International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3515

(07/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Cloud Computing

Cloud computing – Functional architecture of Network as a Service

Recommendation ITU-T Y.3515

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3515

Cloud computing – Functional architecture of Network as a Service

Summary

Recommendation ITU-T Y.3515 provides Network as a Service (NaaS) functional architecture by specifying functionalities and functional components as well as reference points for the operation support system (OSS). This Recommendation also describes the mapping between functionalities and functional requirements of NaaS, relationship between the NaaS functional architecture and software-defined networking (SDN), and illustrated usage of SDN and network functions virtualization (NFV) in support of the NaaS functional architecture.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3515	2017-07-07	13	11.1002/1000/13255

Keywords

NaaS, NaaS functionality, NaaS functional architecture, NaaS functional component, NaaS product, network as a service.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3515

Cloud computing – Functional architecture of Network as a Service

1 Scope

This Recommendation provides the Network as a Service (NaaS) functional architecture by specifying functionalities and functional components as well as reference points for the operation support system (OSS).

The scope of this Recommendation consists of:

– Overview of the NaaS functional architecture;

– NaaS functionalities;

– NaaS functional components;

– OSS reference points in the NaaS functional architecture.

This Recommendation also provides appendixes describing:

– The mapping between NaaS functionalities described in this Recommendation and NaaS functional requirements specified in [ITU-T Y.3512];

– The relationship between the NaaS functional architecture and software-defined networking (SDN);

– An illustrated usage of SDN and network functions virtualization (NFV) in support of the NaaS functional architecture.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.2320] Recommendation ITU-T Y.2320 (2015), *Requirements for virtualization of control network entities in next generation network evolution*.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[ITU-T Y.3302] Recommendation ITU-T Y.3302 (2017), *Functional architecture of software-defined networking (SDN)*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016) | ISO/IEC 17789:2014, *Cloud computing – Framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service*.

[ITU-T Y.3521] Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management*.

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 activity [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.3 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 cloud service product [ITU-T Y.3502]: A cloud service, allied to the set of business terms under which the cloud service is offered.

NOTE – Business terms can include pricing, rating and service levels.

3.1.6 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.7 Network as a Service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.8 product catalogue [ITU-T Y.3502]: A listing of all the cloud service products which cloud service providers make available to cloud service customers.

3.1.9 role [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.10 service catalogue [ITU-T Y.3502]: A listing of all the cloud services of a particular cloud service provider.

3.1.11 service chain [ITU-T Y.3512]: An ordered set of functions that is used to enforce differentiated traffic handling policies for a traffic flow.

3.1.12 service level agreement [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.13 software-defined networking [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.1.14 sub-role [ITU-T Y.3502]: A subset of the activities of a given role.

3.1.15 tenant [ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 NaaS product: A cloud service product for which the cloud service related to that product is of the NaaS cloud service category.

3.2.2 network function: A function of a network infrastructure whose external interfaces and functional behaviour are well specified.

NOTE – Examples of network functions include network switches and network routers.

3.2.3 network service: A collection of network functions with a well specified behaviour.

NOTE – Examples of network services include content delivery networks (CDNs) and IP multimedia subsystem (IMS).

3.2.4 physical network function: A network function implemented via a tightly coupled software and hardware system.

NOTE – Examples of physical network functions include physical network switches and physical routers.

3.2.5 virtualized network function: A network function that can be deployed as a software on a NaaS cloud service provider infrastructure.

NOTE – Examples of virtualized network functions include virtual switches and virtual routers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BSS Business Support System

CCRA Cloud Computing Reference Architecture

CCS Cloud Compute and Storage

CDN Content Delivery Network

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

DevOps Development and Operation

DNS Domain Name System

EMS Element Management System

ID Identifier

IMS IP Multimedia SubsystemIP Internet Protocol

IT Information Technology

KPI Key Performance Indicator

L2 Layer 2

L3 Layer 3

MPLS Multiprotocol Label Switching
NaaS Network as a Service
NC Network Connectivity
NF Network Function
NFV Network Functions Virtualization
NFVI Network Functions Virtualization Infrastructure
NMS Network Management System
NS Network Service
OSS Operation Support System
OTN Optical Transport Network
PNF Physical Network Function
PoP Points of Presence
QoE Quality of Experience
QoS Quality of Service
SDN Software-Defined Networking
SLA Service Level Agreement
vCDN Virtual Content Delivery Network
vEPC Virtual Evolved Packet Core
vIMS Virtual IP Multimedia Subsystem
VM Virtual Machine
VNF Virtualized Network Function
VPC Virtual Private Cloud
VPN Virtual Private Network
VPNaaS VPN as a Service
vRouter Virtual Router
vSwitch Virtual Switch
VXLAN Virtual Extensible Local Area Network
WAN Wide Area Network

5 Conventions

None.

