08-01-2025

Deliverable D5.2
Report on Trust and Identity Services, Enabling Communities and Incubator

Contractual Date:	29-11-2024
Actual Date:	08-01-2025
Grant Agreement No.:	101100680
Work Package:	WP5
Task Item:	Task 1, Task 2, Task 3, Task 4, Task 5, Task 6 and Task 7
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	SUNET, SURF
Document ID:	GN5-1-24-d4af01
Authors:	Maarten Kremers (SURF), Marina Adomeit (SUNET), Paul Dekkers (SURF), Davide Vaghetti (GARR), Christos Kanellopoulos (GÉANT Association), Michelle Williams (GÉANT Association), Casper Dreef (GÉANT Association), Niels van Dijk (SURF), Christoph Graf (Switch)

Abstract

This document reports on the Trust and Identity service families operated in GN5-1 by WP5 Tasks 1, 2, 3 and 4: eduroam, eduGAIN, Core AAI Platform and InAcademia; and on activities in Task 5 Incubator, Task 6 Enabling Communities and Task 7 Distributed Identities. It covers uptake and usage, KPIs, activities, issues and outreach from the beginning of November 2023 to the end of September 2024.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document reports on the services delivered by Work Package 5 Trust and Identity Services Evolution and Delivery (WP5) and related Incubator and outreach activities. WP5 is responsible for managing the Trust and Identity (T&I) services portfolio, which encompasses the development of new services (if new use cases emerge), and the enhancement and operation of existing services with the aim of driving them towards the anticipated maturity levels. This is the second service report of GN5-1 and covers the activities and status of the services from the beginning of November 2023 until September 2024.

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 who manages and organises the work of the service teams in order to ensure effective, efficient and secure services operation, development and support.

During the reporting period, all services met or exceeded their key performance indicators on service availability. Uptake key performance indicators are measured on the project duration time frame and are still being recorded. Highlights over the reporting period include:

- The eduroam team further developed and enhanced supporting software for the service, including new versions of the mobile geteduroam clients as well as the improvement of the underlying infrastructures. eduroam task members put much effort in the responsible disclosure, communication and patching of the Blast-RADIUS vulnerability with eduroam before it was publicly announced.
- eduGAIN Task members continued work on strengthening eduGAIN service delivery by completing the provisioning of a secondary site, achieving a more robust architecture for the service. The Task supported the update of the eduGAIN Constitution and creation of the new eduGAIN governance bodies. This finalised the implementation of the first part of the recommendations of the eduGAIN Futures Working Group; preparation for the second part is underway in collaboration with the new eduGAIN Steering Committee. In collaboration with the T&I Incubator team, eduGAIN is preparing a proof of concept (PoC) of OpenID Federation for eduGAIN. The reporting period was particularly fruitful for the eduGAIN training and security team that performed several activities, as described in more detail in this report.
- The Core AAI Platform team continued development of the platform, adding features to enhance the scalability of its delivery, along with new features requested by the stakeholders of the Core AAI Platform services. Most prominent was the connection of the EOSC EU Node to MyAccessID, a service based on the Core AAI Platform and delivered by this task. Many developments took place to support the requirements of EOSC, the HPC community and research infrastructures, as described in Section 4, Core AAI Platform, of this report.
- The InAcademia service keeps growing both in terms of availability in different federations and in the number of student validations. The InAcademia plugin for WooCommerce, which will become a new onboarding channel to attract small-to-medium enterprises that wish to add an eligibility validation

feature for student discounts to their checkout process, has progressed to the point of preparing this feature for launch.

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

WP5 supported the creation of the GÉANT Trust and Identity Strategy 2025-2027 published online [T&I Strat] presenting the strategic plan for the GÉANT Trust and Identity area. This strategy builds upon the briefing paper shared at the 2023 T&I Chief Technology Officer (CTO) workshop and incorporates feedback from the community. Its purpose is to steer the development of the GN5-2 program and influence various other projects and initiatives under GÉANT. The key principle of this strategy is to ensure that the GÉANT community continues to be the trusted provider for the T&I services in research and education (R&E).

The T&I services delivered by GÉANT, in collaboration with the NRENs, are expected to continue working towards an omnipresent Authentication and Authorization Infrastructure (AAI) for the R&E community. Mirroring the comprehensive reach of network provision, the AAI will be a cornerstone of the GÉANT programme, ensuring it is accessible to every user within the academic and research sphere in Europe. It will provide a pervasive, secure, interoperable and sustainable trust fabric, seamlessly integrated with technological advancements that support and empower a wide array of scholarly and research activities, fostering collaboration and innovation across Europe and beyond. The strategy document was discussed in the CTO workshop organised in November 2023 with 70 participants from the GÉANT community [CTO workshop]. The feedback received was positive with NRENs expressing endorsement and support for the GÉANT T&I programme.

Work Package 5 is mindful of its responsibilities as custodian of the flagship Trust and Identity services that are crucial to the research and education community. Therefore, while the results achieved in the project to date confirm the services' success, WP5 will continue its programme of development and innovation of both existing and new services to ensure 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 R&E collaboration across Europe and the world. The R&E community relies on a trustworthy and secure global authentication infrastructure, where resources can authorise users based on the information received from the user's home organisation (typically a university or NREN) and on the resource policy.

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

The set of services delivered within WP5 is:

- **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 based on the Core AAI Platform; those are listed in Table 4.1
- **InAcademia**: Provides service providers with a quick, reliable and secure way to verify academic affiliation (whether a user is a student, a member of staff or faculty) to determine whether a user is eligible for discounts or academic-only offers, provided the user is registered with a participating eduGAIN identity provider. The service is available in two editions: Commercial (service providers are charged for using InAcademia) and Community (selected not-for-profit service providers in the R&E sector may use InAcademia free of charge).

In addition to these four services, WP5 operates three more activities: the Incubator, the work on the distributed identities and the outreach activities.

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

Lastly, there is a strong push to make identity management more user-centric, giving users greater control and an active role in sharing their information. A specific work item explores use cases better supported by distributed technologies and their impact on current R&E services and infrastructure.

The following sections provide information on the services and activities listed above from the start of October 2023 until the end of September 2024. For each service and activity the document presents a summary description; contact details; data on uptake, usage and key performance indicators (KPIs); and a summary of key activities and any issues encountered in the reporting period.

2 eduroam

Service Owner: Paul Dekkers (SURF)

eduroam (education roaming) [eduroam] provides a secure, worldwide roaming access service for the international 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. 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'.

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

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

Table 2.1: Contact details and information sources for eduroam

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

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 eduroam Policy Declaration [eduroam_PolDecl], which is based on

the eduroam Service Definition [eduroam_ServDef]. In addition, GÉANT operates the over-arching global infrastructure connecting 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 (European Top-Level RADIUS (ETLR) servers), the GÉANT eduroam team also delivers a supporting services suite to facilitate the widespread, global deployment of eduroam. This suite includes:

- A central database (**eduroam db**) [eduroam_db] with information about and provided by participating National Roaming Operators (NROs) and institutions.
- Monitoring and metering tools (**F-Ticks**) [eduroam_Monitor], which are used to monitor the availability of NRO eduroam infrastructure and 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**) [eduroam_CAT], which enables institution administrators to create eduroam installers configured with their local (home institution) setup. End users can then download these installers to configure devices they wish to use for eduroam access with minimal configuration required.

  The CAT tool also provides tools for NROs for purposes such as diagnostics or for the issuing of certificates used in the authentication infrastructure.
- **eduroam Managed IdP** [eduroam_ManIdP], 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 [eduroam_geteduroam] (the portal software is institution-specific via in-app links).
- **eduroam Managed SP (pilot)** [eduroam_ManSPPilot], which is a hosted offering to connect small eduroam Service Providers directly to eduroam, without on-campus authentication infrastructure.

Further development of new eduroam features 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. Development and deployment of eduroam is performed in accordance with the roadmap published on the WP5 Wiki [T&I_Roadmaps], as outlined in Section 2.4, Activities and Issues.

2.2 Uptake

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

On a global scale, 106 territories participate in the eduroam service, (the dark-coloured areas in Figure 2.1 below), of which 52 are in Europe. Of these NROs, 97 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 9,900 participating institutions (6,500+ in Europe) and 39,157 service locations for eduroam (24,526 in Europe).

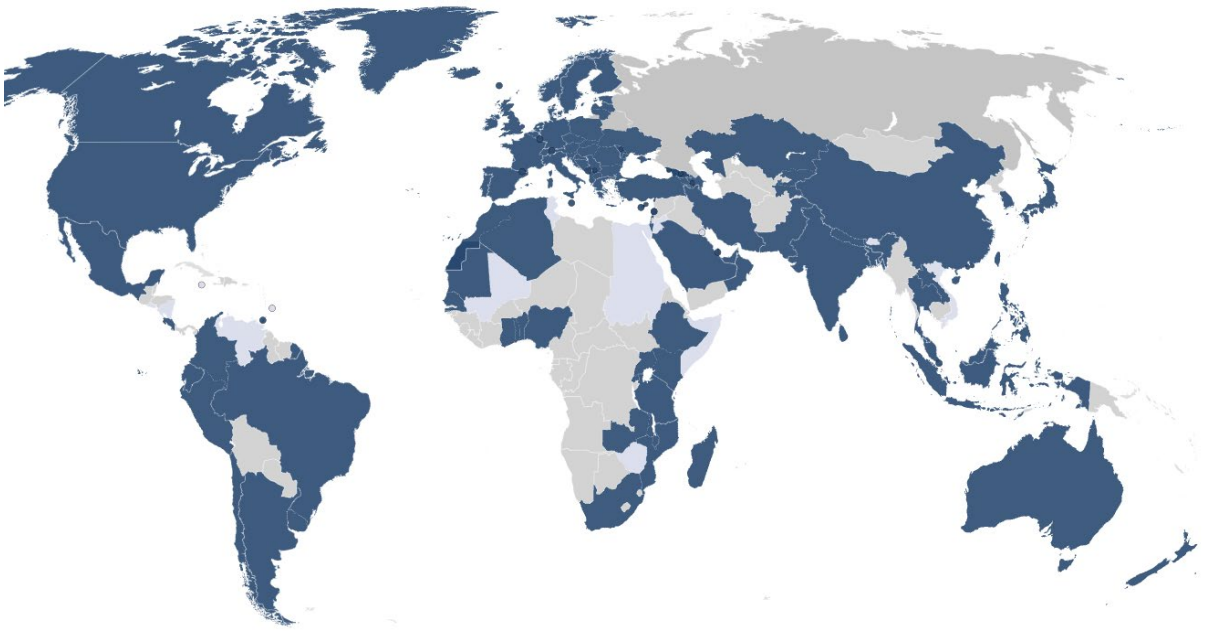

Figure 2.1: Global map of eduroam participants as of the end of the reporting period

The number of successful national and international authentications per month from 1 January to August 2024 is shown in Figure 2.2 below, together with national and international authentications for 2022 and 2023.

