

20-04-2026

Deliverable GN5-2 D5.1

Report on Trust and Identity Services, Enabling Communities and Incubator

Contractual Date:	27-02-2026
Actual Date:	20-04-2026
Grant Agreement No.:	101194278
Work Package:	WP5
Task Item:	T0
Nature of Deliverable:	R
Dissemination Level:	PU
Lead Partner:	GÉANT and SURF
Document ID:	GN5-2-26-BD1CC7
Authors:	M. Kremers (SURF), I. Sidorova (GÉANT Association), P. Dekkers (SURF), D. Vagheti (GARR), C. Kanellopoulous (GÉANT Association), M. Williams (GÉANT Association), A. Todosijević (AMRES), M. Héder (MTA Sztaki), C. Dreef (GÉANT)

Abstract

This document reports on the Trust and Identity service families operated in GN5-2 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 1 January 2025 to 31 December 2025.

Contents

Executive Summary	1
1 Introduction	2
2 eduroam	4
2.1 Service Description	4
2.2 Uptake	5
2.3 Key Performance Indicators	7
2.4 Activities and Issues	7
2.4.1 Operations and Outreach	7
2.4.2 Support	8
3 eduGAIN	9
3.1 Service Description	10
3.2 Uptake	11
3.3 Key Performance Indicators	15
3.4 Activities and Issues	17
3.4.1 eduGAIN OT and Core Services	17
3.4.2 eduGAIN Support Team	18
3.4.3 eduGAIN Supporting Services and Development	18
3.4.4 OpenID Federation Pilot	18
3.4.5 eduGAIN CSIRT	19
3.4.6 Federation as a Service	19
3.4.7 SeamlessAccess	20
3.4.8 Training and Outreach	20
4 Core AAI Platform	21
4.1 Service Description	22
4.2 Uptake	23
4.3 Key Performance Indicators	26
4.4 Activities and Issues	27
4.4.1 Team	27
4.4.2 Development and Operations Highlights	27
5 InAcademia	29
5.1 Service Description	29
5.2 Uptake	30
5.3 Key Performance Indicators	33
5.4 Activities and Issues	34
5.4.1 Development and Operations	34

5.4.2	Outreach and Business Development	34
5.4.3	Issues	34
6	Incubator Activities	36
6.1	Key Performance Indicators	37
6.2	TIM Programme	37
6.3	Incubator Outreach Activities	38
6.4	Activities and Issues	39
6.4.1	Cycle 10 Activities (Completed)	40
6.4.2	Cycle 11 Activities (In Progress)	42
7	Enabling Communities	45
7.1	Key Performance Indicators	45
7.2	Activities and Issues	45
7.2.1	Policy and Technology	45
7.2.2	Wallets	46
7.2.3	T&I Outreach	46
8	Conclusions	47
	Glossary	48
	References	50

Figures

Figure 2.1:	Global map of eduroam participants as of the end of the reporting period	6
Figure 2.2:	eduroam core service usage statistics: number of successful authentications per month in 2023, 2024 and 2025 (both national and international authentications are expressed in millions)	6
Figure 3.1:	Global map of eduGAIN participants (orange: participants, blue: candidates)	13
Figure 3.2:	Identity Providers and Service Providers participating in eduGAIN across 2021–25	14
Figure 3.3:	Uptake of entity categories and attributes across 2021–25 – at the end of 2025, 2,026 SPs had implemented Sirtfi, 463 SPs were tagged R&S, and 312 SPs implemented CoCo, while 1,418 IdPs had implemented Sirtfi, 2,125 IdPs support R&S, 882 IdPs support CoCo	15
Figure 4.1:	Core AAI Platform in the R&E federated identity ecosystem	21
Figure 5.1:	Participating identity federations in InAcademia as of the end of December 2025 (created with mapchart.net)	31
Figure 5.2:	Monthly number of InAcademia validations in 2024 and 2025	33
Figure 6.1:	Timeline showing the T&I Incubator cycles across the GN4-3, GN5-1 and GN5-2 projects	39

Tables

Table 2.1: Contact details and information sources for eduroam	4
Table 2.2: eduroam KPIs for the reporting period	7
Table 3.1: Contact details and information sources for eduGAIN	9
Table 3.2: GÉANT partners' identity federations participating in eduGAIN	12
Table 3.3: New eduGAIN federation members	13
Table 3.4: Progress in the implementation of actions for the eduGAIN Baseline Expectations programme	16
Table 3.5: eduGAIN KPI targets and results for the reporting period	17
Table 4.1: Core AAI Platform deployments and status	26
Table 4.2: Core AAI Platform KPIs for the reporting period	26
Table 5.1: Contact details and information sources for InAcademia	29
Table 5.2: InAcademia customer growth over the reporting period	31
Table 5.3: Participating identity federations in InAcademia as of the end of December 2025	32
Table 5.4: InAcademia KPIs for the reporting period	33
Table 6.1: Incubator KPIs as of the end of December 2025	37
Table 6.2: Actions and measures for communicating with interested parties	38
Table 6.3: List of general presentations	39
Table 6.4: Schedule of GN5-2 Incubator cycles	40
Table 7.1: Enabling Communities KPIs at the end of the reporting period	45

Executive Summary

This document reports on the services delivered by Work Package 5 Trust and Identity (WP5) and related Incubator and outreach activities. WP5 is responsible for managing the Trust and Identity (T&I) services portfolio, which encompasses the operation and enhancement of existing services and the development of new services (if new use cases emerge). This is the first service report of GN5-2 and covers the activities and status of the services and related activities from 1 January 2025 to 31 December 2025.

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, comprising the Core AAI platform, which evolved from the eduTEAMS services in 2023, and InAcademia, the affiliation validation service.

Each service has an appointed service owner who is responsible for service delivery and manages the work of the service teams in order to ensure effective, efficient and secure service operation, development and support. During the reporting period, all services operated to a very high standard and consistently exceeded their key performance indicators across both availability and service uptake.

eduroam maintained exceptional operational performance, achieving 100.0% availability of at least one top-level roaming server throughout the year. Uptake also grew significantly, with over 1.5 billion international eduroam authentications in 2025 – an increase of 11% on the previous year. Development of the service continued through enhancements to diagnostic tools, CAT, geteduroam, and ongoing work on OpenRoaming integration.

eduGAIN demonstrated strong progress, with its Metadata Distribution Service attaining 100% availability. Technical advances included launching an OpenID Federation pilot that attracted participation from numerous identity federations, opening the way for the adoption of next-generation identity federation technologies.

The Core AAI Platform continued its expansion as a foundational component for advanced federated identity use cases, supporting key European R&E initiatives such as EuroHPC and EOSC. Operational enhancements and improved scalability were delivered through infrastructure modernisation. MyAccessID was selected as the identity layer for the new EuroHPC Federated Platform, demonstrating the effectiveness of GÉANT's federated identity capabilities in supporting secure and interoperable research infrastructures.

InAcademia saw steady uptake among both community and commercial users and achieved service availability of 99.99%. Strategic outreach and new merchant onboarding continued throughout the period, along with engagement activities with national identity federations to broaden awareness and drive future adoption.

The T&I Incubator completed its tenth activity cycle and launched the eleventh, onboarding double the targeted number of topics. Work spanned areas such as verifiable credentials, identity security research, accessibility of digital wallets, and tooling for emerging standards. Enabling Communities activities complemented this innovation by strengthening engagement with research communities, standardisation bodies and national stakeholders, and by shaping policy, terminology, and interoperability approaches for digital identity ecosystems. The (annual) CTO workshop in November 2025 continued as a venue for discussion with the GÉANT membership on the strategic direction of the GÉANT T&I area. 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 to date confirm the services' success, WP5 will continue its programme of development and innovation of both existing and new services to ensure this level of achievement is maintained and the community's needs continue to be met.

1 Introduction

Trust and Identity (T&I) services underpin and enable research and education (R&E) collaboration across Europe and the world. The R&E community relies on a trustworthy and secure global authentication infrastructure, where users are authorised to access resources based on the information received from their home organisation (typically a university or NREN) and/or a collaboration, and on the resource policy.

GN5-2 Work Package 5 Trust and Identity (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 WP5 contains the following:

- **eduroam:** Provides a secure, worldwide roaming access service for the international R&E 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 a pilot, eduroam Managed Service Provider (SP).
- **eduGAIN:** Interconnects identity federations around the world, simplifying access to content, services and resources for the global R&E community. The service includes delivery of core global infrastructure (Metadata Aggregator (MDA)) and a set of supporting services (a technical site with eduGAIN check-in tools, entities database, F-Ticks and eduGAIN Reporting).
- **Core AAI Platform:** A platform to realise solutions for advanced federated identity use cases in R&E. The Core AAI Platform enables R&E 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 the development of advanced solutions while reducing complexity. Notable services built on top of the Core AAI Platform include MyAccessID, MyAcademicID, EOSC AAI, GÉANT AAI and the eduTEAMS services. Alongside these, there are a number of bespoke service instances for Research Infrastructures (RIs) based on the Core AAI Platform; those are listed in Table 4.1.
- **InAcademia:** Gives service providers 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 (where 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 T&I Incubator and the Enabling Communities outreach activities:

- The Incubator (WP5 Task 5) aims to develop, foster and mature new ideas in the Trust and Identity space in research and education.
- The outreach activities, under Task 6 Enabling Communities, form a bi-directional channel with key T&I stakeholders to understand their needs and obtain feedback on the work done within T&I 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 1 January 2025 to 31 December 2025. For each service and activity, the document presents a summary description; contact details; data on uptake, usage and key performance indicators (KPIs) where applicable; and a summary of key activities and any issues encountered in the reporting period.

2 eduroam

Service Owner: Paul Dekkers (SURF)

eduroam (education roaming) [1] provides a secure, worldwide roaming access service for the international R&E 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 across the world. Its architecture is based on a specific set of technologies and regulated by a number of agreements that, when combined, provide the essential eduroam user experience: ‘open your laptop and be online’.

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 KPI.

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

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. Authorisation to access local network resources is granted by the visited network. This allows 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 that agree to a set of defined organisational and technical requirements by signing and following the global eduroam Compliance Statement [2] (which includes the most

important standards and requirements for operating eduroam), as well as the additional European eduroam Policy Declaration [3], which is based on the eduroam Service Definition [4]. In addition, GÉANT operates the overarching global infrastructure that connects the members of the Confederation. 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 (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**) [5] with information about and provided by participating National Roaming Operators (NROs) and institutions.
- Monitoring and metering tools (**F-Ticks**) [6], which are used to monitor the availability of NRO eduroam infrastructure and for collecting and processing eduroam authentication statistics. The collection and processing of such data is undertaken in line with eduroam's privacy-preserving approach.
- A Configuration Assistant Tool (**CAT**) [7], which enables institution administrators to create eduroam installers configured for their local (home institution) setup. End users can then download these installers to set up devices they wish to use for eduroam access with minimal configuration required. CAT also provides tools for NROs for purposes such as diagnostics or for the issuing of certificates used in the authentication infrastructure.
- **eduroam Managed IdP** [8], a Software-as-a-Service (SaaS) offering for institutions that encompasses the running of the 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 [9] (the portal software is institution-specific via in-app links).
- **eduroam Managed SP (pilot)** [10], 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, such as contributing to the new EAP method implementation, and 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. The development and deployment of eduroam is performed in accordance with the roadmap published on the WP5 wiki [11], as outlined in Section 2.4.

2.2 Uptake

eduroam uptake data is provided on the eduroam Monitor site [12]. At the end of this reporting period, 38 GN5-2 partners use the eduroam service. However, the number of NROs in Europe is 51, as these cover other European countries in addition to partner countries.

On a global scale, 112 territories participate in the eduroam service (the dark-coloured areas in Figure 2.1 below), of which 51 are in Europe. Of these NROs, 102 have provided detailed data on the distribution of the eduroam service at a national level, which at the end of the reporting period totalled over 15,320 participating institutions (7,184 in Europe) and 45,154 service locations for eduroam globally.

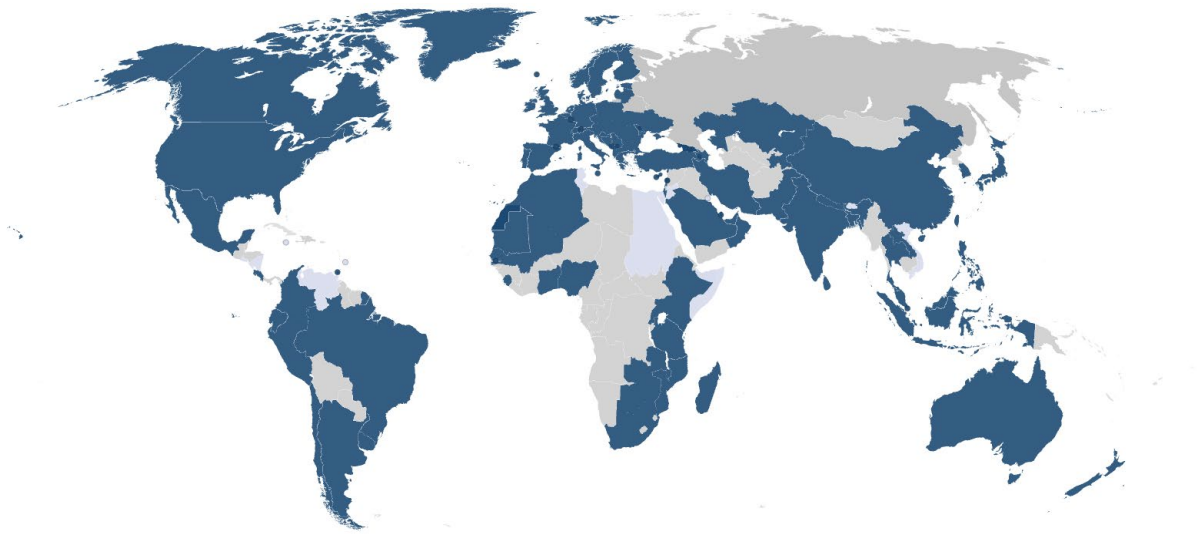


Figure 2.1: Global map of eduroam participants as of the end of the reporting period

The number of successful national and international authentications per month from 1 January 2025 to 31 December 2025 is shown in Figure 2.2 below, together with national and international cycle authentications in 2023 and 2024 for comparison. The seasonal variation in the data is due to the academic cycle throughout the year.

