for eduroam access.

  The CAT tool also provides tools for Roaming Operators (ROs), for instance for diagnostics or to issue certificates used in the authentication infrastructure.
- **eduroam Managed IdP** [eduroam_ManIdP], which is a Software as a Service (SaaS) offering for institutions that encompasses running local (home institution) eduroam authentication infrastructure and issuing eduroam credentials to those end users.
- **geteduroam portal**, providing Managed IdP-like facilities for institutions that are connected via eduGAIN but do not want to issue eduroam credentials on campus. More information is available at [eduroam_geteduroam] (the portal software is institution-specific via in-app links).
- **eduroam Managed SP (pilot)** [eduroam_ManSPPilot], which is a hosted offering to connect small eduroam Service Providers directly to eduroam, without on-campus authentication infrastructure.

Further development of new eduroam features or supporting services is carried out within the GÉANT eduroam Development Team. The GÉANT eduroam Operations Team is responsible for continuous improvement of the existing service infrastructure and feature set. Development and deployment of eduroam is performed in accordance with the roadmap published on the WP5 Wiki [T&I_Roadmaps].

## 2.2 Uptake

eduroam uptake data is provided on the eduroam monitor site [eduroam_Monitor]. At the end of this reporting period, 38 GN5-1 partners use the eduroam service. However, the number of National Roaming Operators (NROs) in Europe is 51, as these cover other European countries in addition to partner countries.

On a global scale, 104 territories participate in the eduroam service (the dark-coloured areas in Figure 2.1 below). Of these NROs, 92 (49 from Europe) provided detailed data on the distribution of the eduroam service at a national level, which at the end of the reporting period totalled 9,288 participating institutions (6,644 in Europe) and more than 38,437 service locations for eduroam (24,121 in Europe).

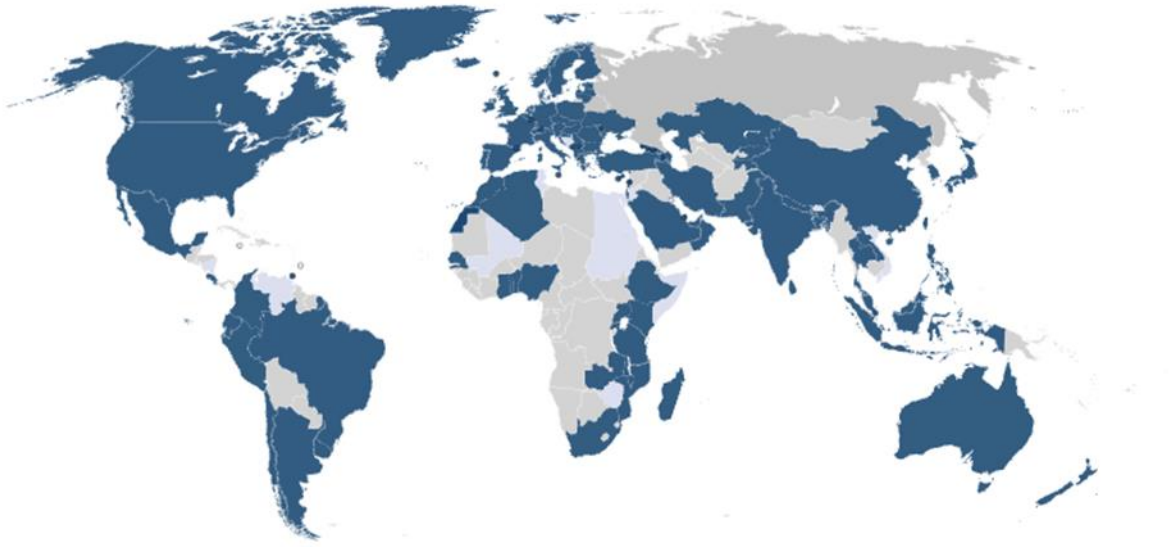

Figure 2.1: Global map of eduroam participants, at the end of reporting period

The growth in eduroam usage is measured monthly by counting the number of successful user authentications, as follows:

- National authentication is the grand sum of all successful roaming authentications in the same country counted via the F-Ticks system for all European countries that provide this information. (Note that pseudonyms are used to protect the data provided. For more information on F-Ticks, see the eduroam Monitor site [eduroam Monitor].)
- International authentication is the total number of successful international (cross-border) authentications counted in the logs of ETLRs.

The graph in Figure 2.2 clearly shows lower numbers in 2021 as part of the COVID-19 pandemic, with more normalised numbers in 2022 and higher numbers in 2023.

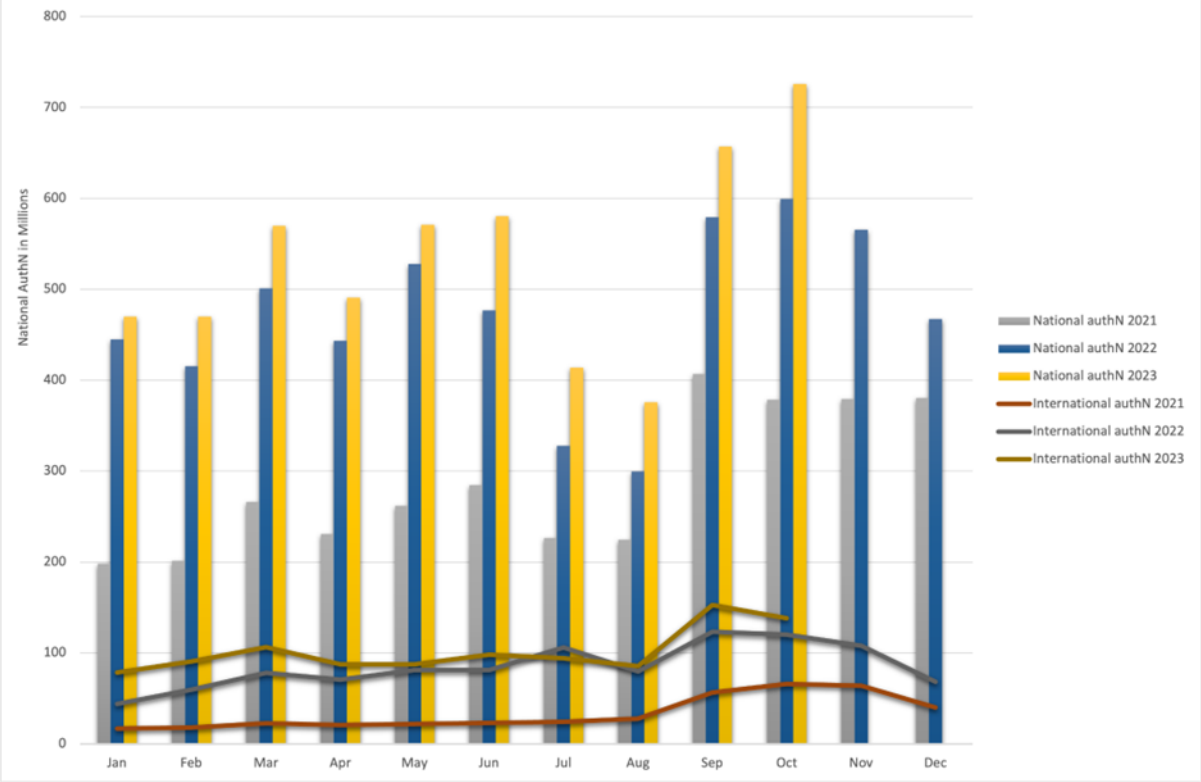


Figure 2.2: eduroam core service usage statistics: number of successful authentications per month

## 2.3 Key Performance Indicators

The KPIs for eduroam measure the availability of its core service (European Top-Level RADIUS servers) and uptake of the eduroam service measured by the number of international authentications. Table 2.2 shows that the services are running with at least one top-level roaming server 100% available, therefore performing better than the set target.

| KPI | Baseline (start of GN5-1) | Target (end of GN5-1) | Measured (end of reporting period) | Comments |
|---|---|---|---|---|
| European Top-Level RADIUS (ETLR) availability | 99.9% | 99.9% | 100% | |
| Number of international authentications | In 2021: 401,44 million<br>In 2022: 1,019,77 million | 5% annual increase | 1,018,741,087 | Figure for the first 10 months of 2023 |

Table 2.2: eduroam KPIs for the reporting period

## 2.4 Activities and Issues

The eduroam core service operated to a very high standard, with at least one top-level roaming server 100% available at all times.

Development of the service continued, with enhancement of eduroam CAT, geteduroam, work on OpenRoaming support, and further development of eduroam Managed Service Provider (SP).

The new eduroam policy documents have been finalised and approved by the Global eduroam Governance Committee (GeGC). The new policy is currently being signed by each NRO. Work has started on reviewing the privacy documents published for the general audience.

Regular monthly conference calls with the eduroam Steering Group were organised and chaired, with minutes shared via the mailing list. In addition, there were regular development calls opened to the larger audience.

Additional activities carried out in the reporting period include:

### Operations and Outreach

All of the core and supporting services' operations activities progressed as usual.

During the reporting period the team released new versions of CAT (providing support for OpenRoaming, delegate eduPKI certificate issuance via eduroam database and CAT, Arabic language support and support to enable geteduroam) and radsecproxy (providing native support dynamic peer discovery) and new geteduroam clients (Linux, together with the T&I Incubator Task; other clients in coordination with the Commons Conservancy Program [Commons_Conservancy]).

### Support

All of the core and supporting services' support activities were provided as usual.

The eduroam service organisation model assumes that the home institution and respective NRO will provide the user with the information and knowledge to use the eduroam service. It is up to the home institution to provide the necessary user support to the roaming user. Furthermore, the NROs and their member institutions are encouraged to provide user support to visiting users, regarding the use of the eduroam service. The Operations Team (OT) primarily provides support to NROs, but also disseminates information and tools that can be used by the local institutions' administrators and end users.

In addition, eduroam has a general support email contact point, help@eduroam.org, served by the GÉANT Operations Centre (OC), which provides first-line support for all user categories and general questions about the eduroam service. NROs use the eduroam Steering Group mailing list as a forum for raising and discussing various eduroam-related topics. The eduroam OT actively participates in this list and provides input.

Similarly, with regard to eduroam supporting services, the CAT developers and CAT users mailing lists serve as forums for raising issues and questions, and the eduroam service team regularly follows up and supports these discussions.

In addition to the above, Web and Wiki content were regularly updated.

# 3 eduGAIN

Service Owner: Davide Vaghetti (GARR)

eduGAIN [eduGAIN] is one of GÉANT's key Trust and Identity services, allowing identities issued by trusted organisations (Identity Providers) to be used to simply and securely access available web content and services (Service Providers). The eduGAIN service interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community.

Through eduGAIN:

- Identity Providers (IdPs) offer a greater range of services to their users, delivered by multiple federations in a truly collaborative environment.
- Service Providers (SPs) offer their services to users in different federations, thereby broadening their target market.
- Users benefit from a wider range of services provided seamlessly and accessed through a single identity. For example:
  - Researchers authenticate at their home institution IdP to collaborate on their specific thematic areas.
  - Students log in at their home institution IdP to access online learning material.

  A selection of user stories is available at [eduGAIN_UStories].

The contact details and information sources for eduGAIN are shown in Table 3.1, below.

| Aspect | Link |
|---|---|
| Website | https://www.edugain.org |
| Wiki | https://wiki.edugain.org |
| Technical site | https://technical.edugain.org |
| Reporting site | https://reporting.edugain.org |
| F-Ticks site | https://f-ticks.edugain.org |
| Support for users (providers of national identity federations, institutions, and individual researchers) | support@edugain.org |
| Security incidents contact | abuse@edugain.org |
| eduGAIN discussion list | eduGAIN-discuss@lists.geant.org |

Table 3.1: Contact details and information sources for eduGAIN

During the reporting period, eduGAIN core and supporting services were operated to a high standard, exceeding the set target for the availability KPI with 100% uptime. The uptake KPI was also largely exceeded: the number of identity federations in eduGAIN is 79, with 1 new federation becoming an eduGAIN participant, bringing the

percentage of R&E identity federations who are full members of eduGAIN to 90.8%. During 2023 the process to update the governance and architecture of eduGAIN gained momentum, with the approval of the new Constitution [eduGAIN_Const] and the setting up of a development site where the current service architecture can be duplicated and evolved.

## 3.1 Service Description

The eduGAIN service delivers a global infrastructure to enable users to log in at their home institution and access all services available in eduGAIN. This is possible thanks to secure and privacy-preserving exchange of information (metadata) between Identity Providers and Service Providers that takes place according to agreed rules (eduGAIN Policy Framework).

