10-02-2020

Deliverable D6.4
Campus Network Management

Deliverable D6.4

Contractual Date:	29-02-2020
Actual Date:	10-02-2020
Grant Agreement No.:	856726
Work Package	WP6
Task Item:	Task 3
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	UoB/AMRES
Document ID:	GN4-3-20-292E3E
Authors:	Maria Isabel Gandia (CSUC/RedIRIS), Ivana Golub (PSNC), Susanne Naegele-Jackson (FAU/DFN), Pavle Vuletić (UoB/AMRES), Tim Chown (Jisc), Jasone Astorga (RedIRIS/University of the Basque Contry), Vidar Faltinsen (Uninett), Asko Hakala (Funet), David Heed (SUNET))

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This document reports on Campus Network Management as a Service activities in the GÉANT and NREN community and offers some guidelines to the NRENs who offer the service to produce their own Service Definition and contract documents.

Table of Contents

Table of Tables

Executive Summary

Campus Network Management as a Service (CNaaS) has emerged as an important topic in the GÉANT and National Research and Education Networks (NREN) community with governments pursuing this as part of their digitalisation strategies. An increasing number of end institutions have been asking their NRENs to take over responsibility for managing their internal network and services as NRENs generally have a good reputation for managing their infrastructures, while many end-institutions struggle with this due to difficulties in recruiting qualified network technicians.

Exploring how the GÉANT project might be able to help and support NRENs on their path to provide CNaaS, the *Monitoring and Management* Task (T3) of the GN4-3 project's *Network Technologies and Services Development* Work Package (WP6) has participated and organised several multilateral meetings and workshops, covering, among others, technical, organisational, service and process aspects of providing the CNaaS service.

This document reports on Campus Network Management as a Service activities in the GÉANT and NREN community, based on information gathered through different community events. It also provides a CNaaS Service Definition which the NRENs can use as guidelines for offering CNaaS services to their users, and provides directions for future work in this area in the community.

1 Introduction

Due to the difficulties in recruiting qualified network technicians, and the good reputation National Research and Education Networks (NRENs) generally have for managing their own infrastructures, a number of end institutions have asked their NRENs to take over responsibility for managing their internal network and services.

Faced with the challenge of offering a new 24/7 secure and reliable network management service, SUNET, UNINETT and NORDUNET proposed working on the development of a concept and a toolkit within the GN4-3 project to help themselves and other NRENs to provide Campus Network Management as a Service (CNaaS) services.

To gather information about different NRENs' requirements for these kind of services, the *Monitoring and Management* Task (T3) of the GN4-3 project's *Network Technologies and Services Development* Work Package (WP6) participated in several meetings and organised a workshop to learn more about the current status and future needs of campus network management services in the community.

As managing campus networks requires repeatedly updating and configuring many devices remotely, the use of orchestration, automation and virtualisation (OAV) techniques is also a key to the success of campus network management services. For this reason, the T3 group working on the service definition for CNaaS also approached the *Network Services Evolution and Development* Task (T2), which worked on OAV in WP6, and whose work in the first half of the project year is summarised in Deliverable D6.2 *Automation and Orchestration of Services in the GÉANT Community* [D6.2].

As a result of the research that took place during the meetings and workshops and also in T2, a number of different NREN approaches to the delivery of Campus Network Management Services were found.

Apart from the Nordic countries, AMRES, ARNES, CARNET, FUNET, HEAnet, KIFU, LITNET and SURFNET are already offering or deploying CNaaS-like services in managing wired and/or Wi-Fi networks for their end institutions. One of the drivers for this is that several governments have asked their NRENs to offer common ICT services to schools and higher education institutions, following the development of digitalisation strategies in their countries.

With such a diversity of cases, approaches, objectives, maturity levels and existing NMS/OSS/BSS systems, it was clear that there is no single solution, service definition or common tool that could fit them all. However, it was realised that the GN4-3 project could help NRENs define their own services through a Service Definition Template/Checklist that could easily be adapted to their own needs.

Section 2 gives an overview of the activities undertaken to gather information about the current status of campus network management services, examples of the different approaches found and use cases from the community.

Section 3 contains the Service Definition Template/Checklist that NRENs can adapt to their own needs to offer the service to their end-institutions.

Section 4 summarises the conclusions and presents planned future work.

2 CNaaS Services in the GÉANT Community

To define a service that could be broadly adopted by the GÉANT community, WP6 T3 had to identify which NRENs were already offering or were going to deploy CNaaS services in their countries, gather their individual requirements and determine common needs.

WP6 T3 discussed these requirements with different NRENs, attending or organising a number of meetings. In addition, T3 liaised with WP6 T2 to benefit from their previous work which provided relevant information about CNaaS needs and use cases.

The following subsections describe the outcomes of some of the more relevant meetings conducted in 2019. The conclusions of all these efforts is provided in Section **Error! Reference source not found.**.

2.1 CNaaS Meeting

The CNaaS Meeting, hosted by SUNET and organised under WP6 T3, was held in Stockholm on 29-30 January 2019, to bring together the proposers of the CNaaS work in the GÉANT project, interested NRENs and the GÉANT WP6 participants. The purpose was to discuss the current status of the CNaaS services in each NREN and what the goals and next steps were going to be in the project. The meeting was attended by 20 people, both on site and via videoconference, from NORDUNET, SUNET, SURFNET and UNINETT and WP6. Presentations and discussions centred around CNaaS service definition and delivery, CNaaS OSS/BSS architecture and tools [ANSIBLE] [OXIDIZED] [NAV] and the use of orchestration and automation for CNaaS.

The discussions showed that even with this small sample of NRENs there were differences in their approaches and the scope of services they offer to their customers (e.g., one NREN considered monitoring campus infrastructure only, another the management of wired or wireless infrastructure). There were also different levels of maturity in the field of automation and campus network management services. One of the important activities that emerged from this discussion was the need to summarise the CNaaS service offering and to create a CNaaS service definition.

After that first face-to-face meeting, the group conducted several video conferences to follow up on the campus network management requirements and further evolution, with presentations from FUNET about the CNaaS services already offered by them and GN4-3 T3 about Network Management as a Service (NMaaS) [NMaaS].

2.2 9th SIG-NOC Meeting

The 9th SIG-NOC Meeting [9SIG-NOC] was hosted by ARNES in Ljubljana on 8-9 April 2019, organised by the Special Interest Group - Network Operation Centres (SIG-NOC) and GÉANT under the theme 'NOC challenges: trapped between monitoring and regulation'. It was attended by more than 30 people, both on site and via video conference, and different perspectives around CNaaS were given.

It was especially relevant to learn about the initiatives regarding school network management services by a number of NRENs, driven by their countries' governments and their short and mid-term digitalisation strategies. For instance, ARNES is offering a centrally managed eduroam/WiFi service in Slovenia for every primary and secondary school, managing RADIUS as a Service. CARNET is including the LAN and the interactive equipment for classrooms as well as the WiFi and user devices, and AMRES is managing the LAN and WiFi services for schools, as well as CPEs for all the institutions.

Presentations and debates around CNaaS included school wireless and local area network management [9SN-CARNET], [9SN-ARNES1], and different tools [9SN-SUNET-CSUC], [9SN-ARNES2].

Similar to the CNaaS meeting, the presented use cases showed the differences in approaches and offerings: from a (relatively) small number of devices in the case of universities to several thousand for schools, or from an optional service for universities to a mandatory one for schools. In some cases, in-house developed tools were used to offer the service with automation [9SN-ARNES-AUTOMATOR].

2.3 WP6 Task2 Research: The Survey on OAV and Meetings

As a part of its work on the possibilities for orchestration, automation and virtualisation (OAV) of network services, WP6 Task 2 conducted a survey on OAV among the GÉANT project partners, to learn more about their current and planned work and strategies. 31 NRENs responded [OAV-SURVEY]. The results were discussed in the GN4-3 Future Service Strategy Workshop, held in Amsterdam in May 2019, at TNC19 in Tallinn in June 2019 and at the 17th STF meeting in Dublin in July 2019.

