25-05-2017

Deliverable D5.2
Service Delivery and Operations Report

Deliverable 5.2

Contractual Date:	30-04-2017
Actual Date:	25-05-2017
Grant Agreement No.:	731122
Work Package/Activity:	5/SA2
Task Item:	Task 2 and Task 3
Nature of Deliverable:	R
Dissemination Level:	PU
Lead Partner:	CARNet/SRCE
Document ID:	GN4-2-17-197CB5
Authors:	I. Golub (CARNet); M. Milinović (CARNet/SRCE); A. Delvaux (PSNC); R. Karlsen-Masur (DFN); N. Ilić (AMRES); T. Wolniewicz (PSNC); M. Adomeit (AMRES).

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Abstract
This document reports on services operated in GN4-2 by SA2 T2 and T3. Technical and operational service descriptions, data on users, uptake and usage, KPIs, and information on activities and issues occurring in the reporting period as well as contact details, are provided for each service.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document reports on the services operated by Tasks 2 and 3 of the Trust & Identity and Multi-Domain Services activity (SA2), which is responsible for operating, monitoring and managing GN4-2 services in production. It covers the activities and status of the services in the first ten months of the GN4-2 project, from the start of May 2016 to the end of February 2017.

During the reporting period, SA2 operated and provided support for six services. Trust and Identity services - eduroam, eduGAIN, Federation as a Service (FaaS) and eduPKI are operated in Task 2 ("Trust & Identity"), while the "Multi-Domain Services" Task (SA2 Task 3) managed perfSONAR and the Brokerage service catalogue. SA2 ensures that the services it operates in production are provided with the infrastructure and support needed to run at the required level. Additionally it executes the day-to-day operation and maintenance of the services following the DevOps paradigm first adopted in GN4-1.

In addition to the operation and maintenance of the services in production, the team worked on the harmonisation of services, the formalisation of business processes, and the creation of a knowledge database, including a set of relevant documents that capture service resources, assets and operational guidelines for internal use by operations teams. Work was started on defining baselines and policies for service operations aspects such as monitoring, backup and archiving, etc. The team is also actively looking at potential continual service improvements in collaboration with the Service Optimisation Task (SA2 Task 4).

GÉANT Trust & Identity and Multi-Domain services are presented in this document, including service descriptions, technical descriptions of the solutions, data on operations and support teams, users, update and usage and Key Performance Indicators (KPIs), and information on activities and issues occurring in the reporting period.

All services have reported progress in terms of increase in usage and footprint and stable operations, and all have exceeded their KPIs for the period. This was all achieved through a strong collaboration between team members within the Activity, as well as with other relevant GÉANT project research, service and networking activities.

1 Introduction

GN4-2 Service Activity 2 (SA2) – Trust & Identity and Multi-Domain Services, delivers and operates services in production, including the Trust & Identity services eduroam, eduGAIN, eduPKI and FaaS, operated by Task 2, and the Multi-Domain Services perfSONAR and the Brokerage Service Catalogue, managed by Task 3:

- eduroam provides a secure, worldwide roaming access service for the international research and education community.
- eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community.
- eduPKI enables certification of GÉANT services that are unable to obtain the needed certificates through other standard bodies.
- FaaS supports GÉANT NREN organisations that have yet to establish their own Identity Federation.
- perfSONAR's active network monitoring suite is provided through GN4- 2 SA2 T3's collaboration with the global perfSONAR team, and its active and target users are organisations, Network Operations Centers (NOCs) or Performance Enhancement Response Teams (PERTs) and individuals world-wide managing and operating communication networks, either within a single domain of administration or in multi-domain environments.
- The Brokerage Service Catalogue provides information on the cloud services offered to the GÉANT community, either by GÉANT or by commercial service providers. The existing Brokerage Service Catalogue is due to be replaced by a new Cloud Service Catalogue that is currently being designed and developed by JRA4.

SA2 ensures that services in production are of acceptable quality, that the relevant procedures, processes and documentation are in place for their efficient operation, and that their operational health and usage are monitored and reported to stakeholders. In addition, the activity coordinates all processes for the transition of services to operations, as well as the various teams involved in the process, to ensure that the services are run with minimal unplanned interruption and improved as needed.

For the purposes of improving service operations, operating teams in Task 2 and Task 3 of the activity also collaborate with the SA2 Task 4 – Production Optimisation team, which is dedicated to the Continual Service Improvement (CSI) of SA2 services. Task 4 serves as a more neutral articulator of emerging improvement ideas and as a resource to provide guidance in their full formulation and implementation, helping to recognise common themes and issues, and formulate best practices across services. All SA2 teams have been working in close collaboration to note and implement initial service improvement opportunities, which are summarised in Deliverable D5.1 "Analysis of Service Elements and Optimisation Opportunities".

This document reports on the status of the services and products operated by SA2 and the related operations and DevOps efforts in the first ten months of the project – from May 2016 to February 2017.

Section 2 presents an overview of all the services operated by SA2, followed by descriptive sections for each individual service, including the four Trust and Identity services (eduroam, eduGAIN, eduPKI and FaaS) and the two Multi-Domain services (perfSONAR and the Brokerage service catalogue). These present an overall description of each service including a technical and operational description, data on users, uptake and usage and KPIs, and activities and any issues occurring during the reporting period. Contact details are also provided for each service.

Finally, some general considerations and comparisons between the services are presented in the Conclusions.

2 Trust & Identity and Multi-Domain Services

GÉANT and its NREN partners provide a number of services to the R&E community, which during their lifecycle transition from development through the pilot phase into production. In the previous GN4-1 project, for the first time in the history of GÉANT projects, a separate activity was created for the production of application services and infrastructure, catering to the transition and production operation of GÉANT services and products.

This division between the development and production operation of services proved very successful and is maintained in GN4-2, where SA2 handles the transition, production operations and optimisation of Trust and Identity (T&I) and Multi-Domain services, including eduroam, eduGAIN, Federation as a Service (FaaS) eduPKI, perfSONAR and the Brokerage Service Catalogue.

All Trust and Identity services and the Brokerage Service Catalogue rely on the infrastructure and support provided by GÉANT and its European NREN partners, while perfSONAR is developed and managed via international cooperation between ESnet, Internet2, Indiana University, University of Michigan, GÉANT project participants and many others.

The operation of all these services is provided in a federated manner. Team members come from different NRENs, or different organisations within an NREN or even based on different continents, and successfully cooperate in the offering, provisioning and daily operation of the services. The infrastructure for the services is also provided by different organisations within or outside of the GÉANT community.

In the sections that follow, the report provides information on the six services that were in production in SA2 T2 and T3 during the first ten months of the GN4-2 project. The reports provided for each service include a service description, a technical description (where appropriate), contact details for operations and support teams, data on uptake and usage and KPIs, and key activities and any issues encountered in service operations.

It is important to note that service KPIs reported here specifically capture the performance indicators for operation of those services in production. KPIs related to the uptake of services fall under the domain of the respective development activities and not within the scope of this report. However, in order to provide a holistic image of services operations in production, some basic uptake figures and trends are also given.

2.1 eduroam

The eduroam service has been recording continuous usage growth. Both operations and accompanying development activity work have focused on supporting services and onboarding users while at the same time maintaining the core and supporting technical infrastructure at the highest level of availability and reliability. eduroam is increasingly offered as a service beyond campuses or even used as an example (i.e. govroam). The eduroam service provided by GÉANT plays an important role in eduroam globally by contributing to the work of the Global eduroam Governance Committee (GeGC) and providing supporting services – eduroam database Configuration Assistant Tool (CAT), monitoring, authentication traffic measurement (f-ticks) – that are used around the world.

2.1.1 Service Description

The purpose of eduroam (education roaming) is to provide a secure, worldwide roaming access service for the international research and education community.

The eduroam service allows students, researchers and staff from participating institutions to obtain Internet connectivity on their mobile devices across their campuses and when visiting other participating institutions. The architecture that enables this is based on a number of technologies and agreements, which together provide the essential eduroam user experience: “open your laptop and be online”.

The basic principle underpinning the security of eduroam is that the authentication of a user is carried out at his/her home institution using the institution’s specific authentication method. The authorisation to access local network resources is granted by the visited network.

GÉANT operates the confederation-level service for members of the European eduroam Confederation, which is formed of autonomous roaming services who agree to a set of defined organisational and technical requirements by signing and following the eduroam policy declaration [eduroam_PolDecl] is based on the eduroam service definition [eduroam_ServDef]. The confederation’s goal is to provide a secure, consistent and uniform network access service to its users.

The European eduroam service is built hierarchically. At the top level sits the confederation-level service, which provides the confederation infrastructure required to grant network access to all participating members of the eduroam service together with a set of supporting services. This confederation service is built upon the national roaming services, operated by the national roaming operators (NROs – in most cases, NRENs). National roaming services make use of other entities, for example, campuses and regional facilities.