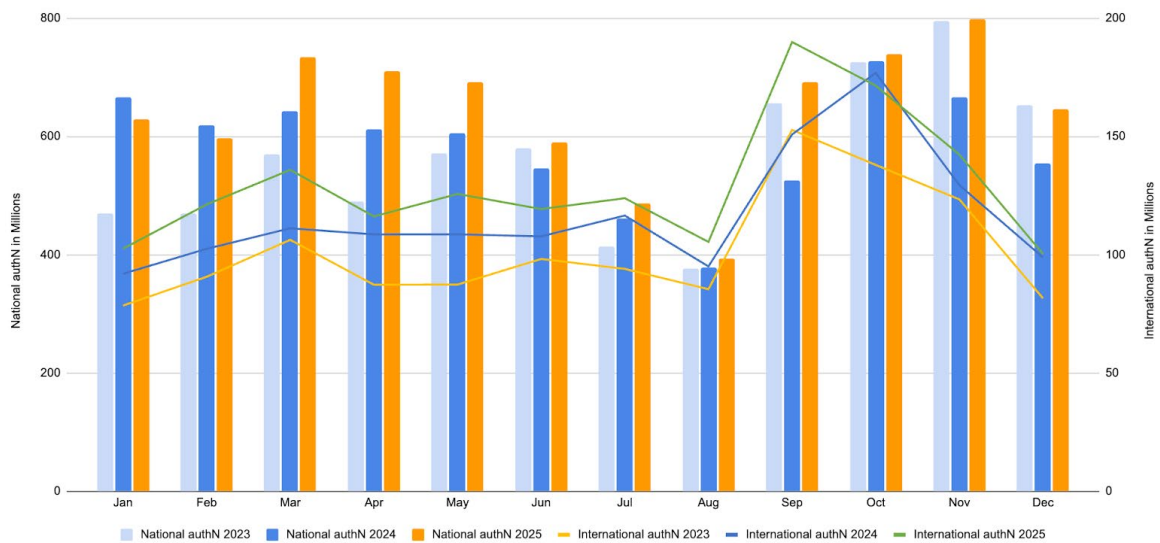


Figure 2.2: eduroam core service usage statistics: number of successful authentications per month in 2023, 2024 and 2025 (both national and international authentications are expressed in millions)

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

- The national authentication figures are 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 [13].)
- International authentications are calculated using the total number of successful international (cross-border) authentications counted in the logs of ETLRs.

2.3 Key Performance Indicators

The KPIs for eduroam shown in the following table measure the availability of its core service (European Top-Level RADIUS servers), and eduroam service uptake measured by the number of international authentications. The following table shows that the services ran with at least one top-level roaming server 100% available, therefore exceeding the set target.

KPI	Baseline (start of GN5-2)	Target (end of GN5-2)	Achieved result (by end of reporting period)
European Top-Level RADIUS (ETLR) availability	99.9%	99.9%	100.0%
Number of international authentications	1.40 billion (2024)	5% annual increase	1.55 billion from January 2025 – December 2025 11% increase

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 SP.

While the new eduroam policy documents have been finalised and approved by the Global eduroam Governance Committee (GeGC), signature of the new policy is ongoing globally. Most countries in Europe have signed the eduroam Compliance Statement, with growing numbers outside of Europe.

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 open to a larger global audience.

The following subsections detail the additional activities carried out in the reporting period.

2.4.1 Operations and Outreach

Operations activities of all core and supporting services progressed as usual.

During the reporting period, the team prepared and released new updated versions of the geteduroam apps for various platforms. Work continues on the release of the macOS client for geteduroam, with the app currently pending in the Apple review process despite numerous interactions with Apple. This is expected to be resolved in the next phase of the project. Additionally, a lot of work was done to improve the geteduroam end-user portal, currently in beta testing, to prepare for a more widespread roll-out in the future.

The team organised a successful mobility day as a side event [\[14\]](#) at TNC25 in Brighton, at which the current status of the eduroam service was discussed, including the latest features of eduroam CAT, ideas for mapping efforts in eduroam and OpenRoaming, and security challenges, alongside industry developments affecting eduroam.

Since eduroam is a member of the Wi-Fi Alliance, the eduroam team continues to monitor Wi-Fi Alliance activities relevant to eduroam and share experiences.

Throughout 2025, there was important work ongoing in the Internet Engineering Task Force (IETF) on improvements to and innovation of the RADIUS protocol [15]. At the end of the reporting period, this has reached the final stages and is ready to become an official standard. This is very relevant for the eduroam infrastructure, and the eduroam team shared insights and experiences with others in the IETF on this topic, especially on deprecating legacy cryptographic elements and improving protocol security, as eduroam protects some metadata better than traditional RADIUS.

Also in the reporting period, the first RADIUS conference was held, with participation by the eduroam team in discussions on the challenges to scaling RADIUS infrastructure [16]. Some improvements to the RADIUS protocol were worked on, and as of the end of the reporting period, are seeing their first implementations and tests.

The eduroam team continues to be a member of the Wireless Broadband Alliance (WBA) and participates in working groups such as those for OpenRoaming. As a part of OpenRoaming, the team provides gateways between eduroam and OpenRoaming for NROs and institutions to use (on an opt-in basis) to make it easier to be a part of both federations. A lot of standardisation work is also being done in the WBA, which continues to be an excellent forum to meet colleagues in the industry and discuss the challenges faced by eduroam.

2.4.2 Support

All 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 eduroam user support to visiting users. The Operations Team (OT) primarily provides support to NROs globally, 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 the 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. There is a Slack community for eduroam members, with specific (open and closed) groups to discuss topics like OpenRoaming, ongoing conferences, geteduroam, CAT, NRO support, new Wi-Fi standards, authentication mechanisms and other discussions relevant to eduroam.

In addition to the above, website and wiki content were regularly updated during the reporting period.

3 eduGAIN

Service Owner: Davide Vagheti (GARR)

eduGAIN [17] is one of GÉANT’s key T&I services, allowing identities issued by trusted organisations (Identity Providers) to be used to simply and securely access available web content and services (Service Providers) worldwide. 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 can authenticate at their home institution’s IdP to collaborate on their specific thematic areas.
 - Students log in at their home institution’s IdP to access online learning material.

A selection of user stories is available on the eduGAIN website at [18].

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 for the eduGAIN Metadata Distribution Service, while the eduGAIN Baseline Expectations programme [19] KPI has reached 31.86% of entities and federations that pass the requirements (the target for the end of the project is 40%, so this progress is significantly ahead of schedule).

Moreover, during the reporting period the eduGAIN Core Services staging site at GARR was promoted to full backup, therefore eduGAIN can now count on two operational sites: the master site at PCSS and the backup site at GARR. Finally, a noteworthy OpenID Federation pilot was begun during the reporting period in order to modernise the available technological profile in eduGAIN.

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 the secure and privacy-preserving exchange of information (metadata) between IdPs and SPs that takes place according to the agreed rules in the eduGAIN Policy Framework [\[20\]](#).

The eduGAIN Policy Framework details the administrative and technical standards that all participating 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 members of the global eduGAIN interfederation, which is formed of autonomous identity federations that agree to a set of defined organisational requirements by signing and following the eduGAIN Policy Framework Declaration and accompanying eduGAIN SAML Profile [\[21\]](#).

The eduGAIN service is governed by the eduGAIN Steering Committee (SC), 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)** – an 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 Aggregator 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** – 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)** – a monitoring service available in eduGAIN for IdPs that tests their actual readiness for eduGAIN, i.e., whether they consume eduGAIN metadata.
- **eduGAIN Access Check (EAC)** – a tool that allows administrators of SPs registered in the eduGAIN interfederation to safely test their service behaviour.
- **eduGAIN Attribute Release Check (EARC)** – a tool that allows IdP administrators to test their attribute release policies.

- **CoCo monitor** – the GÉANT Code of Conduct (CoCo) monitoring service testing for adherence to the CoCo version 1.0 and 2.0 specifications.
- **eduGAIN Reporting** [22] (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 Research and Education FEDerations (REFEDS) standards with an intuitive and visually appealing interface.
- **F-Ticks** [23] – a tool that provides a central collector and visualisation for authentication statistics sent by eduGAIN participants.

The further development of eduGAIN with new features and 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 [24].

3.2 Uptake

Users of the eduGAIN service are listed on the status page of the eduGAIN technical website [25]. At the end of the reporting period, eduGAIN had 83 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).

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
Greece	GRNET
Hungary	eduld.hu
Iceland	WAYF

Country	Identity Federation
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: GÉANT partners' identity federations participating in eduGAIN

New eduGAIN members during the reporting period are listed in the following table.

Country or Region	Identity Federation
Became an eduGAIN member and started supplying metadata:	
Burkina Faso	Burkina Faso Identity Federation
Ghana	GARNET Identity Federation
Malawi	MAREN
Tanzania	TERNET IF
Togo	eduID.tg

Table 3.3: New eduGAIN federation members

The following figure shows the global map of eduGAIN participants.

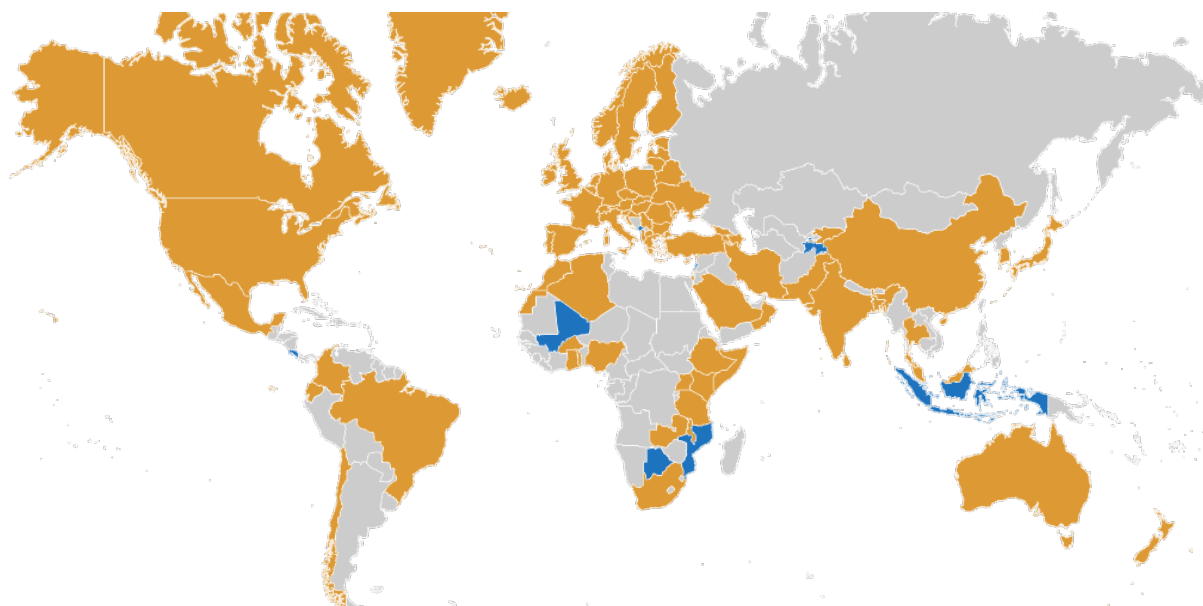


Figure 3.1: Global map of eduGAIN participants (orange: participants, blue: candidates)

At the end of the reporting period, eduGAIN was providing metadata containing 10,108 entities, of which 6,202 are IdPs and 3,906 are SPs. As shown in the following Figure 3.2, this represents 2.5% growth in the sum of IdPs and a 7% increase in SPs over the course of the reporting period.

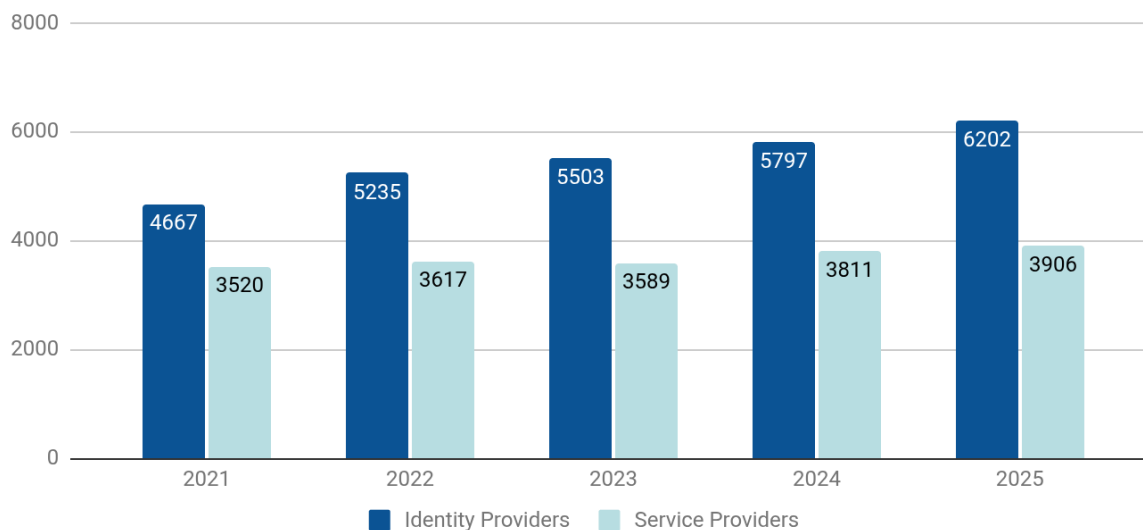


Figure 3.2: Identity Providers and Service Providers participating in eduGAIN across 2021–25

Entity categories and entity attributes are the means for IdPs and SPs to declare that they either comply with the requirements defined by these categories, or that they support them, in order to increase the level of interoperability, trust and security. The ultimate goal is to improve attribute release by IdPs, as this is one of the biggest barriers that SPs face. The entity categories, attributes and frameworks for use in the global R&E T&I sector are specified by REFEDS to 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:

- Research and Scholarship (R&S) [\[26\]](#)
- Security Incident Response Trust Framework for Federated Identity (Sirtfi) [\[27\]](#)
- Code of Conduct (CoCo) versions 1.0 and 2.0 [\[28\]](#)
- Anonymous Access [\[29\]](#)
- Pseudonymous Access [\[30\]](#)
- Personalized Access [\[31\]](#)

Figure 3.3 shows the trend in adoption of REFEDS entity categories and attributes by IdPs and SPs in eduGAIN. The last three entity categories from the list above are excluded as these were defined only recently, and while adoption rates are growing, this is still the very early stages.