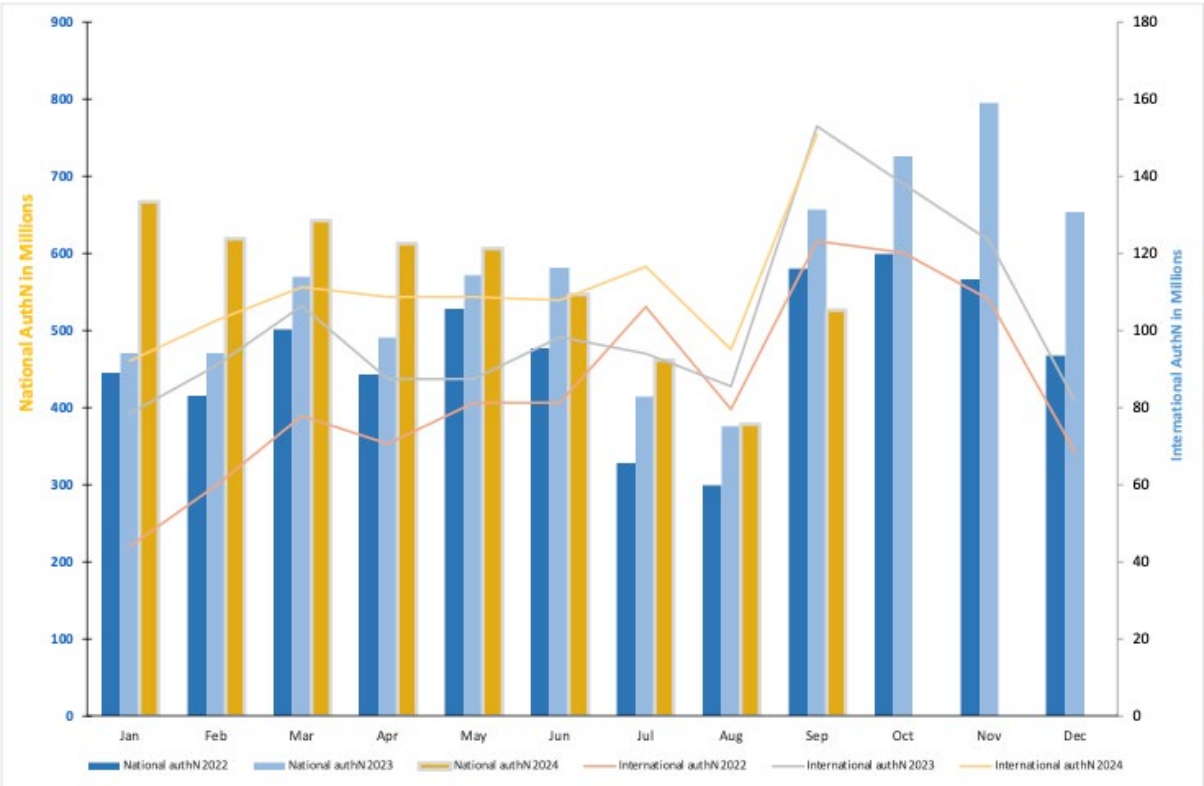

Figure 2.2: eduroam core service usage statistics: number of successful authentications per month

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 [eduroam Monitor].)
- 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 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 are running with at least one top-level roaming server 100% available, therefore performing better than the set target.

KPI	Baseline (start of GN5-1)	Target (end of GN5-1)	Achieved result (by end of reporting period)
European Top-Level RADIUS (ETLR) availability	99.9%	99.9%	100%
Number of international authentications	1.02 billion (2022) 1.22 billion (2023)	5% annual increase	993,245,752*

Note:

* This figure covers the first 9 months of 2024.

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), signing the new policy globally is an ongoing challenge. There is a strong preference to sign the documents digitally as a counter-fraud measure. For eduGAIN digital signatures were easier, but in eduroam the footprint of NROs is broader and truly global. The signing process is thus still waiting for the application of proper digital signatures in some regions, a functionality that is being worked on in other activities.

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 audience.

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

2.4.1 Operations and Outreach

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

During the reporting period the team prepared and released new versions of the geteduroam app for iOS/iPadOS and Android. The Android version became usable for ChromeOS, which was a huge milestone for Chromebook users. The team continued development on CAT, which was also migrated to new VMs for both production and test stages. Preparations are in place for migrating supporting services such as monitoring to microservices/containers.

A lot of work went into mitigating the Blast-RADIUS vulnerability [Blast-RADIUS]. The team was involved in the responsible disclosure of the vulnerability within eduroam. The team communicated about this vulnerability by email, meetings, and via an advisory on the eduroam website; participated in software testing to mitigate Blast-RADIUS for both the radsecproxy software and FreeRADIUS; and patched the central services from eduroam to mitigate this vulnerability. This was all done before the public disclosure of the Blast-RADIUS vulnerability.

The team organised a successful mobility day [TNC24_MobDay] as a side event at TNC24 in Rennes, at which the current status of the eduroam service was discussed, alongside new topics like WPA3 and Wi-Fi 7.

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

The promotion of RadSec was achieved through new options in CAT for NROs, while F-ticks adoption has been delayed due to pending VM migration. The redesign of supporting tools has started but involves the complexity of untangling legacy systems. The development of the radsecproxy has continued, with multiple maintenance releases and with one feature release (introducing TLS-PSK) and as well as the first deployment of the (beta) Windows version in October.

During the reporting period, the eduroam team started work on some innovative topics in which the team also participates and in some cases leads in the Internet Engineering Task Force (IETF). One example is the creation of a novel EAP method that uses FIDO authentication tokens (instead of username/password pairs or certificates). Work is being done on standardisation and proof-of-concept implementations and is supported by the members of other working groups, such as the authors of FreeRADIUS.

Other important work ongoing in the IETF involves improvements to and innovation of the RADIUS protocol. This is very relevant for the eduroam infrastructure, and the eduroam team shares insights and experiences on this topic. The central thrust of this work is to cut out legacy cryptographic elements and make the protocol generally more secure, as eduroam protects some metadata better than via traditional RADIUS.

The eduroam team continues to be a member in the Wireless Broadband Alliance (WBA) and participates in working groups such as those for OpenRoaming. As a part of OpenRoaming, the team provides gateways as a pilot between eduroam and OpenRoaming for NROs or 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 members in the industry and have conversations about the challenges faced in 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, 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 and other discussions relevant to eduroam.

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

3 eduGAIN

Service Owner: David Vaghetti (GARR)

eduGAIN [eduGAIN] 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). The eduGAIN service interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community.

Through eduGAIN:

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

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

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

Table 3.1: Contact details and information sources for eduGAIN

During the reporting period, eduGAIN core and supporting services were operated to a high standard, exceeding the set target for the availability KPI for the eduGAIN Metadata Distribution Service. The uptake KPI was also largely exceeded: the number of identity federations in eduGAIN is 80, with 1 new federation becoming an eduGAIN participant, bringing the percentage of R&E identity federations who are full members of eduGAIN to 91.9%[1]. During the reporting period, the eduGAIN Service Team started a process to update the eduGAIN Declaration due to the approval of the new Constitution [eduGAIN_Const] last year. Moreover, the planning to

[1] Calculation based on the REFEDS data on known research and education identity federations [REFEDS].

make the eduGAIN core services more resilient expanded, and now includes an additional third site at Sunet where the services will be available. Currently, the eduGAIN Core Services are provided by a main site at PSNC, with a development and staging site at GARR that will be turned into a production site.

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 (eduGAIN Policy Framework [eduGAIN_Pol]).

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

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

The eduGAIN service is governed by the eduGAIN Steering 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 for the IdPs available in eduGAIN that tests their actual readiness for eduGAIN, i.e. whether they consume eduGAIN metadata.
- **isFEDERATED check** – a global tool that searches known federations to report whether an institution is already part of the federation and is also in eduGAIN.
- **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 CoCo specification.
- **eduGAIN Reporting** (currently in beta) – a tool that lets federation operators visualise and query their entities in order to assess the overall level of compliance to the eduGAIN and REFEDS standards with an intuitive and visually appealing interface.
- **F-Ticks** – 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 [T&I Roadmaps].

3.2 Uptake

Users of the eduGAIN service are listed on the status page of the eduGAIN technical website [eduGAIN Tech]. At the end of the reporting period, eduGAIN had 80 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	eduId.hu

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

Table 3.2: 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:	
Ethiopia	EFIS Identity Federation

Table 3.3: New eduGAIN federation members

The following figure shows the global map of eduGAIN participants.

