GÉANT

Compendium 2023

of National Research and Education Networks in Europe

GÉANT
Networks • Services • People

22-07-2024

Deliverable D3.3
Compendium Report

Contractual Date:	30-09-2024
Actual Date:	22-07-2024
Grant Agreement No.:	101100680
Work Package:	WP3
Task Item:	Task 1
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT Association
Document ID:	GN5-1-24-80958b
Authors:	M. Adomeit (SUNET), S. Buscaglione (GÉANT Association), V. Capone (GÉANT Association), Z. Fischer (GÉANT Association), T. Fryer (GÉANT Association), S. Garavelli (CSC), D. Luyten (Belnet), A. Moens (GÉANT Association), M. Reale (GÉANT Association), M. Ristkok (EENet), M. Kremers (SURF), J. Ross (GÉANT Association), L. Schäfer (DFN), J. Tendel (DFN), D. Wüstenberg (GÉANT Association)

Abstract

The GÉANT Compendium provides an authoritative reference source for anyone with an interest in the development of research and education networking in Europe and beyond. Published since 2001, the Compendium provides information on key areas such as NREN budget and staffing; end users; involvement in EC-funded projects; network, traffic and capacity; and services. This report primarily covers the period January to December 2022. The GÉANT NREN Compendium can be found online at: https://compendium.geant.org/.

Co-funded by
the European Union

© GÉANT Association on behalf of the GN5-1 project. The research leading to these results has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101100680 (GN5-1).
Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

A GUIDE TO THE GÉANT COMPENDIUM OF NRENS

Research and Education Networks (RENs) are internet service providers that run special communication networks dedicated to supporting the needs of the scientific and academic community. If this happens on the scale of a country, they are called National Research and Education Networks (NRENs). Forty-four European NRENs and RENs are interconnected by the pan-European GÉANT network, the largest and most advanced research and education (R&E) network in the world.

The GÉANT Compendium of National Research and Education Networks in Europe (the Compendium) is a comprehensive portrayal of the networks supporting the research and education community in Europe, giving a full picture of what the NRENs do to meet their users' requirements, the resources they have at their disposal, and the way they are organised.

The Compendium is the result of a broad, collective effort based on data from the annual NREN Compendium survey, which invites Europe's NRENs to provide detailed information about their network, equipment and users. The survey conducted in 2023 focused primarily on the period from January to December 2022, though some NRENs may have added more recent data if they were available. The results, based on responses submitted by 41 of the 44 RENs, are summarised in this document. Publicly available data, data from within GÉANT and data from subject-specific surveys were added to supplement the survey data and to cover additional areas such as trust and identity (T&I). Where such supplementary data were used, and where the data allowed and it seemed useful to do so, the report extends beyond 2022. However, unless otherwise stated, readers can assume that the data in this document originated from the Compendium survey results. The data from this and past NREN Compendium surveys can also be accessed from the online version of the Compendium [Compendium].

The diversity and complexity of the NREN community can make comparisons challenging. Also, due to the voluntary nature of the survey, the data record has gaps, i.e. not all data are present for all years for all NRENs. For time series spanning several years, this means the period over which a meaningful trend analysis is possible will differ, depending on the availability of sufficient comparable data[1].

The aim of the Compendium is to provide an overview of and insights into this multi-faceted community. It is simultaneously a depiction of the diversity of the NRENs and a reminder that, despite their variations and particularities, the European NRENs are built around delivery of the same interlinked core services.

This Compendium is a community-led document, created by the NREN community, for the NREN community, as a means to understand the status of the collective as a whole, as well as of each individual NREN. It is a dataset with which NRENs can inform and shape their strategic decisions.

[1] This is especially true when percentage increases across NRENs are shown (e.g. Figure 2.1: Development of total NREN budgets since 2019; Figure 2.6: Total staff numbers of the NREN sector; Figure 5.1: Increase of traffic into the NRENs from external networks (upper panel) and NREN customers (lower panel) 2020 to 2023; and Figure 5.5: Development of the NRENs' IRU networks 2019–2023). Such a trend analysis requires the same NRENs to be present over all the years in the series and any NREN that has not responded in one year needs to be excluded from the whole dataset. The period over which trends are shown therefore reflects the time over which the data available are still representative for the whole, i.e. the majority of NRENs are present in the numbers and the subset of NRENs in question is not biased geographically or with regard to size.

The Compendium has been compiled from information provided by the people within the NRENs, from the executive directors to technical officers, to service portfolio managers and many more professionals. Subject matter experts reviewed all the responses within a given area and summarised the main data points in this document.

A big thank you to the NRENs that took the time to complete the survey and provide their views.

EXECUTIVE SUMMARY

Published annually, the GÉANT Compendium presents a comprehensive picture of the National Research and Education Networks (NRENs) in Europe. This Compendium Report brings together some of the findings of the annual Compendium survey conducted in 2023 and focuses on the time period from January to December 2022; 41 out of the 44[2] GÉANT member and associate research and education networks took part in the survey. The report covers organisational aspects such as budget and staffing; end users; involvement in EC-funded projects; network and traffic; and services, including security, trust and identity and cloud services. In certain areas, the report draws on supplementary data; for example, the current report makes use of complementary data from other surveys in the sections on security and the section on clouds. Also, in some of these areas, more recent data have been used. The full Compendium Report, as well as the data from this and past surveys, is available online [Compendium].

Like past Compendium surveys, the 2023 results reveal changes and continuing trends in the NREN landscape, although the changes are mostly gradual.

Most European countries have a broadly liberalised telecommunications market, where access to bandwidth and technology is unconstrained by regulation or monopoly. NRENs therefore need to respond to the specific demands of the research and education community if they are to justify their existence to their funding bodies, and to their primary users. The data from the Compendium survey should help to trace how NRENs meet this challenge.

Budget and staff numbers

Reflecting the continuing increase in the importance of data networks in research and education, budgets and staff numbers have expanded between 2022 and 2023 (by 13.6% and 4.1%, respectively). The reported budgets across Europe now add up to €874 million and staff numbers have reached 2,990 employees – though in both cases only 4 NRENs account for about half of those numbers.

This indicates that in some countries NRENs have evolved into infrastructure providers that cover much more than the "classical" NREN portfolio such as network infrastructure, T&I and security services. While it is unlikely to happen in all countries, the emergence of such super-NRENs could be considered a long-term trend.

Organisational context of NRENs

NRENs in Europe share the role of providing network services to their national research and education user institutions. However, they differ considerably in their organisational context. About a quarter of Europe's NRENs are government agencies, while another quarter are member organisations set up by the R&E community. In between those extremes are mixed forms where both user institutions and government participate in the NREN's governance to different degrees. The extent to which NRENs are organised by their user institutions or are government controlled generally correlates (with some exceptions) with their funding model: government agencies tend to receive all or most of their money from the government while

[2] This figure includes BASNET, the NREN for Belarus, which was suspended from the GÉANT Association in 2022; the 5 Nordic NRENs represented in GÉANT by NORDUnet; and KREN, the REN for Kosovo*. For details, see Appendix A. This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo Declaration of Independence.

user-organised NRENs are for the most part user-funded institutions; mixed-governance NRENs tend to receive funding from both sources.

Pan-European activities

A clear trend over the last few years had been an increase in NRENs' involvement at the European level: the number of EC-funded projects (in addition to GN4-3/GN4-3N/GN5-1) which had at least one NREN as a participant almost doubled from 56 in 2018 to 102 in 2022. This trend has, at least for the time being, come to an end as the number has dropped to 88 in 2023. There is no clear reason explaining the drop, and it might be just due to chance. The number still represents a strong involvement of NRENs in EU projects, in particular as it is spread across 28 NRENs. While the project with the most NREN participants is EaPConnect2, which aims to decrease the digital divide within Europe by establishing and operating a high-capacity R&E network in the EU's Eastern neighbourhood, most of the projects that NRENs are involved in are connected to European e-infrastructures, in particular the projects supporting the delivery of the European Open Science Cloud (EOSC).

Traffic

The importance of research and education networks manifests in the volume of traffic NRENs carry. Traffic volumes have mostly increased over the past years, across all NRENs. The COVID-19 crisis interrupted this pattern, but only temporarily. With the pandemic ending, traffic growth has picked up again. It is, however, interesting that it took several years to reach and bypass pre-COVID levels; this suggests that some of the behaviour changes that COVID triggered, such as more ubiquitous working from home, are still present.

In line with the actual traffic growth, NRENs expect the upward trend to continue into the medium term: for the years 2024–2026, virtually all NRENs that responded to the survey forecast traffic growth, and more than half of them anticipate a growth of 50% across all organisations within the NRENs' remit – except for commercial partners. Even higher growth is expected to come from research institutions, with 79% traffic growth, and universities, estimated to grow by 74%, with schools not far behind (with 75% and 72% for primary and secondary schools, respectively). A potentially interesting development can be seen in the second tier of connections: compared with last year, NRENs have revised their expected traffic growth from non-university hospitals (51% vs. 68%), government bodies (37% vs. 52%) and commercial partners (15% vs. 35%). It is tempting to speculate that the hospital numbers anticipate developments in the medical data space, while commercial connections might anticipate the NRENs' role in a future EuroHPC network.

Capacity

While traffic volumes grew significantly during the past year, the capacities of NRENs' backbone and access networks increased at a steady but much slower rate, reflecting the longer timescale of network upgrades. It is noticeable, though, that the access networks keep increasing in capacity, especially for the non-core user types such as schools. The capacities for access to an NREN's network range from 1 Mbps up to 100 Mbps, depending on user types. Generally, 1 Mbps connections are becoming very rare, even for less demanding users such as schools, and connections greater than 1 Gbps are the standard for most demanding user types, universities and research institutes; in some countries, the typical connectivity for these users has reached 10 Gbps, and more than 90% of NRENs provide these high-capacity connections to at least some universities and research institutes.

Another aspect of NREN networks seems to have stalled: the length of their fibre network. Future surveys will show whether this is a momentary halt but a possible interpretation would be that most relevant sites are connected now – which would be in line with the ongoing increase in the capacity of the said network.

Services

NRENs have long since moved beyond their core role as connectivity providers, and now provide additional services, responding to technological changes and changes in the demands of the research and education community. A good example of this is the expansion and improvement of the trust and identity (T&I) infrastructure. Originally focused on securing access to R&E services, T&I infrastructures are increasingly being adapted to deal with the growth in cooperation and sharing of resources across institutions and borders. This is particularly apparent in initiatives such as InAcademia and MyAcademicID, which ascertain the student status to provides access to services that are not strictly speaking an R&E service domain, for example, student discounts. The work around the EU Digital Identity Wallet could eventually take these technologies even further beyond the boundaries of the R&E world and provide the foundation of a general electronic identity.

There has also been work to adapt T&I services for new challenges, on different levels. In response to eduGAIN's worldwide growth, a new governance structure has been installed that makes decision-making more efficient. On a more technical level, the Core AAI Platform (formerly eduTEAMS) has made strides towards establishing itself as the go-to architecture for pan-European research platforms.

Another such development is the ongoing commodification of cloud services. NRENs seek to make it easier for their users to take advantage of this trend, as is visible in the increasing use of the Open Clouds for Research Environments (OCRE) Framework among NRENs. Here, NRENs have moved to make their experience in procurement of these types of services available to their customers, leveraging their market size to gain discounts for their users. Cloud services are a prime example here, but procurement support extends to other areas as well. However, the use of the OCRE Framework is mostly confined to EU member states, a development that highlights a problem within the European NREN community: the status of their home country with regard to the EU essentially creates two classes of NRENs when it comes to procurement – NRENs from EU member states which are fully compliant with the EU Procurement Directive and who are therefore able to use EU-wide frameworks with no obstacles, and NRENs in non-EU countries who face additional challenges around making use of such frameworks.

While the diversity and complexity of the different NRENs can make comparisons challenging, it is the Compendium's ambition to provide an overview of and insights into this thriving, multi-faceted community. Through these annual snapshots, produced each year since 2001, GÉANT continues to monitor the growth and changes among the NRENs in a systematic way, adjusting the scope of the Compendium accordingly to provide a unique dataset with which NRENs can inform and shape their strategic decisions.

1. ABOUT GÉANT

The pan-European GÉANT network plays a fundamental role within Europe's e-infrastructure provider landscape. GÉANT enables scientific excellence, research, education and innovation [GÉANT]. Through its integrated catalogue of connectivity, collaboration and identity services, GÉANT, together with its National Research and Education Network (NREN) partners[3], provides users with highly reliable, unconstrained access to communication, computing, analysis, storage, applications and other resources. The GÉANT network's connections also ensure that Europe's research community is connected to similar infrastructures, both within and beyond Europe.

GÉANT's high-speed backbone provided connectivity with 44 NRENs during the GN4-3 project, reaching tens of millions of users in 10,000 institutions across Europe, and more than 100 countries worldwide through links with other regions. The core backbone is capable of multiple 100 Gbps over each fibre link, and Terabit connectivity can be achieved by a single node.

The network is funded by the GNx-N projects, of which the incarnation relevant for this Compendium Report was GN4-3 (and GN4-3N), with 39 partners[4]. The focus of the GN4 Phase 3 (GN4-3 and GN4-3N) projects [GN4-3; GN4-3N] was to provide the European research sector with an infrastructure that promotes scientific excellence through access to and reuse of research data. It also aimed to make scientific infrastructures Europe-wide more cost-efficient through the promotion of interoperability with other e-infrastructures. GN4-3 and GN4-3N began in 2019 and were funded by the EC's Directorate-General for Communications Networks, Content and Technology [DG_Connect]. GN4-3 continued until the end of 2022 and has since been succeeded by GN5-1, while GN4-3N continued until the end of 2023[5].

The overall objective for the GÉANT partnership is to provide connectivity for European Research. GÉANT aims to offer European researchers the network, communications facilities and access to applications that ensure the digital continuum necessary to allow them to conduct world-class research in collaboration with their peers around the world.

In addition to the pan-European coverage, GÉANT's global connectivity enables the European R&E community to collaborate with peers and access data sources in more than 65 countries and territories outside Europe, with a total global capacity today of nearly 1.9 Tbps, including 1 Tbps to the USA and Canada, 200 Gbps to Latin America, 230 Gbps to Sub-Saharan Africa, nearly 150 Gbps to North Africa and Western Asia, and 260 Gbps to the Asia-Pacific region. Intercontinental links are provided through a variety of approaches, with some funded by GÉANT members and the GÉANT project, and others in collaboration with or by their global R&E networking partners. To maximise the benefit of all global links, GÉANT works with R&E networks in Europe and across the globe to establish mutually supportive back-up collaborations, thereby ensuring that if one link suffers an outage, traffic is quickly and efficiently switched to other paths. This is done today through the Advanced North Atlantic

[3] Not all members and associates of GÉANT are actually National Research and Education Networks (NRENs); some are rather RENs. However, for simplicity, the Compendium refers to "NRENs".

[4] While there are 44 NRENs in Europe, only 38 of them were directly part of the GN4-n (and now the GN5-n) projects. The Nordic NRENs (CSC/Funet, DeIC, RHnet, Sikt and SUNET) have formed their own regional ISP, NORDUnet, which takes part in the GNx-N projects.

[5] GN4-3 had a budget of €118,879,719 (with an EC contribution of €77,500,000); GN4-3 ended in December 2022 and has been followed by GN5-1, which started in January 2023. GN4-3N ran until December 2023 and had a budget of €63,125,000 (with an EC contribution of €50,500,000).

(ANA), Asia-Europe Ring (AER) and Bridging Europe, Africa and the Americas (BEAA) collaborations.

The development of GÉANT's global reach has been substantially advanced thanks to support received over two decades from the European Commission via the Directorate-General for International Partnerships [DG_INTPA] and the Directorate-General for European Neighbourhood and Enlargement Negotiations [DG_NEAR] through regional development programmes: EUMEDCONNECT (North Africa and the Eastern Mediterranean), ALICE (Latin America), TEIN and Asi@Connect (Asia-Pacific), CAREN (Central Asia). Current projects are AfricaConnect3 [AfricaConnect3] and Asi@Connect [Asi@Connect] as well as the GN5-IC1 project which will plan and implement the first phase of a new intercontinental connectivity investment programme to further support the European R&E community [GN5-IC1].

2. NREN ORGANISATIONS

This section of the Compendium Report considers the NRENs as organisations, looking at their annual budgets, funding sources, governance structures and staffing[6].

2.1. Budget

Budgets play a pivotal role in determining an organisation's capacity, which means NREN budget figures are a significant part of the NREN story. In general, budgets allocated to NREN activities have demonstrated a significant increase over the last half-decade, as illustrated in Figure 2.1 (17 NRENs reported an increase in budget)[7]. Of course, this trend does not necessarily hold true for every NREN, as demonstrated by the variation in the 2021 and 2022 budgets of individual NRENs, as depicted in Figure 2.2. A look at individual NRENs reveals changes in the budgets that in some cases go well beyond the average fluctuations. These changes go in both directions and are most often related to projects or infrastructure investments. Certain budgetary increases may also be attributed to accounting changes.

The increase in the combined budgets of Europe's NRENs over the years can be seen as part of the overall investment in research and education infrastructure across the continent. An individual NREN's budget, however, is much more context-dependent, and is part of the story of national circumstances[8]. The roles national NRENs play vary considerably, which is reflected in their budgets.

[6] The data used in this section are mostly taken from the annual Compendium survey of NRENs. Some data come from the World Bank [World Bank].

[7] Some NRENs had single-year gaps in their records (LAT, Sikt, RoEduNet, SURF). To create Figure 2.1, these gaps were filled by extrapolating the missing budgets from those before and after the gap (LAT, Sikt, RoEduNet). For SURF, numbers from SURF's 2-year plan were used.

[8] Some NRENs, such as GRNET, have massively expanded their service portfolio over the years. Others, such as CESNET, have widened their remit, but are now part of a collaboration with other legal entities, an example of the alignment of national e-infrastructures that has taken place in a number of countries (e.g. in Estonia, Norway and the Netherlands, where comparable reorganisations are currently happening). In the Netherlands, the merger of SURFnet (the original NREN) with SURFsara (HPC) and SURFmarket (ICT marketplace) has created SURF, an organisation with a budget of €230 M (SURFnet in 2020 had a budget of €54 M).

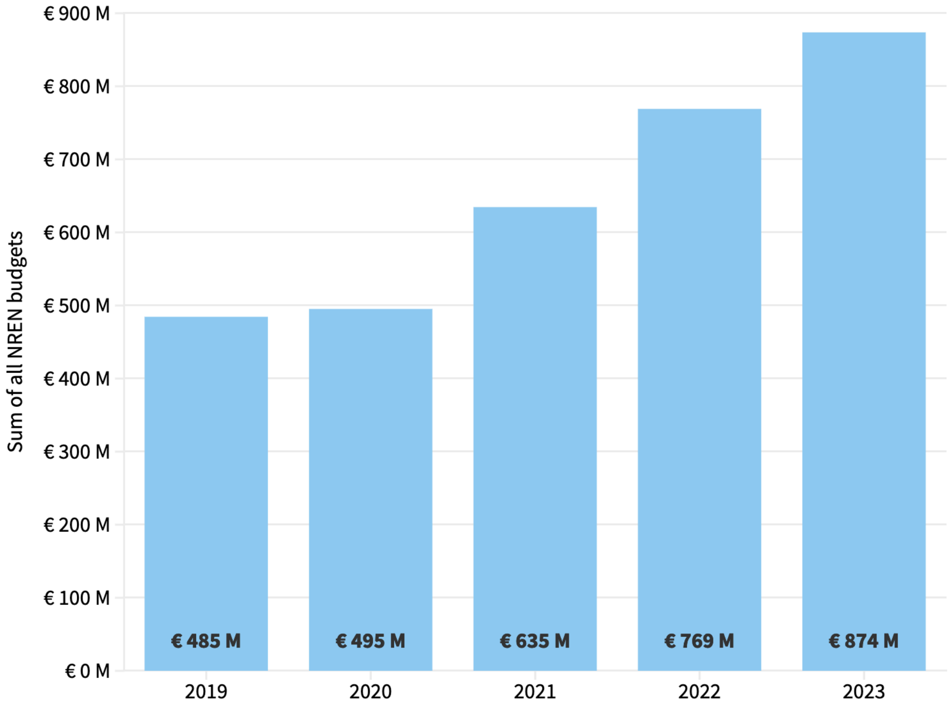


Figure 2.1: Development of total NREN budgets since 2019. *Over this time, NREN budgets have increased considerably. However, this increase spreads very unevenly across the individual NRENs and the reasons for the increase differ. For example, the increase 2020/2021 was dominated by CARNET's budget: the Croatian NREN received project money of €80 Million, accounting for a third of that year's increase. Even more extreme was the increase in 2021/2022, which was almost entirely due to the Dutch NREN SURF.*

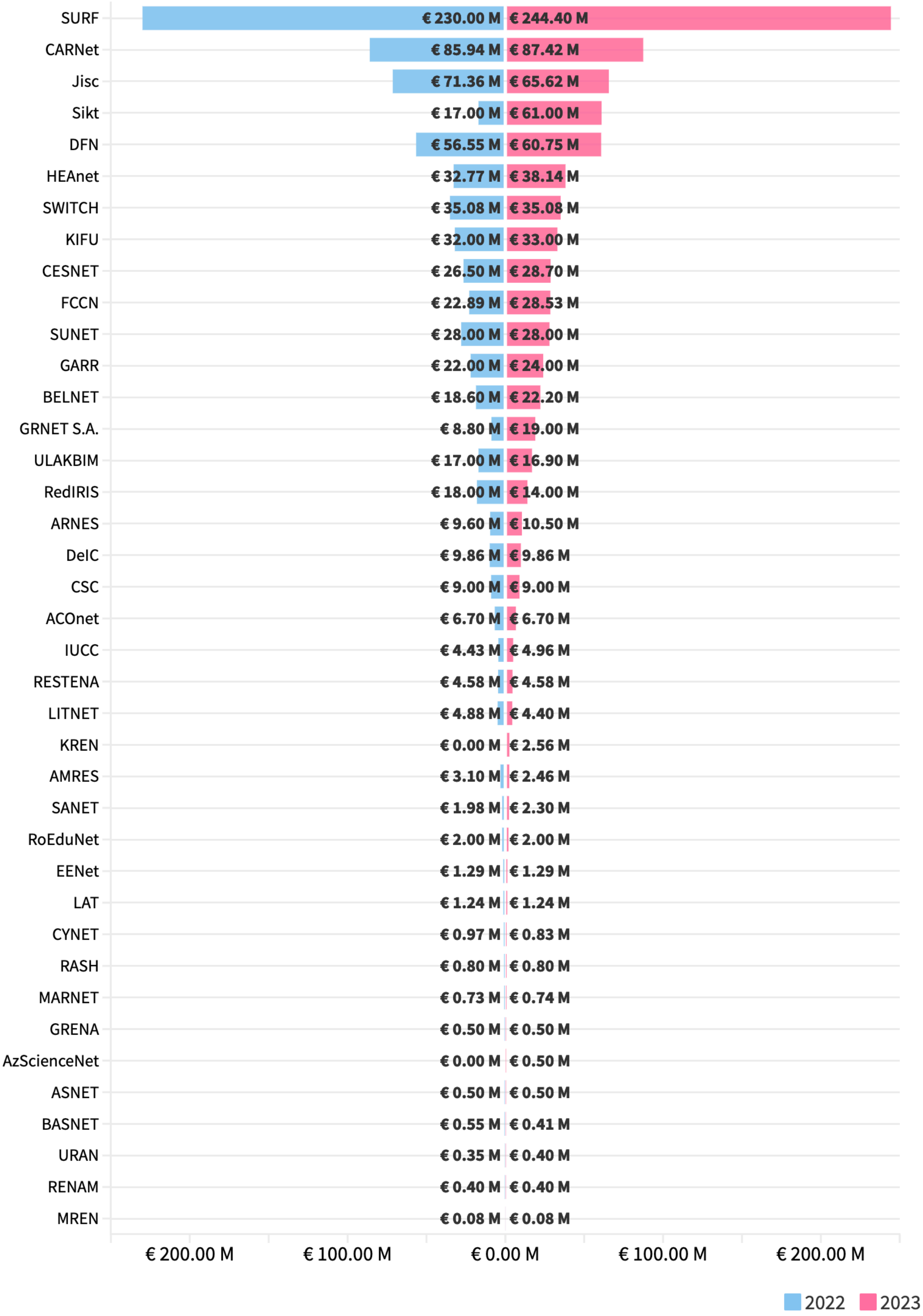


Figure 2.2: Individual NREN budgets 2022 and 2023. *The figure includes NRENs that have provided budget numbers for only one of these years, hence the occasional gap. Noticeable changes are Sikt's budget, which has grown from €17 Million to €61 Million, reflecting a reorganisation that merged several public IT organisations, and RedIRIS's budget dropping from €18 Million to €14 Million, a consequence of the end of project funding. Overall, 17 NRENs reported an increase in budget, 7 no change and 15 a reduced budget. One organisation (KREN) provided figures for the first time in the Compendium. Note that SURF's bar has been cut for visual clarity reasons.*

Budgets reflect the size of an NREN, but this size is, of course, also related to the size of its home country. Large countries have more R&E institutions, and therefore larger NRENs in most instances. This can be seen in the budget list shown in Figure 2.2, where NRENs from larger countries tend to have larger budgets – although there are quite a few exceptions[9]. This becomes even clearer in Figure 2.3, which shows NREN budgets normalised to Gross Domestic Product (GDP) and population. In this case, the correlation between country size and NREN budget that is still visible in Figure 2.2 disappears. Figure 2.3 orders the NRENs by budget per GDP, which allows budgets to be compared based on the economic strength of countries (as reflected in the GDP). As an example, UK's Jisc, which has a large budget in absolute numbers, is average by this measure, while Hungary's KIFÜ, with less than half of Jisc's budget size, sits in second place among all the NRENs. This index reveals that some large RENs such as DFN, Jisc, GARR, RENATER, SWITCH or Belnet are fairly average or even "small" by this measure, while some smaller countries invest comparatively more in this sector – examples would be ARNES, CARNET and KIFÜ.

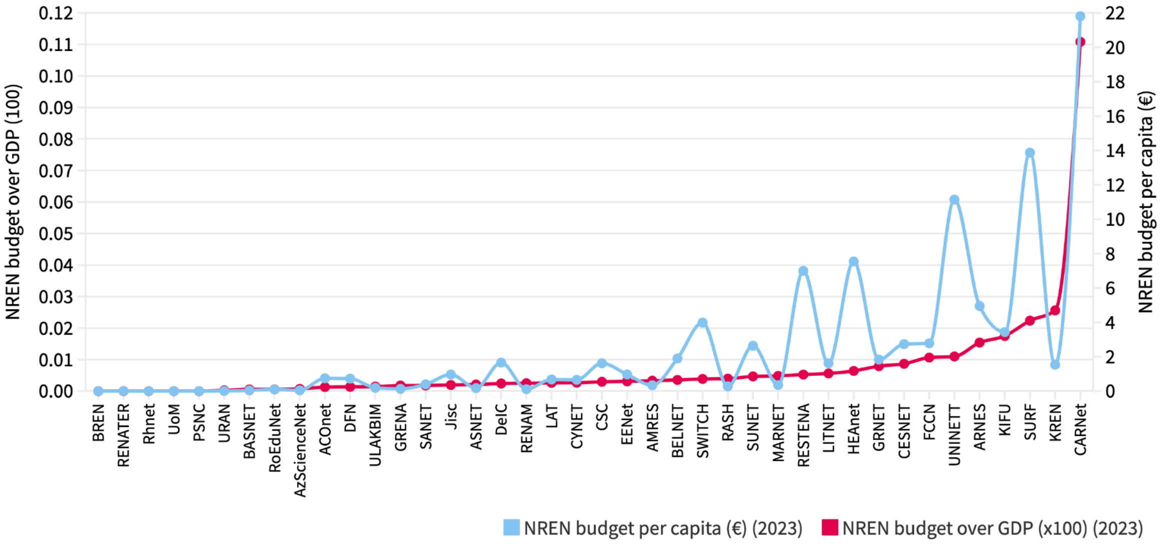


Figure 2.3: NREN budgets normalised to GDP and population. *The numbers shown here are simple indices formed by dividing the NRENs' budgets by the GDP (in Billion € x100) and population sizes. Both indices give a measure of national spending on research and education networks but are looking at different aspects. The NRENs are ordered by budget per GDP, allowing comparison based on the economic strength of countries. NREN budget per capita has a slightly different angle as it is normalised towards population size. The GDP and population numbers come from the International Monetary Fund (IMF) and the United Nations (UN), respectively.*

The data presented in Figure 2.3[10] is indicative of the significant differences observed between NRENs, attributable to a multitude of factors. Of particular relevance to this report is the observation that the business models of NRENs exhibit considerable variability, with some organisations expanding beyond their core function as an academic Internet Service Provider (ISP). NRENs occupying the top ranks in either budget over GDP or budget per capita tend to offer an extensive range of services beyond connectivity, such as procurement support,

[9] Note that the top ten budgets feature the NRENs of only two of the 10 largest European countries (ULAKBIM/Turkey, RedIRIS/Spain, RoEduNet/Romania and URAN/Ukraine are not in the top 10; RENATER/France would be in the top 10 as would be PSNC/Poland, but neither disclosed their budgets). NRENs from several significantly smaller countries, such as SWITCH (Switzerland), CARNET (Croatia), HEAnet (Ireland) and KIFÜ (Hungary), make the ranking instead.

[10] Clearly, this cannot all be captured by business data – the fundamental economic strength of a country plays a part here as well. Richer countries tend to spend more on public infrastructure, which NRENs are (in a wider sense) part of. This is at least partially visible in the population-normalised data, where NRENs from less wealthy countries tend to form the tail-end of the graph (Figure 2.3 NREN budgets normalised to GDP and population).

computational resources, and educational resources, among others. Furthermore, these organisations frequently extend their services to communities beyond the traditional scope of NRENs, necessitating additional funding (and human resources, as elaborated below)[11].

2.2. Funding Sources

The two main income sources for European NRENs are their customers and public funds (i.e. direct government money or money coming from public bodies). Both are logical income sources given the NREN's role as a public infrastructure. In addition, a smaller but still significant source is the European Commission – this money flows through a number of different projects in which many NRENs participate (see also Section 4 Involvement in EC-Funded Projects). Finally, some NRENs generate income by providing services to commercial partners. For the European NRENs, the importance of these four income sources is presented in Figure 2.4.

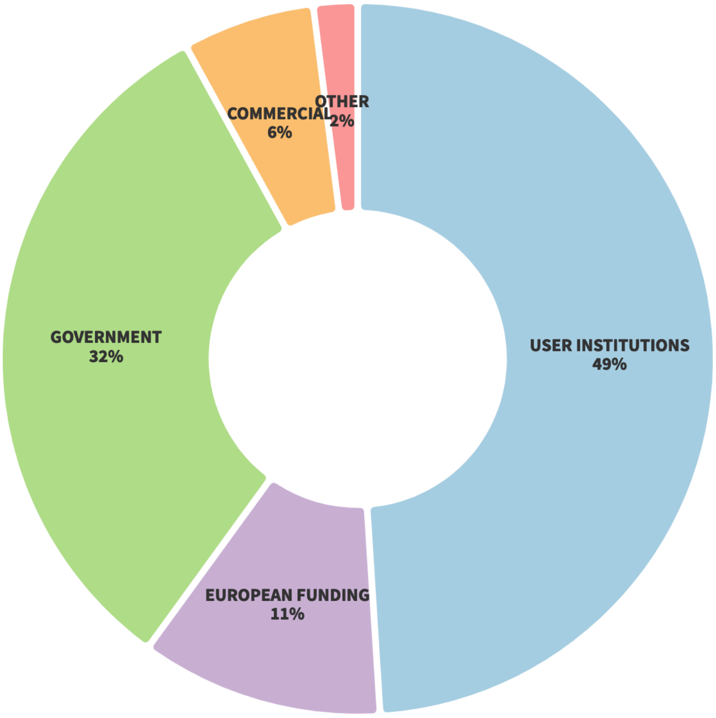


*Figure 2.4: **Funding sources of NRENs.** This figure shows the share of different funding sources for the combined total of European NRENs' budgets. Funding can come directly from the government (e.g. if the NREN is part of a ministry), from their user institutions (i.e. universities and other user institutions pay the NREN for its services) or from participation in EC-funded European projects. Some NRENs also have commercial income. Any funding that is not covered by these four categories appears under "Other". The numbers are based on the survey responses of the NRENs that provided their budget numbers as well as their income sources (39 NREN responses out of 44). The percentage was calculated based on the relative sizes of the individual NRENs' budgets compared with the sum of all budgets, i.e. NRENs were weighted according to their budget.*

Changes compared with 2022 have been limited: the share contributed by client institutions has increased from 45% to 49% while direct government funding has dropped slightly from 34% to 32%. The funding through European funds remained at 11%. While Figure 2.4 suggests that public money and money paid by the NRENs' customers are the financial mainstay, looking at individual NRENs reveals huge differences between them (shown in Table 2.1).

[11] Services that are made possible by a larger budget are provided for example by EENet and CARNET, which not only connect schools, but also provide educational resources; SURF and HEAnet, which maintain procurement schemes for their clients; and KIFÜ and ARNES, which also run HPC centres, etc.

	CLIENT INSTITUTIONS	EUROPEAN FUNDING	GOV/Public BODIES	COMMERCIAL	OTHER
ACOnet	100%				
AMRES			100%		
ARNES		5% (1%)	83% (87%)	12%	
ASNET-AM	10%	45%	43%		2%
AzScienceNet		20%	80%		
BASNET	49% (32%)	23% (51%)	28% (17%)		
Belnet	30% (45%)	8% (1%)	55% (49%)	5%	2% (0%)
CARNET		70% (71%)	25% (27%)	2% (2%)	3% (1%)
CESNET	16%	33% (30%)	42% (47%)	1% (2%)	8% (6%)
CSC	60%		40%		
CYNET	85% (70%)	15% (25%)	0% (5%)		
DeIC	96%	3%	1%		
DFN	87% (97%)	1% (1%)	0% (1%)	0% (1%)	12% (0%)
EENet		1%	99%		
FCCN	3% (3%)	3% (21%)	94% (76%)		
GARR	96% (90%)	4% (2%)	0% (8%)		
GRENA	45%	45%		5%	5%
GRNET		17% (26%)	83% (74%)		
HEAnet	11% (13%)		76% (78%)	7% (8%)	5% (1%)
IUCC	86% (89%)	2% (3%)	12% (8%)		
Jisc	21% (19%)		39% (50%)	40% (31%)	
KIFÜ	8%	2%	90%		
KREN		20%	80%		
LAT			100%		
LITNET		50% (40%)	50% (60%)		
MARnet		22%	25%	53%	
MREN		20%	70%	5% (0%)	5%
RASH	8%	2%	90%		
RedIRIS		42% (39%)	57% (60%)		1%
RENAM	24% (23%)	71% (70%)	1% (3%)	4%	
RESTENA	7%	2%	34%	40%	17%
RoEduNet			100%		
SANET	5% (7%)		95% (94%)		
Sikt	80% (82%)	2% (0%)	18%		
SUNET	70%		20%		10%
SURF	83% (76%)	2%	15% (0%)	0% (22%)	
SWITCH	56%			43%	
ULAKBIM	0% (94%)	3% (3%)	94% (0%)		3% (3%)
URAN	31% (35%)	42% (47%)		13% (16%)	14% (2%)

■ Over 75% ▨ 25% TO 75% □ LESS THAN 25%

Table 2.1: Income sources per NREN. *The table shows the percentage share of their income that individual NRENs derived from different sources. The numbers in parentheses are the income share in the previous year and are only shown when the share has changed between the years.*

The table also reveals that while the average distribution of income sources across all NRENs remained very stable, some NRENs showed larger shifts. The strongest shift is apparent at ULAKBIM, which is now almost entirely government-financed (94% compared with 0% the year before) while it used to be predominantly financed by its users. Not as dramatic but still noticeable were changes at SURF, where the commercial income dropped from 22% to 0%, and FCCN, where government income now covers 94% of the budget, compared with 76% in the year before.