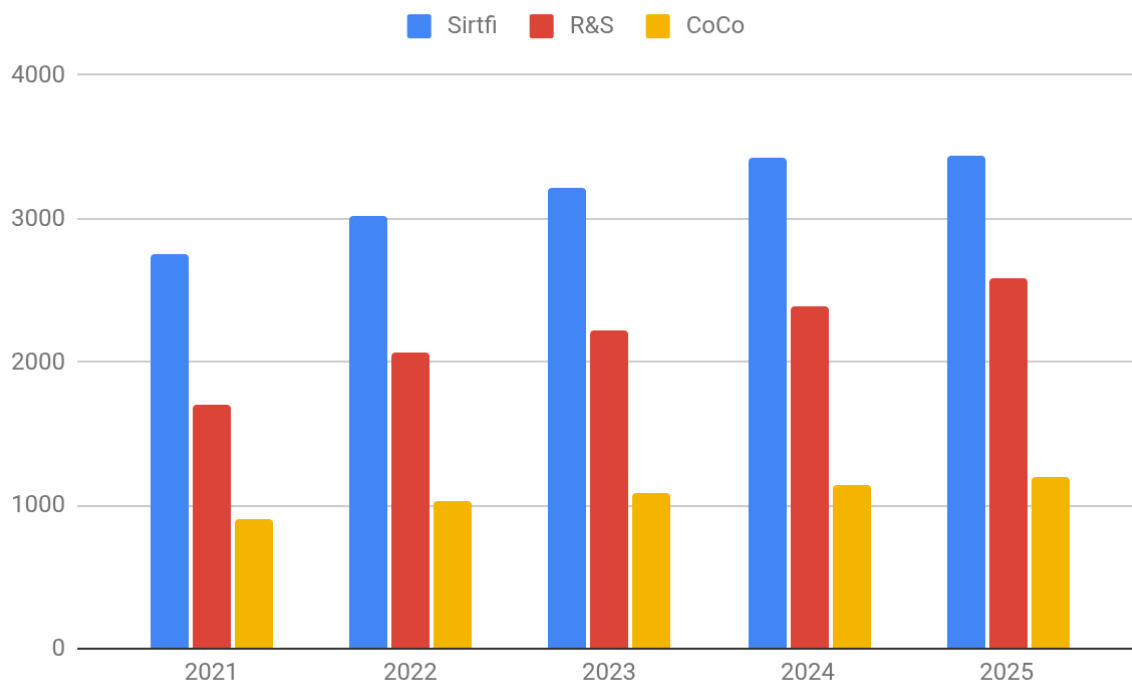


Figure 3.3: Uptake of entity categories and attributes across 2021–25 – at the end of 2025, 2,026 SPs had implemented Sirtfi, 463 SPs were tagged R&S, and 312 SPs implemented CoCo, while 1,418 IdPs had implemented Sirtfi, 2,125 IdPs support R&S, 882 IdPs support CoCo

3.3 Key Performance Indicators

The eduGAIN Futures Working Group [32] has defined a set of recommendations [33] for the implementation of the REFEDS Baseline Expectations [34], accepted by the eduGAIN Steering Group. The following table outlines the specific actions produced for each recommendation, along with each action’s percentage of contribution to the overall value of the eduGAIN Baseline Expectations programme KPI. This KPI, shown in Table 3.5, is calculated on the basis of the progress on implementing these recommendations, as detailed in the following table.

Recommendation	REFEDS Baseline Expectation	Action	KPI %	Notes	Current (M12)
1.1 - Contacts	FO2	Require and periodically check security contact	10	Based on annual communication challenges run by the eduGAIN CSIRT	81/83 (97.6%)
1.1 - Contacts	FO2	Periodically check technical and management contact	10	In progress	N/A
1.2 - Entity filtering	FO1	Implement entity filtering in the eduGAIN MDS	10	In progress	N/A
1.2 - Entity filtering	FO1	Update the technological profiles to define entity requirements	10	In progress	N/A
1.3 - eduGAIN CSIRT	FO4	Implement and promote the action of the eduGAIN CSIRT	10	eduGAIN CSIRT established in 2023	Done (100%)
1.4 - Profiles	FO4	Add requirements to the Technological Profiles to improve interoperability	10	Yet to be implemented	N/A
1.4 - Metadata publication	FO4	Implement eduGAIN requirements for upstream and downstream metadata publishing and refresh	10	Yet to be implemented	N/A
1.5 - Support REFEDS Specification	FO5	Require security contacts per each entity	10	Based on current security contacts per entity in eduGAIN	4512/10126 (44.6%)
1.5 - Support REFEDS Specification	FO5	Require Sirtfi per each entity	5	Based on current Sirtfi adoption per entity in eduGAIN	3577/10126 (35%)
1.5 - Support REFEDS Specification	FO5	Require a privacy policy per each entity	5	Based on current PrivacyStatementURL per entity in eduGAIN	4202/10126 (41.4%)
1.5 - Support REFEDS Specification	FO5	Require a baseline assurance support per each entity	5	Yet to be implemented	N/A
N/A	FO6	Federations collaborate to promote realisation of baseline expectations	5	Based on federation participation in working groups, etc.	N/A
		Weight	100%	Measured	31.86%

Table 3.4: Progress in the implementation of actions for the eduGAIN Baseline Expectations programme

The KPIs for the eduGAIN service measured over the reporting period are shown in the table below.

KPI	Baseline	Target	Achieved Result (by M12)
eduGAIN: MDS availability*	99.5%	99.5%	100.0%
eduGAIN: Start the eduGAIN Baseline Expectations programme with an initial target of 40% of entities that will pass the requirements (by the end of GN5-2)	20.1%	40% of entities to pass requirements by end of GN5-2 project	31.86%

Note:

- * The availability of the eduGAIN MDS is measured on a monthly basis, reporting the lowest value with the exclusion of maintenance windows.

Table 3.5: eduGAIN KPI targets and results for the reporting period

3.4 Activities and Issues

The eduGAIN core services were operated to a very high standard during the reporting period, with performance exceeding the targets set. Day-to-day operations relating to the management of the identity federations and core services were performed by the eduGAIN OT, while supporting services operations were handled by dedicated sub-teams. 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 the coordination of interfederation security incident responses.

During the reporting period, the eduGAIN Service Owner and Secretariat participated regularly in the eduGAIN Steering Committee meetings in order to finalise the eduGAIN Strategy document. This document defines the mission, vision and values of eduGAIN and sets the long-term goals to support the implementation of the REFEDS Baseline Expectations in eduGAIN. The eduGAIN Strategy document [35] was submitted to the eduGAIN Assembly for consultation and finally published at the beginning of 2025.

The following subsections cover activities of note during the reporting period.

3.4.1 eduGAIN OT and Core Services

The eduGAIN OT implemented the new onboarding process (based on the federated digital signature of the eduGAIN Declaration) on the technical website and introduced a new "invited for signing" status for candidates.

During the reporting period, the eduGAIN OT engaged in the following:

- Deployed a new updated version of the eduGAIN Core Services (Metadata Distribution System, the technical site, database, and validator) fully based on Ansible and Docker at both the master PCSS site and the GARR backup site.
- Updated the eduGAIN metadata signing system with the deployment of new hardware security module (HSM) nodes by SUNET.
- Activated the new HSM-based eduGAIN metadata signing system at the eduGAIN Core Services backup site at GARR.

3.4.2 eduGAIN Support Team

The eduGAIN service organisation model assumes that the IdP, 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 themselves 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.

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, eduGAIN Support Team activities were as follows:

- The current Team Lead from ASNET-AM coordinated the eduGAIN Support Team.
- All shifts in the Support Team's weekly rota were covered without any exceptions.
- The Support Team received and processed 48 valid eduGAIN support requests. Examples included:
 - Federation information change requests.
 - Federation candidate proposals.
 - Issues regarding interoperability between certain SPs and IdPs.
 - Resolving issues reported by eduGAIN support tools.
- The eduGAIN support documentation and knowledge base was continuously verified and improved, being used to feed the public knowledge base available to federation operators, SPs and IdPs [36].

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

3.4.3 eduGAIN Supporting Services and Development

During the reporting period, the eduGAIN Connectivity Check Service (ECCS), which is maintained on the eduGAIN core services infrastructure, was updated in order to better assess the availability of the eduGAIN IdPs.

Work continues on a complete revision of the eduGAIN Attribute Release Check, with the adoption of a new engine based on the SWAMID attribute release check. The new eduGAIN Attribute Release Check will be deployed in Q2 2026.

The other eduGAIN checking tools – eduGAIN Access Check (EAC) and CoCo Monitor – have been updated and maintained in full operation.

3.4.4 OpenID Federation Pilot

The eduGAIN OpenID Federation Pilot [37] officially started at the end of July 2025. The eduGAIN Service Team set up the pilot environment comprising:

- The eduGAIN Pilot OpenID Federation Trust Anchor
- Two OpenID Federation subordinate federations
- An OpenID Federation OpenID Connect (OIDC) Provider based on Shibboleth IdP
- An OpenID Federation Relying Party based on OpenID Federation Forward Auth (OFFA)

The eduGAIN OpenID Federation Pilot was warmly received by the community. By the end of the reporting period, a notable 12 eduGAIN members were already participating in the work, 6 of which have registered their Trust Anchor as well as OpenID Federation-enabled OIDC Providers and Relying Party:

- AAF
- UK Federation
- SWAMID
- RCTSaai
- CAF
- ArnesAAI
- DFN-AAI
- Haka
- eduid.hu
- IDEM
- Belnet Federation
- InCommon

3.4.5 eduGAIN CSIRT

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

- Intelligence on security incidents of interest for the R&E community.
- Management of security-related tickets (41 tickets in 2025 related to incidents, vulnerabilities, security contacts).
- Security threat evaluation for known software vulnerabilities.
- Communication Challenges to check the availability of the federations' security contacts. The results of the last Communication Challenges are available on the eduGAIN Wiki [\[38\]](#).
- The eduGAIN CSIRT tabletop security exercise on federated incident-handling in eduGAIN was run by eduGAIN CSIRT team members in March 2025 at the International Symposium on Grids & Clouds (ISGC) in Taiwan.

3.4.6 Federation as a Service

Federation as a Service (FaaS) was in continuous operation throughout the reporting period, with the FaaS software suite updated to the latest available versions throughout the period.

Currently, 4 NRENs are using FaaS to run their identity federations and participate in eduGAIN:

- MARnet (AAIEduMk, North Macedonia) – 4 IdPs, 52 SPs
- ASNET (AFIRE, Armenia) – 2 IdPs, 1 SP
- CYPNET (CyNet Identity Federation, Cyprus) – 10 IdPs, 1 SP
- University of Malta (RicerkaNET Identity Federation, Malta) – 1 IdP

3.4.7 SeamlessAccess

GÉANT continued its participation in the SeamlessAccess consortium, comprising the International Association of STM Publishers, National Information Standards Organization (NISO), Internet2 and GÉANT. This coalition was formed to collaborate on providing SeamlessAccess, which implements the recommendations from the RA21 initiative [39]. 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.

The GÉANT project participates in this coalition via representatives in the technical and governance steering groups, and by providing operational capabilities and a product manager for the service.

During the reporting period, the service continued to be operated by the SUNET NOC, which offers 24/7 support and deploys new versions of the software upon request.

From the product management perspective, the following activities took place during the reporting period:

- The UI saw continuous improvement for accessibility and usability to ensure compliance with the Web Content Accessibility Guidelines (WCAG) 2.2 AA/AAA [40] and the European Accessibility Act [41].
- Development of new features:
 - IdP filtering, allowing SPs to locally add non-federated login to their SeamlessAccess discovery flow.
 - IdP pinning, with which SPs can locally present options tailored to their users. This allows users to select their IdP more quickly to get faster, more streamlined access to the SP's content.
- Updates to infrastructure operations that include:
 - More efficient MDQ service
 - Improvements to deployments:
 - Redundancy during deployment
 - Enhanced deployment operation schedule
 - Monitoring of CDN during deployment
- Product management work was carried out in the REFEDS SeamlessAccess Trustinfo Metadata Working Group to develop specifications that will enable federation operators to make use of the aforementioned IdP filtering features.
- A version of SeamlessAccess was developed as part of the GN5-2 T&I Incubator (see section 6.4.1). This version is compatible with the new identity federation technology, OpenID Federation [42].

3.4.8 Training and Outreach

In the reporting period the eduGAIN Service Owner, the eduGAIN Steering Committee Chair and the GN5-2 WP5 Leader participated in the 59th Meeting of the Asia Pacific Advanced Network (APAN59) meeting, held in March 2025 in Japan, delivering two presentations on eduGAIN [43].

The eduGAIN training team held an online meeting dedicated to the African region, in continuation of the in-person training already delivered in 2024, which resulted in five new participants joining eduGAIN from Africa.

Moreover, the training team prepared a new in-person training activity for federation operators to be held in Paris in April 2026, targeting both new and existing federations seeking to train new personnel on federation technologies.

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 R&E 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 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 European high-performance computing (EuroHPC) area, European research infrastructures, and the broader education sector. The following Figure 4.1 illustrates this extensive ecosystem and the Core AAI Platform's place within it.