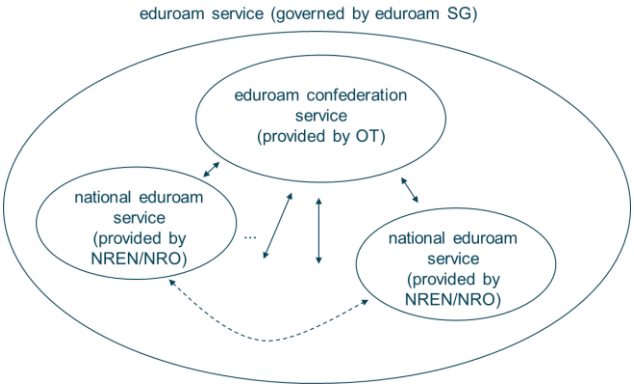

Figure 2.1: eduroam Service Model

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

In addition to operating the service's basic technical infrastructure, the GÉANT eduroam team also delivers a supporting services suite to facilitate the widespread deployment of eduroam. This suite includes a central database (eduroam db) with information about participating institutions, monitoring & metering tools (f-ticks) and a Configuration Assistant Tool (CAT) for end users and campus administrators.

2.1.2 Technical Description

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

2.1.2.1 *Core Services*

The eduroam confederation infrastructure relies on a distributed set of AAA (authentication, authorisation, and accounting) servers. The current configuration uses RADIUS as the AAA protocol. Currently eduroam supports transport over RADIUS/UDP (User Datagram Protocol) and RADIUS/TLS (Transport Layer Security), and recommends the use of RADIUS/TLS as preferable.

Routing of RADIUS messages is implemented in two ways: a baseline-routing model, based on a hierarchy of RADIUS servers, and a dynamic-routing model, based on DNS service discovery. The dynamic-routing model is only supported over RADIUS/TLS. This approach and rationale is described in detail in the eduroam Service Definition [eduroam_ServDef].

The (baseline) RADIUS hierarchy for a national eduroam federation consists of several RADIUS servers located at various institutions, and which are directly or indirectly connected to the federation-level RADIUS proxy server (FLRS).

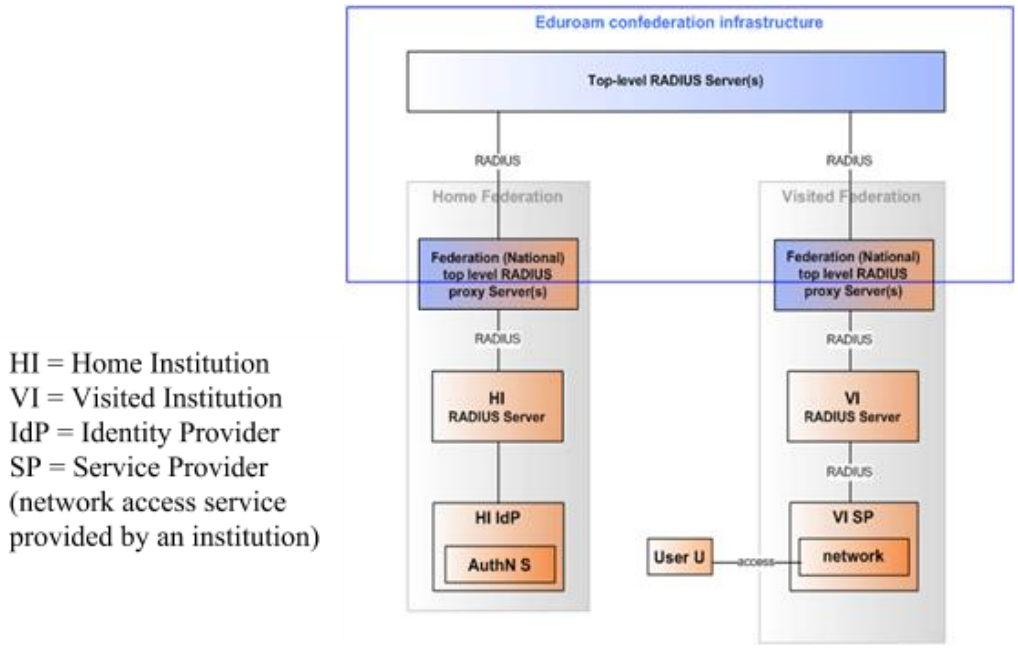

Figure 2.2: European eduroam confederation structure

The eduroam European top-level RADIUS servers (ETLRs) interconnect the participating eduroam federations. They provide the means to find the correct federation-level RADIUS server of a given user's federation, and to transport all information in a secure way. The eduroam ETLRs are maintained by SURFnet and DeIC, who are part of the eduroam Operations team.

In dynamic routing, eduroam Identity Providers (IdP) announce their responsible RADIUS server over DNS. eduroam Service Providers (SPs) that need to authenticate a user look up the appropriate RADIUS server by querying the Domain Name System (DNS) for a special eduroam server record.

This routing model does not require any intermediate RADIUS infrastructure, but can be used even in the presence of intermediates. In particular, if an eduroam IdP does not wish to deploy its own RADIUS/TLS-enabled RADIUS server, it can connect to the FLRS via a static uplink (hierarchical routing), and announce in the DNS record that the RADIUS/TLS endpoint is the IdP's FLRS. Similarly, an eduroam SP that does not wish to perform its own DNS lookups can statically connect its infrastructure to the FLRS. The FLRS in turn can then carry out the DNS lookups for that SP.

eduroam IdPs and SPs always need to have a static route to their FLRS configured as a "default" fall-back routing mechanism, because the publishing of DNS records for eduroam IdPs is optional. As a result, a default routing decision needs to be available should a DNS not yield the routing information.

Further details on the eduroam technical infrastructure are available in the eduroam Service Definition [eduroam_ServDef].

2.1.2.2 *Supporting Services*

The supporting services suite includes a central database containing important information about participating institutions (eduroam db), monitoring & metering tools (f-ticks) and a configuration

assistant tool for end users (CAT). The supporting services suite is maintained by the eduroam Operations Team.

The supporting services suite is designed and delivered to serve three main user groups with the most suitable level of access to targeted information:

- Federation-level personnel – NRO staff running service operations inside a country (federation).
- Institution-level personnel – staff running services at an institutional level (typically operating eduroam IdP and SP functions).
- End users – individuals who use eduroam technology to access the network, either at their home institution or when visiting other sites.

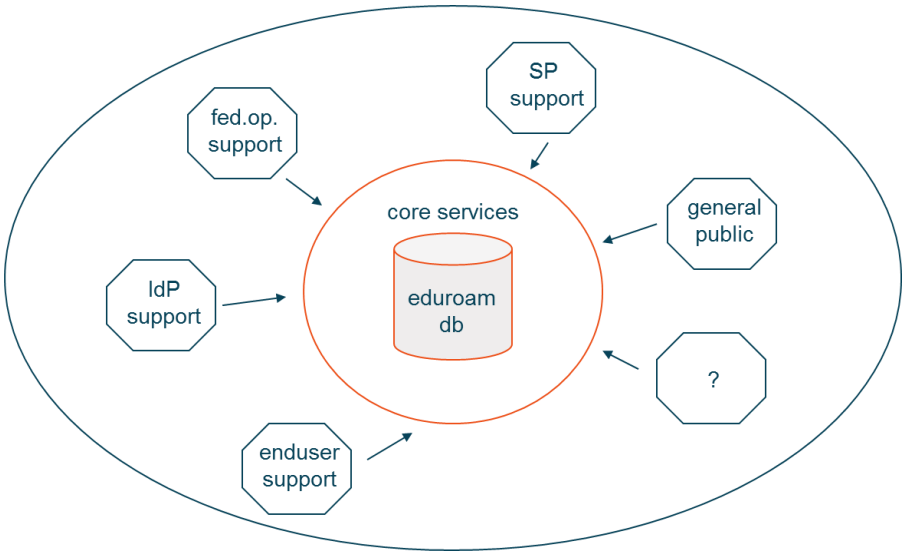

Figure 2.3: eduroam Supporting Services

Information about the core service is publicly available via the eduroam web site [eduroam] and includes references and links to extensive documentation for all user groups.

The web pages for the supporting services [eduroam_Monitor] are being expanded into a supporting suite portal to allow easier navigation and access for the services' respective user groups. The eduroam Configuration Assistance Tool has its own portal [eduroam_CAT].

Further details on the eduroam service description are available in the eduroam Service Definition [eduroam_ServDef].

2.1.3 Operations and Support Team

The eduroam Operations Team (OT) is responsible for running all core infrastructure and supporting services for eduroam, and for handling the required configuration and basic development of its tools using DevOps. The OT also serves as a point of contact for L2 support, escalating queries to higher support levels or appropriate groups. Certain queries not covered by current regulations are passed on to the eduroam Steering Group for discussion, while technical queries related to tools or processes developed by the research activity may be passed to the research activity. L1 support is provided by the GÉANT Helpdesk run by GN4-2 SA3.