The majority of NRENs have a diversified income, split to varying degrees over different categories. Despite the diversity apparent in these numbers, it is possible to distinguish different funding models. A useful categorisation can be formed based on the main funding source of the NREN being the government (government-subsidised), the NREN's users (user-financed) or a mixture of both. Figure 2.5 summarises how NRENs are distributed over these funding models.

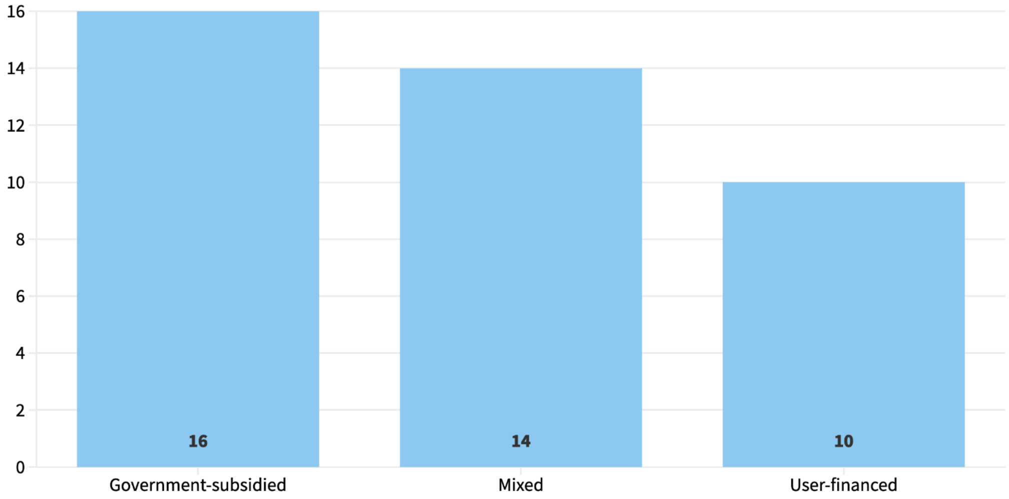


Figure 2.5: NREN funding models. *The boundaries between the categories rely on the ratio of user-derived revenue and government-derived revenue: Government-subsidised: <=1:9 ratio; User-financed: >= 9:1; Mixed funding models have ratios in between these two. 16 NRENs can be considered government-subsidised (AMRES, ARNES, AzScienceNet, CARNET, EENet, FCCN, GRNET, KIFÜ, LAT, MARnet, MREN, RedIRIS, RESTENA, RoEduNet, SANET, ULAKBIM) while 10 NRENs are mostly user-financed (ACOnet, DeIC, DFN, GARR, GRENA, IUCC, RENAM, RHnet, SWITCH, URAN). Mixed funding is used by 14 NRENs (ASNET-AM, Belnet, BREN, CESNET, CyNet, CSC/Funet, HEAnet, Jisc, LITNET, RASH, RENATER, SUNET, SURF, Sikt[12]). Due to lack of data, two NRENs cannot be assigned to a category (PSNC, UoM).*

The common appearance of European funds among the income sources reflects the strategic importance that the EC attaches to e-infrastructures, such as NRENs. This benefits NRENs in two ways: on the one hand the EC supports the development of such structures in its member countries but also in associated countries; on the other hand, NRENs are a natural source of expertise for e-infrastructures and are therefore involved in many European projects of this type. In many cases, money from the EC is an important funding source. This money, though, is connected to projects (see Section 4 Involvement in EC-Funded Projects) and therefore varies over the years.
As not-for-profit organisations, only a minority of NRENs (13 of 44) have a commercial income. A variety of activities are commercialised by NRENs[13] but most commercial income of NRENs

[12] In 2022, the Norwegian NREN Uninett merged with other public digital infrastructure bodies from the research data and higher education sectors to form Sikt, the Norwegian Agency for Shared Services in Education and Research. Both names appear in this report.

[13] URAN offers some commercial services (e.g. IP address block leasing) and the same is true for MREN and SWITCH,

comes from generic ISP activities that are provided by the NREN as part of their duties as a national IT infrastructure. Several NRENs are domain name registrars for national domain names[14] or run national Internet exchanges (IXs)[15].

2.3. Funding Model and Governance Structures

Both the role of users and the role of governments in the governance of NRENs can be mapped into categories. For the role of governments, the following five categories have been used: No representation (8 NRENs), Represented via public funding bodies (4 NRENs), Board representation (9 NRENs), Government-appointed board (7 NRENs) and Government agency (11 NRENs)[16].

The funding models correlate relatively well with the NRENs' governance structures: user-financed NRENs usually have a strong presence of their users (i.e. universities and research institutes) in their governance structures and little formal government oversight, while NRENs that rely very strongly on direct public money, not surprisingly, reveal usually strong government oversight. The correlation between government influence and funding model becomes apparent in Table 2.2 below.

		Government role in NREN governance				
		No government representation	Represented by public funding body	Board representation	Government-appointed board	Government agency
Funding model	User-financed	DeIC, DFN, GRENA, RHnet, URAN	GARR	ACOnet, IUCC, RENAM, SWITCH		
	Mixed funding	ASNET-AM, CESNET	Jisc, SUNET, SURF	BREN, HEAnet, RENATER	CyNet, CSC/ Funet, LITNET	Belnet, Sikt
	Government-subsidised	SANET		AMRES, RESTENA	ARNES, CARNET, GRNET, RedIRIS	AzScienceNet, EENet, FCCN, KIFÜ, LAT, MARnet, MREN, RoEduNet, ULAKBIM

Table 2.2: Funding models and formal government involvement in NREN governance. *Not too surprisingly, there is a slight correlation between government influence and funding model (see Figure 2.5 for details) – increasing government influence is correlated with government funding and vice versa. Some NRENs do not appear in the table as either their governance model (RASH) or their funding model (PSNC and UoM) have not been shared.*

both deriving income from domain name registries. MREN is in addition running an Internet exchange and SWITCH also provides ICT security to the Swiss banking sector.

[14] ACOnet, ARNES, Belnet, CARNET, DFN, EEnet, GARR, GRENA, GRNET, HEAnet, Jisc, KIFÜ, MARNET, MREN, RENAM, RENATER, RESTENA, SANET, Sikt, SURF, SWITCH, URAN register domain names though many of these NRENs limit this service to their traditional users and do not derive commercial income from it.

[15] ACOnet, ARNES, Belnet, CyNet, FCCN, GRNET, MARnet, MREN, PSNC/PIONIER, RASH and RESTENA run Internet exchanges, though not all of these are commercialised.

[16] Note that this categorisation focuses on the maximal extent of government influence (if any) – an NREN that is a government entity will likely have a government-dominated board, but the influence of the government arguably flows from the NREN being part of it in the first place. The same is true about the categories used to present the influence of user institutions.

Similarly, the role of users can be categorised into (with decreasing influence) Membership organisations (13 NRENs), Users present on the Board (15 NRENs) and No user representation (14 NRENs). While there are exceptions, there is a general trend that more government influence means less influence for user groups. This is also visible in Table 2.3, which plots the two stakeholder types against each other – as a rule of thumb, more user influence means less government influence and vice versa.

		Government role in NREN governance				
		No government representation	Represented by public funding body	Board representation	Government-appointed board	Government agency
User representation	Membership organisations	ASNET-AM, CESNET, DeIC, DFN, GRENA, RHnet, SANET, URAN	SURF	ACOnet, IUCC, SWITCH		AzScienceNet
	Users present on the Board	PSNC/ PIONIER	GARR, Jisc, SUNET	AMRES, BREN, HEAnet, RASH, RENAM, RENATER, RESTENA	CARNET, CSC/Funet, LITNET	MARnet
	No user representation	UoM			ARNES, CyNet, GRNET, RedIRIS	Belnet, EENet, FCCN, KIFÜ, LAT, MREN, RoEduNet, ULAKBIM, Sikt

Table 2.3: User representation vs. government representation in NREN governance structures. *NRENs as a public infrastructure have two main stakeholders: their users (with universities and research institutes at their core) and the government (often the main provider of the funding). This table looks at the representation of these two stakeholder groups within the NRENs' governance structures and finds that it varies widely.*

2.4. Staffing

The data presented in this section show the staff engaged in NREN activities in full-time equivalents (FTE).

Across the sector, staff numbers have increased between 2018 and 2023, as shown in Figure 2.6 – similarly to, and of course made possible by, budget increases. The total number of employees declared by NRENs in the 2023 Compendium survey reached 2,976.

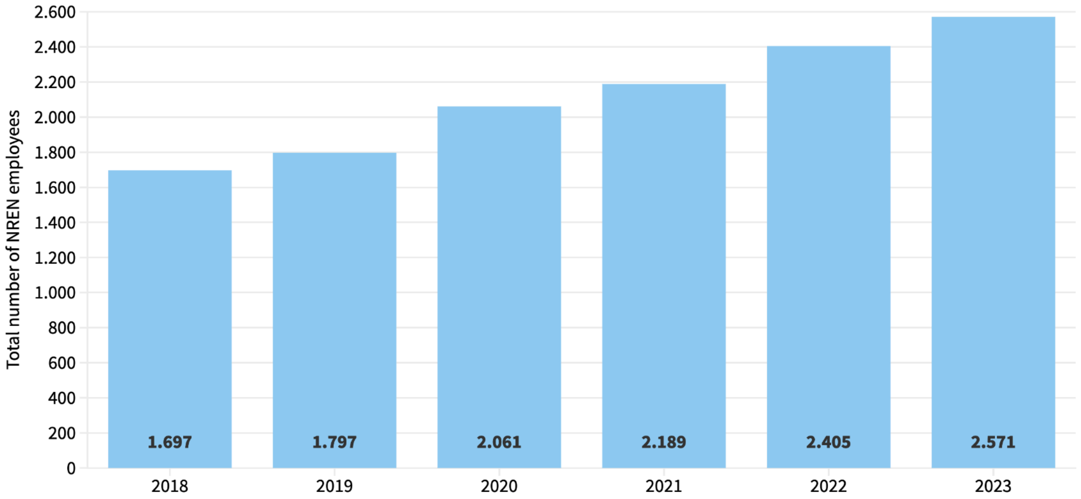


Figure 2.6: Total staff numbers of the NREN sector. *The percentage change is based on the earlier year's staff numbers. While the total number of staff reported in 2023 was 2,976, the data series shown in the graph is based on those NRENs that reported their staff numbers continuously throughout this period, which means that some NRENs are not included (see footnote 1 on p. 1).*

As with budget numbers, staff numbers vary considerably among NRENs, reflecting their differing sizes and the extent of the services they offer. The number of employees of individual NRENs in the years 2022 and 2023 is presented in Figure 2.7. While changes in employee numbers are apparent in these data, they are generally not as large as the swings in budget. This reflects the fact that most large budget changes are dedicated to transient projects (such as network infrastructure renewal), which are most often carried out with the help of contractors and therefore do not entail large changes in the headcount of the NREN. Of course, there are exceptions to this, usually correlated with organisational change[17].

The ratio of permanent employees to subcontracted employees varies markedly between NRENs. In many cases this reflects local circumstances, such as employment law, and business policies that are beyond the scope of this report. However, a common reason to employ subcontracted employees is the temporary availability of funds, usually project funds; examples for this would be CARNET and RedIRIS. The overall ratio between the two employment categories has seen little change over the years, with about 13% of subcontracted positions in 2017, 12% in 2018, 13% in 2019, 14% in 2020, 15% in 2021, 14% in 2022 and – a slight uptick – 18% in 2023. Whether the recent increase is more than a blip remains to be seen.

[17] Two obvious examples for this are SURF and Sikt, which have grown into huge organisations by NREN standards. In both cases, several IT-related organisations merged to form a larger organisation. In SURF's case these were SURFnet (NREN), SURFsara (HPC) and SURFmarket (ICT procurement), which merged in 2020; in Sikt's case these were Uninett (NREN), NSD (Norwegian Centre for Research Data), and Unit (Directorate for ICT and joint services in higher education and research), which merged in 2022. Such large e-infrastructures provide services well beyond the "traditional" role of NRENs as ISPs, which makes it a bit of a judgement call whether to count all employees as NREN employees. Examples of NRENs that have decided to count only the employees of the ISP part of their organisation are Jisc, with more than 1,000 employees, and CSC, which has more than 500 employees. In the Compendium survey, they provide much lower staff numbers: 77 for Jisc and 22 for CSC.

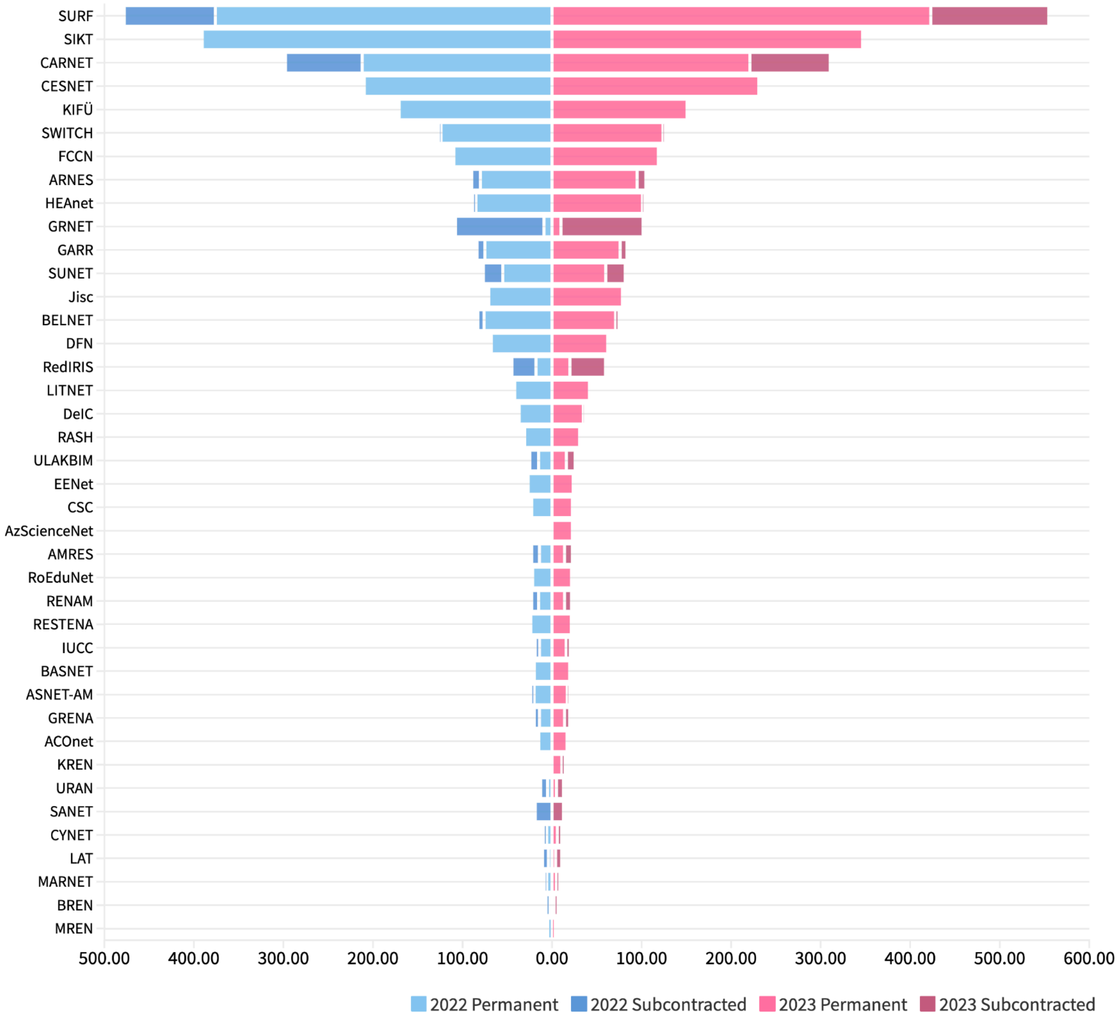


Figure 2.7: Staff numbers of NRENs in the years 2022 and 2023. *The figure includes NRENs that have provided staff numbers for only one of these years, hence the occasional gap.*

Figure 2.8 shows staff roles broken down into two broad categories: technical and non-technical roles. Not surprisingly for network providers, the majority of positions are technical roles[18]. Nevertheless, there is considerable variation between NRENs, which again emphasises how different NRENs are from each other.

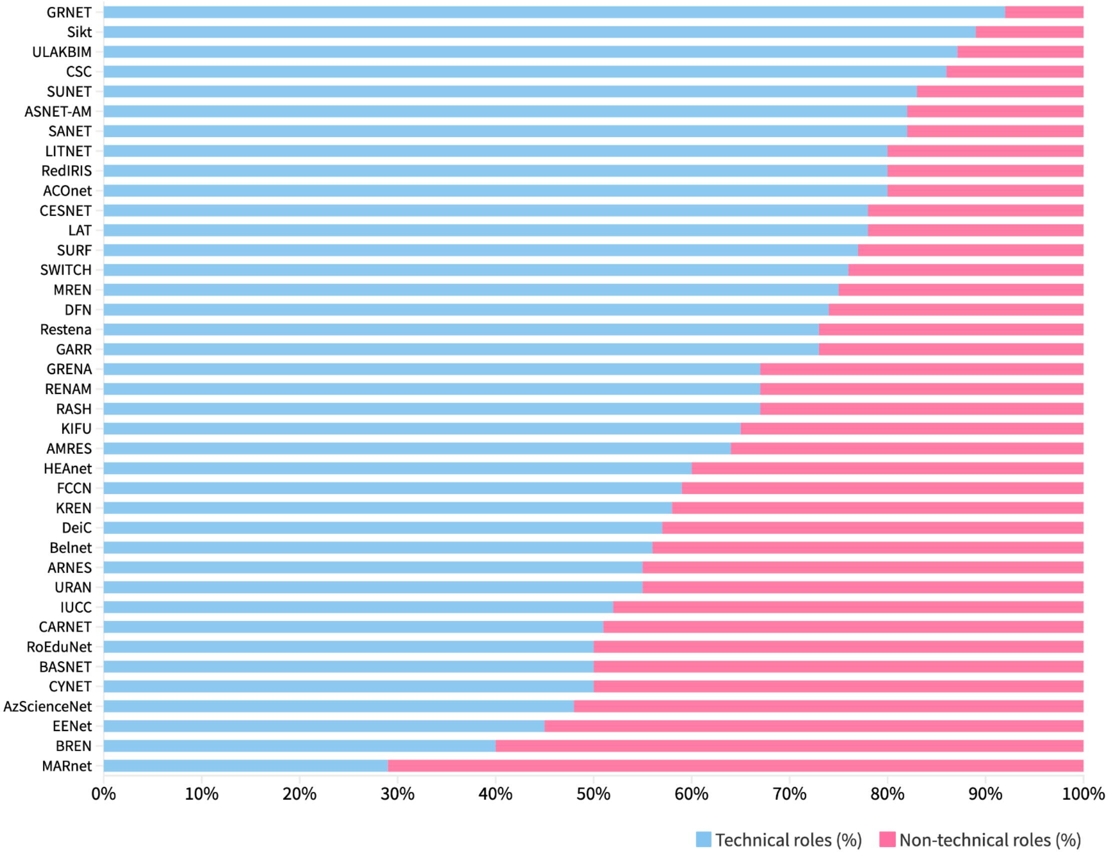


Figure 2.8: Share of technical roles among staff numbers. *For the purpose of this figure, non-technical roles are e.g. legal, finance, HR and PR, while technical roles would be network operation, software development or IT security.*

2.5. Summary

As in previous years, the NREN sector as a whole is showing growth in both funding and staffing. At first sight, this would seem to indicate that the general growth of ICT infrastructures includes the R&E sector in Europe as a whole. However, looking at the individual NRENs, the increase in funding is confined to very few NRENs, while for most NRENs incomes are flatlining.

Funding of what are essentially public infrastructures comes predominantly from public money, though through different channels: The financing is either directly by the government or via contributions from publicly funded customer institutions, i.e. mainly universities and research institutes, with project money being a third important source. All of these main funding channels eventually rely on taxpayer money. However, the relative importance of the first two tends to have a strong influence on the governance structure of NRENs. Direct

[18] At MARnet, the network management and operations roles sit within the university, hence the lack of technical staff.

government funding generally means a strong influence of government institutions, while funding through users generally means an important role of the user institutions in an NREN's governance.

The data presented in this section underscores the diversity of NRENs, not only in funding source, but also in size – reflected in staffing levels and budgets which exhibit significant variations, even when corrected for the size of the NREN's home country. This variability reflects the distinct set of responsibilities NRENs are entrusted with. This remit can change over time as technology evolves, the need of an NREN's user changes – or because strategic decisions expand (or shrink) an NREN's remit. The last decade has seen several examples of NRENs growing into more comprehensive roles, the last example being SURF, the Dutch NREN, which expanded its already large service portfolio considerably. Such "super-NRENs" exist in other countries as well and it could be considered a long-term trend.

3. END USERS

NRENs offer their services to a range of different user types. Research and higher education institutions (i.e. universities and research institutes) are the core end users of all NRENs. However, many NRENs provide connectivity and other services to a wider group of constituencies beyond this core "market". Generally, these are public institutions, including primary and secondary schools, libraries or government organisations. Under some circumstances, and in some countries, NRENs also offer their services to commercial organisations.

This section provides an overview of the NRENs' formal remit, including the users and organisations that they are authorised to connect, acceptable use policies (AUPs), current market shares among the institutions connected to each NREN, and link capacities provided to different types of connected institutions[19].

3.1. Connectivity Remit

NRENs have different funding structures, organisational setups and business models that define their scope and service offerings. An overview of the NRENs' connectivity remit is given in Figure 3.1.

All NRENs connect universities and research institutions. Most are permitted to connect institutes of further education, cultural institutions such as libraries and museums, and government bodies. About half of the NRENs can also connect schools. Only a minority of NRENs are permitted to connect commercial organisations, often only under certain circumstances, usually when the company in question is part of a collaborative project with an academic partner. Another common circumstance under which commercial organisations are connected is where the company is a start-up growing out of the research and education sector.

The remit of the NRENs can be quite dynamic. For example, several NRENs have taken on schools as part of their portfolio at some point, expanding their user base enormously, at least in terms of absolute user numbers. Reasons for changes in the connectivity remit vary. They can happen simply due to market forces, as most organisations choose their ISP autonomously, but as NRENs are part of the "public infrastructure", the more common reasons are a desire for better utilisation of that infrastructure, expansion of value-added services that are of interest to others, and the facilitation of public–private partnerships between publicly funded and commercial research facilities. A big factor here is also what type of organisation the NREN is: those that are closely connected to the government are more likely to be considered a public infrastructure and a resource of expertise that can be repurposed.

[19] To differentiate between different types of education institutions in a consistent way across different national education systems, this section follows the ISCED 2011 classification system (the UNESCO scheme for International Standard Classification of Education) [ISCED 2011].

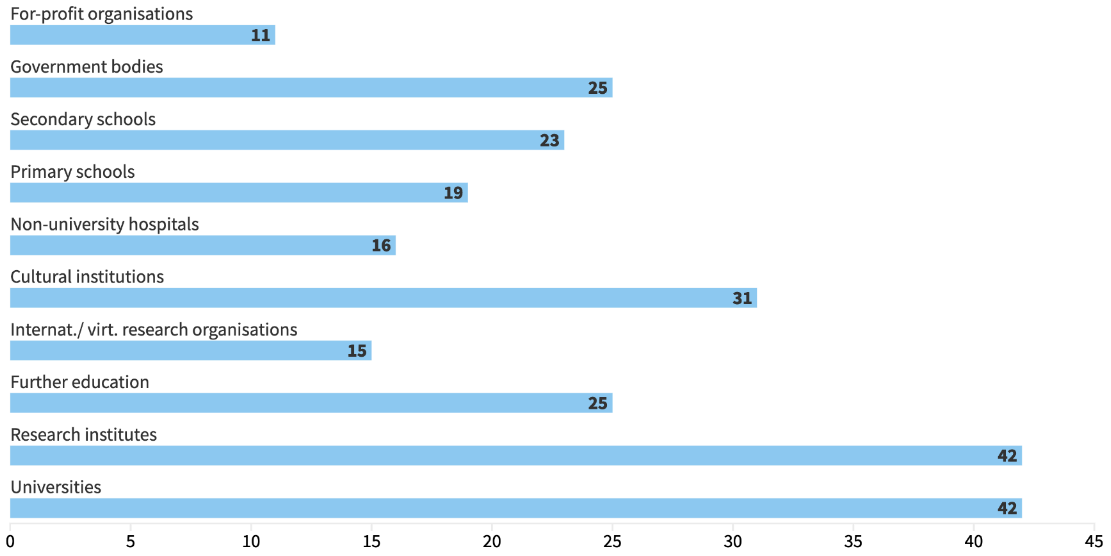


Figure 3.1: The number of NRENs connecting different user types. *While higher education and research are clearly the core of NREN activity, most NRENs also serve other user groups in the public space. Note that some user types are only served under certain circumstances by some NRENs: an example would be For-profit organisations – which most NRENs do not connect normally. Typical exceptions would be start-up companies that have grown out of the R&E sector or companies that are working in a common project with the R&E sector.*

3.2. NRENs' Acceptable Use Policy

The acceptable use policy (AUP) is a key element in defining the formal remit of NRENs in terms of which institutions they are eligible to connect. Most NRENs that responded to the Compendium survey have a formal AUP in place (see Figure 3.2).

An overview of acceptable use for each country, including a link to the AUP, can be found in the online version of the Compendium [Compendium] or is available on request from the Compendium team. (The AUP is also part of the organisational security requirements of NRENs and is therefore briefly discussed in Section 6 Security as well.)

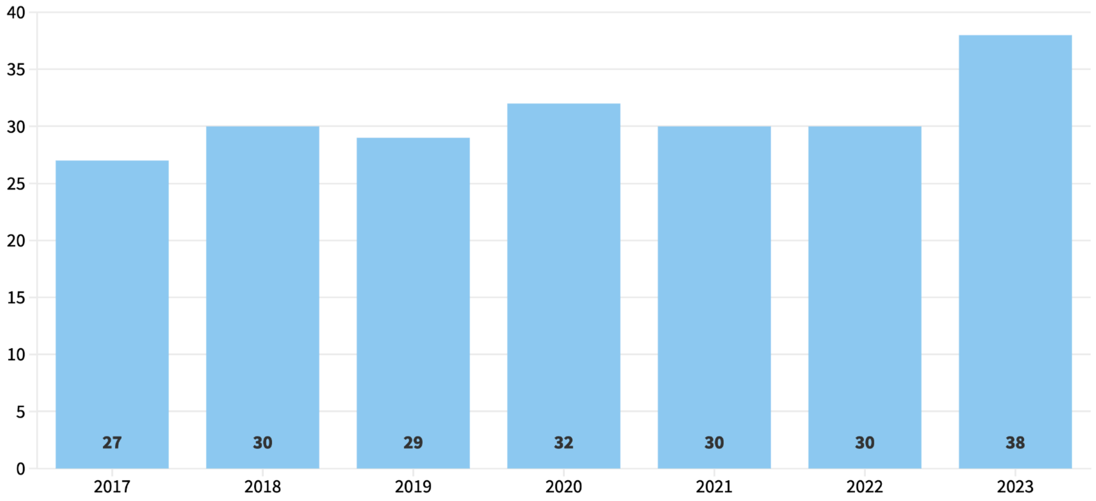


Figure 3.2: Number of NRENs that reported having an acceptable use policy (AUP) in place. *Overall, the number of NRENs with a formal AUP in place has increased, most likely reflecting the professionalisation of NRENs over time. The slight drop in the number of AUPs from 2018 to 2019 and from 2020 to 2021 is due to the varying response rate to the survey. Between 2017 and 2023, no NREN has reported having abandoned an existing AUP.*

3.3. Approximate Market Shares for Different Types of Institutions

An NREN's connectivity remit defines which institution types it may connect but not whether a given category of institutions actually makes up a sizeable part of its customer base[20]. To determine this, the Compendium survey asks NRENs to give an estimate of their market share for different user categories[21]. The estimated market shares per institution type, per NREN, are presented in Table 3.1.

The overall market share distribution in 2023 is comparable to that of 2022. In most countries, all, or a large majority of, universities and research institutions use the NREN for their connectivity needs. As expected, given the formal remit of the NRENs, these types of institutions represent the largest market share, with full or nearly full coverage across most NRENs[22]. Where schools fall into an NREN's remit, the NREN's market share is usually very high, and the same is true for institutions of further education. This is most often the case where NRENs are a directly state-funded "public infrastructure", which makes them a natural resource to turn to when ISP services are needed for public institutions. This is also reflected in the numbers: of the 16 NRENs that are (mostly) government-funded, 8 provide connectivity to a significant number of schools (market share of 40% or more) while of the 10 NRENs that receive no (direct) government-funding, only one (ACOnet) connects schools (see also Section 2 for a discussion of funding models).

Overall market shares are not very dynamic, and large jumps are rare; in most cases, noticeable changes take several years and the 2023 results are almost identical to those of 2022[23].

[20] The categories for the R&E sector (universities, schools, further education) use the ISCED definition (see the glossary entry on p. 108). The other categories refer to institutions that are not part of the university system. i.e. "Hospitals" would be non-university hospitals while "Government" refers to actual government departments (e.g. a ministry), not government-funded research institutions, which would appear under "Research Institutes".

[21] No commercial implications are intended by this term; it is used in the Compendium survey as a convenient shorthand.

[22] There are exceptions. URAN only connects about a third of the Ukrainian universities, and only 50% of Israel's universities are making use of IUCC's services.

[23] It is not always easy for NRENs to estimate their market share in a particular area, especially when large numbers of individual institutions are involved, e.g. schools or libraries. Sometimes, therefore, reassessing the market share with new methods can yield different results without a change in the situation on the ground.

	Universities	Research Ins.	Further Education	Inter'l research Inst	Libraries	Hospitals	Primary Schools	Secondary Schools	Government	For-Profit Orgs
ACOnet	85				40	60	90	90	60	
AMRES	80	80	90		50	3	97	97	2	
ARNES	100	93			87		97	100	10	
ASNET-AM	45	90			34					
AzScienceNet	33	35								
BELNET	90	75	1		1	5		5	20	
BREN	50	100								
CARNet	100	100	30		5	95	99	99	30	1
CESNET	95	97	7	90	3	25	2	6	11	
CYNET	95	70	40						15	
DeIC	100	25	33	50	10	60		1	5	1
EENet	94		65		8		13	50	15	
GARR	65	80		20	0.5	4.4	2.9	6.6		
GRENA	62	50								
GRNET S.A.	100	100	50		2	40	100	100	4	
HEAnet	100	50	100				98	100	1	
IUCC	50									
Jisc	100		100							
KIFU (NIIF)	80	95	95		10	5	94	97	1	
LITNET	90	100	80		15	10	17	51	9	
MARnet	100									
RASH	60	20			10				10	
RedIRIS	90							60		
RENAM	65	70	11		1	3		0.01	5	5
RENATER	100	100								
RoEduNet	95	80	50		60		60	70	10	
SANET	99	70	95		20	15	15	45	5	1
SUNET	100		100	20						
SURFnet	100	90	100		4	10	8	2		1
SWITCH	100				5					
ULAKBIM	87	10			0.1				2	

Over 75%	25% TO 75%	LESS THAN 25%

***Table 3.1: Estimated percentage market share per institution type, per NREN.** Not all NRENs gave an estimate of their market share; these are therefore missing from the table. Note also that market share differs from the connectivity remit of NRENs (Figure 3.1). For example, hypothetically, hospitals could be within the connectivity remit of an NREN, without any hospital being connected to the NRENs network.*

3.4. Typical and Highest Capacity of Connected Institutions

For most NRENs, users have to be connected to the NREN's backbone (see Section 3.5 for a discussion of carrier links, though). The capacity of these links is an important parameter as it determines the amount of data transfer they can support. The typical link capacity for connected institutions ranges from 1 Mbps up to 100 Gbps (Figure 3.3). Looking at both the typical (Figure 3.3) and the highest capacity links (Figure 3.4) provided to different types of institutions shows a pattern that reflects the needs of the respective institution categories. In general, universities and research institutions are provided with the high-capacity links needed to meet their requirements, whereas schools have lower-capacity links.

While these findings are not surprising, it is interesting to look at the development across the last few years. Both figures juxtapose typical and highest capacity links from 2020 and 2023 and for all user categories. The share of high-capacity links (500–1,500 Mbps and >1,500 Mbps) has increased while the share of low-capacity links (<500 Mbps) has decreased. Clearly, many NRENs have upgraded their offers.

Interestingly, the rates at which traffic increases are considerably higher than the pace at which link capacities increase (for details, see Section 5 Network). Fast traffic growth has of course been a constant for years, the COVID-19 period excepted (nicely illustrated by the traffic in GÉANTs network (see Section 5.9.1.2) and also in earlier Compendia) and to accommodate this, networks have a significant overcapacity when they are designed.