The eduGAIN Policy Framework details the administrative and technical standards that all participant federations must adhere to in order to enable the trustworthy exchange of service information to support identity, authentication and authorisation between partner federations.

GÉANT operates the global service for the members of the global eduGAIN interfederation, which is formed of autonomous identity federations who agree to a set of defined organisational requirements by signing and following the eduGAIN Policy Framework Declaration [eduGAIN_Pol] and accompanying eduGAIN SAML Profile [eduGAIN_Profile].

The eduGAIN service is governed by the eduGAIN Steering Group (SG), while day-to-day operations are carried out by the eduGAIN Operations Team (OT). eduGAIN reactive and proactive support is provided by the eduGAIN Support Team. The eduGAIN Security Team provides a central coordination point for security incident responses affecting multiple identity federations.

The technical description of eduGAIN is structured into core and supporting services.

eduGAIN core services include:

- **Metadata Distribution Service (MDS)**, which is the instantiation of the Metadata Profile offering the aggregation of compliant metadata between participant federations. The eduGAIN interfederation service is deployed using the MDS SAML Aggregator Tool. The aggregation tool ensures that the information supplied by each federation meets the technical requirements of the interfederation service.
- **eduGAIN validator** tests metadata syntax and eduGAIN-specific requirements and recommendations.
- **Federations status information** is a list of participating and candidate federations with contact and relevant policy details, as well as information about metadata they supply.
- **eduGAIN entities database** provides a search and reporting interface with current and historical information about the eduGAIN federations and entities.
- **eduGAIN entities database API access** provides selective information from the database.

eduGAIN supporting services comprise a set of information resources and tools targeted at the technical personnel of identity federations who are participating or planning to participate in eduGAIN. The products and resources used to deliver eduGAIN supporting services are:

- **eduGAIN Connectivity Check Service (ECCS)** – monitoring service for IdPs listed in eduGAIN which tests their actual readiness for eduGAIN, i.e. whether they consume eduGAIN metadata.
- **isFEDERATED check** – a global tool that searches known federations to report whether an institution is already part of them and is also in eduGAIN.

- **eduGAIN Access Check (EAC)** – a tool that allows administrators of service providers registered in eduGAIN interfederation to safely test their service behaviour.
- **eduGAIN Attribute Release Check (EARC)** – a tool that allows Identity Providers administrators to test their attribute release policies.
- **CoCo monitor** – GÉANT Code of Conduct (CoCo) monitoring service testing for adherence to CoCo specification.
- **eduGAIN Reporting** – (currently in beta) a tool that lets federation operators visualise and query their entities in order to assess the overall level of compliance to the eduGAIN and REFEDS standards with an intuitive and visually appealing interface.
- **F-Ticks** – (currently in beta) a tool that provides a central collector and visualisation for authentication statistics sent by eduGAIN participants.

eduGAIN further development, of new features or supporting services, is carried out within the appropriate eduGAIN development team. Development of eduGAIN is performed in accordance with the roadmap published on the WP5 Wiki [T&I_Roadmaps].

## 3.2 Uptake

Users of the eduGAIN service are listed on the status page of the eduGAIN technical website [eduGAIN_Tech]. At the end of the reporting period, eduGAIN had 79 participants, of which 41 are GÉANT partners' identity federations; these are listed in Table 3.2 below (the others being identity federations from other world regions). New eduGAIN members during the reporting period are listed in Table 3.3.

| Country | Identity Federation |
|---|---|
| Albania | RASH |
| Armenia | AFIRE |
| Austria | ACOnet Identity Federation |
| Belarus | FEBAS |
| Belgium | Belnet Federation |
| Bulgaria | BIF |
| Croatia | AAI@EduHr |
| Czech Republic | eduID.cz |
| Cyprus | CyNet Identity Federation |
| Denmark | WAYF |
| Estonia | TAAT |
| Finland | HAKA |
| France | Fédération Éducation–Recherche |
| Georgia | GRENA Identity Federation |
| Germany | DFN AAI |

| Country | Identity Federation |
|---|---|
| Greece | GRNET |
| Hungary | eduId.hu |
| Iceland | WAYF |
| Ireland | eduGATE |
| Israel | IUCC Identity Federation |
| Italy | IDEM |
| Latvia | LAIFE |
| Lithuania | LITNET FEDI |
| Luxembourg | eduID Luxembourg |
| Malta | RiċerkaNET Identity Federation |
| Moldova | LEAF |
| Macedonia | AAIEduMk |
| Norway | FEIDE |
| Poland | PIONIER.Id |
| Portugal | RCTSaai |
| Romania | RoEduNetID |
| Serbia | iAMRES |
| Slovakia | safeID |
| Slovenia | ArnesAAI Slovenska izobraževalno raziskovalna federacija |
| Spain | SIR |
| Sweden | SWAMID |
| Switzerland | SWITCHaai |
| The Netherlands | SURFconext |
| Turkey | YETKİM |
| Ukraine | PEANO |
| United Kingdom | UK federation |

Table 3.2: eduGAIN member GÉANT partners' identity federations

| Country or Region | Identity Federation |
|---|---|
| **Became an eduGAIN member and started supplying metadata** | |
| Somalia | SomaliREN Identity Federation |

Table 3.3: new eduGAIN federations

Figure 3.1 shows the global map of eduGAIN participants.

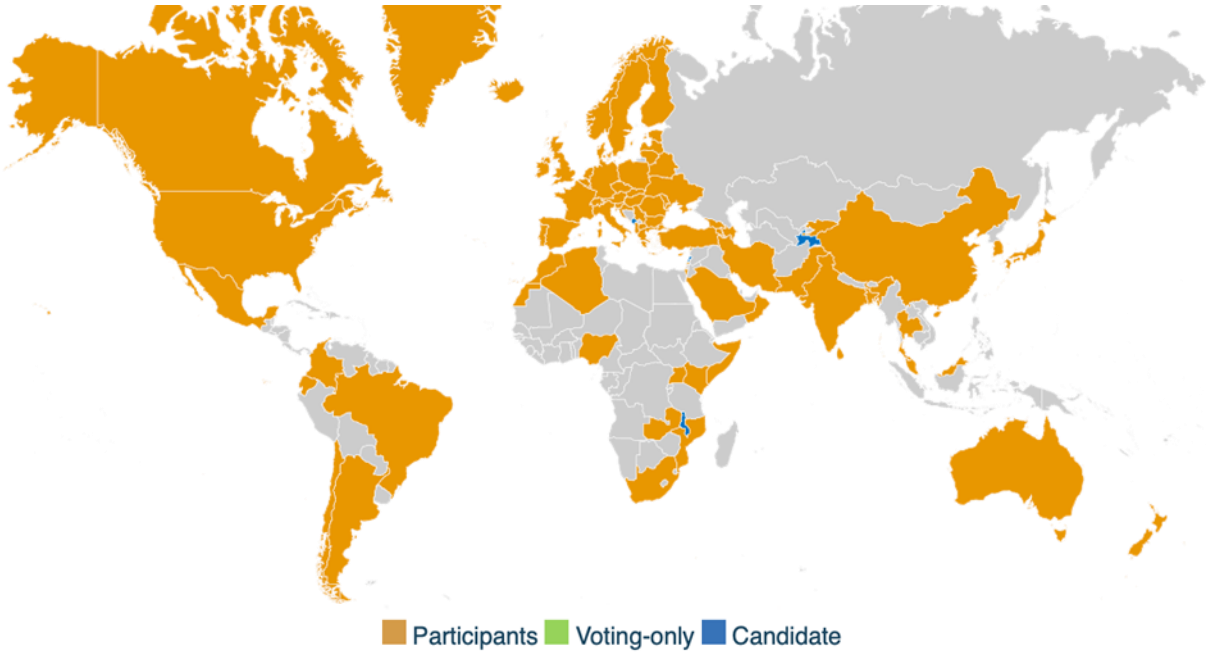


Figure 3.1: Global map of eduGAIN participants

By the end of the reporting period, eduGAIN was providing metadata containing 8,984 entities, of which 5,451 are Identity Providers and 3,552 are Service Providers. Compared with the beginning of the reporting period, growth of 10.2% in the numbers of both Identity Providers and Service Providers is shown (Figure 3.2). The slight drop in the number of Service Providers at the end of the reporting period was a result of one identity federation performing its regular membership review, resulting in the removal of inactive Service Providers.

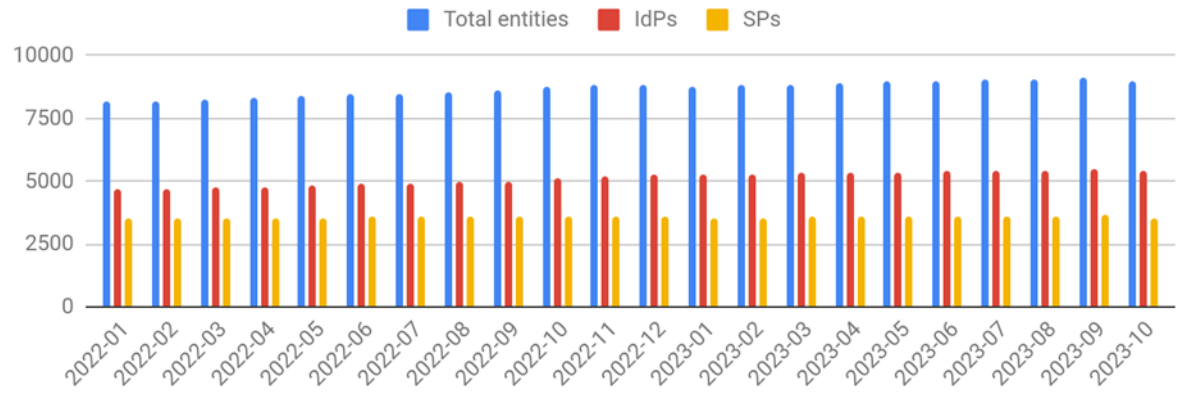


Figure 3.2: Trend of growth of Identity Providers and Service Providers in eduGAIN

Entity categories and entity attributes are the means for Identity Providers and Service Providers to declare that they either comply with the requirements defined by these categories or that they support it, in order to increase the level of interoperability, trust and security. The ultimate goal is to improve attribute release by Identity Providers, as this is one of the biggest barriers that Service Providers are facing. The entity categories, attributes and frameworks for use in the global R&E T&I sector are being specified by REFEDS and they standardise how these trust marks are defined and used. The following entity categories, attributes and trust frameworks are globally recognised and in use within eduGAIN:

- Release and Scholarship (R&S) [REFEDS_R&S].
- Security Incident Response Trust Framework for Federated Identity (Sirtfi) [REFEDS_SIRTFI].
- Code of Conduct (CoCo) [REFEDS_CoCo].
- Anonymous Access [REFEDS_AnonAccess].
- Pseudonymous Access [REFEDS_PseudAccess].
- Personalized Access[REFEDS_PersAccess].

Figure 3.3 shows the trend in adoption of REFEDS entity categories and attributes by Identity Providers and Service Providers in eduGAIN, with the exception of the last three entity categories from the list above, as those have been defined only recently and while the adoption rate is being recorded it is still in its very early days.