The eduroam OT is composed of technical personnel from Srce (CARNet), SURFnet, DeIC and RESTENA. Srce (CARNet), SURFnet and DeIC also provide the technical infrastructure needed to run core and supporting services. Srce (CARNet) is providing the chair of the eduroam Steering Group, who also acts in the role of Service Manager responsible for managing service operations and support.

The contact details for eduroam for all users and interested parties are:

- Web: www.eduroam.org
- Support for users: eduroam@help.geant.org
- Support for National Roaming Operators: eduroam-ot@lists.geant.org
- eduroam Steering Group: eduroam@lists.geant.org

2.1.4 Users, Uptake and Usage

eduroam user data is provided on the eduroam monitor site [eduroam_Monitor]. All 39 GÉANT partners use the eduroam service, and this number remained unchanged during the reporting period. However, the number of NROs in Europe is 46, as these cover more European countries than those of the GÉANT partners.

2.1.5 Key Performance Indicators

eduroam KPIs measure the availability of its core service (European Top Level Radius servers). Table 2.1 shows that the services are running with at least one top-level roaming server 100% available, therefore performing better than the set target.

Name of the KPI	Baseline	Target	Measured
ETLR availability	99%	99.9%	100%

Table 2.1: eduroam KPIs – over the period 01 May 2016–28 February 2017

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

- National authN as grand sum of all successful roaming authentications in the same country counted via f-ticks system for all European countries that provide this info (for more info on f-ticks see the eduroam Monitor site [eduroam_Monitor]).

- International authN as total number of successful international (cross-border) authentications counted in the logs of ETLRs.

2016 was another year of expansion for eduroam, which saw a 23% increase in international authentications and a 26% increase in national authentications. In total, over 2.6 billion national authentications and more than 592 million international authentications were recorded. Figure 2.4 below illustrates these figures for the period from May 2015 to February 2017.

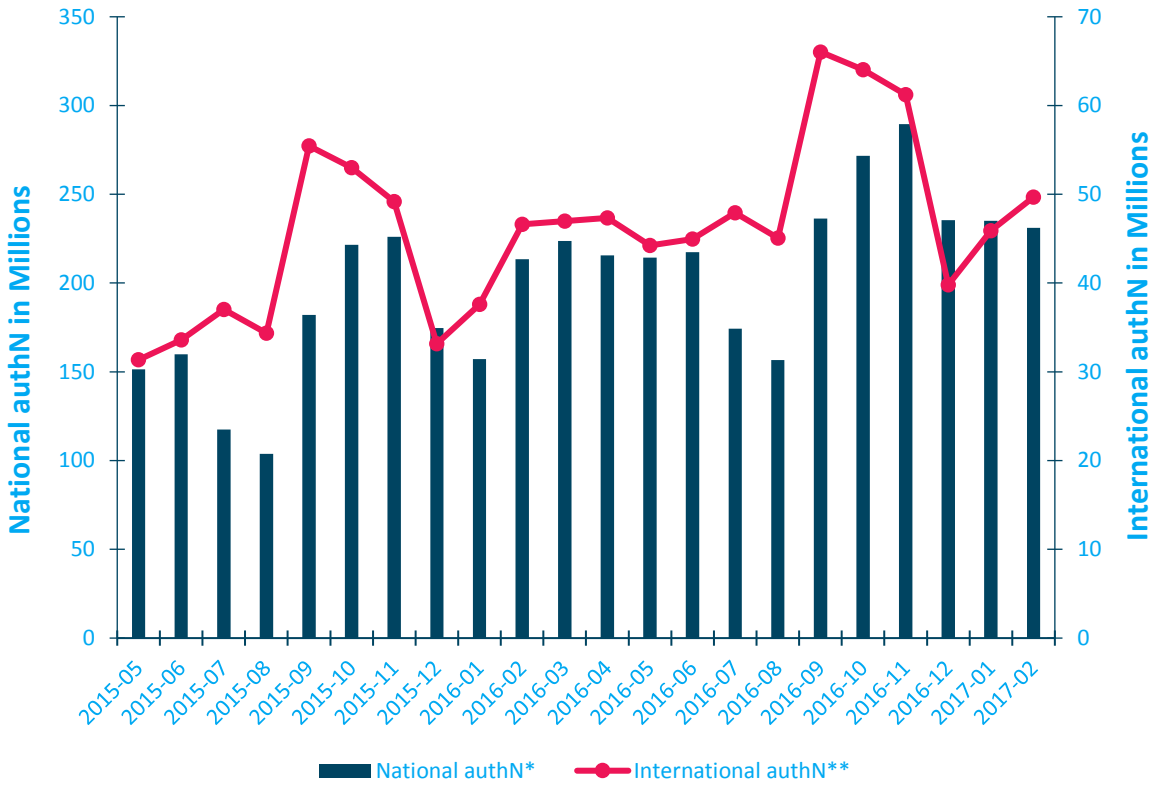

Figure 2.4: eduroam usage statistics: number of successful authentications per month

2.1.6 Activities and Issues

During the reporting period, the operations and support team dealt with standard day-to-day routine activities related to the service. eduroam core services were operated to a very high standard, with at least one top-level roaming server 100% available at all times.

A number of business development questions were received and answered, mostly related to the use of CAT and other supporting services (monitoring, eduroam DB, F-ticks). An increase in interest in eduroam and supporting services outside Europe was noted. Regular monthly conference calls with the eduroam Steering Group were organised and chaired.

Additional activities that were carried out in the reporting period include:

- Work on defining eduroam database version v 2.0, taking into account the input and discussion from the NROs through eduroam SG meetings and the eduroam mailing list. The new version of the database was presented to and endorsed by the GeGC in June 2016. The eduroam OT team started work on implementing eduroam database version 2.0 in production, which is expected to be completed in the first part of 2017.
- The eduroam Configuration Assistant Tool, CAT v. 1.1.3., was released in production in September 2016, accomplishing the goal that was set before the start of the winter semester. The most significant change is the addition of GÉANT Link software, which (re-)introduces support for users whose institutions are using EAP-TTLS-PAP, as it serves as the eduroam installer for Windows client machines running on earlier versions than Windows 8. In November 2016, a feature was added to eduroam CAT to measure the number of downloads per platform per profile.
- In order to provide a background for requests related to user privacy, it was agreed to proceed to the definition of a eduroam privacy policy, starting at the European level and covering the part of the service operated by the eduroam OT in GÉANT. This policy is planned to be published in June 2017.
- In liaison with JRA3, the team contributed to the eduroam Cost Benefit Analysis (CBA) including the special case of the eduroam managed IdP service.

2.2 eduGAIN

eduGAIN is one of GÉANT's key Trust and Identity services, allowing trusted digital identities to be used to simply and securely access available web content and services.

During the reporting period, the eduGAIN infrastructure and service were maintained on a regular basis by implementing updates, applying patches, providing support to federation operators, etc. Operational KPIs were met and exceeded. Various updates to the metadata aggregator and validator were implemented to support the metadata aggregation policy and new features being introduced by the development activity (JRA3). eduGAIN supporting tools were enhanced by integrating new tools developed by JRA3 in the technical web site and making API documentation available. A single issue occurred with a participating federation, which was resolved within one hour with the federation's metadata being removed from eduGAIN.

2.2.1 Service Description

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 offer a greater range of services to their users, delivered by multiple federations in a truly collaborative environment.
- Service providers 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.

The eduGAIN interfederation service delivers a platform for the trustworthy exchange of metadata through the coordination of technical infrastructure and policy. The platform supports the needs of federations in establishing a common baseline for metadata interoperability and furthers the goals of federations to operate in a global identity access and service exchange.

2.2.2 Technical Description

In the same way as for eduroam's description in the previous section, the technical description of eduGAIN is structured into core and supporting services.

2.2.2.1 *Core Services*

The eduGAIN interfederation service consists of two main elements:

1. eduGAIN Policy Framework.
2. Metadata Distribution Service (MDS).

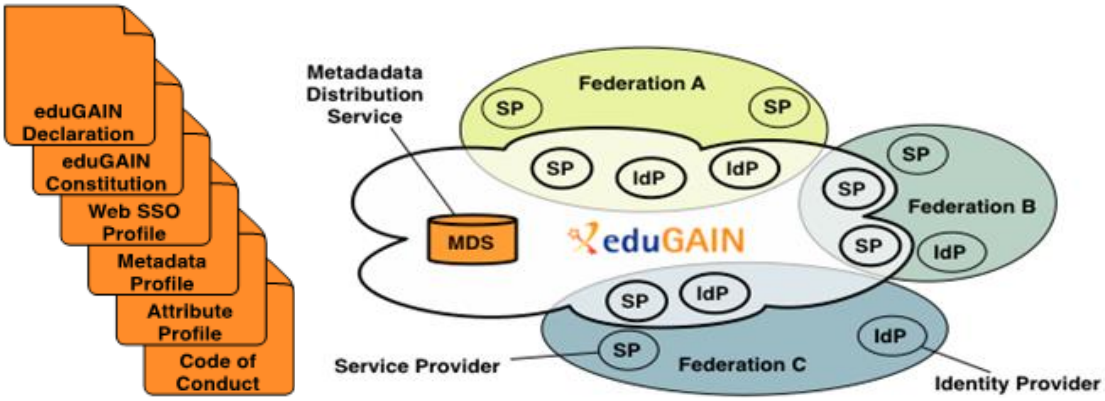

Figure 2.5: eduGAIN Policy Framework and Metadata Distribution Service

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.