6 Overview of NaaS functional architecture

6.1 Key NaaS characteristics

The NaaS functional architecture aims for a scalable and programmable on-demand network allowing the cloud service customer (CSC) to provision network services (NSs) and resources, as needed, automatically or with minimal interaction with the NaaS cloud service provider (CSP). Key NaaS characteristics to be achieved include:

– **Self-service**: the ability to manage network services automatically or with minimal human interaction. Examples include self-provisioning, self-care and self-design;
– **On-demand**: the ability to deploy and adjust (increase or decrease) network services rapidly and as needed. Examples include fast time-to-market, try before you buy, accelerate innovation, easy migration, update and upgrade;
– **Scalability**: the ability to scale network services and resources (scale out, in, up or down) in response to a large usage demand. Example includes scale-up resources based on traffic growth;
– **Programmability**: the ability to access services features through application programming interfaces (APIs). Examples include programmable quality of service (QoS) and network policy rules;
– **Measured service**: metered delivery of services such that usage can be monitored, controlled, reported, and charged. Example includes case of NaaS CSCs charged only for the services or resources that they use.

6.2 NaaS CSC activities

Activities of the NaaS CSC role are described in clause 8.2 of [ITU-T Y.3502]. These activities are applicable to the case of a NaaS CSC involved in a relationship with a NaaS CSP. Taking the use cloud service activity in CSC-CSP relationship (see Annex A of [ITU-T Y.3502]), Figure 6-1 illustrates the relationships between functional components involved in the use cloud service activity of the CSC:cloud service user sub-role.