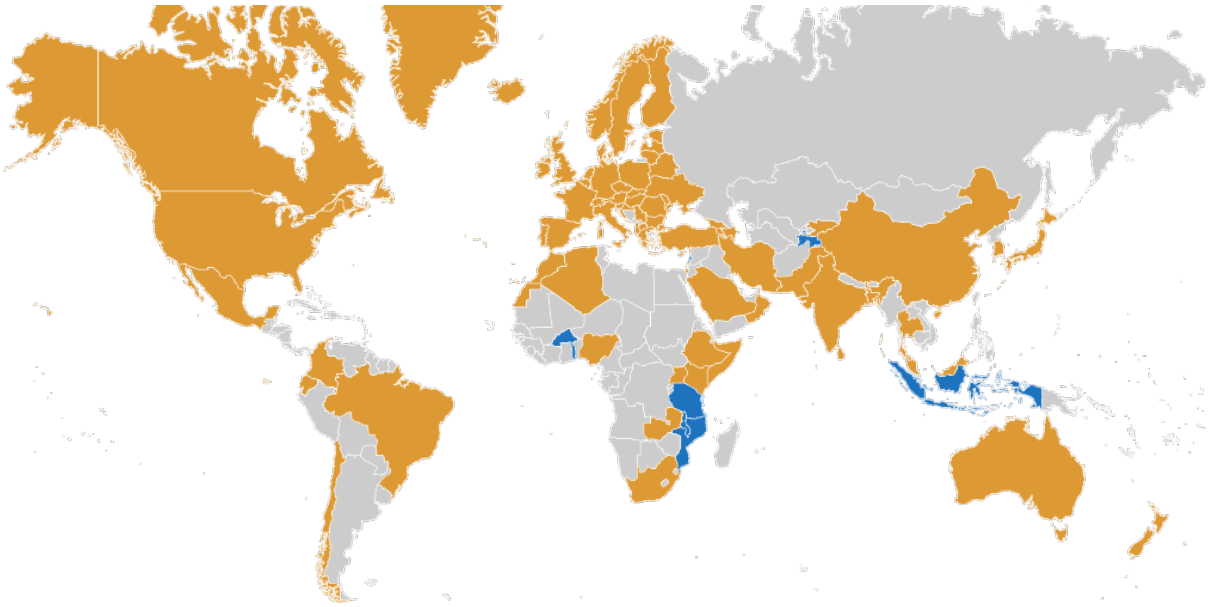

Figure 3.1: Global map of eduGAIN participants

At the end of the reporting period, eduGAIN was providing metadata containing 9,485 entities, of which 5,732 are IdPs and 3,771 are SPs. As shown in the following Figure 3.2, over the course of the reporting period, a growth of 4.5% in the sum of both IdPs and SPs occurred.

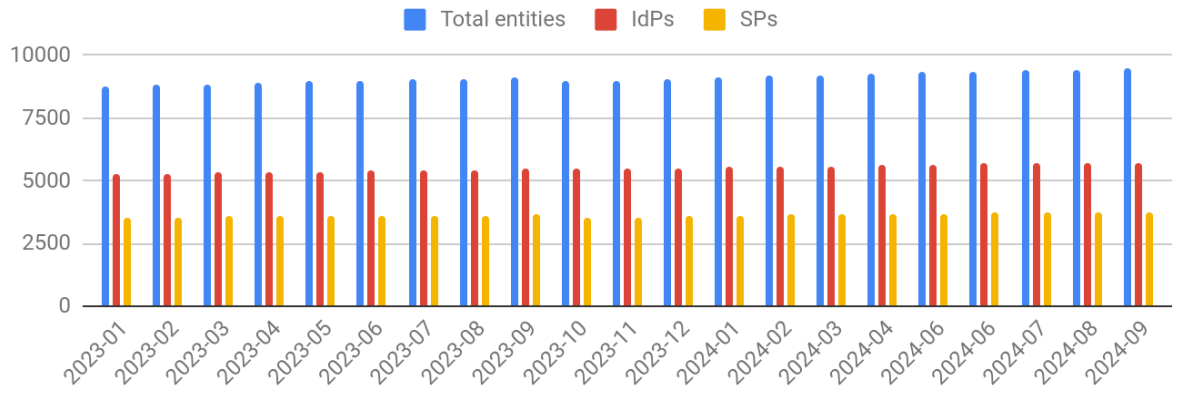

Figure 3.2: Trend of growth of Identity Providers and Service Providers participating in eduGAIN

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

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

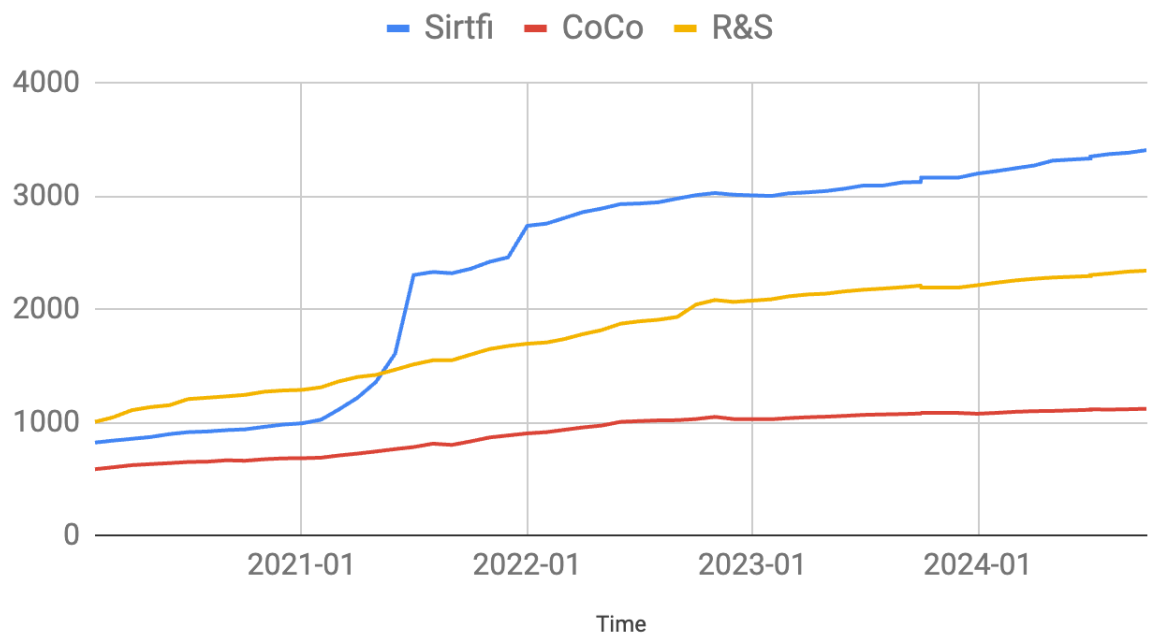

Figure 3.3: Trend of uptake of entity categories and attributes

3.3 Key Performance Indicators

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

KPI	Baseline (start of GN5-1)	Target (end of GN5-1)	Achieved result (by end of reporting period)
Metadata Distribution Service (MDS) availability	99.5%	99.5%	99.9%*
Service Uptake: increase of number of IdPs	4,667 (2021) 5,235 (2022) 5,503 (2023)	8% increase	5,732 (+9.49%)

Note:

* Uptime calculated on a monthly basis; the reported value is the lowest.

Table 3.4: eduGAIN KPIs for the reporting period

3.4 Activities and Issues

The eduGAIN core services were operated to a very high standard during the reporting period and performance has exceeded the targets set. Day-to-day operations relating to the management of the identity federations and the core services was performed by the eduGAIN OT, while supporting services operations were handled by dedicated sub-teams.

During the reporting period the eduGAIN governance bodies changed. The former eduGAIN Steering Group, composed of the delegates and deputies of all the eduGAIN participants, ceased operation and was substituted by two new bodies: the eduGAIN Assembly and the eduGAIN Steering Committee. The Assembly is responsible for voting in new members and approving changes to the eduGAIN Constitution and Declaration, while the Steering Committee is responsible for approving changes to the technological profiles, the work plan and strategy, suspensions, and working groups. The eduGAIN Service Owner and the Secretariat participated regularly in the eduGAIN Steering Committee meetings in order to prosecute the work on the eduGAIN Futures Working Group recommendations implementation activity. 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.

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

3.4.1 eduGAIN OT and Core Services

At the end of the current project, the current eduGAIN OT lead and main developer will retire, therefore a process to expand the current team and hand over the lead was started in the initial phase of the project. This is now functioning consistently, with the main day-to-day operations being processed by new team members pairing with older members retiring from these tasks.

In the reporting period, the process to fully automate the current eduGAIN core services deployment model has been completed and all the related libraries, as well as the operative systems, have been updated to the latest available release.

The team was reinforced by new members from Sunet. In collaboration with the community, development has started across multiple delivery sites on a new architecture for the eduGAIN core services.

The process to duplicate the current eduGAIN core services architecture for a second production site has been completed at the GARR site, with the exception of metadata signing, which will be completed by the end of the project. A process to duplicate the eduGAIN core services in an additional site provided by Sunet has also started.

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 and, in certain cases, to individual IdPs and SPs. Users who raise issues with the eduGAIN Support Team will be routed to the appropriate local support service or team.

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

During the reporting period:

- The current team lead from ASNET-AM coordinated the support team.
- All the shifts in the weekly rota of the eduGAIN Support Team were covered without any exceptions.
- The Support Team received and processed about 48 valid eduGAIN support requests. Examples include support for:
  - Federation information change requests.
  - Federation candidate proposals.
  - Issues regarding interoperability of certain SPs and IdPs.
  - Resolving issues reported by eduGAIN support tools.
- The eduGAIN support documentation and knowledge base is continuously verified and improved and is used to feed a public knowledge base available to federation operators, SPs and IdPs [eduGAIN SupportDocs].

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

3.4.3 eduGAIN Supporting Services and Development

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

The eduGAIN Connectivity Check Service (ECCS), which is maintained on the eduGAIN core services infrastructure, has been updated, converted from a traditional web application to a Docker instance, and the deployment model has been automated.

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

3.4.4 OpenID Federation POC

At the end of 2023, the eduGAIN Service Team started an activity to set up a proof-of-concept (POC) eduGAIN OpenID Federation in collaboration with the Trust and Identity Incubator. The activity consists of the following items:

- Define a draft eduGAIN OpenID Federation technological profile.
- Develop OpenID Federation tools to be used to set up both national identity federations and the interfederation service with the new standard.
- Prepare a pilot of the OpenID Federation to be run in GN5-2.

The activity is currently ongoing. During the reporting period, the draft technological profile was developed and will be shared with the community before the end of GN5-1. The tools defined in the POC were presented at the Trust and Identity Incubator Public Sprint Demo on September 17th 2024. The general plans were presented to the community for feedback at the TNC24 [TNC24 TNI] and the NORDUnet 2024 [NORDUnet Conf] conferences.

3.4.5 eduGAIN CSIRT

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

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

Moreover, in the reporting period the eduGAIN CSIRT managed a major incident in collaboration with Jisc and InCommon/Internet2.

The eduGAIN CSIRT has also created a tabletop security exercise on federated incident handling in eduGAIN. The exercise was run by eduGAIN CSIRT team members at the 72th TF-CSIRT meeting in Prague, and has also been accepted as a laboratory activity at the Internet2 TechEx conference that will be in Boston in December 2024.

3.4.6 Federation as a Service

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

In March 2024, the eduGAIN business development team submitted a survey to the current FaaS users (7 federations in Europe are using FaaS) in order to understand if the service is still considered useful. The answer has been that the service is still crucial for those NRENs to be able to manage their identity federation and participate in eduGAIN.