During the reporting period, SA2 cooperated with the JRA3 development activity and the eduGAIN community to explore pathways for the future expansion of eduGAIN by supporting new trust and identity technologies. This work led to the preparation of an updated eduGAIN policy, which is currently undergoing approval.

The Metadata Distribution Service (MDS) is the instantiation of the Metadata Profile offering the aggregation of compliant metadata between participant federations. The eduGAIN interfederation service is deployed using the MDS SAML Aggregator Tool. The aggregation tool ensures that the information supplied by each federation meets the technical requirements of the interfederation service.

2.2.2.2 *Supporting Services*

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. In particular, there are two main user groups with the most suitable level of access to targeted information:

- Federation-level personnel – Identity federation staff running service operations within a federation.
  - Institution-level personnel – staff running services at institutional or service provider level (typically operating eduGAIN IdP and/or SP functions).

Supporting services are available through the eduGAIN technical website [eduGAIN_tech]; some of the available functions are:

- Collection and representation of information about participation in eduGAIN.
- Access to eduGAIN formal and technical documentation.
- WEB database interface and API service for status monitoring.
- Interface for viewing historical data on eduGAIN participation.
- Support tools for federation technical personnel.

The products and resources used to deliver eduGAIN supporting services are:

- **eduGAIN validator** – eduGAIN metadata 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 are supplying.
- **eduGAIN entities database** – The eduGAIN database search and reporting interface.
- **eduGAIN entities database API access** – API providing selective information from the database. The API is extended on user requests.
- **Technical monitoring documentation** – Technical documentation about eduGAIN and how to use the services to monitor one's own federation.
- **Policy documents** – eduGAIN formal documentation.
- **eduGAIN WiKi** – supporting information service.
- **ECCS** – eduGAIN Connectivity Check Service - monitoring service for IdPs listed in eduGAIN which tests their actual readiness for eduGAIN - i.e. whether they consume eduGAIN metadata.
- **isFEDERATED check** – A global tool that searches known federations to report whether an institution is already part of them and is also in eduGAIN.
- **CoCo monitor** – GÉANT Code of Conduct monitoring service testing for adherence to CoCo specification.

More information can be found on the eduGAIN technical website [eduGAIN_tech], on the eduGAIN Wiki [eduGAIN_Wiki], and on the eduGAIN Monitor site [eduGAIN_Monitor] for CoCo.

2.2.3 Operations and Support Team

The eduGAIN Operations Team (OT) is responsible for running all core and most supporting eduGAIN services and for handling the required configuration and basic development of its tools using DevOps. The OT also serves as a point of contact for L1 and L2 support, escalating queries to higher support levels or to the appropriate groups. Certain queries not covered by current regulations are passed on to the eduGAIN Steering group for discussion; technical queries related to tools or processes developed by JRA3 may also be passed on to this activity.

The eduGAIN OT is composed of technical personnel mainly from PSNC and a smaller number from GÉANT, including the chair of the eduGAIN Steering Group. PSNC also provides the technical infrastructure necessary for running core and supporting services and a Service Manager who is responsible for managing operations and support for all services, with the exception of the CoCo monitor supporting service, which is managed by CARNet.

The contact details for eduGAIN for users and all interested parties are:

- For general information about eduGAIN and joining procedures: edugain@geant.net.
- For technical questions: edugain-ot@lists.geant.org.

2.2.4 Users, Uptake and Usage

Users of the eduGAIN service are listed on the status page of the eduGAIN technical web site [eduGAIN tech]. As at the end of the reporting period, eduGAIN had 41 active members and 7 voting only members. Of those, 32 GÉANT partners' identity federations are active members of eduGAIN; these are listed in the table below:

Country	Identity Federation
AFIRE	Armenia
Australia	AAF
Austria	ACOnet Identity Federation
Belarus	FEBAS
Belgium	Belnet Federation
Croatia	AAI@EduHr
Czech Republic	eduID.cz
Denmark	WAYF
Estonia	TAAT
Finland	HAKA
France	Fédération Éducation–Recherche
Georgia	GRENA Identity Federation

Country	Identity Federation
Germany	DFN AAI
Greece	GRNET
Hungary	eduId.hu
Ireland	eduGATE
Israel	IUCC Identity Federation
Italy	IDEM
Latvia	LAIFE
Lithuania	LITNET FEDI
Luxembourg	eduID Luxembourg
Moldova	LEAF
Macedonia	AAIEduMk
Norway	FEIDE
Poland	PIONIER.Id
Portugal	RCTSaai
Slovenia	ArnesAAI Slovenska izobraževalno raziskovalna federacija
Spain	SIR
Sweden	SWAMID
Switzerland	SWITCHaai
The Netherlands	SURFconext
Ukraine	PEANO
United Kingdom	UK federation

Table 2.2: eduGAIN member GÉANT partners' identity federations

During the reporting period, five new federations joined eduGAIN, including AAIEduMk (Macedonia), Grid Identity Pool (Italy), INFED (India), KAFE (Korea) and SAFIRE (South Africa), three of which – AAIEduMk, KAFE and SAFIRE – as active participants.

By the end of the reporting period, eduGAIN was providing metadata for 3824 entities. This shows a growth of 45% compared to the same period last year. The biggest growth was recorded for Identity Providers (50%), which equalled the increase in opt-out approaches adopted by federations such as InCommon and the increased outreach on the part of federations on the relevance of eduGAIN to their members. The growth of SPs was still very notable (38%). Figure 2.6 shows the growth trends by number of entities in eduGAIN by year.

It should be noted that a similar growth in numbers of entities cannot be expected in the future, as all major research federations, and therefore most existing services and identity providers, are already a part of eduGAIN. Future growth from now on will then mostly reflect the rate of general uptake of federated technology, which will probably occur at a steadier pace.

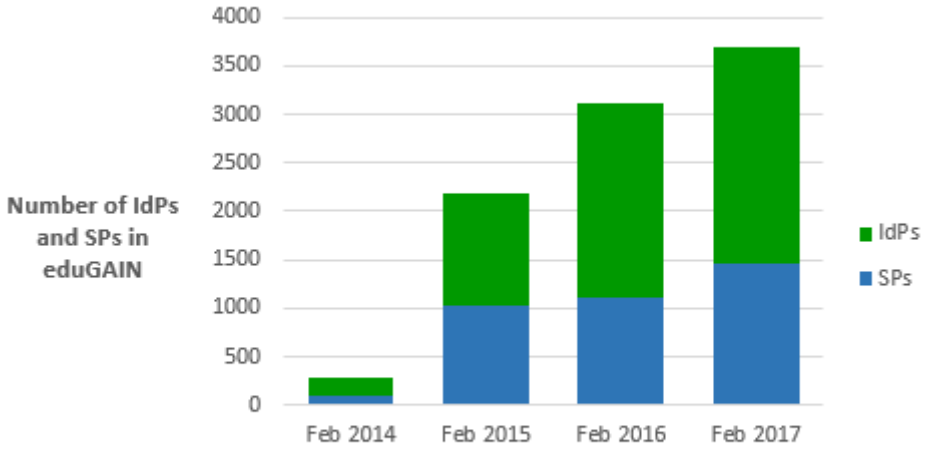

Figure 2.6: eduGAIN uptake statistics: growth in number of entities

2.2.5 Key Performance Indicators

KPIs for eduGAIN measure the availability of the eduGAIN core service (Metadata Distribution Service). Table 2.3 shows that the services are running with minimum disruption and performing better than the set targets.

KPI	Baseline	Target	Measured
MDS availability	99%	99%	99,89*

(*) four outages were reported, one was an announced move of the main MDS host and the three others resulted from local networking problems.

Table 2.3: eduGAIN KPIs – over the period 01 May 2016–28 February2017

2.2.6 Activities and Issues

During the reporting period, DevOps and the support team dealt with standard day-to-day routine activities related to the service. eduGAIN core services were operated to a very high standard.

Additional activities that were carried out in the reporting period include:

- The eduGAIN team participated in the discussion regarding changes to the eduGAIN constitution, in which it represented the point of view of eduGAIN operations.