The survey results and the discussions proved relevant to CNaaS, with NRENs reporting the importance of automation, orchestration and virtualisation to their work on campus network management. Specifically, ARNES, CARNET, FUNET, GRNET, HEAnet, LITNET and SUNET mentioned this in their responses. In some cases, such as for HEAnet, the services were different for the schools' network and for the higher education network.

The results of the survey, the discussions during the meetings and the conclusions of the WP6 T2 work can be found in Deliverable D6.2 *Automation and Orchestration of Services in the GÉANT Community* [D6.2].

2.4 Workshop on Network Management and Monitoring

The Workshop on Network Management and Monitoring [NEMMO] was hosted by NORDUNET in Copenhagen on 21-22 October 2019, organised by the GÉANT project under WP6 T3. It was attended by more than 50 people from 28 NRENs, both on site and via video conference. It mainly focused on CNaaS services, which judging by the high level of attendance, was a very relevant topic for the community. During the workshop, both the technical and organisational aspects of managing end institution networks were discussed:

- Organising network services management for end institutions: managing the whole network, some part of it, such as WiFi, or specific services, such as email, RADIUS servers etc. [NM-AMRES], [NM-ARNES], [NM-CARNET], [NM-FUNET], [NM-KIFU], [NM-SUNET], [NM-SURFNET], [NM-UNINETT].
- Creating a CNaaS service definition or a Service Level Agreement [NM-CN-SD].
- Outsourcing [NM-SURFNET2], [NM-SUNET2].
- Network management tools [NM-GRENA], [NM-GRNET], [NM-NMAAS], [NM-UNINETT2].
- Monitoring customer networks [NM-GRENA], [NM-NMAAS], [NM-UNINETT2].
- Automating management functions (in the NREN and in end institutions if their infrastructure is managed by the NREN) [NM-FUNET2], [NM-SURFNET2], [NM-WB].
- Using white boxes as small routers to offer campus network management services [NM-WB].

The workshop served as a forum for the NRENs to discuss their main concerns, current status, plans, common points of view and differences regarding campus network management services, including also multiple bi-lateral discussions between NREN members. While a summary of this and the previous workshops is given in Section **Error! Reference source not found.**, one of the main remarks during the f inal debate was that one of the most valued tasks that GÉANT could do for the NRENs was to organise more workshops of a similar nature, covering CNaaS aspects, as sharing knowledge, experiences and processes is very important for the NRENs.

2.5 10th SIG-NOC Meeting

The 10th SIG-NOC Meeting [10SIG-NOC] was hosted by CESNET in Prague on 13-14 November 2019, organised by the Special Interest Group - Network Operation Centres (SIG-NOC) and GÉANT, under the theme ‘Keeping the competitive edge in the NREN community’. It was attended by nearly 40 people from 23 NRENs and institutions, both on site and via video conference. Campus Network Management was one of the main topics, together with OAV.

As this was a NOC meeting, there were also some presentations about NOC tools (for monitoring, automating, etc). The SIG-NOC Tools survey was presented and one of the outcomes was that OAV techniques were mostly used for provisioning, especially at the access networks. This is relevant for campus network management services, where the provisioning is usually done remotely and automatically. During the wrap-up session, the attendees agreed that the problem of automating network services overlaps with the problem of campus network management and the tools to be used are largely the same.

2.6 Use Cases

The meetings and previous work showed that some NREN and Regional Networks are already working on a variety of CNaaS services. Some offer mature services, while others are only just beginning to define their services. The current status is summarised below:

NREN	Scope	Reason	Number of devices	Outsourcing?	Automated?	Status	References
AMRES	Several projects: • CPE • Wireless for schools • LAN infrastructure	AMRES strategic goals / Government mandate	• 250 CPE • 900 wireless devices • 24,000 APs in 1,200 schools soon	Partially (initial configuration)	No	• CPE started in 2013 • 3rd project for schools 2019-2021	[NEMMO-AMRES]
ARNES	Several projects: • CPE • Wireless for schools (W2020)	Members needs / National project	• 650 routers • 1,300 switches • 16,000 APs • 20 controllers • 300 routers	Partially (initial configuration)	Yes		[9SN-ARNES] [9SN-ARNES2] [NM-ARNES]
CARNET	Project including: • LAN • Wireless for schools • Laptops for schools' staff	National project to make IT part of the daily life of the schools (e-schools)	• 8,000 switches • 35,000 APs • 70,000 end-user devices	No	Yes	eSchools project:2015-2022	[CARNET-E-SKOLE] [9SN-ESKOLECARNET] [NM-CARNET]
FUNET	Campus: • CPE • Core equipment	FUNET product (Kampus Service)	• 9 deployments • 13 routers • 22 switches	No	Yes	1 year in production	[NM-FUNET]

NREN	Scope	Reason	Number of devices	Outsourcing?	Automated?	Status	References
HEANET	CPE for schools	HEANET service	• 4,000 access routers • 17 core and aggregation routers	No	Yes (islands of automation)	10 years' experience	[TNC-HEANET-OAV]
KIFÜ / HUNGARNET	Core and Endpoints	National DIÁKHÁLÓ project (StudentNet)	• 1000 core devices • 7000 Access devices	Partially (trend to insource)		Starting Deployment	[NM-KIFU]
LITNET	Wireless for schools	National project				Starting the deployment	[LITNET-WIFI]
SUNET	CNaaS Services for Universities	Demand from users		No	Yes	Initial production in 2020	[SUNET-CNAAS]
SURFnet	Wifi for connected entities (SURFwireless)	SURFNET strategy	All the equipment	Partially (operations are outsourced, strategy lies on SURFNET)	Yes	Fully developed	[SURFNET-WIFI] [NM-SURFNET1] [NM-SURFNET2]
UNINETT	CNaaS service for universities	Demand from users / Governmental Digitalisation Strategy			Yes	Initial production in 2020	[NM-UNINETT] [NAV]

Table 2.1: Use cases

The OAV Community Portal [OAV-COM-PORTAL] in the OAV public WIKI [OAV-WIKI] includes all the use cases about CNaaS using automation and can be used by the NRENs as a (live) reference. As can be seen, NRENs differ in almost every aspect presented in Table 2.1. A summary of these differences, which were explored in the presentations and discussions held in CNaaS-related events, are given in the next section.

2.7 Summary of Findings

After studying the presentations and discussions that were conducted during the meetings, the results of the OAV survey [D6.2], the SIG-NOC Tools survey [SIG-NOC-TOOLS], and the current use cases and needs from the NRENs, the following conclusions can be drawn:

- NRENs currently offering or planning to offer CNaaS services differ in maturity stages in terms of service development and use of OAV techniques:
  - Some NRENs have been asked by their end institutions to provide CNaaS services; others are offering them because their government requires them to do so.
  - While some NRENs are managing only edge devices (the CPEs) on the border between the NREN and the institution, others are offering WiFi or LAN services inside the institutions.
  - While some NRENs are working on OAV techniques, having Zero Touch Provisioning (ZTP) as a goal and managing contributions from multiple people (including students' work) through fully integrated CI/CD, code audits, well-defined and regularly executed tests, others are configuring the devices manually or have a semi-automated approach.
  - While some NRENs have outsourced their day-to-day operations or first level support, others are managing this first level support themselves or are in-sourcing previously outsourced functions.
  - While some NRENs have started from scratch by defining an OSS/BSS and/or architecture, others are building upon existing networks and services in order to offer the service.
  - While campus management services have been assumed by the existing NOCs at some NRENs, others have created a separate team to offer them and the NRENs have created new roles to take care of CNaaS services and automation.
  - While some NRENs use the same tools for CNaaS as for their own NREN network or have integrated them in their own platforms, others have created separate instances for each managed institution or have developed new in-house tools to help them with the deployment of campus network management services (for configuration management, change management, monitoring, etc).
  - The number of managed devices differs from a few in some cases to several thousand in others.
  - The network skills of the engineers in the end institutions varies depending on the type of institution and its number of employees.
  - The level of engagement in campus network management projects differs. Some of them run their own helpdesk while others are not able or willing to do so and rely fully on the NREN.
  - Even within the same NREN, a service can differ per user group (user groups define the functionalities of a service).
  - While some NRENs charge for each service package in their campus network management offering to the users, others do not charge anything, as the budget comes from their governments.
  - While some NRENs sign an SLA agreement with their connected institutions and define the responsibilities for each party, others only offer best effort services.

