16-01-2018

Deliverable D3.4 Case Study: Report on Two Cases of User Account Management, PRACE and CLARIN

Deliverable D3.4

Contractual Date:	30-11-2017
Actual Date:	16-01-2018
Grant Agreement No.:	731122
Work Package/Activity:	3/NA3
Task Item:	Task 2
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT
Document ID:	GN4-2-17-23B84F
Authors:	C. Atherton (GÉANT), R. Norman (GÉANT), C. Kanellopoulos (GÉANT), V. Capone (GÉANT), L. Hämmerle (SWITCH)

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 promotes the importance of user account management and collaboration within GN4-2, and provides examples of the ways in which this can improve the impact of research throughout the R&E community. Two use cases are detailed: PRACE, a European e-infrastructure providing supercomputing facilities, and CLARIN, a European e-infrastructure providing resources and technology for language data.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This deliverable provides two examples of user account management in the context of the GÉANT project (GN4-2). CLARIN and PRACE are international user organisations that have diverse partners, functions and services, and as such, have disparate support needs [CLARIN], [PRACE]. In the case of PRACE, a new network topology was required, while CLARIN sought support for users within its Trust and Identity function. In both cases, the GÉANT user account management function followed a pre-defined strategy to gather requirements, design, propose, and then project manage the implementation and operation of the solutions.

Following an introduction, this deliverable consists of three parts:

- The first describes the GÉANT service offerings, which are key to delivering services to users across the research and education community that span multiple countries. The user account management strategy and process is also explored, in order to provide context for the two case studies being presented.

- The second part of the deliverable explores the background of PRACE's wish to develop a new network topology. The reasoning behind why a particular solution was identified, how it was delivered and its benefits to the PRACE organisation have also been detailed.

- The third part of the deliverable investigates the solution delivered to the CLARIN organisation. This includes the pain points within the trust and identity sphere that CLARIN sought to improve for its own users, how the solution was selected and delivered, as well as its future benefits.

1 Introduction

GÉANT, together with its national research and education network (NREN) partners, provides users with highly reliable, unconstrained technologies and services to allow access to computing, analysis, storage, applications and other resources, whenever and wherever they may be. Through the network's connections to similar infrastructures, both in Europe and across all continents, the GÉANT partnership enables collaboration and ensures that Europe remains at the forefront of research.

However, to understand the needs of its users, the GÉANT project (GN4-2) needs to interact with the researchers, scientists and user communities that use the services that GÉANT and NRENs provide. This is achieved through GN4-2's networking activities (NAs). In particular, the NA3 activity exists to provide an interface between GÉANT and the communities that the project serves. It provides account management to ensure NRENs and users get the most from GÉANT services and interfaces with global NRENs to enable international collaboration. The activity also manages the relationship with international user groups and parallel e-infrastructure projects.

The requirements of the users that the GÉANT community serves are diverse, ranging from small community science projects, to multi-national research infrastructures. GÉANT and NRENs fulfil such requirements through trust and identity, security and networking connectivity service offerings. Where delivery of these services by the GÉANT community spans multiple countries, delivery is set in the context of the international user account management function, provided in GN4-2 NA3 T2. Where projects exist within only one country, NRENs exclusively provide services to these user communities.

This deliverable sets out two examples of user account management, which incorporate some of the diverse product offerings that are provided within the GÉANT project. Topics covered include: use of existing services, the ways in which the GÉANT community is helping to improve existing services, and how these changes have improved the way in which European researchers carry out their work. Note that the specific technical or operational details that delve into the technicalities of the work delivered are outside of the scope of this deliverable.

The two selected use cases discussed in this document are based on the interactions and work delivered with PRACE, a European e-infrastructure providing supercomputing facilities, and CLARIN, a European e-infrastructure providing resources and technology for language data.

These use cases cover a subset of the product portfolio offered by the GÉANT community: networking connectivity and trust and identity services. In each case, the following topics will be covered:

- Organisation description
- Opportunity for change

- Solution identification
- Solution delivery
- Benefits of the new system
- Future directions.

This deliverable seeks to explain the role of user account management within Task 2 of GN4-2, Networking Activity 3 (NA3), and provides examples of the ways in which account management can improve the impact of research throughout the R&E community. It also seeks to illustrate collaboration with users through the context of the GÉANT project.

2 GÉANT

GÉANT is the leading collaboration on e-infrastructure and services for research and education, working with National Research and Education Networks to deliver the pan-European GÉANT network and associated e-infrastructure services.

The GÉANT backbone network is the largest and most advanced R&E network in the world. Through interconnections with its national research and education network (NREN) partners, it connects over 50 million users at 10,000 institutions across Europe, supporting all scientific disciplines. The network operates at speeds of up to 500Gbps and reaches over 100 R&E national networks worldwide, allowing European researchers to collaborate on a global scale.

The network and its associated services: trust, identity and security, cloud, real time communications and professional services, are co-funded by the NRENs and the European Commission through the GÉANT project, GN4-2. Within this project, 42 European NRENs collaborate to advance the state of the art in networking and services innovation.

Over 3.9 million Gigabytes of data is transferred via the GÉANT IP backbone every day. More than just an infrastructure for e-science, GÉANT stands as a positive example of European integration and collaboration.

2.1 GÉANT Service Portfolio

The GÉANT community develops the services its members need to support researchers, educators and innovators - at national, European and international levels. Our portfolio of advanced services covers connectivity and network management, trust and identity, and security, real-time communications, storage and clouds and professional services. Two service areas covered in this deliverable are Trust, identity and security, and Connectivity and network management services.

2.1.1 Trust Identity and Security Services

Online services are crucial to research and education. Students, researchers and institute staff rely on them for collaboration through webmail, e-learning, teaching, conferencing, analysing and sharing data, and for accessing journals and libraries. Trusted digital identities underpinned with secure technologies allow them to simply and securely access content and services.

GÉANT services build trust, promote security and support the use of online identities, through a range of activities and international collaborations.

eduGAIN is at the heart of the GÉANT trust and identity service offering. eduGAIN is the GÉANT community and GÉANT project developed inter-federation service that interconnects research and education identity federations around the world. It enables the trustworthy exchange of information between service providers and research and education institutions or other identity providers. This means simpler access to a wider range of online content, services and other resources that benefit collaboration in the research and education community [eduGAIN].

2.1.2 Connectivity and Networking Management Services

The large-scale, high-speed GÉANT backbone network is essential for sharing, accessing and processing the high data volumes generated by research and education communities, and for testing innovative technologies and applications across multiple countries and continents. GÉANT also works in collaboration with GÉANT community members who plan, procure and build their own regional or national research and education networks in order to provide a community-based, end-to-end connection for research and education communities that span multiple countries.

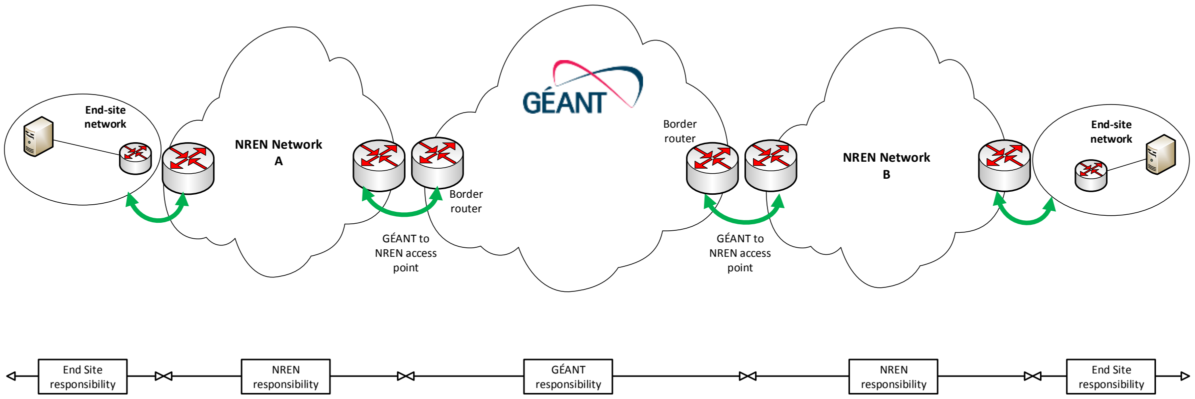

Figure 2.1: GÉANT and NREN service responsibility areas

GÉANT also provides network and collaboration services that facilitate international cooperation between researchers and educators, and bring people together for the human networking that drives innovation. Of note are the GÉANT Point-to-Point Services and the VPN services, which are especially relevant to in the PRACE use case discussed later this document.

The GÉANT point-to-point service is high-performance interconnectivity for the most demanding of network requirements, for when shared IP services cannot provide the capacity or performance needed. The point-to-point service is delivered via GÉANT Plus, an ethernet point-to-point service; GÉANT Lambda, an optical point to point service; Bandwidth on Demand, an automated SDN tool for creating layer 3 circuits across the GÉANT network, and GÉANT Open, an interconnection facility which allows approved R&E and commercial third parties to peer directly with GÉANT and NREN participants.