3.4.7 SeamlessAccess

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

become the go-to IdP discovery service enabling a seamless and consistent experience when accessing resources in eduGAIN.

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

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

- UI continues to be improved in terms of accessibility and usability to ensure compliance with the Web Content Accessibility Guidelines (WCAG) 2.1 AA/AAA compliance [WCAG2.1] and the European Accessibility Act [EurAA].
- Release of the new Identity Provider filtering feature, including development of thiss.js and Metadata Query Protocol (MDQ) components as well as the external library pyFF.
- Updates to infrastructure operations that include:
  - Multiverse for automation, such as installation of the updates.
  - MDQ service used.
  - New tools for ensuring correct metadata is consumed by the service.
  - Tools introduced to further ensure redundancy (Fleetlock).
- Workshops were held with Service Providers using SeamlessAccess Advanced integration to facilitate guidance on best practices for UX.
- Engagement of SeamlessAccess product management in REFEDS (Trustinfo Metadata Working Group) to agree on specifications that would enable federation operators to make use of the filtering features mentioned above.
- Backend, frontend and UX work on the SeamlessAccess smart-button in alignment with the features of the Storage Access API (a tool implemented in all major browsers as a response to the deprecation of third-party cookies and use of third-party storage). This work was done in order to enable the user's choice of identity provider persisting across service providers the user visits.
- Engagement of SeamlessAccess product management and UX with REFEDS (browser changes) and W3C (FedCM, Privacy) over web browser privacy changes that affect SeamlessAccess functionality.

3.4.8 Training and Outreach

In the reporting period the training team held a major eduGAIN and federated authentication training event in collaboration with the African regional organisation UbuntuNet. The training was delivered in Addis Ababa (Ethiopia) between the end of January and beginning of February 2024. Members from 14 African NRENs participated in the training.

The training team activity to convert the current learning material into an online course, which started at the beginning of the year in collaboration with GÉANT Learning and Development (GLAD), has also produced the first artefacts that are currently being reviewed. The first public module will be published on the GLAD learning platform before the end of Q4 2024.

4 Core AAI Platform

Service Owner: Christos Kanellopoulos (GÉANT Association)

The GÉANT Core AAI Platform is set to become a cornerstone in the landscape of advanced 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 high-performance computing 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.

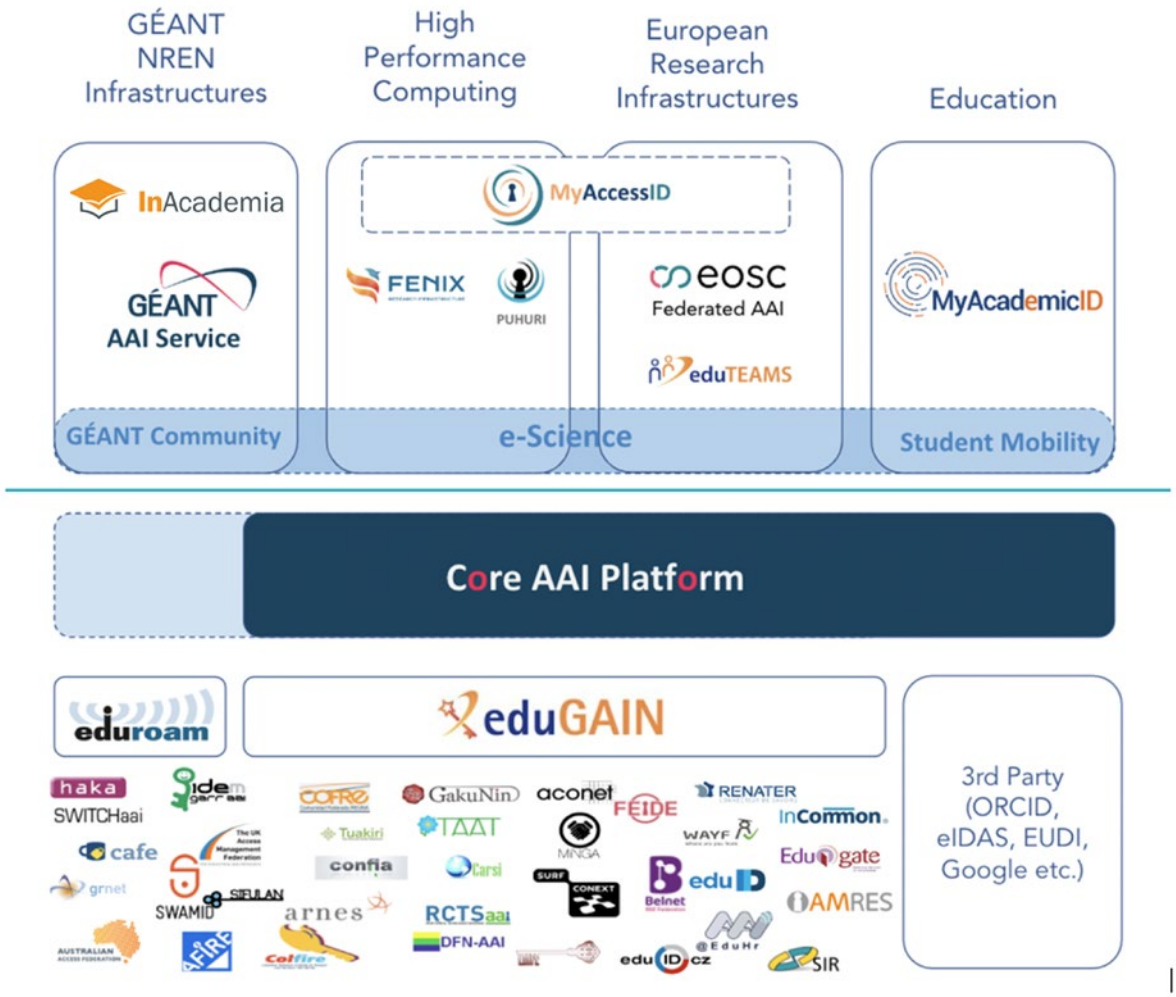

Figure 4.1: Core AAI Platform in the R&E federated identity ecosystem

4.1 Service Description

The Core AAI Platform enables the provision of services that allow research and education communities and infrastructures to securely access and share common resources and services, leveraging the ubiquitous presence of eduGAIN federated identities. It enables them to securely authenticate, identify and manage the roles of their users, and to have one integration point for services – all 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 the complexity from the edge and removing the risks and need for specialised expertise associated with research infrastructures running their own solutions. The development of the Core AAI Platform follows a strongly agile approach, with frequent releases of software enhancements that address stakeholders' requirements.

The Core AAI Platform implements (and enhances) the AARC Blueprint Architecture [AARC BPA] and deploys an IdP/SP proxy that allows 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 and SSH access based on the federated authentication flows.

GN5-1 WP5 funds the development of the Core AAI Platform and the engagement with communities and infrastructures that wish to use its derived services. This engagement includes understanding the stakeholders' requirements, reviewing aspects of integration, and embarking on the design and pre-production phase. The operations of the resulting services are funded in certain cases by the GÉANT project (GN5-1 and predecessors), while in others they may be funded by other projects or infrastructures, as noted in Table 4.1 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** [MyAccessID IAM] – The MyAccessID IAM Service was initially the result of WP5's collaboration with the HPC community. Since then, MyAccessID has been growing 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 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 will use MyAccessID, is expected to begin in January 2025.
  - **EOSC**: EOSC EU Node.
- **GÉANT AAI Service** [GN AAI] – The GÉANT AAI Service, previously known as GÉANT SP Proxy, allows GÉANT services to use federated authentication for identifying users from eduGAIN. During the reporting period WP5 continued supporting the GÉANT Digital Services team to migrate the existing service to the new GÉANT AAI Service based on the Core AAI Platform, offering a wide range of new

capabilities, such as support for OpenID Connect, enhanced user and group management, support for the AARC Blueprint Architecture, and EOSC readiness. In collaboration with WP9, the GÉANT Software Development Tools were migrated from the GÉANT SP proxy to the new GÉANT AAI Service.

- **EOSC AAI Federation** [EOSC AAI] – The goal for the EOSC AAI is to provide the trust mortar with which the many bricks of the current set of scientific communities, collaborations and infrastructures are joined together. The EOSC AAI comprises the AAIs of the science clusters, research infrastructures and e-infrastructure providers brought together through the EOSC AAI Federation. GÉANT continues to contribute to the implementation of the EOSC AAI by further developing the Core AAI Platform to support the emerging requirements coming from EOSC and by delivering the EOSC AAI Federation.
- **EOSC EU Node** – The first phase of the implementation of the EOSC EU Node is complete, 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 using 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 the interoperability goals of the European Open Science Cloud, 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** [MyAcademicID] – The MyAcademicID IAM Service provides identity and federated access management for the services of the European Student Card Initiative [ESCI], the services directly supporting the digitisation of Erasmus+ [Erasmus+] and the European Universities Initiative [Uni Alliances]. The student mobility processes require the use of a number of services, all of which are involved in different stages of the pipeline and need to be able to exchange data about the students. Leveraging the ubiquitous presence of eduGAIN and eIDAS federated identities, the MyAcademicID Service enables the connected services to use the academic attributes that are available through the HEI federated logins provided in combination with the national eID of the users participating in student mobility.

4.2 Uptake

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

The approach being followed during the GN5-1 project is that the requirements analysis, design, and initial implementation activities are funded via WP5. This is a delicate process where subject matter, technical, and integration support from the Core AAI Platform team is necessary in order to come up with 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 the requirements often progress from relatively simple requirements that target a range of use cases, to more complex requirements to address advanced use cases.

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

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

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

Two services running on the GÉANT Core AAI Platform Lifescience AAI and EUROfusion AAI were recently retired, demonstrating the application of effective service lifecycle management. The EOSC Life project, which supported the Lifescience AAI, concluded in August 2023. During this period, the GÉANT Programme provided support to the LifeScience Cluster to ensure a smooth and successful migration of the service from GÉANT to the research infrastructure. The support offered by the Core AAI Platform has been crucial for the LifeScience Cluster, enabling it to consolidate 13 distinct infrastructures, many of which operated their own AAIs, into a single AAI across the entire cluster. This achievement would not have been possible without the capabilities of the Core AAI Platform. In the case of EUROfusion, the service did not progress to a production state, as EUROfusion reprioritized and shifted focus away from technical integration for the time being.