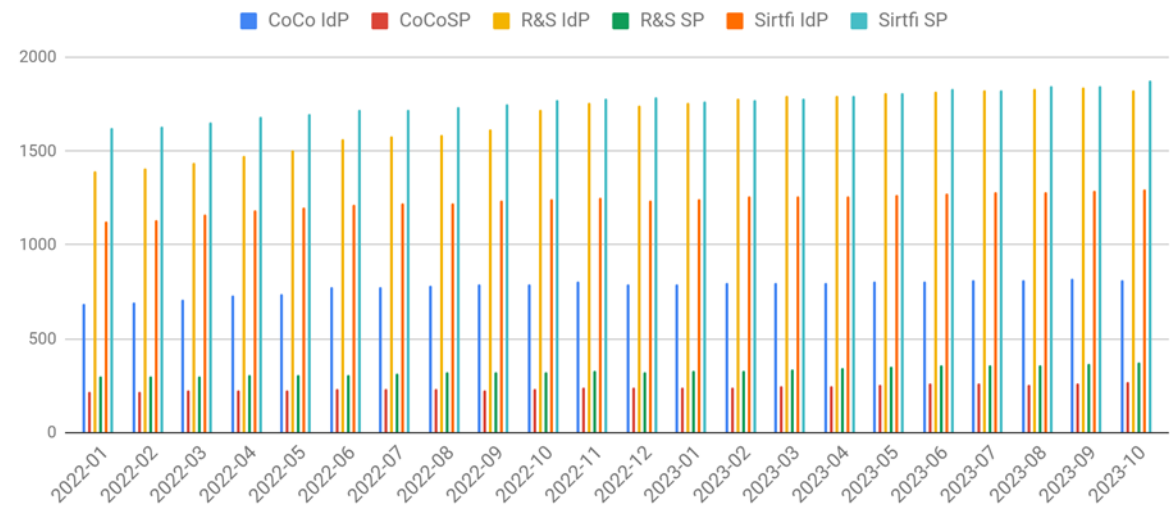


Figure 3.3: Trend of uptake of entity categories and attributes

## 3.3 Key Performance Indicators

The KPIs for eduGAIN measure the availability of its core service (Metadata Distribution Service) and uptake of eduGAIN measured by the number of known federations that have joined eduGAIN. Table 3.4 shows that the services are running with minimum disruption and that uptake is well on track and performing better than the set targets.

| KPI | Baseline (start of GN5-1) | Target (end of GN5-1) | Measured (end of reporting period) | Comments |
|---|---|---|---|---|
| Metadata Distribution Service (MDS) availability | 99.5% | 99.5% | 100% | Uptime calculated on a monthly basis; the reported value is the lowest. |
| Service Uptake: increase of number of IdPs | In 2021: 4,667<br>In 2022: 5,235 | 8% increase | 5,451 (+4.12%) | |

Table 3.4: eduGAIN KPIs for the reporting period

## 3.4 Activities and Issues

The eduGAIN core services were operated to a very high standard and performance has exceeded the targets set. Day-to-day operations relating to the management of the identity federations and the core services have been performed by the eduGAIN OT, while supporting services operations have been taken care of by dedicated sub-teams. The eduGAIN Service Owner, the eduGAIN OT Manager and eduGAIN Secretariat participated regularly in the eduGAIN SG meetings in order to report on the service and share the feedback of the community. eduGAIN support was delivered via a dedicated Support Team whose work is organised in a weekly rota, while the eduGAIN Computer Security Incident Response Team (CSIRT) provided support for coordination of interfederation security incidents. During the reporting period, the eduGAIN Secretariat and the eduGAIN

Service Owner worked extensively with the community to update the eduGAIN Constitution [eduGAIN Const] in order to implement the first part of the recommendation of the eduGAIN Futures Working Group [eduGAIN FWG]; the new Constitution will become effective in 2024.

Activities to be noted in the reporting period include:

### eduGAIN OT and Core Services

- The eduGAIN OT has been expanded to compensate for the retirement of members that will happen at the end of the current project. The process to hand over the eduGAIN OT lead and day-to-day management operations has started.
- The current architecture of the eduGAIN core services has been successfully duplicated on the GARR Cloud infrastructure. The site is used for development and staging. Currently the team is developing a fully automated deployment strategy for the eduGAIN core services.
- The team was reinforced by new members from SUNET. In collaboration with the community, development of a new architecture for the eduGAIN core services that will be based on multiple delivery sites started.

### eduGAIN Support Team

The eduGAIN service organisation model assumes that the Identity Provider (IdP), Service Provider (SP) or respective federation will provide localised and contextualised user support. The support provided by the eduGAIN Support Team is primarily available for the federations and, in certain cases, to individual IdPs and SPs. Users who raise issues with the eduGAIN Support Team will be routed to the appropriate local support service or team.

The eduGAIN support service provides two types of support: reactive and proactive [eduGAIN Support]. The first is related to requests sent to the eduGAIN support contact; the second is based on the daily check of the warnings detected on the eduGAIN participants' upstream feeds and it is targeted to the federation operators. eduGAIN support is provided primarily through the support@edugain.org email contact point and organised through a weekly rota of federation operator experts.

During the reporting period:

- The team leader from SWITCH concluded his employment and consequently left the project. He has been substituted by one of the current team members from ASNET-AM, who stepped up to take the team leader role.
- All the shifts in the weekly rota of the eduGAIN Support Team were covered without any exceptions.
- The Support Team received and processed about 35 valid eduGAIN support requests. Examples include support for:
  - Federation information change requests.
  - Federation candidate proposals.
  - Issues regarding interoperability of certain SPs and IdPs.
  - Resolving issues reported by eduGAIN support tools.
- The Support Team sent about 10 proactive support alerts to federation operators. Examples include:
  - Violation of specifications in the upstream metadata feed.
  - Technical suspension process forewarn messages.

- The eduGAIN support documentation and knowledge base is continuously verified and improved and it is feeding a public knowledge base available to federation operators, SPs and IdPs [eduGAIN SupportDocs].

In addition to the official support email address, the eduGAIN OT, Service Owner and Secretariat provide support through participation in various eduGAIN-related mailing lists and the eduGAIN dedicated Slack channels.

### eduGAIN Supporting Services and Development

In the reporting period, the eduGAIN reporting tool has undergone a thorough revision in order to improve the user experience. The tool, which has been developed in conjunction with the Incubator Task, lets federation operators explore their metadata and entities in order to assess the overall level of compliance to the eduGAIN and REFEDS standards with an intuitive and visually appealing interface. The tool collects, elaborates and visualises the information provided by the eduGAIN APIs.

All the other eduGAIN checking tools – eduGAIN Connectivity Check Service (ECCS), eduGAIN Access Check (EAC), eduGAIN Attribute Release Check (EARC), CoCo Monitor – have been updated and maintained in full operation.

### eduGAIN CSIRT

The eduGAIN CSIRT continues to supply security services on request by the eduGAIN Community, such as:

- Intelligence on security incidents of interest for the R&E community.
- Security threat evaluation for known software vulnerabilities.
- Communication Challenges to check the availability of the federations' security contacts.

In addition, the eduGAIN CSIRT established relationships with the most prominent eduGAIN participants' security officers and teams.

### Federation as a Service

In the reporting period Federation as a Service (FaaS) has been continuously operated. In July 2023 there was a hardware failure on the storage of the data centre that provides FaaS. As a consequence, the metadata endpoint was not available. The service was restored and service disruption was limited because metadata validity is 8 days. No data was lost in the incident. Currently 9 federations (LITNET, MREN, ASNET-AM, GRENA, MARnet, AMRES, CyNet, RičerkaNet, RASH) use Federation as a Service tools to manage their federations.

### SeamlessAccess

GÉANT continued its participation in the SeamlessAccess consortium, comprising the International Association of STM Publishers, NISO, Internet2 and GÉANT. This coalition was formed to collaborate on providing SeamlessAccess, which implements the recommendations from the RA21 initiative [SeamlessAccess]. SeamlessAccess addresses the need for a consistent experience in accessing federated resources; its main objectives are to enable user friendliness and IdP persistence. GÉANT's ambition is for SeamlessAccess to become the go-to IdP discovery service enabling a seamless and consistent experience when accessing resources in eduGAIN.

GN5-1 participates in this coalition by having representatives in the technical and governance steering groups, and by providing operational capabilities and the product manager for the service.

During the reporting period, the service continued to be operated by the SUNET NOC, which offers 24/7 support, deploying new versions of the software based on request. From the product management perspective, the following activities took place:

- UI was updated to improve accessibility and usability, achieving Web Content Accessibility Guidelines (WCAG) 2.1 AA/AAA compliance [WCAG2.1].
- Demo site was released [SeamlessAccess demo].
- Design of the UX and UI for the new Identity Provider filtering feature was done, including exploration, mockups, user A/B testing.
- Backend and frontend work on the new Identity Provider filtering feature progressed, including development of thiss.js and Metadata Query Protocol (MDQ) components.
- A group for Service Providers using SeamlessAccess was formed, to facilitate guidance on best practices for UX.
- UX sketch work on SeamlessAccess smart-button was aligned with the features of FedCM (Federated Credential Management (FedCM) is a W3C community group in response to browser changes following privacy requirements).
- Engagement from product management and UX with REFEDS (browser changes) and W3C (FedCM, PrivacyCG) over web browser privacy changes that affect SeamlessAccess functionality.

### Training and Outreach

In the reporting period the training team organised a series of webinars on eduGAIN Operations and Hub & Spoke Federation Architectures.

In addition, the training team made an agreement with the African regional organisation UbuntuNet to deliver training on identity federations and eduGAIN to the many African NRENs that are interested in eduGAIN. The training will be delivered in Q1 2024.

The training team also started to work with GÉANT Learning and Development (GLAD) to create a set of self-learning material on identity federations and eduGAIN. The activity will be concluded in Q4 2024.

# 4 Core AAI Platform

Service Owner: Christos Kanellopoulos (GÉANT Association)

The GÉANT Core AAI Platform is set to become a cornerstone in the landscape of advanced research and education use cases for federated identity, providing the critical infrastructure for key European initiatives such as the European Open Science Cloud (EOSC) AAI, EuroHPC and programmes supporting student mobility across the continent. It serves as the foundational backbone for a suite of identity services which are built on top of eduGAIN, including InAcademia, MyAcademicID, MyAccessID and the EOSC Federated AAI, enabling the delivery of a ubiquitous AAI to the GÉANT community, the high-performance computing area, European research infrastructures, and the broader education sector (Figure 4.1).

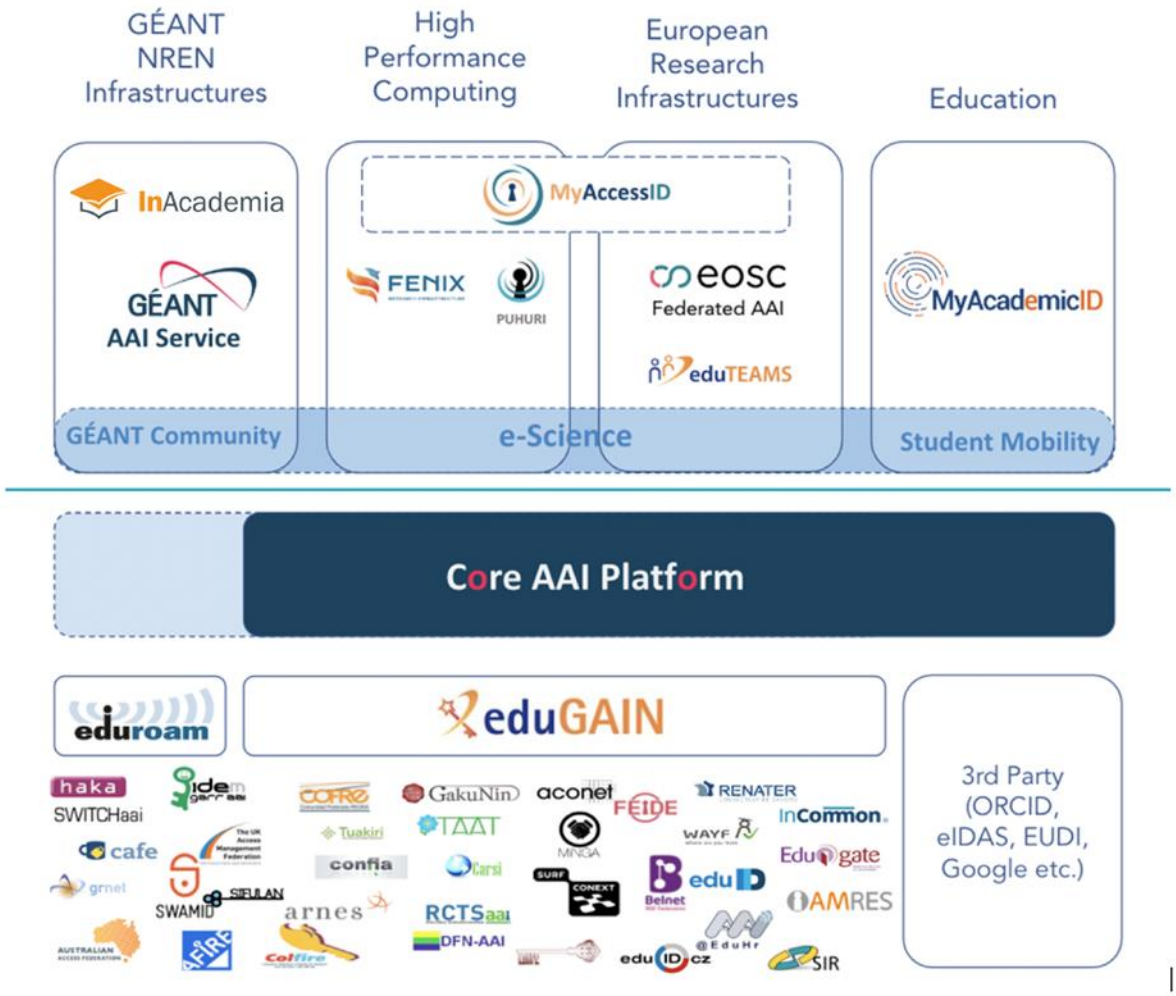


Figure 4.1: Core AAI Platform in the R&E federated identity ecosystem

The contact details and information sources for the Core AAI Platform are currently being updated in line with rebranding following its evolution from eduTEAMS.