GÉANT VPN services have been developed for the many research projects requiring the additional security and reassurance of a virtual private network (VPN) to ensure data services are isolated from general IP (internet protocol) traffic. By creating a virtual IP network, all sites on the VPN can flexibly communicate, without the need to arrange separate networks, whilst benefiting from the privacy and security of a private infrastructure. GÉANT and the national research and education network (NREN) organisations have worked together to provide a range of VPN services, such as Layer 3 VPN and Multi-Domain Virtual Private Networks.

2.2 GÉANT Account Management Services

Large and small user groups exist within the R&E community that span multiple countries and jurisdictions. These user groups are highly visible to the public, often drive innovation in the sciences and encourage uptake of NREN services. As such, they are very important to the GÉANT project and the NREN community. In order to adequately cater for the bespoke needs of these unique, multi-national user organisations, GÉANT provides an account management service on behalf of the GÉANT community. This is to ensure that these users are dealt with in a consistent and professional manner.

In order for the NRENs to remain successful, they need to maintain a competitive advantage over commercial network providers within the R&E sector. International user organisations and international research projects are a key aspect of this sector. Within Europe, GÉANT Limited acts as coordinator on behalf of the European NREN community to provide a one-stop-shop and leverage the key strengths of the GÉANT community: high- level technical expertise; high levels of local and pan-European network market experience, access to cutting edge technologies; an understanding of the network, trust & identity and security requirements of the R&E community; European and global partnership reach; and subsidised, pan-European connectivity and services.

As an organisational process, the account management service interaction strategy is focused around three areas:

- Account management
- Technical customer support
- Commercial management

The account management function ensures that user records are kept, enquiries answered and relationships with the international user organisations are maintained. A point-of-contact is provided for project management purposes, taking responsibility for the technical and commercial offerings of the community and the proactive anticipation of the user organisation’s needs. The technical customer support function aims to understand the detailed requirements of the user application and to propose suitable service offerings, as well as developing technical designs for any proposed GÉANT/NREN solution. Commercial management provides a coherent, pan-European response to commercial enquiries, and aims to provide a competitive alternative to commercial offerings. The process for interaction by the account management team follows a set lifecycle that is divided into five sections, as shown in Figure 2.2.

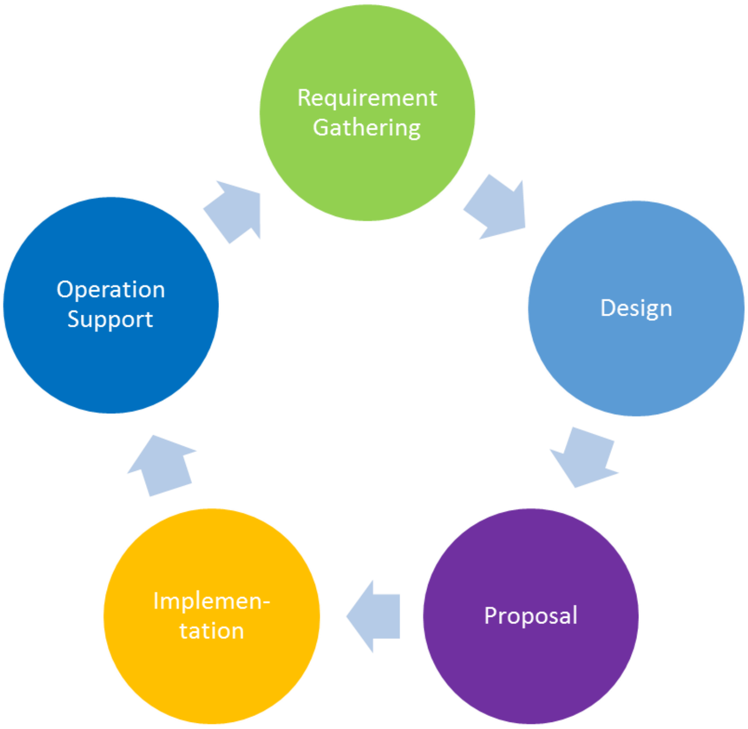

Figure 2.2: User interaction lifecycle

One of the key stages of the GÉANT user interaction lifecycle is requirement gathering. This is where regular interactions are held with the user organisation via the account management function. In this stage, interactions between the users and the account managers define the potential service that is required. Such interactions cease when it is clear an acceptable solution for the user organisation's needs is not required. Clear logging of interactions and requirements is essential during this stage.

Initiation of the requirement gathering process can be started by a lead NREN interacting with GÉANT or from a GÉANT staff member who has been developing the lead via user community event attendance. In either case, a lead NREN is involved with the GÉANT user interaction lifecycle, in a joint interaction with the user organisation. The lead NREN is typically designated according to the nation where the headquarters of the user organisation resides. However, in some circumstances it can be collaboratively decided by the NRENs involved that it is more appropriate to select the NREN from the nation where the primary operation for a particular project is being delivered. This NREN then becomes the GÉANT community designated lead NREN for the user interaction lifecycle.

Leading on from the requirement gathering phase, a solution progresses through a number of logical sequences: the design, service proposal, implementation and then operation and support of the service. For the design phase, a team member from GÉANT or the GÉANT community puts together a technical proposal which meets the criteria gathered during the requirement gathering phase. The design includes an overview of how the solution is to be operated and supported during its lifetime, as well as the technical capabilities of the solution. This is then reviewed by GÉANT departments and the NRENs responsible for the delivery of the solution, to ensure that the proposal is fit for purpose and to give operational visibility of the proposed solution to all concerned parties. It is at this point that an implementation design is put together by those respective departments or organisations.

Editing and approval by all concerned GÉANT departments and involved NRENs takes place via a series of emails. The solution document is communally edited by all before finally being compiled by GÉANT. Once the proposal is finalised, it is formerly proposed to the end user by GÉANT on behalf of the GÉANT community. Once accepted by the end user organisation, the procedure then calls for the Business Development team within GÉANT to "kick-off" the request (for network services or trust, identity and security) to the respective operations team. This "kick-off" ticket within the GÉANT OTRS system then begins the implementation phase, which is tracked via the GÉANT ticketing system and follows the implementation design defined in the earlier phase. Once the solution is implemented, the Business Development team is handed back the ticket in order for the client to be notified of the service going live. The solution then enters into the operation and support phase which involves monitoring and maintenance of the service as defined during the design phase. Following completion of a specific project, regular meetings with the user organisation continue, to ensure that GÉANT and the GÉANT community can cater for the user organisation's current and future needs.

To conclude, the account management function exists to provide a streamlined, professional approach to the support of international user organisations and their bespoke network and associated service requirements.

3 PRACE

3.1 The PRACE Organisation

The mission of PRACE (Partnership for Advanced Computing in Europe) is to enable high-impact scientific discovery, engineering research and development across all disciplines to enhance European competitiveness for the benefit of society. PRACE seeks to realise this mission by offering world-class computing and data management resources and services through a peer review process.

PRACE also seeks to strengthen the European users of HPC in industry through various initiatives. The organisation also has a strong interest in improving energy efficiency of computing systems and reducing their environmental impact.

The organisation was established as an international not-for-profit association with its seat in Brussels. It has 24 member countries whose representative organisations create a pan-European supercomputing infrastructure, providing access to computing and data management resources and services for large-scale scientific and engineering applications at the highest performance level.

The computer systems and their operations, accessible through PRACE, are provided by supercomputing sites throughout the 24 member countries. Out of all of the PRACE consortium members, five (BSC of Spain, CINECA in Italy, CSCS located in Switzerland, GCS of Germany and GENCI situated in France) are the largest, home to some of the most powerful super computers in Europe. Four hosting members (France, Germany, Italy, and Spain) secured funding for the initial PRACE funding period from 2010 to 2015. In 2016, a fifth hosting member, CSCS (Switzerland) opened its system via the PRACE Peer Review Process to researchers from academia and industry. Keeping pace with the needs of the scientific communities and technical developments, systems deployed by PRACE are continuously updated and upgraded to be at the apex of HPC technology.

3.2 Opportunity for Change

PRACE links several high performance computing sites around Europe. Originally, this was a closed community of connections to a DEISA switch in Frankfurt, Germany, hosted by the Jülich Supercomputing Centre. Although 24 NRENs were involved in the delivery of services to the PRACE consortium end sites, the core operation of the PRACE network resided in Germany. As such the German NREN, DFN, was identified by the NRENs involved in the delivery of services to PRACE as the lead NREN for interactions with this user group.

The network design in place at the time of the requirement gathering process was a star topology of optical wavelengths of 10Gbps per second. There was also a separate 1Gbps bridge, which allowed access to the network at a lower speed, via an IPsec gateway. This 1Gbps bridge was for the other members of the PRACE consortium that did not have high networking capacity requirements. This allowed consortium connections to be established to the PRACE topology in a shorter timescale when compared to an optical network connection, with the sole disadvantage of access at a reduced speed.