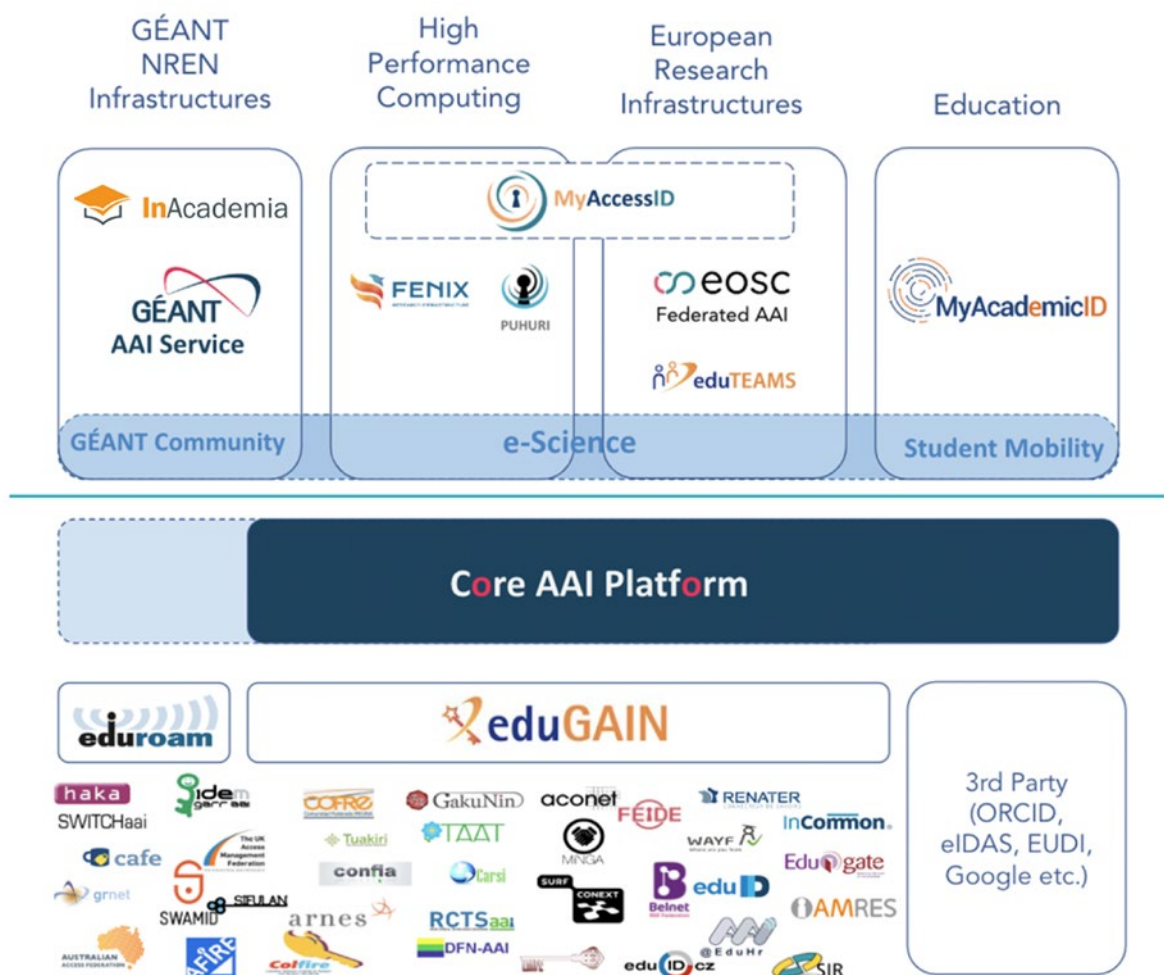


Figure 4.1: Core AAI Platform in the R&E federated identity ecosystem

4.1 Service Description

The Core AAI Platform enables the provision of services that allow R&E 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 while concealing the complexity of dealing with the diverse international landscape of federated identity. It introduces the possibility of providing centralised solutions for more advanced use cases, thus moving complexity away from the edge and removing the need for the specialised expertise required when research infrastructures run their own solutions. The development of the Core AAI Platform follows a strongly agile approach, with frequent releases of software enhancements that address stakeholders' requirements.

The Core AAI Platform implements (and enhances) the AARC Blueprint Architecture [44] and deploys an IdP/SP proxy that allows the 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 use cases explored and implemented during this reporting period include an identity-vetting step-up solution, SSH access based on the federated authentication flows, multi-factor authentication (MFA) capability, and the addition of external IdPs to support users without federated identities.

GN5-2 WP5 funds the development of the Core AAI Platform and engages communities and infrastructures seeking to use its derived services. This engagement includes gathering stakeholders' requirements, reviewing aspects of integration, and embarking on the design and pre-production phase. Operation of the resulting services is funded in certain cases by the GÉANT project (GN5-2 and its predecessors), while others are funded by other projects or infrastructures, as outlined in Table 4.1 in the following section.

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

- **MyAccessID Identity & Access Management (IAM) Service** [45] – The MyAccessID IAM Service was initially the result of WP5's collaboration with the HPC community. Since then, MyAccessID has grown into a solution for research infrastructures and clusters; EuroHPC via the EuroHPC Federation Platform; national HPC systems; and EOSC. MyAccessID provides a unified identity layer, enabling users from various institutions and countries to authenticate and access resources over OIDC and SAML2 through a streamlined, consistent interface. This approach not only enhances the user experience by reducing the need for multiple logins but also strengthens security by implementing federated identity management principles. The MyAccessID IAM solution provides a common identity layer for:
 - **Research infrastructures:** Social Science and Humanities (SSH Open MarketPlace), Photon and Neutron RIs (UmbrellaID AAI).
 - **National research infrastructures:** UK AI Infrastructure and DeIC HPC Access (in progress).
 - **HPC allocation systems and EuroHPC sites:** FENIX RI, Puhuri and Lumi.
 - **EuroHPC Federation Platform:** Development of the EuroHPC Federation Platform, which is using MyAccessID, began in January 2025, with the first phase expected to be delivered in production in April 2026.
 - **EOSC:** EOSC EU Node.

- **GÉANT AAI Service** [46] – The GÉANT AAI Service allows GÉANT services to use federated authentication to identify users from eduGAIN. During the reporting period, WP5 continued supporting the GÉANT IT Services team to migrate existing services from SAML to OpenID Connect, offering a wide range of new capabilities, such as enhanced user and group management, support for the AARC Blueprint Architecture, external identity provider capability (GuestIDP) and EOSC readiness.
- **EOSC AAI Federation** [47] – The goal for the EOSC AAI is to provide the trust mortar to join together the many bricks of the current set of scientific communities, collaborations and infrastructures. The EOSC AAI comprises the AAIs of the science clusters, research infrastructures and e-infrastructure providers brought together through the EOSC AAI Federation.

The MyAccessID service, built on top of the Core AAI Platform and operated by GÉANT, acts as the trust and identity layer for the EOSC AAI Federation. The EOSC AAI Federation continues to expand, with six EOSC nodes connected to MyAccessID in a testing environment and four nodes integrated in production during the reporting period. Further production integrations are ongoing, with additional nodes expected to join as the federation develops.

- **EOSC EU Node** – The EOSC EU Node marked one year of production operation in October 2025, with the EOSC EU Node AAI being built on top of the GÉANT Core AAI Platform. In addition to this robust foundation, the EOSC EU Node leverages MyAccessID as its identity layer. This integration enables users to seamlessly access both EuroHPC and EOSC resources via a single, unified identity. By incorporating MyAccessID, the EOSC EU Node AAI aims to enhance user accessibility across multiple research infrastructures, reducing the need for multiple login credentials and simplifying the authentication process.

This approach supports EOSC's interoperability goals, fostering a connected ecosystem where researchers can engage with resources from different infrastructures through a single, consistent identity layer. This setup not only streamlines access for end-users but also strengthens the security of the federated environment. By ensuring compliance with established identity assurance frameworks, MyAccessID contributes to the trustworthiness and scalability of the EOSC Federation. As the EOSC EU Node progresses, the combined capabilities of the GÉANT Core AAI Platform and MyAccessID will play a crucial role in supporting the EOSC's vision of a collaborative, open, and secure digital research environment across Europe.

- **MyAcademicID** [48] – The MyAcademicID IAM Service provides identity and federated access management for the services of the European Student Card Initiative (ESCI) [49], the services directly supporting the digitisation of Erasmus+ [50] and the European Universities Initiative [51]. These student mobility processes require a number of services throughout the pipeline and need to be able to exchange data about the students. Leveraging the ubiquitous presence of eduGAIN and eIDAS federated identities, MyAcademicID enables connected services to verify students' identities using the academic attributes available via HEI federated logins in combination with students' national eIDs.

4.2 Uptake

Core AAI Platform users are research communities or e-infrastructure providers engaging in international scientific collaborations. They include small, medium and large communities and infrastructures, along with long-tail collaborations.

In the GN5-2 project, the requirements analysis, design, and initial implementation activities are funded via WP5. This is a delicate process necessitating subject-matter, technical, and integration support from the Core AAI Platform team to develop an optimal solution that is integrated not only within the specific service, but within the platform as a whole. This is an ongoing process, as requirements often progress from the relatively simple, targeting a range of use cases, to more complex requirements needed to address specific advanced use cases.

The Core AAI Platform provides the underlying technical stack upon which dedicated AAI service offerings are built, such as FENIX-AAI [52] (>300 registered users), Puhuri/LUMI AAI [53] (>10,000 registered users), MyAccessID IAM [54] (almost 19,000 registered users) and PaNOSC-AAI [55] (almost 1,000 registered users).

The Core AAI Platform shared instance is used by smaller research communities that do not need a dedicated instance, such as LAGO [56], SSHOC-AAI [57] and VESPA [58] (>900 users in total across smaller research communities).

The EuroHPC Federated Platform (EFP) is being developed to provide a secure and interoperable access layer for high-performance computing (HPC) resources across Europe. Within this initiative, GÉANT is responsible for delivering the Authentication & Authorisation Infrastructure (AAI) package, providing federated identity management, single sign-on (SSO), and centralised user management capabilities. The AAI enables users from participating organisations to access EuroHPC services and HPC resources through a unified authentication framework. MyAccessID has been selected by the EuroHPC Joint Undertaking as the platform's identity layer. The adoption of MyAccessID within the EFP architecture demonstrates the effectiveness of GÉANT's federated identity capabilities in supporting secure and interoperable European research infrastructures. The service enables federated authentication and authorisation for users from both academic and non-academic organisations. User identities are verified using passport validation mechanisms and protected through mandatory MFA. The adoption of a common identity service supports compliance with recognised identity assurance frameworks and facilitates interoperability across participating research infrastructures.

The EOSC EU Node AAI is implemented on top of the GÉANT Core AAI Platform and uses MyAccessID as its trust and identity layer within the EOSC AAI Federation. Users authenticate through MyAccessID and are subsequently recognised across EOSC EU Node services and the services of other participating nodes. MyAccessID supports authentication using credentials issued by users' home organisations via eduGAIN, national electronic identity schemes under eIDAS, EU Login, and other trusted identity providers. This federated approach ensures consistent identity assurance, reduces credential fragmentation, and enables cross-infrastructure interoperability across EOSC and related European research initiatives.

During the reporting period, GÉANT submitted a bid for the HORIZON-INFRA-2025-01-EOSC-01 call, with the project proposal under the name EOSC4ALL being selected for implementation. Under EOSC4ALL, GÉANT will, in addition to other activities, be responsible for the AAI EOSC Federating Capability. The EOSC AAI federation will provide authentication and authorisation services across all participating EOSC nodes, ensuring interoperability and secure cross-border access. The service will be designed to scale in line with the anticipated growth of the EOSC ecosystem and to maintain alignment with emerging regulatory and technical frameworks, including eIDAS 2.0 and integration with the European Digital Identity (EUDI) Wallet. As part of the proposal commitments, GÉANT will deliver the AAI Node Core Capability. This includes the provision of an Infrastructure Proxy built on top of the Core AAI platform, as well as Community AAI components. Together, these elements will enable all EOSC members to implement compliant AAI functionality, irrespective of their technical maturity or available resources, thereby supporting harmonised and inclusive participation across the EOSC Federation.

In GN5-2, further efforts are being undertaken to facilitate the integration of research infrastructures with MyAccessID. Building on the experience gained in GN5-1, where the value of shared AAI capabilities became increasingly evident, WP5 continues actively supporting RIs to transition AAI solutions to a common federated approach.

The following table details the current Core AAI Platform deployments and their respective statuses.

Deployment	Status
eduTEAMS Service	Production
CESSDA/SSHOC	Production
eduGAIN	Production
LAGO-AAI – The Latin American Giant Observatory Collaboration AAI	Production
LUTH-HE – Le Laboratoire Univers et Théories, Observatoire de Paris	Production
LITNET	Production
ORP-H2020 – Opticon RadioNet	Pilot
PADC – Paris Astronomical Data Centre	Production
VESPA (EuroPlanet) – Virtual European Solar and Planetary Access	Production
RevLog	Production
ASTRON Science Data Centre (demo)	Production
SUBMERSE	Production
ECLA	Production
EISCAT	Production
DataCube-AAI – Federated DataCube AAI	Production
IVOA – International Virtual Observatory Alliance	Production
IT4Innovations	Production
MBNA – Mircea cel Batran Naval Academy, Romania	Production
SunetDrive	Production
VAMOS spectrometer community	Production
FENIX (*)	Production
PaNOSC (UmbrellaID)	Production
MyAccessID (EuroHPC + Research Infrastructures + EOSC)	Production
Puhuri ISD Proxy	Production
MyAcademicID (Student Mobility) (*)	Production
SRAM (SURF) (*)	Production
GÉANT AAI Service	Production
EOSC Association AAI	Production
EOSC AAI Federation	Production
EOSC EU Node (*)	Production

Deployment	Status
EuroHPC Federated Platform AAI	Pre-production
Estimated Number of Users	
<p>Under the Core AAI Platform, users are linked to a scientific collaboration or project they are involved with. Thus, the number of users varies depending on the specific research collaboration / cluster. In current deployments, the size of communities is expected to span between 3,000 and 50,000 per collaboration. However, some deployments such as MyAcademicID track over 680,000 users.</p>	

Note:

- * These deployments are supported through projects other than GN5-2, 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 GN5-2 project.