  - While some NRENs offer brownfield services (managing devices that were already in the network), others only offer greenfield services (with newly deployed infrastructure).
  - The tender process is different depending on the NREN and several models are used (buying the equipment for the end-institution, buying it but keeping the devices as property of the NREN, managing existing devices, etc).
- There is not a single model that can fit all the currently existing cases. Several ways to offer CNaaS services are possible, with different approaches regarding architecture, tools, procedures, service delivery, administrative models, etc.
- Given the high level of interest, sharing knowledge, experiences and processes among NRENs offering CNaaS services, is one of the most valued tasks that the GÉANT project can provide to the NRENs.
- Having a set of recommendations to help each NREN create its own Service Definition documents is more useful for the NRENs than having a single monolithic Service Definition document that could only support one approach.
- The GÉANT project can also potentially help with some of the existing services:
  - Kubernetes/Docker based multi-tenant app provisioning seems to be a promising way forward (NMaaS) [NMaaS].
  - A very lightweight perfSONAR (on raspberryPi) for monitoring boxes could be useful, perhaps integrated with WiFiMon [WIFIMON] in the same device.
- Even if some NRENs are not using OAV techniques, they all understand that automation is an important part of the way forward, as documented in [D6.2].

Following the users' requirements, WP6 created a CNaaS Service Definition Template/Checklist to help the NRENs with a list of relevant topics to consider when writing their own documents (service definitions, SLAs, contracts, etc.). The Service Definition can be easily adapted for any approaches and strategies for offering network management functions. It includes suggestions for service delivery, and the service policy and recommendations to handle administrative questions and data privacy topics.

3 CNaaS Service Definition Template/Checklist

3.1 CNaaS Service Definition

As the CNaaS service can be offered in different ways, the NREN, regional network or institution offering CNaaS services (the 'provider') and the end-institution (the 'customer') must agree on the exact definition and scope of the service:

- What is included in the service in the basic package.
- What is added as an extended or supported package.
- Define any demarcation points between the provider and the customer.

It is very important to define and agree all details before going into production. The provider and customer can sign a contract or Service Level Agreement (SLA) that will contain particular aspects of the CNaaS service – quality, availability, responsibilities – agreed between them.

This section provides a service definition, based on ITILv3[1] processes and functions [ITILv3], that is easy to adapt and replicate for different providers. It can also be used as a reference when writing the contract or Service Level Agreement. When writing its own Service Definition Document, the provider can modify the text to fit its needs and adapt the examples. It is up to the provider to include as many technical details as desired, although where many details are given, they are more likely to change in the future. The provider should reserve the right to change the architecture, software, configuration mechanisms or monitoring infrastructure in the future according to the needs of the service, the evolution of the technology, the tools and the network.

3.2 Terminology

There are several important terms for the CNaaS Service Definition, whose meaning, as used in this document, is provided below:

- **Provider** -The organisation that is providing the CNaaS service (NREN, Regional network, institution or service provider).

[1] A new version of ITIL, ITILv4, appeared by the end of 2019, although not all the books were released by the time of writing this document. According to AXELOS [AXELOS], ITILv4 does not invalidate earlier versions of ITIL, therefore the ITIL v3 approach is still valid.

- **Customer** - The end-institution contracting the CNaaS service (University campus, school or some other organisation that plans to outsource the network monitoring, network configuration and management or some of its functions).
- **Supported Service Package** - Set of activities, that form a service that the provider offers to the customer as a part of the CNaaS service. One or more service packages can be offered by the provider and contracted between the provider and the customer.
- **Supported Network Items and Services** - Network Items and Services which are under the scope of the contract.
- **Additional Network services** - Services that are related to the network but not specifically a part of the wired or wireless network. Some examples would be DHCP, DNS, VPN, RADIUS, LDAP, NTP, VoIP or other network-related services that must be agreed upon beforehand between the provider and the customer.
- **Network Management and Monitoring System** - System used by network administrators to manage the network components and constantly observe and measure parameters to check the health of the network (software, hardware and environmental parameters) and for notifying the network administrator in case of trouble.

3.3 Contacts/Roles

The contact details for all the roles must be exchanged between the provider and the customer and updated promptly if it changes. More than one person can be associated with a role. Likewise, depending on the case, more than one role can be assigned to a single person.

The provider should define a person or a group for each one of their defined roles. Some suggested roles are:

- **Product Manager**: the main person responsible for continuously developing and managing the CNaaS service as a whole and for handling its commercial aspects.
- **Service Manager**: a person that will follow all the stages of the CNaaS service and will be the liaison between the customer and the CNaaS team at the provider. This person will also try to resolve any complaints received about the service and make any adjustments or further development that may be needed, referring to the Product Manager or the DevOps team if necessary.
- **Technical Advisor**: a person that provides technical knowledge and advice to support the customer during the Design and Transition stages.
- **NOC Team**: Network Operation Centre that assists the customer during the Operation stage, providing 2nd (and depending on the agreement, 3rd) level support.

The customer should define a person or a group for each one of their defined roles. Some suggested roles are:

- **Service Coordinator:** the customer's main point of contact with the provider will be the main person responsible for continuously following the evolution of the service, attending meetings, asking for incident reports, suggesting service improvements and passing on any complaints to the provider.

- **Helpdesk Team:** the team responsible for supporting end users in using the CNaaS service on site and provide the main point of contact in case of any issues.

During the Service Design stage, at least the Service Manager, the Technical Advisor and the Service Coordinator should meet face-to-face and exchange information to define the exact scope, involved packages, architecture, expected timeline, SLAs and any other relevant parameters to define the service.

If necessary, the provider and the customer can also specify some roles to be used for the Transition stage of the CNaaS service and for Change Management for the entire service lifecycle. For instance:

- The members of the Change Advisory Board (CAB), responsible for oversight of all changes in the production environment.
- The members of the Emergency Change Advisory Board (ECAB), responsible for oversight of all emergency changes in the production environment (for example, to resolve a major incident or implement a security patch).

3.4 Service Delivery Model

As the CNaaS service will be offered by each provider to its customers, the Service Delivery may differ from one provider to another. Therefore, the provider and the customer must agree on the offered packages, related parameters and prices, if applicable, before offering the service. The next sections suggest possible supported packages as well as service elements to be agreed beforehand for each customer and service package.

3.4.1 Supported Service Packages

The service can be offered in separated standardised packages by the provider. A basic package can be defined with the minimum requirements and offerings of a CNaaS service (for example, monitoring of the infrastructure). Subsequent packages (like configuration and management of the wired/wireless network or additional services) can be added to the basic package, depending on the customer's needs and the provider's offerings. The following subsections show some suggested packages to be offered by the provider to the customer in CNaaS as an orientation, although each provider can define other service packages for its customers.

3.4.1.1 *Monitoring of the Infrastructure*

The scope of the monitoring should be defined in this package and the level of detail given in the Service Definition may vary depending on the case. For instance, it may indicate that the provider will install all the necessary software tools for the correct monitoring of the infrastructure, without listing the specific software tools.