In order for a new supercomputing site to connect, it would contact its NREN. The NREN would then liaise with the GÉANT business development team in order to establish the optical connection. A similar arrangement existed when non-optical connections needed to be made to the bridge.

The issues that were inherent in this topology were its lack of flexibility, a single point of failure in the central switch and the fact that the switch was soon to come to its end of life.

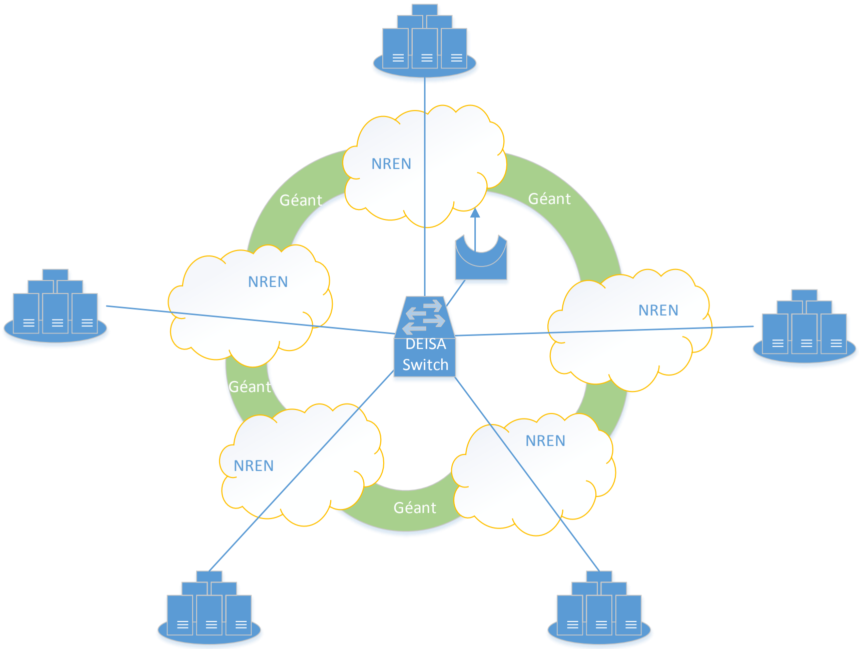

Figure 3.1: High-level overview of PRACE network topology prior to switch to MD-VPN system

In 2014, PRACE wanted to look at evolving its network topology from the star topology it had been operating for some time. The GÉANT business development team had been in regular contact with PRACE as part of the user account management function. The GÉANT community at that time was providing services for the existing network topology. It was during the regular account management interactions that the GÉANT community was approached about a requirement to update the current network topology. Following a requirements gathering process, the GÉANT community proposed a mesh network in order to fulfil PRACE's needs. However, due to costs and the complexities involved in moving over to this new topology, the suggested solution was not taken forward.

Instead, a period of time elapsed before the PRACE technical team looked at the network architecture once more. On this occasion there was a renewed emphasis on quickly replacing the topology due to the vendor ceasing support for the core switch. In 2016, during a regular PRACE service call, the GÉANT Community was approached for support to explore alternative, long-term network topology solutions.

This time emphasis was placed on delivering a solution in a short timescale. Another motivating factor was that the Swiss supercomputing centre at CSCS also intended to join the PRACE network, although this has been delayed due to the cost of establishing an optical point-to-point circuit with the PRACE network.

In summary, two motivating factors, cost and speed of delivery, helped to set the framework within which the GÉANT community had to deliver a solution.

3.3 Identification of a Segregated Network Solution

PRACE partners initially proposed that PRACE investigate the various service offerings from the GÉANT community. During a series of meetings between representatives of PRACE, GÉANT Association and the GÉANT Community designated lead NREN, DFN, a number of features were established as requirements in order to help define the proposed solution. This was to allow an unbiased comparison between service offerings to determine the most appropriate solution for the PRACE future network. Not all of the features were of equal value, but instead allowed an indication of the associated risk/effort needed to deliver the various solutions. The required features were as follows:

- Status monitoring of user connectivity.
- Recording of international PRACE traffic volumes.
- Recording of per site PRACE traffic volumes.
- Recording, reporting and analysis of PRACE traffic flow information.
- Use of perfSONAR for additional monitoring and logging purposes [perfSONAR].
- NREN endorsement.
- Ease of addition of new users.

Upon analysis of the traffic levels across all of the PRACE optical links by GÉANT, it was discovered that bandwidth rarely exceeded 1Gbps for production traffic. On the occasions where it did exceed 1G, testing of the link was the cause. Due to the traffic levels falling within the capabilities of existing NREN connections to the GÉANT backbone, a purely optical solution was not essential. This meant that a more novel and ultimately cost effective approach to delivering this solution was possible.

Two options were put forward for consideration: L3VPN and MD-VPN. Both solutions utilised the existing NREN infrastructure and GÉANT backbone. This negates the need for new optical circuits to be established between the existing supercomputing centres and would also mean that connections could take advantage of the multiple forms of redundancy across the NREN and GÉANT networks. This further strengthened the resiliency of the delivered solution compared to a purely optical point-to-point circuit. By not requiring point to point circuits, costs would also be minimised for existing and new centres that joined the new topology.

However, the choice of MD-VPN was largely a consensus decision among a large group of NRENs.

Due to the need for a speedily rolled out, segregated network solution with strong backing from NRENs, the MD-VPN service developed by the GÉANT community in GN4-1 SA4, was put forward.

3.3.1 MD-VPN

The multi domain virtual private network (MD-VPN) service delivers seamless, private interconnection of two or more networks across multiple network domains [MD-VPN]. This allows the users of the IPv4/IPv6 (or layer 2) networks to work as if their networks were coupled. This service is offered collaboratively by GÉANT and a number of adjacent NREN networks. These joint networks form a multi-domain area where the service is provided. One of the advantages of the service is that it uses well known and standardised protocols and technologies, which are available on many routing and switching platforms. This expands the scope of the service to almost all European NRENs.

The service is designed for situations where users need a dedicated and independent network for transfer of data (IP or native Ethernet traffic) between two or more end points. This is typically the case if the user premises are spread over a large geographical area. The service is always enabled, meaning that once established, no further operations are needed on a daily basis, reducing management and maintenance costs. The service offers high security in the sense that the carried traffic is isolated from other traffic. It should be noted that the traffic is isolated at the logical layer and not necessarily at the physical layer. This means that the core networks will carry data from multiple users, but there will be no ‘crosstalk’ between these traffic streams. From the users’ perspective, each instance of the service is a virtual private network. Hence MD-VPN service is an ‘umbrella’ infrastructure, which enables participating NRENs to provide VPN services for end users.

MD-VPN is an enabling service and only available to NRENs that use MPLS at their borders with the GÉANT backbone network. To join MD-VPN an NREN sets up a ‘carrier of carriers’ VLAN with GÉANT, establish a BGP labelled unicast session with their GÉANT gateway router, and establishes a BGP session with two GÉANT route reflectors (located in Paris and Ljubljana). Once MD-VPN is setup like this, then that NREN can work with any and all other MD-VPN participating NRENs to setup a VPN of their choosing without any further action on the part of GÉANT staff. As of the writing of this document MD-VPN only officially supports L3VPN, although L2VPN may be possible in the future. If an NREN cannot or chooses not to setup MD-VPN with GÉANT, it can still join NREN VPNs by asking GÉANT to run a proxy for them. If they do this, then their participation is, for them, just like connecting to a normal layer 3 VPN. Because the MD-VPN traffic is aggregated through the existing NREN-GÉANT connections, visibility of which end sites are using the MD-VPN service is lost. Instead, it is only known which NRENs request to join the carrier of carriers VLAN and which NRENs request a MD-VPN proxy.

A typical MD-VPN scenario is that of a user group or organisation geographically dispersed into smaller sites within the GÉANT service area. Each geographically separate office needs to be connected with other sites in the same user group. This is illustrated in Figure 3.2, below.