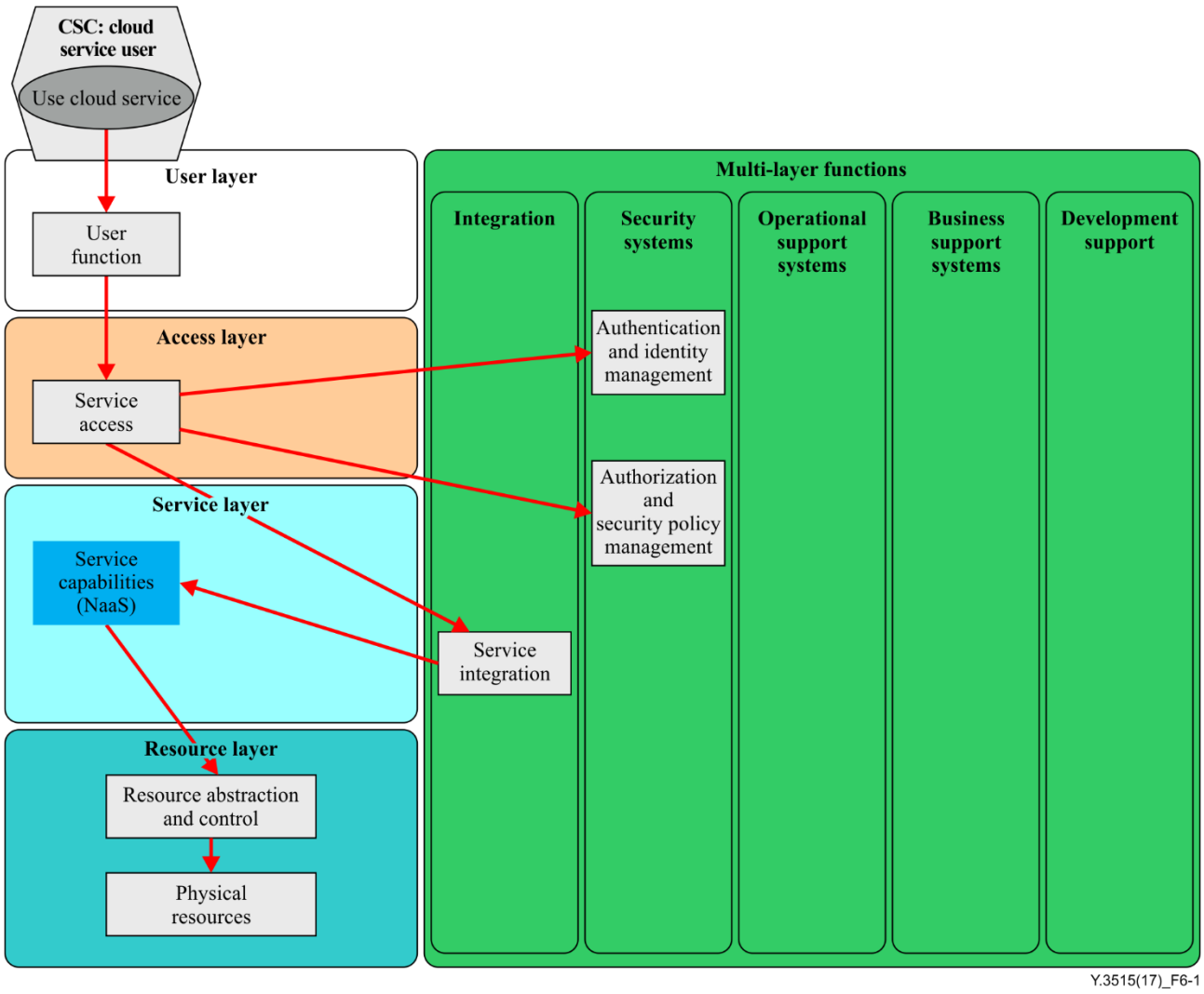

Figure 6-1 – Use of a NaaS service

As for any cloud service, NaaS service capabilities (together with NaaS administration and business capabilities) are positioned in the service layer of the cloud computing layering framework (see clause 9.2 in [ITU-T Y.3502]).

NaaS services are made available to the CSC:cloud service users via an endpoint and interface enabled by the service access functional component. The CSC:cloud service user performs the use cloud service activity through the user function functional component, which then invokes NaaS through the service access functional component. The service access functional component performs any authentication of the CSC:cloud service user and establishes authorization to use particular NaaS service capabilities of NaaS. If authorized, the service access functional component invokes the NaaS service's software implementation which then handles the request.

NaaS services provide self-service capabilities allowing the NaaS CSC to control, manage, monitor and optimize the resources offered as a service by the NaaS CSP in a programmable manner.

Resources offered by the NaaS CSP to the NaaS CSC depend on the type of NaaS service (e.g., NaaS connectivity, NaaS applications as described in [ITU-T Y.3512]) being provided by the NaaS CSP. These resources can be negotiated by the NaaS CSC with the NaaS CSP through the use of the service interface provided by the NaaS CSP. For example, subject of such negotiation can cover connectivity parameters for a NaaS connectivity service provided by the NaaS CSP.

Service requests made by the NaaS CSC via the service interface will trigger interactions with other NaaS CSP's functionalities such as evolved real-time OSS functionalities (see clause 7.7) and NaaS

CSP's resource functionalities (e.g., network elements), for example for instantiating network services, network functions, for allocating cloud computing resources and network connectivity resources in NaaS CSP's infrastructure. The service interface can also allow the NaaS CSC to instantiate and operate flexible, scalable and functionally expandable virtualized networks as well as provide unified control and management functionalities to the NaaS CSC for changing, moving, or removing resources associated to such virtualized networks being offered by the NaaS CSP.

6.3 Virtualization of network functions

As described in [ITU-T Y.3512], NaaS services include:

– NaaS application and NaaS platform services such as virtual IP multimedia subsystem (vIMS), virtual evolved packet core (vEPC) and virtual content delivery network (vCDN);

– NaaS connectivity services such as virtual private network (VPN) services and bandwidth on demand.

These NaaS services rely on network services (see clause 3.2.3) and network functions (see clause 3.2.2) provided on-demand by the NaaS CSP to the NaaS CSC. When deployable as software by the NaaS CSP, network functions are known as virtualized network functions (VNFs) (see clause 3.2.5). Examples of such VNFs are virtualized control network entities (see [ITU-T Y.2320]). When implemented via a tightly coupled software and hardware system, network functions are considered as physical network functions (PNFs) (see clause 3.2.4).