## 4.1 Service Description

The Core AAI Platform enables provision of services that allow research and education communities and infrastructures to securely access and share common resources and services, leveraging the ubiquitous presence of eduGAIN federated identities. It enables them to securely authenticate, identify and manage the roles of their users and to have one integration point for services – all of that while concealing the complexity of dealing with the diverse international landscape of federated identity. It introduces the possibility to provide centralised solutions for more advanced use cases, thus moving the complexity from the edges and removing the risks and need for specialised expertise associated with research infrastructures running their own solutions. The development of the Core AAI Platform follows a strongly agile approach, with the frequent release of software enhancements that address stakeholders' requirements.

The Core AAI Platform implements (and enhances) the AARC Blueprint Architecture [AARC BPA] and deploys an IdP/SP proxy that allows connection of SAML Identity Providers, OIDC Providers, SAML Service Providers and OIDC Resource Providers, enabling the use of preferred identity sources and services regardless of the authentication protocol used. The Core AAI Platform proxy component is also responsible for aggregating the user attributes from various identity sources, enforcing community- and platform-wide policies and providing one persistent user identifier and a harmonised set of attributes to the connected services. Depending on the stakeholders' requirements, the Core AAI Platform can deliver centralised solutions for advanced use cases. The cases that are being explored and implemented during this reporting period include identity vetting step-up solution and SSH access based on the federated authentication flows.

GN5-1 WP5 funds the development of the Core AAI Platformand the engagement with communities and infrastructures that wish to use its derived services. This engagement includes understanding the stakeholders' requirements, reviewing integration aspects, and starting the design and pre-production phase. The operations of the resulting services are funded in certain cases by the GÉANT project (GN5-1 and predecessors), while in others they may be funded by other projects or infrastructures, as noted in Table 4.1.

Some of the most notable services which are operated on top of the Core AAI Platform are:

- **MyAccessID Identity Access Management (IAM) Service** [MyAccessID_IAM] – The MyAccessID IAM Service was the result of WP5's collaboration with the HPC community, namely with FENIX [FENIX] and Puhuri/LUMI [Puhuri], [LUMI]. The MyAccessID IAM Service provides a common identity layer for FENIX and Puhuri/LUMI. With this architecture, the FENIX and Puhuri/LUMI resource allocation systems and HPC services are used to connect and manage the access to the FENIX and Puhuri/LUMI resources, while users are authenticated and identified via the common MyAccessID IAM Service. The Core AAI Platform has been enhanced to support different registration flows per connected services and is working with Puhuri/LUMI and the federation operators to ensure that assurance is supported by those IdPs whose users access Puhuri/LUMI resources. An identity vetting step-up solution has been piloted in collaboration with the SUNET eduID team, in order to support those users whose IdPs do not deliver sufficient level of assurance.

- **GÉANT AAI Service** [GN_AAI] – The GÉANT AAI Service, previously known as GÉANT SP Proxy, allows GÉANT services to use federated authentication for identifying users from eduGAIN. During GN4-3, WP5 started the work of migrating the existing service to the new GÉANT SP Proxy based on the Core AAI Platform, offering a wide range of new capabilities, such as support for OpenID Connect, enhanced user and group management, support for the AARC Blueprint Architecture, and EOSC readiness. This migration is expected to be completed in 2024.

- **EOSC AAI** [EOSC_AAI] – The goal for the EOSC AAI is to provide the trust mortar with which the many bricks of the current set of scientific communities, collaborations and infrastructures are joined together. The EOSC AAI is comprised of the AAIs of the science clusters, research infrastructures and e-infrastructure providers which are being brought together through the EOSC AAI Federation. The EOSC AAI Federation is fully operational, with EOSC AAI e-infrastructure SP proxies and cluster community AAIs fully integrated into the EOSC AAI Federation. As part of the upcoming EOSC EU Node, GÉANT will continue to deliver the EOSC AAI Federation and in addition the EOSC AAI Identity Hub and the EOSC Exchange Infrastructure Proxy.

- **MyAcademicID** [MyAcademicID] – The MyAcademicID Identity and Access Management Service provides identity and federated access management for the services of the European Student Card Initiative [ESCI] and the services directly supporting the digitisation of Erasmus+ [Erasmus+]. The student mobility processes require the use of a number of services, all of which are involved in different stages of the pipeline and which will need to be able to exchange data about the students who are in mobility. Leveraging the ubiquitous presence of eduGAIN and eIDAS federated identities, the MyAcademicID Service enables the connected services to use the academic attributes that are available through the HEI federated logins provided in combination with the national eID of the users participating in student mobility.

## 4.2 Uptake

Core AAI Platform users are research communities or e-science infrastructure providers engaging in international collaborations. They can be small, medium or large communities or infrastructures and/or long-tail collaborations.

The Core AAI Platform provides the underlying technical stack upon which dedicated AAI service offerings are built, such as FENIX-AAI, Puhuri/LUMI AAI, MyAccessID IAM, PaNOSC-AAI, EUROfusion and EOSC-Life [FENIX; Puhuri; LUMI; MyAccessID_IAM; PaNOSC; EUROfusion; EOSC-Life].

The Core AAI Platform shared instance is used by smaller research communities that do not need a dedicated instance, such as LAGO [LAGO], SSHOC-AAI [SSHOC] and VESPA [VESPA].

The Core AAI Platform is collaborating with SURF, where the Core AAI Platform delivers a solution for their SRAM offering [SRAM] to support national scientific collaborations.

One of the most significant developments in the reporting period has been the procurement launched by the EuroHPC JU for the EuroHPC Federated Platform [EuroHPCFP_Proc], where the JU requests all procurers to integrate with the MyAccessID Service as a procurement requirement.

The approach being followed during the GN5-1 project is that the requirements analysis, design, and initial implementation activities are funded via WP5. This is a delicate process where subject matter, technical and integration support from the Core AAI Platform team is necessary in order to come up with the optimal solution that is integrated not only within the specific service, but within the platform as a whole. This is an ongoing process, as the requirements often progress from relatively simple requirements that target a range of use cases, to more complex requirement to address advanced use cases. During the first year of GN5-1 the WP has noticed a significant shift where Research Infrastructures, which until recently required their own AAI services, have realised the strong benefits of using horizontal AAI services, such as MyAccessID. The WP expects that this trend will continue and become even stronger in the coming years.

| Deployment | Status |
|---|---|
| eduTEAMS Service | Production |
| CESSDA/SSHOC | Production |
| eduGAIN | Production |
| LAGO | Production |
| Le Laboratoire Univers et Théories (Observatoire de Paris) | Production |
| LITNET | Pilot |
| Opticon RadioNet | Pilot |
| Paris Astronomical Data Center | Production |
| VESPA (EuroPlanet) | Production |
| FENIX (*) | Production |
| PaNOSC (UmbrellaID) | Production |
| EOSC-Life (*) | Production |
| MyAccessID (EuroHPC) | Production |
| Puhuri ISD Proxy | Production |
| MyAcademicID (Student Mobility) (*) | Production |
| Cloud services procured via the FPA (i.e. OCRE) | Production |
| SRAM (SURF) (*) | Production |
| GÉANT AAI Service | Production |
| EUROFusion | Pre-production |
| EOSC AAI | Production |
| EOSC AAI Federation | Pre-production |

Note:

* These deployments are supported through projects other than GN5-1, but are accomplished using the Core AAI Platform and are presented in the table both for completeness and to show the impact that the Core AAI Platform has beyond the GN5-1 project.

Table 4.1: Core AAI Platform deployments and status

## 4.3 Key Performance Indicators

The KPI targets and results for the Core AAI Platform for the reporting period are shown in Table 4.2, below.

| KPI | Baseline 01/01/23 (start of GN5-1) | Target 31/12/24 (end of GN5-1) | Achieved Result (by end of reporting period) | Comments |
|---|---|---|---|---|
| Core AAI Platform: GÉANT SP Proxy Service availability | 99.5% | 99.5% | 100% | |
| Core AAI Platform service uptake: GÉANT AAI Service Connected Services | 0 | 100 | 29 | The connection of the end-user services to the GÉANT AAI Service is being done by the GÉANT IT team and WP9. Currently, the GÉANT IT team is working on automating the migration of ~200 websites to the new GÉANT AAI Service. |

Table 4.2: Core AAI Platform KPIs for the reporting period

## 4.4 Activities and Issues

During the previous GÉANT projects, the eduTEAMS service was delivered as an Identity and Access Management (IAM) solution to enable research and education communities to securely access and share common resources.

The adoption and use of eduTEAMS expanded significantly, leading to the creation of numerous dedicated service instances for different research infrastructures. There are now several Authentication and Authorisation Infrastructure (AAI) service implementations that use eduTEAMS, such as the eduTEAMS Shared Service tailored for smaller research groups, MyAcademicID for supporting student mobility programmes like Erasmus+, MyAccessID for the European High-Performance Computing (HPC) service, the EOSC AAI, SURF's Research and Access Management service, and others. (It is worth noting the distinction between eduTEAMS, the platform, and the eduTEAMS Shared Service, a specific AAI service implemented by GÉANT using the eduTEAMS platform.)

Given this growth, a shift in the delivery mechanism for the service was required to transform eduTEAMS from an IAM solution to a comprehensive platform solution, renamed the Core AAI Platform. This redefinition and rebranding of the service began in the initial phase of the current, GN5-1 project.

This transformation has proved consequential: by separating the IAM platform from the AAI services built upon it, WP5 T3 is now in a position to focus separately on the evolution of the platform itself, and the development and delivery of services. This not only enables the team to work on optimising the platform but also provides greater flexibility in the customisation of services to suit the unique needs of various users.

By leveraging the globally recognised infrastructure federation, eduGAIN, the Core AAI Platform provides a customisable AAI solution for research and education, on top of which additional, complementary services can be built to enable users to effectively use their institutional identities when accessing different services, thereby ensuring a streamlined and efficient user experience.

Other notable activities that took place in the reporting period are as follows:

## Team

- Several new members of the Core AAI Platform team were recruited and joined the existing team:
  - Two members in the Site Reliability Engineering team (SRE).
  - Two full-stack developers.
  - One backend developer for SATOSA focusing on OIDC and SAML.
  - Two solution architects (new role).
  - One project manager (new role).
- The SRE team held a face-to-face meeting in Amsterdam to set the direction for the infrastructure side of the GÉANT Core AAI Platform.
- The support and solution architects team held a face-to-face meeting to set out the roadmap for their further work.

## Development and Operations Highlights

- The service was operated to a high standard, with continuous improvements to the operational model in order to enable the increased automation and scalability of the deployments. Development was undertaken in an agile manner in order to address the requirements in an effective way.
- Following several years of dedicated effort, the OpenID Connect Provider (OP) component of the Core AAI Platform has now reached a level of stability, with a comprehensive set of features including enhancements implemented during the reporting period:
  - The OP has undergone significant improvements, now encompassing support for client credentials as well as audience restrictions specific to the introspection endpoint. Moreover, the OP's codebase has been meticulously refactored to integrate the newly developed OpenID Connect (OIDC) library [IDPy OIDC], a commendable initiative by the Identity Python community. Throughout this refactoring process, the Core AAI Platform team played a pivotal role, making substantial contributions to the library's development with an emphasis on ensuring stability and robustness.
  - The team is now preparing to make the OP widely available to the open-source community. As part of this process, the remaining elements are being finalised and the technical documentation is being prepared. The successful completion of this activity will significantly bolster the Identity Python ecosystem by introducing a production-ready OIDC Provider component. This addition promises to be a valuable asset to the Identity Python community, facilitating the secure authentication of users across a wide array of applications.
- A new OIDC Relying Party component has been implemented and open-sourced, serving as the backbone for SATOSA [IDPy SATOSA]. This replaces the earlier implementation that depended on libraries with limited capabilities.
- Development work was started on the Service Management Portal and API. This will enable the users of the Core AAI Platform to directly manage the services they are connecting on the platform and thus reduce the effort required by the Core AAI Support and SRE teams while empowering users to self-manage their deployments.
- In order to support the user identity Level of Assurance requirements of the HPC community, a solution of step-up identity vetting is being explored. This solution should enable every user to have an alternative and provide a higher level of assurance for their identity, in the case that their Identity Provider does not have such capabilities. In the initial phase, a collaboration with the SUNET eduID team was established in order to benefit from this team's experience in integrating such a solution. Initial proof of concept has been defined and the work will continue with integrating an identity vetting solution in 2024.