The following list shows examples of items that can be included in the Service Definition. The same list can be used as a reference for the monitoring of additional services:

- What will be monitored (included pieces of equipment):

  - Routers
  - Switches
  - Firewalls
  - Access-points
  - Network links
  - Intrusion Detection Systems
  - Radio links

- What will the monitoring system do:
  - Trigger alarms when defined thresholds are reached (send to the Campus HelpDesk/the NOC/an alarm console, etc..).
  - Generate graphs (Daily/Weekly/Monthly/Yearly, on-demand, etc.)
  - Automatically generate tickets when defined thresholds are reached (supported platforms).
  - Monitor certain Key Performance Indicators agreed with the customer.
  - Generate automatic reports.
  - Store monitoring data.

- Parameters to be monitored:
  - CPU usage
  - Memory usage
  - Interface input/output traffic
  - Interface input/output errors
  - Tx/Rx optical power (where possible)
  - Specific log entries like up/down interfaces
  - General availability
  - Latency in pre-defined links
  - Module up/down (for chassis based or stacked equipment)
  - Power up/down (for redundant power)
  - Fan out
  - Environmental parameters (like temperature, humidity, etc.)

- How will the monitoring be done:
  - Remotely (from the provider, from a central point in the campus, etc.)
  - Locally (on site, per building, etc.)
  - Centralised
  - Distributed (per campus, building, etc.)

- What mechanisms will be used (the specific software tools do not need to be included; if they are specified, the provider should reserve the right to change them in the future):
  - SNMP
  - Syslog

- Flow Monitoring
- Streaming Telemetry
- Active probes

- Where will the monitoring system/infrastructure be installed:
  - Physical platform
  - Virtual platform (VM)
  - Hybrid - Physical and virtual platform

- How will the provider manage the Network Management System (NMS) required for CNaaS:
  - From the provider
  - Through external services

- How will the customer be able to access the monitoring system (if applicable):
  - Certificate
  - Federation
  - Login/password
  - A combination of the above

- Who will install all the necessary software tools for the correct monitoring of the infrastructure:
  - The provider
  - The customer

- Set of reports that the provider will send to the customer (see Section 3.5.3).

- Needs of the monitoring system that may involve actions from the customer. For instance, the monitoring system should be:
  - Accessible to the provider (appropriate access for the provider – e.g. SNMP access, flow monitoring access, etc. – this has to be configured).
  - Able to send alerts to the providers' servers for monitoring, alerting and ticket generation (filtering at the customer may be involved).
  - Able to send emails.
  - Able to open tickets to a previously defined list of recipients.
  - Able to send alerts to the alarm console.
  - Have access through firewalls that depend on the customer.

3.4.1.2 *Monitoring of Additional Services*

The provider may offer the customer the monitoring of services that are not specific pieces of equipment or links on the network but are network-related services. As for Monitoring of the infrastructure (see Section 3.4.1.1), the level of detail given in the service definition may vary depending on the case. For instance, it may indicate that the provider will install all the necessary software tools for the correct monitoring of the infrastructure, without listing the specific software tools.

The following lists show examples of items to be included in the service definition for the monitoring of additional services:

- List of supported additional services (other ICT services such as email, web, directory service or other servers can be out of the scope of the service):
  - DHCP
  - DNS
  - VPN
  - RADIUS
  - LDAP
  - NTP
  - VoIP
- List of parameters to be monitored for each additional service (see the list in Section 3.4.1.1 for more examples):
  - General availability.
  - Disk usage.
  - Service-specific parameters (like number of requests/s for DNS, number of authentications in Radius, number of requests in NTP, time-to-respond, etc).

The list in Section 3.4.1.1 may also be used for the monitoring of additional services.

3.4.1.3 *Configuration and Management of the Wired Network*

The provider can offer greenfield services (with new infrastructure) and brownfield services (using existing infrastructure at the customer's premises). It is very important that the provider and the customer agree on the Service Elements covered by this service package in CNaaS.

The campus architecture design typically has three layers - core, distribution and access, although the network on each campus may vary and the exact scope of the service should be defined.

As in the previous sections, the level of details given in the service definition depend on the case. For instance, it may indicate that the provider will configure the equipment, without specifying how this configuration will be done.

The following list shows examples text that can be included in the service definition for the configuration and management of the wired network:

- The network architecture, that can be designed as a part of CNaaS can:
  - Consist of three layers: core, distribution and access (for big campuses), or
  - Consist of two layers: core and access (for small campuses), or
  - Follow a two-layer Spine/Leaf topology.

  The provider may reserve the right to further develop the architecture and network design. The customer should undertake to follow such changes.

- Network services that can be offered as a part of CNaaS:
  - The core will be IP-based (IPv4/IPv6 access will be provided to all end users).
  - Layer 2 connectivity will be possible between any two ports in the network.
  - IP over layer 2 can be terminated in the core using separate routing policies (VRF).
  - Layer 2 connectivity over the core will be implemented using overlay techniques (VXLAN or MPLS).
  - IP can, when necessary, terminate in a firewall.

- The configuration and management:
  - For core routers, the configuration will be manually done via CLI, locally in the customer premises.
  - For all the equipment, the setup will be automated.
  - For access switches, the setup will be automated, making the network devices acquire a temporary DHCP address through which automated scripts will configure the initial setup based on data from a centrally maintained configuration database, that can be managed by the provider or by the customer (this must be agreed in the contract between the provider and the customer).
  - For firewalls, the traffic-filtering and rate-limiting rules must be defined by the provider and the customer.
  - Standard changes in the network equipment will be automated. See Section 3.4.3.

- The bandwidth delivered to each point in the access network (depending on the ability of the customer to provide the wiring that complies with quality standards and length).

3.4.1.4 *Configuration and Management of the Wireless Network*

The provider can offer greenfield services (with new infrastructure) and/or brownfield services (using existing infrastructure at the customer's premises). It is very important that the provider and the customer agree on the Service Elements covered by this service package in CNaaS.

As in the previous sections, the level of details given in the service definition may vary depending on the case. For instance, it may indicate that the provider will configure the equipment, without specifying how this configuration will be done.

The following list shows examples of items that can be included in the Service Definition for the configuration and management of the wireless network:

- Architecture:
  - Centralised/Distributed/Standalone or adhoc (all the devices communicating peer-to-peer without controller or APs).
  - One/Several wireless controllers (for redundancy, due to the size of the network, etc.).
  - One/Several wireless access points.

- CNaaS can offer the customer, for instance:
  - The wireless network design will consist of a minimum of one access point.

- The wireless network design will consist of a minimum of one controller and access point.
- The exact number of access points and their location will be jointly reviewed by the provider and the customer.
- The service will cover a minimum of two SSIDs: eduroam and a guest network, although more SSIDs can be defined.
- For eduroam, differentiated access will be provided for the customer's employees and eduroam guests.
- The provider will assist with the setup of the customer's profile on cat.eduroam.org, so that each user can download their own installation.

3.4.1.5 *Configuration and Management of Additional Network Services*

The provider may offer the customer the configuration and management of services that are not specific pieces of equipment or links on the network but are network-related services. As in the previous sections, the level of detail given in the service definition may vary depending on the case. For instance, it may indicate that the provider will configure the additional service, without specifying how this configuration will be done.

The following list shows examples of items to be included in the service definition for the configuration and management of additional network services:

- List of supported additional network services (other ICT services such as email, web, directory service or other servers can be out of the scope of the service):
  - DHCP
  - DNS
  - VPN
  - RADIUS
  - LDAP
  - NTP
  - VoIP
- Additional network services:
  - The primary and secondary DNS servers will be managed by the provider. The resolver service will not be included.
  - The customer will be provided with a graphical user interface to interact with the service (to add DNS entries/NTP servers...).
  - The service configuration will be automated.
  - The provider will offer its own IPv4 and IPv6 address blocks for DHCP and/or SLAAC.
  - IP addresses assigned via VPN will not be on the same ranges as on the local network.