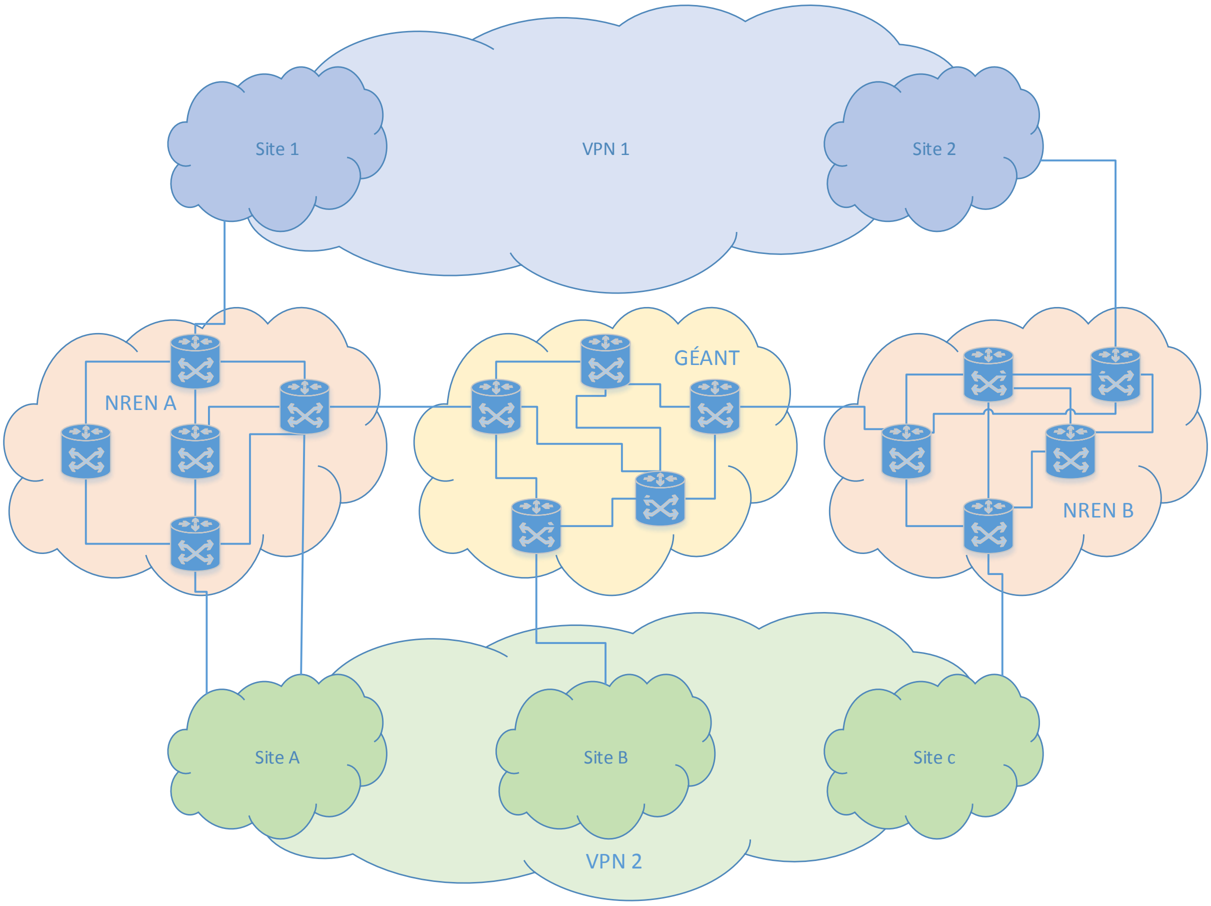

Figure 3.2: MD-VPN Service Overview

The middle row of Figure 3.2, above, illustrates three, independent domains that deliver the MD-VPN service to two different user groups labelled VPN1 (blue) and VPN2 (green). One main advantage of the MD-VPN service is that the user-group clouds can be connected to the GÉANT service area, illustrated by the middle row (yellow and orange clouds) by a number of different technologies, ranging from dedicated private lines to logical lines delivered by local service providers or universities. The network elements within the GÉANT service domain are configured to exchange traffic between the VPNs with the same colour, which make it appear as if they were connected to the same local network. The MD-VPN service may be offered with local redundancy, as indicated for VPN2 in the NREN A domain. Here, two different connections are used to carry the traffic into the provider (NREN) network. The appropriate signalling protocols, will assure redundancy over loop-free network. MD-VPN supports cross-border fibre between two NRENs in order to improve the service reliability. If the site is not directly connected to an NREN, the NREN can use any appropriate technologies to deliver the service, in particular, the same technologies used in MD-VPN.

The MD-VPN service can be very useful when researchers (end users) wish to exchange data between different departments or labs located anywhere in the GÉANT service area, and cooperate on a daily basis. One advantage of MD-VPN is that it does not always require new network resources, because existing routers and links can be used to provide the service.

3.4 Solution Delivery

Prior to the full implementation of MD-VPN across the entire PRACE infrastructure, it was mutually agreed that a pilot project should be delivered first, so as to demonstrate the feasibility of the suggested service. This was in order to de-risk the network transition and prove service capability. The PRACE consortium itself suggested to start with the PRACE sites involved in the Human Brain project, as a suitable test case for the MD-VPN-based solution. This project would link the participating supercomputing sites around Europe located in Spain, France, Germany, Switzerland and Italy.

The Human Brain project is a H2020 Future and Emerging Technologies (FET) flagship project, which strives to accelerate the fields of neuroscience, computing and brain related medicine [HUMAN BRAIN]. This acceleration is achieved by strategic alignment of scientific research programmes in fundamental neuroscience, advancing simulation and multi-scale modelling with the construction of an enabling research infrastructure.

The newly developed MD-VPN system was delivered by a number of NREN partners in the respective countries where the five Human Brain sites and supercomputing centres are located. The NRENs involved were RedIRIS, RENATER, DFN, SWITCH and GARR.

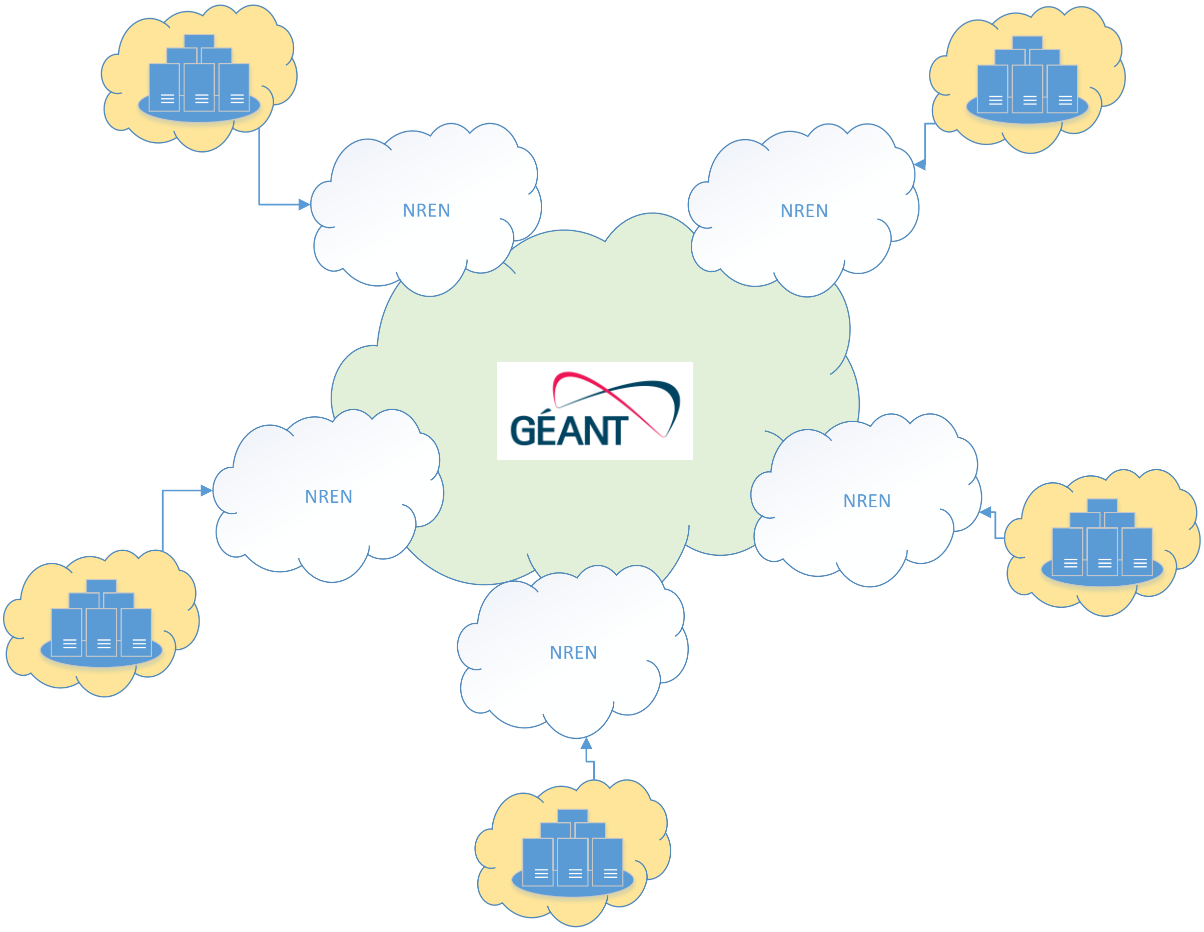

Figure 3.3: PRACE high-level MD-VPN network design

The delivery of the new system involved implementing the MD-VPN configurations between the participating NRENs and GÉANT, allowing for the established end- site connections to the respective NRENs to be utilised. The pilot project was ordered by PRACE in May 2016, and delivered by October, with GÉANT Limited acting as the co-ordinating partner between the user and the NRENs. The pilot project was fully implemented and operational by the end of 2016.

As previously stated, GÉANT, through its account management function, acts as a single point of contact for large, multi-national user groups, in order to provide a co-ordination function between the NRENs and the user organisation. This helps large organisations with establishments in multiple NREN jurisdictions to streamline their interactions and contacts, increases productivity and allows user communities to focus on their own day-to-day operations.