The EuroHPC Joint Undertaking (JU) procurement for the EuroHPC Federated Platform [EuroHPCFP_Proc], which requests all procurers to integrate with the MyAccessID service as a procurement requirement, demonstrates an alignment with the broader vision of establishing a secure, federated authentication and authorisation infrastructure that facilitates seamless access for researchers across Europe. The contract award for this procurement is in its final stages at the time of writing this report.

One of the most significant developments in the reporting period is the award of the EOSC EU Node procurement that aims to provide access to a rich portfolio of FAIR (Findable, Accessible, Interoperable, Reusable) data and professional-grade interoperable services in all relevant domains from data handling to computing, processing, analysis and storing. GÉANT is part of the winning consortium for LOT1 - Core Federation Services for the EOSC EU Node [EOSC_Proc]. The consortium is set to provide professionally managed services for the core components of the EOSC EU Node including the Federated Identity Management and Single-Sign-On solution. During the reporting period, the implementation of the EOSC EU Node was accomplished, with the EOSC EU Node AAI built on top of the GÉANT Core AAI Platform. A number of development activities driven by EOSC EU Node implementation were completed in the Core AAI Platform, improving or introducing additional features and optimising service delivery. In addition to this robust foundation, the EOSC EU Node leverages MyAccessID as its Identity Layer. This integration will enable users to seamlessly access both EuroHPC and EOSC resources using a single, unified identity.

During the first year of GN5-1 the research infrastructures, which until recently required their own AAI services, have realised the strong benefits of using horizontal AAI services such as MyAccessID. As a result, several of them have shifted to direct integration with MyAccessID. The WP expects that this trend will continue and become even stronger in the coming years.

Deployment	Status
eduTEAMS Service	Production
CESSDA/SSHOC	Production
eduGAIN	Production
LAGO	Production
Le Laboratoire Univers et Théories (Observatoire de Paris)	Production
LITNET	Pilot

Deployment	Status
Opticon RadioNet	Pilot
Paris Astronomical Data Center	Production
VESPA (EuroPlanet)	Production
FENIX (*)	Production
PaNOSC (UmbrellaID)	Production
EOSC-Life (*)	Retired
MyAccessID (EurpHPC+Research Infrastructures + EOSC)	Production
Puhuri ISD Proxy	Production
MyAcademicID (Student Mobility) (*)	Production
Cloud services procured via the FPA (i.e. OCRE)	Production
EUROfusion	Retired
SRAM (SURF) (*)	Production
GÉANT AAI Service	Production
EOSC AAI	Production
EOSC AAI Federation	Pre-production
EOSC EU Node (*)	Production

Note:

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

Table 4.1: Core AAI Platform deployments and status

4.3 Key Performance Indicators

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

KPI	Baseline (start of GN5-1)	Target (end of GN5-1)	Achieved result (by end of reporting period)
Core AAI Platform: GÉANT SP Proxy Service availability	99.5%	99.5%	100%
Core AAI Platform Service Uptake: GÉANT AAI Service connected services	0	100	31*

Note:

* The focus up to the end of the previous period (December 2023) was on complex services that require authorisation management. In this period (January 2024–December 2024) the focus shifted to services adopting the OpenID Connect protocol. In addition, the GÉANT Digital Services (DS) team, responsible for managing and operating the services, has taken the opportunity to re-evaluate the portfolio of services, which led to retirement of services that were not in active use.

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

- Two new members were recruited and joined the Core AAI Platform service delivery management team.
- The Core AAI team held face-to-face meetings in July 2024 and in September 2024 in Amsterdam to discuss the roadmap for the GÉANT Core AAI Platform.
- The Core AAI team development team held a face-to-face meeting in August 2024 in Amsterdam to onboard the new service development managers and to discuss the development goals for the GÉANT Core AAI Platform.

4.4.2 Development and Operations Highlights

- The service was operated to a high standard, with continuous improvements made to the operational model in order to enable the increased automation and scalability of the deployments. Development was undertaken in an agile manner in order to address the requirements in an effective way.
- The new SCIM (System for Cross-domain Identity Management) API and its integration with the Membership Management Platform (Perun), including the implementation of required workflows and fine-tuning on the Perun side, in order to implement customer use cases, was delivered. It is a capability that we are bringing to the whole Core AAI Platform and will be foundational for what is coming up next.
- The new features of the OIDC frontend, allowing the Core AAI Platform to provide support for Service Accounts and much more, were developed.

- The discovery service was greatly improved by implementing the possibility for customer-themed discovery UIs and performing code refactoring, serving to improve the discovery experience for the Core AAI Platform.
- A performance-testing framework was put in place, laying a solid foundation for future work.
- Development on introducing a step-up Multi-Factor Authentication function is reaching its conclusion and will soon be incorporated, further enhancing the Platform's capabilities.
- The work in moving from Ansible to Terraform is almost complete, and will be soon incorporated into the Platform's deployments, further improving the efficiency and effectiveness of the tool-chain.
- Operational resilience was improved by implementing the seamless infrastructure switch, overcoming limitations with IP addresses and the shared RDS Cluster across environments.
- Another big step forward for the platform's evolution was the progress with Letty for Service Management and the ground-breaking design work for moving the SATOSA configuration to an external API.
- Work on the Guest IdP feature has progressed.
- The SSH CA feature, offering customers the possibility to use federated authentication when their users access resources through SSH, was shaped into a pilot offering and is being promoted to the customers to try out.
- A vendor identity vetting solution for integration into the platform was explored in order to deliver the necessary level of assurance when users cannot get such assurance with their federated identity. To that end, GÉANT has prepared a procurement that will be ready to launch by the end of 2024.

5 InAcademia

Service Owner: Michelle Williams (GÉANT Association)

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

The InAcademia service is available in two service models: 'Commercial Edition' for online retailers that are making a profit from offering services that leverage InAcademia affiliation information, and 'Community Edition' for Service Providers that are not for profit, where the models are differentiated by pricing strategy. End users and Identity Providers benefit from InAcademia as it provides a privacy-preserving way to validate the user's affiliation, compared with the manual process many online retailers 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
General information	info@inacademia.org
Support for merchants	support@inacademia.org

Table 5.1: Contact details and information sources for InAcademia

5.1 Service Description

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

Identity federations are encouraged to actively promote InAcademia to their constituents and are invited to participate in the InAcademia Steering Committee. The InAcademia support model 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 DevOpsTeam 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 DevOpsTeam, in collaboration with the Core AAI Platform Development Team. The InAcademia DevOpsTeam 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 [T&I_Roadmaps].

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 (Figure 5.1) of the 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.

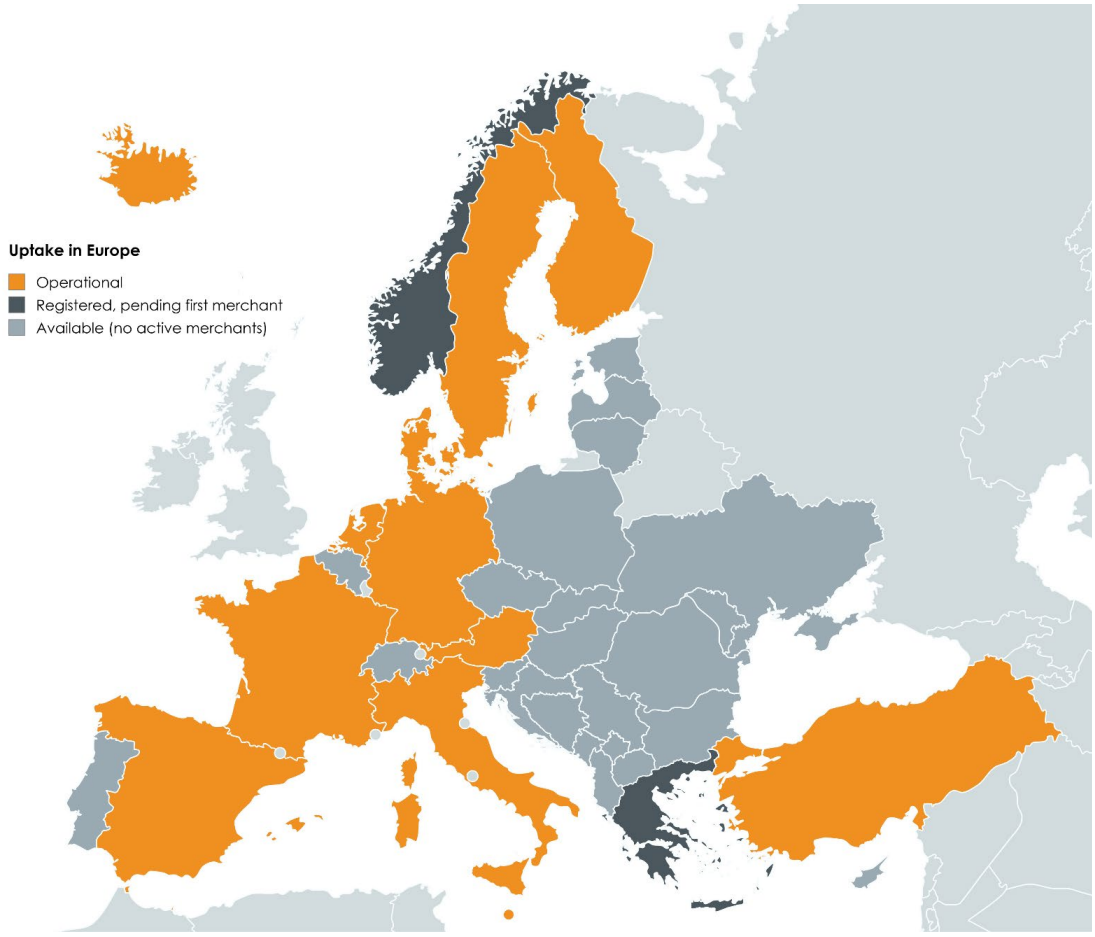

Figure 5.1: Participating identity federations in InAcademia as of the end of September 2024 (created with mapchart.net)

The reporting period started with two 'community' customers and five 'commercial' customers. By the end of the reporting period, an additional two 'commercial' customers had joined.

The customers that registered to InAcademia during earlier project cycles continued to increase the scope of their use of the service, increasing the number of validations processed by the service. The InAcademia DevOps team continued to inform federation operators about any misconfigured IdPs identified during the operation of the InAcademia service, particularly in the Turkish national identity federation, YETKİM, which has recently grown due to the success of the InAcademia sister service, MyAcademicID [MyAcademicID]. The participating identity federations are outlined in the following table.