- The extraction of historical metadata from backups was completed and the results were passed on to JRA3 for analysis. Historical metadata were processed and loaded into the database. The new database holds statistics starting from 27 August 2011. Detailed statistics for 114 days were collected in the period from that date to 31 December 2014, and have been collected daily since 2015. API calls to produce historical data have been prepared and also put in production.
- Various updates to the metadata aggregator and validator were implemented, including:
  - Changes to support the metadata aggregation policy such as a new rule addressing the issue of duplicate entity categories, empty attribute checks, geolocation metadata syntax checks and compressed metadata collection;
  - Update of database for supporting services to fix issues that affected the ECCS service;
  - Addition of Code of Conduct formal checks to the validator;
  - Addition of support for REFEDS SIRTFI (Security Incident Response Trust Framework for Federated Identity);
  - Further code polishing of metadata aggregator.
- Access API documentation was written and made available to the eduGAIN community. A code repository was set up and filled with the core services' code.
- The eduGAIN Wiki was moved to a new server, improving its speed and stability.
- The isFederated service has been integrated with the eduGAIN technical website; during the transition, initial graphics updates were made to make the look consistent.
- A test facility for the eduGAIN infrastructure was set up, to be used as a test environment by the DevOps team.

The Operations Team also managed a number of issues unrelated to the core services themselves, but which nevertheless impacted the service, such as federation metadata feeds nearing their expiry dates or the need for a signing key rollover. One of these issues can be ranked as serious and resulted in all entities from the Swedish Federation SWAMID being removed from eduGAIN. The issue was responded to within one hour; the metadata was restored and, at the same time, a diagnosis of the situation was performed in cooperation with the Swedish federation, leading to the discovery that the error had been caused by the load balancer on the SWAMID side.

In November 2016, a security incident was reported by ORCID [ORCID]. This did not relate to the eduGAIN interfederation service, but was caused by misconfiguration of several IdPs available through eduGAIN. A summary of the events relating to the incident along with a high-level debriefing are detailed on the GÉANT Community Blog [eduGAIN_Security_article]. Although the current support provided by the eduGAIN team already targets identity federations, work is underway to provide enhanced support to handle incidents such as these. This is being piloted by JRA3 who also coordinated the management of the specific incident in question. In this area, eduGAIN will continue to depend on the cooperation of its member federations and the administrators of the entities within these federations, as these have access to the most detailed information and systems.

2.3 eduPKI

eduPKI supports GÉANT services in defining their requirements for digital certificates. It helps coordinate the provision of certificates at a pan-European level as well as enables existing Certification Authorities (CAs) to issue certificates for GÉANT services that require them.

During the reporting period, the eduPKI infrastructure and service were maintained on a regular basis by implementing updates, applying patches, issuing new certificates, etc. No issues were reported, and the operational KPIs were met and exceeded. The operations team also provided extensive support to other services, especially to the eduroam Managed IdP and letsRADsec, through consultations and discussions with development teams in JRA3 T4's eduroam subtask.

2.3.1 Service Description

The eduPKI service provides other GÉANT services with support in defining their security requirements and issuing the digital certificates they require. eduPKI CA is a Certification Authority that issues X.509 digital certificates for GÉANT Services who are not able to obtain suitable certificates from a CA local to them. The certificates are issued in accordance with the Trust Profiles defined by the eduPKI Policy Management Authority (PMA) to meet the demands of GÉANT Services. Two GÉANT services have eduPKI trust profiles – eduroam and the family of the GÉANT Multi-Domain Network services.

2.3.2 Technical Description

eduPKI offers four main facilities:

- The Policy Management Authority (PMA), which defines procedures to determine the requirements of GÉANT services and categorises them into profiles and processes to assess existing national CA operations against the agreed profiles.
- A dedicated Certification Authority (eduPKI CA), which is operated for test purposes and to support those NREN users that cannot rely on a national CA service.
- The TACAR (Trusted Academic Certificate Authority Repository), which stores and distributes the root certificates of Certificate Authorities participating in eduPKI (including the eduPKI CA root) in a secure manner.
- A website (www.edupki.org), which hosts all documentation related to eduPKI PMA work, including Trust Profiles and the eduPKI CA Certificate Policy (CP) and Certification Practice Statement (CPS), and provides links to the eduPKI CA and TACAR websites. The website also provides a single point of contact email address for participating CAs and GÉANT services. The TACAR and eduPKI CA websites also provide an email address for requests that are specific to those services.

2.3.3 Operations and Support Team

Two NRENs participate in the operation and support of the eduPKI service: DFN and CESNET. While DFN manages the infrastructure and the service offering, the role of CESNET is to participate in the eduPKI PMA process.

The contact details for eduPKI for users and all interested parties are:

- Official website: www.edupki.org
- E-mail: contact@edupki.org

2.3.4 Users, Uptake and Usage

eduPKI's users are the GÉANT services and tools that require valid and up-to-date certificates. As at the end of the reporting period, those services included eduroam and the GÉANT Multi-Domain Network services.

As regards the eduroam eduPKI trust profile, the following NRENs have one or more certificates issued for their constituency (either for the NREN federation operator or for individual institutions within the NREN): ACOnet, Belnet, SWITCH, CESNET, DFN, NORDUNET (DeIC), redIRIS, NORDUnet (FUNET), RENATER, CARNet, NIIF/HUNGARNET, HEANET, RESTENA, NORDUnet, SURFnet, NORDUnet (UNINETT), PIONIER, FCCN, NORDUnet (SUNET), SANET, and Jisc/Janet. At the end of the reporting period, 19 new certificates had been issued, bringing the number of valid certificates issued for the eduroam eduPKI trust profile overall to 91.

The main user of the GÉANT Multi-Domain Network eduPKI trust profile is GÉANT, followed by the NRENs GRNET, RENATER, DFN, Janet, PIONIER and HEAnet. There are currently 19 valid certificates issued for these users.

2.3.5 Key Performance Indicators

The eduPKI service's KPIs measure the availability of the Certification Authority (CA) and Certificate Status Check services. The availability of the Certificate Status Check is shown by measuring the availability of the current Certificate Revocation List (CRL) and responses via Online Certificate Status Protocol (OCSP) through their dedicated web services. Table 2.4 shows that the services are running with minimum disruption and performing better than set targets.

KPI	Baseline	Target	Measured
Availability of Certificate Status Check	99.9%	99.9%	100%
Availability of CA Service	99.7%	99.9%	99,99%*

(*) planned downtimes for the CA service which cumulated to 20 minutes

Table 2.4: eduPKI KPIs – over the period 01 May 2016–28 February 2017

2.3.6 Activities and Issues

During the reporting period, the DevOps and support team dealt with standard day-to-day activities related to the service. Additional activities carried out in the reporting period include:

- Extensive support provided especially for the eduroam Managed IdP and letsRADsec, through consultations and discussions with JRA3 T4's eduroam subtask.
- Operation of eduPKI CA and issuance of certificates for eduroam RADsec infrastructure servers.
- Setup of an RA in the eduPKI Test CA for LetsRadSec pilot integration with the eduPKI Test CA API.
- Routine maintenance on the eduPKI CA systems, including system and software updates on the OCSP-Responder servers and preparation work for centralised configuration management for the set of redundant OCSP-Responder servers. One of the redundant CA servers was moved to a secure co-location. The operating system on the RA cluster was upgraded.

No issues were reported related to service operations.

2.4 FaaS

GÉANT Federation as a Service (FaaS) provides an easy entry point for NRENs joining eduGAIN who are developing or are in the early stage of operating a WebSSO Identity federation. FaaS is offered to Federation Operators (typically NRENs), to facilitate them in the uptake and day-to-day operation of their identify federation. By taking advantage of the FaaS offer, Federation Operators can:

- Operate their Identity federation in a scalable manner according to best current practices.
- Exchange metadata with the eduGAIN metadata service in an automated manner.

During the reporting period, FaaS user instances were maintained on a regular basis by implementing updates, applying patches, supporting users, etc. No issues were reported, and the operational KPIs for the service were met and exceeded. The service's reliability was improved by implementing secondary (back-up) HSM used for signing the federation metadata.

2.4.1 Service description

FaaS delivers a service that supports NRENs by providing them with the infrastructure needed to operate an identity federation (web based Single Sign-on) with access to eduGAIN included.

The FaaS offering can be accessed via a server name chosen by the NREN, and the Web UI localised as desired (language, logo, etc.) to maintain the same look and feel of services provided by the NREN Federation Operator for NREN members.

2.4.2 Technical description

FaaS provides a toolbox to enable the management of Identity federation metadata and its exchange with other federations through the eduGAIN service. The toolbox is built using open source software and is provided as a hosted single-tenant service, where each FaaS customer have their own instance that can be localised and branded as desired.

FaaS comprises a front end and a back end. The front end is a web UI where Federation Operators and administrators of IdPs and SPs can register SAML entities in the federation registry application. The web UI enables registration of SAML entities by simply pasting the entity's metadata in a text box. The application then presents raw SAML metadata as a rich UI with the option of adding a variety of supplementary data (such as metadata user interface elements, entity categories etc.). The Federation Operator oversees and approves the registration. Once an IdP/SP is registered, it can become a member of its local federation and/or eduGAIN.

The back end is a metadata aggregator, which consumes metadata of local federation entities (registered in the front-end web UI) and eduGAIN metadata, and produces two metadata streams:

- Federation upstream for publishing to eduGAIN.
- Federation downstream for publishing to Federation members.