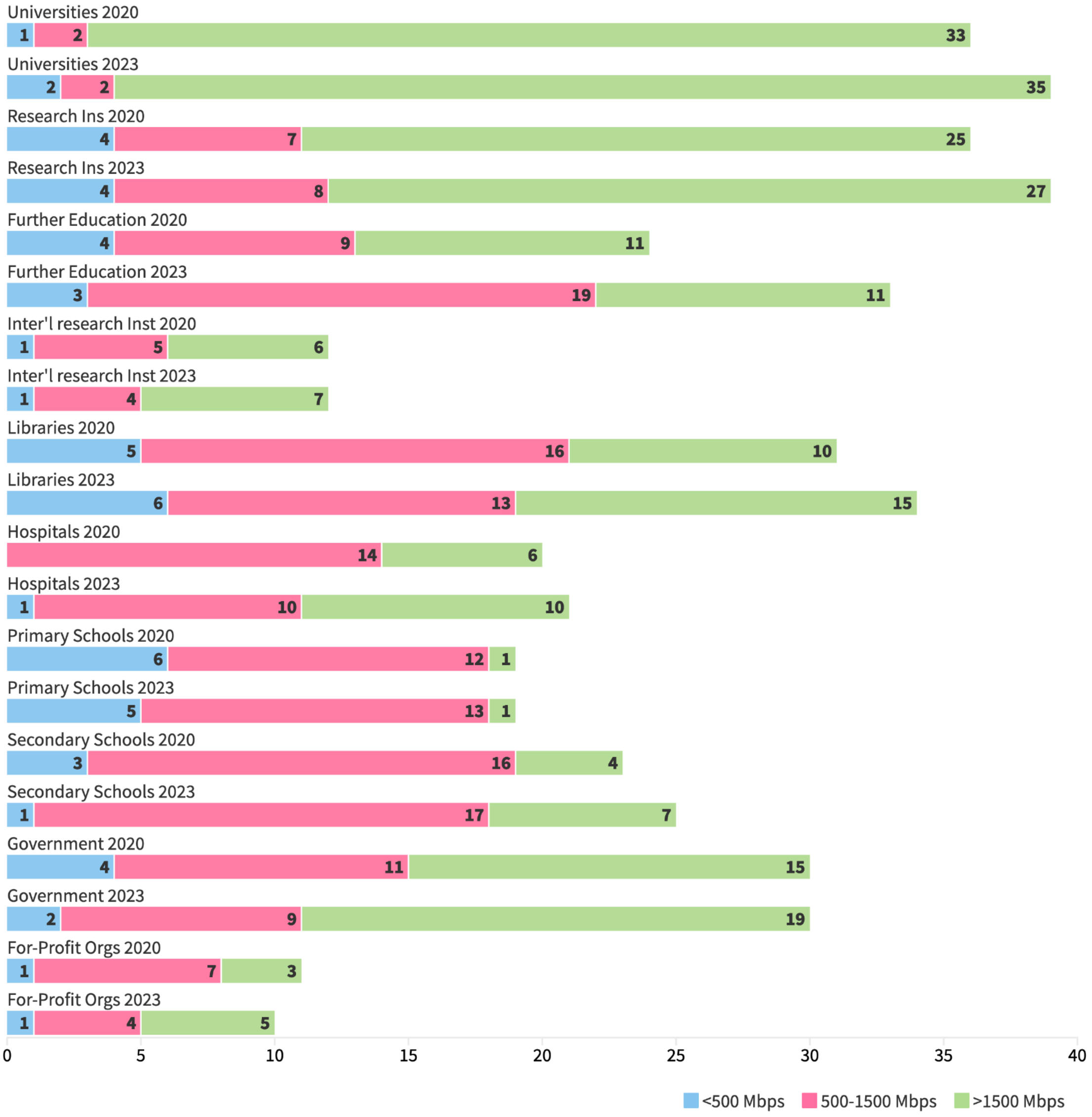


Figure 3.3: Typical link capacities provided by NRENs to different types of connected institutions in 2020 and 2023. *Link capacities have been grouped into three capacity categories: less than 500 Mbps, 500–1,500 Mbps, and beyond 1,500 Mbps. Most NRENs typically provide their core users (universities and research institutes) with high-capacity links, reflecting the capacity needs of these institutions. Other user groups (e.g. libraries or schools) are on average provided with lower-capacity links which will often reflect lower needs; in addition, schools are often not connected by the NREN itself but via commercial links (see Section 3.5). The comparison between 2020 and 2023 also illustrates the overall increase in link capacity.*

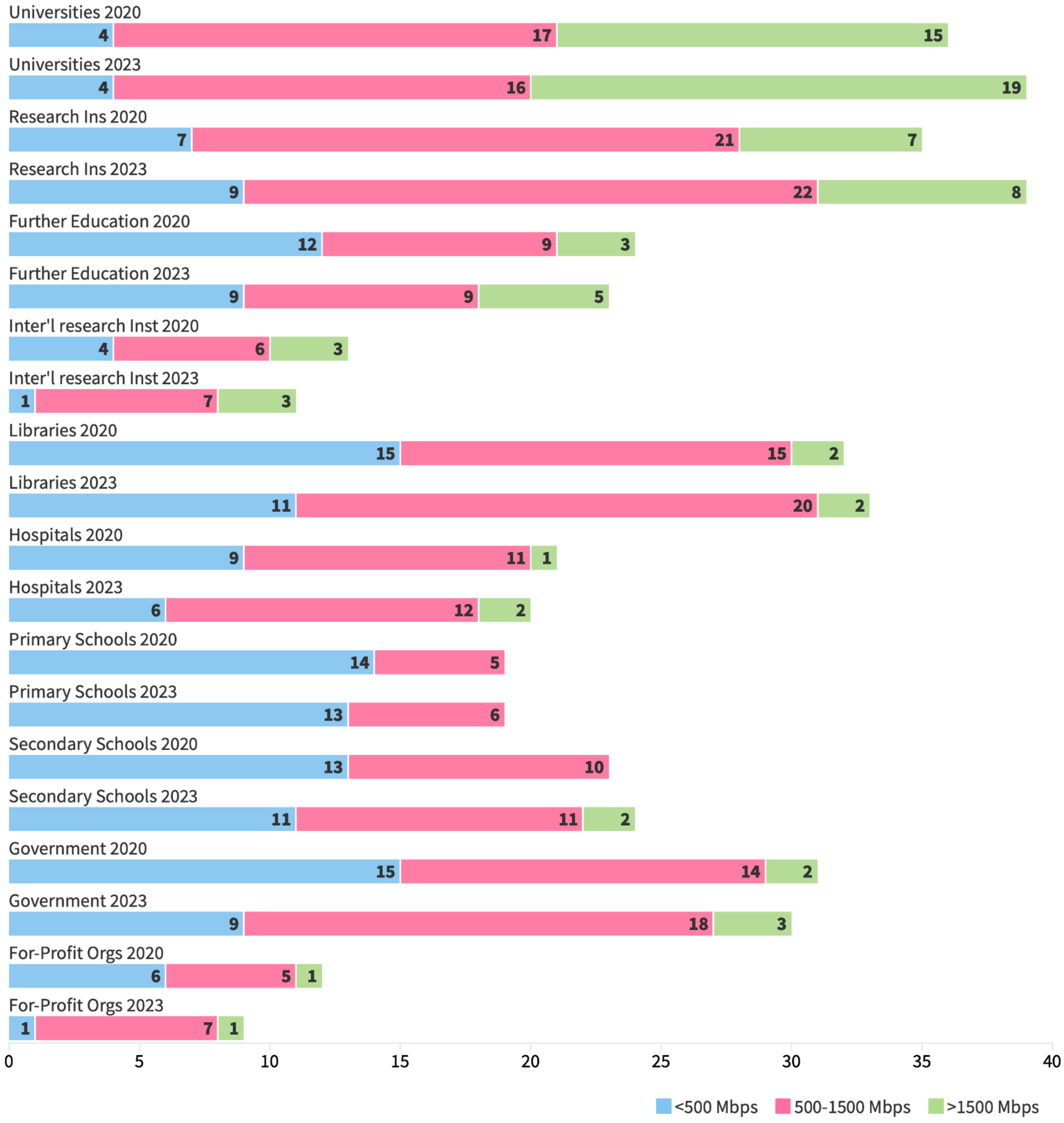
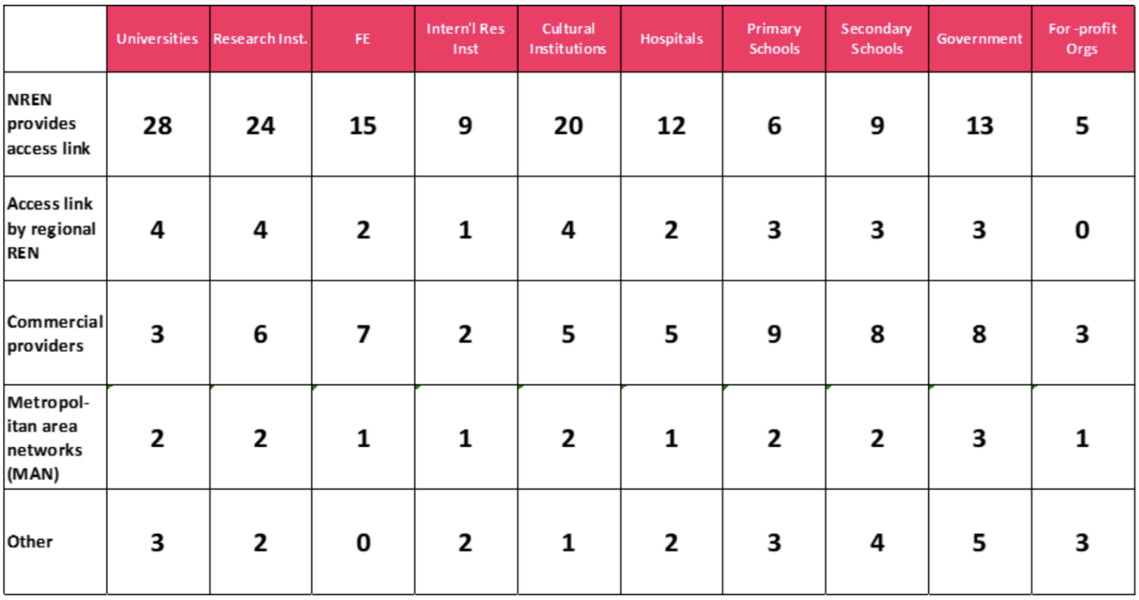


Figure 3.4: Highest link capacities provided by NRENs to different types of connected institutions in 2020 and 2023. *Link capacities have been grouped into three capacity categories: less than 500 Mbps, 500–1,500 Mbps, and beyond 1,500 Mbps.*

3.5. Access Link Carriers

As access links are a crucial piece of infrastructure, it is interesting to look at how NRENs provide them for their users. There are two main options: an NREN can provide the necessary link directly or rely on a third party for this service.

The third party can be a commercial provider (which often means that the users have to pay for the link) or the role can be fulfilled by local networks (e.g. local or regional research and education networks (RRENs) or metropolitan area networks (MANs) (Table 3.2). Looking at the numbers, most NRENs provide the access links for their users themselves or through local providers (the exception to the rule being schools – see below), while commercial access links are used by only a few NRENs (up to 7 NRENs, depending on the user type, excluding schools). NRENs tend to apply the same method to provide access links regardless of the user type (again with the notable exception of schools), so most of the variation between different user types in Table 3.2 arises from the fact that not all NRENs connect all user types.



	Universities	Research Inst.	FE	Intern'l Res Inst	Cultural Institutions	Hospitals	Primary Schools	Secondary Schools	Government	For -profit Orgs
NREN provides access link	28	24	15	9	20	12	6	9	13	5
Access link by regional REN	4	4	2	1	4	2	3	3	3	0
Commercial providers	3	6	7	2	5	5	9	8	8	3
Metropol-itan area networks (MAN)	2	2	1	1	2	1	2	2	3	1
Other	3	2	0	2	1	2	3	4	5	3

Table 3.2: How NRENs provide access links to their users-number of NRENs per method and user type. *Schools excepted, NRENs tend to be consistent across their user spectrum when it comes to the carrier types. Regarding schools, a majority of NRENs opt for commercial traffic carriers to provide the access links, a reversal of the situation seen among the other user types. Note that not all NRENs connect all user types. Note also that some NRENs have not provided this information and are therefore not present in this table (BREN, LAT, RHnet, UoM).*

Among the NRENs that use different methods to connect different users, most provide the access links to universities themselves (RENAM, ULAKBIM) while using commercial providers to connect the rest (ACOnet, CESNET, LITNET, RENAM, RoEduNet, SWITCH, ULAKBIM). Belnet uses a MAN for all institutions within the Brussels area and PSNC/PIONIER uses MANs for all their links.

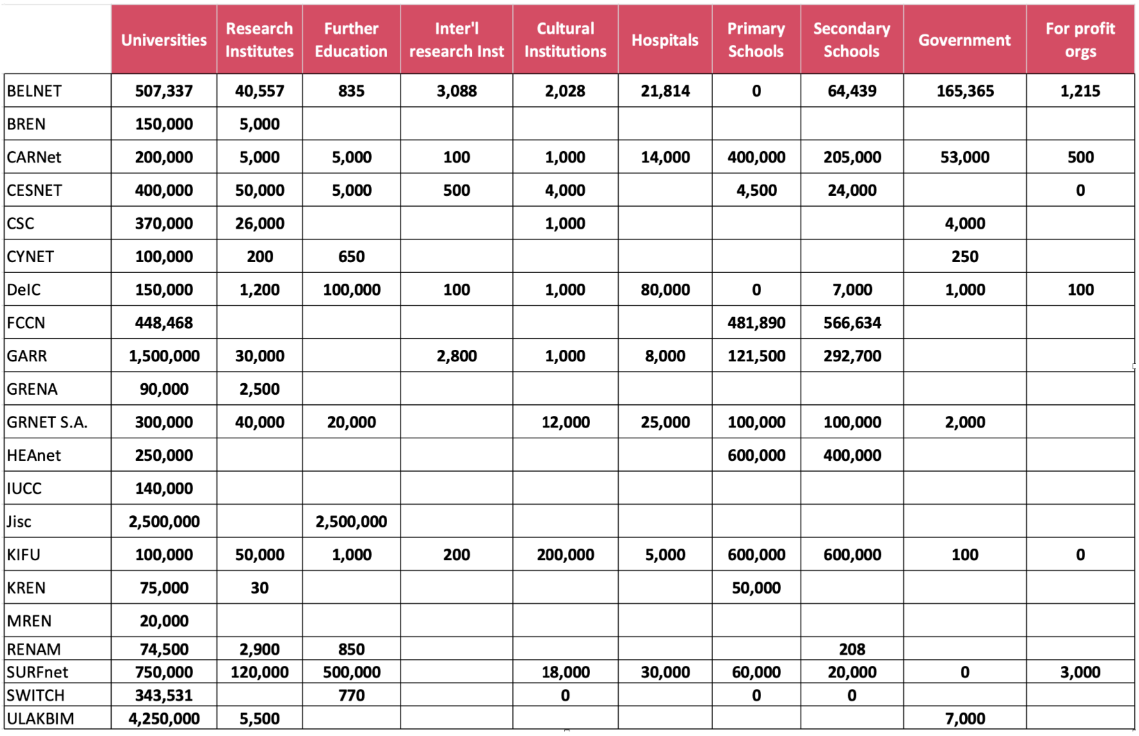
As mentioned above, schools are an exception to both of these rules of thumb. Here, the majority of NRENs use commercial providers to provide access links and only a minority provide the access links themselves. This of course reflects the huge difference in numbers between schools and any other user type: while universities – even in large countries – are counted in the hundreds, school numbers are about two orders of magnitude above that.

3.6. User Numbers

While NRENs provide their services to institutions, not to individual users, the question of how many individual users are actually making use of an NREN's network and other services is nonetheless important. Because their relationship to the end users is indirect, NRENs cannot in all cases easily or reliably answer this question. However, some NRENs provided estimates of how many people use their networks via the different institutions the NRENs serve (Table 3.3).

In addition, using publicly available data, it is possible to estimate user numbers across all NRENs. Combining the number of students per country and the estimated market share of

NRENs among their user categories, the number of end users of NREN networks and services in Europe amounts to about 40 million users[24].



	Universities	Research Institutes	Further Education	Inter'l research Inst	Cultural Institutions	Hospitals	Primary Schools	Secondary Schools	Government	For profit orgs
BELNET	507,337	40,557	835	3,088	2,028	21,814	0	64,439	165,365	1,215
BREN	150,000	5,000								
CARNet	200,000	5,000	5,000	100	1,000	14,000	400,000	205,000	53,000	500
CESNET	400,000	50,000	5,000	500	4,000		4,500	24,000		0
CSC	370,000	26,000			1,000				4,000	
CYNET	100,000	200	650						250	
DeIC	150,000	1,200	100,000	100	1,000	80,000	0	7,000	1,000	100
FCCN	448,468						481,890	566,634		
GARR	1,500,000	30,000		2,800	1,000	8,000	121,500	292,700		
GRENA	90,000	2,500								
GRNET S.A.	300,000	40,000	20,000		12,000	25,000	100,000	100,000	2,000	
HEAnet	250,000						600,000	400,000		
IUCC	140,000									
Jisc	2,500,000		2,500,000							
KIFU	100,000	50,000	1,000	200	200,000	5,000	600,000	600,000	100	0
KREN	75,000	30					50,000			
MREN	20,000									
RENAM	74,500	2,900	850					208		
SURFnet	750,000	120,000	500,000		18,000	30,000	60,000	20,000	0	3,000
SWITCH	343,531		770		0		0	0		
ULAKBIM	4,250,000	5,500							7,000	

Table 3.3: Estimates of the number of individual users per institution type. *While there are many gaps in the data that NRENs can provide about the number of end users, it is possible to estimate the number of end users using the market share estimates provided by NRENs (Table 3.1) and the number of students in Europe in schools and universities, as these make up by far the largest user group in terms of headcount. A smaller, but still significant contribution comes from the staff of universities and schools.*

3.7. Digital Health

While the remit of NRENs and therefore their user categories rarely change, there are current developments in the health sector that could see NRENs (or at least some of them) taking on additional roles in the health sector. Currently, European NRENs are supporting the national and international Digital Health community at various levels, and with different degrees of involvement, thus providing a very heterogeneous landscape within the GÉANT community in relation to engaging with the health community.

Health community support ranges from advanced involvement by the NREN, providing tailored storage services, specific cloud computing services, or cloud-based authentication

[24] The formula used is the following: market share (schools, universities, FE sector) x student numbers (schools, universities, FE sector) x 1.08 (staff-student ratio factor).
The student numbers for European countries are based on publicly available Eurostat and UNESCO sources. The staff-student ratio is equally based on publicly available data from the same sources. The ratio varies considerably between countries, so the number of 12.5 is based on the Eurostat estimate for the average across the 28 EU states (2018). Where NRENs have not provided an estimate of their market share (with DFN and PSNC/PIONIER, this includes two NRENs from countries with large student populations), a market share for universities of 80% has been assumed (possibly an underestimate) and a 0% market share for schools (which is true for DFN but not entirely true for PSNC/PIONIER). Another assumption is that all other user groups (research institutes, hospitals, government bodies, etc.) have a much lower headcount compared with schools and universities, so adding them would not significantly change the estimate. That this assumption is plausible is also illustrated by the end-user estimates in Table 3.3.of individual institutions are involved, e.g. schools or libraries. Sometimes, therefore, reassessing the market share with new methods can yield different results without a change in the situation on the ground.

and authorisation infrastructure (AAI) solutions for Health, to a very minimal engagement with Health institutions or key Health initiatives and projects – or even no engagement at all. It is therefore challenging to define what common goals, challenges and ambitions could be pursued within the GÉANT NRENs in relation to the support to be provided to the Digital Health community.

Despite this heterogeneity of the Digital Health landscape, there are common interests among involved NRENs.

The first key common element is the great interest about the forthcoming EU regulations, and, specifically, the European Health Data Space (EHDS)[25]. The EU is working towards the definition of interoperable common European Data Spaces, including EHDS1 ("MyHealth@EU"), a continental e-infrastructure that regulates the access to personal health records for primary health care and for the provisioning of cross-border health services. The aim of this e-Infrastructure is to integrate patient medical records and electronic health record (EHR) systems, and to ensure that healthcare workflows involving physicians and patients can be implemented cross-border within the EU. While this infrastructure will possibly be based on a set of specific providers, many NRENs are interested in learning how to position themselves in relation to this upcoming e-infrastructure and the corresponding national health initiatives.

NRENs are likely to play a more substantial role in the implementation of the EHDS2 ("HealthData@EU") infrastructure, aimed at hosting, storing, and sharing (anonymised) Digital Health data for secondary use (research). Here NRENs are well positioned. In many cases they already interconnect major data centres, both nationally and internationally, and provide access to HPC centres involved in many Digital Health research projects, such as the Human Brain Project, the Digital Human Twins Project and forthcoming initiatives within the Destination Human roadmap addressed by the European Commission.

Many NRENs are also closely supporting initiatives related to Health and Life Sciences, such as EOSC-Life and ELIXIR, and their national nodes. In many cases, the support provided to these research infrastructures is tightly related to cloud computing and cloud storage services provided either directly by the NRENs, or by some of their stakeholder institutions. In 2023, several European NRENs went forward with their implementation of tailored services for Health, mainly in the areas of T&I and cloud storage. Examples for this would be RENATER, GARR and CESNET, which adapted their cloud-based Identity Providers to meet the needs of eHealth institutions. CESNET is also currently working on Sensitive Cloud for eHealth, in the context of their e-Infra CZ project. SURF is collaborating with Health-RI, a public-private partnership in health research and care, on the definition of their IT architecture and its implementation. SURF is also involved in Secure ANalysis Environment (SANE), a project to implement a Trusted Research Environment. Interest has also increased in the domain of Trusted Research Environments and Secure Processing Environments, as foreseen by the European Health Data Space (EHDS) regulation proposal.

AAI is another key area where NRENs are likely to provide crucial support to the eHealth sector. The currently adopted GÉANT community solutions (e.g. eduGAIN and the Core AAI Platform (formerly eduTEAMs)) on the one side and the new eIDAS 2.0 Regulation, together with the new EU Digital Identity (EUDI) Wallet initiative on the other, make it likely that NRENs will provide significant support to the Digital Health community.

[25] EHDS will be one of the official Data Spaces supported by EOSC, which will need to be interoperable with EOSC and the common EU Data Spaces framework for data, which will likely be based on the Simpl middleware currently being procured by the EC.

For this reason, NRENs have expressed the need for the GÉANT community to proactively track key initiatives and projects in this domain[26].

3.8. Summary

In general, NRENs dominate their core "market" of universities and research institutions while other user categories show a more varied picture, though changes are slow. This reflects the NRENs' function as a public infrastructure rather than a for-profit enterprise.

Despite its static appearance, change in the user base of NRENs can happen. Increases in the user base could come from expanding into additional areas of the public service sector, as happened some years ago when several NRENs started providing services to schools. There are other "natural" fields that could see an expansion of the NRENs' remit – "natural", because NRENs are already engaging such users (non-university hospitals, government bodies) or because of external developments. The latter might be happening with hospitals in response to European regulations on medical data exchange. Another development that could add new end users is the upcoming implementation of EuroHPC, (discussed in the next section, Section 4 Involvement in EC-Funded Projects).

[26] To assess the situation in this domain, the GÉANT Community Programme (GCP) eHealth Task Force (TF-eHealth) was established in July 2021. In 2023, the eHealth Task Force has been turned into an established, permanent Special Interest Group (SIG) under the GÉANT Community Programme, with a focus on the data aspects of eHealth, which are more closely related to the GÉANT community, and which will play a key role in the forthcoming implementation of the Common European Data Spaces (CEDS). The newly established SIG has been named SIG-DHD, Digital Health Data. SIG-DHD is working to keep the community informed about developments in the eHealth space but also works with other e-infrastructures to coordinate efforts in the eHealth space.

4. INVOLVEMENT IN EC-FUNDED PROJECTS

Many NRENs participate in several projects funded by the European Commission other than the GNx projects and/or play a crucial role in key European-level initiatives not strictly dealing with network connectivity. This section analyses those activities and draws conclusions based on the emerging trends[27]. The figures are taken from the responses to the Compendium survey but have also been validated by cross-checking with CORDIS, the European Commission's primary public repository and portal to disseminate information on all research projects funded by the European Union (EU)[28].

The data show that in 2023 29 individual NRENs participated in a total of 88 unique projects. This means that the number of participating NRENs has dropped somewhat compared with previous years (35 in 2021 and 2022). Equally, the number of projects has decreased compared with 2022, when 104 projects were recorded. Many of the projects are related to EOSC and Open Science, underlining the growing importance of above-the-net services to many NREN portfolios.

Figure 4.1 provides an overview of NREN involvement in EC-funded projects other than GN4-3/GN4-3N and GN5-1. The graph shows that many NRENs have multiple commitments to collaborations in international science. However, this also necessitates a level of resources that is not available to every NREN. It is also worth bearing in mind that most EC-funded projects are not fully funded by the EC and that the NREN needs to contribute a certain level of its own resources to participate. It is therefore no surprise that the NRENs that contribute to multiple EC-funded projects tend to be large and well-equipped, with a substantial budget, though the data also suggest a pattern that some smaller NRENs have an active strategy to participate in many projects. The consistently high level of engagement is therefore impressive.

The five NRENs involved in the most EC-funded projects are CSC/Funet, GRNET, PSNC/PIONIER, SURF and CESNET. Data derived from CORDIS also led to reporting projects for NORDUnet, an international collaboration representing the NRENs of the five Nordic countries, which does not ordinarily appear in the Compendium.

[27] This section looks at EC project involvement beyond the GN4-3/GN4-3N/GN5-1 projects, which include all European NRENs.

[28] Data were cross-checked for 78 projects, as well as for membership of the EOSC Association, since some respondents simply stated involvement in EOSC. This cross-checking revealed under-reporting of project participation in the Compendium survey in several cases. Initiatives have not been checked for NREN participation.

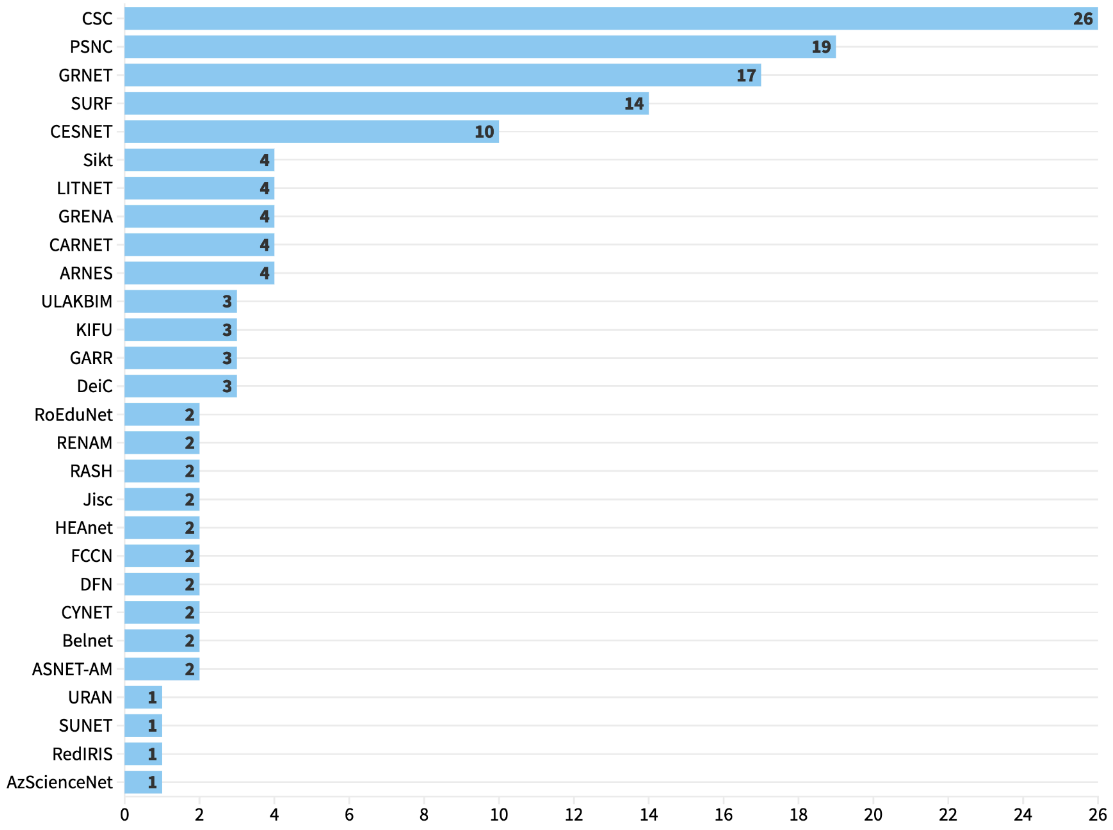


Figure 4.1: NRENs' participation in EC-funded projects other than GNx – total number of projects per NREN

4.1. Overview of Top EC-Funded Projects

This section gives a brief overview of the most popular EC-funded projects in terms of NREN participation. All these projects have multiple partners, i.e. the NRENs are by no means the only contributors to these projects. Several are EOSC-related (EOSC Future, EGI-ACE, DICE, NI4OS), while others address the network, regional collaborations or computing.

Project	No. of participating NRENs
EaPConnect 2	14
EOSC Future	11
NI4OS	7
SUBMERSE	6
EGI-ACE	5
DICE	4
FAIR IMPACT	4
Skills4EOSC	4
C-Scale	3
FAIRCORE4EOSC	3
GraspOS	3
EuroQCI	3

Table 4.1: Summary of the projects with most NREN participants. *The Compendium survey responses were cross-checked and supplemented with data from CORDIS.*

European Open Science Cloud (EOSC) Projects and Procurement Actions

The European Open Science Cloud (EOSC) is an EC-funded initiative to create a pan-European platform that acts as a web of Findable, Accessible, Interoperable and Reusable (FAIR) data and services for research. To accomplish its far-reaching goal, the EC has invested in a wide range of EOSC projects and procurement actions. Several of these have enlisted NRENs among their supporters.

An overview of projects in which NRENs participate is provided in Table 4.2. These projects receive EC funding through the Horizon Europe programme, under the INFRAEOSC calls or procurements.

Project	Project Profile	Main Focus	Contributing NRENs
EOSC Future [EOSC Future]	EOSC Future is an EU-funded H2020 project that is implementing the European Open Science Cloud (EOSC). EOSC will give European researchers access to a wide web of FAIR data and related services. EOSC Future runs from 1 April 2021 to 31 March 2024.	EOSC Exchange, AAI	CESNET, CSC/ Funet, DFN, GRNET, HEAnet, Jisc, KIFÜ, NORDUnet, PSNC/PIONIER,[31] SUNET, SURF, Sikt
FAIRCORE4EOSC [FAIRCORE4EOSC]	The FAIRCORE4EOSC project focuses on the development and realisation of nine core components for EOSC: EOSC Compliance Assessment Toolkit, EOSC Metadata Schema and Crosswalk Registry, EOSC Data Type Registry, EOSC PID Meta Resolver, EOSC Research Software APIs and Connectors, EOSC Software Heritage Mirror, EOSC Research Activity Identifier Service, EOSC PID Graph, EOSC Research Discovery Graph	EOSC Core, Metadata, PIDs, Knowledge Graphs	CSC/Funet, GRNET, SURF
FAIR-IMPACT [FAIR-IMPACT]	FAIR-IMPACT supports the implementation of FAIR-enabling practices, tools and services across scientific communities at a European, national and institutional level	FAIR practices and tools	CSC, DeIC, Sikt, SURF
EOSC Focus [EOSC Focus]	EOSC Focus is the CSA supporting the EOSC Association activities, in particular the preparation of EOSC post-2027	Support to EOSC Governance	Belnet, CSC
EuroScienceGateway [EuroScienceGateway]	EuroScienceGateway delivers a robust, scalable, seamlessly integrated open infrastructure for data-driven research, contributing an innovative and customisable service for EOSC that enables operational open and FAIR data and data processing, empowering European researchers to embrace the new digital age of science	Unified access to tools, workflows, storage and computing resources	CESNET, ULAKBIM
C-SCALE [C-SCALE]	C-SCALE disseminates Copernicus data, and offers tools, resources and services to make use of them to European researchers, institutions and initiatives	Copernicus data	CESNET, GRNET, SURF

Project	Project Profile	Main Focus	Contributing NRENs
Skills4EOSC [Skills4EOSC]	Skills4EOSC aims to create a training ecosystem for open and FAIR science to contribute to an EOSC-ready skilled European workforce, connecting existing Competence Centres in open science and scientific data management. The aim is to develop common methodologies, activities and training resources to unify the current training landscape into a collaborative and reliable ecosystem and to provide dedicated community-specific support to leverage the potential of EOSC for open and data-intensive research.	Competence Centres, curricula, training, skills	CSC, GARR, GRNET, PSNC
AI4EOSC [AI4EOSC]	The vision of the AI4EOSC project is to increase the service offer in the EU landscape by expanding the European Open Science Cloud (EOSC) ecosystem to support the effective utilisation of state-of-the-art AI techniques by the research community	AI	PSNC
Blue-Cloud 2026 [Blue-Cloud 2026]	Blue-Cloud 2026 aims at a further evolution of the Blue-Cloud results into a federated European ecosystem to deliver FAIR and open data and analytical services, instrumental for deepening research of oceans, EU seas, coastal and inland waters. It develops a thematic marine extension to EOSC for open web-based science, serving the needs of the EU Blue Economy, Marine Environment and Marine Knowledge agendas.	Data Federation, Marine Research	GRNET
AQUAINFRA [AQUAINFRA]	AQUAINFRA develops a virtual environment equipped with FAIR multi-disciplinary data and services to support marine and freshwater scientists and stakeholders restoring healthy oceans, seas, coastal and inland waters	Data Federation, Marine Research	CSC
GraspOS [GraspOS]	GraspOS aims to develop, assess and operate an open and trusted federated infrastructure for next-generation research metrics and indicators, offering data, tools, services and guidance	Infrastructure supporting Research Assessment	CSC, GRNET, ULAKBIM

Table 4.2: Overview of EOSC-connected projects and participating NRENs

In addition to the EOSC grants, NRENs are also playing a key role in the first EOSC-related procurement action: "Managed Services for the European Open Science Cloud Platform (EOSC)"[29].

[29] Ref. CNECT/LUX/2022/CD/0023 published under the Horizon Europe Research Infrastructures Work Programme 2022.

The purpose of European Open Science Cloud (EOSC) procurement is to build and deploy a fully operational enabling infrastructure for EOSC – referred to as the EOSC EU Node – providing access to a rich portfolio of FAIR data and professional-quality interoperable services in all relevant domains from data handling to computing, processing, analysis and storing.

The public tender for this procurement was organised in three lots for Core Federation Services (T&I), Exchange Infrastructure Services (network and computational resources), and Exchange Application Services (end-user applications). In all three areas, NRENs will provide important contributions[30].

EOSC Association

The EOSC Association is an umbrella organisation that was founded to coordinate the various EOSC initiatives and, as part of the tripartite collaboration with the EC and Member States, to provide a legal entity needed to maintain contractual arrangements to make the EOSC ecosystem sustainable[31]. A number of NRENs are active in the governance structures of the EOSC Association, as is GÉANT. GÉANT was also one of the founding members and in 2023 was represented on the Board of Directors, along with the Finnish NREN CSC/Funet. It is hoped that more NRENs will stand for Board positions in future years, given their engagement in EOSC initiatives. Nineteen NRENs (and GÉANT and NORDunet) are members of the EOSC Association: 18 NRENs are full members and one NREN has observer status. Eleven NRENs have been appointed as Mandated Organisations to represent their national interests. This is a significant proportion, given that there are only 29 Mandated Organisations in total, reflecting a recognition of their role as national service providers and representation of community interests. GÉANT and the NRENs are also well represented on the 13 EOSC Association Task Forces. Five of the 29 co-chairs[32] and 50 of the members come from the NREN community. Similarly, the NREN community is represented in 12 of the 13 Task Forces (all except Data Stewardship), with higher levels of participation in those Task Forces that are significant to NREN activities, as shown in Table 4.3.

[30] Core Federation Services: CESNET and GRNET, as well as GÉANT. Exchange Infrastructure Services: PSNC, NORDUnet and Sikt. The provider of the underlying network will be GÉANT. Exchange Application Services: PSNC, NORDUnet, SUNET and CESNET.

[31] The EOSC Association was founded in Brussels on 29 July 2020 as an international non-profit association (AISBL). It is composed of 133 Members and 87 Observers (figures accurate as of May 2023) representing research-performing organisations, service providers and funders. It. More information can be found at [EOSC].

[32] The EOSC Association Task Force co-chairs from the GÉANT community are Helen Clare of Jisc in the Upskilling Countries to Engage in EOSC Task Force, Christos Kanellopoulos of GÉANT in the AAI Architecture Task Force, Jan Meijer of Sikt in the Financial Sustainability Task Force, Themis Zamani of GRNET in the Persistent Identifier (PID) Policy and Implementation Task Force, and Raimundas Tuminauskas of PSNC in the Rules of Participation (RoP) Compliance Monitoring Task Force.

EOSC Association Task Force	No. of NRENs that are Task Force Members	Total No. of Task Force Members
AAI Architecture	11	34
Financial Sustainability	7	29
FAIR Metrics and Data Quality	3	26
Infrastructures for Quality Research Software	1	41
Long-term Data Preservation	5	36
PID Policy and Implementation	4	24
Research Careers, Recognition and Credit	1	27
Researcher Engagement and Adoption	4	42
Rules of Participation (RoP) Compliance Monitoring	3	22
Semantic Interoperability	3	44
Technical Interoperability of Data and Services	4	64
Upskilling Countries to Engage in EOSC	4	25

Table 4.3: Overview of GÉANT and NREN participation in EOSC Association Task Forces. *A detailed description of the remit of the Task Forces can be found at [EOSC_AG].*

EaPConnect2

Eastern Partnership Connect (EaPConnect) [EaPConnect] started its second iteration, EaPConnect2, in 2021, which aims to decrease the digital divide within Europe by establishing and operating a high-capacity broadband Internet network for R&E across five Eastern Partnership (EaP) partner countries in the EU's Eastern Neighbourhood: Armenia, Azerbaijan, Georgia, Moldova and Ukraine[33]. Part of the role of EaPConnect2 is to support the deployment of eduroam and to stimulate the integration of GÉANT services generally. The project will also facilitate the participation of local scientists, students and academics in global R&E collaborations.

EaPConnect2 partners – in addition to the NRENs of the now five partner countries (ASNET, AzScienceNet, GRENA, RENAM, URAN) – are DFN, GARR, GRNET, LITNET, PSNC/PIONIER, RoEduNet , who provide extra support and expertise.