Table 4.1: Core AAI Platform deployments and status

4.3 Key Performance Indicators

The Core AAI Platform KPI targets and results for the reporting period are shown in the following table.

KPI	Target	Achieved Result (by end of reporting period)
GÉANT SP Proxy service availability	99.5%	100.0%
GÉANT AAI Service connected services	Connection of 100% of the services developed in the project and which require user authentication	99.3%

Note:

- * The number of services connected to GÉANT AAI that had authentication activity during the reporting period. The GÉANT IT Service team manages and operates services integrated with the GÉANT AAI Service. The Core AAI Platform team's responsibilities include onboarding new services, reconfiguring existing services upon request, and ensuring stable service operations, maintenance, and updates.

Table 4.2: Core AAI Platform KPIs for the reporting period

4.4 Activities and Issues

The following subsections cover notable activities that took place during the reporting period in the context of the Core AAI Platform.

4.4.1 Team

- During the reporting period, one full-time Solutions Architect left the organisation. An immediate recruitment process was initiated and resulted in the selection of a new Solutions Architect in October 2025, who will take up the role in April 2026.
- Recruitment is currently ongoing for:
 - A Site Reliability Engineer (SRE) to replace a team member who departed during the reporting period.
 - An additional Support Team Lead to strengthen operational capacity and ensure service continuity.
- The team held three face-to-face meetings (May, November, and December 2025) to:
 - Align on strategic priorities.
 - Produce the internal development and service delivery roadmap.
 - Address technical challenges and identify improvement areas.
 - Facilitate structured knowledge-sharing across the team.
- The planning and delivery process was further improved during the reporting period through the introduction of a more structured agile approach. This has enhanced prioritisation, increased workload transparency, and optimised the overall allocation of team capacity.

4.4.2 Development and Operations Highlights

During the reporting period, substantial progress was made in advancing the Core AAI Platform. The following key achievements are aligned with strategic objectives, including strengthening platform capabilities, expanding service adoption, and preparing for emerging identity and authentication requirements:

- The service was operated to a high standard, with continuous improvements made to the operational model to enable the increased automation and scalability of deployments. Agile development approaches were used to address requirements efficiently and effectively.
- Maintaining and enhancing the Core AAI Platform:
 - Efforts focused on improving scalability, automation, and security across the platform. Key developments included infrastructure modernisation, delivery of the Unified Identity Management Application (CUID App), MFA, and the External User Identity Provider (Guest IdP).
 - System for Cross-domain Identity Management (SCIM)-based user data management was implemented, improving interoperability and enabling automated user provisioning.
 - Work on supporting OpenID Federation Specification proceeded, with the introduction of support for device code flow, user re-authentication, and remote token introspection compliant with AARC-G052 guidelines.
 - A major infrastructure modernisation programme was completed, migrating 25 deployments from Ansible to Terraform with near-zero downtime, improving operational efficiency, resilience, and maintainability. In addition, a proof of concept for operating the platform on Kubernetes was initiated, focusing on stabilisation to support future scalable deployments.

- Engagement with NRENs, RIs, and stakeholders:
 - Engagement activities with RIs, NRENs, and community forums were carried out for requirements gathering, pilot deployments, and improved interoperability across the EOSC ecosystem. As a result, multiple EOSC Nodes were onboarded to MyAccessID, progressing from acceptance testing to production integration. This enabled SSO and supported cross-node workflow execution.
- Operation, enhancement, and support of Core AAI Services:
 - eduTEAMS continued to support research communities by providing secure, federated collaboration services.
 - The GÉANT AAI Service improved interoperability through the migration of services from SAML to OpenID Connect. The Guest IdP became operational and is actively used within the GÉANT AAI Service to support users without institutional identities.
 - MyAccessID expanded adoption across EOSC Nodes, EuroHPC sites, and national services.
- Exploration of advanced identity capabilities:
 - Work progressed on advanced authentication and trust capabilities, including identity vetting services, federated SSH access, OpenID Federation support, SSH certificate enhancements, and user profile development. These activities support higher-assurance identity use cases and contribute to future alignment with eIDAS 2.0 and the European Digital Identity (EUDI) wallet ecosystems.

5 InAcademia

Service Owner: Michelle Williams (GÉANT Association)

InAcademia [59] became a production service in February 2020. It allows online retailers to easily validate whether a customer is a student or otherwise affiliated with an educational institution, as a member of staff or faculty, for example. For user authentication, InAcademia uses the IdPs available in eduGAIN. It provides an OIDC protocol interface for connecting online retailers with the SAML protocol used within eduGAIN and R&E federations.

The InAcademia service is available in two service models: ‘Commercial Edition’, for online retailers that make a profit from offering services that leverage InAcademia affiliation information, and ‘Community Edition’, for Service Providers (SPs) that are not for profit. These two models are differentiated by pricing strategy. End users and Identity Providers (IdPs) benefit from InAcademia as it provides a privacy-preserving and streamlined way to validate the user’s affiliation, compared with the manual process many online retailers often use, such as requesting personal documents as proof of academic affiliation.

The contact details and information sources for InAcademia are shown in the following table:

Aspect	Link
Website	https://www.inacademia.org
Contact: General information	info@inacademia.org
Contact: 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 with 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 academic affiliation.

Customers of the InAcademia service are typically retailers using e-commerce sales channels (merchants). They are often commercial organisations, although some are not-for-profit organisations (which are entitled to access the service without charge). Customers have to register in accordance with the instructions given on the InAcademia website in order to use the service [60]. Each customer has to agree to specific terms and fees, and can expect service delivery according to the Service Policy published on the InAcademia website [61].

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 includes collaboration with federation operators to resolve issues regarding their member institutions.

From a technical perspective, the InAcademia service is a web service that enables communication between an e-commerce application and the user's home institution's IdP, either for purchase of goods and services, or for registration to access restricted resources. The web service provides a REST interface for clients to request a user validation using the OIDC protocol. InAcademia then communicates with IdPs typically using SAML, processes the information received from the IdP, and returns a privacy-preserving response to the client. 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 DevOps 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. The InAcademia Steering Committee is composed of representatives of most participating federations, meeting at least 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 and supporting services for InAcademia is carried out within the WP5 T4 InAcademia DevOps Team, in collaboration with the Core AAI Platform Development Team. The InAcademia DevOps 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 develop iterative software enhancements that address stakeholders' requirements. Development of InAcademia is performed in accordance with the roadmap published on the WP5 wiki [\[62\]](#).

5.2 Uptake

Whilst InAcademia is technically available across the whole eduGAIN landscape, at the launch of the service, it was decided to limit the geographical scope (see Figure 5.1) of initial usage on the following grounds, which continue to be valid:

- 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.

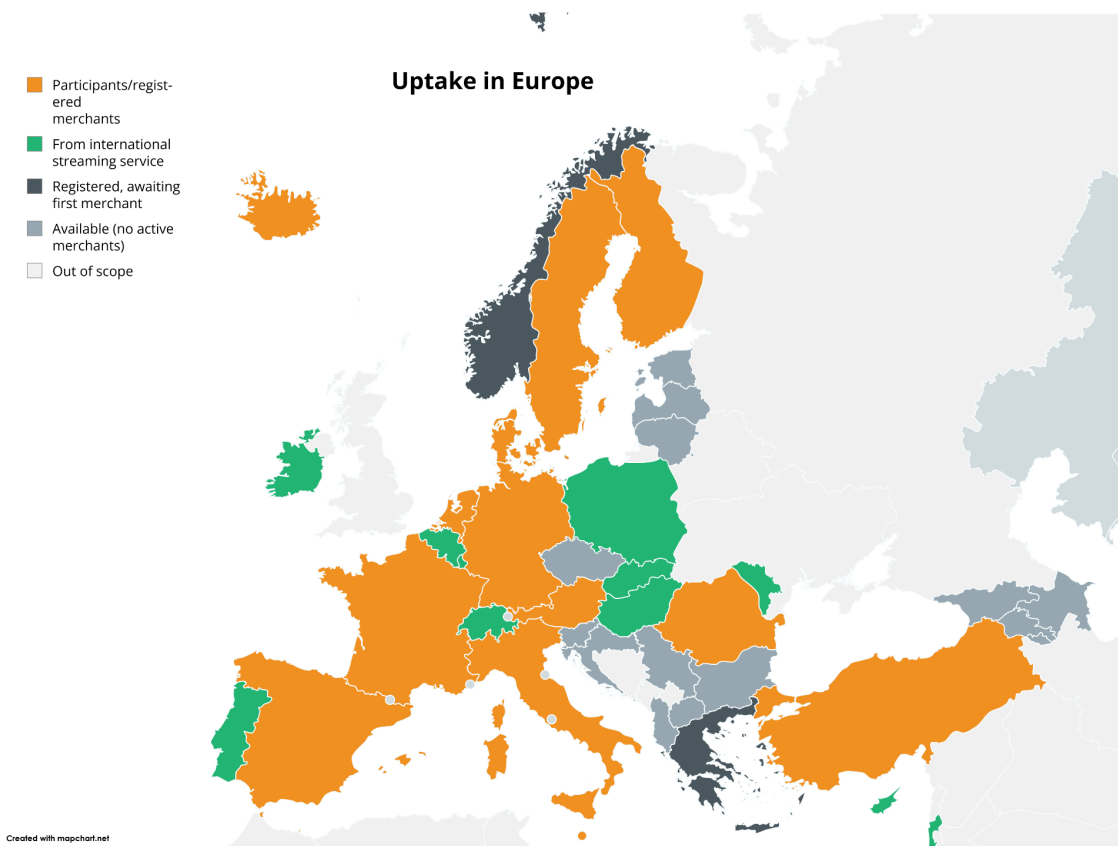


Figure 5.1: Participating identity federations in InAcademia as of the end of December 2025 (created with mapchart.net)

Shown in the following table are the totals of InAcademia customers of both the Commercial and Community Editions at the start and end of the reporting period, demonstrating an increase of 1 customer for both Editions.

Type of customer	Start of reporting period	End of reporting period
Community Edition customers	2	3
Commercial Edition customers	7	8

Table 5.2: InAcademia customer growth over the reporting period

The customers registered with InAcademia in earlier project cycles continued to expand the scope of their use of the service, with the number of validations processed by the service increasing, as shown in the following Figure 5.2. The InAcademia DevOps Team continued to inform federation operators about any misconfigured IdPs identified during the operation of the InAcademia service. Participating identity federations are outlined in the following table.

Country	Identity Federation	Status
Austria	eduID.at	Operational + Steering Committee members
Denmark, Iceland and Greenland	WAYF	Operational + Steering Committee members
Finland	HAKA	Operational
France	Fédération Éducation–Recherche	Operational + Steering Committee members
Germany	DFN AAI	Operational + Steering Committee members
Greece	GRNET	Registered in Federation, pending first merchant
Italy	IDEM	Operational + Steering Committee members
Spain	SIR	Operational + Steering Committee members
Sweden	SWAMID	Operational + Steering Committee members
The Netherlands	SURFconext	Operational + Steering Committee members
Norway	Feide	Registered in Federation, pending first merchant
Turkey	YETKİM	Operational + Steering Committee members
Uganda	RIF	Pathfinding pilot
Malta	RiċerkaNetIdentity Federation	Operational
Additionally from Romanian streaming service [63]:		
Ireland (Edugate), Belgium (Belnet R&E Federation), Switzerland (SwithAAI)		10–50 verifications each
Cyprus (CYNET), Greece (GRNET AAI), Israel (IUCC), Portugal (RDCTSaai), Moldova (LEAF), Slovakia (safeID), Luxembourg (eduID), Poland (PIONIER.Id), Hungary (eduID.hu)		<10 verifications each

Table 5.3: Participating identity federations in InAcademia as of the end of December 2025

The monthly totals of InAcademia validations over the reporting period are presented in Figure 5.2 below, where the percentage of ‘community’ use cases accounts for less than 1% of the total. For comparative analysis, the chart also provides the statistics for the previous year. The highest recorded number is 957,000 validations in October 2025, caused by a combination of the start of the new school year and the onboarding of a new service that was very popular with students.

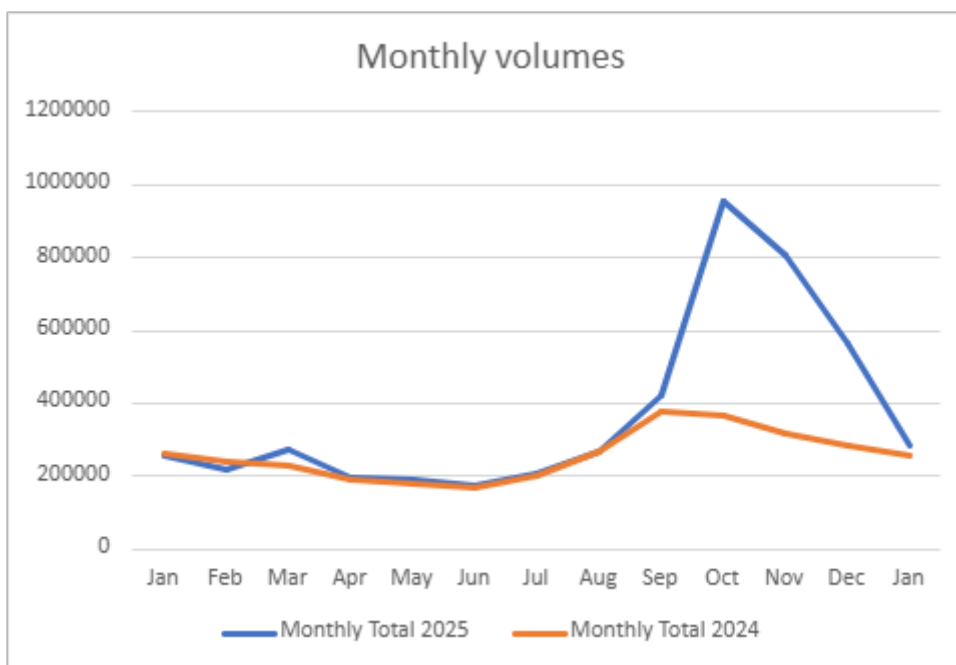


Figure 5.2: Monthly number of InAcademia validations in 2024 and 2025

Uptake of the service continues to be tied to national policy and the profit drivers of commercial services in eduGAIN. During the reporting period, GÉANT and RENU (the Ugandan NREN) continued the pathfinding pilot that seeks to understand how InAcademia could be implemented on a regional basis outside Europe and commenced work to design the implementation.