The metadata aggregator performs signing of the metadata in each of the streams using an HSM (Hardware Security Module), a cutting-edge technology used for secure signing. The key used for signing is securely stored in hardware.

There are two HSM partitions for all FaaS instances. Each partition is hosted on a different HSM appliance at different locations in Stockholm, Sweden. On each FaaS instance an HA (High Availability) group is defined and the metadata aggregator is set to address its requests to the HA group instead of to any partitions directly. This approach provides the following benefits:

- High availability – if one HSM appliance fails, the remaining appliance continues to provide the service.
- Load balancing – the load spans over all HSM partitions in the HA group.

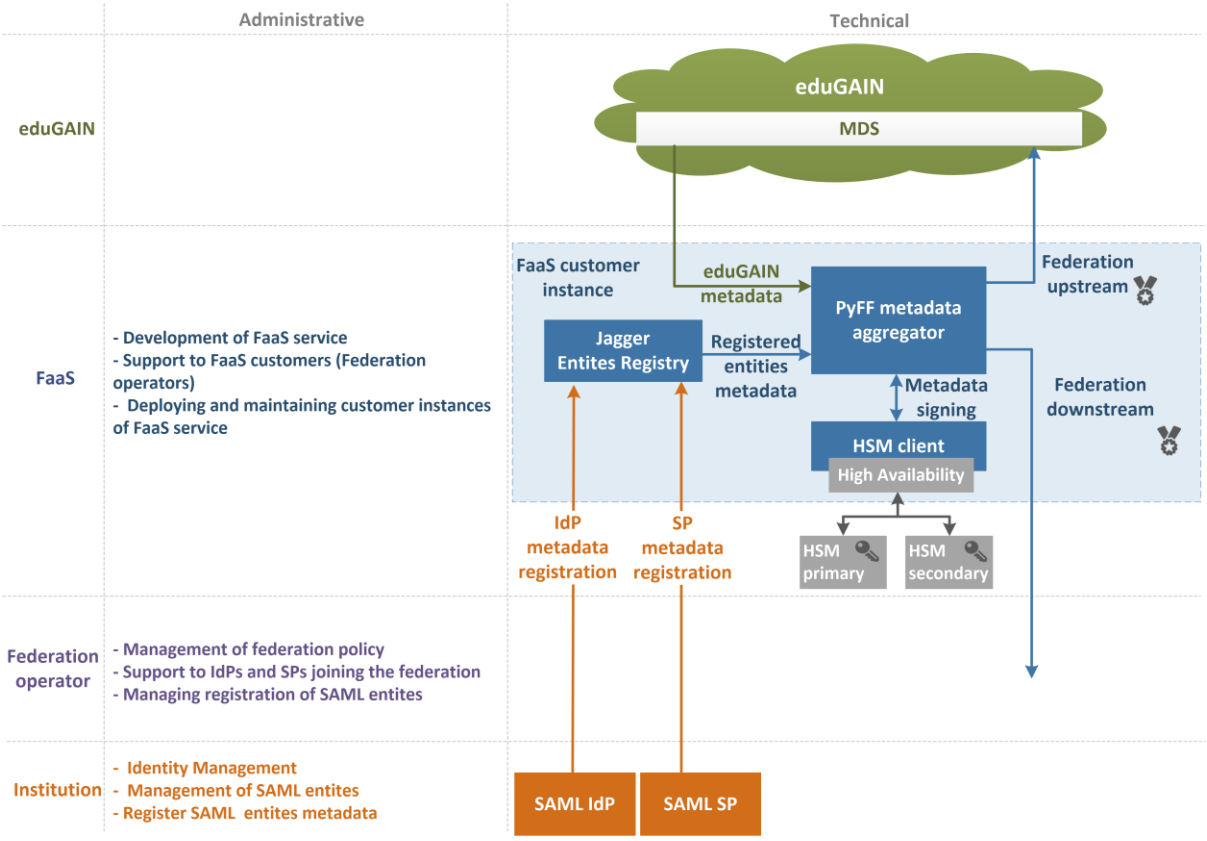

Figure 2.7: FaaS architecture

2.4.3 Operations and Support Team

The FaaS operations team is responsible for service management and operations, and for providing L1 and L2 user support. Three NRENs participate in the FaaS operations team: PSNC, AMRES and NORDUnet. PSNC hosts and manages the virtual machines on which the FaaS instances run, NORDUnet provides the primary and secondary HSM, and AMRES provides a Service Manager who manages and supervises service operations.

The contact details for FaaS for users and all interested parties are:

- Website: http://www.geant.org/Services/Trust_identity_and_security/Pages/FaaS.aspx
- e-mail address: faas@lists.geant.org

2.4.4 Users, Uptake and Usage

FaaS users are GÉANT Partners who have not yet deployed or are in the early stages of operating a SAML2-based Federation. With FaaS these users benefit from a hosted set of tools (SaaS - Software as a Service) that help significantly decrease the effort required in creating and maintaining a secure Identity Federation.

At the time of writing, five NRENs are using FaaS: LITNET, MREN, GRENA, ASNET and MARnet.

Considering that FaaS offers tools for identity federation management, the number of entities registered through a FaaS instance could be used as an indicator of service usage. As this number depends on the level of federation progress and growth and is also an indicator of federation maturity, it may also be of interest in terms of assessing internal federation developments. As at the end of the reporting period, there were 41 entities registered overall in all FaaS user instances.

2.4.5 Key Performance Indicators

KPIs for FaaS measure the availability of FaaS user instances. This availability is calculated based on the mean value of the availability of the Apache SSL service of all FaaS user instances. Table 2.5 shows that FaaS user instances are available with minimum disruption and performing better than set targets.

Name of the KPI	Target	Baseline	Measured
Availability of FaaS user instances	99 %	99%	99,75%

Table 2.5: FaaS KPIs – over the period 01 May 2016–28 February 2017

2.4.6 Activities and Issues

During the reporting period, the operations and support team dealt with standard day-to-day routine activities related to the service.

Additional activities that were carried out during the reporting period include:

- Setup of a new FaaS service instance for the MARNet identity federation.
- Regular system and software updates on all FaaS instances.
- Finalisation of change of DNS names from geant.net to geant.org.
- Several certificates used on web servers on production instances expired during September 2016, and as FaaS instances are hosted on users' domains and it is their responsibility to provide the valid certificates, the FaaS team resolved this issue in coordination with the users. In order to help users react in timely fashion to this issue in the future, the team added a function to monitor certificate time validity that is used to notify users when their certificates are about to expire.
- Implementation of secondary HSM to ensure high availability for metadata signing.

No issues were reported related to service operations for FaaS.

2.5 perfSONAR

perfSONAR is an open-source, modular and flexible architecture for active network performance monitoring that provides a view of network performance across multiple domains, allowing NOC and PERT engineers to seamlessly analyse and diagnose network behaviours across the entire end-to-end path.

The tools provided in the perfSONAR suite perform active measurements of throughput, packet loss, delays and jitter, and record network route and path changes. Measurement Points (MP) installed independently on selected network paths and coordinated within a single organisation or between multiple partners, can be used together thanks to a lookup service listing all publicly available MPs. MPs can be made visible outside of their own domain and their measurements and status made available for stakeholders from external domains, thus creating a multi-domain monitoring environment. The perfSONAR suite contains all necessary gears for setting up a successful performance-monitoring dashboard.

SA4 Task 2 team offers two types of perfSONAR-related services:

- perfSONAR software, developed, maintained and supported by the international perfSONAR collaboration, and which involves the participation of the perfSONAR SA2 T3 team.
- perfSONAR consultancy and expertise, where advice, training and support are provided in designing and deploying a perfSONAR-based measurement architecture, primarily for the GÉANT community.

2.5.1 perfSONAR International Project

Through participation in a global team, perfSONAR team members in SA2 Task 3 contribute to the development and maintenance of the perfSONAR solution and provide support to its users worldwide.

2.5.1.1 *Service Description*

perfSONAR is an open source project supported by five international partners: ESnet, Internet2, Indiana University, University of Michigan and GÉANT. The global perfSONAR team develops, maintains, distributes and provides support for the full perfSONAR tools suite that is installed and used on several R&E networks around the world to perform active measurements and monitor network performance.

These tools enable network and performance engineers of one or multiple domains in a federated environment to scope and focus on a specific problem recognised by the network-monitoring tool on a specific path, thus enabling faster problem resolution.

The GN4-2 project team also participates in the global team by providing user support following the perfSONAR international collaboration agreement through the perfsonar-user mailing list, the documentation on the official perfSONAR website perfsonar.net and the perfSONAR software distribution through a European repository, both for Debian and RHEL packages.

2.5.1.2 *Technical Description*

perfSONAR software enables active measurements to be carried out in the network on selected links within one or multiple domains. Individual tools, orchestrated by the perfSONAR scheduler, perform measurements of one-way delay, round-trip time, jitter, packet loss and throughput on network paths. Measurement data is then stored in a database (a Measurement Archive, MA) and measurement retrieval for detailed visualisation is carried out on demand via a web interface, or presented on a dashboard. Additional tools enable users to look up and search for installed MPs and MAs worldwide.