3.4.2 Service Elements

The following subsections show the items that should be agreed between the provider and the customer beforehand for each service package and can be changed to fit the needs of each provider, customer and service.

3.4.2.1 *Supported Network Items or Servers*

The provider, through the CNaaS service, should define, update and maintain a list of CNaaS-supported network items and servers from different vendors for each one of the network layers and services, including minimum supported software and hardware versions. This list should include the support of standard protocols, agreed by the provider and the customer during the Design Stage. The list of supported network items or servers should include, for instance:

- Switches
- Routers
- Firewalls
- Wireless controllers
- Servers
- Network Attached Storage systems
- Radio links

It is recommended that the provider offers the service using automation tools that facilitate the replication of the configuration in the network items and servers and has a configuration management system (CMS) with the databases and tools to manage the configuration data for all of them. Thus, for instance, every time a new device is included in the CNaaS service, it can be registered in the system through the mechanism provided by the provider, which should automatically generate the monitoring configuration.

The network equipment or servers of brownfield services also needs to be included in the Supported Network Items or Servers list.

3.4.2.2 *Equipment Procurement*

There are four possibilities for a model that the provider and the customer can agree related to the equipment procurement, depending on who is making the specification and who is running the procurement and owns the bought equipment:

- The provider makes the equipment specification and runs the procurement.
- The customer makes the equipment specification and runs the procurement.
- The provider makes the equipment specification and the customer runs the procurement.
- The customer makes the equipment specification and the provider runs the procurement.

As an equipment specification made only by the customer might lead to incompatibilities between the procured equipment and the provider's expertise, the provider and the customer may also need to jointly work on the equipment specification.

3.4.2.3 *Equipment Ownership*

There are two possibilities, once the procurement is done:

- The provider owns the equipment
- The customer owns the equipment

The ownership of the equipment must be agreed beforehand.

3.4.2.4 *Physical Installation of the Equipment*

There are two main options related to the physical installation of the equipment:

- The provider will be responsible for the physical execution of the work, including but not limited to assembly and connection of equipment, restart of power on equipment etc.
- The customer will be responsible for the physical execution of the work, including but not limited to assembly and connection of equipment, restart of power on equipment etc.

A third scenario with shared responsibility is also possible. For instance, the initial installation is done by the provider, but later smaller changes, cable patching and so on is done by the customer or a third party under the customer's responsibility. For any of the options, it is exceptionally important to clearly define the responsibilities of both sides to avoid misunderstandings.

3.4.2.5 *Level of Redundancy*

The level of redundancy must be specified for each supported package, layer and service. For instance, there can be some redundant elements in a layer that are not redundant in another layer. Some examples can be:

- Redundant/non-redundant core layer (redundancy is highly recommended for the core network).
- Redundant/non-redundant distribution.
- Redundant/non-redundant access.
- All core equipment will have redundant power supplies, fans, supervisors, etc.
- All the core links will be redundant.
- The redundant architecture will include network elements and links at all levels except access ports.
- The architecture is partially redundant, with redundancy in some network elements or links (that need to be specified).
- The wireless network service will have redundant controllers.

3.4.2.6 *Software Tools*

CNaaS will use a set of tools that will be defined by the provider and does not need to be included in the Service Definition, although it is up to the provider to include them if desired.

Different tools may be used for:

- Customer Relationship Management (CRM)
- Monitoring
- Ticketing
- Inventory
- Configuration management and Backup
- Billing

The integration between the different tools can be defined.

Due to the nature of the CNaaS service, it may be necessary to have a database tool for the location of buildings, room numbers, locally specific information, rack access keys, etc.

3.4.3 Change Management

The exact scope of the required changes related to any part of the CNaaS service should be defined in advance. It is suggested to follow the ITIL recommendations and processes for Change Management [ITIL-CM]. What will be considered a standard change (pre-authorised, with an accepted and established procedure, possibly automated), a normal change (requires a Request For Change (RFC) and/or the CAB approval) or an emergency change (must be introduced as soon as possible, requires ECAB approval) should be identified. Once identified, different changes can be included in the service (for instance, those changes that can be automated), while others can be excluded (like manual or complex changes). Some examples of the type of changes that could be included or excluded are given below.

The service can include the following standard changes:

- Software upgrades.
- Changing common global configuration parameters like NTP server, console password, etc.
- Adding new VLANs with attributes.
- Adding or changing routed IP prefixes.
- Provisioning security measures.
- The VLAN for any port in the wired network.
- The SSID for the wireless network.
- The access-lists rules for core equipment.
- Security rules in the firewalls.
- DNS modifications.
- Other type of change agreed between the provider and the customer.

The service does not include the following changes:

- The core architecture routing design.
- The wireless setup on the individual client.

The list of changes should be regularly reviewed, re-negotiated and updated as appropriate.

3.4.4 Incident Management

An incident is defined as an unplanned interruption of the service, or the failure of a service component that has not yet impacted the service. A problem is a cause of one or more incidents. The aim of incident management [ITIL-IM] is to restore the service to normal service operation as quickly as possible through a workaround or a permanent solution to the problem. A definition of what normal service operation means is desirable (for instance, whether any packet loss or jitter in the service is acceptable).

3.4.4.1 *Types of Incident*

The incidents are usually classified in categories according to their impact and urgency, and given priority levels. The provider must offer a way to classify incidents to the customer. Common ways to classify incidents are:

- Non-critical/Critical
- Low/Medium/High
- Very Low/Low/Medium/High/Critical

For instance, an incident can be considered Critical if the service is not reachable at all or degraded by more than <n%> packet loss, has more than a specified jitter or latency between two fixed points or affects certain critical customers.

A special type of high priority incident is a Major incident. Major incidents have a direct impact on the business (they typically affect a lot of customers at a time / affect VIP customers / affect the customer's reputation) and should trigger a specific process to handle them.

3.4.5 Support Service

The provider and the customer should agree the level of the support service that will be provided, including clear steps to take for each type of incident. The list of elements that such agreement might include:

- Number of hours per day
- Service support over weekends and holidays
- Calendar (holidays should be taken into account and they may be local to a city or a region)
- Response time
- Resolution time

Some common options are:

- 24x7: The support service will be offered 24 hours a day, 7 days a week, with a response time of 1 hour and a resolution time of 4 hours from the registration of the incident.

- 8x5 next business day (NBD): The support service will be offered 8 hours a day (from XX:XX to YY:YY), 5 business days a week, except holidays, with a response time of 1 hour and a resolution time of 4 working hours from the registration of the incident.

The provider and the customer should agree the different levels of the support service that will be provided. For instance:

- The helpdesk will be run by the customer and will provide a single point of contact for all trouble ticket reports.
- The provider will offer second- and third-line operations and it must be operated in collaboration with the IT staff/helpdesk at the institution, which will provide the first-line support.
- During the operation stage, the NOC, in coordination with the customer helpdesk, will follow the daily operations of the networks (events, incidents, problems) on a 24x7 basis.

3.5 Service Policy

It is important to define the Key Performance Indicators (KPI) that will be used to measure the quality of the service and the expected Service Level Targets (SLT). The following subsections show some examples of parameters and paragraphs that can be included in the Service Definition regarding Service Level Management [ITIL-SLM], provider/customer responsibilities and communication flows.

3.5.1 Service Level Management and Service Availability

To measure the quality and the performance of the service, relevant objective parameters and expected scheduled downtimes need to be agreed beforehand.