5.3 Key Performance Indicators

KPI	Baseline (M1 GN5-2)	Target (by end of GN5-2)	Achieved Result (by end of reporting period)
Availability of the InAcademia nodes	99.5%	99.5%	99.99%
InAcademia service uptake: number of national federations participating* in the service	9	15	13

Note:

- * Defined as: actively promoting the service, assisting merchant migrations to the service, and/or Steering Committee members

Table 5.4: InAcademia KPIs for the reporting period

5.4 Activities and Issues

Activities in the reporting period included development and operations, outreach, and business development.

5.4.1 Development and Operations

New software releases during the period, all of which ensure the product is well maintained, included:

- SVS 4.6.3, March 2025: Introduced support for SATOSA 8.5.1 and pysaml2 7.5.2.
- SVS 4.6.5, November 2025: Introduced support for pyop 3.4.2 and minor enhancements.
- Student Discount for WooCommerce versions 1.0.1 to 1.0.6: These updates brought the WordPress plugin's code base into line with security patches to its three underlying software libraries.

Additional effort was spent on supporting a pilot operated by SURF to use InAcademia as an underlying service to allow researchers to verify their academic affiliation for display on Mastodon profiles, enabling the curation of social media content by university libraries.

5.4.2 Outreach and Business Development

Wide-scale community engagement took place during the reporting period to increase uptake and usage, and ensure that federation operators and the NREN community are on board with the direction the service is taking:

- Three InAcademia Steering Committee meetings were held.
- Bilateral engagement was carried out with federations interested in participating in InAcademia, with more detailed conversations undertaken with:
 - Feide/Norway – A new item was published to raise awareness amongst Feide members.
 - Ireland – The team investigated parallels between services offered in Ireland and how InAcademia could support its use cases.
 - Hungary – Possibilities to increase commercial uptake of InAcademia were explored in collaboration with Pro-M.
 - Czechia – Appetite for formal participation in InAcademia was investigated.
- Supported the SwitchAAI team in publishing content to the Switch website [64] presenting InAcademia as an option for new services.
- Supported IDEM in announcing that all commercial services will be filtered from eduGAIN feeds [65], and the subsequent extension of utilisation by a large student discount marketplace.
- Refreshed the content on the InAcademia website [66], migrating technical content to a separate Docs subdomain [67] in order to improve SEO on the main site.
- Continued working with RENU (the Ugandan NREN) to establish how to offer InAcademia to Ugandan merchants as part of a regional pathfinding pilot.

5.4.3 Issues

There continues to be friction in migrating long-term commercial customers of eduGAIN to InAcademia, as it is perceived as having to pay a fee for reduced functionality (InAcademia limits the personal information released and pseudonymises user data). While many services express interest in using InAcademia, there are challenges in converting this interest into usage, as InAcademia's competitors provide a customer-acquisition service, which involves using student data and/or buying habits as a commodity – something that the InAcademia community is unlikely to support.

Furthermore, making the product visible to the commercial, business-to-business market is challenging as it is a very crowded retail marketing space. Effort continues to be made to address this challenge by presenting the service as a credible solution in both general and targeted marketing activities. Funding was invested in dedicated marketing activities during the reporting period, resulting in some promising leads that are still being worked. The service onboarded two new merchants:

- Onda Ventures V.O.F., is a student startup designed to create a pre-loved/re-commerce service dedicated to students, but has since stopped using InAcademia [\[68\]](#).
- Il Post S.R.L, is an online Italian-language newspaper published since April 2010 [\[69\]](#).

6 Incubator Activities

Task Leaders: Andrijana Todosijević (AMRES) and Mihály Héder (MTA SZTAKI)

The Trust and Identity Incubator (further: ‘T&I Incubator’ or ‘Incubator’) aims to develop, foster and mature new ideas in the T&I space in R&E. The Incubator investigates new technologies, solutions, policies 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 new features for potential adoption in 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 are 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 value by 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 may submit a topic suggestion via the public Call for Ideas page [70]. 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 its introduction in GN4-3 [71], but is continuously improved based on 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 [72] to implement as many topics as possible within a short timeframe. Therefore, GN5-2 is split into multiple cycles, each lasting 7 months. The Incubator currently has two teams (Wallets and OI DFed), which are structured to work on several different activities (4–8) 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 and published, and may then be transferred to the ownership of another party.

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 followed up with a report 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. More than 18 innovations over the lifetime of the incubator have delivered tangible impact on services and the community. However, every outcome delivers value, including the few that do not progress into fully operational solutions, as they provide essential learning, generate research-based evidence, and inform future innovation.

6.1 Key Performance Indicators

The Incubator KPI measures the number of activities (topics) carried out during the GN5-2 project. Table 6.1 shows that the Incubator completed four activities in the first cycle in 2025 and achieved its objective for the project phase. With the next cycle, which started in October 2025, and the start of eight additional activities, this KPI has already been met.

KPI	Baseline (start of GN5-2)	Target	Achieved result (by end of reporting period)
Number of topics that went through the incubator cycles	0	4 topics per project period	Cycle 10: 4 Cycle 11: 8*

Note:

* Cycle 11 will end in May 2026.

Table 6.1: Incubator KPIs as of the end of December 2025

6.2 TIM Programme

Back in GN4-3, as part of its commitment to enable broad engagement with 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 GN5-2 project and ultimately for the European NREN community.

Participants, who are usually students, and their mentors are nominated by their local GÉANT partner and 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.

For Cycle 10, one new student was enrolled in the TIM programme. It is worth noting that the TIM student from UKIM/MARnet, who was enrolled in the previous cycle, was offered a position at a local institution and was subsequently proposed by UKIM/MARnet as a participant in the GÉANT project, and was happily welcomed on board. For Cycle 11, we accepted two student applications, one of which included a proposed topic that also required the assignment of a mentor.

The TIM programme continues in GN5-2, aiming again to support at least two candidates per activity cycle. More information about this initiative is available on the GLAD public wiki page [\[73\]](#).

6.3 Incubator 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 engage 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/spaces/G52W5/pages/923959352/T5+-+Trust+and+Identity+Incubator
Dashboard	Public wiki page	https://wiki.geant.org/spaces/G52W5/pages/1212809217/TII+Incubator+Dashboard
Call for ideas	Public wiki page	https://wiki.geant.org/spaces/G52W5/pages/927596665/TII+call+for+Ideas
Public sprint demos	Presentations and recordings	https://wiki.geant.org/spaces/G52W5/pages/1049624681/Cycle+10+half-time+Demo https://wiki.geant.org/spaces/G52W5/pages/1139736659/Cycle+10+final+Demo
GLAD TIM promotion	Public website	https://community.geant.org/trust-and-identity-mentorship/

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	
GÉANT Trust and Identity Cycle 10 halftime demo	Online event	✓	✓	✓	✓	https://events.geant.org/event/1908/
GÉANT Trust and Identity Cycle 10 final demo	05-05-2025	✓	✓	✓	✓	https://events.geant.org/event/1946/
GÉANT Trust and Identity Cycle 11 halftime demo	Online event	✓	✓	✓	✓	https://events.geant.org/event/2066/

Subject	Event	Target Group*				Reference
		R&E	NREN	GC	IN	
Attending and presenting at multiple sessions, plus an Incubator side meeting	25-09-2025	✓	✓	✓		https://tiime-unconference.eu/
Attending and Presenting at TechEX25 Denver	Online event	✓	✓	✓	✓	https://events.internet2.edu/website/84273/

Note:

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

Table 6.3: List of general presentations

Activities and Issues

The Incubator started in GN4-3 and completed a total of 6 activity cycles during that project, with the next three cycles running in the GN5-1 project. During the reporting period of January–December 2025, the first year of GN5-2, the Incubator completed its tenth cycle and started the eleventh, as illustrated in the following figure.

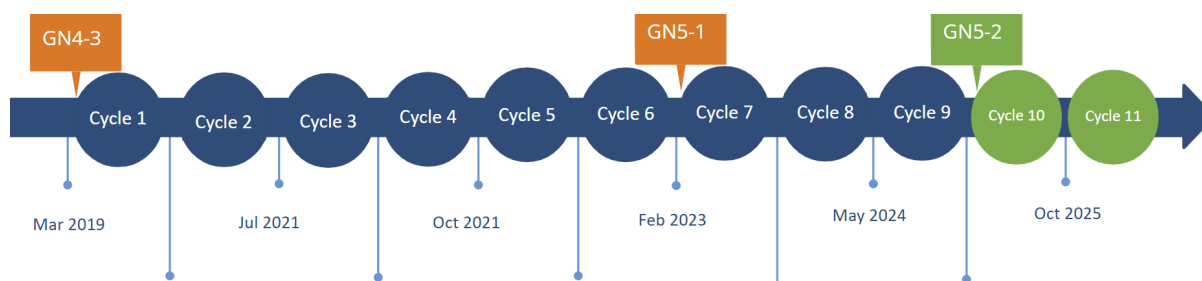


Figure 6.1: Timeline showing the T&I Incubator cycles across the GN4-3, GN5-1 and GN5-2 projects

The schedule shown in the following Table 6.4 is based on cycles of about seven months, comprising sprints that each last five weeks. The cycles have been chosen to ensure sufficient time to investigate and implement a 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 and GN5-1, a transition period of one to three weeks has been introduced between the cycles. This enables the team to wrap up work, gain familiarity with the new topics, and perform kick-off meetings before the cycle starts.

Cycle	Start	End	Status	Activities	Activity page
10	01 Feb 2025	30 Sep 2025	Completed	4	https://wiki.geant.org/spaces/G52W5/pages/978059397/Activity+Cycle+10
11	01 Oct 2025	31 May 2026	In Progress	8	https://wiki.geant.org/spaces/G52W5/pages/1197900011/Activity+Cycle+11

Table 6.4: Schedule of GN5-2 Incubator cycles

All Incubator activities can be found on the Incubator Dashboard [74]. It lists completed activities and their results, along with ongoing activities. The Dashboard will be continuously updated at the beginning of every new cycle.

6.4.1 Cycle 10 Activities (Completed)

The Incubator started its tenth cycle (the first cycle under GN5-2) during the reporting period. During this cycle, four topics were explored.

Bona Fide Researcher Verification

The Bona Fide Researcher Verification activity explored how to automatically verify a researcher's credibility using trusted digital data sources. The goal was to strengthen trust between parties who may not know each other by leveraging existing academic records such as publications, supervision history, collaborations, and committee participation. Instead of relying on manual checks or unreliable name matching, the activity investigated structured integrations with sources such as ORCID, arXiv, Crossref, and DBLP, while also considering metadata from eduGAIN and institutional registries to enrich academic identity information.

The activity focused on developing and testing several proof-of-concept solutions, including integrations with Open Journal Systems (OJS) and enhancements connected to the CoreAAI service MyAccessID. The expected outcomes include practical tools, workflows, and best-practice guidance. These will help editors, review boards, funding bodies, and research infrastructures quickly assess the legitimacy and research track record of an individual. Ultimately, the initiative aimed to increase trust in digital academic identities and improve automated researcher verification across the R&E community. The output of this activity (the OJS module) was published as an open-source module usable by independent scholarly journals.

More details about this activity are available on the project page [75].

Implement OID4VCI/VP in SimpleSAMLphp and Shibboleth IdP

The VC issuer IdPs activity aimed to enable popular IdP software to act as Verifiable Credential (VC) issuers under emerging standards like OpenID for Verifiable Credential Issuance (OID4VCI) and Verifiable Presentations (OID4VP). The motivation was to leverage the rich identity and academic data already held within institutional IdPs – such as affiliations, grades, official names, and academic titles – and make these available to users' wallets

in a secure, standards-based way, so researchers and students can present trusted credentials in decentralised ecosystems and wallet use cases.

The work involved investigating use cases and architectural options, prototyping flows with different types of wallets, and producing proof-of-concept code, documentation, and learning materials demonstrating how SimpleSAMLphp and Shibboleth IdP can issue and interact with verifiable credentials. The results delivered are currently being used in an NREN activity and include demo integrations with specific wallets (e.g., Sphereon and Lissi) and working plugins or flows that show the feasibility of credential issuance from IdPs, helping the R&E community participate in the broader verifiable credential and wallet ecosystem.

More details about this activity are available on the project page [\[76\]](#).

SeamlessAccess with OIDFed Support

The OIDFed DC PoC: SeamlessAccess with OIDFed Support activity focused on integrating the existing SeamlessAccess discovery and login experience with the emerging OpenID Federation (OIDFed) standard. SeamlessAccess is a widely used federated discovery service that lets users sign in via their home organisation with a familiar interface; this activity investigated how to make it work seamlessly with OIDFed in the same way it currently does with SAML-based identity providers, so users wouldn't notice any difference in the login flow. The primary goals were to explore OIDFed discovery and OP listing mechanisms, understand the SeamlessAccess architecture for integration points, and create a proof of concept that interoperates with broader OIDFed efforts such as the eduGAIN PoC.

The deliverables of this work include an OIDFed Discovery flow prototype, an Entity Collection Endpoint with associated code repository and rendered HTML view, and extensions to the OpenID Federation metadata to support these use cases. These outcomes demonstrate that SeamlessAccess can list and utilise OIDFed-capable OpenID Providers similarly to how it handles SAML IdPs, helping support the transition to OIDFed within the R&E identity ecosystem and informing further development and standardisation efforts. Application of the output of this activity is expected when production OID Federations need to use discovery.