EuroHPC JU

The European High Performance Computing Joint Undertaking (EuroHPC JU) [EuroHPC_JU] is a joint initiative between the EU and 34 member states and associated countries and private partners to develop a world-class supercomputing ecosystem in Europe. As a Joint Undertaking, the EuroHPC JU administers its own work plan and distributes funding accordingly. EuroHPC JU aims to deliver the supercomputing ecosystem for Europe, which includes the objective of hyperconnectivity (terabit connectivity) across all 27 EU Member States. Most recently a procurement was undertaken to federate the ecosystem (this includes a strong AAI component).

[33] BASNET, the Belarusian NREN, was suspended from the EaPConnect2 project in March 2022.

As the current provider of connectivity to all EuroHPC sites including quantum computers, GÉANT and the NRENs are well placed to understand and respond to changing requirements. NRENs are involved in the infrastructure advisory group (INFRAG) of EuroHPC (SURF, PSNC, CSC/Funet, ULAKBIM); additionally, three NRENs are also now running EuroHPC sites (GRNET, CSC and KIFÜ). Regular EuroHPC NREN coordination meetings are held between GÉANT and the NREN community to ensure that the community is well placed to meet both the current, and any future needs that the HPC community may have in the areas of secure connectivity, trust and identity or other priority areas.

4.2. Summary

NRENs across Europe are participating in a large number of EC-funded projects – including mainly scientifically oriented projects as well as societal programmes, which deal with health, education and regional development. These efforts continue the support that NRENs have provided to the R&E community for over 20 years.

In many cases this reflects that connectivity is an essential requirement for many projects and an NREN's core competency, making NRENs very useful project partners.

Other projects, in particular those around the European Open Science Cloud (EOSC) and the efforts around EuroHPC, aim to build a pan-European digital infrastructure which in many ways resembles services that many NRENs are offering their users "at home". This obviously makes NRENs compelling partners in these areas as a source of expertise – and often leverages their pre-existing infrastructure. At the same time, this also offers NRENs the opportunity to shape such pan-European infrastructures and to demonstrate their enduring relevance.

5. NETWORK

At the core of each NREN's work is its network; interconnecting users and making the delivery of services possible. Networks are not uniform; they are composed of a broad spectrum of infrastructure and communications technologies.

NREN networks, like the countries in which they reside, are unique and tailored to fit the community they serve, within the limits of the resources at their disposal. This section presents an overview of NREN network traffic, infrastructure, and services.

5.1. Network Traffic

This section considers the rate of growth of NREN traffic, and how the traffic type and destination have changed over time. Figure 5.1 shows the total amount of traffic into the NRENs from external networks (upper graph) and from NREN end users (lower graph) for 2020 to 2023. While these figures are only representative of a subset of NRENs, the developments visible in the graphs are indicative for all NRENs. Traffic in general has increased every year; this trend was interrupted by the COVID-19 pandemic but resumed thereafter.

Naturally, the absolute contributions to these figures differ considerably between NRENs, as can be seen in Figure 5.2. At the extremes are Jisc, with about 863,000 Tbytes of data from outside the NREN, and RASH, with just 26 Tbytes. The volume of traffic is driven by several factors, including the size of the country, the number of users, the capacity of their R&E infrastructure and geographic position, which makes some countries natural traffic hubs. Therefore, NRENs from large countries with high-capacity infrastructures such as Germany, France and the UK carry a lot of traffic, though clearly this is not the only factor here, as the order does not neatly follow country size.

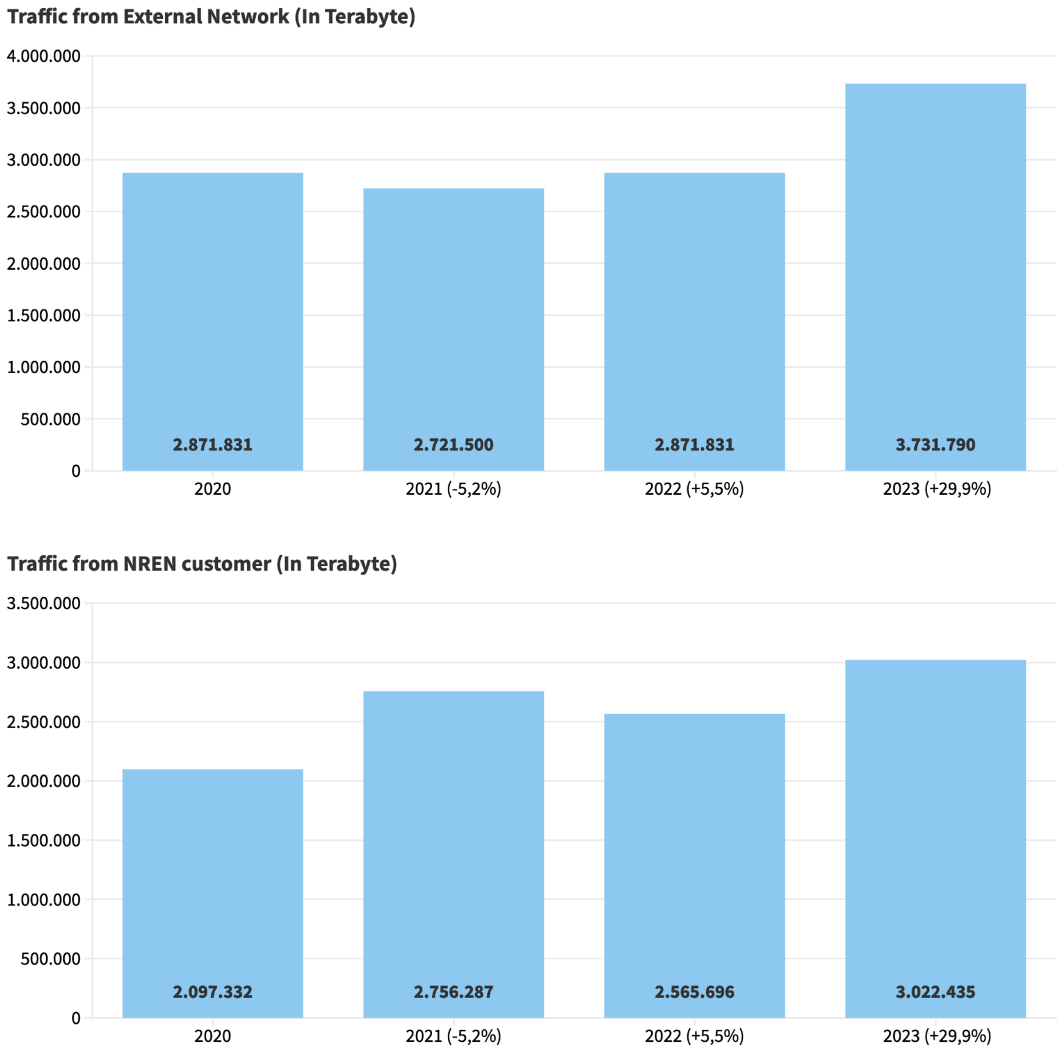


Figure 5.1: Increase of traffic into the NRENs from external networks (upper panel) and NREN customers (lower panel) 2020 to 2023. *"External network" denotes sources that are outside the NREN's domain, such as GÉANT, general/commercial Internet, Internet exchange, peerings, other NRENs. "NREN customer" (also referred to as end user) denotes sources that are part of the remit of an NREN's domain. The overall increase in traffic continues a long-standing trend – which was interrupted by the COVID-19 pandemic in 2020/2021 but has resumed since. The figures are based on traffic data from 21 NRENs for which there are continuous traffic records from 2020 to 2023 (Belnet, CARNET, CESNET, DeIC, DFN, FCCN, GARR, GRENA, GRNET, HEAnet, IUCC, Jisc, PIONIER, RASH, RedIRIS, RENAM, RENATER, RESTENA, SURF, SWITCH, ULAKBIM).*

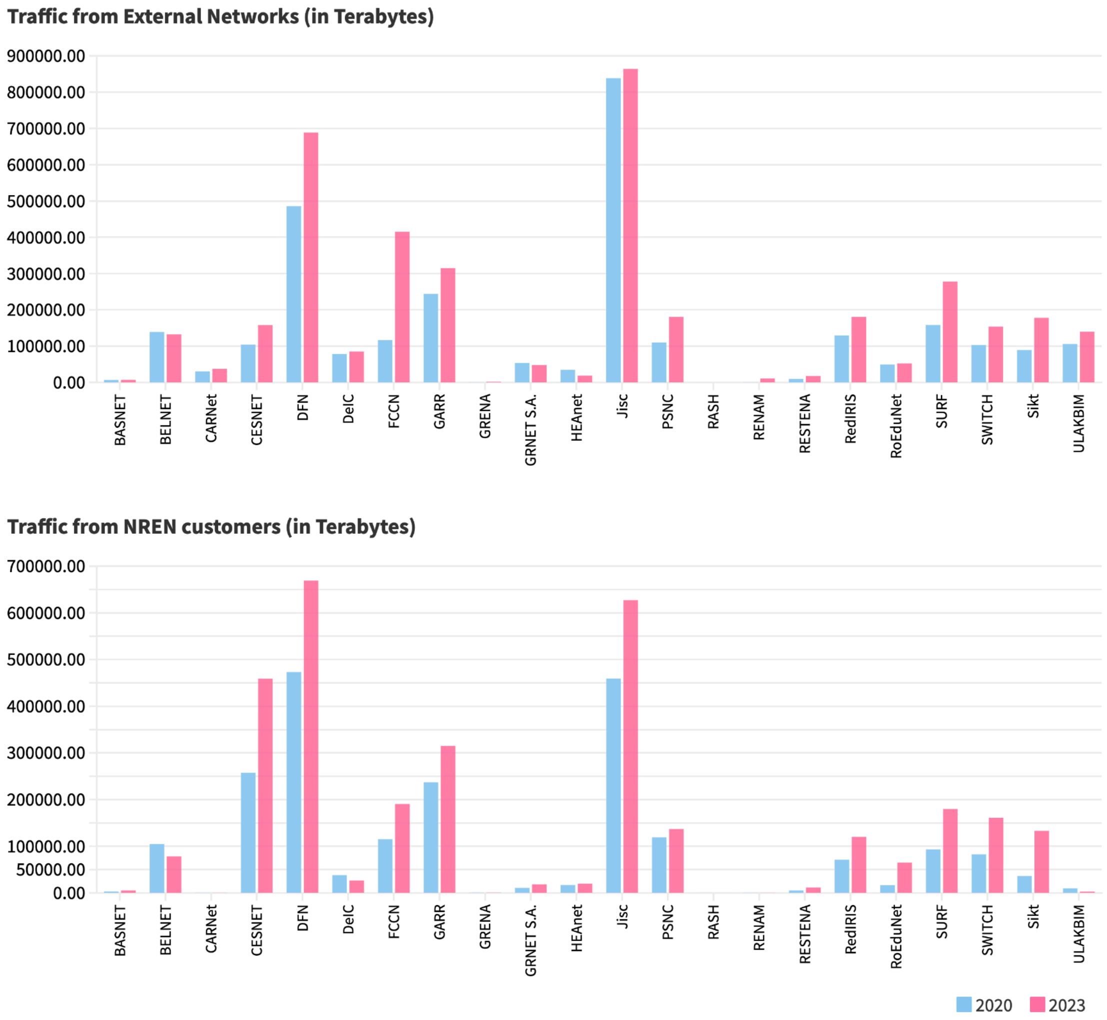


Figure 5.2: Traffic per NREN from external networks (upper panel) and NREN end users (lower panel) 2020 and 2023. *The figure shows all NRENs that reported their traffic volumes in both the 2020 and 2023 surveys; to make the figure easier to read (and emphasise changes), 2021 and 2022 data were omitted. As in the previous figure, "External network" denotes sources that are outside the NREN's domain, such as GÉANT, general/commercial Internet, Internet exchange, peerings, other NRENs. "NREN end user" denotes sources that are part of the remit of an NREN's domain.*

5.2. Traffic Growth Forecast

Since 2017, the Compendium survey has asked NRENs to provide an estimate of the growth in their traffic, by institution type, over the coming three years[34].

NRENs expect traffic to grow in the medium term: all 32 NRENs that provided estimates expect traffic growth over the three years 2024 to 2026, 14 of them by more than 50%, across all organisations within their remit. The highest growth is expected to come from the core users of all NRENs, universities and research institutes, with 77% and 79%, respectively. Schools (which are divided into primary and secondary schools) follow closely, with an anticipated growth of 75% and 72%, respectively. Two other categories have seen their anticipated growth increase: traffic of non-university hospitals is expected to grow by 68% and traffic to government bodies is expected to rise by 52% (see Figure 5.3).

[34] Projections like these are of course an important tool as they provide the foundation for determining how much investment in the network infrastructure will be needed.

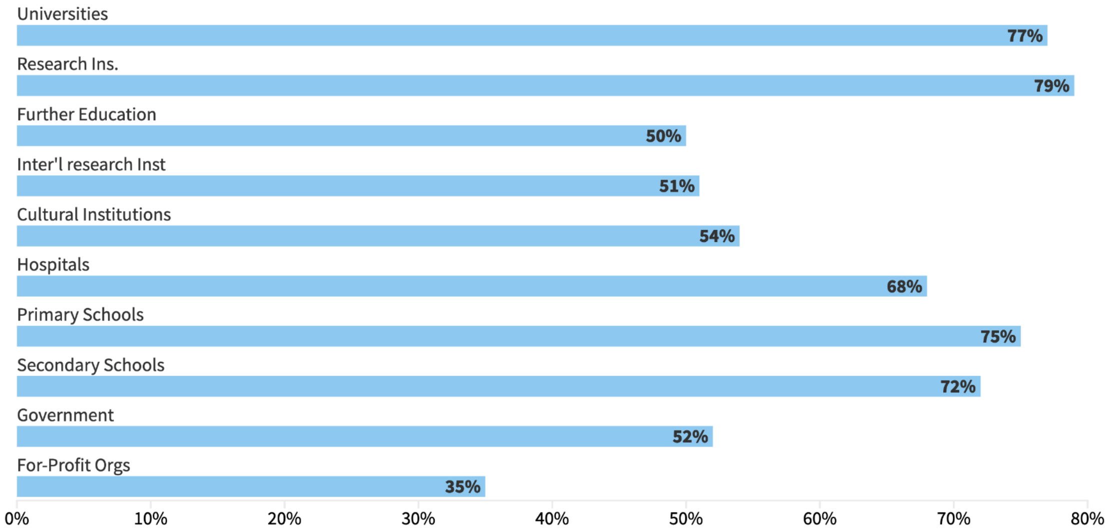


Figure 5.3: Average of the NRENs' forecast percentage traffic growth for the years 2024 to 2026, by institution type *(based on 32 responses).*

The continued traffic growth in the research sector, especially from research institutes, reflects the accelerating trend of data digitalisation and possibly the increasing role of centralised research facilities. The anticipated high growth rate in the school sector similarly reflects the increased use of digital resources, a trend accelerated by the COVID-19 pandemic. The traffic growth rate forecast in other categories is lower, but still significant. Note, however, that these growth numbers are percentages – the absolute expected growth in the volume of traffic is vastly bigger for universities and research institutions than it is for schools, the latter having much more modest needs.

Table 5.1 below gives an overview of the expected percentage growth in traffic over the three-year period 2024 to 2026, by NREN, and by institution type.

	Universities	Research Ins.	Further Education	Inter'l research Inst	Cultural Institutions	Hospitals	Primary Schools	Secondary Schools	Government	For-Profit Orgs
ACOnet	75	100	70		50	50	200	200	50	
AMRES	90	90	90		90	90	150	150	30	
ARNES	20	30	1	10	15	15	20	20	15	10
ASNET-AM	80	80		20	40				30	
AzScienceNet	400	300			100					
Belnet	150	150	100	50	150	200		150	150	
BREN	5	5		100	100	100	100	100	100	100
CARNET	30	30	20		20	30	30	30	30	30
CESNET	15	20	15	10	20	20	5	15	20	
CSC	90	90			90				90	
CYNET	30	10	10							
DeIC	120	100	100	100	50	200			50	
FCCN	20	50						20	20	
GARR	80	100		100	50	70	50	50	20	
GRENA	60	60		60	60	60		60	60	
HEAnet	10	10	10				20	20		
IUCC	50	30			30					
Jisc	50	50	50		20			10	20	20
KIFU	150	200	200		150	100	200	200	100	
KREN	100						100	100		
LAT	100	30			30			30	30	
MARnet	100	100								
MREN	60	50			50				50	
RASH	100	100			50				100	
RENAM	5	5	5		1	10			10	10
RESTENA	150	150						150		
RoEduNet	50	100	30	20	20		20	20		
SANET	70	60	50		60	40	40	50	40	40
Sikt	30	30						30		
SUNET	30	175	20		15	1				
SWITCH	35	35	35	35	35	35	35	35	35	35
ULAKBIM	100	100			50				100	

LESS = 40	OVER 40-100	OVER 100

__Table 5.1: Forecast percentage traffic growth by NREN and institution type for the years 2024 to 2026.__ Light-grey shading indicates forecast growth of less than 40%; dark-grey shading indicates forecast growth of 40–100%; black shading indicates forecast growth of more than 100%

5.3. IPv6

Internet Protocol version 6 (IPv6) [IPv6] is the most recent version of the Internet Protocol (IP), the underlying network protocol used by all applications and devices that communicate over the Internet.

With the IPv4 address space exhausted, the adoption of IPv6, with its significantly larger 128-

bit addressing, is very important to facilitate the future growth of the Internet and support the availability of globally unique IP address space for tens of billions of devices.

Having first been published as an IETF standard back in 1995, the core IPv6 specification was republished as a full Internet Standard, RFC8200, in 2017, confirming its high degree of technical maturity and a widely held belief that it provides significant benefit to the Internet community. IPv6 is usually deployed to run in parallel with "traditional" IPv4 networking, a model known as "dual stack". Sites therefore do not need to remove IPv4; they can initially benefit by running dual stack, particularly on their public-facing services.

The deployment of IPv6 among networks around the world is geographically very uneven, reaching more than 60% in some places (e.g. India, France) but usually being much lower. The R&E networks have a higher rate of deployment on their backbone networks, with at least 85% of NRENs carrying IPv6 traffic, while the GÉANT backbone network is also fully IPv6-enabled.

Overall, around 39–45% of Internet traffic is IPv6, based on a variety of measurements from different sources such as the Asia Pacific Network Information Centre (APNIC) and Google, which can be found at the World IPv6 Launch site [WIPv6LM]. The past three to four years have seen a rapid increase in commercial IPv6 Internet traffic, which now matches NREN IPv6 traffic which is also about 35% of the overall traffic (between April 2022 and March 2023, 35% of all traffic in the GÉANT network was IPv6), as the commercial ISPs and content providers have adopted IPv6 and have closed the gap to the R&E networks. However, while IPv6 is widely available in R&E backbones, this is not necessarily the case with campuses and networks that connect to the backbone, so the challenge now is to see its deployment grow on campuses.

That said, there have been substantial increases in traffic using IPv6 in R&E networks. In April 2018, the GÉANT network was transferring an average of 20 Gbps of IPv6 traffic (approximately 6% of total traffic); 12 months later, this had increased to an average of 110 Gbps or 22% of total traffic – a five-fold increase. The average for the year to March 2022 showed 119 Gbps of IPv6, representing 25% of the total traffic, October 2022 showed another increase to 253 Gbps and in October 2023 IPv6 traffic reached 305 Gbps. Figure 5.4 shows the IPv6 traffic average into GÉANT from its partners for October 2023.

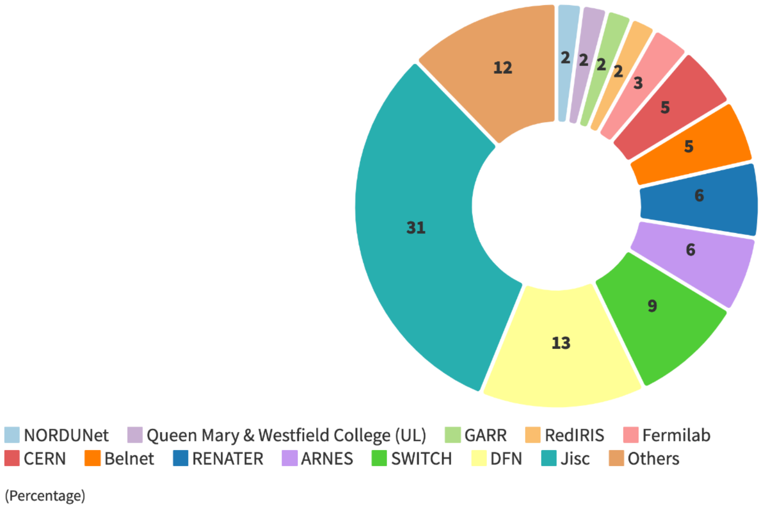


Figure 5.4: Top 12 GÉANT IPv6 traffic sources in October 2023. *Most of the traffic is reported by NREN, which hides the origin of the traffic; three NRENs (Jisc, DFN and SWITCH) source more than half of the incoming IPv6 traffic to GÉANT. Also interesting is that some research institutions have more IPv6 traffic than most NRENs altogether. The total IPv6 traffic for this month was 305 Gbps [Source: GÉANT Kentik tool].*

5.4. Network Infrastructure: Dark Fibre

Dark fibre refers to fibre optic cable leased or purchased from another supplier in the dark state (i.e. unlit), hence the name "dark" fibre. The fibre is then lit by the NREN using their own equipment (generally dense wavelength division multiplexing (DWDM) transponders and amplifiers). This term is used mostly interchangeably (if not fully accurately) with Indefeasible Rights of Use (IRU) (see textbox).

While not all NRENs use IRUs[35], the NREN community has gradually increased its ownership of dark fibre over the years. Changes in IRU use among NRENs are slow, reflecting the considerable costs involved, and the long-term commitment of capital that is required. The data also show that the yearly increase in dark fibre is slowing down – possibly hinting at a saturation effect. The increase as well as the slowing growth rate is documented in Figure 5.5. In 2023, the NRENs reported a total of over 150,000 km of dark fibre. Figure 5.6 below shows the number of kilometres of fibre each NREN reported in its own network[36]. This NREN-operated fibre interconnects with GÉANT's 11,000 km of intercity dark fibre, forming a strong community infrastructure (see Section 5.9 GÉANT Network Updates).

IRU

Indefeasible Rights of Use (IRU) is the long-term lease of fibre (generally dark fibre when it comes to NRENs, though it can technically be about other communication systems) that cannot be undone (hence "indefeasible"). With an IRU, the NREN essentially becomes the owner of the fibre for the duration of the contract, which is almost always long term, 10 years or longer (the current median among NRENs is 11 years). An IRU owner needs to cover operating and maintenance costs for the duration of the lease, which makes this a long-term commitment of capital.

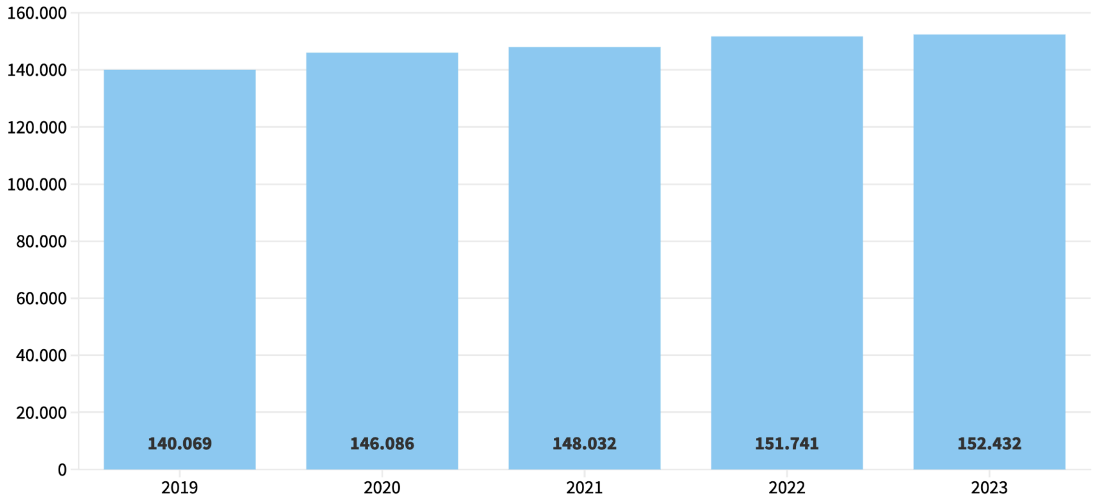


Figure 5.5: Development of the NRENs' IRU networks 2019–2023. *To make numbers comparable across the years, the figure shows only the IRUs of NRENs that have provided IRU data in all Compendium surveys from 2019 to 2023. Note the total length of the fibre network is even greater, as only IRUs are counted here, but some connectivity is provided by rented fibres – some NRENs even completely rely on rented connectivity over IRUs (BREN, CARNET, CyNet, MARnet, ULAKBIM).*

[35] 33 NRENs affirmed their use of IRUs in the Compendium survey, while 5 NRENs stated that they did not use IRUs (BREN, CARNET, CyNet, MARnet, ULAKBIM).

[36] In past reports, the Norwegian NREN Sikt listed 12,600 km of dark fibre. Recently Sikt reclassified 11,100 of those, leaving them with 1,500 km. To make the numbers comparable across years, this has been applied to older numbers in Figure 5.5 and Figure 5.6.

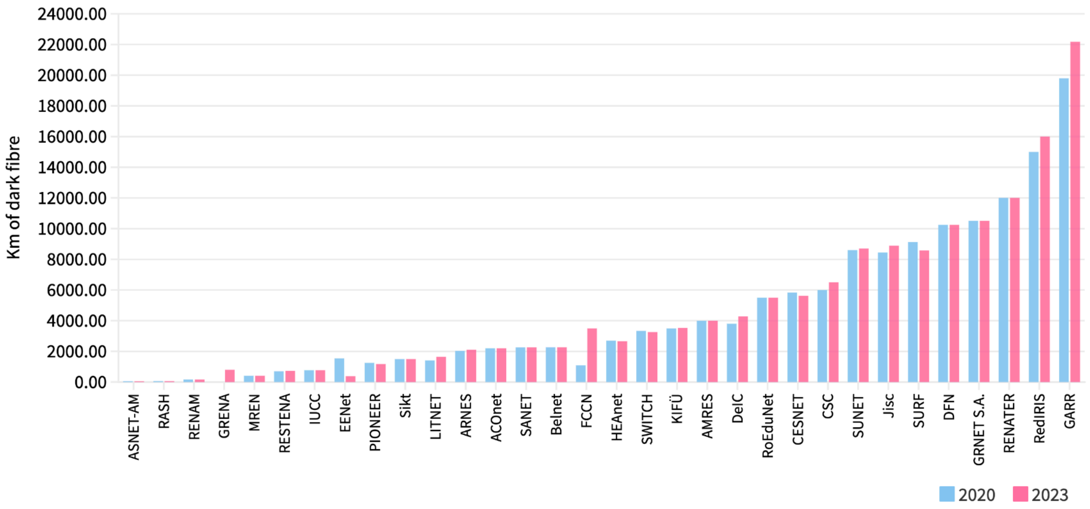


Figure 5.6: Number of kilometres of IRU network per NREN 2020 and 2023. For visual clarity, 2021 and 2022 were omitted from the graph. Overall, only small changes have taken place. The figure shows numbers for all NRENs that reported on their IRU network in the 2023 Compendium survey, i.e. NRENs that reported in previous years but did not do so in 2023 are missing.

5.5. Alien Waves

In the optical network world, the term "alien wavelength" or "alien wave" (AW) is used to describe wavelengths in a DWDM line system that pass through the network, i.e. they are not sourced/terminated by the line-system operator's equipment (hence "alien"). This setup is in contrast to traditional DWDM systems, where the DWDM light source (transponder) operates in the same management domain as the amplifiers.

Alien waves are an important part of infrastructure sharing, as the use of this technology is an important prerequisite for dark-fibre spectrum to be shared between multiple research network providers[37].

According to the survey results, 17 NRENs are currently making use of alien waves within their network[38]. Integrating alien fibre in an NREN's own network is not the only way to make use of this technology – 12 NRENs use alien wave services provided by third parties and 5 more are planning to do so[39]. While still representing only a minority of NRENs, both numbers have increased over the years, reflecting the increased use of alien wave technology: in 2019, only 13 NRENs had alien waves in their network (and 5 used third-party services).

Examples of spectrum sharing currently in use in the NREN community include the following:

- NORDUnet has taken steps towards building its entire network using spectrum provided by its local NREN members (DeIC, CSC/Funet, RHnet, SUNET, Sikt).

[37] The same technology allows the sharing of infrastructure between NRENs and GÉANT that is discussed in Section 5.9 GÉANT Network Updates. This also means that the sharing of fibres between NREN networks and the GÉANT network is limited to those networks where this technology is available.

[38] 39 NRENs (out of 44) responded to this question. The 17 NRENs making use of alien waves within their network are ACOnet, ARNES, CESNET, DeIC, FCCN, CSC/Funet, GARR, GRNET S.A., HEAnet, LITNET, PIONIER, RENATER, RESTENA, SUNET, SURF, SWITCH, Sikt.

[39] NRENs that use third-party services are: ARNES, Belnet, CESNET, CSC, DeiC, EENet, GARR, PSNC, RESTENA, Sikt, SUNET, SURF. Note that most of these NRENs use third-party services in addition to their own alien wave services (the exceptions are Belnet and EENet). BREN, GRNET, HEAnet, KIFÜ and RENAM are planning to add alien waves to their portfolio in the near future.

- NRENs' alien wave services also have the advantage that they can double as part of the pan-European R&E network: GÉANT has made use of as much NREN spectrum as possible when building its new network in 2020–2023. More details about this can be found in Section 5.9 GÉANT Network Updates, including an explanation of spectrum in Section 5.9.2.2.

5.6. Network Monitoring

A crucial aspect for NRENs is to understand what type of traffic flows via their network. Network monitoring aims to target network performance (speed, efficiency), integrity (failing hardware, bad configurations) and security (vulnerabilities, malware, malicious activity). In the longer term it is also important for capacity planning purposes. While every NREN monitors its network, not all are using the same methods. The general flow of information can be monitored using metadata, but for a more in-depth analysis, the data themselves need to be analysed, which only a minority of NRENs do: among the 37 NRENs that responded to this question, only 10 monitored their networks, using either SPAN ports (4) or TAPs (4) or, in two cases, both.

Network data are, of course, not only useful for the NREN but also for the network users, so most NRENs provide tools to their users that allow them to monitor their use of the network (Figure 5.7).

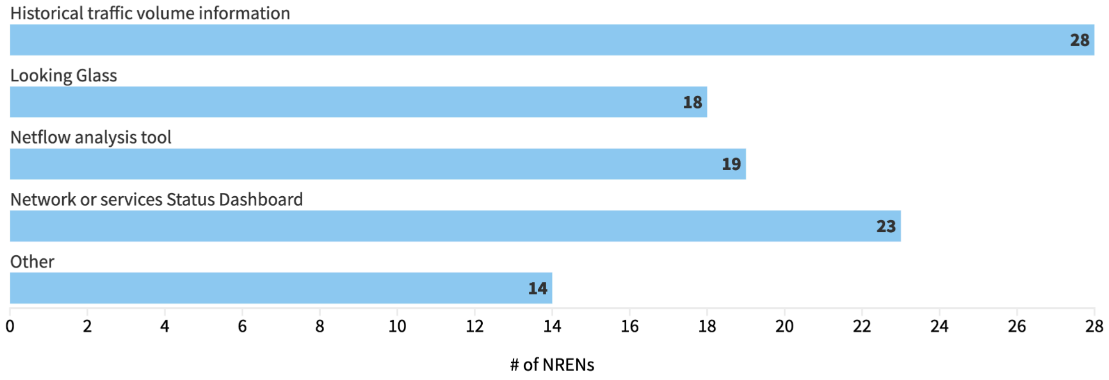


Figure 5.7: Overview of the most common tools that NRENs provide to their users to monitor their network use.
A total of 38 NRENs provided a response and many NRENs put several different tools at the disposal of their users.

5.7. IP Backbone Capacity

Principal data routes, to which customers are connected, are the backbone of an NREN's network. This means that the capacity of the network has to fit the needs of a country's research and education sector. As a consequence, the different capacities of the NRENs' backbones reflect the size of this sector – as well, of course, factors such as the funding that is available. An overview of the typical backbone capacity of individual NRENs is shown in Figure 5.8.

NRENs that serve a large research and education sector are increasingly using 100G technology to light their fibre. Eighteen NRENs have reported having typical backbone capacities of 100G or more. Overall, the average capacity of backbones has increased over the years (as can also be seen in Figure 5.8). This is also reflected in the median capacity across NRENs, which has increased noticeably over the last 3 years, having now reached 100 Gbps (with 40 Gbps in 2020, 60 Gbps in 2021 and 80 Gbps in 2022, after hovering around 20 Gbps for several years before that). However, as is clear from Figure 5.8, there is considerable spread among NRENs, which reflects that there is a long tail of relatively small NRENs that do not necessarily have the need for high capacities (or, in some cases, might lack the means to achieve them). Also, increases of the typical capacity result from network renewals, which are undertaken only in intervals of several years.

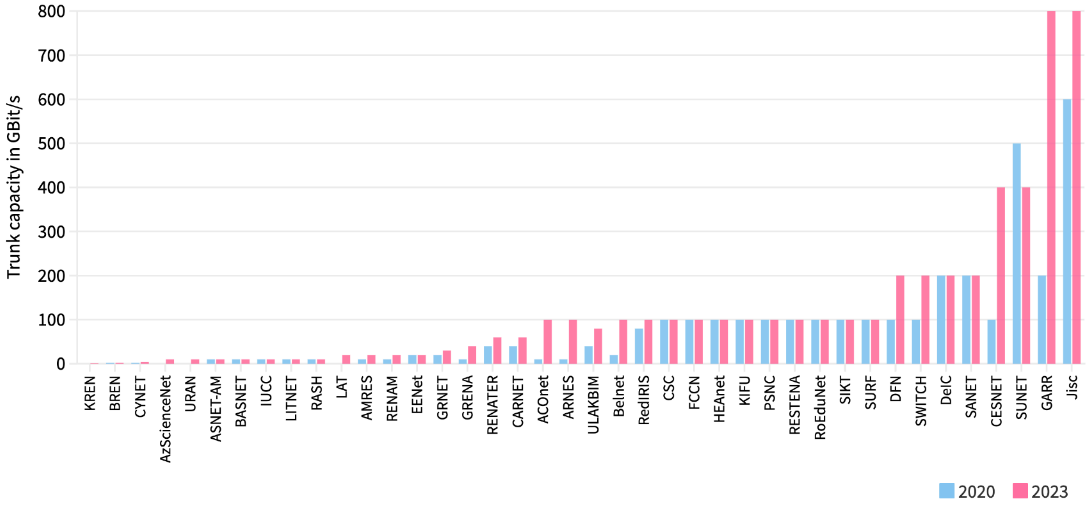


Figure 5.8: NRENs' typical core usable backbone IP trunk in Gbps 2020 and 2023. *The figure shows all NRENs that provided data on their trunk capacity in the 2020 and 2023 surveys; NRENs that reported in previous years but did not do so in 2023 are missing. For visual clarity, the 2021 and 2022 data were omitted from the graph. Most NRENs' backbone capacity has not changed. However, there are some notable increases: ACOnet, ARNES, Belnet, CESNET, GRNET, ULAKBIM, DFN, GARR, SWITCH and Jisc have significantly increased their capacity, and smaller increases have been implemented by AMRES, GRENA and RedIRIS.*

5.8. Network Peering

"Network peering" refers to the direct exchange of Internet traffic between two networks. For this to be possible, the two networks need to be physically connected, which often happens via an Internet exchange point (IXP) (public peering), but other arrangements are possible as well, e.g. by a direct point-to-point connection between the two networks (private peering). A peering agreement usually waives any fees for network traffic between the two networks.

Most NRENs have at least some direct peering agreements with commercial networks and content providers. The number of peering networks will also vary according to specific needs. Many NRENs aim to cover general Internet use with their peering agreements and will therefore have peering agreements with large international and regional networks. Some NRENs include academic collaborations with, for example, commercial entities in their peering agreements, which can lead to very large numbers[40].