In the case of the PRACE solution delivery, GÉANT acted as the co-ordinating function, providing account management, pricing and technical liaison during the planning and deployment of the solution. It is important to note that the establishment of contracts for the MD-VPN service still remained between the end sites and their respective NRENs, as this was the most productive way for the end sites to interact with the NREN community.

Although the establishment of the MD-VPN solution should have been relatively quick, the interaction and co-ordination between the NRENs on behalf of PRACE took six months to finalise, due to gathering the pricing and contractual arrangements involved in the delivery of the MD-VPN service. However, the resulting working practices mean future deployments of the MD-VPN service for other user organisations can benefit from this work now having already been completed.

Following the successful deployment of the MD-VPN system in December 2016 for the Human Brain Project, PRACE reviewed the suitability of the delivered platform. This milestone was critical in the decision to move the PRACE network over to the new topology. Moving across to this new platform required acceptance by the networking team at PRACE, a transition period for each site, followed by the dismantling of the old Star topology network.

In January 2017, replacement of their existing network was ordered by the board of PRACE. Acceptance of new MD-VPN platform as being fit for purpose was a major milestone, not just for the PRACE community, but for the NREN community as a whole, given that this technology was developed by the NRENs in the GN4-1 project. This opens up a new chapter in the networking capabilities and the service offering that GÉANT can provide to the European research community as a whole. As the pilot platform was in production, PRACE was able to move its existing traffic over to the live MD-VPN system with very limited configuration work required compared with a new setup. Utilising the existing MD-VPN platform developed and built for the Human Brain project saved both time and money for PRACE. To compare, setting up an optical, point-to-point connection could take up to 280 days to be delivered.

To facilitate the switch over from the old star topology to the new MD-VPN platform, a four-month transition period was established by PRACE for the end sites, starting from January 2017, shortly after the decision was taken, to May 2017. Once the transition period was completed, dismantling of the old network topology began. In addition, a mailing list for information exchange between the sites and the NREN engineers was also established. This provided support for the day-to-day operations and ensured a smooth transition.

Given that MD-VPN traffic is aggregated across an existing NREN link to the GÉANT backbone, it is difficult to accurately identify which end sites are now being assisted through this new system. However, as of writing this document, there are 11 proxies which have been setup by GÉANT to assist 8 NRENs in participating in the MD-VPN solution and 20 MD-VPN BGP unicast sessions set up jointly by GÉANT and 14 NRENs. These are detailed in the tables below:

NREN	Date of Service Activation
ARNES	2017-04-18
CESNET	2014-06-20
CESNET	2017-04-21
CYNET	2017-05-31
CYNET	2017-06-08
REDIRIS	2014-06-20
REDIRIS	2016-11-17
SANET	2017-11-28
SURFNET	2017-04-06
SWITCH	2016-10-24
ULAKBIM	2017-08-18

Table 3.1: MD-VPN Proxy list

The following NRENs have been assisted in setting up “full” MD-VPN:

NREN	Date of Service Activation
AMRES	19/06/2014
Belnet	22/07/2014
BREN	21/01/2015
CARNet	19/06/2014
DFN	19/06/2014

NREN	Date of Service Activation
DFN	19/06/2014
FCT-FCCN	31/08/2017
GARR	20/11/2014
GARR	20/11/2014
GRNET	17/07/2014
HEAnet	03/12/2015
HEAnet	03/12/2015
KIFÜ	29/05/2014
NORDUnet	19/06/2014
NORDUnet	04/11/2015
PSNC	19/06/2014
PSNC	26/04/2017
RENATER	19/06/2014
RENATER	19/07/2016
SURFNET	03/04/2017

Table 3.2: MD-VPN BGP Sessions list

As described, compared to a purely optical approach, the speed of turnaround in solution delivery following completion of the pilot project was relatively quick. This highlights one of the key advantages of the MD-VPN system when compared with alternative solutions. This also represents a key advantage of the user support activity within the project, where the latest technologies developed can be leveraged to support user communities, so as take advantage of improved efficiencies and working practices. In this case, the affordability, adaptability and resiliency of the PRACE network was improved, compared with the previous optical star topology.

3.5 Solution Benefits

The adoption of the new MD-VPN platform marked a step change in the affordability of the network service for PRACE. Purely optical connections are expensive to install and maintain compared to utilising layer 3 connectivity, especially if guaranteed bandwidth is not required. Prices for optical circuits vary depending on the distance between the two connection points, but can be anywhere within the range of tens of thousands to hundreds of thousands of euros per year. Whereas, MD-VPN utilises the existing NREN connections to the GÉANT backbone.

Due to differences in the payment structure or payment arrangement for each local NREN, PRACE participating sites pay differing amounts for their connection and additional services, such as a point-to-point circuit, to their local NREN. For the old network topology it is not known what the exact total savings equate to, as a result of implementing the new MD-VPN solution. This is because, as mentioned before, each NREN has their own pricing policy towards a site within their jurisdiction, both for the point-to-point circuit and the MD-VPN solution. This figure is unknown to GÉANT. It can, however, be reasonably assumed that the NRENs would not continue to charge for the point-to-point service that is no longer provided. As such, the cost that GÉANT passed on to the NRENs for the old topology can be used as a plausible figure for the savings to the PRACE end sites. This has been calculated collectively at €225,000 per year in total. Such cost is no longer incurred by the PRACE end sites as a result of the switch to the MD-VPN solution.

Without this architecture change, costs would have been incurred by PRACE for the replacement of the central DAISA switch. Additional, much higher, costs would also have been incurred if any new optical connections were required in order for a new facility to join the closed network. Instead, the cost of the new system was limited to the connection of the end site to the local NREN and a fee for the establishment and maintenance of the MD-VPN system. This was significantly less than the cost of the solution based on the optical platform. Prices for the end sites to connect to the MD-VPN solution ranged from zero to below EUR40 000. This change in the underlying technology and topology of the network will also increase the affordability of the platform for PRACE and its contributing supercomputing centres going forward.

Another significant advantage the new platform delivered for PRACE was an increase in flexibility. New connections to the PRACE VPN can now be made in shorter timescales, when compared to the previous topology. Also, due to the MD-VPN system utilising technology that is already supported on the NREN networks, no or little additional equipment would be required to set up a connection. Again, lowering the barrier for joining the PRACE community. Instead, the work involved in the setup largely revolves around configuration of the routers that connect the end site to the NREN. This speed of delivery along with the reduced technical barrier of entry means that PRACE are now in a position to be more flexible and adaptable when future projects require temporary connections.

The new system, utilising the inbuilt resilience and redundancy of the NREN and GÉANT backbone, is a vast improvement compared to the former network design. Previously, the star topology represented a single point of failure in the central DIASA switch. The current implementation of the GEANT IP backbone underpinning the MD-VPN service, in partnership with participating NREN networks, is an inherently resilient and redundant network. Such characteristics are also part of the PRACE MD-VPN-based solution. If a link drops, re-routing via alternative paths now takes place automatically and transparently to the user. In the former design, if an optical link dropped, reestablishment of the route only took place once the optical path was re-established, unless the circuit had optical protection, which was an additional up-front cost. Responding to and resolving these types of network issues on a purely optical system takes time and a significant co-ordination effort between multiple actors. A connection issue on the former infrastructure, such as the one just mentioned, would have impacted significantly on PRACE's operations. Instead, the new MD-VPN platform is able to deliver significantly better resiliency and robustness in comparison.

The MD-VPN system also ensures the efficient use of the available networking infrastructure between the end sites. Previously, there was an excess of available capacity on the optical point-to-point connections, as described in Section 3.3. By using MD-VPN, the end site traffic is now aggregated across the existing NREN/GÉANT backbone connections, utilising the existing capacity monitoring and management put in place by both the respective NREN and GÉANT (via NA3 T1). This also means that future growth of the PRACE network traffic can take advantage of the existing capacity on the NREN/GÉANT backbone links as well as assisting NRENs in utilising more of the existing capacity without impacting on other service users.

By utilising well-established networking technologies, supported by all the NRENs' architectures in a new way, required little to no configuration work for the new topology. New connections can now be established within a few weeks, compared with months when using the old optical network. For instance, when the Swiss supercomputing centre joined the PRACE network's new MD-VPN system in 2016 it was able to connect without additional investment in expensive optical equipment. This demonstrates how the MD-VPN system reduced the barrier of entry for participants joining PRACE following the adoption of MD-VPN.

3.6 Future Directions

In future, PRACE intends to award grants to research institutes to allow connections to the PRACE system. Institutes would be able to connect temporarily in order to utilise the compute facilities offered by PRACE to perform their research. As a pilot, the Human Brain project allowed the MD-VPN system to be demonstrated as fit for this type of purpose. Such flexibility could not be achieved using the previous system.

The user support team continues to liaise regularly with representatives from PRACE in order to ensure that the existing system meets their requirements as well as exploring PRACE's needs and pain points to anticipate future service interests.