Country	Identity Federation	Status
Austria	eduID.at	Operational
Denmark, Iceland and Greenland	WAYF	Operational
Finland	HAKA	Operational
France	Fédération Éducation–Recherche	Operational
Germany	DFN AAI	Operational

Country	Identity Federation	Status
Greece	GRNET	Registered in Federation, pending first merchant
Italy	IDEM	Operational
Spain	SIR	Operational
Sweden	SWAMID	Operational
The Netherlands	SURFconext	Operational
Norway	Feide	Registered in Federation, pending first merchant
Turkey	YETKİM	Operational
Uganda	RIF	Pathfinding pilot
New for this reporting period:		
Malta	RicerKaNet Identity Federation	Operational

Table 5.2: Participating identity federations in InAcademia as of the end of September 2024

The monthly number of InAcademia validations for the reporting period is presented in the following Figure 5.2. For comparative analysis the chart also presents the statistics for the same period of the previous year. History shows that there are seasonal trends of affiliation validations which peak at the beginning of the academic year and reach low points during the summer break. Comparing the same months of consecutive years, steady growth in the number of validations can be observed. The highest recorded numbers are 379K validations in September 2024.

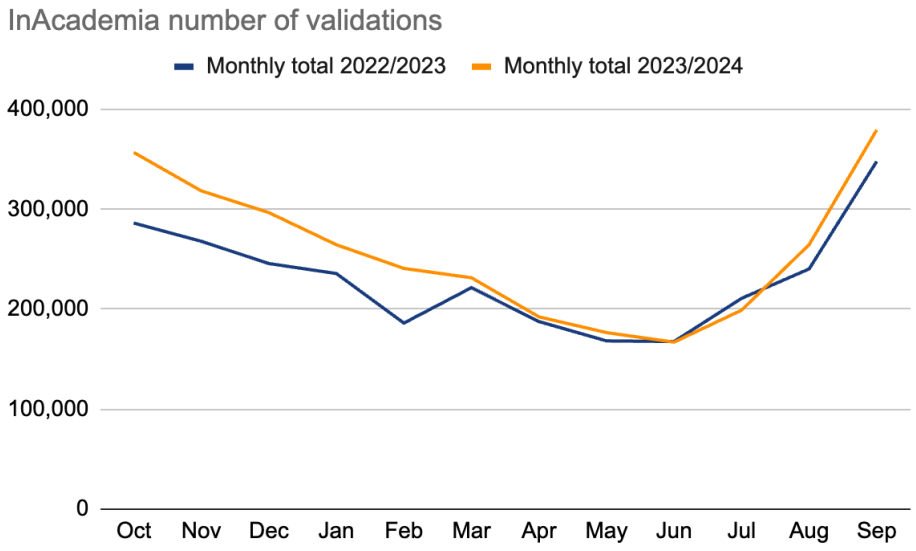

Figure 5.2: Monthly number of InAcademia validations

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 the NREN for Uganda (RENU) signed the necessary sublicense agreements that marked the commencement of a 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

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

KPI	Baseline (start of GN5-1)	Target (end of GN5-1)	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	11*

Note:

* Plus 3 national federations where InAcademia is registered and ready for business, but without active merchants (GRNET AAI, Feide and RIF).

Table 5.3: InAcademia KPIs for the reporting period

5.4 Activities and Issues

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

5.4.1 Development and Operations

New software releases during the period, all of which improve the merchants' and users' experience and ensure the product is well maintained, included:

- SVS 4.6.0, January 2024: User consent screen updated for enhanced accessibility.
- SVS 4.6.1, February 2024: Introduced support for pysaml2 v7.5.0.

Since the last SVS release, significant effort has been invested in development as follows:

- The InAcademia plugin for WooCommerce, created in the last period, progressed beyond PoC. This will become a new onboarding channel to attract small-to-medium enterprises that wish to add a feature to validate eligibility for student discounts to their checkout process. Development and testing of the technical onboarding and offboarding procedures based on the design principles agreed upon in the previous period were completed. Additional work was carried out with the related GÉANT functions:
  - Full IPR analysis performed.
  - Produced merchant/subscriber-facing 'click to accept' terms and conditions.
  - Privacy analysis performed and privacy statement produced.
  - Financial regulatory compliance and associated configuration of finance rules to ensure compliance when processing fees from subscribers.
  - Completed WordPress mandatory review.
  - Finalised the service model and updated inacademia.org ready for release.

- Working with the Core AAI team, a new, branded SeamlessAccess-based discovery service for InAcademia [InAcademia_Discovery] was implemented in production, retiring the previous unbranded discovery service. The new, branded service is shown in the following figure:

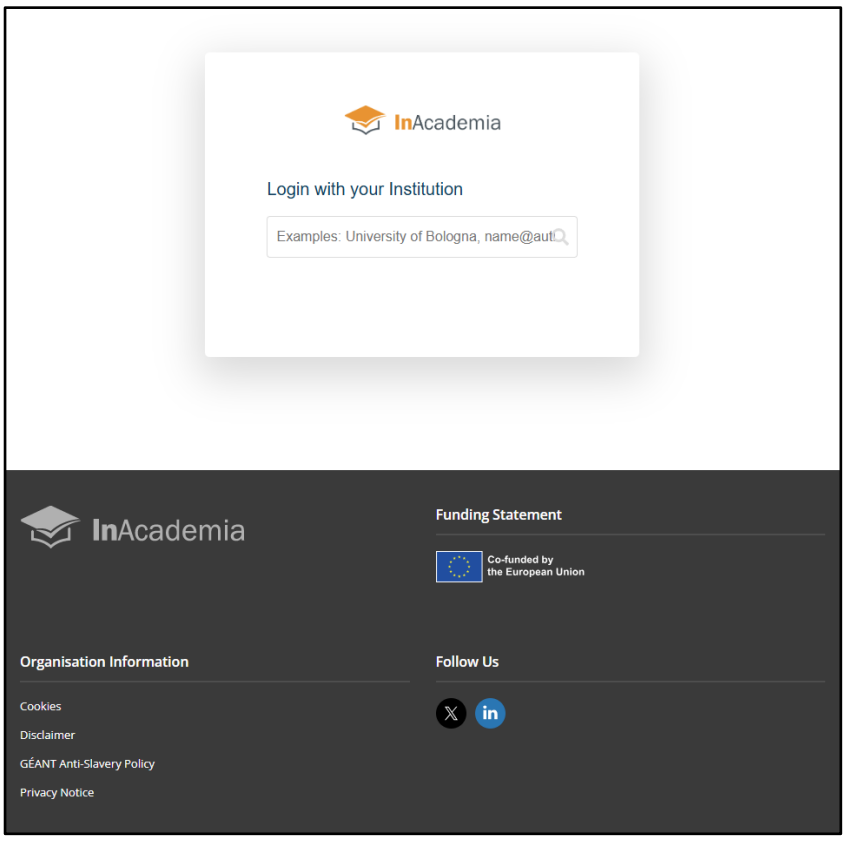

Figure 5.3: InAcademia's new SeamlessAccess-based Discovery service

5.4.2 Outreach and Business Development

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

- Hosted two InAcademia Steering Committee meetings.
- Worked bilaterally with each federation that is interested in participating in the service, with more detailed conversations undertaken with:
  - Feide/Norway, where we completed the registration process, and continued investigations as to how to raise awareness amongst Feide members.
  - Belnet/Belgium, where discussions were held with a representative of Belnet Federation to discuss potential options for InAcademia in Belgium, and how any policy change might be approached.
  - The service's largest customer started using InAcademia in Malta at the request of RickerkaNet Identity Federation in February 2024, making it the 11th identity federation to participate in the InAcademia service.
  - Discussions continued on possibilities for collaboration with SAFIRE, South Africa and InCommon, USA.
  - The Sublicensor Agreement for the Ugandan NREN, RENU, to offer InAcademia to Ugandan merchants as part of a regional pathfinding pilot, was completed.

5.4.3 Issues

It continues to be difficult to migrate long-term, commercial users of eduGAIN to InAcademia, because they perceive it as a fee being levied for reduced functionality (InAcademia limits personal information being released and pseudonymises the user information). While many services are expressing interest in using InAcademia, the team is finding it challenging to convert that interest to usage, as:

- It is difficult to give evidence of coverage unless the service is operational in that country.
- Often only publicly funded institutions are included in the national federation, meaning that merchants need to find a number of different solutions in order to validate user affiliation across all higher education facilities in a specific country.

It is proving very difficult to make the product visible to the commercial, business-to-business market as it is a very crowded retail marketing space. Differing approaches are being assessed by activities that are funded outside the GÉANT project, however, during the reporting period, this activity resulted in onboarding two new merchants, making a lifetime total of 9:

- Student Mobility BV, the very first EU train booking engine focusing on students and youth [StuMob].
- Prodigy Finance, "borderless" student loans for international students [ProdFin].

6 Incubator Activities

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, policy and business models that currently do not (yet) have a place in the services or technology stack of the T&I ecosystem in GÉANT. This may include testing and experimenting with potential new features for services or technology in T&I areas; business case development for potential new services and developments that would improve data protection and privacy aspects in services or software is also in scope.

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

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

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

6.1 Key Performance Indicators

The Incubator KPI measures the number of activities (topics) carried out during the GN5-1 project. Table 6.1 shows that the Incubator completed four activities in the first cycle in 2023 and achieved its objective for the first year. With the next cycle for 2024 completing four more activities by April 2024, this KPI has already been met. An additional four Incubator activities have since begun, so there is a chance that the targeted value will be exceeded by the end of GN5-1 if these activities are completed.

KPI	Baseline (start of GN5-1)	Target	Achieved result (by end of reporting period)
Number of topics that went through the incubator cycles	0	2023: 4 2024: 8	8*

Note:

* Another 4 activities have started in this period and should be completed by the end of GN5-1, bringing the total to 12.

Table 6.1: Incubator KPIs at the end of October 2024

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 GN5-1 project and ultimately for the European NREN community.

Participants, who are usually students, and their mentors are nominated by their local GÉANT partner and 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 the third activity cycle, unfortunately no new students were enrolled into the TIM programme. Even though several applications were received, none were found to be suitable. It is worth mentioning that the TIM student from CyNet, enrolled in the previous cycle, was offered a position at a local institution and was subsequently offered by CyNet as a participant to the GÉANT project, which we were very happy to take onboard.