In the 2023 survey, of the 35 NRENs responding to this question, 11 reported an increase in the number of non-R&E peering networks, 2 reported a drop, while the remaining 22 NRENs did not see a change in the number of peering agreements (see Figure 5.9).

[40] NRENs can negotiate peering agreements with any number of networks and some NRENs maintain many such agreements. Another solution that is available to NRENs is peering services provided by GÉANT. In this case, GÉANT has negotiated peering agreements with a number of commercial networks for its members. Some NRENs make use of both options, possibly complementing the more internationally oriented peering possibilities of the GÉANT services with local peering agreements.

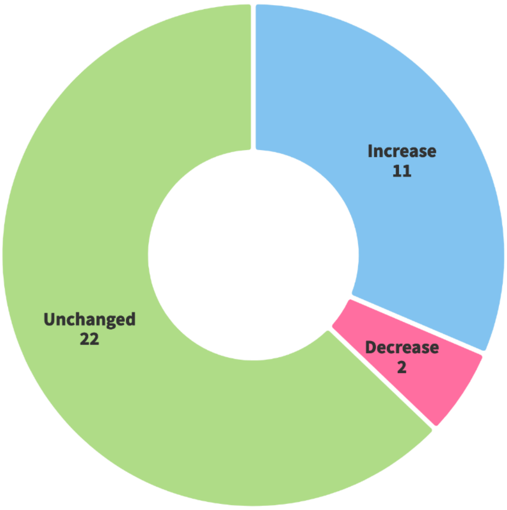


Figure 5.9: Development in number of NRENs' non-R&E network peerings 2022 to 2023

The number of peering agreements per NREN is shown in Figure 5.10. The policy of individual NRENs towards peering agreements varies widely but most NRENs have only a moderate number of them (single digit or low double-digit numbers), while some NRENs maintain large numbers. As a consequence, 80% of the peering agreements are held by just 7 NRENS (ACOnet, Belnet, DFN, GARR, SUNET, SURF, SWITCH).

In terms of absolute numbers, the number of peering agreements across all NRENs has increased to 3,364 compared with 2,926 in 2022. Generally, there is a constant flux in this area: in 2020 a high-water mark of 3,417 was reached and since then the number of peering agreements has dropped to the 2,926 in 2022 (with 2,976 in 2021). An overview of the changes from 2021 to 2023 is shown in Figure 5.10.

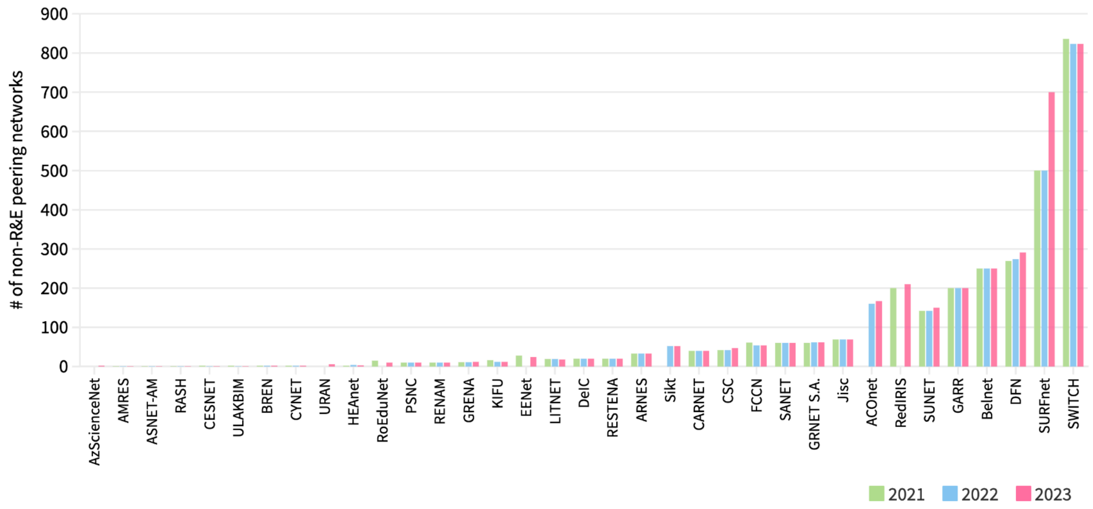


Figure 5.10: Number of non-R&E peering networks 2021 to 2023. *The figure shows numbers for all NRENs that reported on their peering agreements in all years shown in the figure. All NRENs in the graph maintain some peering agreements, though the numbers for some are too low to make a visible bar; only NRENs that did not report in one of these three years are missing from the graph. The figure shows that only a minority of NRENs maintain a large number of peering agreements.*

5.9. GÉANT Network Updates

The GÉANT network interconnects 40[41] research and education networks in Europe (a topology map is shown in Figure 5.11). This section presents a snapshot of the GÉANT network, including statistics such as IP/MPLS traffic growth, and an overview following the network refresh activities as part of GN4-3N.

The GN4-3N deployment is now complete and its final design provides 32 IP/MPLS routing sites and 15 DWDM add/drop only sites. All routing sites are also DWDM add/drop sites which connect to NRENs and/or international partners.

With the upcoming IP/MPLS deployment a new design for the network has been drafted, including 35 routing sites.

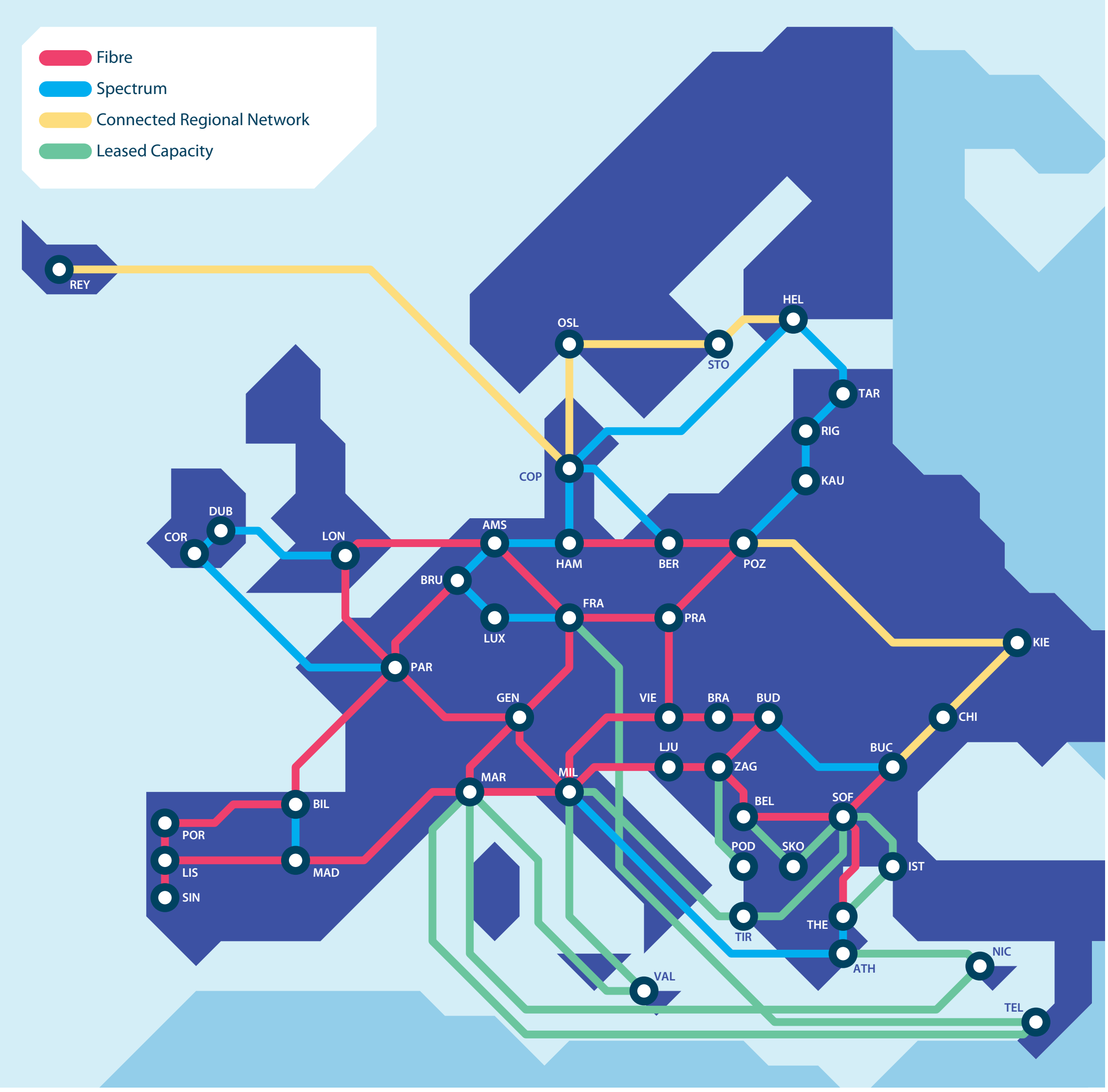


Figure 5.11: GÉANT pan-European network topology map (GN4-3N design)

[41] The five Nordic NRENs form their own regional ISP, NORDUnet. It is NORDUnet that is a member of GÉANT Association, while the Nordic NRENs are associates.

5.9.1. Current GÉANT Network and Statistics

5.9.1.1. Current GÉANT Network Structure

The GÉANT network is divided into three parts, as shown in Figure 5.12: the Infinera DWDM open line system, the Infinera DWDM transponders layer and Juniper-based Internet protocol / multiprotocol label switching (IP/MPLS) network [Infinera; Juniper][42].

The open line system runs on top of dark fibre and spectrum links (for spectrum, see also the textbox below) and provides management of the optical, DWDM signals generated by the transponders layer, that is, amplification, multiplexing and power balancing. The "open" nature of the line system means that this layer can accept signals generated by different sources without restriction to a specific vendor or a specific technology.

Spectrum services for NRENs or R&E partners are delivered directly by this layer.

The next layer up the stack is the transponders layer, constructed utilising Infinera Data Centre Interconnect (DCI) transponders. This layer is responsible for activating point-to-point capacity over the line system routes. Transponders terminate short-reach Ethernet signals of 10, 100 and 400 Gbps capacity, and generate high-capacity DWDM signals for transmission over the DWDM line system. These high-capacity point-to-point connections are used for carrying the trunks between the IP/MPLS routers of GÉANT. In some cases transponders are directly connected to spectrum supplied by a provider; this is the case when either the amount of spectrum is very limited (therefore not justifying the investment in the line system deployment), or there are limitations preventing the deployment of the full line system (see Figure 5.12).

"Managed Wavelength" services, or point-to-point high-capacity guaranteed Ethernet services to NRENs or R&E partners are also delivered directly by this layer.

The upper layer of the stack is the IP/MPLS layer, which is today managed by Juniper MX series routers; this layer is undergoing change as part of the IP/MPLS refresh where Juniper MXs will be replaced by Nokia 7750 SR-7s and SR-2se devices (see Section 5.9.2.3 for further detail). This layer is responsible for transmission of IP packets and Ethernet frames between connectors across the GÉANT network.

All connectivity services not delivered by the other layers are delivered by the IP/MPLS layer.

[42] It is important to note that GÉANT retendered for the supplier of the IP/MPLS kit in 2023, with significant changes to this layer expected in 2023–2025. Further detail is provided in Section 5.9.2.3.

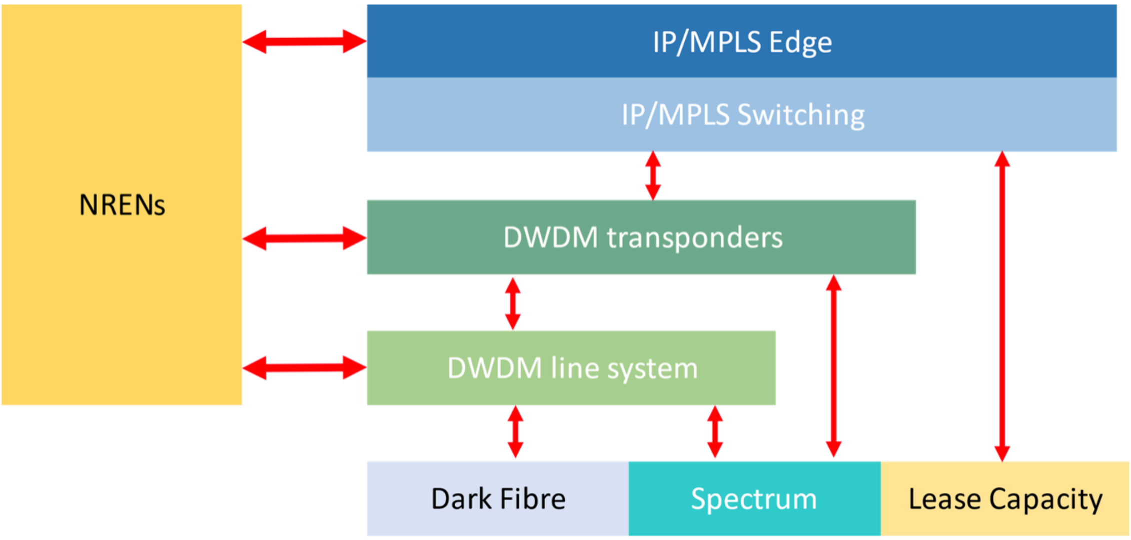


Figure 5.12: The current layered structure of the GÉANT network. *The IP/MPLS routing part of the network, provided by Juniper MXs, is shown in two shades of blue (top of the figure), while the optical transport network (OTN) / DWDM part, provided by Infinera, is shown in two shades of green (middle of the figure). The arrows represent demarcation points between building blocks.*

5.9.1.2. GÉANT Network Statistics

In 2023 the GÉANT network received 3.2 Exabytes of traffic, representing an increase of 6.8% from the previous year's figure. Figure 5.13 shows the year-on-year traffic growth from 2015 to 2023. After continuous growth until 2019, a significant drop in traffic is followed by a sequence of 7 quarters with comparatively low traffic levels. The decline is due, to a large extent, to the impact of COVID-19 and the subsequent move of users from locations where connectivity is provided by GÉANT (universities, research centres, etc.) to residential settings. This assessment is corroborated by the results of the traffic analysis for the major categories of traffic carried by GÉANT, where mostly user-dominated data traffic types have decreased while machine-to-machine traffic, such as LHCONE[43], has remained relatively strong.

However, traffic has grown again in 2021, 2022 and 2023, with the overall yearly traffic levels in 2023 reaching the highest level yet (Q4 2022 remains the strongest quarter in terms of traffic volumes) (Figure 5.13). It is important to note that while IP/MPLS traffic keeps growing, Managed Wavelength Services (formerly Lambda services) have been declining since 2018.

[43] The LHC Open Network Environment (LHCONE) network is part of the infrastructure that underlies the global collaboration of computing centres that provide global computing resources to store, distribute and analyse the massive volume of physics data generated by the Large Hadron Collider (LHC) experiments at CERN.

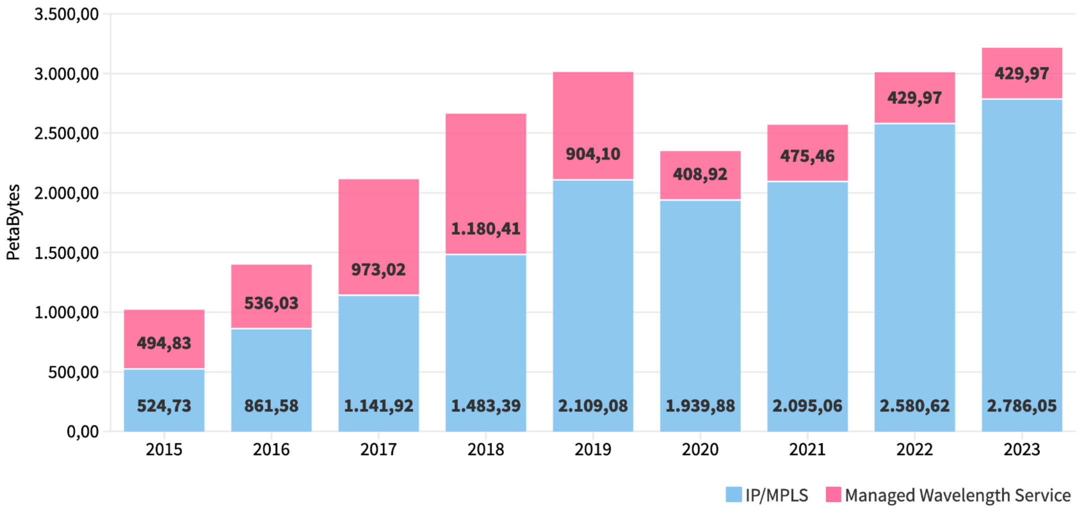


Figure 5.13: ***Overall yearly traffic volumes in PetaBytes.*** *The figure shows the yearly volume of traffic received by GÉANT in PetaBytes from 2015 to 2023 distinguishing between IP/MPLS traffic and Managed Wavelength Service (formerly Lambda) point-to-point traffic. The data show a dip during the COVID epidemic. Managed Wavelength traffic for 2023 is estimated (*).*

5.9.2. Evolution of the GÉANT Network

5.9.2.1. Network Topology

As part of the network refresh activity, funded under the GN4-3N project, GÉANT has expanded, bringing long-term stability to its network footprint by acquiring infrastructure on a long-term IRU basis.

The new GN4-3N topology has been developed in close collaboration with the NRENs. The new network footprint will be based in large part on fibre or spectrum (fibre shares) under long-term contracts (15 years or longer), which will connect many areas previously covered by lease capacity (normally procured on short-term contracts of 1 to 3 years).

The number of countries connected directly via GÉANT fibre has increased from 14 to 28, with dark fibre / spectrum routes doubling in number and tripling in length (see Figure 5.14 for details).

It is important to note that a considerable number (about 25%, 7,200 km, in terms of overall length) of connections that form part of the new network are provided by NRENs, sharing existing infrastructure with GÉANT. This ensures that infrastructure duplication is minimised and GN4-3N funding was used in places where it was most needed[44]. Full details can be found in the latest revision of the GÉANT Network Evolution Plan [GN5-1_D7.1].

The GN4-3N project ended at the end of 2023, with all routes planned, procured and implemented.

[44] GN4-3N funding could only be used to cover costs paid to commercial providers. With the use of IRU-type contracts, where a considerable amount of the overall contract costs are paid at the start as capital costs, this meant that wherever connectivity could be provided without making use of commercial entities, GN4-3N funding remained available and could be deployed elsewhere, where adequate NREN infrastructure was not available.

GN4-3N

Together with GN5-1, GN4-3N is the most recent iteration of a series of projects (GN1, GN2, GN3, GN3plus, GN4-1, GN4-2 and GN4-3) that have helped develop the pan-European network of the GÉANT project. The GN4-3N project restructured the GÉANT backbone network through exploration and procurement of long-term Indefeasible Rights of Use (IRUs), leased lines and associated equipment. It was the most significant refresh of the GÉANT network in a decade, designed to support the needs of Europe's research and education community for the next 15 years.

SPECTRUM

Spectrum services (or spectrum) are a way to better utilise the capacity of optical fibres. Just as in mobile networks, where network operators use different frequency blocks of the radio spectrum, it is possible to divide the optical spectrum in a fibre network, assigning different frequency bands to different users. Spectrum provides most of the benefits of a dark fibre without the need for acquiring and running a full dark-fibre link. The provider of the spectrum service (usually the owner of the dark fibre) is responsible for running the line system, while the client/customer is responsible for owning and operating the transponders. Spectrum fills the large gap that exists technically and financially between a dark-fibre link and leased capacity.

5.9.2.2. Transmission/DWDM

Together with the acquisition of a new fibre/spectrum footprint as part of GN4-3N, GÉANT awarded a contract for the commissioning and provisioning of a new network DWDM system to Infinera.

As part of this contract, Infinera is deploying its most recent open line system (OLS), FlexILS, combined with transponders in Data Centre Interconnect (DCI) form factor.

This new system has replaced the previous DTN-X (OTN switching) based system, implementing GÉANT's transition towards a disaggregated system where the transponders and line system are separate building blocks. This transition enables GÉANT to manage the two building blocks more efficiently, allowing selection of the "best of breed" for each block, including having multiple vendors.

This system will also allow GÉANT to take full advantage of packet optical integration – this is the deployment of DWDM optics directly on router interfaces. This option has now gained significant momentum thanks to the efficiency gains of transponders, allowing the packaging of DWDM optics into QSFP-DD (or OSFP) form factor and the standardisation of the ZR optics (400G) as part of the Ethernet. The GÉANT disaggregated optical system provides the optimal platform to take advantage of this option.

Finally, the new system allowed GÉANT to define a new "Spectrum" service offer as part of its services portfolio.

As part of the tendering process for the new network DWDM system, GÉANT has also established a new procurement framework to replace the PRISM framework, which had been in place since 2015. Using the new framework agreement, both GÉANT and the NRENs will be able to procure transmission layer equipment from a selection of vendors under preferential conditions.

5.9.2.3. Packet Layer

In 2023 GÉANT finalised the process of tendering for a new IP/MPLS layer to replace the Juniper MX-based one deployed in 2012, awarding the contract to Nomios (integrator) with Nokia (vendor).

As part of the new network deployment, GÉANT will deploy Nokia 7750 SR-s devices at all IP/MPLS PoPs, which will provide support for a high number of 400G Ethernet interfaces, allowing GÉANT to upgrade trunk capacities for all links between transit IP/MPLS nodes to use 400G Ethernet from the current 100G Ethernet.

Lower costs and a high count of high-speed interfaces will allow GÉANT to leverage the fibre investment of GN4-3N by providing very high data rates to all transit points in the network. This design will support upcoming interconnecting high-capacity intercontinental links to the edges of Europe, improving the quality of transit services for all NRENs, in particular those not in the central European area.

The tender was finalised in June 2023, with lab testing in Q3/4 2023. Deployment started in Q1 2024 and is expected to continue throughout 2024 and 2025.

Together with the change to the IP/MPLS hardware, GÉANT is also significantly investing in automation to ensure that the configuration of the IP/MPLS devices is handled by automated processes rather than through manual configuration. This will reduce the risk of human errors, speed up service deployment and ensure regular updates and consistency of configurations. All migration activities will be carried out with the use of automation.

5.10. Summary

Reflecting the ever-increasing importance of digital services in the R&E world, network traffic is expected to keep growing in the coming years. The expected traffic growth is reflected in the increase of network capacity, which is upgraded in stages, meaning that the overall increase of network capacity is modest year on year. R&E networks, such as GÉANT, are overprovisioned by design, to ensure that bandwidth is no limitation to data exchange or processing and that additional traffic can be accommodated. This is of particular relevance for "Big Science" but the R&E sector as a whole benefits. While capacity (and traffic) keeps increasing at a steady pace, the growth of the networks themselves seems to have slowed, possibly because most NRENs have by now connected all or the majority of the relevant R&E locations.

6. SECURITY

Cyber security is a growing issue in any ICT environment and the R&E sector is no exception. That the R&E sector is a target for cyber criminals has been demonstrated in the past by several (successful) major cyber-security attacks on R&E institutions, both universities and research organisations[45]. As the primary providers and enablers of ICT services for the research and education sector, NRENs are in a central position regarding security.

The exact role of an NREN in cyber security depends on the fields in which it operates. Most NRENs limit their activity to the R&E sector and therefore are mainly involved in cyber-security efforts concerning the R&E community. On the other hand, some NRENs are also responsible for critical national infrastructure such as the top-level domain (TLD) registry (e.g. Belnet, RESTENA, SWITCH), or the NREN is considered critical infrastructure in itself. The latter is more or less automatically the case when the NREN delivers services to government bodies (e.g. Belnet). Another factor that can have an impact on the reach of an NREN's cyber-security measures is its organisational model: some NRENs are government bodies (e.g. Belnet, FCCN, RedIRIS, Sikt), while others are not autonomous legal entities but part of larger organisations, usually universities (e.g. ACOnet, UoM – see also the discussion about funding and governance in Section 2.3).

Such differences are reflected in the way cyber security is dealt with, both in and for the NREN: whether ISO certification is needed, what and how many services are provided, the level of contribution in the GNx-N project, the available skill set, and the risk of becoming the target of attacks.

This challenge is compounded by an increasingly heterogeneous infrastructure in the R&E sector. R&E institutions use numerous network-related resources at the same time, such as different cloud suppliers, data lakes, app stores, computer centres, etc. This trend has been present for some time and the NREN community has tackled this challenge by investing in a number of standardisation projects such as the policy kits developed in the AARC projects [AARC] and by supporting the development of standards such as Sirtfi (see also Section 7 Trust and Identity) and the Security Baseline for NRENs document [GN4-3_D8.2].

In addition to the security aspects that are intrinsic to their role as ISPs, NRENs also face a changing regulatory landscape, as bodies such as the EU react to the changing cyber-security situation by creating regulations. Examples include the General Data Protection Regulation (GDPR) or the Network and Information Security Directive (NIS2), the directive on Critical Entities Resilience (CER) and the Cyber Resilience Act (CRA). NRENs will also need to comply with changes to the funding structure of procurement grants, which include implications for security.

The data presented in this section illustrate the current efforts of the NRENs in the two broad areas of organisational security and security services. The data originate from the NREN

[45] A number of large NRENs observe and are involved with cyber-attacks on a daily basis, ranging from "run-of-the-mill" Distributed Denial of Service (DDoS) attacks to full-scale DDoS attacks crippling complete universities. To give some examples: there have been ransom attacks on the Dutch research funding organisation NWO (February '21) and Maastricht University (December '19), hacktivist attacks on Italian universities (February '20), attacks that might have been politically motivated on Polish military universities (June '20) and Belgian political and scientific institutions (May '21). Other published incidents were attacks on universities in Thessaloniki (May '17), Northumbria/UK (September '20), Rijeka/Croatia (November '20), Sunderland/UK (October '21), Hamburg/Germany (December '22), Mechelen/Belgium (September '23), Bremen/Germany (October '23). It should also be noted that not all incidents become public, as the information policies around security issues vary.

Compendium survey, where NRENs provide data about their service portfolio, from GÉANT's Partner Relations team, and from the Trusted Introducer (TI) programme[46], a survey on security awareness carried out among NRENs in 2023, and a series of interviews that GÉANT's security team held with NREN security officers.

6.1. Organisational Security

The data about the organisational security of NRENs are presented by area – policy, people, threats and operations – in alignment with the security framework laid out in the Security Baseline for NRENs document [GN4-3_D8.2][47]. Organisational security looks at the processes within an organisation and how they take security issues into account. This would include defined security incident responses but also formal policies concerning security-relevant areas. Figure 6.1 shows the number of NRENs adopting security features for the period 2020 to 2023, grouped by security area.

[46] Services for security and incident response teams [TI]. The TI programme has a maturity scheme for Computer Security Incident Response Teams (CSIRTs). Teams can be listed, accredited, or certified.

[47] Only some of the sub-topics defined in Security Baseline for NRENs can be assessed using the data available in the Compendium, and only at a limited level of detail, so a full evaluation of NREN security competence is not within the scope of this report.

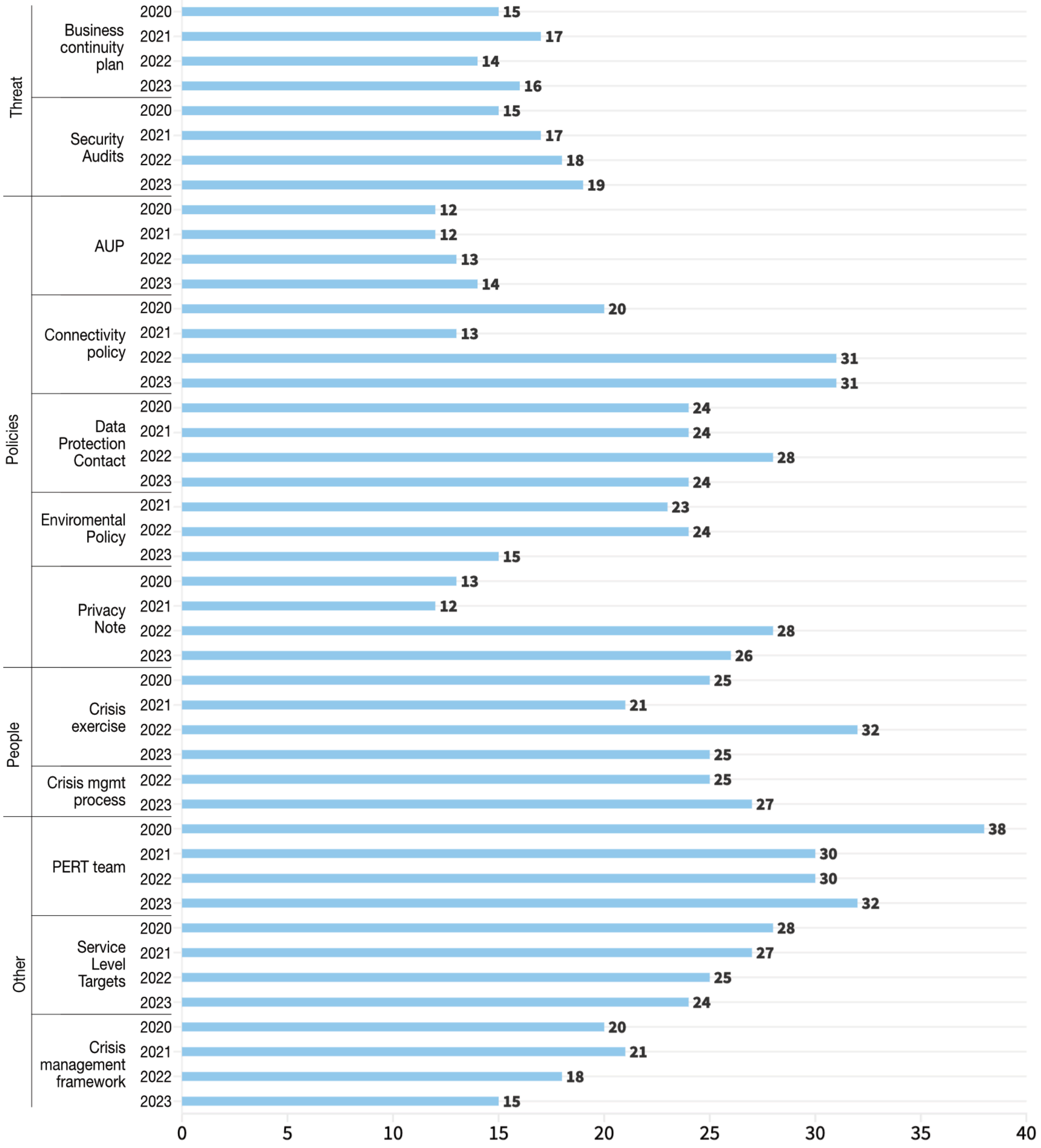


***Figure 6.1: Development of the adoption of organisational security features by security area**, number of NRENs 2020–2023. Not all data are available for all years. The number of surveyed NRENs was 43 for all years. Numbers missing from that count are due to non-responding NRENs.*

Policy

An Acceptable Use Policy (AUP) and a Connectivity Policy are important security-related policies. As they are fundamental for an ISP, these are among the NRENs' oldest policies; almost all NRENs that responded to the Compendium survey have an AUP in place and have had for some years (see also Section 3.2 NRENs' Acceptable Use Policy). Dedicated connectivity policies are not quite as widespread, possibly reflecting that some NRENs are part of larger organisations that set such policies instead or reflecting a more operational approach to security.

Another important policy area is the adherence to the GDPR or similar privacy regulations for non-EU countries. Part of the GDPR is the requirement for a Privacy Notice, so this can be taken as an indicator of efforts in this area. In 2023, about 28 of 41 NRENs stated that they have a privacy notice. This suggests some NRENs do not yet fulfil this particular legal requirement.

There are of course limitations to these data. The survey only asks for the existence of policies, not details of their content. Nonetheless, the existence of dedicated policies can be taken as commitment to best practice. In that regard, the relatively high numbers of AUPs, Connectivity Policies, Data Protection Contacts and Privacy Notices in place are encouraging. Arguably, however, they should be higher: as mentioned above, a Privacy Notice is required by law in most jurisdictions, as are data protection contacts, so the numbers of these policies can be expected to grow further in the coming years as NRENs will catch up with regulations.

People

An important factor regarding IT security is the expertise within an organisation and large knowledge gaps in this field are common. Most organisations have a higher demand for security specialists than are available on the job market and therefore struggle to find the experts to fill vacancies – and this situation is unlikely to change in the near future. Training offers are an important way to mitigate this situation[48].

Some training opportunities are provided by GÉANT, which offers some security training (e.g. TRANSITS, CLAW[49]) which some members are using, but many other training options are available. In addition, the majority of NRENs prepare their staff specifically for the case of a security crisis, for example by participating in workshops such as CLAW or carrying out crisis exercises within their organisation (see Figure 6.2).

[48] Unfortunately, there are no numbers available that would document how NRENs make use of training opportunities.

[49] TRANSITS are courses designed for Computer Security Incident Response Team (CSIRT) personnel which are offered regularly but they are not limited to NRENs. The material used in these courses is freely available under an open-source licence which enables other providers to offer equivalent courses [TRANSITS]. However, it is not possible to track how many NRENs participate in such courses. CLAW is an annual workshop on crisis management for NRENs, which has taken place since 2017.

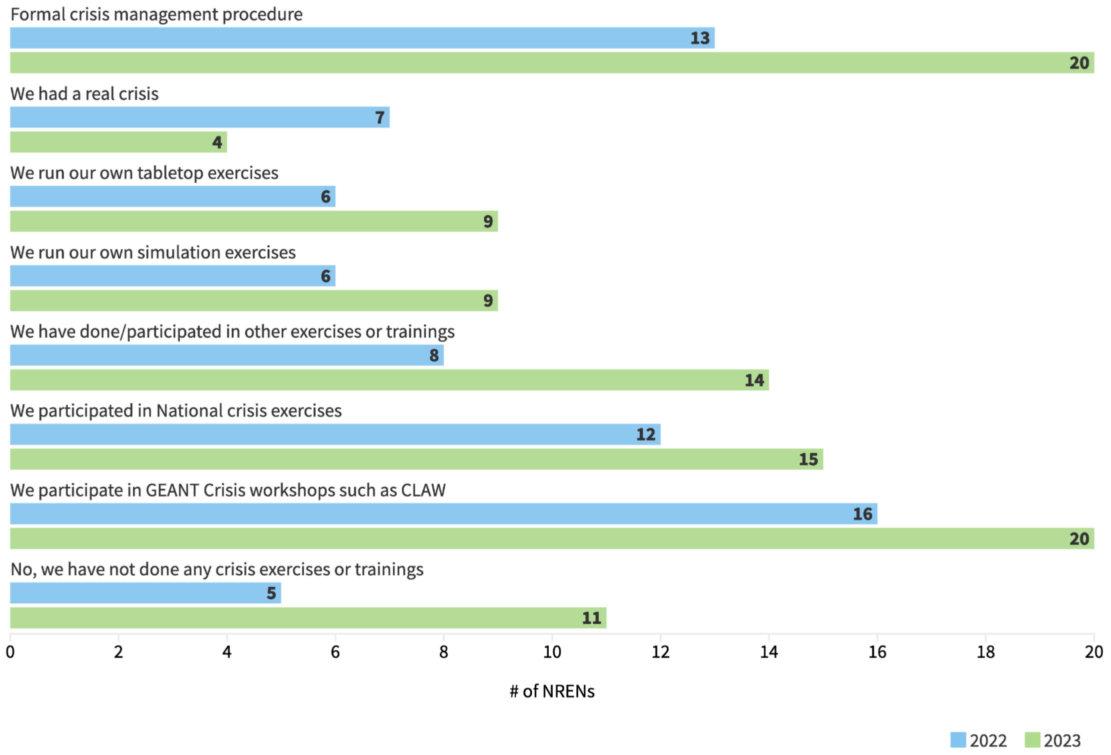


Figure 6.2: NREN crisis preparation. *The figure shows how many NRENs have a formal crisis management process in place (20 NRENs, up from 13 in 2022) and also summarises what kind of crisis preparation NRENs did. A number of NRENs took several different measures. Most numbers have gone up since 2022, reflecting the increased focus on security. On the other hand, the number of NRENs who have not done any crisis exercise or training in 2023 is lower than in 2022. This seeming contradiction reflects that some NRENs carry out multiple security activities (training, different exercise types, etc.).*

Security awareness

Managing human risk is one of the major security challenges that organisations face. It is therefore important for organisations to protect themselves against cyber crime not only with adequate technical security measures, but also by raising awareness and training their employees. This also applies to National Research and Education Networks. Data collected from NRENs show that the majority of them consider the "human factor" to be a key element of cyber security and are actively taking steps to train their employees[50]. As expected, the maturity of NRENs in this area was found to vary widely. Where some NRENs have a programme that is designed primarily to meet specific compliance or audit requirements, others have more mature programmes which focus on behaviour change (Figure 6.3).