3.7 PRACE Solution Summary

By adopting the new MD-VPN platform developed by the GÉANT community, as suggested by the user support team, PRACE have changed the way in which it offers services to users as well as to the wider European research community. It has provided new levels of affordability, adaptability and resiliency in the design and operation of the network, when compared with the previous optical private network topology.

The new MD-VPN technology was successfully tested in a pilot project for PRACE, benefiting the Human Brain research programme. Five European Tier 1 supercomputing centres were connected using the new solution during the pilot project: BSC (Spain), CINECA (Italy), CSCS (Switzerland), GCS (Germany) and GENCI (France). This could only have been achieved through the collaboration with the NRENs RedIRIS, GARR, SWITCH, DFN and RENATER.

For PRACE, switching to the MD-VPN system has opened up new ways to provide user services, quicker connectivity, and enabled temporary connections. This is in marked contrast to the inflexibility of the old network platform which was slow to configure and difficult to connect.

4 CLARIN

4.1 The CLARIN Organisation

CLARIN is the Common Language Resource and Technology Infrastructure. It is a distributed network, made up of the CLARIN Governance and Coordination body: CLARIN European Research Infrastructure Consortium [CLARIN_ERIC], national consortia, centres of expertise and online services. It is a research infrastructure initiated from the vision that all digital language resources and tools from Europe and beyond are accessible through a single sign-on, online environment for the support of researchers in the humanities and social sciences.

In 2012, CLARIN ERIC was established to create and maintain an infrastructure to support the sharing, use and sustainability of language data and research tools. CLARIN provides easy and sustainable access to digital language data, in written, spoken and multimodal form. It also offers advanced tools to discover, explore, exploit, annotate, analyse or combine such datasets, wherever they are located. This is enabled through a networked federation of centres: language data repositories, service centres and knowledge centres, with single sign-on access for all members of the academic community in all participating countries. Tools and data from different centres are interoperable, so that data collections can be combined and tools from different sources can be chained to perform complex operations to support researchers in their work.

The CLARIN infrastructure is fully operational in many countries, and more than 30 participating centres offer access services to data, tools and expertise. At the same time, CLARIN continues to be rolled out in recently joined countries, and datasets and services are constantly being improved and updated.

4.2 Opportunity for Change

CLARIN operates its own service provider federation (SPF), with a setup following an evaluation of the existing trust and identity frameworks between 2008 and 2011. Operating the SPF involves coordinating identity providers, users and over 30 service providers. For example, every time a new service provider joined the CLARIN infrastructure, further work was required in order for the participating institute to conform to the authentication, authorisation and identification (AAI) management processes and procedures established by CLARIN’s in-house system. This often meant that if a new service provider institute required a previously unreleased AAI attribute to be released by other institutes, CLARIN would need to contact and negotiate that attribute release from the other CLARIN-centres [CLARIN-Centres]. Only by releasing the required attributes could a user access the resources from the service provider. Attribute release represented a significant management overhead for CLARIN.

CLARIN’s overall ambition was to connect all European countries to their service. As the number of institutes and countries joining CLARIN increased, the concern was that the management overhead would grow exponentially. This would increase costs for CLARIN and could slow down the uptake of new service users, institutes and countries to the CLARIN project.

The other challenge CLARIN faced was that in order to reach all intended users would require complete agreement of identity providers in each country to join the SPF. This required an explanation of how the SPF operated and then negotiating with thousands of identity providers, unless a national identity federation had been established/targeted. Although not every IdP would have automatic enrolment in CLARIN if the national federation signed up to CLARIN’s SPF. To compound these issues, a national identity federation was not always present in each country. As of early 2014, CLARIN had connected 202 identity providers and 6 national identity federations to the 11 CLARIN service providers.

It was with these challenges in mind that GÉANT approached CLARIN to collaborate on eduGAIN service improvements. These would not only help to improve access for CLARIN to an expanded IdP pool and user base but would also help the wider eduGAIN community.

4.3 Solution Identification

CLARIN was one of the early adopters of federated identity management technology in the research and education community. CLARIN required a system that was able to deal with the access and identification of a large number of distributed users across several country nodes, where authorisation rights had to stay within the responsibility of each centre. Relying upon federated identity management made sense to CLARIN, to deal with the distributed nature of providing services to its user base. As such, significant investment was made in the federated identity management concept at an early stage of CLARIN. Back in 2012 when CLARIN ERIC was launched, eduGAIN was not yet production-ready. Instead, CLARIN created its own service provider federation it could fulfil the service that CLARIN was designed to provide. This made it possible for CLARIN to become a full, official member of different national identity providers.

However, there were a number of issues. Each service provider had to sign an agreement with each respective national identity federation. As CLARIN grew, further signatures from new identity federations were required. When a country did not have a national identity federation, this caused additional complications as signatures would have to be sought from individual identity providers, where possible, in that country. Getting agreement from an identity provider, explaining the SPF structure to new identity federations and managing the systems required to run the service created a significant bureaucratic overhead. Although eduGAIN does not interact with individual identity providers, GÉANT assists national research and education networks in creating their own national identity federations and to help these new federations join eduGAIN. This helps grow the opportunities for identity providers to reach larger audiences than they typically would reach on their own. Each national federation is responsible to define its own internal policies regarding the addition and operation of federation entities, such as identity and service providers.

Prior to the creation of CLARIN ERIC, between 2008 and 2011, CLARIN had evaluated eduGAIN as a possible solution to its AAI conundrum. eduGAIN was still a prototype, as it launched as a service in April 2011. Further evaluation by CLARIN in late 2013 deemed eduGAIN still not ready to meet its trust and identity requirements, largely due to the relatively limited number of IdPs that were signed up to eduGAIN at that point [CLARIN_EVAL].

In 2013, due to the increasing administrative burden in co-ordinating service providers, CLARIN amended its SPF agreement in such a way that enabled the CLARIN consortium to sign AAI agreements on behalf of service providers. This was predominantly used for signing agreements with national identity providers. The intention behind changing the agreement was to expedite the uptake in identity providers and therefore end users. However, the burden of having to manage the signup and curation of identity providers to CLARIN's in-house SPF grew. One advantageous consequence provided by the change in the SPF agreement was that it meant any agreement reached between the GÉANT community and CLARIN would not necessitate the individual sign off of each CLARIN centre.

The GÉANT community approached CLARIN to offer support and collaboration with AAI. Cooperative work on attribute release checks were proposed, which could then be incorporated into the eduGAIN AAI service. This would then also benefit the wider trust and identity community at large. Under development separately, although coinciding with the development of an identity release check facility as part of eduGAIN, the GÉANT community also provided an overview of the identity provider's opt-in rate per country.

4.4 eduGAIN

eduGAIN enables the trustworthy exchange of information, related to identity, authentication and authorisation (AAI), between service providers and research and education institutions or other identity providers. eduGAIN achieves this by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange. This exchange of information contributes to the seamless operation of services, whether they are developed within the GÉANT Project, provided by other communities represented by, or associated with, the GÉANT partners, or provided by commercial Service Providers, which benefit collaboration in the research and education community.

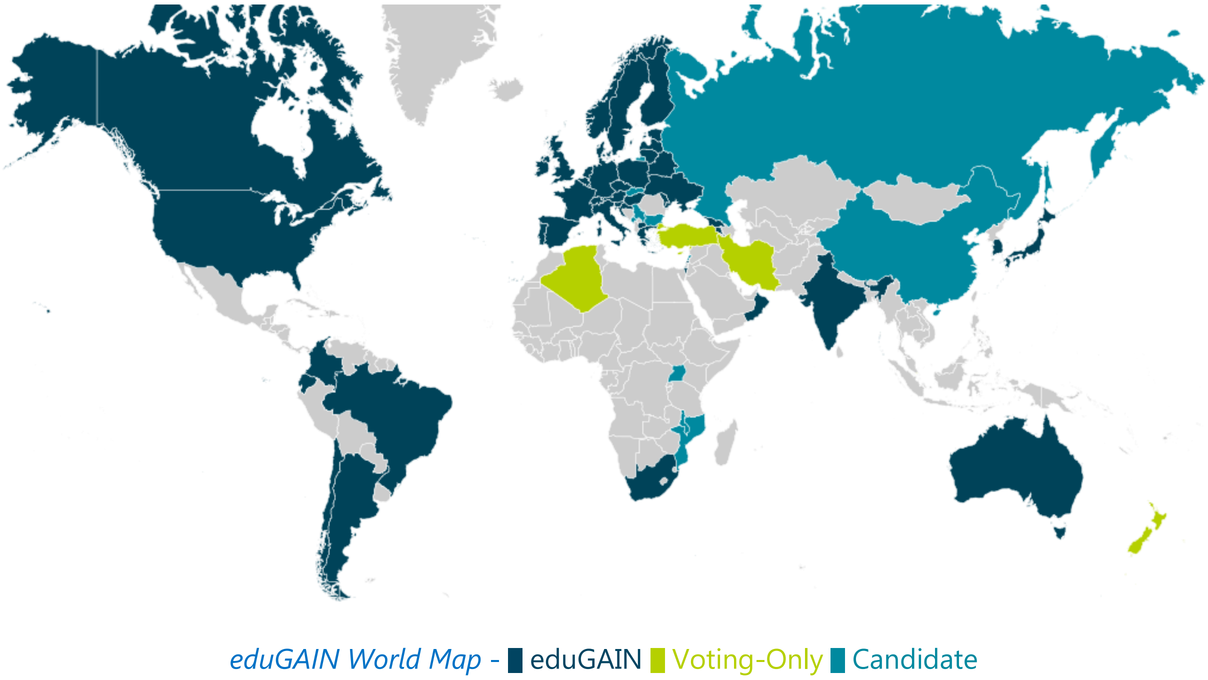

Figure 4.1: eduGAIN member world map, August 2017

eduGAIN provides access to all the online services that students, researchers and educators need, while minimising the number of accounts users and service providers have to manage. This reduces costs, complexity and security risks; giving service providers access to a larger pool of users internationally, and allows users to access resources of peer institutions or commercial or cloud services using their one trusted identity.