It is planned that the TIM programme continues in GN5-2. The goal is again to support at least two candidates per activity cycle. More information about this initiative is available on the GLAD public Wiki page [GLAD TIM].

6.3 Outreach Activities

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

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

Name	Type	Reference
Incubator home	Public Wiki page	https://wiki.geant.org/display/GWP5/T5+-+Trust+and+Identity+Incubator
Dashboard	Public Wiki page	https://wiki.geant.org/x/kQATIw
Call for ideas	CONNECT article	https://connect.geant.org/2024/04/03/call-for-submissions-for-the-trust-and-identity-incubator-closes-shortly-2
Community demo invitation	CONNECT article	https://connect.geant.org/2023/08/30/trust-identity-incubator-demo-online-7-september-2023
Public sprint demos	Presentations	https://wiki.geant.org/x/VAVBJg
GN5-1 TIM announcement	CONNECT article	https://connect.geant.org/2024/02/19/trust-identity-incubator-mentorship-programme-returns-for-2024
GLAD TIM promotion	Public Wiki page	https://wiki.geant.org/x/AQJBJg

Table 6.2: Actions and measures for communicating with interested parties

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

Subject	Event	Target Group*				Reference
		R&E	NREN	GC	IN	
Incubator workshop on auto SP deployment	Online event 12-12-2023	✓	✓	✓		https://events.geant.org/event/1586
Incubator workshop on SAML signature validation	Online event 12-12-2023	✓	✓	✓		https://events.geant.org/event/1585
T&I Incubator Demo	Online event 23-01-2024	✓	✓	✓		https://events.geant.org/event/1437

Subject	Event	Target Group*				Reference
		R&E	NREN	GC	IN	
Attending and presenting at multiple sessions, Incubator side-meeting	TIIME Unconference	✓	✓	✓		https://tiime-unconference.eu/
T&I Incubator Demo	Online event 02-05-2024	✓	✓	✓		https://events.geant.org/event/1439
T&I Incubator Demo	Online event 17-09-2024	✓	✓	✓		https://events.geant.org/event/1716

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

In the third GN5-1 Incubator cycle (Cycle 9), the usual community approach [Incubator_CFI] was used again to select the topics. One activity (OpenID PoC for eduGAIN) was defined in collaboration with the eduGAIN service owner.

In collaboration with the GÉANT Association, NRENs and community partners, the Incubator has revived the Trust and Internet Identity Meeting Europe [TIIME]. This unconference-style meeting was held from 2013–2020 as the only T&I innovation conference in Europe focusing on R&E. The 2024 edition of the conference was held in Copenhagen and was very well received. Approximately 150 participants from all over Europe and beyond joined. Many participants from other sectors were also present. This important event will return in early 2025 with a new TIIME conference being organised in Reading, UK, to serve as a platform for sharing new and innovative ideas within the T&I community, which will ultimately serve as a source of projects for future Incubator cycles.

6.4 Activities and Issues

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

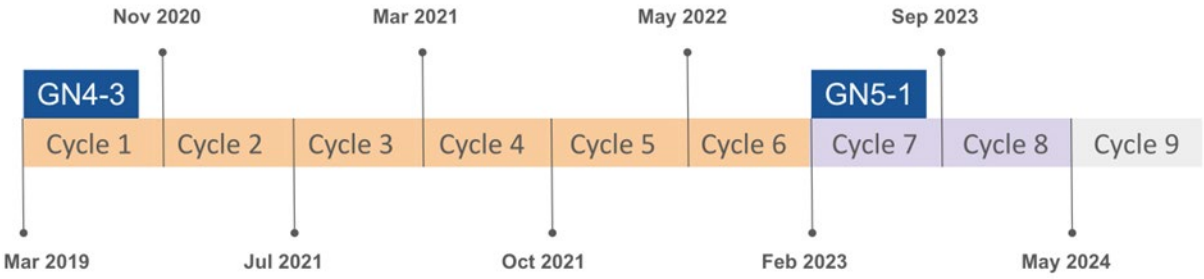

Figure 6.1: Timeline showing GN4-3 and GN5-1 start dates

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

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

Table 6.4: Schedule of GN5-1 Incubator cycles

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

6.4.1 Cycle 8 Activities (Completed)

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

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

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

This activity investigates a proxy approach to aggregate the services and potentially simplify the deployment and integration of tools. The goal is to create a PoC of at least one scenario and present it to federation operators.

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

Scalable Testing for Insecure SAML Signature Validation

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

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

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

Trust Fabric for Wallets

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

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

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

Webwallet for Research Use Case

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

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

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

6.4.2 Cycle 9 Activities (In Progress)

eduGAIN OpenID Federation PoC

The eduGAIN service activity will set up a PoC in order to evaluate the new OpenID Federation (OIDfed) [OIDfed] standard and wants to eventually create an official eduGAIN Technology Profile to extend the current service.

The Trust and Identity Incubator has over the years accumulated considerable experience of developing tooling, implementing OpenID Federation in various products and languages, and evaluating e.g. REFEDS specifications in the context of OpenID Federation.

This activity seeks to contribute to the eduGAIN PoC by:

- Sharing existing experience and providing a sparring partner to the eduGAIN PoC team.
- Contributing to standards and policy development for eduGAIN and national federations (upon request of the eduGAIN PoC team).
- Developing or further enhancing software tools, including, but not limited to:
  - Contributing to existing software development for the eduGAIN PoC.
  - Building a (scalable) resolver which can be deployed by federation operators and eduGAIN.
  - Further improving visualisation and reporting tooling.
  - Further improving Go-based OpenID Relying Party (RP) and OpenID Provider (OP).

The Incubator will work on these in close collaboration with the eduGAIN PoC team.

Implement OpenID Federation into SimpleSAMLphp and Shibboleth IdP

Related to the above eduGAIN OpenID Federation pilot, it is necessary to add OpenID Federation capabilities to commonly used software in our ecosystem. This activity will complete the work on implementing OpenID Federation into SimpleSAMLphp [SimpSAML], as well as starting on an implementation for Shibboleth IdP [ShibIDP]. A Go implementation was also created [Go_OIDfed].

The activity is conducted in close collaboration with subject-matter experts in CSC (Shibboleth) and SRCE (SimpleSAMLphp).

TI-Wizard

Managing the relations between services and identity providers is a challenge for emerging adopters of federation technologies, collaborative organisations and institutions alike. Typically technical complexity and a steep learning curve are the limiting factors in the ability to manage a SAML- or OIDC-based ecosystem.

A Graphical User Interface (GUI) may help reduce the complexity of managing the environment, as it provides a single integration and organisational interface for managing the relations. Even so, current proxy products are still rather technically inclined and do not provide an easy-to-use interface to configure the entities.

This activity takes inspiration from the prototype built in the TIM programme in the previous cycle and aims to create a (browser-based) GUI to allow (proxy) IdP and SP operators to easily configure them. The GUI will be built in such a way that it can be deployed independently from the product. A reference implementation will then be built for both SimpleSAMLphp and SaToSa.

Verifiable Credentials Schema for eduPerson, SCHAC and voPerson

W3C Verifiable Credentials (VC) are increasingly important to our community with the rise of decentralised identity and wallet ecosystems. Several VC-based credential definitions already exist for expressing skills and

micro-credentials, such as the Open Badges 3.0 specification. However, there is no consistent and community-driven definition for expressing the 'identity-related' credentials of the commonly used schema managed by REFEDs, such as eduPerson, SCHAC and voPerson.

The REFEDS schema board is setting up a subcommittee [VC Subcommittee] to define the VC representations of these well-known credentials so they may be used in an standardised and interoperable way. Several members of the incubator team will join this activity in REFEDs to learn and share.

7 Distributed Identity Activities

There has recently been a strong movement to make the whole identity space more user-centric to allow users greater control of their identities (and other related information) and a more active role in the process of sharing their information with other parties.

This task explores the use cases that would be better supported via distributed technologies and the implications on the current services and infrastructure used in the R&E community.

7.1 Analysis Work

To gain an overview of the field of distributed identities, we used the Trust-over-IP model to break it down into components for individual analysis. This is to gain an overview of the topic at hand, its opportunities, risks, and transformative aspects, as well as ongoing engagements in our community. Due to the high activity in this field this is by no means conclusive, but rather to be considered a snapshot.

The most important driver for distributed identities in Europe is the EC, with its policy push [EC_eID] towards universities in the areas of mobility (Erasmus+ and alliance forming) and identity (eIDAS). The latter in particular is expected to become relevant in other sectors as well and will allow our community to better serve cross-sectorial use cases in the future and to profit from common tooling.

While today's identity services operated in the research and education sector enjoy high adoption and high readiness, the emerging standards, tools and services in the field of distributed identities are still in their infancy and are of experimental nature, with important aspects still out of scope.

There is substantial engagement in our community in the area of distributed identity. Several NRENs and GÉANT are participating in the EC-funded LSPs (Large Scale Pilots) for the EUDI (European Digital Identity) wallet [EUDI_LSP]. Most prominent is DC4EU (Digital Credentials for Europe) [DC4EU], where education use cases are being explored. A small number of NRENs are participating in the national EUDI wallet activities as well. The Incubator and eduGAIN tasks of WP5 are running a PoC for the OpenID federation, which is a trust mechanism that is fit to be used within our sector to complement usage of the eduGAIN trust fabric for the wallets.

7.2 Identified Opportunities and Risks

Based on the analysis, a high-level risk assessment was carried out to help devise recommendations on the next steps to take to best serve our community.

We identified opportunities for funding attached to the EC policy push, the ability to easily scale use cases reaching beyond the R&E sector, and synergies by using cross-sectorial solutions.

Substantial risks were identified in the still-uncertain positioning of GAFAM (Google, Apple, Facebook. Amazon, Microsoft) with respect to embracing the emerging EC standards; uncertainties around user acceptance due to the still-experimental state of standards and tooling; and also governance issues due to the shift of responsibility from IdPs to end users. Another area of substantial risk is the adoption of the new EU policies on a global scale: use cases for the wallets in R&E need to be considered in the context of preserving global interoperability, which is inherently important for the R&E sector.

7.3 Interim Conclusions and Dissemination

Continued monitoring, analysis, and dissemination in our community remains important. The level of activity in the field of distributed identities is going to stay very high and gaining an oversight of relevant activities is difficult for the community members.