- A solution for federated SSH is being explored to fulfil requirements of the HPC community, which needs to enable non-Web user access to the supercomputer machines. The SSH solution currently in place is user cumbersome and does not provide high security as the rollover of SSH keys is long. A just-in-time-of-access generation of SSH keys is being explored, and a proof of concept that involves an SSH Certificate Authority (CA) solution already in place in DeIC has been implemented.
- A streamlined pipeline has been established to seamlessly push Core AAI Platform updates to every customer. This automation not only simplifies the configuration update process but also significantly cuts down the duration of update operations. During the reporting period, there were 127 releases of the Core AAI Platform, 1 major, 48 minor and 78 patch releases.

## Service Highlights

Several dynamic activities are currently underway within individual service deployments. Highlights from this reporting period include:

### GÉANT AAI Service

- The migration of GÉANT IT and WP9 services from the legacy GÉANT SP Proxy remains ongoing. The GÉANT IT team has already migrated 23 production services. It is currently working on the automation of the migration of ~200 WordPress websites and the migration of the Confluence platform. As part of the migration of the Confluence platform, GÉANT IT is investigating switching from SAML to OpenID Connect and taking advantage of the new capabilities that that new GÉANT AAI Service provides. The WP9 team has migrated 6 production services and 2 more services are in the pipeline.
- Collaborations are ongoing with the Digital Services, GDPR, and Security teams to optimise and streamline this transition process.

### eduTEAMS Service

- A new Virtual Organisation (VO) for LITNET has been created.
- Expressions of interest have been received from several entities, including University Alliances, EOSC Raise, and KU Leuven HPC site.

### Engagement with the HPC Community

- The **FENIX RI** has integrated its acceptance AAI environment with the **MyAccessID** service. Discussions concerning the GRNET EuroHPC site are underway. Efforts are in place to integrate SUNET's identity vetting service, aiming to cater to users whose Identity Providers might not offer sufficient Level of Assurance data. In collaboration with **Puhuri**, significant strides have been made to engage federation operators and augment Identity Provider capabilities to release the necessary Level of Assurance.
- A highly productive face-to-face meeting with the **Puhuri** community took place to refine development strategies and chart an ambitious and at the same time pragmatic roadmap for deeper engagement and collaboration within the community.

  A significant outcome of this meeting was the decision to establish the **MyAccessID Task Force**, which is driving requirements for MyAccessID. MyAccesssID Task Force was established in September 2023, with representatives from Fenix RI, Puhuri, AARC community and GEANT, and the work is gaining momentum.

### Engagement with EOSC

- The **EOSC AAI Federation** is running as a pre-production service connecting the AAIs of four science clusters (ESCAPE, Life Sciences, PaNOSC and SSHOC) and the e-infrastructure AAIs (EGI Check-In, EUDAT B2ACCESS, GÉANT eduTEAMS and OpenAIRE). Components of the Core AAI Platform have been used in

the delivery of the EOSC AAI Federation. Part of the development plan of the Core AAI Platform includes the full support of the production EOSC AAI Service in 2024.

- The **Life Science AAI** service has further expanded to also support the Biobanking and BioMolecular resources Research Infrastructure (BBMRI). This is the second major pan-European research infrastructure to migrate successfully from their own AAI solution to the Life Science AAI. The migration was completed in May 2023. Currently the Life Science AAI service connects 52 services and serves a user base of 15,957.

### Engagement with the Erasmus Student Mobility Programme

- The **MyAcademicID IAM Service** currently serves a substantial user base of 300,000. Thanks to the collaborative efforts of national academic federations and NRENs, 845 of the 1,474 Higher Education Institutions across 31 national federations have rolled out support for the European Student Identifier. Notably, MyAcademicID boasts the largest volume of users, emphasising the imperative for the Core AAI Platform to ensure robustness and scalability.
- A pilot activity has been started with the EPICUR University Alliance [EPICUR] where the MyAcademicID IAM Service is used as the authentication services for the Alliance. The WP expects that this pilot will result in a blueprint for other European university alliances.

## Outreach

Key global outreach activities that took place in the reporting period are:

- A workshop at TNC23 [TNC23] was held to promote the achievements of the Core AAI Platform and to look at further plans.
- A presentation about the work done within Puhuri and MyAccessID was given at TNC23.
- A workshop at the Internet 2 Technology Exchange 2023 [TechEx23] was held to present the AARC BPA and related guideline documents.

## Issues

Finding specialised resources remains a challenge. This was partially accomplished during the reporting period by employing new people for the core Operations Team in GÉANT. However, delay with filling the new positions resulted in an underspend. The budget was rephased, with new positions for hiring in GÉANT opening for 2024.

# 5 InAcademia

Service Owner: Michelle Williams (GÉANT Association)

InAcademia [InAcademia] became a production service in February 2020. It allows online retailers to easily validate whether a customer is a student or otherwise affiliated to an education institution, as a member of staff or faculty for example. For user authentication, InAcademia uses the Identity Providers available in eduGAIN. It provides an OIDC protocol interface for connecting online retailers with the SAML protocol that is used within eduGAIN and R&E federations. End users and Identity Providers benefit from InAcademia as it provides a privacy-preserving way to validate the user's affiliation, compared with the manual process many online retailers are currently using, which includes uploading personal documents to their sites. The InAcademia service is available in two service offerings: Commercial for online retailers that are making a profit from offering services that leverage InAcademia affiliation information and Community for Service Providers that are not for profit.

The contact details and information sources for InAcademia are shown in Table 5.1 below:

| Aspect | Link |
|---|---|
| Website | https://www.inacademia.org |
| General information | info@inacademia.org |
| Support for merchants | support@inacademia.org |

Table 5.1: Contact details and information sources for InAcademia

## 5.1 Service Description

InAcademia is a simple online service that allows online retailers to validate whether a customer is a student or otherwise affiliated to an academic institution. It is the real-time, digital equivalent of asking a student to show their student card in order to access or buy services and products, and provides merchants with a quick, easy, reliable, privacy-preserving and secure way to validate student affiliation.

Customers of the InAcademia service are typically retailers, using e-commerce sales channels (merchants); they are either commercial organisations or not-for-profit organisations. Customers have to register in accordance with the instructions given on the InAcademia website in order to use the service [InAcademia_Reg]. Each customer has to sign a contract, agreeing to specific terms and fees, and can expect service delivery according to the Service Policy published on the InAcademia website [InAcademia_SvcPol].

Identity federations are encouraged to actively promote InAcademia to their constituents and are invited to participate in the InAcademia Steering Committee. The InAcademia support model relies on collaboration with federation operators to resolve issues regarding the institutions from the member groups.

From a technical perspective, the InAcademia service is a web service that enables communication between an e-commerce application (either for purchase of goods and services, or for registration to access restricted resources) and the user's home institution's Identity Provider (IdP). The web service provides a REST interface for clients to request a user validation using OpenID Connect (OIDC) protocol. InAcademia then communicates

with IdPs typically using SAML. In addition to this core functionality, the InAcademia service includes a portal for collecting and reporting usage statistics.

The service is operated by the GÉANT project, delegating technical operations to the SUNET Network Operations Centre (NOC) and ULAKBIM (for quality control of Turkish IdPs in particular). The Operations Team is responsible for managing and maintaining the service, and for providing support on operational issues according to the agreed Operational Level Agreement (OLA).

InAcademia is governed by the identity federation community responsible for overseeing the service; the InAcademia Steering Committee is composed of representatives of most participating federations, meeting twice a year to discuss strategic matters that impact and influence the direction of the service. The intention is to ensure that the service strategy is in line with the expectations and desires of the identity federation community, and to act as both a sounding board for new ideas, and an escalation point for any operational issues.

Development of new features or supporting services for InAcademia is carried out within the GÉANT InAcademia Development Team, which is aligned to the Core AAI Platform Development Team. The InAcademia Operations Team is responsible for continuous improvement of the existing service infrastructure and feature set. The development of InAcademia follows a strongly agile approach, utilising short sprints to release software enhancements that address stakeholders' requirements. Development of InAcademia is performed in accordance with the roadmap published on the WP5 Wiki [T&I Roadmaps].

## 5.2 Uptake

Whilst InAcademia is technically available across the whole eduGAIN landscape, it was decided to artificially limit the geographical scope of the initial usage on the following grounds:

- There are regulatory and taxation matters that require specific analysis in each country and therefore each country is subject to consultation with the GÉANT Finance team prior to expansion.
- National interpretation of the federated identity technical standards in some cases requires specific treatment in order for the service to function as intended, and it is important to be able to prepare for that in advance of registering commercial use cases.

The reporting period started and ended with two national 'community' customers, and five paying 'commercial' customers.

The customers that registered to InAcademia during the GN4-3 project cycle continued to increase the scope of their use of the service as the number of participating identity federations grew (see Table 5.2 below), increasing the number of validations processed by the service. As InAcademia requests a set of attributes common to many other services in eduGAIN, it is therefore able to provide 'live' assessments of the performance of each IdP that responds, and effort has been apportioned to informing federation operators about any misconfigured IdPs identified during the operation of the InAcademia service, particularly in the Turkish national identity federation, YETKİM, which has recently grown due to the success of the sister service MyAcademicID [MyAcademicID].

Uptake of the service continues to be tied to national policy and attitudes to the presence of commercial services in eduGAIN. During the reporting period, GÉANT and the National Research and Education Network for Uganda (RENU) collaborated to design a pathfinding pilot that seeks to understand how InAcademia could be implemented on a regional basis outside Europe. At the end of the reporting period, a Memorandum of Understanding (MoU) is in place, and further work will be undertaken to design the implementation.

| Country | Identity Federation | Status |
|---|---|---|
| Austria | eduID.at | Operational |
| Denmark, Iceland and Greenland | WAYF | Operational |
| France | Fédération Éducation–Recherche | Operational |
| Germany | DFN AAI | Operational |
| Greece | GRNET | Registered in Federation pending first merchant |
| Italy | IDEM | Operational |
| Spain | SIR | Operational |
| Sweden | SWAMID | Operational |
| The Netherlands | SURFconext | Operational |
| Norway | Feide | Registered in Federation pending first merchant |
| Turkey | YETKİM | Operational |
| **New for this reporting period:** | | |
| Finland | HAKA | Operational |
| Uganda | RIF | Pathfinding pilot |

Table 5.2: Participating identity federations in InAcademia as of November 2023


Figure 5.1: Participating identity federations in InAcademia as of November2023

## 5.3 Key Performance Indicators

The KPIs reported here relate to the reporting period starting from January 2023.

| KPI | Baseline (start of GN5-1) | Target (end of GN5-1) | Measured (end of reporting period) | Comments |
|---|---|---|---|---|
| Availability of the InAcademia nodes | 99.5% | 99.5% | 99.999% | |
| InAcademia service uptake: number of national federations participating in the service | 9 | 15 | 10 | |

Table 5.3: InAcademia KPIs for the reporting period

## 5.4 Activities and Issues

Activities of note in the reporting period include development and operations, outreach and business development.

### Development and Operations

New software releases during the period, all of which improve the merchants' and users' experience and make the product more valuable/desirable, included:

- SVS 4.0.1, January 2023: removed support for sha1-hash-based IdP Hinting, and deployed additional minor bug fixes.
- SVS 4.1.0, March 2023: introduced support for SATOSA 8.2.0, deprecated the 'idp_hint' parameter (aarc_idp_hint parameter introduced in 2022), updated the InAcademia branding at the Consent Handler, and made additional logging improvements.
- SVS 4.4.0, August 2023: introduced support for SATOSA 8.4.0, implemented support for Finnish language at the user consent screen, fixed minor bugs and deployed logging enhancements.

Since the last release, significant effort has been invested in the development of:

- Updated Discovery workflow based on Seamless Access, planned for release winter 2023.
- A new onboarding channel, designing a new e-commerce plugin and associated subscription services, planned for release in early 2024.