With eduGAIN participants from more than 2000 identity providers accessing services from over 1,500 service providers, eduGAIN has fast become the primary mechanism to inter-federate for research and education collaboration around the world.

Federated Identity Management in eduGAIN works by having a group of institutions and organisations signing up to an agreed set of policies for exchanging information about users and resources, so as to enable access to and use of resources provided by a service provider. Many organisations use AAI to build a trusted environment where users can be identified electronically using a single identity. These systems can also contain information about a user’s access rights based on attributes characterising their role. Resource owners (service providers) may use these federated environments to control federation participants’ access to the provided resources.

The existence of multiple AAIs and multiple identity federations makes it technically and administratively difficult when a user attempts to gain access to protected resources and services from other federations. The user must first be successfully authenticated by his/her home AAI and then authorised by the visited service provider.

eduGAIN enables different AAIs to interact securely. The eduGAIN infrastructure contains a "Metadata Distribution Service", which regularly retrieves and aggregates information from participating federations about services and identity providers, and makes this information available to those who are part of the eduGAIN community.

eduGAIN coordinates necessary elements of the federations' technical infrastructure by providing a policy framework controlling the exchange of this information. eduGAIN also liaises with other federation initiatives such as REFEDS (Research and Education Federations) and the GÉANT project's Federation-as-a-Service team.

4.5 Solution Delivery

In early 2015, following a series of interactions between the GÉANT community and CLARIN, GÉANT proposed collaboration on the attribute release check. The early interactions took place on the GÉANT-hosted REFEDs mailing list and through personal encounters during conferences and meetings, such as FIM4R and the European Workshop for Trust and Identity [FIM4R], [EWTI]. These interactions were born out of problems CLARIN were having with their trust and identity SPF. The work focussed on the release of attributes to service providers from identity providers and the uptake of identity providers to their SPF. By this time eduGAIN had over 2600 identity and service providers as part of its framework, which out-stripped CLARIN's aggregated IdP numbers.

Mindful of CLARIN's difficulties, a solution aimed to address the following points was put forward:

- Consolidation of CLARIN service providers to a single national federation.
- Ability for future CLARIN service providers to join a single national federation.
- Development of an attribute release check.

Although CLARIN's existing service providers were already members of eduGAIN at the time, this was via separate identity federations. Having each service provider register with their own respective national AAI federation was becoming increasingly more difficult to co-ordinate. However, choosing which registrar and the corresponding Authentication and Authorisation Infrastructure (AAI) to collectively sign-up to, was a challenge to overcome.

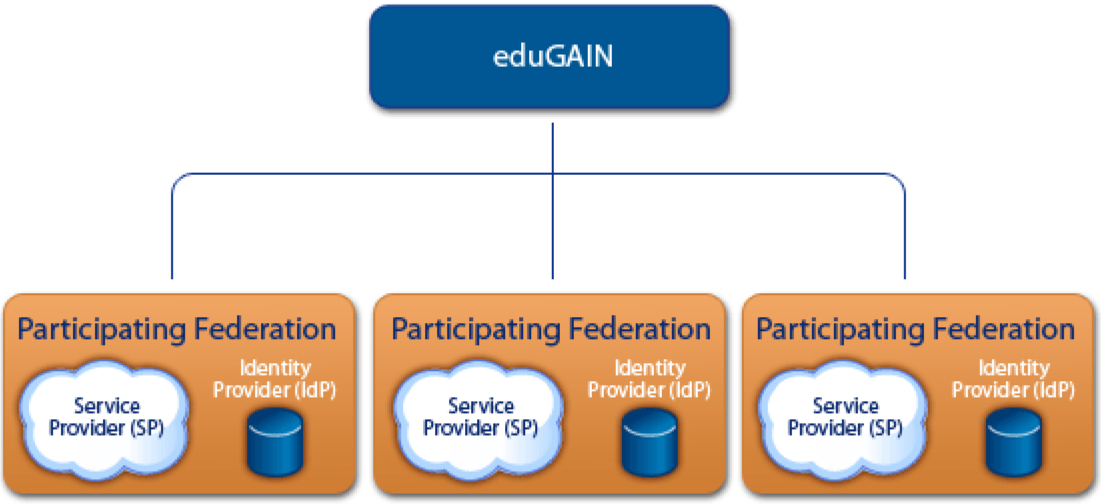

Figure 4.2: eduGAIN identity federation overview

eduGAIN acts as the glue which allows participating identity federations to be interoperable with each other. Each federation agrees on a set of common standards and policies which ensures this interoperability. For a service provider to join eduGAIN, they must first join an identity federation which is a member of the eduGAIN service. Once they have joined, it is then down to the identity federation to add service providers into the eduGAIN system.

Choosing which identity federation to join is not necessarily geographically dependant on where the service provider, or organisation headquarters, is located. Instead, each identity federation has its own merits and costs for joining. GÉANT helped CLARIN to gain an understanding of the identity infrastructures it could join based on a set of requirements defined by CLARIN. It was eventually decided that the DFN-AAI was the most appropriate authentication and authorisation infrastructure to join for them. This was one of the biggest hurdles that had to be overcome for CLARIN to join the eduGAIN system.

While the negotiations to select and join an identity infrastructure were taking place an attribute release service was also being developed, in collaboration with CLARIN. This is a service that allows the use of a request to release attributes that had not previously been released to inform identity providers. Attribute release checks had already been developed for access and authorisation infrastructures but on a much simpler scale.

The release of attributes was a problem both for eduGAIN and for CLARIN's service providers. There were, and still are, a number of examples of institutions and national identity providers not releasing attributes in the early days of eduGAIN [ANALYSIS]. However, the introduction of the attribute release check service streamlined the resolution of one of the largest problems faced in trust and identity, that being identity providers not releasing the required attributes that service providers needed to allow users access to their systems or platforms.

One of the primary motivations behind identity providers not releasing attributes is due to security and privacy concerns. This is especially true when considering that data privacy legislation is not a common framework around the world. Instead, most nations have their own data privacy legislation, which may or may not align with other nation states, especially relevant given that eduGAIN reaches beyond Europe. Within the EU, the Data Protection Directive and latterly its replacement, GDPR (since May 2016) are followed.

European legislation is also seen by some as complex and nuanced. This has led to a small number of individuals responsible for data privacy in identity provider organisations to take the simple decision of locking all data down, rather than trying to define the risk and releasing the needed profiles. This is not an indicator of a lack of motivation to provide effective trust and identity services to researchers, but is predominantly due to significant under-investment in identity management technologies at a local level.

There is also the added complication of a lack of proper processes and procedures to effectively manage data protection within some identity provider organisations. eduGAIN has made significant progress in this area over the years, providing guidance and tools to make data release safe and easy. For example, in 2014, the Research and Scholarship entity category was released [REFEDS]. This was designed to provide a safe way of releasing a small bundle of attributes to service providers that had proven they required the attributes requested for research and scholarship needs. This need is verified with the service providers T&I registrar, according to the specifications established through REFREDS.

The attribute release check goes further than this, putting users in the position to request from their own organisations that their attributes be released. This puts the level of consent back in control of the user, rather than the user's organisation. Operators are much more willing to release attributes when contacted by their own users first, rather than pre-emptively by the service provider.

Along with the attribute release check, further work was done in collaboration with CLARIN, on the content and structure of automated error messages sent to identity providers if attributes weren't released. This helped identity providers to quickly understand the reasoning and justification behind why a particular attribute was required. It allowed a quick way for the right person to be notified at an institution about which organisation was requesting particular identity attributes and the steps required to release those needed attributes. This helps end users who experience problems in accessing the content they require for their research to have a resolution quickly, without having to do that administrative work themselves. It now means an administrative task which used to cause frustration for users, is much more streamlined and simplified allowing researchers to get on with the research they are taking part in.