Since most NRENs are small to medium-sized organisations[51], it is not surprising that those who are responsible for internal awareness frequently combine this work with other, often primary, responsibilities. Most internal awareness officers within NRENs are part of the Security

[50] The data presented here come from a survey conducted among 25 NRENs that was conducted in 2023 by the Awareness subtask, part of the GN5-1 project, WP8 Security – T2 Human Factor. Detailed results are available in [GN5-1_SoCSAwNRENs]. Participating organisations: ARNES, ASNET-AM, Belnet, CARNET, CESNET, CSC/Funet, CyNet, DeIC, DFN, GARR, GÉANT, GRENA, GRNET, HEAnet, Jisc, LITNET, RASH, RedIRIS, RENAM, RENATER, RESTENA, SUNET, SURF, SWITCH, ULAKBIM.

[51] The EC definition of micro, small and medium-sized enterprises is based on staff headcount, annual turnover and annual balance sheet total. The headcount criterion for micro organisations is fewer than 10 staff, for small organisations it is fewer than 50 staff, and for medium-sized organisations it is fewer than 250 staff. See [EC_UGtoSME]. Only 3 NRENs (or 5, if CSC and Jisc are counted according to their full headcount) are large organisations; the majority (24) are small organisations). See also Section 2.4 Staffing.

or CERT teams and coordinate their work with other departments such as Marketing & Communication, IT Support or Legal teams.

Regarding external awareness activities, most NRENs help their communities to tackle security challenges by providing them with communication materials and e-learning, and organising security events and conferences, etc. The same difference in maturity as for internal awareness is also evident in these initiatives (Figure 6.4).

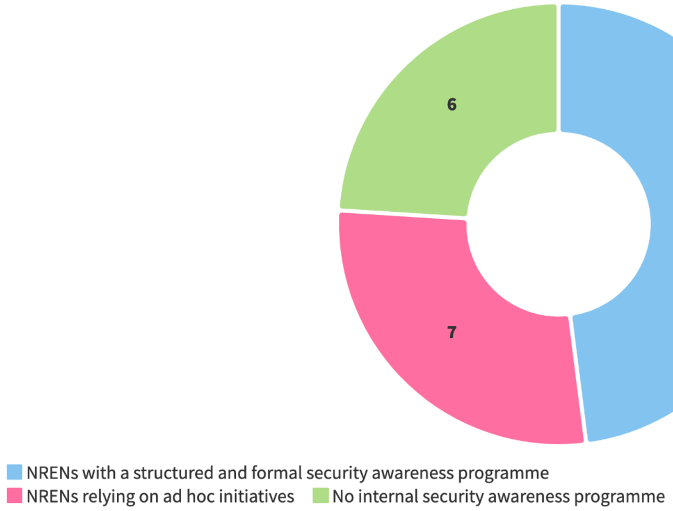


Figure 6.3: NRENs and internal security awareness programmes. *Internal security awareness refers to measures that aim to raise employees' awareness of security risks. The survey presented NRENs with three options for the state of their internal security awareness portfolio. As shown here, most of the 25 NRENs in the survey run an internal security awareness programme, albeit at different formality levels. A formal and structured internal security awareness programme entails a strategic plan that has identified the scope, goals and objectives, while ad hoc initiatives means that there is no strategic plan, training topics are chosen ad hoc, and training is deployed at random times.*

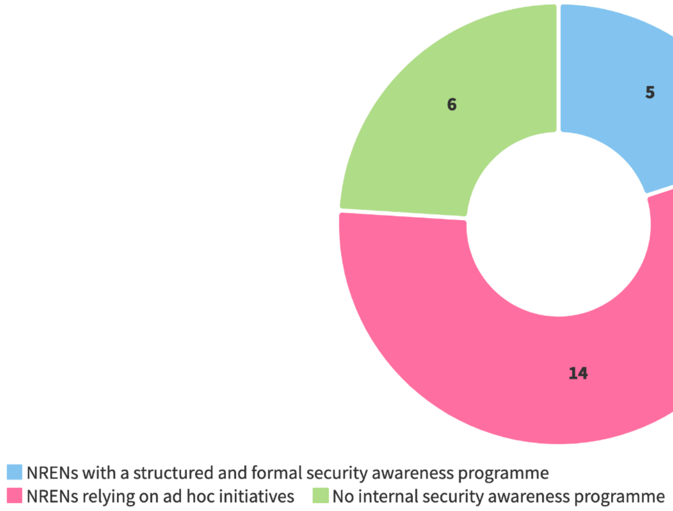


Figure 6.4: NRENs and external security programmes. *External security awareness programmes mean that NRENs offer security awareness training to their users. The survey presented NRENs with three options for the state of their external security awareness portfolio. A little less than half of the 25 NRENs in the survey run external security awareness programmes. Similar to the criteria used for internal security (Figure 6.3), a formal and structured external security awareness programme entails a strategic plan that has identified the scope, goals and objectives, while ad hoc initiatives means that there is no strategic plan, training topics are chosen ad hoc and training is deployed at random times, following the availability of resources and the needs of users.*

Threats

As threats are proliferating, NRENs are working to counter them in various ways.

On the network level, a growing number of NRENs operate Security Operations Centre (SOC) or Security Information and/or Event Management (SIEM) functions or are preparing to do so. In 2023, 13 NRENs reported using SOC / SIEM.

On an organisational level, many NRENs perform security audits of their organisation or their services – this, of course, is good practice but is increasingly required by legal frameworks, as briefly discussed above. Twenty-eight out of 41 NRENs have some kind of security audit of their organisation; roughly half of them (18) make use of international security certification standards such as ISO 27001[52].

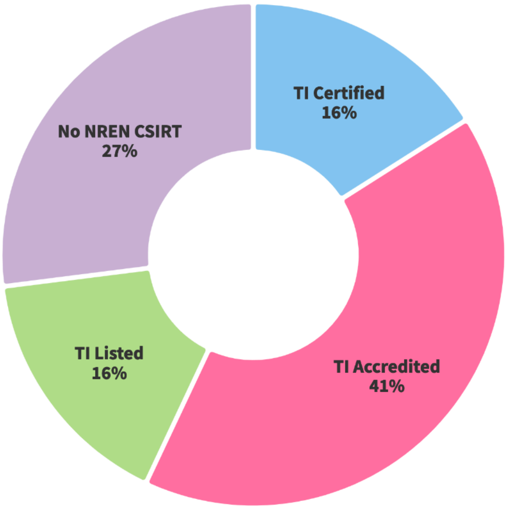


Figure 6.5: Numbers of NRENs with CSIRTs and their level of Trusted Introducer (TI) participation. *32 out of 44 NRENs have a CSIRT that is participating in the TI programme, i.e. the CSIRT is either TI certified, accredited or listed. In December 2023, 7 CSIRTs were certified or candidates for (re-)certification, 18 were accredited or candidates for accreditation, and 7 were listed. "Listed" means that contact information is listed in a central, public register. When a team hands in a basic set of documentation which is proof of a defined level of best practices and acceptance of the established TI policies, then the team becomes accredited. A team can be certified if they have been accredited before and can prove a confirmed level of maturity as defined by the TI Security Information Management (SIM) framework, by means of an external audit.*

Business continuity plans are another way to prepare for threats and currently 20 NRENs have one of these in place. While there is progress in this area (in 2021, only 18 NRENS had a business continuity plan in place), there is clearly still work to be done. Again, this could be covered elsewhere if the NREN is part of a bigger organisation (as some are) but the relatively low number is an area to be addressed[53].

Finally, most NRENs (32 out of 44) also have a Computer Security Incident Response Team (CSIRT) (see Figure 6.5). Those NRENs that do not have a CSIRT usually have this function covered by closely associated organisations.

[52] Certification against ISO 27001 for the whole organisation or for a part of its processes, for example NRENs that also manage a national top-level domain registry. At least 13 NRENs reported having an ISO 27001 certification or are working on it; some are also following government-defined certification rules.

[53] A guidance document for setting up business continuity was developed in the GN4-3 WP8 (Security) Business Continuity Task [GN4-3_D8.12].

Operations

Services and tooling are seen as a major instrument in the fight against cyber crime [Register BIIC] and the Compendium survey asked the NRENs about the use of security tools as part of their operations. Forty NRENs named at least one security tool; this is a high number, and as not all NRENs respond to all questions it seems likely that all NRENs utilise some kind of security tool, especially as the list of measures includes very mundane measures such as anti-virus suites, anti-spam and firewalls[54]. However, this is a very wide field, which also includes more sophisticated measures such as integrity checkers or network segmentation. Figure 6.6 presents an overview of how many NRENs use which types of security tool.

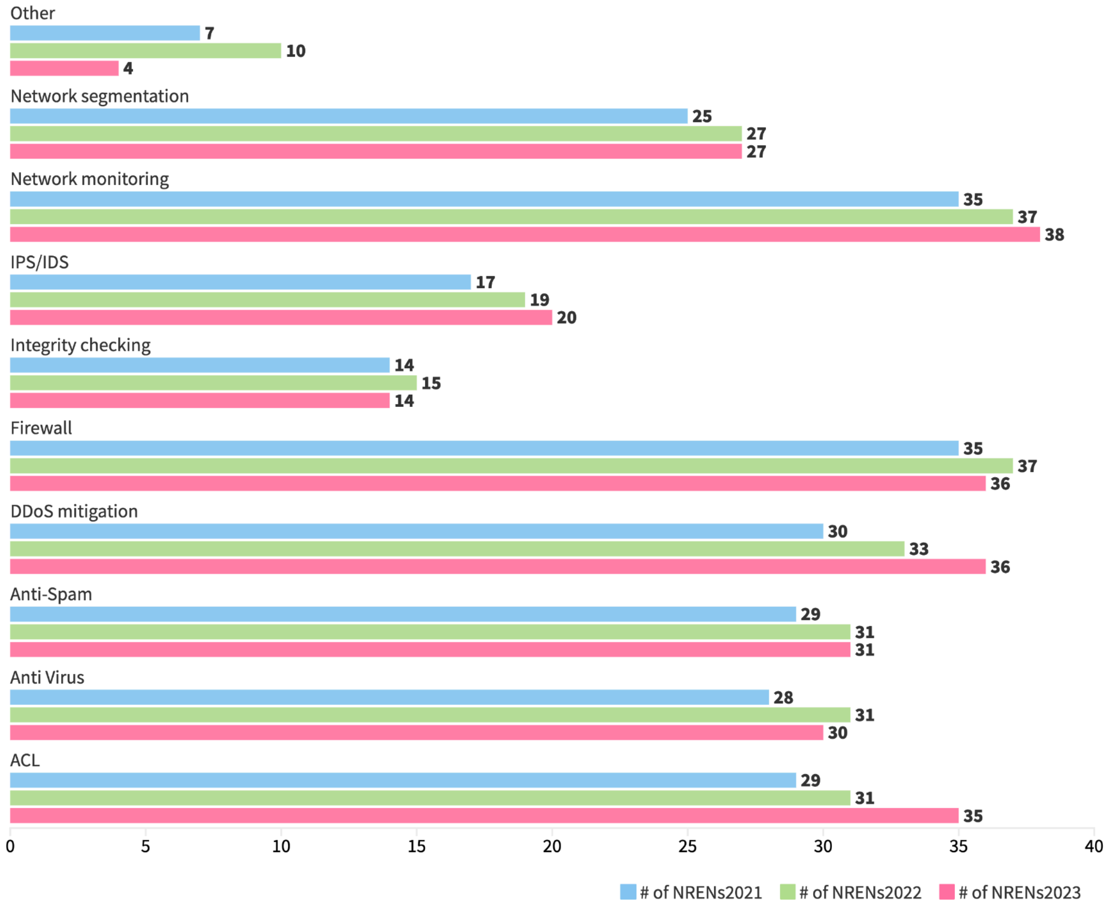


Figure 6.6: Cyber-security tools used by NRENs. *The bars indicate how many NRENs are using this particular type of security tool.*

6.2. Security Services

As service provider and ICT experts, NRENs are also well placed to provide cyber-security services to their customers. Therefore, many NRENs also offer services to support their users' ICT security. This can mean technical services but also providing advice to users – an overview can be found in Figure 6.7.

[54] A plausible case for NRENs genuinely not using such tools would be if an NREN is part of a larger organisation that is providing the cover for the NREN. This is likely the case for NRENs such as AzScienceNet (part of the Azeri Academy of Science), FCCN (which is part of the larger research organisation FCT) and the Maltese NREN (part of the University of Malta).

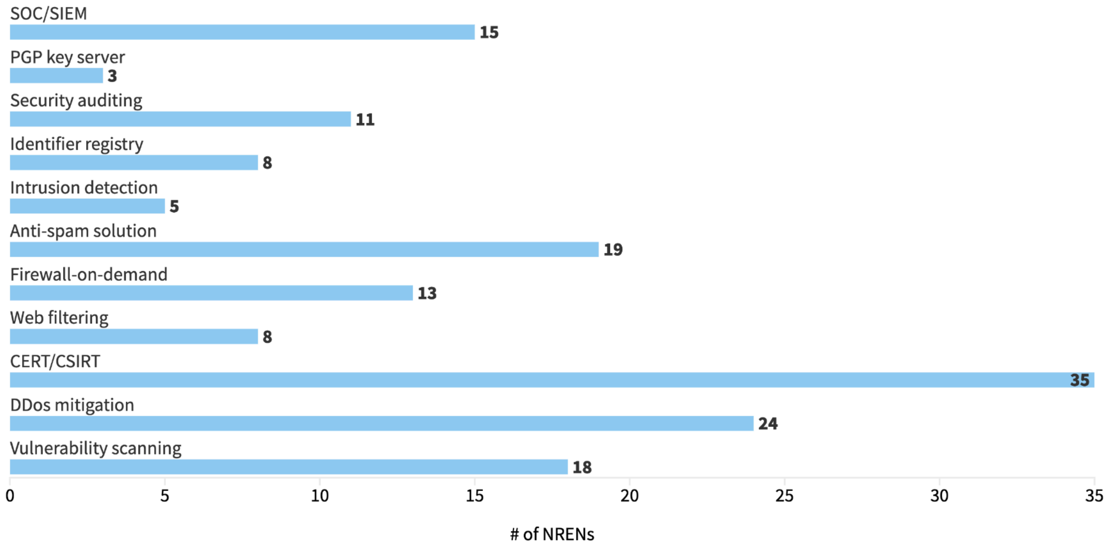


Figure 6.7: Security services offered by NRENs to their users

An important development in this area is the increase in the use of SOC/SIEM tools that has already been mentioned above. Currently, 15 NRENs have reported running a full SOC[55]. This is a major effort and involves considerable resources, which means it is not a service that every NREN will be able to offer. Some CSIRT services are gradually growing into SOC services. SOC services are a major subject in the current GN5-1 project.

Another upcoming service is eduVPN. The COVID-19 pandemic has sped up the adoption of eduVPN both by NRENs and directly by universities. eduVPN gives the NREN/university the opportunity to offer state-of-the-art, privacy-preserving VPN services to large numbers of users[56].

In recent discussions with the NRENs, more interest has been shown in security intelligence sharing, DDoS mitigation, business continuity and crisis management, as illustrated, for example, by the continuous demand for crisis management events such as CLAW.

Some security-related services for the NREN community are provided by GÉANT, notably Trusted Certificate Service (TCS)[57], which is currently used by 35 NRENs, and Firewall on Demand (FoD), currently used by 30 NRENs.

6.3. Security Readiness among NRENs

Security for NRENs is a dynamic field, not least due to regulatory requirements that have developed in the past years. This is exemplified in the increasing importance of the Network and Information Security Directive (NIS2) and security certifications such as ISO 27001. NRENs have moved to adapt to these challenges at different paces, resulting in a security landscape within the GÉANT community that is very diverse. The current state of these developments was assessed in a series of interviews, whose results are summarised in this section.

[55] ACOnet, AMRES, CARNET, CESNET, DeIC, DFN, GRNET S.A., Jisc, LITNET, RENATER, RESTENA, RoEduNet, Sikt, SURF and SWITCH. The most common system used is Splunk (4).

[56] eduVPN is currently offered by 12 European NRENs and tested or piloted by 7 more. It is also used by more than 100 universities worldwide.

[57] TCS takes advantage of a bulk purchasing arrangement which allows participating NRENs to issue almost unlimited numbers of certificates provided by Sectigo, a commercial certification authority (CA).

As mentioned in the previous paragraph, the approach taken, and the progress made, in implementing the NIS2 Directive varies considerably between NRENs. While some NRENs prepare to comply with regulations by taking steps such as ISO certification, others align themselves with government regulations. However, there are still some who remain uninformed about their scope and the requirements regarding NIS2. This diversity reflects the complexities surrounding NIS2 compliance. These arise from uncertainty regarding the potential consequences for an NREN if its members were to fall under the NIS2 Directive (supply-chain effect) or complications that may arise if an NREN also provides services in other sectors such as to (academic) hospitals and to government agencies.

Different approaches to security standards and compliance are also reflected in the diversity of certification processes among NRENs. Some NRENs are already certified, others are in the process of certification, and some have not obtained any formal certification. However, even without formal certification, many NRENs adhere to ISO 27001 standards or best security management practices. Generally, NRENs remain confident in their ability to comply with regulatory requirements such as NIS2.

Another important pillar of organisational security is the structure of the security teams within the NRENs. Again, this varies considerably between NRENs, including security teams of different sizes and whether the NRENs have a Chief Information Security Officer (CISO) or a similar position. Direct comparisons between NRENs here are difficult for a number of reasons – one being that in some NRENs network security is the responsibility of the network team rather than the dedicated security team, another being that NRENs themselves vary widely in size and resources. The latter means naked numbers do not tell the full story - however, naked numbers give a feel for the diversity: commonly, security teams comprise fewer than 10 people, but in some NRENs up to or more than 50 staff are part of the security team.

Notwithstanding such exceptions, many NRENs report resource constraints, such as limited staff and support, that hinder their ability to improve security measures. CISOs also commonly struggle to find the time and means to effectively share information and learn from peers. On the positive side, there is a strong sense of trust and cooperation among member NRENs, allowing open conversations about security challenges which in turn help to provide support. Close cooperation between some NRENs and their member universities is proving effective in dealing with security incidents quickly and efficiently, with some NRENs even taking responsibility for monitoring university networks and sending out alerts when vulnerabilities are detected.

6.4. Security Community Groups

As with other areas of general interest to the community, NRENs meet in regular groups to discuss, share and increase their knowledge on security best practice. For security, there is a Special Interest Group (SIG) and a Task Force (TF), as detailed below:

- **Special Interest Group on Information Security Management (SIG-ISM).** SIG-ISM offers Chief Information Security Officers (CISOs) of NREN organisations the opportunity to share best practice and learn from each other's experience of safeguarding their networks against security incidents and threats. Taking part in SIG-ISM can help equip NRENs with the skills to manage information security within their research and education community. Between a third and a half of GÉANT NRENs are actively involved in SIG-ISM.

- **Task Force on Computer Security Incident Response Teams (TF-CSIRT).** TF-CSIRT provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination[58]. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards. The Task Force also develops and provides services for CSIRTs, promotes the use of common standards and procedures for handling security incidents, and coordinates joint initiatives where appropriate. This includes the training of CSIRT staff and assisting in the establishment and development of new CSIRTs. As with SIG-ISM, between a third and a half of GÉANT NRENs are actively involved in TF-CSIRT, which means that not all European NRENs with TI-listed CSIRTs participate regularly.

6.5. Network Security - RPKI

While most of this section has dealt with the organisational security of the NRENs and security services, NRENs as ISPs are also in charge of the security of their networks within the wider Internet. The Internet is organised as a network of smaller networks, called autonomous systems (ASs), typically run by Internet service providers (importantly including NRENs) or other large organisations. Each of these ASs has been assigned blocks of IP addresses which are unique to them.

When data are sent across the Internet, they come from one IP address and go to another, often hopping across multiple ASs. This routing is done using the Border Gateway Protocol (BGP), which serves as a sort of postal service for the Internet. However, without any additional measures, BGP takes any IP address at face value, which means inadvertent errors or deliberate fakes by malicious actors (BGP leaks or hijacking, respectively) can potentially reroute Internet traffic, creating a security problem. Resource Public Key Infrastructure (RPKI) is a security framework that seeks to remedy this problem by using cryptographically signed records called Route Origin Authorisations (ROAs) to validate which network operator is allowed to announce which IP addresses. This ensures that only authorised parties are announcing a given IP address.

Currently, many ASs have not implemented RPKI for all of their IP addresses, which means only a percentage of routings is actually secured against BGP leaks/hijacking. There is, however, an increasing pressure on major ISPs (including NRENs) to implement RPKI to close this security gap. This large push by the Internet community is causing more and more organisations to acquire ROAs for their IP address block. Table 6.1 below shows the current state among the NRENs on implementing RPKI by indicating the share of ROA-signed routings.

[58] It is notable that members of TF-CSIRT include not only NRENs but also R&E institutions and commercial organisations. To reflect this diversity, the TF-CSIRT community has decided to move into a more independent position; GÉANT will continue to support and promote TF-CSIRT.

NREN	RPKI valid	NREN	RPKI valid	NREN	RPKI valid
ACOnet	26%	FCCN	100%	RENAM	89%
AMRES	0%	GARR	80%	RENATER	50%
ARNES	94%	GRENA	95%	RESTENA	86%
ASNET-AM	0%	GRNET	77%	RHnet	100%
AzScienceNet	0%	HEAnet	94%	RoEduNet	13%
Belnet	20%	IUCC	95%	SANET	25%
BREN	0%	Jisc	13%	Sikt	0%
CARNET	63%	KIFÜ	45%	SUNET	61%
CESNET	90%	LITNET	80%	SURF	87%
CSC	29%	MARNet	0%	SWITCH	82%
CyNet	100%	MREN	0%	ULAKBIM	100%
DeIC	78%	PIONIER	0%	UoM	29%
DFN	67%	RASH	100%	URAN	100%
EEnet	100%	RedIRIS	37%		

Table 6.1: Percentage of routings secured by RPKI

6.6. Summary

The focus on security keeps growing and recent geopolitical developments show that now there is not only cyber crime to worry about: state-sponsored, politically motivated threats are real and visible in day-to-day life[59].

Security-related activities include policies and training as well as technical measures, all of which have to be addressed. While NRENs are working to fulfil these requirements, the status of these efforts varies considerably, even with regard to the security readiness of the NREN organisations and networks themselves. The security of their users is another area in which NRENs could play an important role – but not all NRENs will move into this area. For example, while a sizeable number of NRENs now offer sophisticated services such as SOC/SIEM systems and/or offer consultancy or training to their users, a majority of NRENs do not and might never expand their service portfolio in a similar way. The NREN community can help to close such gaps to a certain point – a good example for this would be the existence of CSIRTs across almost all NRENs, and also the option for NRENs to acquire some security services from the GÉANT service portfolio.

[59] Russia's invasion of Ukraine in 2022 and the international sanctions have implications of an unprecedented nature [NCSC_Advice].

7. TRUST AND IDENTITY

The Trust and Identity services delivered by National Research and Education Networks (NRENs) and GÉANT are striving towards an omnipresent authentication and authorisation infrastructure (AAI) for the research and education community[60]. Mirroring the comprehensive reach of network provision, AAI is becoming a cornerstone of the GÉANT programme, ensuring it is accessible to every user within the academic and research sphere in Europe as shown in Figure 7.1. It provides a pervasive, secure, interoperable and sustainable trust fabric, seamlessly integrated with the technological advancements, that supports and empowers a wide array of scholarly and research activities, fostering collaboration and innovation across Europe and beyond.

IdPs, SPs and Identity Federations

Identity providers (IdPs) provide users with digital identities that enable authentication to take place. At any request for authentication of the user (log in), the IdP provides the information necessary to identify the user and her/his privileges.

Service providers (SPs) are any providers of services to users. Typical services include e-journal access; access to e-learning platforms; access to collaborative tools, such as wikis; access to storage and cloud services, and to more complex services required for science.

An identity federation is a framework of common identity security standards and protocols which allow the use of user identities across different identity management systems (hence the name "federation"). SPs in a federation can use IdPs in the same federation to authenticate users, which minimises the amount of user management they have to perform. This enables a user registered in the identity management system of, e.g., a university to access services provided either by that university or by other institutions participating in the identity federation.

Building on the foundation of national identity federations and eduGAIN, more complex services can be created to support EOSC requirements (see Section 4 Involvement in EC-Funded Projects) or GÉANT services such as InAcademia or eduTEAMs.

The GÉANT Core AAI Platform[61], building upon the eduGAIN trust fabric, is integral to support GÉANT NREN infrastructures, High Performance Computing, European Research Infrastructures and Education. This integration ensures a cohesive user experience and streamline access to resources, driving forward the capabilities and the reach of digital identity and access management across Europe's academic and scientific landscapes. The platform will be instrumental in enabling GÉANT and NRENs to deliver a spectrum of value-added services, fostering a more innovative, secure, and collaborative environment within the research and education sectors.

[60] The Research and Education Federations group (REFEDS) is a worldwide association, supported by GÉANT, the eduGAIN secretariat and the eduroam secretariat. The data presented here reflect this global nature, not just the use of eduroam and eduGAIN use among the European NRENs. Unlike the rest of this report, numbers here report on global uptake and use.

[61] Because the survey was conducted in 2023 and focuses on the time period from January to December 2022, before the renaming/rebranding of eduTEAMS to Core AAI platform was underway, and because the process is not yet complete, both terms, Core AAI Platform and eduTEAMS, are use in this text.

This section outlines the NRENs' and GÉANT's involvement in the following T&I initiatives and services:

- REFEDS
- eduGAIN
- eduroam
- Core AAI Platform
- MyAccessID
- MyAcademicID
- GÉANT AAI service
- EOSC AAI
- eduTEAMS
- InAcademia

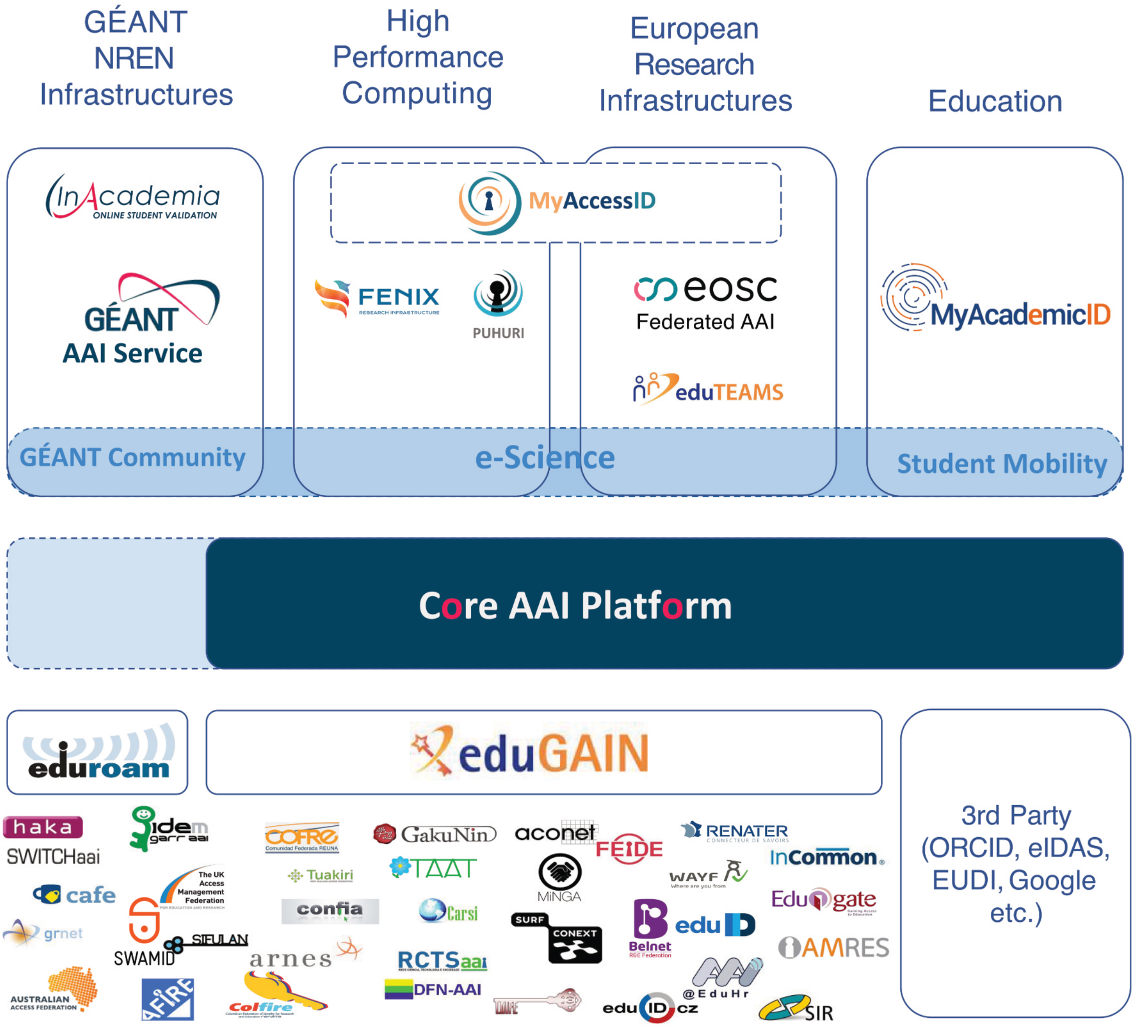

GÉANT NREN Infrastructures
High Performance Computing
European Research Infrastructures
Education
InAcademia ONLINE STUDENT VALIDATION
GÉANT AAI Service
MyAccessID
FENIX
PUHURI
eosc Federated AAI
eduTEAMS
MyAcademicID
GÉANT Community
e-Science
Student Mobility
Core AAI Platform
eduroam
eduGAIN
3rd Party (ORCID, eIDAS, EUDI, Google etc.)

Figure 7.1: GÉANT's Trust and Identity services in the R&E ecosystem

7.1. REFEDS

The Research and Education Federations group (REFEDS) brings together identity federations across the globe to share experience and define common practice.

As shown in Figure 7.2, in 2023 there were 87 known research and education federations worldwide (the same as in 2022), 79 of which are part of eduGAIN (up from 74 in 2022) (see Section 7.2 below). Most of the identity federations are operated by NRENs, though at least some are brokered by other non-commercial entities. Within Europe, there are 42 REFEDS members and, except for one, all of them are operated by NRENs[62].

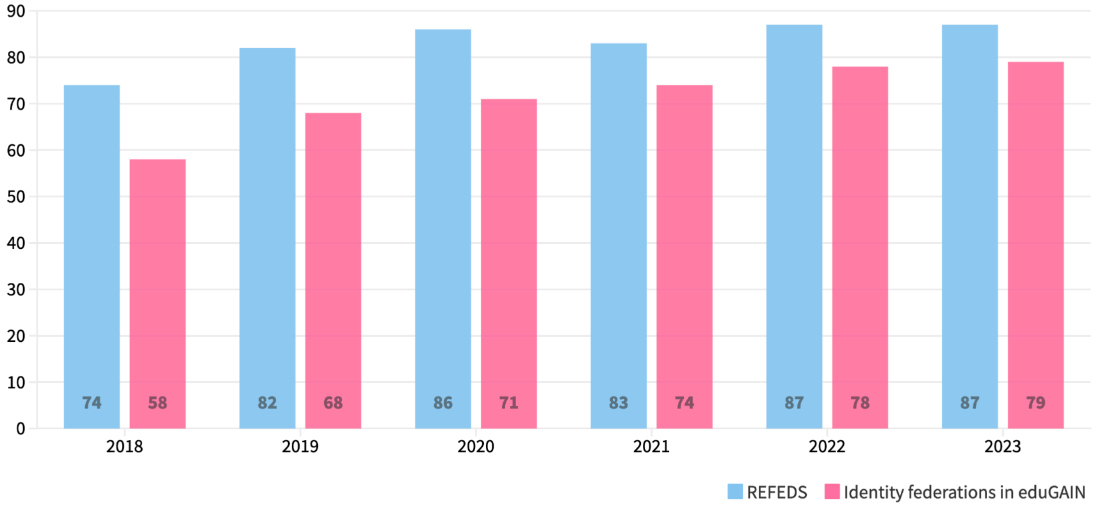


Figure 7.2: Number of known REFEDS members and number of identity federations using the eduGAIN service 2018–2023. *Note that all identity federations in eduGAIN participate in REFEDS but not vice versa. Federations will join REFEDS early on in their development process and before they reach the maturity needed to join eduGAIN, so REFEDS participation can be considered a pipeline to eduGAIN participation.*

Security and Privacy Aspects

Running authentication and authorisation infrastructure (AAI) incurs security challenges. A measure of the preparedness of REFEDS members to deal with actual incidents is their adoption of the Security Incident Response Trust Framework for Federated Identity (Sirtfi – see the next section and also Section 7.2 eduGAIN below). To support the need to use only relevant user information in authentications and to use this data sparsely, REFEDS has conceived the Research and Scholarship (R&S) attribute release specification as a simple and scalable way for identity providers to release minimal amounts of required personal data to service providers serving the research and education community. Finally, the REFEDS Code of Conduct (CoCo) is a set of rules intended to ensure that service provider organisations have taken measures to properly protect the attributes in line with regulatory requirements. These three aspects are explored in more detail below.

Sirtfi

The Security Incident Response Trust Framework for Federated Identity, or Sirtfi, aims to enable the coordination of incident responses across federated organisations, thereby defining a baseline for security incident response capabilities.

[62] In Croatia, AAI@EduHr is operated by the University Computing Centre of the University of Zagreb; another peculiarity is WAYF, which is operated by the Danish NREN DeIC but which also covers Iceland and Greenland. More information on REFEDS can be found at [REFEDS].

Attribute Release Specifications and Code of Conduct

In a federated identity management system, the identity of the user is validated by the identity provider (IdP). If the authentication succeeds, the IdP will release some information (attributes) about the user to the service that initiated the authentication request. The service provider (SP) will use the information to authorise the use of the service. In order to comply with data protection regulations, SPs are recommended to request only the minimum set of attributes required to deliver the service. To support this process, the REFEDS community has defined specifications with the aim of automating the release of the attributes. One such specification is the Research and Scholarship entity for services (R&S), which enables the automatic release of a limited, specific set of attributes to services that operate in the research and education sector. To facilitate the release of attributes, REFEDS, in collaboration with eduGAIN, has also defined the Data Privacy Code of Conduct (CoCo). Service providers are encouraged to declare compliance with CoCo, that is, to follow the principles of data minimisation and of attributes processing as defined in CoCo[63].

Adoption of REFEDS' R&S and CoCo is only recommended, not mandatory, and only a (growing) minority of service providers in the federations that responded to the REFEDS survey comply with these standards.

To date, the release of attributes remains problematic because services in eduGAIN have no confidence in what attributes they may or may not receive, as this is determined by the identity providers. This can have an impact on the user's experience, as they may not be able to access their desired service.