Effort went into supporting merchants and federations during the rollout of the service to new countries. Support was provided to a large customer providing 'instant verification' to global brands and retailers and to another large customer providing validation of entitlement to register at student marketplaces in Finland.

### Outreach and Business Development

Wide-scale community engagement took place during the reporting period, with the following specific outreach activities undertaken in order to increase uptake and usage, and to ensure that federation operators and the NREN community are onboard with the direction the service is taking:

- Hosted one InAcademia Steering Committee meeting.
- Worked bilaterally with each federation that is interested in participating in the service, with more detailed conversations undertaken with:
  - Feide/Norway – currently working through the registration process.
  - HAKA/Finland – now operational, as of spring 2023.

In spring 2023 significant effort was made in collaboration with WP2 Marcomms, Events and Policy Engagement to update the InAcademia brand. This included a redesigned logo, refresh of the colour palette, refresh of the 'about InAcademia' videos used for promoting the service, a new set of brand guidelines [InAcademia_Branding] and an update of the theme and content at inacademia.org to reflect the new branding.

| | |
|---|---|
|  |  |
| Old logo | New logo released March 2023 |

Figure 5.2: Old and new InAcademia logos

## Issues

- It continues to be difficult to migrate long-term, commercial users of eduGAIN to InAcademia, because they perceive it as a fee being levied for reduced functionality (InAcademia limits personal information being released and pseudonymises the user information). While many services are expressing interest in using InAcademia, the team is finding it challenging to convert that interest to usage, as:
  - It is difficult to give evidence of coverage unless the service is operational in that country.
  - Often only publicly funded institutions are included in the national federation, meaning that merchants need to find a number of different solutions in order to validate user affiliation across all higher education facilities in a specific country.
- It is proving very difficult to access the commercial, business-to-business market in a very crowded retail marketing space, and differing approaches are being assessed by activities that are funded outside the GÉANT project.

# 6 Incubator Activities

The Trust and Identity Incubator ('T&I Incubator', or 'Incubator') aims to develop, foster and mature new ideas in the Trust and Identity (T&I) space in research and education (R&E). The Incubator investigates new technologies, solutions, policy and business models that currently do not (yet) have a place in the services or technology stack of the T&I ecosystem in GÉANT. This may include testing and experimenting with potential new features for services or technology in T&I areas; business case development for potential new services and developments that would improve data protection and privacy aspects in services or software is also in scope.

The Task supports the incubation of new ideas or potentially disruptive T&I technologies that are considered sufficiently mature within the project's technology readiness level (TRL) constraints. The work of the Incubator is based on ideas and suggestions from the GÉANT community and from the GÉANT T&I leadership team following the GÉANT strategic direction for the T&I area. These ideas need to demonstrate a value for either enhancing existing services or exploring new service models and/or new potential services or technologies in line with emerging use cases. Any community member might submit a topic suggestion via the public Call for Ideas page [Incubator_CFI]. This call is advertised regularly at events and in different newsletters and community mailing lists to raise awareness in the R&E community.

The basic methodology for working on selected topics has not changed since it was introduced in GN4-3 [Incubator_Method], but it is continuously improved based on the lessons learned. The Incubator follows an agile approach that enables frequent topic changes and fast results. It uses roles and terminology loosely based on the Scrum framework [Scrum] to implement as many topics as possible within a short timeframe. Therefore, GN5-1 is split into multiple cycles, each lasting 7 months. The Incubator currently has two teams (Alpha and Omega), which are structured to work on several different activities (2–4) in parallel during a cycle. Their work is regularly showcased at public sprint demos, which take place in the middle and at the end of each cycle. Once a cycle ends, the results are documented, published and then might be transferred to another party who will take ownership.

Incubator results are either handed over to the T&I service Tasks for further development and integration into existing services, made available as software and business cases to the R&E community, or a report is provided as to why a specific work item is not worth pursuing. If an activity needs additional effort before release, it is proposed that the work continues, refocused, as another incubator topic in a new cycle.

## 6.1 Key Performance Indicators

The Incubator KPI measures the number of activities (topics) carried out during the GN5-1 project. Table 6.1 shows that the Incubator completed four activities in one cycle and achieved its objective for the first year. With the next cycle having already started with four more activities, the KPI will be met in April 2024. Thus, there is a chance that the targeted value will be exceeded by the end of GN5-1.

| KPI | Baseline (start of GN5-1) | Target | Measured | Comments |
|---|---|---|---|---|
| Number of topics that went through the incubator cycles | 0 | Y1: 4; Y2: 8 | 4 | Measured at the end of Month 10. Includes the activities from the first cycle. |

Table 6.1: Incubator KPIs at end of Month 10

## 6.2 TIM Programme

Back in GN4-3, as part of its commitment to enable broad engagement of the R&E community, the Incubator Task joined forces with the GÉANT Learning and Development (GLAD) team to initiate the T&I Incubator Mentorship (TIM) programme. TIM is an initiative that enables sponsoring NRENs to bring together ambitious young minds and subject matter experts to pioneer and prototype new ideas in the T&I field.

TIM is a collaboration between subject matter experts of the Incubator, GLAD, the NRENs (home mentors) and young professionals (participants) across Europe. The overall aim of the programme is to contribute to a viable and sustainable pipeline of T&I products and services for the GN5-1 project and ultimately for the European NREN community.

Participants – who are usually students – (and their mentors) are nominated by their local GÉANT partner and they collaborate directly with the Incubator teams. On this journey, they are mentored by the Incubator experts as well as their home institution. GLAD provides additional support through training opportunities for both participants and mentors. Finally, all participants may present their work at an international event or conference supported by the GÉANT Future Talent training programme. The expected duration of each TIM programme cycle is 7 months, in line with the regular activity cycles of the Incubator.

Due to the new project phase, which led to significant changes in the Incubator team, no TIM candidate was accepted in the first half of GN5-1. After an extensive information campaign conducted by GLAD, the TIM programme started in September 2023 with the second GN5-1 Incubator activity cycle, with a total of six students applying from four different NRENs. This has shown that the broader promotion on other channels such as social media has been successful in reaching new organisations. Even students whose institutions were not previously part of the GÉANT collaboration applied directly to the programme.

Three students (two from KIFÜ and one from CyNet) were selected to support the SP automation and Webwallet activities, which are described in Section 6.4. They will contribute to the development work and present their results at the Trust and Internet Identity Meeting Europe (TIIME) [TIIME] (un)conference in the beginning of 2024. Once again, the TIM programme successfully attracted NRENs and institutions to participate for the first time. This was also the first time that applications had been received directly from students who were interested in this learning opportunity. Supported by GÉANT Partner Relations, GLAD was able to establish effective communication between all parties and bring the candidate and mentor together.

It is planned that the TIM programme continues in the last, third, cycle of GN5-1. The goal is to support at least two additional candidates. More information about this initiative is available on the GLAD public Wiki page [GLAD_TIM].

## 6.3 Outreach Activities

The Incubator attaches great importance to cooperation with the NRENs, other project partners and the community. Everything from proposals for new ideas and the direction of activities to the delivery of results is intended to take place through this close cooperation. For this reason, a number of initiatives have been launched to increase public awareness and to get in touch with stakeholders.

The actions and measures listed in Table 6.2 have been undertaken to inform interested parties about the Incubator and its activities:

| Name | Type | Reference |
|---|---|---|
| Incubator home | Public Wiki page | https://wiki.geant.org/display/GWP5/T5+-+Trust+and+Identity+Incubator |
| Dashboard | Public Wiki page | https://wiki.geant.org/x/kQATIw |
| GN5-1 Incubator introduction | CONNECT article | https://connect.geant.org/2023/05/15/unleashing-innovation-the-geant-trust-identity-incubator |
| Community demo invitation | CONNECT article | https://connect.geant.org/2023/08/30/trust-identity-incubator-demo-online-7-september-2023 |
| Public sprint demos | Presentations | https://wiki.geant.org/x/VAVBJg |
| GN5-1 TIM announcement | CONNECT article | https://connect.geant.org/2023/06/28/tim-2023-needs-you-trust-identity-incubator-mentorship-programme-is-back |
| GLAD TIM promotion | Public Wiki page | https://wiki.geant.org/x/AQJBJg |

Table 6.2: Actions and measures for communicating with interested parties

Members of the Incubator activity have presented the work of the Incubator at various events. Table 6.3 presents a list of recent presentations:

| Subject | Event | Target Group* | | | | Reference |
|---|---|---|---|---|---|---|
| | | R&E | NREN | GC | IN | |
| Personal Profile Page Improvement | TNC 08-06-2023 | ✓ | ✓ | ✓ | ✓ | https://tnc23.geant.org/demo/#253 |
| Personal Profile Page Improvement | TechEx/ ACAMP 21-09-2023 | ✓ | ✓ | ✓ | ✓ | https://spaces.at.internet2.edu/display/ACAMP/ACAMP+Unconference+2023+Home |
| Passkeys for R&E | Workshop 16-05-2023 | ✓ | ✓ | ✓ | ✓ | https://events.geant.org/event/1458/ |
| Profile Page, Auto SP Deployment, SAML Signature Validation | eduGAIN and REFEDS Town Hall 2023 11-10-2023 | ✓ | ✓ | ✓ | | https://wiki.geant.org/x/jwS-JQ |

Note:

* Target Group: Research and Education (R&E), National Research and Education Network (NREN), GÉANT Community (GC), Industry (IN)

Table 6.3: List of general presentations

Topics for the first Incubator cycle in GN5-1 (Cycle 7) were selected from community proposals and distilled during the project preparation phase. In the second GN5-1 Incubator cycle (Cycle 8), the usual community approach [Incubator CFI] was used again to select the topics. Unfortunately, the Incubator received only a limited set of topics that were in scope. An effort will be made to address this issue next year through increased outreach, such as the through the TIIME initiative.

In collaboration with the GÉANT Association, NRENs and community partners, the Incubator is reviving the Trust and Internet Identity Meeting Europe [TIIME]. This unconference-style meeting was held from 2013–2020 as the only T&I innovation conference in Europe focusing on R&E. This important event will return in early 2024 to serve as a platform for sharing new and innovative ideas within the T&I community, which will ultimately serve as a source of projects for future Incubator cycles. Planning for the event was successfully completed in August 2023.

## 6.4 Activities and Issues

The Incubator started in GN4-3 and completed a total of 6 activity cycles during that project phase. Three additional cycles were planned for the GN5-1 project phase. During this reporting period, the Incubator completed its seventh cycle and started the eighth.

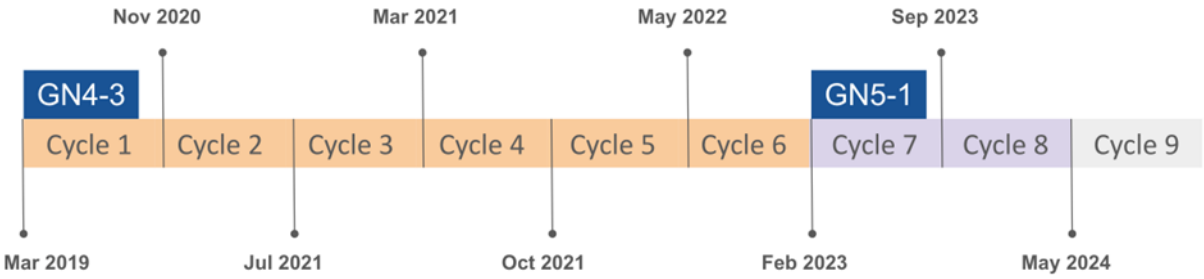


Figure 6.1: Timeline showing GN4-3 and GN5-1 start dates

| Cycle | Start | End | Status | Activities | Activity page |
|---|---|---|---|---|---|
| 7 | 06 Feb 2023 | 03 Sep 2023 | Completed | 4 | https://wiki.geant.org/x/hgATIw |
| 8 | 25 Sep 2023 | 21 Apr 2024 | In progress | 4 | https://wiki.geant.org/x/igATIw |
| 9 | 13 May 2024 | 15 Dec 2024 | Planned | 2–4 | https://wiki.geant.org/x/jAATIw |

Table 6.4: Schedule of GN5-1 Incubator cycles

The schedule shown in Table 6.4 is based on cycles of about seven months, constituting sprints which each last five weeks. The cycles have been chosen to ensure sufficient time to investigate and implement a proof of concept (PoC), but also to deliver results as quickly as possible and thus evaluate a PoC's chances of success. Based on the lessons learned from GN4-3, a transition period of three weeks has been introduced between the cycles. This enables the team to wrap up work, learn about the new topics and perform kick-off meetings before the cycle starts.