More details about this activity are available on the project page [\[77\]](#).

OIDFed National Federations PoC

The OIDFed National Federations PoC activity, part of the Trust & Identity Incubator's work on modern identity federation standards, explored how OIDFed could be adopted by NRENs that traditionally operate SAML federations. Team members leveraged their experience running federations to simulate the transition of different federation types – including small, large, proxy-based, and mesh models – to understand whether existing tools, operational practices, and educational materials are sufficient, and to identify gaps in tooling or training needed to support OIDFed adoption.

The outcomes of this activity included the creation of an OpenID Federation R&E testbed, tooling such as instant integration via the Apache AuthMemCookie module, and the OpenID Federation Forward Auth (OFFA) project with related code, documentation, and a live demo. These deliverables serve to demonstrate feasibility and provide concrete resources that help NRENs, the wider R&E community, and services like eduGAIN experiment with and evaluate OIDFed, assisting them in planning their own transitions from legacy federation standards. The deliverables of this incubator activity have been directly translated into eduGAIN (testbed).

More details about this activity are available on the project page [\[78\]](#).

6.4.2 Cycle 11 Activities (In Progress)

Fuzzing TI Endpoints

The Fuzzing TI endpoints activity in the T&I Incubator focuses on researching the security of Single Sign-On (SSO) implementations by applying fuzz testing techniques to popular identity protocols like OpenID Connect and SAML. The goal is to systematically investigate how these authentication systems handle unexpected, malformed, or anomalous inputs — a process known as fuzzing, which can uncover implementation flaws, validation issues, or vulnerabilities by feeding protocols random or invalid test data and observing unexpected behaviour such as crashes or security weaknesses.

The project's scope includes conducting literature reviews on fuzzing methodologies, analysing the most widely used SSO protocol implementations within the R&E community, setting up the necessary infrastructure (potentially across several NRENs), and performing actual fuzzing campaigns. Based on the findings, the team plans to produce a white paper documenting results and, where appropriate, engage with vendors and developers about any vulnerabilities discovered.

More details about this activity are available on the project page [\[79\]](#).

DIIP Wallet Interoperability

The DIIP wallet interoperability activity within the T&I Incubator aims to improve practical interoperability between verifiable credential issuance and wallet implementations by adopting the Decentralised Identity Interop Profile (DIIP) — a community-driven profile that defines a minimal, interoperable set of protocols, formats, and parameters for digital credential ecosystems. DIIP provides defaults for credential formats, signature algorithms, issuance and presentation protocols (e.g., leveraging OID4VCI/VP) and helps avoid the combinatorial explosion of options that otherwise makes implementations incompatible with each other. This task focuses on implementing and testing DIIP support for Shibboleth and SimpleSAMLphp identity provider VC issuers so that they can interoperate with DIIP-conformant wallets and successfully pass DIIP conformance tests.

In addition to basic issuance interoperability, the activity investigates revocation mechanisms — particularly the IETF Token Status List model — to ensure both scalability and privacy-respecting support in future wallet ecosystems, including the forthcoming European Digital Identity Wallet ecosystem. The planned outcomes are a proof-of-concept DIIP-compliant VC issuer for Shibboleth/SimpleSAMLphp or a detailed gap analysis identifying obstacles, plus engagement with the broader DIIP/FIDES community and real DIIP-compliant wallets during testing. These results are intended to benefit the R&E community by aligning institutional IdPs with a practical, interoperable wallet ecosystem.

More details about this activity are available on the project page [\[80\]](#).

Accessibility and UX in Wallets

The Accessibility and UX in wallets activity focuses on understanding and improving how digital identity wallets are experienced by users in R&E, with special attention to accessibility and the needs of underrepresented groups such as persons with disabilities. The task is driven by real-world testing of existing wallets to assess whether they are usable, intuitive, and inclusive across a diverse range of users — not only tech-savvy individuals but anyone interacting with digital identities in academic contexts. It aims to collect insights from people with varying abilities to identify usability gaps and barriers that could prevent equitable access to wallet functionalities.

The intended outcomes are recommendations and guidance for wallet developers and the broader R&E community on how to make wallets more accessible and user-friendly, ensuring that the benefits of digital identity tools are truly available to all. While the immediate focus is on wallets, the methodology and findings

are expected to inform broader user experience improvements in Trust & Identity interfaces beyond wallets, helping designers and implementers build solutions that respect usability, accessibility standards, and inclusive design principles.

More details about this activity are available on the project page [\[81\]](#).

Apache mod_oidfed

The Apache mod_oidfed activity focuses on creating a native Apache HTTP Server module that understands the OIDFed protocol, enabling Apache-hosted applications to act as OIDFed relying parties (RPs). Because no such native module currently exists, the work investigates how to design and implement this functionality — for example, by building on top of existing modules like mod_auth_openidc or mod_auth_memcookie — and defining a clean interface between the module and a backend OIDFed stack. The goal is to make it easy to install and deploy the module on typical Linux systems, and to support high-availability and load-balanced environments where Apache serves as the frontend for federated authentication.

The deliverables of the activity include proof-of-concept code demonstrating the feasibility of the approach and documentation of the module design. By providing an Apache-native OIDFed RP module, the project aims to broaden the ecosystem of OIDFed-capable components, making it easier for organisations, services, and research infrastructures to adopt OpenID Federation in real-world deployments.

More details about this activity are available on the project page [\[82\]](#).

php OIDFed Library and RP

The php oidfed library and RP activity addresses a gap in the OpenID Federation (OIDFed) ecosystem by developing a generic PHP library and relying party (RP) implementation for OIDFed. While many IdPs (especially SimpleSAMLphp) have gained federation support, there is a lack of reusable PHP-based RP code beyond very specific examples tied to individual federations. This activity therefore defines a scope for a reusable OpenID Federation library in PHP and attempts to build a proof-of-concept RP implementation — for example, integrated with SimpleSAMLphp — that can serve as a basis for broader adoption and development in the R&E community.

The expected outcome is a functional proof-of-concept SSP RP using the new PHP library, demonstrating how PHP applications can act as OIDFed relying parties without relying on one-off code. By creating these components and documenting their design, the project aims to make it easier for services written in PHP to participate in OIDFed environments and encourage further ecosystem growth.

More details about this activity are available on the project page [\[83\]](#).

Local Discovery for OIDFed

The Local Discovery for OIDFed activity investigates how to implement embedded OIDFed discovery — that is, enabling applications to determine the correct OpenID Provider (OP) endpoint for a user's home organisation based on their input (such as an email domain) without relying on third-party or centralised discovery services. Because OpenID Federation does not natively provide a universal discovery mechanism by default, this task explores patterns and architectural options to support local discovery within services and relying parties, including how to store, cache, and manage federation metadata effectively. It also assesses how existing discovery approaches in other protocols (like SAML's WAYF/Discovery) can inform OIDFed usage models in R&E contexts.

The activity has so far produced proof-of-concept code and documentation showing how local discovery can be implemented in practice, helping developers understand how to build OIDFed-aware applications that can locally resolve user identifiers to OPs. These deliverables aim to lower the barrier for adoption of OpenID

Federation in real-world deployments by services and relying parties by providing concrete guidance on discovery flows, metadata handling, and error conditions when federated OPs are not immediately resolvable.

More details about this activity are available on the project page [\[84\]](#).

OpenID Federation Registry

The OpenID Federation Registry activity focuses on creating a centralised repository and tooling for managing OIDFed metadata published by federations, OpenID providers, and relying parties. Because OIDFed relies on signed metadata to establish trust between entities, having a well-organised registry helps developers, operators, and federations discover and consume metadata efficiently. The work includes prototyping a registry service, developing APIs and user interfaces for searching and accessing federation metadata, and defining best practices for how metadata should be formatted, published, and maintained to support interoperability.

This activity's deliverables include a proof-of-concept registry implementation, documentation of metadata schemas and usage patterns, and guidance on how federations and services can publish to and sync with the registry. By providing a searchable store of OIDFed metadata and tools to interact with it, the project aims to lower barriers to adoption of OIDFed, improve consistency in metadata usage, and support real-world deployment and tooling in the R&E identity ecosystem.

More details about this activity are available on the project page [\[85\]](#).

Token Introspection Proxy for Supporting AARC-G052

The Token Introspection Proxy for supporting AARC-G052 activity in the T&I Incubator focuses on building a proof-of-concept implementation of the AARC-G052 OAuth 2.0 Proxied Token Introspection specification — a method that extends OAuth 2.0 token introspection to allow an authorisation server (AS) to validate and gather metadata about tokens it did not issue by consulting a trusted upstream AS. This capability is required by services like CoreAAI and broader federated AAI deployments because it enables robust validation of access tokens in cross-domain and federated environments without requiring direct trust relationships between every service and every issuer.

The team has so far created an initial proxy component called TIP that can be deployed alongside an OpenID Provider and used as the endpoint for token introspection, avoiding changes to the OP itself. The work includes extending functionality to support OIDFed, improving deployability and documentation, and producing an updated version of the TIP prototype. The intended outcome is a usable introspection proxy that can be integrated with existing AAI infrastructures, helping R&E communities and services implement AARC-G052 workflows effectively.

More details about this activity are available on the project page [\[86\]](#).

7 Enabling Communities

Task Leader: Casper Dreef (GÉANT Association)

Within GN5-2 WP5, part of the effort is aimed under Task 6, Enabling Communities (EnCo), at providing a bi-directional channel with key T&I stakeholders, including research communities, identity federations and other relevant communities and initiatives, to understand their needs and obtain feedback on the work done within T&I services. Their input is used to drive the evolution of existing T&I services, set out the requirements for new services or tools, and undertake engagement in the area of EUDI wallets. This work is carried out under three subtasks: Policy and Technology, Wallets, and T&I Outreach.

7.1 Key Performance Indicators

The Task's KPI for the reporting period is shown in Table 7.1 below.

KPI	Baseline (start of GN5-2)	Target (by end of GN5-2)	Achieved result (by end of reporting period)
Number of initiatives, standardisation bodies and research communities engaged	0	8	9 (AARC, REFEDS, NRENS4Education, FIM4R, AEGIS, IETF, SKA, EOSC, and HEIF)

Table 7.1: Enabling Communities KPIs at the end of the reporting period

7.2 Activities and Issues

7.2.1 Policy and Technology

Throughout 2025, the Policy and Technology subtask participated in events to foster community collaboration. In collaboration with the GÉANT Association, NRENS and community partners, the Enabling Communities and Incubator tasks continued the revived annual Trust and Internet Identity Meeting Europe (TIIME) [87]. This unconference-style meeting, was held from 2013–20 as the only T&I innovation conference in Europe focusing on R&E. Building on a successful revival in 2024, the 2025 edition was held in Reading (UK) and was very well received, with approximately 150 participants from all over Europe and beyond. Many participants from other sectors were also present. Planning is already underway for the next TIIME Unconference in Amsterdam (NL) in 2026, intended to serve as a platform for sharing new and innovative ideas within the T&I community that will ultimately serve as a source of projects for future Incubator cycles.

Alongside the main TIIME Unconference meeting, the team also organised and led the Federated Identity Management for Research (FIM4R) meeting at the same time, as well as attending the Higher Education Interoperability Framework (HEIF) workshop on 29–30 September in Brussels.

The team leveraged these gatherings to advance specific initiatives, including contributing to the Identity Use Case task force and the NRENs4Education initiative. Targeted face-to-face meetings were also held at the 64th and 65th European Policy Management Authority for Grid Authentication (EUGridPMA) events, and subtask members initiated discussions at TNC25 regarding the revitalisation of the WISE community. This momentum was carried into future planning, with preparations underway for two upcoming FIM4R meetings at Internet2 TechEX25 (8–12 December, Colorado, US) and at TIIME26 (9–13 February, Amsterdam, NL). Subtask members also began exploring a potential proposal for the April 2026 Security Days conference.

Parallel to the community outreach work, the team made significant progress in shaping policy and aligning strategic technology efforts. Ongoing support was provided for the AARC TREE project's policy activities and collaboration was initiated on OpenID Federation pilot with the eduGAIN team. Additionally, to improve interaction within the EnCo task and enable alignment with broader policy efforts, the Wallets subtask activities were integrated into the future programming of EUGridPMA+, GN5-2 WP5 Policy and Technology, and AARC meetings.

7.2.2 Wallets

Based on the results of GN5-1 WP5 T7 Distributed Identities Activities, a list of initial work items for the Wallets subtask was developed at the beginning of the reporting period, focusing on mapping the digital identity, wallets and credentials landscape in European R&E and beyond, establishing a shared terminology, and supporting wallet and credential interoperability.

Most progress during the reporting period was made on work items reviewing the current state of digital identity wallets, developing the shared terminology [88], outlining the role of identity federations in the wallet ecosystem, and supporting interoperability for digital wallets and credentials. Notably, as part of the work done on identifying the current state of digital wallets, the subtask sent out a questionnaire to the European NRENs to understand the current state of their work on Wallets. The results of the questionnaire were used to prepare for the CTO Workshops in November 2025 and contributed to the whitepaper [89] that was shared with the community's CTOs in advance. Subtask members also published an additional briefing document [90] to support the session on wallets.

A face-to-face meeting was held at the Leibniz Supercomputing Centre in Munich at the end of May 2025, where team members shared updates and jointly planned short-, medium-, and long-term objectives. The subtask also worked on identifying national initiatives and stakeholder groups related to digital wallets, including the EUDI wallet, and exploring the potential role of identity federations in this space. The Wallets subtask tracks all progress on a dedicated wiki [91].

7.2.3 T&I Outreach

A key priority for the T&I Outreach subtask this period was the development of a communications plan to support wider outreach activities, focusing primarily on Wallets subtask branding and the promotion of a series of national InAcademia success stories. Input was also provided to GN5-2 deliverable *D3.1 Stakeholder Engagement Plan* and ongoing outreach topics were regularly discussed in the monthly meetings.