3.5.1.1 *Key Performance Indicators (KPI)*

Key Performance Indicators (KPI) need to be defined per time period for Service Level Management. Some examples are:

- Number of incidents
- Number of problems
- Number of implemented standard changes (not approved by the CAB)
- Number of implemented normal changes
- Number of implemented emergency changes
- % of changes that caused incidents
- Average change closure duration (between Request For Change (RFC) is raised and closed)
- Average time to respond to an RFC
- Average time to solve critical incidents
- Average time to solve non-critical incidents
- Average time to close request tickets (information, documentation)

- Average time to solve problems

The exact list of KPIs and the time period must be agreed between the provider and the customer. It can be reviewed and re-negotiated as needed and the contract should be updated accordingly.

3.5.1.2 *Service Level Targets (SLT)*

For each service package, availability is defined as the total number of minutes in a calendar month during which the service is available, divided by the total number of minutes in a calendar month and represented as a percentage.

The Service Level Target (SLT) for CNaaS availability for a certain period should be agreed (for instance, <n%> monthly availability) [ITIL-SLM], ignoring planned maintenance windows.

If there are any constraints, they should also be stated in the contract. For instance, if the helpdesk is responsible for opening incidents and escalating them to the second level when needed, the expected SLA times for incidents will begin once the incident is escalated to the second level (for instance, via the ticketing system).

The following examples of Service Level Targets can be defined:

- The Time to Respond to a critical incident ticket target (for instance, 30 minutes).
- The Time to Respond to a non-critical incident target (for instance, 24 hours).
- The Time to Respond to a request target (for instance, 24 working hours).
- The Time to Fix a critical incident target (for instance, 4 hours).
- The Time to Fix a non-critical incident target (for instance, 48 hours).
- The Time to make a Change; target times are (RFC required):
  - For standard changes (for instance, 48 hours).
  - For normal changes (for instance, 2 weeks, after the CAB has accepted the change).
  - For emergency changes (for instance, 2 hours, after the ECAB has accepted the change).

The exact list of SLTs and the time period must be agreed between the provider and the customer. It can be reviewed and re-negotiated as needed and the contract should be updated accordingly.

3.5.1.3 *Scheduled Downtimes*

The provider should inform the customer how scheduled downtimes will be handled. For instance:

- Scheduled downtimes or planned maintenance windows will be accepted by the CAB, except for emergency changes, that will be accepted by the ECAB.
- Once agreed, downtimes will be announced by the provider via email at least <n> days before they happen, except for emergency changes, which will be announced as soon as possible. They will include the reasons for the scheduled maintenance and the expected downtime.
- Upgrades and replacements in the core and distribution layers can be done during working hours (for instance, if all architecture components are redundant). The access layer maintenance tasks will need to be agreed with the customer (as access ports are not usually redundant).

A specific maintenance window can be agreed for some tasks. Pre-agreed weekly or monthly windows can be defined during the Design Stage, so that maintenance tasks are always performed during this time slot. Then, the provider will only have to inform the customer of the task, date and duration of the task.

3.5.2 Responsibilities

The responsibility demarcation point between the provider and the customer should be defined. For instance, for the wired network it can be the port on the managed equipment towards the infrastructure managed by the customer.

The Service Definition should clearly reflect the provider and the customer responsibilities.

3.5.2.1 *Service Provider Responsibility*

The provider can be responsible, for instance:

- For at least one on-site visit to get to know the network before starting to offer CNaaS services.
- For managing the equipment and services specified in the service description within the boundaries of KPI defined for the service.
- For the correct patching update of the network items managed by the provider, in order to avoid security leaks. If an upgrade on a CNaaS-covered device triggers an update on a customer managed device, the provider and the customer should collaborate and coordinate the actions to prevent the service from being affected.
- For providing and maintaining the issue tracking system (trouble-ticketing system) for the second and third level support that the provider is responsible for.
- For providing procedures for Requests For Changes, issue and problem reports.
- For responding within the KPI boundaries to the justified Requests For Changes on the managed equipment from the service customer.
- For responding within the KPI boundaries to the reports about the problems and incidents from the service customer.
- For providing and maintaining the tools required for providing this service and manage automation.
- For providing second and third line support for the issues reported by the service customer.
- For maintaining the technical logs with the information about the network items, services and servers and ensure appropriate information security for these logs.
- For maintaining a central CMDB (Configuration Management Database) for all network equipment and services.

The service provider will not be responsible, for instance:

- For the performance or incidents on external links or pieces of equipment not covered by the CNaaS agreement (like cloud services, multi-tier structures, testbeds, etc.).
- For the information security of the end-user devices.

- For small changes to the customers physical infrastructure (e.g. patch cables, power supplies and cabling).
- For establishing appropriate environmental conditions for the equipment stored on customer premises (temperature humidity).
- For providing fire-protecting infrastructure and policies at the customer site.
- For the configuration setup and management of the local customer devices not included in the service.

3.5.2.2 *Service Customer Responsibility*

The customer can be responsible, for instance:

- For the entire passive network infrastructure within the campus (cabling, patch-panels, racks and the like).
- For the proper operation and up-to-date configuration of all the ICT equipment (e.g. switches, routers, computers, laptops, servers, IP telephones, access points, etc.) in the campus which is not explicitly mentioned as being managed by the service provider.
- For the information security of all the ICT equipment in the campus mentioned in the previous bullet (e.g. patching software, applying antimalware software and similar).
- For controlling physical access to the equipment managed by the provider. Access can be allowed only to authorised persons from the provider, customer and equipment vendor. The list of authorised persons will be agreed between the customer and the provider. The procedure for the physical access should also be agreed, including:
  - Authorisation procedure.
  - Changing the list of authorised persons.
  - Access logging.
  - Information sharing about physical access - who should receive / acknowledge / approve the physical access to the devices.
- For allowing service provider personnel physical access to the managed equipment.
- For maintaining the environmental conditions (e.g. temperature, humidity, power consumption) of all the ICT equipment at the customer's facilities managed by the service provider within the boundaries defined by equipment manufacturer.
- For following fire safety guidelines (e.g. having enough gas for fire suppression in the data centre or assistance for fire extinction).
- For planning the location of Wi-Fi access-points appropriately, according to building and fire regulations guidelines.
- For executing simple operations on managed equipment (e.g. power cycle, changing the patch cable, and similar) only upon the request or with the permission of the service provider.
- For actively participating in debugging and problem-solving activities on managed ICT equipment by timely providing relevant information to the service provider, especially upon the request from service provider and executing previously mentioned simple operations.
- For following the Requests For Changes and issue reporting procedures and to use the tools for reporting the problems and issues specified by the service provider.

- For providing the first line of support to the users of the campus network. The provider will not react to calls from the end users from the campus network. The customer should designate persons authorised to communicate with the provider.
- For any potentially malicious end user activities.
- For informing their users of all relevant procedures and policies, of how the network and the resources should be used, including - if appropriate - relevant elements of the contract between the provider and the customer.
- For supporting the CNaaS service on-site and providing a point of contact for all trouble ticket reports (if the helpdesk is run by the customer).

The customer will not be responsible, for instance:

- For the configuration and management of the equipment under the CNaaS agreement.

3.5.3 Communication Flows

The provider and the customer should agree the different communication channels between the previously defined roles as well as the expected communication flows and define them in the contract. The following subsections show some examples that can be used when defining the service.

3.5.3.1 *Communication Flows for Service Level Management*

The provider and the customer should specifically agree on the communication flows for Service Level Management, to review the quality of the service.

The following list gives some examples:

- Regular/On-demand meetings:
  - The Service Manager from the provider CNaaS team and the Service Coordinator from the customer team should regularly meet (face-to-face or remotely via VC) to follow-up on the needs of the service and possible improvements.
  - The Service Coordinator or the Service Managers can require adhoc meetings when needed, with a maximum of <n> meetings per month.
- Regular/On-demand reports:
  - Based on the monitoring and the logs, the Service Manager will periodically (or at customer request, if preferred) provide customer with the following reports, which can be automatically generated where possible:
    - Availability statistics.
    - SLT and KPI review results, including SLA violations, if any.
    - Service improvement plan.
    - Incident report.
  - The customer can ask for special incident reports in relevant cases, with a maximum of <n> incident reports per month.
- Complaints or special cases:

- Complaints will be sent to the Service Manager and discussed during regular meetings, unless an urgent incident requires a special meeting.
- In case of relevant critical incidents, any side can require special meetings with a representative of the other side.