Figure 6-2 provides a representation of aspects that need to be controlled and managed by NaaS CSP.

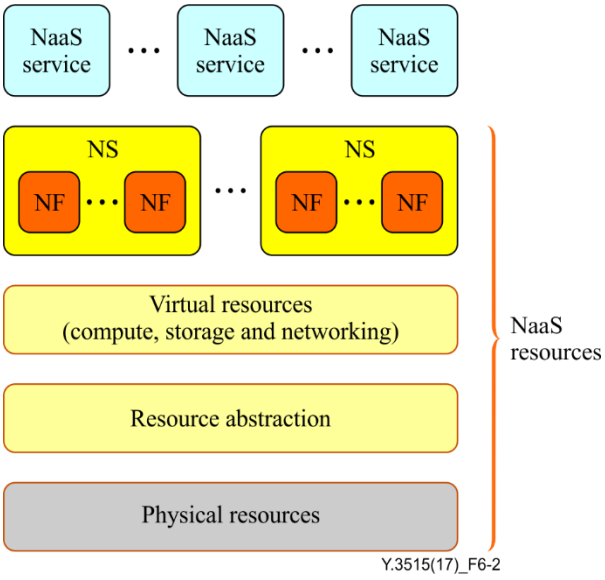

Figure 6-2–Aspects managed by NaaS CSP

NaaS services offered to NaaS CSCs are based on NSs and network functions (NFs) that need to be managed by the NaaS CSP. Although not illustrated in Figure 6-2, connectivity between NFs needs also to be managed by the NaaS CSP, including connectivity between NFs in a given NS and connectivity between different NSs.

Other aspects to be managed by the NaaS CSP include physical (hardware) resources (compute, storage and networking resources), resource abstraction and virtual resources. The main functions of resource abstraction are:

– abstraction of physical resources allowing decoupling of NFs from underlying physical resources;

– allocation of virtual resources from physical resources;

– provision of virtual resources (virtual compute, virtual storage) for execution of NFs as well as virtualized network connectivity resources for interconnecting NFs of a given NS or for interconnecting multiple NSs.

7 Functionalities for NaaS

This clause aims to provide the functionalities which are derived from the functional requirements specified in [ITU-T Y.3512]. The mapping between NaaS service functional requirements and the functionalities described in this clause is presented in Appendix I.

7.1 NaaS business related functionalities

Business related functionalities in the NaaS architecture are mainly related to the interaction between the NaaS CSC and NaaS CSP regarding NaaS products offered by the NaaS CSP. This includes NaaS CSP functionalities related to the selection and purchasing of specific NaaS products from a product catalogue by the NaaS CSC and all other business related aspects, such as billing. An instance of a NaaS product represents the subscription to a NaaS product by a given NaaS CSC.

NaaS business related functionalities cover cloud customer management and cloud product management functionalities supported by the NaaS CSP as per [ITU-T Y.3521] where the cloud customer is a NaaS CSC and the cloud product is a NaaS product. These functionalities include NaaS CSP's functionalities concerned with the lifecycle of NaaS products offered to and purchased by NaaS CSCs, i.e., functionalities related to NaaS products' order management, performance management, usage statistics, as well as the management of NaaS product instances delivered to NaaS CSCs. More details about lifecycle management of cloud products and services can be found in [ITU-T Y.3522].

7.2 Functionalities for NaaS service instantiation

7.2.1 Description of NaaS service instantiation

These functionalities are responsible for the instantiation of a NaaS service following the receipt of a valid NaaS product (and associated NaaS services) order request from a NaaS CSC (e.g., a request for a vCDN service or VPNaaS service). NaaS service instantiation functionalities maps the validated NaaS CSC request to specific NaaS service deployment policies. For the requested NaaS service instance, the NaaS service functionalities requests to the NaaS service orchestration functionalities (see clause 7.3) to realise the corresponding automatic configuration of required NaaS resources (including network services, network functions and resources) in the different infrastructure domains of the NaaS CSP (e.g., in access transport domain, core transport domain and virtualization infrastructure domain) in a programmable manner.