Additionally, the T&I Outreach subtask organised monthly meetings throughout the reporting period, allowing representatives of the other WP5 tasks to meet up with members of WP2 and WP3 to feed back to (international) NREN stakeholders on progress made within WP5's different services and tasks. Furthermore, in collaboration with the eduGAIN task (WP5 T2), the team published an article on the OpenID Federation Pilot and the Technical Profiles Working Group in the October 2025 edition of the CONNECT Magazine [92].

While some changes occurred within the GÉANT Partner Relations team during the reporting period, these have not affected the subtask's progress.

8 Conclusions

This document provided an overview of the progress made by WP5 Trust and Identity in the delivery of its services and activities in the first twelve months of the GN5-2 project. Each service has an appointed service-owner who is responsible for ensuring the delivery, operation, development and support of their respective service. All key performance indicators have not only been met, but exceeded for all services during the reporting period.

New ideas in the T&I space in research and education have been developed, fostered and matured in the T&I Incubator (Task 5), which successfully completed its tenth cycle during the reporting period. The T&I Incubator demonstrates its continued relevance and success, attracting eight activities for its newly initiated eleventh cycle – double the KPI target of four. Likewise, the annual CTO workshops continue to excel as a venue for discussion with the GÉANT membership on the strategic direction of the GÉANT T&I area.

GÉANT T&I 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 GN5-2 project and to create a better communication channel with other projects and communities, facilitating the input of these key stakeholders to drive the evolution and development of both existing and new T&I services.

WP5 will continue its programme of development and innovation, encompassing the existing services and the Incubator, to ensure the continued delivery of high-quality Trust and Identity services to meet the needs of the research and education community.

Glossary

AAI	Authentication & Authorisation Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
AEGIS	AARC Engagement Group for Infrastructures
CAT	Configuration Assistant Tool
CoCo	GÉANT Code of Conduct
CSIRT	Computer Security Incident Response Team
CUID	Community User Identifier
DIIP	Decentralised Identity Interop Profile
EAC	eduGAIN Access Check
EARC	eduGAIN Attribute Release Check
ECCS	eduGAIN Connectivity Check Service
EFP	EuroHPC Federated Platform
EnCo	Task Enabling Communities
EOSC	European Open Science Cloud
ESCI	European Student Card Initiative
ETLR	European Top-Level RADIUS
EUDI	European Digital Identity
EUGridPMA	European Policy Management Authority for Grid Authentication
EuroHPC	European High-Performance Computing
FaaS	Federation as a Service
FIM4R	Federated Identity Management for Research
GeGC	Global eduroam Governance Committee
GLAD	GÉANT Learning and Development
HEIF	Higher Education Interoperability Framework
HPC	High-Performance Computing
HSM	Hardware Security Module
IAM	Identity & Access Management
IdP	Identity Provider
IETF	Internet Engineering Task Force
ISGC	International Symposium on Grids & Clouds
KPI	Key Performance Indicator
MDA	Metadata Aggregator
MDS	Metadata Distribution Service
MFA	Multi-Factor Authentication
NISO	National Information Standards Organization
NOC	Network Operations Centre
NREN	National Research and Education Network
NRO	National Roaming Operator
OC	Operations Centre
OFFA	OpenID Federation Forward Auth
OIDVCI	OpenID for Verifiable Credential Issuance
OIDVP	OpenID for Verifiable Presentations
OIDC	OpenID Connect
OIDFed	OpenID Federation

OJS	Open Journal Systems
OLA	Operational-Level Agreement
OP	OpenID Provider
OT	Operations Team
R&E	Research & Education
R&S	Research and Scholarship
RI	Research Infrastructure
REFEDS	The Research and Education FEDerations group
SaaS	Software as a Service
SCIM	System for Cross-domain Identity Management
SG	Steering Group
Sirtfi	Security Incident Response Trust Framework for Federated Identity
SKA	Square Kilometre Array
SP	Service Provider
SRE	Site Reliability Engineer
SSO	Single Sign-On
STM Association	International Association of Scientific, Technical, and Medical Publishers
T&I	Trust and Identity
TIIME	Trust and Internet Identity Meeting Europe
TIM	T&I Incubator Mentorship programme
TRL	Technology Readiness Level
VC	Verifiable Credential
WBA	Wireless Broadband Alliance
WCAG	Web Content Accessibility Guidelines
WP	Work Package

References

- [1] eduroam <https://www.eduroam.org/>
- [2] eduroam Compliance Statement https://eduroam.org/wp-content/uploads/2025/07/eduroam_Compliance_Statement_v2-FINAL.pdf
- [3] eduroam Policy Declaration https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-194_eduroam-policy-for-signing_ver2-4_1_18052012.pdf
- [4] eduroam Service Definition https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf
- [5] eduroam_db https://monitor.eduroam.org/fact_eduroam_db.php
- [6] eduroam Monitor <https://monitor.eduroam.org/>
- [7] eduroam CAT <https://cat.eduroam.org/>
- [8] eduroam Managed IdP <https://hosted.eduroam.org>
- [9] geteduroam <https://www.geteduroam.app>
- [10] eduroam Managed SP (pilot) <https://msp-pilot.eduroam.org/>
- [11] T&I Services Roadmaps <https://wiki.geant.org/spaces/G52W5/pages/1027735695/Trust+and+Identity+Services+Roadmaps>
- [12] eduroam Monitor – see [6]
- [13] eduroam Monitor – see [6]
- [14] TNC25 Mobility Day side meeting <https://wiki.geant.org/spaces/TFMNM/pages/966426732/Mobility+Day+at+TNC25>
- [15] IETF: Deprecating Insecure Practices in RADIUS <https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/>
- [16] RADIUS Conference <https://radiusconference.org/>
- [17] eduGAIN <https://www.edugain.org>
- [18] eduGAIN User Stories <https://edugain.org/edugain-users/>
- [19] eduGAIN Futures working group recommendations <https://wiki.geant.org/download/attachments/483754120/eduGAIN%20Futures%20WG%20recommendations-2.pdf>
- [20] eduGAIN Policy Framework <https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf>
- [21] eduGAIN SAML Profile <https://technical.edugain.org/doc/eduGAIN-saml-profile.pdf>
- [22] eduGAIN Reporting <https://reporting.edugain.org/>
- [23] eduGAIN F-Ticks <https://f-ticks.edugain.org/>
- [24] T&I Services Roadmaps – see [11]
- [25] eduGAIN technical site <https://technical.edugain.org>
- [26] REFEDS Research & Scholarship <https://refeds.org/research-and-scholarship>
- [27] REFEDS Sirtfi <https://refeds.org/SIRTFI>
- [28] REFEDS Code of Conduct <https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

- [29] REFEDS Anonymous Access <https://refeds.org/category/anonymous>
- [30] REFEDS Pseudonymous Access <https://refeds.org/category/pseudonymous>
- [31] REFEDS Personalized Access <https://refeds.org/category/personalized>
- [32] eduGAIN Futures Working Group Charter
<https://wiki.geant.org/spaces/eduGAIN/pages/288161849/eduGAIN+Futures+Working+Group+Charter>
- [33] eduGAIN Futures Working Group recommendations
<https://wiki.geant.org/download/attachments/483754120/eduGAIN%20Futures%20WG%20recommendations-2.pdf>
- [34] REFEDS Identity Federation Baseline Expectations <https://refeds.org/baseline-expectations>
- [35] eduGAIN Strategy 2025–2030 <https://edugain.org/wp-content/uploads/2025/06/eduGAIN-Strategy.pdf>
- [36] eduGAIN Support Knowledge Database
<https://wiki.geant.org/display/eduGAIN/eduGAIN+support#eduGAINsupport-eduGAINSupportKnowledgeDatabase>
- [37] OIIDF eduGAIN pilot – technical information <https://github.com/GEANT/edugain-oidf-pilot>
- [38] eduGAIN CommsChallenge 2025-12 Results
<https://wiki.geant.org/spaces/eduGAIN/pages/1258913865/eduGAIN+CommsChallenge+2025-12+Results>
- [39] SeamlessAccess governance <https://seamlessaccess.org/about/governance/>
- [40] WCAG 2.2 AA/AAA compliance guidelines <https://www.w3.org/TR/WCAG22/>
- [41] European Accessibility Act <https://ec.europa.eu/social/main.jsp?catId=1202>
- [42] OpenID Federation 1.0 approved <https://openid.net/openid-federation-1-0-final-specification-approved/>
- [43] APAN59 Meeting <https://apan59.apan.net/>
- [44] AARC Blueprint Architecture https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf
- [45] MyAccessID wiki <https://wiki.geant.org/display/MyAccessID/MyAccessID+Home>
- [46] GÉANT AAI Service <https://wiki.geant.org/display/GSPP/GEANT+AAI+Service>
- [47] EOSC AAI <https://op.europa.eu/en/publication-detail/-/publication/d1bc3702-61e5-11eb-aeb5-01aa75ed71a1/language-en/format-PDF/source-188566729>
- [48] MyAcademicID wiki <https://wiki.geant.org/display/SM/MyAcademicID+Identity+and+Access+Management+Service>
- [49] European Student Card Initiative (ESCI) https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en
- [50] Erasmus+ https://ec.europa.eu/programmes/erasmus-plus/node_en
- [51] European Universities Initiative <https://education.ec.europa.eu/education-levels/higher-education/european-universities-initiative>
- [52] FENIX <https://fenix-ri.eu/>
- [53] Puhuri <https://puhuri.io/>
- [54] MyAccessID IAM <https://wiki.geant.org/display/MyAccessID/MyAccessID+Home>
- [55] PaNOSC <https://www.panosoc.eu/>
- [56] LAGO <http://lagoproject.net/>
- [57] SSH Open Cloud (SSHOC) <https://sshopencloud.eu/>
- [58] VESPA / Europlanet <http://www.europlanet-vespa.eu/>

- [59] InAcademia <https://www.inacademia.org>
- [60] InAcademia – Register Your Service <https://inacademia.org/registering-your-service/>
- [61] InAcademia Service Policy <https://inacademia.org/service-policy/>
- [62] T&I Services Roadmaps – see [11]
- [63] Antena Group streaming service <https://antenagroup.ro/about-us>
- [64] Switch: How to join edu-ID <https://help.switch.ch/aai/join/>
- [65] GARR AAI: Filtering Student Verification Services <https://www.idem.garr.it/federazione-idem/blog/903-filtraggio-dei-servizi-di-verifica-dello-status-di-studente-filtering-student-verification-services#english-version>
- [66] InAcademia – see [48]
- [67] InAcademia Docs <docs.inacademia.org>
- [68] OndaHub <https://ondahub.com/>
- [69] Il Post <http://ilpost.it/>
- [70] Incubator Call for Ideas wiki <https://wiki.geant.org/spaces/G52W5/pages/927596665/TII+call+for+Ideas>
- [71] T&I Incubator Methodology <https://wiki.geant.org/spaces/gn43wp5/pages/120500277/T+I+Incubator+Methodology>
- [72] Scrum framework <https://scrumguides.org/scrum-guide.html>
- [73] TIM Programme <https://community.geant.org/trust-and-identity-mentorship/>
- [74] T&I Incubator Dashboard <https://wiki.geant.org/spaces/G52W5/pages/1212809217/TII+Incubator+Dashboard>
- [75] Bona Fide Researcher Verification Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/978059406/Bona+Fide+researcher+verification>
- [76] Implement OID4VCI/VP in SimpleSAMLphp and Shibboleth IdP Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/978059399/VC+issuer+IdPs+Implement+OID4VCI+VP+in+SimpleSAMLphp+and+Shibboleth+IdP>
- [77] SeamlessAccess with OIDFed Support Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/978059401/OIDFed+DC+PoC+SeamlessAccess+with+OIDFed+Support>
- [78] OIDFed National Federations PoC Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/978059403/OIDFed+NRENs+PoC+OIDFed+National+Federations+PoC>
- [79] Fuzzing TI Endpoints Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/1197900015/Fuzzing+TI+endpoints>
- [80] DIIP Wallet Interoperability Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/1197900013/DIIP+wallet+interoperability>
- [81] Accessibility and UX in wallets Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/1246855211/Accessibility+and+UX+in+wallets>
- [82] Apache mod_oidfed Incubator activity https://wiki.geant.org/spaces/G52W5/pages/1197900023/Apache+mod_oidfed
- [83] php oidfed library and RP Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/1197900021/php+oidfed+library+and+RP>
- [84] Local Discovery for OIDFed Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/1197900019/Local+discovery+for+OIDFed>
- [85] OpenID Federation Registry Incubator activity <https://wiki.geant.org/spaces/G52W5/pages/1197900017/OpenID+Federation+Registry>

- [86] Token Introspection Proxy for supporting AARC-G052 Incubator activity
<https://wiki.geant.org/spaces/G52W5/pages/1197900025/A+Token+Introspection+Proxy+for+supporting+AARC-G052>
- [87] TIIME Unconference <https://tiime-unconference.eu/>
- [88] Digital identity wallet terminology
<https://wiki.geant.org/spaces/G52W5/pages/972226805/2+Digital+identity+wallet+terminology>
- [89] Trust and Identity CTO Workshop Briefing paper 2025 [*federated login required*]
<https://wiki.geant.org/spaces/PR/pages/1083867426/CTO+Workshops+2025?preview=/1083867426/1238335501/2025%20-%20Trust%20and%20Identity%20CTO%20workshop%20briefing%20paper.pdf>
- [90] CTO Workshops 2025 – WP5T6 Wallets briefing paper
<https://wiki.geant.org/spaces/PR/pages/1083867426/CTO+Workshops+2025?preview=/1083867426/1238335500/CTO%20WS%20Wallets%20briefing.pdf> [*federated login required*]
- [91] GN5-2 WP5 T6 Wallets subtask <https://wiki.geant.org/spaces/G52W5/pages/958103668/Subtask+-+Wallets>
- [92] eduGAIN piloting use of OpenID Federation | CONNECT Online
<https://connect.geant.org/2025/10/13/edugain-piloting-use-of-openid-federation>