All activities, both GN4-3 and GN5-1, can be found on the Incubator Dashboard [Incubator Dashboard]. It lists completed activities and their results as well as ongoing activities. The Dashboard will be continuously updated at the beginning of every new cycle.

### 6.4.1 Cycle 7 Activities (Completed)

The Incubator completed its seventh cycle (first cycle in GN5-1) during the reporting period. During this cycle, four topics were explored. All of them were successfully completed.

#### Further Improve the Personal Profile Page

Usually, there is no way for federated users to have an historical overview about which service providers they used their account to log in to. This activity developed a mechanism to show a user their federated signing-in events, allowing them to check recent authentication activity. Users can see the list of authentications containing date and time, IP address and attributes released to a service provider during the login, helping them to spot suspicious activity.

The Incubator developed a user profile page as part of an Identity Provider user interface. The software is available as a Shibboleth and SimpleSAMLphp module, which are the most-used Identity Provider technologies in the R&E sector. It enables end users to gain insight into where and when their personal data was last released, from their home organisation Identity Provider perspective. The module is ready to use, was made publicly available by contributing to the SimpleSAMLphp development project, and will be maintained by the original

developers during GN5-1. Supported by the WP5 Enabling Communities Task, they will work with the community to integrate both modules as an integral part of the respective products.

The results of this activity are available on the project page [Incubator_FItPpP].

### geteduroam Linux Client

The geteduroam service provides a novel way for end users to configure eduroam on their devices. It helps them to get the correct and secure configuration by combining federated web login with the provision of an x.509 client certificate to use for authentication, makes deploying eduroam more secure, and minimises the risk of sensitive credentials leaking due to a mistaken, insecure configuration. If a basic client is available for Linux users, this provides instant value and also makes it easier for the community at large to implement more incremental improvements later on.

The Incubator implemented a Linux client that interfaces with geteduroam and configures and refreshes the credentials. This includes a graphical user interface as well as a command line tool integrated into the default network manager used by most distributions. The product maintenance will be continued by eduroam and the geteduroam developers.

The results of this activity are available on the project page [Incubator_gLC].

### OIDCfed Support on SimpleSAMLphp

OpenID Connect federation (OIDCfed) will provide the basis for multilateral connections between Rps and OPs in a scalable way. Adding OIDCfed support to Shibboleth has already been proposed as a potential item to be put on the roadmap of the Shibboleth project [Shibboleth_Roadmap], but many of the AAI proxies for research in the AARC BPA, and at research institutions, are running SimpleSAMLphp as the basis for their proxy.

Based on the previous success of its OIDC OP project, the Incubator was in an excellent position to add native OIDCfed support, with support for hierarchical trust path construction and the ability for policy filtering, to SimpleSAMLphp. To this end, the existing SSP module authoauth2 was extended to include additional key features. Furthermore, a testbed architecture was designed and a functional implementation was created. In addition, a command line interface was developed to support future tasks.

The results of this activity are available on the project page [Incubator_OSoS].

### Passkey for R&E

Passkey promises a new way of implementing passwordless login. However, this type of login does not contain an attestation. How does this new protocol work, then? how does it integrate into GÉANT's current ecosystem and how would this work in combination with new paradigms such as wallets?

The Incubator set out to explore passwordless authentication within the realm of identity federations. This innovative approach sought to yield valuable insights into the viability and potential advantages of utilising passkeys as an authentication factor or even as an alternative to multi-factor authentication (MFA). The outcome comprised a comprehensive white paper encompassing an in-depth analysis of passkeys in the context of R&E, along with the presentation of test results derived from existing implementations; the white paper is available both on the geant public website [GN5-1_WP_Passkeys] and in the open-access repository Zenodo [GN5-1_WP_Passkeys_Zenodo]. An abridged version of the report was also made available to the community and distributed to interested users [GN5-1_Passkeys_Intro].

The results of this activity are available on the project page [Incubator_PforR&E].

### 6.4.2 Cycle 8 Activities (In Progress)

The Incubator started its eighth cycle (second cycle in GN5-1) during the reporting period. During this cycle, four topics are being explored.

#### Automation of Deployment and Configuration of Initial Set of SPs for New Federations

While supporting new federations in setting up their infrastructures, there is not much automation in place. Everything is done very manually, and takes a lot of time. With regard to the SPs, both for the installation and configuration of the services themselves, and the required operations to federate them, in order to be able to provide them in a federated (e.g. eduGAIN) fashion, almost everything still involves manual setup. It would be useful for (new) federations to be able to deploy an initial set of services, those which could de facto start to attract users towards the newly deployed federation infrastructure and the federated IdPs.

This activity investigates a proxy approach to aggregate the services and potentially simplify the deployment and integration of tools. The Incubator will make an inventory of relevant services and discuss integration scenarios with stakeholders. The goal is to create proof of concept of at least one scenario and present it to federation operators.

More details about this activity are available on the project page [Incubator_AofSPs].

#### Scalable Testing for Insecure SAML Signature Validation

The SAML 2.0 protocol relies on XML signatures as the foundation of its security. It is notoriously complex and allows for many ways to create one or more signatures for any document, which means an implementation can easily fall victim to accepting data that is not properly signed. Even common R&E implementations such as Shibboleth and SimpleSAMLphp have had issues here in the past. As well as these common products, which at least are periodically audited for such problems, a much larger risk is custom implementations that use different or even home-grown libraries.

The goal of the activity is to deliver a (software or service) solution that assists identity federation operators in testing at scale several core security aspects of SAML Service Providers within their federation. This topic includes the technical implementation of the use cases to test against. In addition, it designs a concept to support operators to deploy the test suite both technically and operationally.

More details about this activity are available on the project page [Incubator_STfISSV]].

#### Trust Fabric for Wallets

Europe is working towards a wallet-based identity ecosystem. The Architecture and Reference Framework (ARF) [ARF] is intended to serve as a basis for the implementation of the proposal for the European Digital Identity Wallet Architecture and Reference Framework [EDIWARF]. The current version of the ARF has declared the organisational trust out of scope. The OIDC federation specification seems to have many characteristics that would allow such a wallet ecosystem to be defined.

The goal of this activity is to investigate and test the use of the OIDC federation protocol as a trust fabric for a wallet ecosystem. This activity will evaluate ARF for trust framework-related requirements; describe how OIDC federation may be leveraged with OpenID for Verifiable Credentials (OpenID4VC); and plan and build a test setup to verify the usability of OIDC federation in the context of a wallet ecosystem.

More details about this activity are available on the project page [Incubator_TFfW].

### Webwallet for Research Use Case

The current ARF assumes all interactions will be handled via an app on a mobile phone. While this may suffice for many users, it will leave out groups that cannot or will not use such devices. In addition, it creates a dependency on the vendors of the devices and the software they run on. Finally, users may not be willing to store and aggregate work-related data on a personal device.

This activity will investigate whether a browser-based wallet may be created which can support (parts of) the ARF. A first version of such a webwallet has been developed as part of the eDiplomas wwWallet Ecosystem activity [wwWallet_Ecosystem]. To confirm usability for the GÉANT R&E community, the browser-based wallet should be tested with the same scenarios as were previously tested in the Incubator using mobile-based wallets. The goal is to describe scenarios, set up a test environment and release at least one new version of the existing wwWallet [wwWallet].

More details about this activity are available on the project page [Incubator_WWfRUC].

# 7 Outreach Activities

Within GN5-1 Work Package 5 Trust and Identity Services Evolution and Delivery, part of the effort is aimed at providing a bi-directional channel with key T&I stakeholders to understand their needs and obtain feedback on the work done within Trust and Identity services. Their input is used to drive the evolution of existing T&I services or to set out the requirements for new services or tools. The Enabling Communities Task (WP5 Task 6) brings together project partners and identity federation operators in the field of higher education; it reaches out to other communities such as research infrastructures, other relevant initiatives and other EC-funded projects.

Central to the Enabling Communities Task is outreach and engagement with key stakeholders, such as eScience and identity federations, and other sectors (e.g. eGov/eIDAS, industry). This work involves a two-fold approach. On the one hand there is the T&I business development coordination in collaboration with the other services in WP5 and with the User and Stakeholder Engagement Work Package (WP3). On the other hand the eScience global engagement is carried out by liaising with and contributing to external projects and initiatives such as EOSC-related projects, FIM4R, REFEDS and WISE as well as other e-infrastructures.

Finally, the Enabling Communities Task facilitates the AARC Engagement Group for Infrastructures (AEGIS) group, a spin-off of the Authentication and Authorisation for Research and Collaboration (AARC) project, bringing together global representatives from AAI operators in research and e-infrastructures to discuss the adoption of policy and technical best practices that facilitate interoperability across e-infrastructures [AEGIS Charter].

## 7.1 Engagement with Key Stakeholders and Other Sectors

Engagement with the key stakeholders and other sectors is done by means of the business development coordination work where the Task acts as a bi-directional channel between the outreach teams of the GN5-1 project and the T&I services in WP5.

The outreach teams – WP3 User and Stakeholder Engagement, together with Services Marketing (WP2, Task 2) – are the front line of service promotion to the prospective customers. The service owners within T&I are responsible for correctly identifying target groups and for supporting the outreach teams by providing them with the knowledge, training and material needed for outreach. Where more specialised and technical engagement is needed, this is conducted by the respective T&I service teams.

The work on the business development itself, and details of any additional outreach activities, are included in the respective sections on each service.

## 7.2 Liaison with and Contribution to External Projects and Initiatives

Although the GN5-1 project reaches out to a wide community, it often proves to be more successful to carry out work in more open fora (e.g. REFEDS, WISE, FIM4R, etc.) in order to secure the buy-in of key communities. The Enabling Communities Task ensures that the relevant people can contribute to such activities. It also liaises with other projects such as EOSC-related projects, MyAccessID and MyAcademicID to build on any relevant results. During the reporting period, activities proposed as part of the work plan were exposed to different communities for feedback.

The work items outlined below were discussed in a wider community at combined meetings with the AARC community, WISE, REFEDS and EUGridPMA. Meeting agendas and notes are available [EUGridPMA].

### Interoperable Global Trust Federation (IGTF)

The Task contributed to the AARC/IGTF work on the *Guidelines for Secure Operation of Attribute Authorities* [AARC-G071]. This work was approved by AEGIS.

### WISE Trust Framework for Security Collaboration among Infrastructures (SCI)

The Task is coordinating the work on updating the Policy Development Kit produced by the AARC project within the WISE community.

### Federated Identity Management for Research (FIM4R)

The Task contributes to FIM4R in two ways: by supporting the periodic meetings and by contributing effort to the more specific tasks carried out by the FIM4R group [FIM4R].

Outreach was undertaken again in person on the whole range of the work of the Task at the International Symposium on Grids & Clouds (ISGC) 2023 Conference [ISGC_2023] and the 2023 Internet2 Community Exchange [I2ComEx_2023].

## 7.3 AEGIS

The AARC Engagement Group for Infrastructures (AEGIS) brings together representatives from research and e-infrastructures, operators of an AAI that follows the AARC BPA, a de facto standard for research communities to manage access to their users and their resources services. AEGIS offers a forum for these operators to exchange experiences in operating an AARC BPA-compliant infrastructure, identify policy and technical challenges in the AARC frameworks and improve them accordingly, as well as to expand the AARC artefacts. The AARC Blueprint Architecture and AEGIS are fundamental building block for the AAI interoperability in EOSC and EuroHPC and of course for the GÉANT Core AAI Platform. The chair of AEGIS along with the chairs of the Architecture Working Group and the Policy Working Group are supported by WP5.

In 2023 the AEGIS community grew from eight member infrastructures to nine, and a total of ten observer infrastructures [AEGIS]. The WP5 Enabling Communities Task facilitates the work of AEGIS by offering the necessary support to manage the group and the calls that are organised on a monthly basis. In the reporting period, AEGIS held 8 online meetings.

# 8 Conclusions

This document has provided an overview of the progress made with the services delivered by the Trust and Identity Work Package (WP5) in the first ten months of the GN5-1 project. Each service has an appointed service-owner who is responsible for ensuring the delivery, operation, development and support of their respective service. The key performance indicators have been met for all services.

New ideas in the T&I space in research and education have been developed, fostered and matured in the T&I Incubator (Task 5).

The services were promoted through various events including training, presentations aimed at different audiences and participation in conferences. The Enabling Communities Task (Task 6) has helped to streamline outreach outside the GN5-1 project and to create a better communication channel with other projects and communities.