The perfSONAR software suite provides a complete set of measurement and visualisation tools. To fit user demand and based on appropriate usage scenarios it is offered in the following bundles:

- The perfSONAR tools only include the command line clients to run on-demand measurements.
- The perfSONAR testpoint provides all that is necessary to run an MP and make it available to other R&E network engineers.
- The perfSONAR toolkit provides the testpoint, an MA and a web interface for configuration, measurement setup and local measurements visualisation.
- perfSONAR central management provides administrative tools to maintain a collection of MPs and a mesh of measurements, to collect the data centrally and to present it on a dashboard to easily and seamlessly monitor and visualise measurements for all the MPs.

The perfSONAR suite is provided with all needed supporting documentation including:

- General usage documentation and detailed installation instructions are provided through the perfsonar.net website, which is maintained collaboratively by all global team partners.
- Developer documentation, source code and issue tracking is provided through a github.com dedicated project account shared between all partners.
- User support for installation, measurement setup and usage in general is provided through a dedicated public mailing list.

perfSONAR software is packaged, distributed and supported for different versions of the CentOS and Debian linux distributions. The packages are available for public download from a main repository and multiple mirrors worldwide.

2.5.1.3 *Development and Support team*

The GÉANT project partners that are providing resources for the development, maintenance and support of perfSONAR are AMRES, CARNet, DFN-FAU and PSNC. PSNC also provides a perfSONAR Service Manager, who is responsible for managing and supervising development, operations and support.

Contact details for the perfSONAR project are:

- Main website: http://www.personar.net
- Installation and usage documentation: http://docs.perfsonar.net
- User mailing list as the entry point for any support request: perfsonar-user@internet2.edu or https://lists.internet2.edu/sympa/info/perfsonar-user
- Developers' resources are available at: http://github.com/perfsonar/

2.5.1.4 *Users, Uptake and Usage*

Active network measurements are useful to network engineers, PERT engineers, system administrators, researchers and students. The more perfSONAR MPs are available along a network path, the more possibilities for active measurements exist, rendering the perfSONAR ecosystem even more useful to all its users.

perfSONAR users include:

- Organisations (e.g. Universities, GÉANT NRENs and GÉANT itself) that want to provide active network measurement possibilities to their users or to any collaborating organisations' users (enabling multi-domain measurement possibilities).
- Organisations that want to perform active measurements within their own domain or any other perfSONAR-enabled domain.
- Individual users who want to monitor end-to-end performance or performance on particular links of interest.
- Network researchers interested in developing or monitoring and assessing the performance of new high-speed networks, technologies and protocols.

perfSONAR users are located worldwide and form the global perfSONAR community. The current usage map is available on the perfSONAR website [perfSONAR_usage]. The publicly available perfSONAR installations in Europe, totalling over 400 MPs, are shown in Figure 2.8.

Figure 2.8: perfSONAR installations in Europe

2.5.1.5 *Key Performance Indicators*

The key performance indicator for perfSONAR measures the number of perfSONAR major releases per year.

Name of the KPI	Target	Baseline	Measured
Number of perfSONAR major releases per year	1	1	0

Table 2.6: perfSONAR KPIs – over the period 01 May 2016–28 February 2017

The major perfSONAR 4.0 release was originally planned for autumn 2016. However, owing to the many changes that are being introduced in new release, it was rescheduled for spring 2017.

2.5.1.6 *Activities and Issues*

During the reporting period, the work of the perfSONAR global team focused on the new major release, perfSONAR version 4.0. New features will include: the new scheduling and orchestration software – pScheduler (that will replace BWCTL); a more informative GUI with improved presentation; OS support upgrade to include Debian 7 and 8; Ubuntu 14 and CentOS 7 while still supporting CentOS 6; a new mesh configuration GUI; and MaDDash improvements and alerting. The roadmap for the project can be found on the perfSONAR website [perfSONAR_roadmap] and a presentation on the new release will be given at the Service and Technology Forum in March 2017.

The GÉANT team contributed to building, testing, and fixing all the Debian/Ubuntu packages, helping with the portage to CentOS7, testing and debugging of perfSONAR 4.0 release candidates, major review of the installation and configuration documentation, etc.

Since it will introduce several changes, the final release is scheduled for spring 2017 to give enough time for thorough testing and preparation to enable the requisite high quality standards to be met.

There were no issues recorded in the reporting period, and the support provided via the mailing list was mostly related to first installations by new users and feedback about the installation and usage of the new perfSONAR 4.0 release candidates.

2.5.2 perfSONAR Consultancy and Expertise

perfSONAR Consultancy and Expertise aims to disseminate perfSONAR usage in the GÉANT community.

2.5.2.1 *Service Description*

The Consultancy and Expertise service offers four different activity types:

- Helping to ensure that design measurement architectures and infrastructures based on perfSONAR fit the performance monitoring and measurement needs of the requesting party.
- Providing specific training on perfSONAR deployments, usage and best practices.

- Providing extra support in deploying and operating perfSONAR in GÉANT and the NRENs whenever requested.
- Maintaining and operating a set of perfSONAR services useful to the perfSONAR community in general and the GÉANT area perfSONAR users in particular.

In order to support these activities, a new centrally managed perfSONAR deployment was established in the GÉANT network for the GÉANT community within the perfSONAR Small Nodes project. Preparation for the project started during GN4-1 with the objective of enabling users to gain first-hand experience on running a perfSONAR node for their own organisation, and of introducing perfSONAR on low-cost hardware in Europe and consequently providing a perfSONAR network measurement infrastructure.

The perfSONAR toolkit was installed on about 20 low-cost devices and distributed to GÉANT NREN partners and universities to deploy in their network. The SA2 T3 team operates a central server with a performance dashboard to manage and collect the measurements from these nodes. This serves both as an example of perfSONAR deployment for new users running the nodes and as a showcase of perfSONAR's capabilities for the global perfSONAR community.

2.5.2.2 *Technical Description*

The perfSONAR Consultancy and Expertise service is comprised of the following elements:

- A Jira-based service desk system where users can enter their service requests and from where the perfSONAR team can answer them and provide guidance, advice or help in deploying their perfSONAR systems.
- A GÉANT area public instance of the perfSONAR Simple Lookup Service (SLS), where European perfSONAR deployments will generally register their services (the registration service is automatic and should choose the closest SLS).
- A public psUI instance providing a demonstration and testing of the perfSONAR features and their usefulness in troubleshooting network performance.
- The perfSONAR small nodes measurement infrastructure, created within the perfSONAR Small Nodes project, where users can view the performance dashboard, perform active measurements and use historical data to assess network performance.

The perfSONAR Small Nodes measurement infrastructure, via 20 nodes installed at NRENs and universities, performs regular IPv4 and IPv6 throughput, latency and loss measurements towards five GÉANT Measurement Points (MPs). Measurement data is collected on a central MA hosted in the GÉANT network and is presented via a MaDDash dashboard where measurements are compared with expected thresholds and marked green, amber or red accordingly.

One or more of these elements can be used for any of the aforementioned activity types.

2.5.2.3 *Operations and Support Team*

The GÉANT area NRENs providing resources in this project are AMRES, CARNet, DFN-FAU and PSNC, which also provides a Service Manager who supervises and manages service operations and support.

The contact details for perfSONAR Consultancy and Expertise are:

- Main website: http://www.personar.net
- Demo psUI instance: http://psui.geant.net
- perfSONAR Small Nodes project dashboard: http://perfsonar-smallnodes.geant.org/

2.5.2.4 *Users, Uptake and Usage*

The target users of this service are teams and individuals from the GÉANT community. Since active network measurements and network performance monitoring require specific and advanced knowledge, it is expected that potential users will come from Network Operating Centres (NOCs) and/or the Performance Emergency Response Teams (PERTs) of NRENs, the NRENs' constituencies or cross-domain projects that they might participate in. However, the service's availability is not limited to a specific user group.

The partners involved in the perfSONAR Small Nodes project are: AMRES, ASNET-AM, DFN, EENET, FCCN, GARNET, GÉANT, Janet, Longborough University, NgREN, NORDUnet, PSNC, RIPE NCC, RoEduNet, UCAD/snRER, SRCE/CARNet, University of Erlangen, University of Trieste, Vilnius Gediminas Technical University and Vilnius University.

As a part of the perfSONAR Small Nodes project evaluation, a survey was conducted among the project participants. The project gathered excellent feedback and received an overall average rating of 4.77 (out of 5), with 100% of respondents recommending the continuation of the project and the usage of perfSONAR on small nodes. Of those surveyed, 92% answered that they would be interested to have more GÉANT managed perfSONAR small nodes in their network, 75% that they would install and run some perfSONAR small nodes themselves, 58% that they would install and run a fully-fledged perfSONAR server themselves and 58% 'that they are interested in having their own measurement mesh in their network.