In all, the duration of the collaboration to define, develop and test the attribute release check with CLARIN took 18 months. The design work for the attribute release check was started in GN4-1 SA5 Task 5 (Enabling Users), while the operation and development is continued by GN4-2 JRA2 Task 2 (eduGAIN Service Development - Research and Service Providers). Contributions for the delivery of eduGAIN and the attribute release check as part of the GÉANT project were from the NRENs DFN (Wolfgang Pempe), CSC (Sami Silén), KIFU (Frank Tamás and Kristof Bajnok) and SWITCH (Lukas Hämmerle). From CLARIN's side, contributions to the development and adoption of eduGAIN were from Martin Matthiesen, Dieter Van Uytvanck and Jozef Mišutka.

During this time, CLARIN signed a special agreement with DFN-AAI to be able to register new SPs of their SPF using a simple and pragmatic workflow that provides benefit for all involved parties. This further expanded the eduGAIN community through the service providers which CLARIN made available, as well as developing an additional feature for eduGAIN. This feature is now being adopted by other members of the community, enforcing the belief that focusing on development of features on behalf of the wider community has the largest impact.

4.6 Solution Benefits

The adoption of eduGAIN by CLARIN has led to many improvements and benefits for them, concerning trust and identity. It enabled trustworthy exchange of information between identity federations without the need for many bilateral agreements. It reduces the cost of developing and operating services. Improves the security and end-user experience of services; as well as enabling CLARIN to greatly expand its user base compared with just utilising its own SPF. The interaction between CLARIN and the GÉANT community also meant that CLARIN now has a knowledgeable group of contacts from across Europe who they can talk about AAI with, allowing CLARIN to benefit from the future technical developments being worked upon by NRENs and the GÉANT project, while at the same time having a single point of contact, through DFN, for support queries. This reduces the overall administrative burden on CLARIN when dealing with any AAI related technical issues.

However, as much as the solution benefited CLARIN, the wider community was strengthened and improved far more, through the increased number of services now available to identity providers and their end users. The attribute release check and friendly error messages also provides a level of service not previously encountered or developed in the R&E trust and identity community. This service, although simple in its approach, has had a deep reaching impact on how trust and identity federations can now work. By allowing users to prompt their AAI operators to release attributes without needing to understand the technical details behind this release. It opens up eduGAIN to further involvement from new service providers and goes some way to address those service providers who were previously concerned about the lack of attributes which were released by identity providers, limiting the user base that they could securely support. These developments ensure eduGAIN can be considered one of the R&E community leading trust and identity frameworks to adopt.

4.7 Future Directions

One of CLARIN's biggest concerns was that it would not be able to reach as many users as forecast. Given CLARIN's objective to provide language services to a global community, the ability for identity providers to release the required attributes was crucially important. Now that the attribute release check has been developed, each time a country is added to the eduGAIN community, CLARIN and any other future service provider, can be assured with the development of the attribute release check, identity federations and identity providers received a helpful tool, which allows verifying that attributes to eduGAIN services – such as those from CLARIN – are released according to the best common practices. This will always be a work in progress, due to the complexities in data security and the jurisdictions that each country operate within. With the development of the friendly error messages and the attribute release check, this work in progress becomes much more streamlined, much more user friendly, ultimately benefiting the wider community as well as CLARIN.

From this viewpoint of trying to serve the community as a whole, eduGAIN pushes to develop new working practices within the context of the framework, so as to further enhance and solidify the core aspirations of the eduGAIN project.

4.8 CLARIN Solution Summary

The CLARIN SPF and notably the CLARIN IdP (which is only trusted within CLARIN) made it possible to develop AAI based services, within CLARIN, that would work at least as well as national service within the SPF. The CLARIN IdP could even accommodate users that could not use their home organisations credentials.

Although CLARIN did make headway in developing its own SPF, it became increasingly challenging as the number of identity providers multiplied. This growth in management overhead, in line with CLARIN's desire to reach as many users as possible, along with the advances and developments in eduGAIN, led to an operational adjustment that adhered to the organisation's pragmatic approach.

With the rapid uptake and expansion of the eduGAIN identity providers across the world, as well as the offer by the GÉANT community to collaborate on developing an attribute release check, eduGAIN became an attractive solution. Following the adoption of the DFN-AAI, work was conducted on an attribute release check service with enhanced error messages to assist identity providers in releasing the required attributes for service providers. This means that CLARIN can continue to build services using its SPF where practical, while maintaining eduGAIN compatibility. This made it possible for the CLAIRN community to slowly get out of a vicious circle of “No attributes – No services” towards a more progressive “Let’s release attributes (also via eduGAIN), because our users demand it” approach. This path is especially attractive to CLARIN participating organisations outside of Europe and shows in the statistics [CLARIN_STATS].

This work was conducted over 18 months, through a collaboration of staff from GÉANT, NRENs and CLARIN, and culminated in the delivery of a service which benefits the entire R&E trust and identity community. However, the solution has proved very beneficial for CLARIN. Martin Matthiesen, Senior Application Specialist CSC-IT (Finland), summarised the interaction for the Finnish CLARIN group as such [FIN-CLARIN]:

“I can confirm that that collaboration has proven very useful at least from FIN-CLARIN’s perspective. Users can now quickly inform their operators about their AAI needs without having to understand technical details. Operators are much more willing to release attributes when they are contacted by their own users first, rather than pre-emptively by the Service Provider.”

5 Conclusion

Both use case examples presented in this document show the impact of user engagement provided by the GÉANT community through the GÉANT project, GN4-2. This is not just beneficial for the individual organisations and their research communities, but for the wider European and global research and education communities at large. It shows how the collaboration between the National Research and Education Networks raises European research to the next level by enabling European researchers to conduct cutting edge research in collaboration with their peers worldwide, unhindered by network connectivity or system accessibility.

In the case of CLARIN, the GÉANT project assisted in the development of an attribute-release check feature which helped to refine the eduGAIN project, making it that much richer and a more valuable service for the global research and education community.

For PRACE, the development of the proof of concept MD-VPN system in a research and education framework was ground breaking. It signified a shift in the capabilities, flexibility and resiliency that can now be achieved for HPC users via their NRENs.

In each case, user account management was approached in a logical and strategic way, building upon long-term relationships, account management, requirements gathering and exploration of pain points experienced, both for the user communities mentioned and for the wider, global research and education community. In both cases, technologies developed within the GÉANT project by the GÉANT community were demonstrated and proven to deliver value and cutting edge services with the highest community impact. The use cases describe how NA3 T2, and the project at large, work closely with a variety of communities, providing first point-of-contact through to organising and co-ordinating access to technical, managerial and policy advice, to build and deliver solutions for network and trust and identity services.

References

[ANALYSIS]	https://www.clarin.eu/sites/default/files/CE-2013-0247-analysis-edugain.pdf
[CANARIE]	https://www.canarie.ca/about-us/
[CLARIN]	http://www.clarin.nl/node/6
[CLARIN-Centres]	https://www.clarin.eu/content/clarin-centres
[CLARIN_ERIC]	https://www.clarin.eu/content/governance
[CLARIN_EVAL]	https://www.clarin.eu/sites/default/files/CE-2013-0247-analysis-edugain.pdf
[CLARIN_STATS]	https://lindat.mff.cuni.cz/services/aaggreg/
[EaPConnect]	https://www.eapconnect.eu/
[eduGAIN]	https://www.geant.org/Services/Trust_identity_and_security/eduGAIN
[eduTEAMS]	https://www.geant.org/Innovation/eduteams
[ESnet]	https://www.es.net/
[EWTI]	http://identityworkshop.eu/topics.html
[FIM4R]	https://fim4r.org/events/
[FIN-CLARIN]	https://kitwiki.csc.fi/twiki/bin/view/FinCLARIN/KielipankkiFrontpage
[GÉANT IP]	https://www.geant.org/Services/Connectivity_and_network/Pages/GEANT_IP.aspx
[HUMAN BRAIN]	https://www.humanbrainproject.eu/en/
[Internet2]	https://www.internet2.edu/
[MD-VPN]	https://tnc15.terena.org/getfile/2962
[perfSONAR]	https://www.perfsonar.net/
[PRACE]	http://www.prace-ri.eu/
[RedCLARA]	https://redclara.net/index.php/en/
[REFEDS]	https://refeds.org/category/research-and-scholarship
[SPF]	https://www.clarin.eu/content/service-provider-federation
[TEIN]	http://www.teincc.org/teincc/about/overview.do
[UbuntuNet Alliance]	https://ubuntunet.net/

Glossary

AAI	Authentication and Authorisation
EaP	Eastern Partnership
ERIC	European Research Infrastructure Consortium
FET	Future and Emerging Technologies
GN4-2	GÉANT Network 4, Phase 2
H2020	Horizon 2020 (EU Research and Innovation Programme, 2014 to 2020)
HPC	High Performance Computing
idP	Identity Provider
IP	Internet Protocol
NA	Networking Activity
NISN	NASA Integrated Services Network
NREN	National Research and Education Network
OTRS	Open-Source Ticket Request System
PRACE	Partnership for Advanced Computing in Europe
R&E	Research and Education
SDN	Software Defined Networking
SP	Service Provider
SPF	Service Provider Federation
T&I	Trust and Identity
VPN	Virtual Private Network