3.5.3.2 *Communication Flows for Incident Management*

The provider and the customer should agree the alarm and ticket recipients and escalation procedures, which will depend on the resolution times (see Section 3.4.5).

Alarm Recipients

Several options can be considered:

- Alarms triggered on the monitoring system will be sent to the alarm console at the helpdesk and open a ticket in the helpdesk system.
- Alarms triggered on the monitoring system will be sent to the alarm console at the provider's NOC.
- Alarms triggered on the monitoring system will be sent to the alarm console at the provider's NOC and the helpdesk, and open a ticket in the helpdesk system.

Notifications can be automatically sent to the customer helpdesk by the monitoring system and while the monitoring system cannot monitor itself, the central monitoring system at the provider can issue notifications if the monitoring system has a failure itself.

The provider and the customer may agree on different recipients depending on the nature of the alarms (for instance, when major incidents are detected). Alarms can also trigger automatic calls or send text messages.

Ticket Recipients

There are several options:

- The helpdesk receives the alarms.
- The provider's NOC receives the alarms.
- Both the helpdesk and the NOC receive the alarms.

Escalation Procedures

The escalation procedures between the provider and the customer in case of an incident should be defined and agreed by both parties. For instance:

- The Service Coordinator at the customer may escalate the incident to the Service Manager or the Product Manager at the provider when an incident is not solved in the agreed resolution time or when there is a major incident. Some common options are:
  - Service Manager if the incident is not solved in the agreed resolution time.
  - Service Manager when the Service Level Target (SLT) is reached for an incident.
  - Product Manager if the incident is not solved in the agreed resolution time plus <n> hours.

- Product Manager when 2 times the SLT is reached for an incident.
- Product Manager if there is a major incident.
- Provider Chief Technical Officer (CTO, Management) when 3 times the SLT is reached for an incident.

- If an issue is escalated, the incident must be sent to the provider's NOC (for instance, via the Trouble Ticketing System).

3.6 Duration, Changes and Termination

The contract should include information about the service's duration, the scope for the provider and customer making changes to the service during the contract period and causes for termination. Both parties could request advice from their legal specialists.

Some examples are:

- Duration of the service:
  - The service will begin when the agreement is signed and will remain in effect for an initial term of <n> months / years.
  - This service only applies to the pilot period in the project CNaaS (if it is a project) for the duration of <n> months / years.

- Possibilities to change the service:
  - The agreement may not be modified, amended, changed or discharged, in whole or in part, except by an agreement in writing signed by the provider and the customer.

- Renewals:
  - The agreement will automatically renew for successive <n> years unless the provider or the customer provide at least <n> days prior written notice to the other party of their desire not to renew the agreement.

- Causes for termination:
  - The provider or the customer may terminate the agreement immediately should the other party admit in writing its inability to pay its debts as they become due.

- Notice period for termination:
  - In the event either party desires to terminate this agreement or any of the associated services, the party shall provide at least <n> days written notice of the termination date to the other party, unless the receiving party agrees, in writing, to a shorter notice period.

3.7 Prices and Billing

Several charging model options are possible and can be added or combined according to the offered services. Some examples are:

- Fixed fee (one-off, monthly, annual, etc.).
- Variable charging (depending on the number of tickets, requests, number of users, number of students, connected buildings, etc.).
- Free of cost (included in the basic connectivity quota, paid by the government, etc.).
- Part of the connection fee to the NREN.
- Specific quota for each service package.
- Specific quota for each managed device, additional service, building, users, etc.

The provider can generate a price list of the different options offered to the customers.

The billing periods, if applicable, also must be defined. For instance:

- Monthly
- Quarterly
- Yearly

3.8 GDPR Privacy Note

Depending on where sensitive data is stored and whether the provider has access to it, different policy notes may be used. In the process of the GDPR assessment, the usage of the <service_name> data inventory Template [Template] and GDPR Templates [GDPRtemplate] from the GÉANT wiki might be considered to determine what data the GDPR applies to is processed. Both the provider and the customer obtain the advice of their GDPR specialists.

In some cases, a separate contract that regulates the relationship between the controller (who determines the purposes of the processing of personal data) and the processor (who processes the data) might be needed, especially if the provider has some subcontractors (e.g. a company that maintains servers or storage where customer's monitoring data is stored) which could obtain access to the customer's private data. The following paragraphs are an example of what should be defined for each service package.

3.8.1 What Data is Processed?

The provider and the customer should agree who is keeping CNaaS-related logs of events in the network items, servers, services and monitoring system(s), and who is able to access the logs for troubleshooting. These logs should contain at least the following data:

- The network item, server or service involved.
- The date and time of the event.

- The IP address of the user.

The data controller of this data should also be specified.

3.8.2 Purposes of the Processing

Logs are kept to investigate and solve network problems and incidents, open tickets and collect aggregate statistics about the services.

The CNaaS provider has no means to correlate technical log data with personal data. The provider will not provide technical log data to anyone, unless ordered to do so by law, for example as part of a criminal investigation.

The legal basis for processing personal data is the customer's consent.

3.8.3 Consent

The customer consents to have the data listed above logged by the provider.

3.8.4 Data Storage

All the data is stored within the EEA (European Economic Area).

3.8.5 Retention Period

The provider and the customer should agree on the retention period for which a technical log of the transactions will be stored. For instance, a period of 6 months or 1 year from the date of the event.

3.8.6 Security of Data

Access to the technical logs data is restricted and can only be accessed in a secure way by CNaaS staff. To prevent unauthorised access or disclosure, the provider has put in place technical and organisational procedures to secure the data collected.

3.8.7 Customer Rights

The customer may request a copy of the technical log data the provider is storing of the events as described in Sections 3.8.4 and 3.8.5.

3.8.8 Changes to this Notice

This privacy statement may be changed at the provider's discretion at any time. If the provider makes changes to this notice, the last modified date is updated, and the customer notified.

4 Conclusions

Several European NRENs are facing the challenge of offering campus network management services to their connected institutions. These are either their end institutions, which have difficulties recruiting qualified network technicians, or their governments, as part of the development of their digitalisation strategies.

The *Monitoring and Management* Task (Task 3) and the *Network Services Evolution and Development* Task (Task 2) in the *Network Technologies and Services Development* Work Package (WP6) of the GN4-3 project have worked together to gather requirements from the NRENs on offering campus management services and then determine how the project might offer some common organisational, administrative and technical approaches and strategies.

After several discussions with the NRENs that are currently offering or planning to offer these services, it can be concluded that there is no single, common approach. However, the GÉANT project is providing help in several ways.

One way is by providing them with a Service Definition Template/Checklist where they can find all the relevant topics to consider when writing their own documents such as service definitions, SLAs, contracts, etc. This document can be adapted to the various needs and strategies of the NRENs for offering network management functions. As the Service Definition Template is based on ITILv3 processes and functions, a future step might be to align the document to ITILv4 principles, concepts and practices once all the ITILv4 documentation is available.

Another way for the GÉANT project to help the NRENs is through organising events and infoshares to allow NRENs with different levels of maturity to share their knowledge, experiences and ideas. WP6 T3 has already started working in this area by participating in several meetings, organising the NEMMO workshop and planning further events.