NaaS service instantiation results in the instantiation of NaaS functional components (i.e., NaaS service capabilities and NaaS administration capabilities components) in the service layer [ITU-T Y.3502] of the NaaS CSP. For example, in the case of a VPNaaS service being instantiated, dedicated VPNaaS capabilities functional components will be instantiated in the service layer. These VPNaaS service and administration capabilities provided by the service layer will allow the NaaS CSC to request for management and configuration changes of a VPN instance to the NaaS CSP and also enable the NaaS CSC to request dynamic VPN network reconfiguration.

7.2.2 Modelling for NaaS service instantiation

As part of NaaS service instantiation functionality, a global, coherent and abstract view and representation of NaaS resources (including network resources, network services, network functions and network operational policies) used during the lifetime of the NaaS service instance will be provided and presented to the NaaS CSC. This representation avoids the direct communication and interaction between the NaaS CSC and these NaaS resources (e.g., network elements of the NaaS CSP infrastructure) and masks implementation specific aspects of NaaS resources used in the context

of the NaaS service instance. This abstract view presented to the NaaS CSC also allows real-time configuration change demands from the NaaS CSC to be reflected by the NaaS CSP on its own resources. Therefore, a hierarchical and extensible framework, which can be realised by a set of information models, needs to be designed to hide the protocol specific and/or vendor specific details of the resources being used by the NaaS CSP. The modelled objects being part of these NaaS information models can be grouped as NaaS resource model, NaaS service model, and NaaS service operational policy model.

NaaS resource models reflect in an abstract manner NaaS CSP's resources including their associated topological view across different layers (e.g., layer 2 (L2) and layer 3 (L3)). NaaS resource models designed by the NaaS CSP or cloud service partners (CSNs) (e.g., service developer) are used by the NaaS CSP to represent NaaS CSP's resources at a conceptual level, including physical and/or virtualized network functions as well as connectivity links. NaaS resource models are not exposed to the NaaS CSC.

A NaaS service model is service specific, i.e., specific to the NaaS service being offered to the NaaS CSC by the NaaS CSP but rely on underlying NaaS resource models. Once a NaaS service is instantiated for a NaaS CSC, the corresponding NaaS service model designed by the NaaS CSP is exposed to the NaaS CSC.

A NaaS service operational policy model is service specific, i.e., are specific to the NaaS service being offered to the NaaS CSC. This model defines NaaS CSP-wide policies applicable for the corresponding NaaS service and is designed by the NaaS CSP or CSN (e.g., service developer). During the instantiation of a NaaS service, the NaaS service operational policy model is combined with the NaaS service model and mapped into a target configuration of NaaS CSP's resources (e.g., network elements), according to NaaS resource models.

NOTE – The usage example of modelling is provided in Appendix II.

7.3 Functionalities for NaaS service orchestration

The NaaS service orchestration functionalities are responsible for cross-domain service orchestration within the NaaS CSP, e.g., for a NaaS connectivity service, the functionality will be capable to orchestrate NaaS resources (including network services, network functions and resources) in multiple NaaS CSP domains (including legacy domains and virtualized network domains).

Upon receipt of a NaaS service request from the NaaS CSC, these functionalities are responsible for decomposing, as necessary, the request into several independent requests and for distributing each of the resulting requests to the relevant control functions of the NaaS CSP. An example of a composite NaaS service is a service chain path, i.e., an ordered list of connection points forming a chain of network functions (PNFs and/or VNFs), along with policies associated to the list.

The NaaS service orchestration functionalities interact with the NaaS service instantiation functionalities to address NaaS service decomposition and configuration of requests received from NaaS service instantiation functionalities (see clause 7.2.1).

In case of a non-composite NaaS service request received from the NaaS CSC, the NaaS service orchestration functionalities can transfer this request to the relevant domain control function.

The NaaS orchestration functionalities are also responsible for ensuring that NaaS resources (e.g., NSs, NFs, connectivity) are appropriately instantiated throughout the different NaaS CSP domains (e.g., across one or network domains that can be using different networking connectivity technologies).

7.4 Functionalities for network analytics

Functionalities for network analytics are responsible for data collection from the NaaS CSP's network environment (such as network jitter, delay, packet loss rate, round-trip time, domain name system

(DNS) resolution time) and events listening to continuously monitor NaaS services during their lifecycle. These functionalities help to provide customized analytical network applications and provide the analysed results to the related functional components (such as resource abstraction and control) for further action, including healing the service, appropriately scale up or scale down the service, dynamically adjust routing, etc. The analytical network applications are used to match specific conditions based on the analytical results. Once a condition is matched, the application can activate the pre-defined event and the further actions will depend on the specific policies associated with this condition.