WP5 will continue its programme of development and innovation, within the existing services and via the Incubator, to ensure the level keep delivering high quality services to meeting the needs of the research and education community.

# References


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

[AARC-G071] https://aarc-community.org/guidelines/aarc-g071/

[AEGIS] https://wiki.geant.org/display/AARC/AEGIS

[AEGIS_Charter] https://aarc-project.eu/wp-content/uploads/2019/12/AEGIS-Charter-v1.0.pdf

[ARF] https://code.europa.eu/eudi/architecture-and-reference-framework

[Commons_Conservancy] https://commonsconservancy.org/

[EDIWARF] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[eduGAIN] https://www.edugain.org

[eduGAIN_Const] https://technical.edugain.org/doc/eduGAIN-Constitution-v4-final.pdf

[eduGAIN_FWG] https://wiki.geant.org/display/eduGAIN/eduGAIN+Futures+Working+Group+Charter

[eduGAIN_Monitor] http://monitor.edugain.org/coco/

[eduGAIN_Pol] https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf

[eduGAIN_Profile] https://technical.edugain.org/doc/eduGAIN-saml-profile.pdf

[eduGAIN_Support] https://wiki.geant.org/display/eduGAIN/eduGAIN+support

[eduGAIN_SupportDocs] https://wiki.geant.org/display/eduGAIN/eduGAIN+support#eduGAINsupport-eduGAINSupportKnowledgeDatabase

[eduGAIN_Tech] https://technical.edugain.org

[eduGAIN_UStories] https://edugain.org/edugain-users/

[eduroam] https://www.eduroam.org/

[eduroam_CAT] https://cat.eduroam.org/

[eduroam_db] https://monitor.eduroam.org/fact_eduroam_db.php

[eduroam_geteduroam] https://www.geteduroam.app

[eduroam_ManIdP] https://hosted.eduroam.org

[eduroam_ManSPPilot] https://msp-pilot.eduroam.org/

[eduroam_Monitor] https://monitor.eduroam.org/

[eduroam_PolDecl] https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-194_eduroam-policy-for-signing_ver2-4_1_18052012.pdf [this document is being updated; the link is to the current official published version]

[eduroam_ServDef] https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf [this document is being updated; the link is to the current official published version]

[EOSC_AAI] https://op.europa.eu/en/publication-detail/-/publication/d1bc3702-61e5-11eb-aeb5-01aa75ed71a1/language-en/format-PDF/source-188566729

[EOSC-Life] https://www.eosc-life.eu/

[EPICUR] https://epicur.edu.eu/

[Erasmus+] https://ec.europa.eu/programmes/erasmus-plus/node_en

[ESCI] https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en

[EUGridPMA] https://www.eugridpma.org

[EUROfusion] https://euro-fusion.org/

[EuroHPCFP_Proc] https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=15701

[FENIX] https://fenix-ri.eu/
[FIM4R] https://fim4r.org
[GLAD_TIM] https://wiki.geant.org/x/AQJBJg
[GN5-1_Passkeys_Intro] https://wiki.geant.org/display/GWP5/Passkey?preview=/589070371/633276338/Introduction%20to%20Passkeys%20Usage%20and%20Implementation.pdf
[GN5-1_WP_Passkeys] https://resources.geant.org/wp-content/uploads/2023/11/GN5-1_White-Paper_Passkeys-Use-and-Deployment-for-RE-Services.pdf
[GN5-1_WP_Passkeys_Zenodo] https://doi.org/10.5281/zenodo.10210492
[GN_AAI] https://wiki.geant.org/display/GSPP/GEANT+AAI+Service
[I2ComEx_2023] https://internet2.edu/2023-internet2-community-exchange/
[IDPy_OIDC] https://github.com/IdentityPython/idpy-oidc
[IDPy_SATOSA] https://github.com/IdentityPython/SATOSA/pull/439
[InAcademia] https://www.inacademia.org
[InAcademia_Branding] https://inacademia.org/branding/
[InAcademia_Reg] https://inacademia.org/registering-your-service/
[InAcademia_SvcPol] https://inacademia.org/service-policy/
[Incubator_AofSPs] https://wiki.geant.org/x/goqBJw
[Incubator_CFI] https://wiki.geant.org/x/jwATIw
[Incubator_Dashboard] https://wiki.geant.org/x/kQATIw
[Incubator_FItPPP] https://wiki.geant.org/x/IIAcIw
[Incubator_gLC] https://wiki.geant.org/x/KoAcIw
[Incubator_Method] https://wiki.geant.org/x/NbAuBw
[Incubator_OSoS] https://wiki.geant.org/x/J4AcIw
[Incubator_PforR&E] https://wiki.geant.org/x/I4AcIw
[Incubator_STfISSV] https://wiki.geant.org/x/_YmBJw
[Incubator_TFfW] https://wiki.geant.org/x/ioqBJw
[Incubator_WWfRUC] https://wiki.geant.org/x/f4qBJw
[ISGC_2023] https://indico4.twgrid.org/event/25/
[LAGO] http://lagoproject.net/
[LUMI] https://www.lumi-supercomputer.eu/
[MyAcademicID] https://wiki.geant.org/display/SM/MyAcademicID+Identity+and+Access+Management+Service
[MyAccessID_IAM] https://wiki.geant.org/display/MyAccessID/MyAccessID+Home
[PaNOSC] https://www.panosc.eu/
[Puhuri] https://puhuri.io/
[REFEDS_AnonAccess] https://refeds.org/category/anonymous
[REFEDS_CoCo] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
[REFEDS_PersAccess] https://refeds.org/category/personalized
[REFEDS_PseudAccess] https://refeds.org/category/pseudonymous
[REFEDS_R&S] https://refeds.org/research-and-scholarship
[REFEDS_SIRTFI] https://refeds.org/SIRTFI
[Shibboleth_Roadmap] https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/1120895029/Project+Roadmap#Under-Discussion
[Scrum] https://scrumguides.org/scrum-guide.html
[SeamlessAccess] https://seamlessaccess.org/
https://seamlessaccess.org/about/governance/
[SeamlessAccess_demo] https://demo.beta.seamlessaccess.org
[SRAM] https://www.surf.nl/en/surf-research-access-management-easy-and-secure-access-to-research-services

[SSHOC] https://sshopencloud.eu/
[T&I_Roadmaps] https://wiki.geant.org/display/GWP5/Trust+and+Identity+Services+Roadmaps
[TechEx23] https://internet2.edu/2023-internet2-technology-exchange/
[TIIME] https://tiime-unconference.eu/
[TNC23] https://tnc23.geant.org/programme/
[VESPA] http://www.europlanet-vespa.eu/
[WCAG2.1] https://www.w3.org/TR/WCAG21/
[Wi-Fi] https://www.wi-fi.org/
[wwWallet] https://github.com/wwWallet
[wwWallet_Ecosystem] https://wwwallet.github.io/wallet-docs/

# Glossary

| | |
|---|---|
| **AAI** | Authentication and Authorisation Infrastructure |
| **AARC** | Authentication and Authorisation for Research and Collaboration |
| **AARC BPA** | AARC Blueprint Architecture |
| **AEGIS** | AARC Engagement Group for Infrastructures |
| **API** | Application Program Interface |
| **ARF** | Architecture and Reference Framework |
| **BBMRI** | Biobanking and BioMolecular resources Research Infrastructure |
| **BPA** | Blueprint Architecture |
| **CA** | Certificate Authority |
| **CAT** | Configuration Assistant Tool |
| **CoCo** | Code of Conduct |
| **CSIRT** | Computer Security Incident Response Team |
| **EAC** | eduGAIN Access Check |
| **EARC** | eduGAIN Attribute Release Check |
| **EC** | European Commission |
| **ECCS** | eduGAIN Connectivity Check Service |
| **eduroam** | education roaming |
| **EGI** | European Grid Infrastructure |
| **eID** | Electronic Identification |
| **eIDAS** | Electronic Identification, Authentication and Trust Services |
| **EOSC** | European Open Science Cloud |
| **EPICUR** | European Partnership for an Innovative Campus Unifying Regions |
| **ESCAPE** | European Science Cluster of Astronomy & Particle physics ESFRI research infrastructures |
| **ESFRI** | European Strategy Forum on Research Infrastructures |
| **ETLR** | European Top-Level RADIUS server |
| **EUDAT** | European Data Infrastructure |
| **EUGridPMA** | European Policy Management Authority for Grid Authentication in e-Science |
| **EuroHPC** | European High-Performance Computing |
| **EuroHPC JU** | European High-Performance Computing Joint Undertaking |
| **FaaS** | Federation as a Service |
| **FedCM** | Federated Credential Management (W3C) |
| **FIM4R** | Federated Identity Management for Research |
| **GDPR** | General Data Protection Regulation |
| **GeGC** | Global eduroam Governance Committee |
| **GLAD** | GÉANT Learning and Development |
| **HEI** | Higher Education Institution |
| **HPC** | High-Performance Computing |
| **IAM** | Identity Access Management |
| **IdP** | Identity Provider |
| **IGTF** | Interoperable Global Trust Federation |
| **ISD** | Infrastructure Service Domain |
| **ISGC** | International Symposium on Grids & Clouds |
| **KPI** | Key Performance Indicator |
| **LAGO** | Latin American Giant Observatory |

| | |
|---|---|
| **MDA** | Metadata Aggregator |
| **MDQ** | Metadata Query Protocol |
| **MDS** | Metadata Distribution Service |
| **MFA** | Multi-Factor Authentication |
| **MoU** | Memorandum of Understanding |
| **NISO** | National Information Standards Organization |
| **NOC** | Network Operations Centre |
| **NREN** | National Research and Education Network |
| **NRO** | National Roaming Operator |
| **OC** | Operations Centre |
| **OCRE** | Open Clouds for Research Environments |
| **OIDC** | OpenID Connect |
| **OIDCfed** | OpenID Connect Federation |
| **OLA** | Operational Level Agreement |
| **OP** | OIDC Provider |
| **OpenID4VC** | OpenID for Verifiable Credentials |
| **OT** | Operations Team |
| **PaNOSC** | Photon and Neutron Open Science Cloud |
| **PKI** | Public Key Infrastructure |
| **PoC** | Proof of Concept |
| **PrivacyCG** | Privacy Community Group (W3C) |
| **R&E** | Research and Education |
| **R&S** | Release and Scholarship |
| **RA21** | Resource Access for the 21st Century |
| **RADIUS** | Remote Authentication Dial-In User Service |
| **REFEDS** | Research and Education Federations group |
| **REST** | Representational State Transfer |
| **RI** | Research Infrastructure |
| **RO** | Roaming Operator |
| **RP** | Relying Party |
| **SaaS** | Software as a Service |
| **SAML** | Security Assertion Markup Language |
| **SATOSA** | SAML to SAML, a configurable proxy for translating between different authentication protocols such as SAML2, OpenID Connect and OAuth2 |
| **SCI** | Security Collaboration among Infrastructures |
| **SG** | Steering Group |
| **Sirtfi** | Security Incident Response Trust Framework for Federated Identity |
| **SP** | Service Provider |
| **SRAM** | SURF Research Access Management |
| **SRE** | Site Reliability Engineering |
| **SSH** | Secure Shell |
| **SSHOC** | Social Sciences and Humanities Open Cloud |
| **SSP** | SimpleSAMLphp |
| **STM** | Scientific, Technical and Medical |
| **SWAMID** | Swedish Academic Identity Federation |
| **T** | Task |
| **T&I** | Trust and Identity |
| **TIIME** | Trust and Internet Identity Meeting Europe |
| **TIM** | T&I Incubator Mentorship programme |
| **TNC** | The Networking Conference |
| **TRL** | Technology Readiness Level |

| | |
|---|---|
| **UI** | User Interface |
| **UX** | User Experience |
| **VESPA** | Virtual European Solar and Planetary Access |
| **VO** | Virtual Organisation |
| **W3C** | World Wide Web Consortium |
| **WCAG** | Web Content Accessibility Guidelines |
| **WG** | Working Group |
| **WISE** | Wise Information Security for Collaborating e-Infrastructures |
| **WP** | Work Package |
| **WP1** | Work Package 1 Project Management |
| **WP2** | Work Package 2 Marcomms, Events and Policy Engagement |
| **WP3** | Work Package 3 User and Stakeholder Engagement |
| **WP5** | Work Package 5 Trust and Identity Services Evolution and Delivery |
| **WP9** | Work Package 9 Operations Support |