7.2. eduGAIN

eduGAIN is a key service supporting the increasingly borderless education and research sector by providing international interfederation to connect national identity federations [eduGAIN]. eduGAIN is the trust anchor between the service and identity providers of participating federations and facilitates technical interoperability, ultimately enabling the secure exchange of identity information between the entities. This allows higher education institutions to offer a wider portfolio of services (those in eduGAIN) to their users: eduGAIN enables users from one federation to access services from other federations and enables services offered in one federation to be accessed by users from other federations.

Established research and education identity federations worldwide participate in eduGAIN (Figure 7.3; note, though, that most, but not all, identity federations are in eduGAIN). As the service has matured, the number of identity providers and service providers added by federations has increased dramatically from about 5,000 entities in 2018 to more than 9,000 in 2023 (Figure 7.3).

As the membership of eduGAIN and the number of entities within the service has continued to grow, it was time to run a check on whether this foundation was still strong enough. Using the REFEDS Identity Federation Baseline Expectations white paper as a starting point [REFEDS_BE], the eduGAIN Futures Working Group set out to identify room for improvement and created a set of recommendations for the service [eduGAIN_FWGR]. One aspect that was identified for improvement was the governance structure and to make that possible the eduGAIN Constitution needed to be changed. After consulting the broader community, the

[63] A revision of CoCo started in 2020, to align it with the GDPR and to seek formal approval by the European Data Protection Board (EDPB). The new CoCo (v. 2.0) was approved by the REFEDS Steering Committee in March 2022. More information on R&S and CoCo can be found at [REFEDS_R&S] and [CoCo] respectively.

future governance structure will rely on a small, elected Steering Committee and a larger assembly consisting of the eduGAIN Delegates and Deputies (i.e. the representatives of the member federations). The assembly will have an oversight role within the service. The proposal has been approved and the new eduGAIN Constitution will become effective in 2024.

The first task of the Steering Committee will be to prioritise the other recommendations of the eduGAIN Futures Working Group, such as updating the service model, implementing a baseline for federation operators and monitoring emerging technologies and their interaction with eduGAIN.
The service continues to mature and expand its core competencies. The eduGAIN CSIRT provides a central coordination point at the interfederation level for security incident responses. The eduGAIN training team continues to improve NREN competences to establish and operate identity federations, resulting in new federations being formed and joining eduGAIN. The eduGAIN operational model is being revised striving for higher reliability and to ensure sustainability. Due to the emergence of decentralised, wallet-based ecosystems, an eduGAIN trust framework based on the OpenID federation protocol is being explored and a proof-of-concept activity is envisaged for 2024.

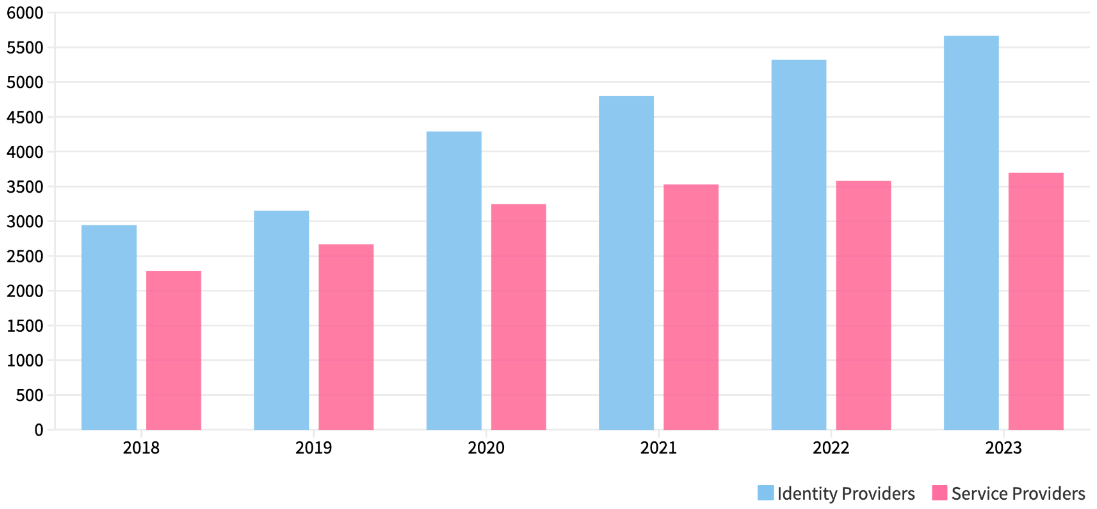


Figure 7.3: IdPs and SPs that are part of the eduGAIN service. *The numbers have increased considerably over the years, with varying but overall impressive growth rates until 2023, when an increasing trend in creating service gateways that host multiple services, but are represented as single entity in the federations, has been observed (increase of IdPs 2018/19: 7%; 2019/2020: 36%; 2020/2021: 12%; 2021/2022: 11%; 2022/2023: 6%; increase of SPs 2018/19: 17%; 2019/2020: 22%; 2020/2021: 9%; 2021/2022: 1%; 2022/2023: 3%.*

7.3. eduroam

eduroam is a Wi-Fi roaming service that gives users seamless Internet connectivity both within their home campus and at other participating institutions [eduroam]. eduroam is a global collaboration between thousands of institutions. In Europe, the national and international operation of this infrastructure is undertaken respectively by the Roaming Operators (ROs) and a central eduroam Operational Team funded by the GÉANT project.

Since its inception in 2003, eduroam has expanded enormously and is now available in 104 territories. Globally, the service is delivered by regional confederations. The European service is operated by GÉANT for members of the European eduroam federation. This alliance comprises autonomous roaming services who agree to a set of defined organisational and technical requirements that ultimately constitute eduroam.

eduroam is present in all European countries, and its usage is growing, with most authentications happening nationally (Figure 7.4). In 2023 both international and national eduroam traffic has recorded approximately 20% growth compared with 2022. For comparison, data for 2021 are also included, when traffic was clearly influenced by significantly less study, travel and movement activities due to the COVID-19 pandemic.

eduroam continued engagement with OpenRoaming [OpenRoaming], to widen the footprint of eduroam access locations to spaces other than academic institutions and positively influence eduroam usage and traffic. The latest developments concentrate on improving the support for user onboarding of eduroam and OpenRoaming, while also providing new managed services for service providers (SPs) and identity providers (IdPs). One notable collaboration involves partnering with the geteduroam project [geteduroam]. The geteduroam project provides apps and managed IdP features and integrates with the services from the central Operational Team.

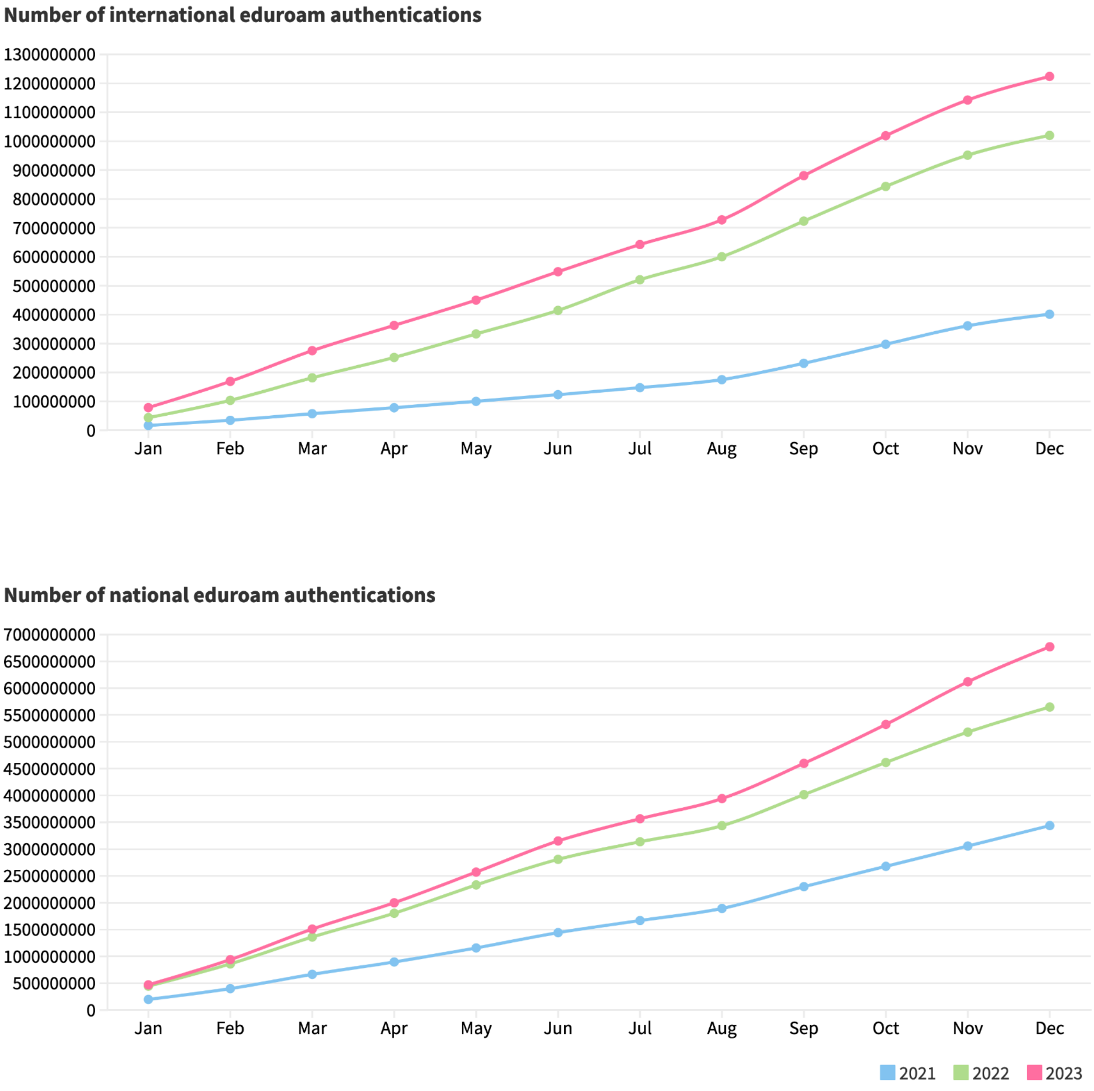


__Figure 7.4: Authentications by eduroam month on month for the years 2021–2023.__ The majority of authentications happen nationally, i.e. within the same country (bottom graph), while international authentications (e.g. visiting scholars, exchange students, etc.) are considerably lower, making up about 15% of authentications in 2023 (top graph). A post-COVID-19 effect is evident in 2022 as recovery of both national and international traffic is tracked, with an approximately 70% increase compared with 2021 and 20% growth between 2022 and 2023.

7.4. Core AAI Platform

The GÉANT Core AAI Platform is envisioned to be a cornerstone in the landscape of advanced research and education, providing the critical infrastructure for key European initiatives such as the European Open Science Cloud (EOSC) AAI, EuroHPC and programmes supporting student mobility across the continent. It serves as the foundational backbone for a suite of essential identity services, including InAcademia, MyAcademicID, MyAccessID, and the EOSC Federated AAI, enabling the delivery of an omnipresent AAI to the NREN infrastructures, the High-Performance Computing area, European Research Infrastructures, and the broader education sector.

The evolution of the GÉANT Core AAI Platform represents a stride towards a more integrated, secure, and user-centric digital infrastructure for the European R&E community. As the needs of this community grow increasingly complex, the platform's role in simplifying, securing, and scaling service delivery becomes ever more critical, cementing GÉANT's position as a leader in digital identity services for R&E on a global scale.

The strategic design of the Core AAI Platform, with its clear demarcation from the AAI services layered above, is set to provide a dual evolution path, ensuring that each can progress in its domain without impeding the other. This separation enables AAI services to innovate and grow independently, fostering the development of distinct business models and service offerings that still rest on a robust and enduring technological base. Such a foundational separation is poised to maximise both agility and stability within GÉANT's service ecosystem, supporting a diverse and dynamic environment for R&E advancements, with the end goal of providing a converged user experience.

7.5. MyAccessID

MyAccessID [MyAccessID] is establishing itself as an identity layer within the High-Performance Computing ecosystem, being used by Puhuri for access to LUMI HPC [Puhuri] and by FENIX for access to federated HPC resources in Europe [FENIX]. Its essential role has been further solidified by the EuroHPC Joint Undertaking's tender call in 2023, which stipulates that the EuroHPC Federated Platform must utilise MyAccessID. The MyAccessID model, strategically designed to integrate infrastructure service domains rather than individual services, offers a scalable and robust framework that is conducive to the sustained expansion of service use cases.

This is a considerable leap forward; however, to fully realise the ambition of creating an omnipresent AAI for the research and education sector, continued efforts and developments are necessary. MyAccessID spearheads a number of innovations that were introduced in the AARC Blueprint Architecture and which are first implemented by the Core AAI Platform. Support for compensating identity vetting controls and second factor authentication capabilities were designed, while support for a new paradigm of terminal access via SSH, critical for a large number of scientific use cases, was in pilot in 2023.

7.6. MyAcademicID

Student mobility has become a very important and strategic area for the NRENs and GÉANT, in light also of its higher importance at European level. The European Commission is supporting the digital transformation of the Erasmus+ programme [Erasmus+] via the European Student Card Initiative [ESCI] and via dedicated projects funded under the Connecting Europe Facility (CEF) programmes [CEF]. GÉANT and the European NRENs have been particularly active in this space since 2019.

GÉANT continues the MyAcademicID project [MyAcademicID], which aims to design and deploy a platform to enable electronic identification (eID) and authentication of higher education students through a single European student eID scheme. The European Student eID for Higher Education is the result of the integration of eduGAIN, eIDAS (the EU regulation on electronic identification and trust services for electronic transactions in the European Single Market [eIDAS]) and the European Student Identifier (ESI), a digital identifier to uniquely identify students when they access student mobility services online; the ESI is released by the higher education institutions the students belong to.

7.7. GÉANT AAI Service

The GÉANT AAI Service, previously known as GÉANT SP Proxy, is a service that allows GÉANT services to use federated authentication for identifying users from eduGAIN [GN_AAI]. The work to migrate the existing service to the new GÉANT SP proxy based on the Core AAI Platform started during GN4-3. This enabled the service to offer a wide range of new capabilities, such as support for OpenID Connect, enhanced user and group management, support for the AARC Blueprint Architecture and EOSC readiness. This migration was completed in early 2024, replacing the GÉANT Central Access Management System (CAMS) as well, and enabling all of the GÉANT services to now utilise an AAI system based on Core AAI Platform.

7.8. EOSC AAI

The goal for the EOSC AAI is to provide the trust mortar with which to join the many bricks of the current set of scientific communities, collaborations and infrastructures together [EOSC_AAI]. The EOSC AAI is comprised of the AAIs of the Science Clusters, Research Infrastructures and e-Infrastructure Providers, which are being brought together through the EOSC AAI Federation. The EOSC AAI Federation is fully operational with EOSC AAI e-infrastructure SP-proxies and cluster community AAIs fully integrated to EOSC AAI Federation.

7.9. eduTEAMS

eduTEAMS has been a trailblazer in implementing advanced AAI services tailored for long-tail research collaborations, following the AARC Blueprint Architecture. It operates with two distinct business models: eduTEAMS Shared and eduTEAMS Dedicated. eduTEAMS focus was on enhancing its community, collaboration, and group management features.
The eduTEAMS service has evolved into the Core AAI Platform (see Section 7.4). Initially delivered as an Identity and Access Management (IAM) solution, it experienced significant growth, leading to the creation of various AAI service implementations. This expansion prompted a transformation into the Core AAI Platform during the initial phase of the GN5-1 project. This shift allows a separate focus on platform evolution and service development, providing flexibility for customisation and ensuring a streamlined user experience built on top of the globally recognised identity federation infrastructure eduGAIN.

7.10. InAcademia

InAcademia is a service that allows online retailers to easily validate whether a customer is a student or otherwise affiliated to an education institute [InAcademia]. It performs this service by asking users to authenticate at participating identity providers available in eduGAIN. It offers an OIDC protocol interfaced service proxy that connects online retailers with the SAML protocol to connect to institutions in eduGAIN and R&E federations, which releases the necessary attributes for InAcademia to determine whether a user is a student. The InAcademia service is available in two service offerings: "Commercial" for online retailers that profit from offering paid-for services to users and "Community" for services that are not for profit but only need a simple validation of affiliation.

End users and identity providers benefit from InAcademia as it acts as a privacy-preserving layer to validate the user's affiliation, compared with alternative methods that might expose more personal information to the retailer than is necessary, such as asking users to upload personal documents and as an alternative to direct federation membership. Identity federations are encouraged to actively participate in promoting InAcademia to their constituents and are invited to participate in the InAcademia Steering Committee when the service becomes operational in their country. The InAcademia support model relies on collaboration with federations operators to optimise attribute release.

In 2023, the service has continued to grow, with almost 3 million validations processed in 2023, contributing to its established revenue stream of income from commercial merchants using InAcademia. Eligible users in the Netherlands, Germany, Denmark, Spain, France, Italy, Sweden, Turkey, Austria, Iceland and Finland can now protect their privacy when registering for a wide range of well-known global brands or when signing up to one of the world's largest student marketplace platforms.

7.11. Summary

Trust and identity has been at the heart of the NREN world for a long time, and the scope of the projects and initiatives discussed in this section illustrates that the utility and importance of the T&I field for the R&E community is constantly increasing. It is also clear that more recent services, such as those built on top of the Core AAI Platform and on pre-existing T&I trust frameworks and infrastructures such as eduGAIN and eduroam, in turn make the latter business proposition more attractive and creates a kind of virtuous cycle.

New developments in the area of EUDI wallets are creating a huge potential for the eduGAIN trust framework to become a part of this new paradigm. While the EUDI wallets might carry the high-level assurance identity, the academic sector remains well placed to provide specific credentials such as the academic affiliation or education credentials. This means that supporting OpenID in eduGAIN and the Core AAI Platform would be beneficial and work started in 2023 to explore an OpenID federation in eduGAIN and OpenID capabilities for verifiable credentials issuance and presentation in the Core AAI Platform. GÉANT, alongside NRENs, will be pivotal in providing the trust fabric that ensures the security and authenticity of educational credentials within this framework. Amidst intense competition in the digital wallet space, the trust and reliability offered by GÉANT and NRENs will be crucial.

8. CLOUD SERVICES

The previous four years (2020–2023) have seen an incredible acceleration in the development and adoption of advanced digital services and platforms, and demand for high-quality and high-performance digital services in R&E is here to stay. As the IT service facilitators for R&E, NRENs have the opportunity and the responsibility to continuously drive towards ensuring the best value of the services provided to research and education institutions. This will require a reassessment and recalibration of where the finite R&E resources are best applied to maximise the outcomes of the GÉANT community's research and education efforts to match their communities' needs. The COVID-19 pandemic demonstrated the value of digital online services and communications platforms in enabling distributed collaboration – in short, of cloud-based services.

Cloud Services Delivery

There are three types of cloud services delivery:

***Private cloud**, where an organisation provides a cloud service to its own staff only, and with no associated billing. This is the simplest delivery type in terms of access management and business model and can be highly tuned for a specific set of known use cases.*

***Community cloud**, offered to a wider target "community", allows resource sharing between participating organisations and easy data collaboration across a greater number of users. This sets a higher standard for access management, but the financial model is most frequently organised around in-kind contribution of member organisations, or third-party/public funding. The best community cloud services offer added value specific to their target community.*

***Public cloud** describes commercial services available to everyone on the open market. They are typically operated in large data centres that benefit from effects of scale to reduce the infrastructure overhead payable by each user, as well as enabling "as-a-service" business models permitting each individual user a great flexibility in varying their resource usage over time. In turn, there are extremely high requirements for robust access control and security mechanisms and other "cost of doing business" items, as well as a requirement to support a great variety of use cases. Successful public cloud providers have the financial and organisational resources and a strong incentive to develop their cloud service portfolio on an ongoing basis to cover a large variety of user requirements at a very high level.*

Similar priorities have been expressed within the NREN community. The 2021 GÉANT CTO workshop on Clouds, Collaboration, and Education Services resulted in the production of a roadmap for collective GÉANT community activities on digital services, which prioritised a focus on collective procurement and adoption support for new framework contracts, as well as collective strategy development within the R&E community, to integrate positions on both commercial as well as community-developed services. This informed the project planning for the new GN5-n GÉANT projects, including its current iteration, GN5-1. The roadmap was reaffirmed by the 2022 and 2023 CTO workshops. Partly because of this endorsement, the GÉANT Cloud Framework is being publicly procured for its third iteration, OCRE 2024.

This section provides an overview of the benefits for users presented by cloud services, opportunities for NRENs, feedback from the NREN and R&E community, uptake of the GÉANT Infrastructure as a Service (IaaS) Frameworks, and the conditions determining cloud services adoption.

8.1. Benefits for Users

Individuals and teams benefit from the location-independent use of cloud services. The quality of such services is driven by the degree to which they are developed and operated by providers dedicated to optimising performance, reliability, and feature development of that service. Organisations can benefit from adopting cloud offerings by reducing the need to run local IT services and focusing resources on more specific value-add activities, while at the same time being able to offer their staff more varied, powerful, flexible IT resources at shorter response times and at improved value for money. This shift from offering a select few services completely in-house to offering a larger number of third-party services brings with it a need to manage complexity and dependencies.

8.2. Opportunities for NRENs

While institutions will surely continue to deliver certain specialised or sensitive services to their staff on their own (e.g., via a private cloud model), many individual users are incentivised to use available public cloud services for their work in an individual and ad hoc way, out of a perception of greater accessibility, usability, or performance. This may not be in the best interest of their home institutions, but these may also struggle to offer viable equivalent private cloud services from within their own resources. The NRENs can play one or a combination of several valuable roles in enabling and easing access to community cloud and public cloud services for their institutions. Among those roles are: directly operating and providing cloud resources themselves, facilitating the use of community clouds, and brokering commercial clouds. To further add value to such a service offering, an NREN can become a cloud competence centre for their institutions.

8.2.1. Supply or Facilitate Community Cloud Services

The NREN community members across Europe have a close affinity with IT infrastructure operation for networks and data centres. The resources and the ability exist in the community to build and offer community cloud services to cover a larger target audience than simply the staff of one institution. In any one country, this may either take the form of the NREN or a central institution supplying a community data infrastructure centrally, or the NREN may create a marketplace for individual community cloud offerings from institutions willing to offer use of their resources to peers[64].

The role of an NREN as a full-stack national community cloud provider is, in most cases, reliant on a government-level mandate and corresponding funding and capacity building. Therefore, this path is realistically not available to an NREN purely by its own choice and, given current technology trends, may not materialise in the foreseeable future for any NRENs not already in that role today.

[64] Examples of NRENs offering community cloud services are numerous, though the extent of such services varies considerably. At the upper end would be NRENs such as SWITCH, GRNET or PSNC/PIONIER, with a comprehensive portfolio of cloud-based services, while NRENs such as RESTENA or Belnet offer mostly cloud storage. Other NRENs that offer cloud services of their own are CESNET, AzScienceNet, GARR, GRENA, FCCN, Jisc, SURF, CSC, Sikt, KIFÜ, CARNET and IUCC. Marketplaces where NREN users can offer services to other users have been established by, for example, DFN and SWITCH.

The model of an NREN coordinating a national marketplace for community cloud services offered by individual institutions can be successful in bringing together institutions willing to share their existing services with users looking to avoid operating their own. The service provider institutions grant access to their cloud service to third-party users within the community, to improve the utilisation of their infrastructure and generate some income to offset costs, and a number of small user communities are spared the effort of operating their own local instance. This model, however, faces a challenge often encountered by efforts to share publicly funded resources across funding boundaries, namely the difficulties of building a real business model that includes defining and collecting charges for usage from users outside the scope of the infrastructure funding. That scope may be the national borders, federal state borders within the nation, or even institutional borders. There have been successes with establishing the NREN as a financial clearing house[65], trusted by all parties involved, to handle the financial transactions. What remains, however, is that community cloud services provided by individual institutions struggle with offering sufficient service quality, stability, and scalability to an entire national R&E community for anything more advanced than simple file-sharing.

In previous iterations of the GÉANT project, some work was done to investigate the ambition to develop federation and resource sharing for such national community clouds across the European R&E community [GN4-3_D4.1]. This investigation encountered many challenges surrounding the sharing of publicly funded resources outside the scope of that funding, i.e. across country or state borders. Ultimately, no general-purpose cross-border fee model compliant with legal and funding terms could be developed. For further details, see the GN4-3 deliverable [GN4-3_D4.3].

8.2.2. Brokerage or Procurement Support for Public Clouds

An alternative or complement to community clouds is to establish community-specific environments on top of commodity commercial cloud infrastructures, with the aim to use finite R&E resources to provide more scalable services where the invested manpower and expertise can most optimally improve research and education outcomes for many. An NREN is well placed to facilitate centralised, and therefore efficient, procurement activities for commercial public cloud services on behalf of its community. The pan-European cloud tenders performed by GÉANT in 2016, 2020 and 2024 take this approach one step further, executing pan-European public tenders that provide NRENs with ready-made publicly procured Framework Contracts to make commercial public cloud services available in their country.

Such Framework Contracts do not solve all challenges faced by institutions when adopting cloud services, and the detailed work of developing and implementing a digital transformation strategy remains unique to each institution. However, Frameworks remove a considerable amount of effort and uncertainty from an institution at an early stage of that process. The effort and time saved at institutions across Europe makes the time invested in the GÉANT cloud tender effort well worth it.

8.2.3. Cloud Competence Centre

Independent of direct cloud procurement support activities, NRENs can add tremendous value to their community by collating and drawing together specialist knowledge and circulating experiences, thereby developing into a centre of competence for their community on many subjects (e.g. networking, security, T&I), and so also on matters of cloud usage. A solid

[65] For example, DFN-Cloud "Federated Services", by the German NREN DFN.

base of cloud consulting capability, available to all institutions as they start their journey, is a great asset to the community and a real opportunity for NRENs to establish their status as trusted adviser in digital services.

This was confirmed by NRENs at the strategic cloud and Chief Technology Officer (CTO) discussions in 2022 and 2023, once more ratifying the Cloud Framework part of the 2021 GÉANT Cloud Roadmap. This places a strategic priority on maintaining continuity for the Infrastructure as a Service Plus (IaaS+) Framework by re-tendering in 2024, and on developing a forward-looking NREN strategy on cloud and above-the-net services. Both these objectives are dedicated activities in the GN5-1 project (Work Package 4 Above-the-Net Services). In total, the NRENs, together with their IT partners at institutions, can evolve their role from IT resource operators to include more full-service solution facilitators and thereby keep their value visible to their user communities in an environment of increasing digital transformation[66].

8.3. Community Feedback

Community feedback was gathered via the 2023 GÉANT Cloud Survey for National Research and Education Networks (NRENs) and Research and Education (R&E) institutions. In preparation for the next pan-European tender, the GÉANT Cloud team needed an overview of the R&E community's awareness and use of the GÉANT cloud services, along with institutions' cloud usage plans and future requirements, to learn of obstacles to framework adoption, as well as to gather feedback on what kind of support was most needed and what can be improved or solved in the next tender. The survey indicated a shift towards hybrid cloud usage among respondents, with increased adoption through NRENs, highlighting the necessity for investment in various areas to support the framework utilisation effectively[67].

8.4. Uptake of the GÉANT IaaS Cloud Frameworks

Since 2016, the GÉANT Frameworks for infrastructure clouds (in the following called IaaS) have offered centrally procured commercial cloud services with improved conditions for R&E institutions and have been very successful in fulfilling the demand for such services wherever it was expressed through the NRENs. The 2016 IaaS Framework (2017–2020) saw consistent annual growth throughout its duration (Figure 8.1 below).

The availability of the second-generation Framework for IaaS+ services (infrastructure and beyond) from December 2020 onwards (here termed either IaaS+ or OCRE 2020 Framework)[68] coincides with a dramatic increase in uptake, the annual 2021 spend on both Frameworks almost equalling the total of the preceding four years, as shown in Figure 8.1. The year-on-year growth since then approximates to 50% per annum.

[66] Examples of NRENs that act as cloud competence centres for their users are ACOnet, HEAnet, IUCC, Jisc, Sikt and SURF. In most (but not all) cases, this offer is centred around the IaaS+ Framework.

[67] The 2023 GÉANT Cloud Survey was carried out in March–April 2023, addressing National Research and Education Networks (NRENs) and Research and Education institutions. 137 responses were gathered from 24 European countries. Most respondents (ca 70%) were from large institutions (more than 500 employees), i.e. universities and research institutions. Approximately 80% of all the respondents were from Northern or Western European countries and about 20% from Southern or Eastern European countries.

[68] The tender for the 2020 IaaS+ Framework was run by the Open Clouds for Research Environments (OCRE) project [OCRE].

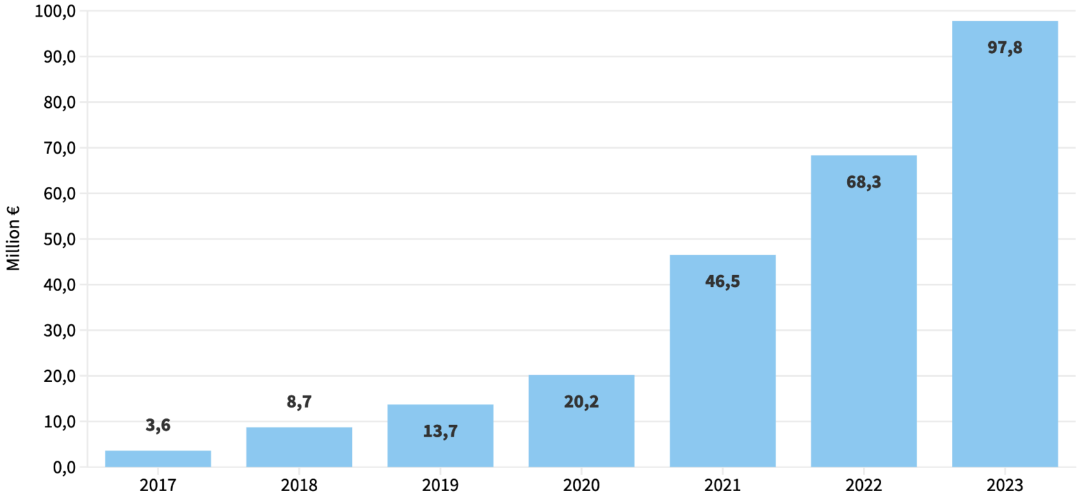


Figure 8.1: Yearly spending via the GÉANT Cloud Frameworks (IaaS 2016 and OCRE 2020) 2017–2023

Moving beyond the initial group of NRENs making up the usage under the first Framework, the growth in consumption under the OCRE 2020 IaaS+ Framework is significantly driven by growth of usage in additional countries. These growth numbers demonstrate national-level cloud procurement aggregation through the Frameworks, indicating the progress that more NRENs are making in becoming cloud procurement pathways for their national communities. Several more countries are making significant steps in growth relative to their previously modest or even non-existent levels of purchasing aggregation. Of the 39 NRENs that joined the 2020 IaaS+ Framework procurement, 28 are in countries fully compliant with the EU Procurement Directive and therefore able to consume with no obstacles. Of these all 28 are reporting Framework usage in 2023, meaning a 100% coverage of the directly addressable market (Figure 8.2). The remainder are mostly in non-EU countries that face some additional procurement challenges around making use of the Framework.

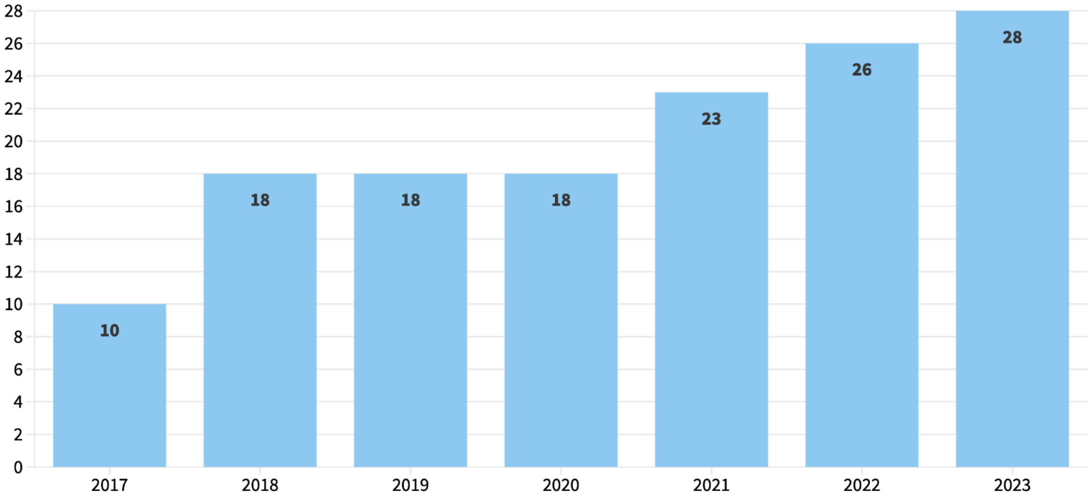


Figure 8.2: Number of countries with active Framework consumption 2017–2023

Those NRENs that are channelling their institutions' cloud purchases through the OCRE Framework are delivering significant value to those institutions in the form of effort and time saved on procurement and access to discounts negotiated by the GÉANT procurement. Cost reductions of this order are unachievable to any single institution, so the Framework is saving taxpayer money across Europe and improving research and education outcomes. The value of the OCRE Framework and the NRENs' value-add is most visible to those institutions that have developed a cloud-inclusive IT procurement and service management practice and can optimally exploit the Framework benefits.

8.5. Conditions Determining Cloud Services Adoption

Despite the continuing digital transformation of workflows across the world, accelerated even more by the pandemic-driven change in patterns of work and mobility, the European research and education institutions are not adopting infrastructure-cloud services at the same rate as other sectors, with some notable exceptions in individual countries. There are several driving and delaying factors at play here, many of them cultural:

Driving Factors

- End-user demand. The capability to deliver state-of-the-art digital experiences quickly and flexibly is becoming a competitive playing field for universities and research institutes looking to recruit top-level talent and to increase the excellence of their graduates and research output. This is a driver particularly towards services with highly developed user interfaces and functional integration. Software (cloud-connected "as-a-service") is the first choice where the desired functionality is available, whereas for flexible and powerful application/research development with low IT-management overhead but maintaining high levels of customisation, Platform as a Service (PaaS) is state of the art, with integrated features such as autoscaling databases, accelerated computing, or machine learning. Older IT paradigms such as virtual machines or container platforms have become infrastructure that end users have little interest in personally interacting with any longer.

- Value. A transition from large one-time hardware purchases to ongoing payment for resources as used ("CAPEX to OPEX" shift) allows more flexible cost/value optimisation. This enables trade-offs of the "time is money" kind to be made, using the elastic nature of large-scale cloud platforms, where more processing resources are always available, for extra cost.

- Legislation and regulations. GDPR issues affect both in-house and externally sourced services, with increasing pressures on in-house-operated services to satisfy, and be certified to, professional IT security standards. This changes the value calculation of on-premises versus cloud, especially when existing local data centres reach their end-of-life and the necessary investment decisions for a replacement are made.

- Multi-cloud. Data and application interoperability and portability between different clouds have come a long way in recent years. De-facto-standard data transfer APIs have emerged, along with platform-abstraction layers such as Kubernetes that allow orchestration and migration of workloads across cloud platforms. The parallel usage of multiple cloud platforms, even within one application, is emerging as the best practice. This capability also enables resilience against instability in any one cloud service platform.

- Scalability/elasticity. As the gap in capacity between locally operated cloud services and hyperscale platforms widens, operators of local resources increasingly face issues in relation to accommodating applications with high short-term resource requirements, making a suitably large-scale and elastic cloud-hosted application platform more attractive for applications with time-variable resource requirements.