As orchestration, automation and virtualisation (OAV) techniques are already commonly used by NRENs that offer campus network management services, the work on CNaaS in WP6 T3 is naturally linked to the work on OAV under WP6 T2. The current work on the definition of a reference architecture and framework for OAV, the OAV terminology and the creation of a public regularly updated wiki can also be used as a reference for campus network management services. A focus group under WP6 T2 has been created to explore and support CNaaS, not just from the perspective of network infrastructure and services management and operations, but also in the area of methodology, community and user engagement.

The GÉANT project can also work on promoting the usage of WP6 tools and services such as NMaaS, which can be helpful for service provisioning, as well as perfSONAR and WiFiMon for monitoring campus networks.

References

[9SIG-NOC]	9th SIG-NOC Meeting https://wiki.geant.org/display/SIGNOC/9th+SIG-NOC+meeting
[9SN-ARNES]	https://geant.app.box.com/s/68pzsqbkbcx9683j8qybgoi5zlu7jhtz
[9SN-ARNES2]	https://geant.app.box.com/s/0fvbk4tcjvekjd40ehvf55oud4gnthan
[9SN-CARNET]	https://geant.app.box.com/s/fji5tdbv2dhxlfed137kl7mj806mmi16
[9SN-SUNET-CSUC]	https://geant.app.box.com/s/n7f4km3yktx4e6jy96dba2ly66ceb5h4
[10SIG-NOC]	10th SIG-NOC Meeting https://wiki.geant.org/display/SIGNOC/10th+SIG-NOC+meeting
[10SN-GEANT]	https://geant.app.box.com/s/ff3qjlax4d68aznf1zmmovsd6bh54vhg
[ANSIBLE]	https://www.ansible.com/
[AXELOS]	https://www.axelos.com/
[CARNET-E-SKOLE]	https://www.e-skole.hr/en/results/adequate-ict-infrastructure-in-pilot-schools/
[D6.2]	Deliverable D6.2 *Automation and Orchestration of Services in the GÉANT Community* https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D6-2_Automation-and-Orchestration-of-Services-in-the-GEANT-Community.pdf
[GDPR]	https://gdpr-info.eu/
[GDPRtemplate]	https://wiki.geant.org/display/gn43wp6/GDPR+Templates (Note that eduGAIn credentials are required to access this page)
[ITILv3]	ITIL® Service Lifecycle Publication Suite, 2011 Edition, ISBN: 9780113313235
[ITILv4]	https://wiki.en.it-processmaps.com/index.php/ITIL_4
[ITIL-CM]	ITIL® Service Transition, 2011 Edition, ISBN: 9780113313068
[ITIL-IM]	ITIL® Service Operation, 2011 Edition, ISBN: 9780113313075
[ITIL-SLM]	ITIL® Service Design, 2011 Edition, ISBN: 9780113313051
[LITNET-WIFI]	https://www.litnet.lt/lt/vykdomi-projektai/rezultatai
[NAV]	https://nav.uninett.no/#download, https://github.com/Uninett/nav
[NEMMO]	Workshop on Network Management and Monitoring https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring
[NM-AMRES]	https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635136/Inside%20campus%20networks%20-%20AMRES%20UCs%20-%20Copenhgen%202019%20-%20final.pdf
[NM-AMRES]	

[NM-ARNES]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635132/arnes_nms_workshop_cop_2019_oct.pdf

[NM-CARNET]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635133/lightning_talks-1.pdf

[NM-CN-SD]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635142/CNaaSServiceDefinition-NEMMO-WS-MIG-GN4-3-WP6-T3.pdf

[NM-FINAL]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/133759224/2019-10-22-MandM%20summary.pdf

[NM-FUNET]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131633379/Funet%20Kampus%20Service.pdf

[NM-FUNET2]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131633380/Funet%20Kampus%20Configuration%20Automation.pdf

[NM-GRENA]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635030/Perfsonar_Grena.pptx

[NM-GRNET]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131634938/Copenhagen_nkostopoulos.pdf

[NM-KIFU]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635135/Network_Management_KIFU%CC%88_20191022_1.1.pptx

[NM-NMAAS]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/133759028/WoNM%26M%20Copenhagen%20October%202019%20NMaaS%20as%20a%20platform%20for%20management%20service%20outsourcing%20v1.0.pdf

[NM-SUNET]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635130/CNaaS%20-%20GE%CC%81ANT%20workshop%20Dennis.pdf

[NM-SUNET2]
https://wiki.geant.org/display/PUB/Workshop+on+Network+Manag

ement+and+Monitoring?preview=/131629403/131635139/CNaaS%20software%20architecture%20GeantMnMworkshopOkt2019.pdf

[NM-SURFNET] https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131634984/session1-monitoring-management-surfnet.pdf

[NM-SURFNET2] https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635051/session2-monitoring-and-networkmanagement.pdf

[NM-UNINETT] https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/131635129/cnaas%20in%20Noreway%20gn4.3%20workshop%20Oct%202019-Uninett-3222.pdf

[NM-UNINETT2] https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/133759056/2019-10-22%20Monitoring%20and%20alert%20aggregation.pdf

[NM-WB] https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring?preview=/131629403/133759303/Workshop%20on%20Network%20Management%20and%20Monitoring_Copenhagen%2C-Nov.2019-v10.pdf

[NMAAS] https://www.geant.org/Services/Connectivity_and_network/NMaaS

[OXIDIZED] https://github.com/ytti/oxidized

[OAV-WIKI] https://wiki.geant.org/pages/viewpage.action?pageId=123792049

[OAV-COM-PORTAL] https://wiki.geant.org/display/OAV/OAV+COMMUNITY+PORTAL

[OAV-SURVEY] https://wiki.geant.org/display/gn43wp3/GN4-3+Future+Service+Strategy+Workshop?preview=/120492175/122756591/2019-05-09-OAV-Survey-Results-by-Topic.pdf (Note that eduGAIn credentials are required to access this page)

[SIG-NOC-TOOLS] 3r SIG-NOC Tools Survey Report https://wiki.geant.org/display/SIGNOC/SIG-NOC+Tools+Survey+2019

[SUNET-CNAAS] https://wiki.sunet.se/pages/viewpage.action?pageId=30441624

[SURFNET-WIFI] https://www.surf.nl/en/surfwireless-wifi-as-a-service

[Template] https://wiki.geant.org/display/gn43wp6/%3Cservice_name%3E+data+inventory+Template (Note that eduGAIn credentials are required to access this page)

[TNC-HEANET-OAV] Automation and Orchestration, TNC BoF session presentation https://wiki.geant.org/download/attachments/123793644/TNC19-OAV-HEANet-v1.pdf?version=1&modificationDate=1561006298421&api=v2

[WIFIMON] https://www.geant.org/wifimon

Glossary

CAB	Change Advisory Board
CI/CD	Continuous Integration/Continuous Delivery
CLI	Command-Line Interface
CMDB	Configuration Management Database
CNaaS	Campus Network Management as a Service
CRM	Customer Relationship Management
CTO	Chief Technical Officer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECAB	Emergency Change Advisory Board
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MPLS	Multiprotocol Label Switching
NMaaS	Network Management as a Service
NOC	Network Operations Centre
NTP	Network Time Protocol
NREN	National Research and Education Network
OAV	Orchestration, Automation and Virtualisation
perfSONAR	Performance focused Service Oriented Network monitoring ARchitecture
PMP	Performance Measurement Platform
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Change
SIG	Special Interest Group
SIG-NOC	Special Interest Group - Network Operation Centres
SLA	Service Level Agreement
SLT	Service Level Target
SNaaS	School Network Management as a Service
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
VC	Video Conference
VLAN	Virtual Local Area Network

VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VRF	Virtual routing and forwarding
VxLAN	Virtual Extensible LAN
WIFI	Family of wireless networking technologies defined in IEEE 802.11x
WiFiMon	Wireless Crowdsourced Performance Monitoring and Verification
WP	Work Package
ZTP	Zero Touch Provisioning