2.5.2.5 *Activities and Issues*

During the reporting period, the SA2 Task 3 perfSONAR team provided the service per request and according to best effort. Support was provided to the GÉANT Network team through cooperation with SA1 for the installation of perfSONAR and perfSONAR UI.

The team gave several presentations and training sessions during the reporting period, as listed in Appendix A, related either to the new perfSONAR release or to the Small Nodes project and measurement platform. The success of the perfSONAR Small Nodes project inspired some NRENs, such as Jisc, NORDUnet and PSNC, to install their own measurements platform.

perfSONAR Small Nodes was planned to run initially for six months and is now entering the evaluation phase that will determine the next steps for the project.

An article about the perfSONAR Small Nodes project was published in issue #24 of the GÉANT CONNECT magazine, and a paper on the project and its results has been accepted for the TNC17 conference that will take place in Linz, Austria on 29 May – 2 June 2017.

There were no issues recorded in the reporting period.

2.6 Brokerage Service Catalogue

The Brokerage Service Catalogue was set up as a result of the efforts of the GN4-1 SA7 team to promote and facilitate the adoption of cloud and application services in the research and education community. The cloud services and providers included in the catalogue were assessed through a questionnaire developed during the GN3plus project.

The home page of the service [GÉANT_cloud_catalogue] describes it as follows: "GÉANT's cloud catalogue is a growing resource for the European research and education community with a structured listing of a number of service providers and cloud services. It provides NRENs and the research and education community with a quick and easy guide to cloud providers' answers to the cloud requirements of the R&E community, and aims to clarify the capabilities of providers, helping in the procurement of cloud services."

2.6.1 Service Description

The Brokerage Service Catalogue enables all interested parties to obtain more information about the services offered to the GÉANT community by either GÉANT/NREN or commercial service providers. In order for service providers to be included in the catalogue and provide services to the GÉANT community they must comply with the indicative cloud requirements prepared by GÉANT.

The existing Brokerage Service Catalogue is due to be replaced by a new Cloud Service Catalogue that currently being designed and developed by JRA4.

2.6.2 Technical Description

The Brokerage Service Catalogue is structured in two main areas, one focusing on participating providers and the other on available services. More information is available for registered users after login, and the catalogue provides different views for each of the three user groups – service providers, users and administrators.

The information available for each cloud provider includes Name, Description, Country, and URL. The following data are available for each service after login:

- Description and list of available services.
- List of 28 indicators that can be used for service comparison and rating including IPR in Respect of Customer Data, Ownership of Data, Data Protection, External Security Audit Certificate, Security of the Cloud Service, Managing Security Incidents, and Data Backup and Restore, among others.
- Contact details for providers.

The lists of providers and services can be searched by name or sorted alphabetically by provider service or country.

2.6.3 Operations and Support Team

GRNET provides the technical infrastructure and service catalogue operations team, which is responsible for the management and operation of the catalogue itself, and for providing support to JRA4. Management and maintenance of the content of the catalogue and the cloud services offered, as well as partner relations and service uptake are the domain of JRA4.

Contact details for the Brokerage Service Catalogue are:

- Website: https://catalogue.clouds.geant.net/#/
- E-mail: brokerage-service-catalogue@lists.geant.org

2.6.4 Users, Uptake and Usage

There are two main group of users of the Brokerage Service Catalogue:

- Users – NRENs and institutions from the GÉANT community.
- Providers – who offer their services to the GÉANT community (including potential future providers interested in doing so).

A special third group includes administrators who maintain the site by uploading relevant information relating to either of the two groups of users above, but have special tasks and therefore additional administrative rights.

As at the end of the reporting period, there were 16 service providers and 28 services listed in the Catalogue.

2.6.5 Key Performance Indicators

The KPI for the Brokerage Service Catalogue measures the availability of the catalogue web server.

Name of the KPI	Target	Baseline	Measured
Cloud catalogue availability	99%	99%	99,9%

Table 2.7: Cloud service catalogue KPIs – over the period 01 May 2016-28 February 2017

2.6.6 Activities and Issues

The role of the operations team is to maintain the Brokerage Service Catalogue until JRA4 develops and deploys the new Cloud Service Catalogue. Therefore, no major activities except day-to-day operations and fulfilling JRA4's requests to export the database and update the web content were carried out in the reporting period. Upon JRA4's request, the operations team will support the transition by exporting the existing database.

No issues were reported related to service operations.

3 Conclusions

The Trust & Identity and Multi-Domain Services Service Activity (SA2) manages the services fully or partially developed within the GN4-2 project. At the time of writing, these include four Trust & Identity services – eduPKI, eduroam, eduGAIN and FaaS – and two Multi-Domain services – perfSONAR and the Brokerage Service Catalogue.

From the service summaries, it can be seen that the individual services differ significantly in nature, target users and scope. eduroam, eduGAIN, eduPKI and FaaS fall under the Trust & Identity service category, while perfSONAR enables multi-domain active monitoring and the Brokerage Service Catalogue provides a repository of information for GÉANT users to learn more about the services offered to the community by cloud providers. Despite these differences, the operation of all these services is provided in a federated manner. Team members come from different NRENs, and different organisations within an NREN and even from different continents, and successfully cooperate in the offering, provisioning and daily operation of the services. The infrastructure for the services is also provided by different organisations within or outside of the GÉANT community.

This report covers the first ten months of operations of those services in the GN4-2 project. Two more such reports will be produced during the course of the project, each covering the subsequent ten-month periods.

The KPIs for all services for the reporting period were met and exceeded. The DevOps paradigm introduced in GN4-1 once again gave excellent results with operations teams maintaining agile and high-quality service operations while at the same time responding efficiently to users and needs imposed by technology. Each of the services recorded a number of DevOps activities that were performed in line with day-to-day operations. Some minor issues were reported but with no impact to the delivery of the services.

The operations teams cooperated closely with development activities, moving new features into production for eduGAIN and eduroam. The service managers and continual service improvement (CSI) managers continue to constantly monitor, assess and evaluate all services to maintain their performance and strive to increase their levels of excellence.

Appendix A

List of presentations and trainings provided to the GÉANT community by the perfSONAR team.

#	Type of Activities[1]	Main Leader	Title	Name of Event	Date/ Period	Place
1	Conference	Trocha Sz.	Building low-cost measurement infrastructure with perfSONAR	NORDUnet Conference 2016	20/09/2016	Helsinki, FI
2	Workshop	Delvaux A.	pSmall Nodes project in GÉANT	SIG-PMV Meeting 2016	03/11/2016	Zurich, CH
3	Workshop	Delvaux A., Garnizov I.	perfSONAR Measurement Mesh Workshop (together with SA3T5)	eduPERT training 2016	04/11/2016	Zurich, CH
4	Conference	Trocha Sz.	Building the Modern Performance Monitoring with perfSONAR	ARNES national conference	24/11/2016	Ljubljana, SI

References

[eduGAIN_Monitor]	http://monitor.edugain.org/coco/
[eduGAIN_Security_article]	https://blog.geant.org/2017/01/23/handling-security-incidents-in-edugain/
[eduGAIN_tech]	https://technical.edugain.org
[eduGAIN_Wiki]	https://wiki.edugain.org/
[eduroam]	www.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
[eduroam_ServDef]	https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf
[eduroam_Monitor]	https://monitor.eduroam.org/
[eduroam_CAT]	https://cat.eduroam.org/
[GÉANT_cloud_catalogue]	https://catalogue.clouds.geant.net
[ORCID]	https://orcid.org
[perfSONAR_roadmap]	https://www.perfsonar.net/project-information/project-roadmap/
[perfSONAR_usage]	https://www.perfsonar.net/about/who-is-uisng/

Glossary

AAA	Authentication, authorisation, and accounting
ARP	Address Resolution Protocol
CAT	Configuration Assistant Tool
CRL	Certificate Revocation Check
CSI	Continual service improvement
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
eduroam OT	eduroam Operations Team
eduroam SG	eduroam Steering Group
EAP	Extensible Authentication Protocol
ETLR	European top-level RADIUS server
FLRS	Federation-level RADIUS proxy server
GeGC	Global eduroam Governance Committee
HI	Home Institution
IdM	Identity Management
IdP	Identity Provider
KPI	Key Performance Indicator
L1	Layer 1
L2	Layer 2
LDAP	Lightweight Directory Access Protocol
MA	Measurement Archive
MAC address	Media access control address
MDS	Metadata Distribution Service
MP	Measurement Point
NAPTR	Name Authority Pointer
NAT	Network address translation
NOC	Network Operating Centre
NREN	National Research and Education Network
NRO	National Roaming Operator
OT	Operations Team
PERT	Performance Enhancement Response Team
RADIUS	Remote Authentication Dial-In User Service
SAML	Security Assertion Markup Language
SLS	Simple Lookup Service
SP	Service Provider
TLS	Transport Layer Security
UDP	User Datagram Protocol
VI	Visited Institution