There is already considerable engagement in our community in areas relevant to distributed identities, namely standardisation, trialling of new solutions, and leveraging existing (inter-)federation services. We need to network these players and work towards establishing a community consensus.

The EU policies need to be transformed into national law and many details affecting our community will be decided on that level. To get the best out of the efforts spent, we need to make use of our NRENs to effectively lobby on a national level for our community consensus positions.

These interim conclusions were shared in a well-attended infoshare that this task organised for the GÉANT members in September 2024, with over 100 participants [CONNECT Infoshare].

7.4 Outlook

During the remaining months of the project, a white paper will be written to summarise the findings of this task. This work will continue in GN5-2, with a sub-task dedicated to this work.

8 Outreach Activities

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

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

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

8.1 Engagement with Key Stakeholders and Other Sectors

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

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

During the reporting period, this task was organising regular meetings with the business development teams in WP5, WP3, and WP4, facilitating the planning and information exchange. The work on the business development itself, and details of any additional outreach activities, are included in the respective sections on each service.

8.2 Liaison with and Contribution to External Projects and Initiatives

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

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

Interoperable Global Trust Federation (IGTF) and AARC Community

The Task contributed to the AARC/IGTF work on Guidance for notice management by Proxies (G-083) and Trust in Distributed Proxy Scenarios (I-082).

Federated Identity Management for Research (FIM4R)

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

Outreach was undertaken again in person on the whole range of the work of the Task at the International Symposium on Grids & Clouds (ISGC) 2024 Conference [ISGC_2024] and a dedicated FIM4R co-located with the TIIME workshop [TIIME_2024].

eduGAIN Service

The task contributed to the realisation of the eduGAIN CSIRT tabletop exercise as mentioned in the eduGAIN chapter.

8.3 AEGIS

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

In 2024 the AEGIS community had 9 member infrastructures, and grew from 10 to 11 observer infrastructures [AEGIS]. The WP5 Enabling Communities Task facilitates the work of AEGIS by offering the necessary support to manage the group and the calls that are organised on a monthly basis, along with facilitating the work of the Architecture Working Group. AEGIS held 7 online meetings during the reporting period.

9 Conclusions

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

New ideas in the T&I space in research and education have been developed, fostered and matured in the T&I Incubator (Task 5). The annual CTO workshops are a venue for discussion with the GÉANT membership on the strategic direction of the GEANT T&I area.

The 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 GN5-1 project and to create a better communication channel with other projects and communities.

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.

References

[AARC_BPA] https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf
[AARC-G071] https://aarc-community.org/guidelines/aarc-g071/
[AEGIS] https://wiki.geant.org/display/AARC/AEGIS
[AEGIS_Charter] https://aarc-project.eu/wp-content/uploads/2019/12/AEGIS-Charter-v1.0.pdf
[ARF] https://code.europa.eu/eudi/architecture-and-reference-framework
[Blast-RADIUS] https://www.blastradius.fail/
[Commons_Conservancy] https://commonsconservancy.org/
[DC4EU] https://www.dc4eu.eu/
[EC_eID] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61682
[EDIWARF] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework
[eduGAIN] https://www.edugain.org
[eduGAIN_Const] https://technical.edugain.org/doc/eduGAIN-Constitution-v4-final.pdf
[eduGAIN_FWG] https://wiki.geant.org/display/eduGAIN/eduGAIN+Futures+Working+Group+Charter
[eduGAIN_Monitor] http://monitor.edugain.org/coco/
[eduGAIN_Pol] https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf
[eduGAIN_Profile] https://technical.edugain.org/doc/eduGAIN-saml-profile.pdf
[eduGAIN_Support] https://wiki.geant.org/display/eduGAIN/eduGAIN+support
[eduGAIN_SupportDocs] https://wiki.geant.org/display/eduGAIN/eduGAIN+support#eduGAINsupport-eduGAINSupportKnowledgeDatabase
[eduGAIN_Tech] https://technical.edugain.org
[eduGAIN_UStories] https://edugain.org/edugain-users/
[eduroam] https://www.eduroam.org/
[eduroam_CAT] https://cat.eduroam.org/
[eduroam_db] https://monitor.eduroam.org/fact_eduroam_db.php
[eduroam_geteduroam] https://www.geteduroam.app
[eduroam_ManIdP] https://hosted.eduroam.org
[eduroam_ManSPPilot] https://msp-pilot.eduroam.org/
[eduroam_Monitor] https://monitor.eduroam.org/
[eduroam_PolDecl] https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-194_eduroam-policy-for-signing_ver2-4_1_18052012.pdf [this document is being updated; the link is to the current official published version]
[eduroam_ServDef] https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf [this document is being updated; the link is to the current official published version]
[EOSC_AAI] https://op.europa.eu/en/publication-detail/-/publication/d1bc3702-61e5-11eb-aeb5-01aa75ed71a1/language-en/format-PDF/source-188566729
[EOSC_EU_Node] https://open-science-cloud.ec.europa.eu
[EOSC-Life] https://www.eosc-life.eu/
[EOSC_Proc] https://eosc.eu/news/2023/11/european-commission-announces-results-of-the-eosc-procurement
[EPICUR] https://epicur.edu.eu/
[Erasmus+] https://ec.europa.eu/programmes/erasmus-plus/node_en
[ESCI] https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en

[EUDI_LSP] https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet
[EUGridPMA] https://www.eugridpma.org
[EurAA] https://ec.europa.eu/social/main.jsp?catId=1202
[EUROfusion] https://euro-fusion.org/
[EuroHPCFP_Proc] https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=15701
[FENIX] https://fenix-ri.eu/
[FIM4R] https://fim4r.org
[GLAD_TIM] https://wiki.geant.org/x/AQJBJg
[GN5-1_Passkeys_Intro] https://wiki.geant.org/display/GWP5/Passkey?preview=/589070371/633276338/Introduction%20to%20Passkeys%20Usage%20and%20Implementation.pdf
[GN5-1_WP_Passkeys] https://resources.geant.org/wp-content/uploads/2023/11/GN5-1_White-Paper_Passkeys-Use-and-Deployment-for-RE-Services.pdf
[GN5-1_WP_Passkeys_Zenodo] https://doi.org/10.5281/zenodo.10210492
[GN_AAI] https://wiki.geant.org/display/GSPP/GEANT+AAI+Service
[Go_OIDfed] https://github.com/zachmann/go-oidfed
[I2ComEx_2023] https://internet2.edu/2023-internet2-community-exchange/
[IDPy_OIDC] https://github.com/IdentityPython/idpy-oidc
[IDPy_SATOSA] https://github.com/IdentityPython/SATOSA/pull/439
[InAcademia] https://www.inacademia.org
[InAcademia_Branding] https://inacademia.org/branding/
[InAcademia_Discovery] https://inacademia.org/inacademia-implementation-guidelines/#321_Allow_the_user_to_search_for_the_institution_using_a_Discovery_Service
[InAcademia_Reg] https://inacademia.org/registering-your-service/
[InAcademia_SvcPol] https://inacademia.org/service-policy/
[Incubator_AofSPs] https://wiki.geant.org/x/goqBJw
[Incubator_CFI] https://wiki.geant.org/x/jwATIw
[Incubator_Dashboard] https://wiki.geant.org/x/kQATIw
[Incubator_FItPPP] https://wiki.geant.org/x/IIAcIw
[Incubator_gLC] https://wiki.geant.org/x/KoAcIw
[Incubator_Method] https://wiki.geant.org/x/NbAuBw
[Incubator_OSoS] https://wiki.geant.org/x/J4AcIw
[Incubator_PforR&E] https://wiki.geant.org/x/I4AcIw
[Incubator_STfISSV] https://wiki.geant.org/x/_YmBJw
[Incubator_TFfW] https://wiki.geant.org/x/ioqBJw
[Incubator_WWfRUC] https://wiki.geant.org/x/f4qBJw
[ISGC_2023] https://indico4.twgrid.org/event/25/
[LAGO] http://lagoproject.net/
[LUMI] https://www.lumi-supercomputer.eu/
[MyAcademicID] https://wiki.geant.org/display/SM/MyAcademicID+Identity+and+Access+Management+Service
[MyAccessID_IAM] https://wiki.geant.org/display/MyAccessID/MyAccessID+Home
[OIDfed] https://openid.net/specs/openid-federation-1_0.html
[PaNOSC] https://www.panosc.eu/
[Puhuri] https://puhuri.io/
[REFEDS] https://refeds.org/federations
[REFEDS_AnonAccess] https://refeds.org/category/anonymous
[REFEDS_CoCo] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
[REFEDS_PersAccess] https://refeds.org/category/personalized
[REFEDS_PseudAccess] https://refeds.org/category/pseudonymous
[REFEDS_R&S] https://refeds.org/research-and-scholarship
[REFEDS_SIRTFI] https://refeds.org/SIRTFI

[Scrum]	https://scrumguides.org/scrum-guide.html
[SeamlessAccess]	https://seamlessaccess.org/ https://seamlessaccess.org/about/governance/
[SeamlessAccess_demo]	https://demo.beta.seamlessaccess.org
[SimpSAML]	https://github.com/simplesamlphp/openid
[Shibboleth_Roadmap]	https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/1120895029/Project+Roadmap#Under-Discussion
[ShibIDP]	https://git.shibboleth.net/view/?p=java-idp-oidc.git;a=summary
[SRAM]	https://www.surf.nl/en/surf-research-access-management-easy-and-secure-access-to-research-services
[SSHOC]	https://sshopencloud.eu/
[T&I_Roadmaps]	https://wiki.geant.org/display/GWP5/Trust+and+Identity+Services+Roadmaps
[TechEx23]	https://internet2.edu/2023-internet2-technology-exchange/
[TIIME]	https://tiime-unconference.eu/
[TNC23]	https://tnc23.geant.org/programme/
[TNC24_MobDay]	https://wiki.geant.org/display/TFMNM/Mobility+Day+at+TNC24
[Uni_Alliances]	https://education.ec.europa.eu/education-levels/higher-education/european-universities-initiative
[VESPA]	http://www.europlanet-vespa.eu/
[WCAG2.1]	https://www.w3.org/TR/WCAG21/
[Wi-Fi]	https://www.wi-fi.org/
[wwWallet]	https://github.com/wwWallet
[wwWallet_Ecosystem]	https://wwwallet.github.io/wallet-docs/

Glossary

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

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

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