Delaying Factors

- Lack of clarity in legislation and regulations (GDPR)

  - Most R&E infrastructure operators consider the legal risks (and necessary efforts) of data protection to be lower for on-premises solutions. With externally sourced services, contracts must be checked and revised, and processes on the supply and demand side have had to be changed. This perceived gap in data protection effort and risk will reduce as requirements around equivalent IT security and certifications are applied more systematically to all data and applications for which institutions are responsible.
  - Schrems II: The CJEU ruling invalidating the US-EU Privacy Shield agreement sparked significant uncertainty about the consequences and risks around the US cloud suppliers' obligation under the US Cloud Act to deliver EU users' data to US authorities under search warrants. To continue to abide by GDPR, EU users of US cloud providers need to take additional measures to satisfy data protection requirements. Community experience shows that this additional effort naturally becomes best practice, as digital transformation matures in the organisation. Meanwhile, the associated public uncertainty and doubt over the issue is slowing adoption of all cloud services, even in clearly legal use cases. The next iteration of the trans-Atlantic agreement is under development, and it remains to be seen how this will affect the community debate in future.

- Difficulty with cost management. R&E institutions and projects mostly work with hard budget caps and specific allocations of budget segments to specific uses. Therefore, there is a conflict with the pay-as-you-go model as the simplest form of cloud consumption, since it causes variable spending and is hard to manage in the context of fixed-time fixed-budget situations. Proper budget planning and consumption monitoring to mitigate this problem is possible but requires specific experience and is therefore a hindrance and risk factor for first-time adopters. However, solutions (technical, organisational, and regulatory) are solidifying.

- Uncertainty and risk aversion. Many institutions are adopting a "me second" approach to cloud adoption – waiting for other institutions to be the leaders. The NREN community will continue to share user experience and coordinate best practice examples to reduce the uncertainty of cloud adoption.

- Data-sovereignty concerns. Not all users and IT decision makers are comfortable with the idea that their data might be stored outside of their "comfort zone", be that their immediate organisation or further afield, even outside their national jurisdiction. In some edge-case legal contexts, a certain physical location and access to hardware infrastructure may still be a legal requirement. These reservations overlap partially with the legal concerns that led to Schrems II (see above).

- Low awareness of the Framework's existence at institutions. Not all NRENs have the resources to advertise the GÉANT IaaS+ Framework widely to their users and consequently the IaaS+ Framework lacks visibility among the institutions in some countries – as does the NRENs' role in making it available. A related problem is that the potential users of these services within the R&E institutions are frequently not the NREN's points of contact. This is a missed opportunity to connect demand with an optimised NREN-community supply, resulting often in small ad hoc cloud procurements by individual user groups, without oversight and at less advantageous conditions.

8.6. Summary

The outreach and requirements gathering on above-the-net services in the NREN community show clearly that many of the target audiences traditionally served by NRENs, with technology building-blocks and back-end services to integrate into in-house-developed service portfolios, are increasingly interested in consuming fully realised integrated services instead. There is a high and rapidly growing demand for state-of-the-art digital services throughout the R&E community, and the cloud model of service delivery plays a valuable and significant part in the service landscape, meriting the close attention of the NREN community. Within institutions, those user groups with existing needs for commodity services (e.g. admin, teaching) are already gravitating towards using Software as a Service (SaaS) tools. Others such as researchers seek greater scalability in infrastructure resources but must maintain a high level of customisability of the running code. These are moving towards Platform as a Service (PaaS) offerings. There is a great opportunity for NRENs to forge a role for themselves in delivering value to their institutions through aggregating demand and centralising effort around facilitating access to cloud resources, either through brokerage or procurement. As demonstrated by the 2022 and 2023 GÉANT CTO workshops and the 2023 GÉANT Cloud Survey, most NRENs recognise and acknowledge this development.

Cloud services developed and operated from within the R&E community can differentiate themselves from generic public services by being highly integrated with the R&E service ecosystem and by addressing community requirements around sovereignty or niche applications not well served by general-purpose cloud providers. However, to achieve the required levels of service quality and performance, a minimum amount of scale will be necessary in the future and the required operating models to achieve this from within the R&E community are not readily accessible to most community members. Work in the community continues to harmonise community- and public-cloud approaches into a unified strategy framework in which NRENs can find their optimal role.

The consumption data for the GÉANT 2016 Cloud Framework and 2020 OCRE Framework show a steady increase in the number of NRENs that report significant uptake by their institutions. The data also show that all 28 NRENs with direct access to the EU Procurement Directive underpinning OCRE are now reporting consumption. This 100% market penetration indicates that these NRENs have the opportunity to orchestrate procurement aggregation activities and demonstrate the value and savings that NRENs can deliver to their communities. Total consumption across all the IaaS+ Frameworks since 2017 has exceeded €260 million as of December 2023. Effort and time saved on individual procurements, as well as a significant percentage in discounts on that sum total across Europe, add up to massive savings of tax money that is available to improve research and education outcomes instead.

9. OUTLOOK

The Compendium's ambition is to provide an overview of and insights into the multi-faceted NREN community. It aims to simultaneously depict the diversity of the NRENs as well as illustrate that, despite their variations and particularities, the European NRENs are built around delivery of the same core, interlinked services.

Changes in the world of NRENs are generally slow but happen on many levels. Some concern the NREN organisations themselves: over the past years several NRENs have gone through reorganisations, in most cases resulting in a larger organisation with responsibilities that extend beyond those of a "typical" NREN. Others reflect the developing needs of the NRENs' users and/or technological possibilities. To track and present such changes, the right parameters need to be assessed. Therefore, a project such as the Compendium needs to expand its scope when necessary, to document developments that shape and alter the ways NRENs are serving their user base.

One recent addition to the Compendium reports on NRENs' activities in the Digital Health sector. While providing connectivity to hospitals has been part of the portfolio of many NRENs for a long time, more recent initiatives at the European level have brought up Digital Health as a possible area for NREN involvement. Future developments here might lead to an expansion of this section.

Examples of trends can also be found among the services that NRENs have been running for a long time – the T&I sector was from the beginning by its very nature an area where NRENs interacted intensely. Out of this, supra-national infrastructures and services have been born that go beyond the activity of individual NRENs. The international integration in this field is continuing – which of course is documented by the Compendium.

While the Compendium is in substantial part based on its eponymous annual Compendium survey, it has always drawn from other data sources, which have become more important over the years. The sections on cloud services and T&I are good examples as they are mostly or entirely based on data that are completely separate from and independent of the Compendium survey. In this way, information from disparate teams/workgroups can be consolidated and made available in one place. However, the use of external data means that they are not always available in time to be included. In the current Compendium Report, the education section that has featured for several years fell victim to this – though it will reappear in future reports. On the other hand, the activities of the security team at GÉANT have provided data that allowed additional parts to be added to the security section. This means that the Compendium continues to provide a platform where results from subject-specific studies from within the NREN community are presented in a summarised form.

For NRENs, the Compendium has often been a source of data they could use for various purposes such as lobbying or benchmarking. While the report format has advantages for such purposes as it provides ready-made figures and analysis, it cannot possibly present all aspects of the data obtained by the survey, and while all those data have – in principle – been available to everyone who asked for them, this was not a convenient way to access the data and few people have made use of this option. To change this inconvenient situation, the team behind the Compendium has been working for some time to make the data from the Compendium survey available online. With the launch of the new Compendium website in the spring of 2024 [Compendium], this has become a reality and the community can now access the data from the Compendium survey online. This also means that it is time to reassess the role of the

Compendium Report. As mentioned above, while the report cannot present all the data as the website can, it can summarise, analyse and provide context for the data in ways the website cannot. So without question, there is value in the report but the team will now review whether the Compendium Report should continue in its current form or whether it should be changed in any way.

A. CONTACT LIST

Table A.1 below lists the RENs and NRENs that responded to the 2023 Compendium survey and contains links to their respective websites (see also [ASSOCIATION].

Short Name	Full Name	Country	Website
ACOnet	Vienna University Computer Centre	Austria	www.aco.net
AMRES/UoB	Akademska mreža Republike Srbije / Univerzitet u Beogradu	Serbia	www.amres.ac.rs
RASH	Academic Network of Albania / Rrjeti Akademik Shqiptar	Albania	www.rash.al/en/
ARNES	Academic and Research Network of Slovenia	Slovenia	www.arnes.si
ASNET-AM	Institute for Informatics and Automation Problems	Armenia	www.asnet.am
AzScienceNet	Institute of Information Technology of the Azerbaijan National Academy of Sciences	Azerbaijan	www.ict.az/en
BASNET	UIIP NASB	Belarus	www.basnet.by/en/
Belnet	Belnet	Belgium	www.belnet.be
BREN	Bulgarian Research and Education Network	Bulgaria	www.bren.bg
CARNET	Hrvatska akademska I istrazivacka mreza	Croatia	www.carnet.hr
CESNET	CESNET, zajmove sdruzeni pravnickych osob	Czech Republic	www.ces.net
CSC/Funet	Finnish University and Research Network	Finland	www.csc.fi/en/
CyNet	Κυπριακο Ερευνητικο και Ακαδημαϊκο Δικτυο (Kypriako Erevnitiko kai Akadimaiko Diktyo)	Cyprus	www.cynet.ac.cy
DeIC	Danish e-infrastructure Cooperation	Denmark	www.deic.dk/en/front
DFN	Verein zur Förderung eines Deutschen Forschungsnetzes e.V.	Germany	www.dfn.de
EENet	EENet, a structural unit of the Department of Technology Management of the Ministry of Education and Research	Estonia	www.eenet.ee
FCT | FCCN	Fundação para a Ciência e a Tecnologia | Computação Cientifica Nacional	Portugal	www.fct.pt
GARR	Consortium GARR	Italy	www.garr.it
GRENA	Georgian Research and Educational Networking Association	Georgia	www.grena.ge
GRNET	Greek Research and Technology Network	Greece	www.grnet.gr
HEAnet	HEAnet Limited	Ireland	www.heanet.ie
LAT	Ministry of Education and Science	Latvia	www.lumii.lv
IUCC	Inter University Computation Centre	Israel	www.iucc.ac.il
Jisc	Jisc Collections and Janet Limited	UK	www.jisc.ac.uk/

Short Name	Full Name	Country	Website
KREN	Kosovo Research and Education Network	Kosovo	www.kren-ks.eu/
LITNET	Kauno Technologijos Universitetas	Lithuania	www.litnet.lt
MARnet	Macedonian Academic and Research Network	Former Yugoslav Republic of Macedonia	www.marnet.mk
MREN	Javna Ustanova Univerziteta Crne Gore Podgorica	Montenegro	www.mren.ac.me
KIFÜ	Kormányzati Informatikai Fejlesztési ÜgynökségNemzeti	Hungary	www.kifu.gov.hu/main-page/
NORDUnet (Representative Member)		Denmark, Finland, Sweden, Norway, Iceland	www.nordu.net
PSNC/PIONIER	Poznan Supercomputing and Networking	Poland	www.man.poznan.pl
RedIRIS/RED.ES	Entidad pública empresarial RED.ES	Spain	www.rediris.es
	Hrvatska akademska I istrazivacka mreza	Croatia	www.carnet.hr
	CESNET, zajmove sdruzeni pravnickych osob	Czech Republic	www.ces.net
CSC/Funet	Finnish University and Research Network	Finland	www.csc.fi/en/
CyNet	Κυπριακο Ερευνητικο και Ακαδημαϊκο δικτυο (Kypriako erevnitiko kai akadimaiko diktyo)	Cyprus	www.cynet.ac.cy
DeIC	Danish e-infrastructure Cooperation	Denmark	www.deic.dk/en/front
DFN	Verein zur Förderung eines Deutschen Forschungsnetzes e.V.	Germany	www.dfn.de
EENet	EENet, a structural unit of the Department of Technology Management of the Ministry of Education and Research	Estonia	www.eenet.ee
FCT | FCCN	Fundação para a Ciência e a Tecnologia | Computação Cientifica Nacional	Portugal	www.fct.pt
GARR	Consortium GARR	Italy	www.garr.it
GRENA	Georgian Research and Educational Networking Association	Georgia	www.grena.ge
GRNET	Greek Research and Technology Network	Greece	www.grnet.gr
HEAnet	HEAnet Limited	Ireland	www.heanet.ie
LAT	Ministry of Education and Science	Latvia	www.lumii.lv
IUCC	Inter University Computation Centre	Israel	www.iucc.ac.il
Jisc	Jisc Collections and Janet Limited	UK	www.jisc.ac.uk/
RENAM	Research and Educational Networking Association of Moldova	Moldova	www.renam.md

Short Name	Full Name	Country	Website
RENATER	Groupement d'Intérêt Public Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche	France	www.renater.fr
RESTENA	Réseau Téléinformatique de l'Education Nationale et de la Recherche	Luxembourg	www.restena.lu
RHnet	Rannsókna og háskólanet Íslands hf.	Iceland	www.rhnet.is/english/
RoEduNet	Agentia de Administrare a Retelei Natinale de Informatica Pentru Educatie si Cercetare	Romania	www.nren.ro
SANET	Slovak Academic Network Association	Slovakia	www.sanet.sk
Sikt	Sikt – Norwegian Agency for Shared Services in Education and Research	Norway	www.sikt.no/en/home
SURF	SURF b.v.	Netherlands	www.surf.nl/
SWITCH	SWITCH	Switzerland	www.switch.ch
ULAKBIM	Turkiye Bilimsel Ve Teknolojik Arastirma Kurumu	Turkey	www.ulakbim.gov.tr
UoM	L-Università ta' Malta	Malta	www.um.edu.mt/itservices/research
URAN	Association of Users of Ukrainian Research and Academic Network	Ukraine	www.uran.net.ua

Table A.1: List of 2023 Compendium survey respondents

B. COMPENDIUM AUTHORS

Marina Adomeit, T&I Project Manager (SUNET), focuses on international projects and T&I services. She has been working in the NREN community since 2006, with long experience of participating in GÉANT projects in tasks related to AAI, and is currently joint leader of the Trust and Identity Work Package in GN5-1. Marina has been working within international projects such as Seamless Access Consortium, Puhuri AAI infrastructure for access to EuroHPC LUMI supercomputer and others.

Sebastiano Buscaglione, Senior Network Architect (GÉANT), has several years of experience working in large-scale service provider networks. Before joining DANTE (now GÉANT) in 2012, he worked as part of the AT&T Global Operations department supporting global enterprise VPN services. His main interests are extraction and analysis of network data and its use in driving optimisation in network architectures. Sebastiano's career path includes networking at the CISCO Networking Academy within London Metropolitan University, and industry certifications such as CCNP and MEF-CECP.

Vincenzo Capone, Head of Research Engagement and Support (GÉANT), is responsible for user support for network solutions provided to pan-European and international scientific groups and collaborations, and in Science and Research engagement activities, with a background in computer science and networking. Previous positions include the Department of Physics at the University of Naples, where Vincenzo was the Network Architect and manager in charge of the computing resources for physics experiments, and Technical Associate to the ATLAS experiment collaboration at CERN.

Zoë Fischer, Information Security Graduate (GÉANT), holds a Master's degree in communication science, with a specialisation in political communication, from the University of Amsterdam. In her role at GÉANT, Zoë supports the security team by assisting with organisational and communication tasks. This includes coordinating events such as the GÉANT Security Days conference, writing reports, helping to manage a certification process, and being the service owner of the vulnerability management service. Zoë is interested in combining her background in communication science with the technical field of cyber security. She sees opportunities to use her understanding of information dissemination to improve cyber-security strategies, and to bridge the gap between technical complexity and user awareness.

Tom Fryer, Head of International Relations (GÉANT), joined GÉANT as a member of the International Relations team in 2008. He leads the team that supports GÉANT's relationships with R&E networking partners in other world regions and that manages EU-funded regional development projects. Tom supports dialogue with global R&E network partners in Latin America, Canada and the US and leads GÉANT's involvement in the BELLA programme, in which he is a member of the BELLA Steering Committee and is project manager for the EC funding contracts for BELLA. Tom has a degree in modern languages and linguistics from the University of Essex.

Sara Garavelli, Strategic European Engagement and Coordination Development Manager (CSC), is the coordinator of the EOSC Finnish Forum, the EOSC national structure supported by the Finnish Ministry of Education and Culture in charge of organising the EOSC activities and engagement at country level. Sara has more than ten years of experience in the areas of stakeholder engagement, outreach and international collaboration in the research infrastructures landscape. Sara has a degree in telecommunications engineering and a Master's degree in logistics and organisation for industry and commerce.

Davina Luyten, Communications Officer (Belnet), has a background in translation, journalism and corporate communication. At Belnet, she focuses on external communication, public relations, crisis communication and security awareness. She has participated in the GÉANT project since 2020, where her involvement includes the annual cyber security awareness campaign.

Alf Moens, Senior Information Security Officer (GÉANT), has been the Chair of the Special Interest Group on Information Security Management (SIG-ISM) since 2015 and plays a prominent role in GN5-1 where he is joint Work Package Leader of Work Package 8 Security. Before joining GÉANT, Alf was Corporate Security Officer for SURF, the Netherlands NREN.

Mario Reale, Senior Research Engagement Officer (GÉANT), holds a PhD in high energy physics from the University of Wuppertal, Germany (1997). He worked as grid middleware tester and integrator on grid computing for DataGrid, EGEE, and EGI. In 2006, he joined the Italian NREN GARR, where he worked on the IPv6 compliance of grid middleware. Subsequently, Mario joined the GARR Cloud activities, dealing with the automation of the deployment of OpenStack clusters in Italy. He joined the activities of IDEM, the Italian Identity Federation, in 2018–2019. In July 2019 he joined the GÉANT Association as a Senior Research Engagement Officer, supporting large international user communities in the adoption of GÉANT community services, and as coordinator of special interest groups on eHealth and Cloud. He is also involved in the business development of eduGAIN, supporting the establishment and onboarding of new identity federations worldwide.

Maria Ristkok, joint Work Package Leader for the GN5-1 project Above-the-Net Services Work Package (WP4) (EENet), has approximately 20 years of experience in the European networking community, having had different roles, both technical and non-technical, also in the GÉANT project teams (Clouds, Intelligence Gathering, Communication, Campus Best Practice) and Task Forces. She has been the chair and co-chair of the GÉANT Task Force on Marketing Communication and Public Relations and a member of the SIG-Marcomms Steering Committee. Maria has an MA in social sciences with a focus on communication management. Maria's great-grandfather was announced the holy hieromartyr (saint) of the Greek Orthodox Church in 2012, establishing a spiritual cloud connection as well.

Maarten Kremers, Technical Product Manager Trust, Identity and Security (SURF), joined the Dutch NREN SURF in 2007 and in his current role as a project manager and technical product manager is responsible for the innovation and development of SURF trust and identity services. Within the current iteration of the GÉANT project (GN5-1) Maarten is joint leader of the Trust and Identity Work Package (WP5) for the European research and education community.

Jennifer Ross, Partner Relations Officer (GÉANT), has experience in public relations and stakeholder management within the public and non-profit sector. Since joining GÉANT in mid-2020 she has been involved in coordinating the production, release and promotion of the Compendium Report 2019, 2021 and 2023.

Leonie Schäfer, Global Liaison Manager (DFN), is responsible for coordinating the DFN contribution to international projects and joint developments. At GÉANT, Leonie takes on various tasks in the areas of EU Liaison, International Relationships and Stakeholder Management within the framework of GÉANT projects. Prior to joining DFN, Leonie spent several years in science where she conducted own research and was responsible for managing EU research projects. Later she served as Scientific Officer at the EU Commission, DG INFSO (the former name of DG Connect), dealing with innovation policies, new research trends and emerging research communities in respect to ICT-related technologies. Leonie graduated and received her PhD in computer science from the Technical University of Berlin.

Jakob Tendel, Cloud Services Manager and primary research liaison (DFN), is joint Work Package Leader for the GN5-1 project Above-the-Net Services Work Package (WP4) and supports GÉANT in its European procurement efforts for cloud services. Jakob is responsible for coordinating the activities of DFN and German user organisations in cloud services adoption and activities in international big data science projects. He holds a PhD in meteorology (having studied clouds quite literally) from the Hannover Leibniz University and joined DFN in 2013.

Daniel Wüstenberg, Community Research Officer (GÉANT), is responsible for collecting, collating and analysing information from and about the NREN community to provide GÉANT and the NRENs with business intelligence. He runs the yearly NREN Compendium survey as one of his main responsibilities. He holds a PhD in Biology from the Free University of Berlin and joined GÉANT in 2018, after working in market research and business intelligence in different settings for several years.

C. COMPENDIUM ADVISORY BOARD

The Compendium Advisory Board has been recruited from the NREN community to help the Compendium team to steer the development of the Compendium according to the needs of the community. Its current members are:

János Mohács, Head of Research and Development (KIFÜ), is responsible for coordinating national and European e-infrastructure development within the Agency. Since 1996, he has led or participated in more than 20 European and Hungarian projects related to research and e-infrastructures, cloud and information systems, computer, network development and applications, and the formal description of network protocols and solutions. He has been and still is involved in major projects such as Sulinet+, GÉANT, SEEREN, VI-SEEM and HBONE+. The latter resulted in a European quality research e-infrastructure in Hungary. In these projects, he has gained extensive knowledge in the development of national and European research e-infrastructure. Previously a member of the GÉANT Programme Planning Committee (GPPC), he is now a member of the GÉANT Board and Vice President of the European Open Science Cloud (EOSC) Steering Committee and the Hungarian IPv6 Forum.

Hank Nussbacher, Director of Network & Computing Infrastructure (IUCC), has been working for IUCC since 1986 and has been involved with GÉANT since 2000. Hank has worked as a consultant to numerous companies including Cisco, AT&T, IBM, Checkpoint, Orange and many others, and is a co-author on a patent for selective diversion which is used by all DDoS mitigation companies. He is also the co-author of two IETF RFCs and has presented lectures at numerous RIPE, NANOG, FIRST and Terena conferences. In 1996 and 1997 he was a representative on the International Ad Hoc Committee (IAHC) to determine the future structure of the generic top-level domain system, which served as the basis for the establishment of ICANN, the Internet Corporation for Assigned Names and Numbers.

REFERENCES

[AARC]	https://aarc-project.eu/policies/
[AfricaConnect3]	https://www.africaconnect3.net/
[AI4EOSC]	https://ai4eosc.eu/
[AQUAINFRA]	https://aquainfra.eu/
[Asi@Connect]	http://www.tein.asia/main/?mc=0
[ASSOCIATION]	GÉANT Association Members: https://about.geant.org/membership/members-associates-general-assembly-representatives/
[Blue-Cloud 2026]	https://blue-cloud.org/
[CEF]	https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en
[CoCo]	https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
[Compendium]	https://compendium.geant.org/
[C-SCALE]	https://c-scale.eu/
[DG_Connect]	https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en
[DG_INTPA]	https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/international-partnerships_en
[DG_NEAR]	https://ec.europa.eu/info/departments/european-neighbourhood-policy-and-enlargement-negotiations_en
[EaPConnect]	https://www.eapconnect.eu/
[EC_UGtoSME]	https://ec.europa.eu/docsroom/documents/42921/attachments/1/translations/en/renditions/native
[eduGAIN]	https://edugain.org/
[eduGAIN_FWGR]	https://wiki.geant.org/display/eduGAIN/2022+eduGAIN+Futures+Working+Group+Report+Consultation?preview=/483754120/483754123/eduGAIN%20Futures%20WG%20recommendations.pdf
[eduroam]	https://www.eduroam.org/
[EGI-ACE]	https://www.egi.eu/projects/egi-ace/
[eIDAS]	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
[EOSC]	https://eosc.eu
[EOSC_AAI]	https://op.europa.eu/en/publication-detail/-/publication/d1bc3702-61e5-11eb-aeb5-01aa75ed71a1/language-en/format-PDF/source-188566729
[EOSC_AG]	https://eosc.eu/eosc-task-forces/
[EOSC_Focus]	https://eosc.eu/eosc-focus-project/
[EOSC_Future]	https://eoscfuture.eu/
[EOSC_NI4OS]	https://ni4os.eu/
[Erasmus+]	https://erasmus-plus.ec.europa.eu/
[ESCI]	https://education.ec.europa.eu/education-levels/higher-education/higher-education-initiatives/european-student-card-initiative
[EuroHPC_JU]	https://eurohpc-ju.europa.eu/
[EuroScienceGateway]	https://galaxyproject.org/projects/esg/
[FAIRCORE4EOSC]	https://faircore4eosc.eu/

[FAIR-IMPACT] https://fair-impact.eu/

[FENIX] https://fenix-ri.eu/

[GÉANT] https://www.geant.org/

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

[GN4-3_D4.1] GN4-3 Deliverable D4.1 Community Clouds Delivery Plan Services Selection, Business Models and Proposed Development Roadmap https://geantprojects.sharepoint.com/:b:/r/sites/gn4-3/Work-Packages/WP4/Deliverables%20Documents/Community%20Clouds%20Delivery%20Plan%20Services%20Selection,%20Business%20Models%20and%20Development%20Roadmap/D4-1_Community-Clouds-Delivery-Plan-Services-Selection-Business-Models-and-Development-Roadmap.pdf?csf=1&web=1 [federated login required]

[GN4-3_D4.3] GN4-3 Deliverable D4.3 Review of Community Clouds Delivery https://geantprojects.sharepoint.com/:b:/r/sites/gn4-3/Work-Packages/WP4/Deliverables%20Documents/Review%20of%20Community%20Clouds%20Delivery/D4-3_Review-of-Community-Clouds-Delivery.pdf?csf=1&web=1 [federated login required]

[GN4-3_D8.2] GN4-3 Deliverable D8.2 Security Baseline for NRENs https://resources.geant.org/wp-content/uploads/2022/02/D8-2_Security-Baseline-for-NRENs.pdf

[GN4-3_D8.12] GN4-3 Deliverable D8.12 GÉANT Community Requirements for Business Continuity Planning https://resources.geant.org/wp-content/uploads/2022/02/D8-12_GE%CC%81ANT-Community-Requirements-for-Business-Continuity-Planning.pdf

[GN5-1_D7.1] GN5-1 Deliverable D7.1 Network Evolution Plan [federated login required] https://geantprojects.sharepoint.com/:b:/r/sites/gn5-1wp7/Deliverables/Network%20Evolution%20Plan/GN5-1_D7.1_Network-Evolution-Plan.pdf?csf=1&web=1&e=3nR7L7

[GN5-1_SoCSAwNRENs] Status of Cyber Security Awareness within National Research and Education Networks https://resources.geant.org/wp-content/uploads/2024/02/GN5-1_Status-of-Cyber-Security-Awareness-within-NRENs.pdf

[GN5-IC1] https://network.geant.org/gn5-ic1/

[GN_AAI] https://wiki.geant.org/display/GSPP/GEANT+AAI+Service

[GraspOS] https://graspos.eu/

[InAcademia] https://inacademia.org/

[Infinera] https://www.infinera.com/

[IPv6] https://datatracker.ietf.org/doc/rfc8200/

[ISCED 2011] http://www.uis.unesco.org/Education/Documents/isced-2011-en.pdf

[Juniper] https://www.juniper.net/uk/en/

[MyAcademicID] https://www.myacademic-id.eu/

[MyAccessID] https://wiki.geant.org/display/MyAccessID/MyAccessID+Home

[NCSC_Advice] https://www.ncsc.gov.uk/news/uk-joins-international-partners-to-issue-advice-on-latest-russian-cyber-threat-

[OCRE] https://www.ocre-project.eu/

[OpenRoaming] https://wballiance.com/openroaming/

[Puhuri]	https://neic.no/puhuri/
[REFEDS]	https://refeds.org/federations
[REFEDS_BE]	https://refeds.org/baseline-expectations
[REFEDS_R&S]	https://refeds.org/research-and-scholarship
[Register_BIIC]	https://www.theregister.com/2022/04/07/security_driving_down_ransomware_payments/
[Skills4EOSC]	https://www.skills4eosc.eu/about
[TI]	https://www.trusted-introducer.org/
[TRANSITS]	https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS_Training.aspx
[World_Bank]	https://data.worldbank.org/
[WIPv6LM]	https://www.worldipv6launch.org/measurements/

GLOSSARY

AAI, Authentication and Authorisation Infrastructure
AARC, Authentication and Authorisation for Research and Collaboration
AER, Asia-Europe Ring
AI, Artificial Intelligence
AISBL, Association Internationale Sans But Lucratif / International Non-Profit Association
ANA, Advanced North Atlantic
API Application Programming Interface
APNIC, Asia Pacific Network Information Centre
AS, Autonomous System
AUP ,Acceptable Use Policy
AW, Alien Wave or Wavelength. Data transmission laser light from third-party equipment; an alien wave system multiplexes alien light together with local signals using DWDM.
BEAA, Bridging Europe, Africa and the Americas
BELLA, Building the Europe Link with Latin America
BGP, Border Gateway Protocol
CA, Certification Authority
CAMS, Central Access Management System
CAPEX, Capital Expenditure
CCNP, Cisco Certified Network Professional
CEDS, Common European Data Spaces
CEF, Connecting Europe Facility
CER, Critical Entities Resilience
CERN, European Organisation for Nuclear Research
CERT, Computer Emergency Response Team
CISO, Chief Information Security Officer
CJEU, Court of Justice of the European Union
CLAW, Crisis Management Workshop for the NREN Community
CoCo, Code of Conduct
CORDIS, Community Research and Development Information Service
CRA, Cyber Resilience Act
CSA, Coordination and Support Action
C-SCALE, Copernicus – eoSC AnaLytics Engine
CSIRT, Computer Security Incident Response Team
CTO, Chief Technology Officer
DCI, Data Centre Interconnect
DdoS, Distributed Denial of Service
DG Connect, EC Directorate-General for Communications Networks, Content and Technology
DG INTPA, EC Directorate-General for International Partnerships
DG NEAR, EC Directorate-General for European Neighbourhood and Enlargement Negotiations
DICE, Data Infrastructure Capacity for EOSC
DTN, Data Transmission Network
DWDM, Dense Wavelength Division Multiplexing
EaPConnect, Eastern Partnership Connect
EB, Exabyte (1018 bytes of data)
EC, European Commission
EDPB, European Data Protection Board
eduroam, education roaming. The secure, world-wide roaming access service developed for

the international research and education community.

EuroHPC JU, European High Performance Computing Joint Undertaking

EGI-ACE, Advanced Computing for EOSC, coordinated by the EGI Foundation

EHDS, European Health Data Space

EHR, Electronic Health Record

eID, Electronic Identification

eIDAS, Electronic Identification, Authentication and Trust Services

ELIXIR, A European intergovernmental organisation that is made up of life scientists, computer scientists and support staff. Its goal is to help researchers take advantage of the huge amounts of data produced in life science, so that new insights can be gained into how living organisms work in health and disease.

EO, Earth Observation

EOSC, European Open Science Cloud

ESCI, European Student Card Initiative

ESI, European Student Identifier

EU, European Union

EUDI, EU Digital Identity

EuroQCI, European Quantum Communication Infrastructure

FAIR, Findable, Accessible, Interoperable and Reusable

FE, Further Education

FoD, Firewall on Demand

FTE, Full-time equivalent

Gbps, Gigabits per second

GCP, GÉANT Community Programme

GDP, Gross Domestic Product

GDPR, General Data Protection Regulation

GN4-3, GÉANT Network 4 Phase 3 project, part-funded from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726

GN4-3N, GÉANT Network 4 Phase 3 Network project, part-funded from the EU's Horizon 2020 research and innovation programme under Grant Agreement No. 856728

GN5-1, GÉANT Network 5 Phase 1 project, part-funded from the EU's Horizon Europe research and innovation programme under Grant Agreement No. 101100680

GPPC, GÉANT Programme Planning Committee

GraspOS, Next Generation Research Assessment to Promote Open Science

H2020, Horizon 2020

HPC, High-Performance Computing

HR, Human Resources

IaaS, Infrastructure as a Service

IaaS+, Infrastructure as a Service Plus Framework

IAM, Identity and Access Management

ICT, Information and Communications Technology

IdP, Identity Provider

IETF, Internet Engineering Task Force

IMF, International Monetary Fund

INFRAEOSC, Enabling an operational, open and FAIR EOSC ecosystem

INFRAG, Infrastructure Advisory Group

IP, Internet Protocol

Ipv4, Version 4 of the Internet Protocol (StB IETF), a connectionless protocol used on packet-switched networks. Employs 32-bit IP-addresses.

Ipv6, Version 6 of the Internet Protocol (StB IETF), The successor to IPv4, employing a 128 bit IP-address. In addition to a larger addressing space, IPv6 deals with addresses in a hierarchal

manner and improves route aggregation.
IRU, Indefeasible Rights of Use
ISCED, International Standard Classification of Education

The classification is:
Level 8: Doctoral or equivalent level
Level 7: Master's or equivalent level
Level 6: Bachelor's or equivalent level
Level 5: Short-cycle tertiary education
Level 4: Post-secondary non-tertiary education. This can include, for example, short vocational training programmes.
Level 3: Upper secondary education
Level 2: Lower secondary education
Level 1: Primary or basic education
Level 0: Early childhood or pre-primary education
The different institutions types are classified as follows:
Universities and other (ISCED 6–8)
Further education (ISCED 4–5)
Secondary schools (ISCED 2–3)
Primary schools (ISCED 1)
Research institutes
Libraries, museums, archives, cultural institutions
Non-university public hospitals
Government departments (national, regional, local)
International (virtual) research organisations
For-profit organisations

ISO, International Organisation for Standardisation
ISP, Internet Service Provider
IX, Internet Exchange
IXP, Internet Exchange Point
LHC, Large Hadron Collider
LHCONE, Large Hadron Collider Open Network Environment
LUMI, Large Unified Modern Infrastructure (the EuroHPC JU supercomputer located in Finland)
MAN, Metropolitan Area Network
MEF, (formerly) Metro Ethernet Forum
MEF-CECP, MEF Carrier Ethernet Certification Program
MPLS, Multiprotocol Label Switching
NI4OS, National Initiatives for Open Science
NIS2, Network and Information Security Directive
NREN, National Research and Education Network
OCRE, Open Clouds for Research Environments project. OCRE aims to accelerate cloud adoption in the European research community by providing a framework for providers and users of cloud services and Earth Observation (EO).
OIDC, OpenID Connect
OLS, Open Line System
OPEX, Operating Expenditure
OSFP, Octal Small Form Factor Pluggable
OTN, Optical Transport Network
PaaS, Platform as a Service
PB, Petabyte (1015 bytes of data)
PID, Persistent Identifier

PoP, Point of Presence
PR, Public Relations
QSFP-DD, Quad Small Form Factor Pluggable – Double Density
R&E, Research and Education
R&S, Research and Scholarship
REFEDS, Research and Education Federations group
REN, Research and Education Network
RFC, Request for Comments. A formal document drafted by the IETF that describes the specifications for a particular technology. When an RFC is ratified, it becomes a formal standards document.
RO, Roaming Operator
ROA, Route Origin Authorisation
RPKI, Resource Public Key Infrastructure
RREN, Regional Research and Education Network
SaaS, Software as a Service
SAML, Security Assertion Markup Language
SANE, Secure ANalysis Environment
SIEM, Security Information and Event Management
SIG, Special Interest Group
SIG-DHD, Special Interest Group on Digital Health Data
SIG-ISM, Special Interest Group on Information Security Management
SIM, Security Information Management
Simpl, The smart middleware that will enable cloud-to-edge federations and support all major data initiatives funded by the European Commission, such as common European Data Spaces
Sirtfi, Security Incident Response Trust Framework for Federated Identity
SOC, Security Operations Centre
SP, Service Provider
SPAN, Switch Port Analyser
SSH, Secure Shell
SUBMERSE, SUBMarine cablEs for ReSearch and Exploration
T, Task
T&I, Trust and Identity
TAP, Test Access Point
TB, Terabyte (1012 bytes of data)
TCS, Trusted Certificate Service
TF, Task Force
TF-CSIRT, Task Force on Computer Security Incident Response Team
TF-eHealth, Task Force on eHealth
TI, Trusted Introducer
TLD, Top-Level Domain
TRANSITS, State-of-the art, high-quality training, coordinated by GÉANT, for Computer Security and Incident Response Team (CSIRT) personnel, as well as individuals with an interest in establishing a CSIRT
UN, United Nations
VPN, Virtual Private Network
WG, Working Group
WP, Work Package
WP8, GN4-3 Work Package 8 Security

GÉANT