These functionalities can be achieved along with other related functionalities, such as NaaS service instantiation, NaaS service orchestration, resource abstraction and control, and evolved real-time OSS, and can help to complete the whole NaaS service lifecycle management in an iterative way. More details on the lifecycle management of cloud services can be found in [ITU-T Y.3522].

7.5 Autonomic functionalities

Autonomic functionalities in the NaaS architecture are responsible for making decisions on their own, using high-level policies. They constantly check and optimize their status automatically and adapt themselves to changing conditions.

From an operational point of view, closed control loops driven through autonomic functionalities can be included at resource level (PNFs, VNFs) as well as in the different OSS functionalities described in clause 7.8. Typically, a closed loop control is comprised of functionalities for collecting and monitoring data from the system being managed, analysing (through filtering, correlation and other mechanisms), planning (different actions based on inferring trends, finding causes of the problem) and executing the decided plan(s). Autonomic functionalities can therefore involve and rely on the use of network analytics functionalities (see clause 7.4). Policies can be used with control loops to guide their operation (see clause 7.6 regarding policy related functionalities).

7.6 Policy related functionalities

Policy related functionalities in the NaaS architecture play an important role in realizing lifecycle management (refer to different OSS functionalities, see clause 7.8), network operational policy modelling (refer to NaaS service instantiation functionalities, see clause 7.2) as well as closed loop automation (refer to autonomic functionalities, see clause 7.5) and network analytics functionalities (see clause 7.4). The main goal of policy functionalities is to control in a simple manner the behaviour of the NaaS CSP system using configurable policies and rules.

Policy related functionalities include:

– Policy creation: used to design and validate policies rules, identify and resolve overlaps and conflicts between policies. A policy can be of a high-level nature to create a condition, requirement or constraint that must be provided, maintained, and enforced. A policy may also be defined at a lower level, such as a machine-readable rule or software condition. Policies can be created in conjunction with NaaS services (refer to development functionalities in clause 7.9 or independently from NaaS services (e.g., policies unrelated to NaaS services such as NaaS CSP internal security policies).
– Policy distribution: after being created, policies available in repositories are distributed to the right policy-enabled components in the NaaS architecture;
– Policy decision and enforcement: at runtime, policies that were previously distributed to policy-enabled NaaS components will be used by those components to control or influence their functionality and behaviour, including any decisions and actions that have to be taken.

7.7 NaaS resource functionalities

The NaaS resource functionalities include the functionalities necessary for the support of NaaS services. This include functionalities such as network services, network functions, as well as the resources used in underlying cloud computing infrastructures and network infrastructures (see clause 6.3 for further description of NaaS resources). For example, these NaaS resource functionalities can be used to provide virtualized networks exposed by the service layer to the NaaS CSC.

NaaS resource functionalities include network connectivity functionalities used in the different NaaS CSP domains. Network connectivity functionalities include interworking functionalities between the different networking layers used by the NaaS CSP, covering interworking of the relevant control functionalities, forwarding functionalities as well as management functionalities for each of these networking layers.

7.7.1 Functionalities for mapping between physical resources and virtualized networks

As part of NaaS resource functionalities, these functionalities are responsible to support the mapping between underlying physical resources and virtualized networks exposed to the NaaS CSC as part of NaaS services, via which, the near real-time utilization of underlying physical resources (physical nodes, physical links, etc) can be obtained.

7.8 Functionalities for an evolved real-time OSS

The OSS functionalities for NaaS consist of a set of capabilities for accessing the relevant OSS functions related to NaaS. They are related to functional components of the operations support systems defined in the multi-layer functions. These functions span the layered framework of the cloud computing reference architecture (CCRA).

As presented in clause 6.3, aspects to be controlled and managed in real-time by the OSS include the following:

- NaaS services;
- network services (see definition in clause 3.2.3);
- network functions (see definition in clause 3.2.2);
- virtual cloud compute and storage (CCS) resources;
- virtualized network connectivity;
- physical resources (compute, storage, networking).

Figure 7-1 describes the organization of the OSS functionalities to fulfil the management of the above aspects.

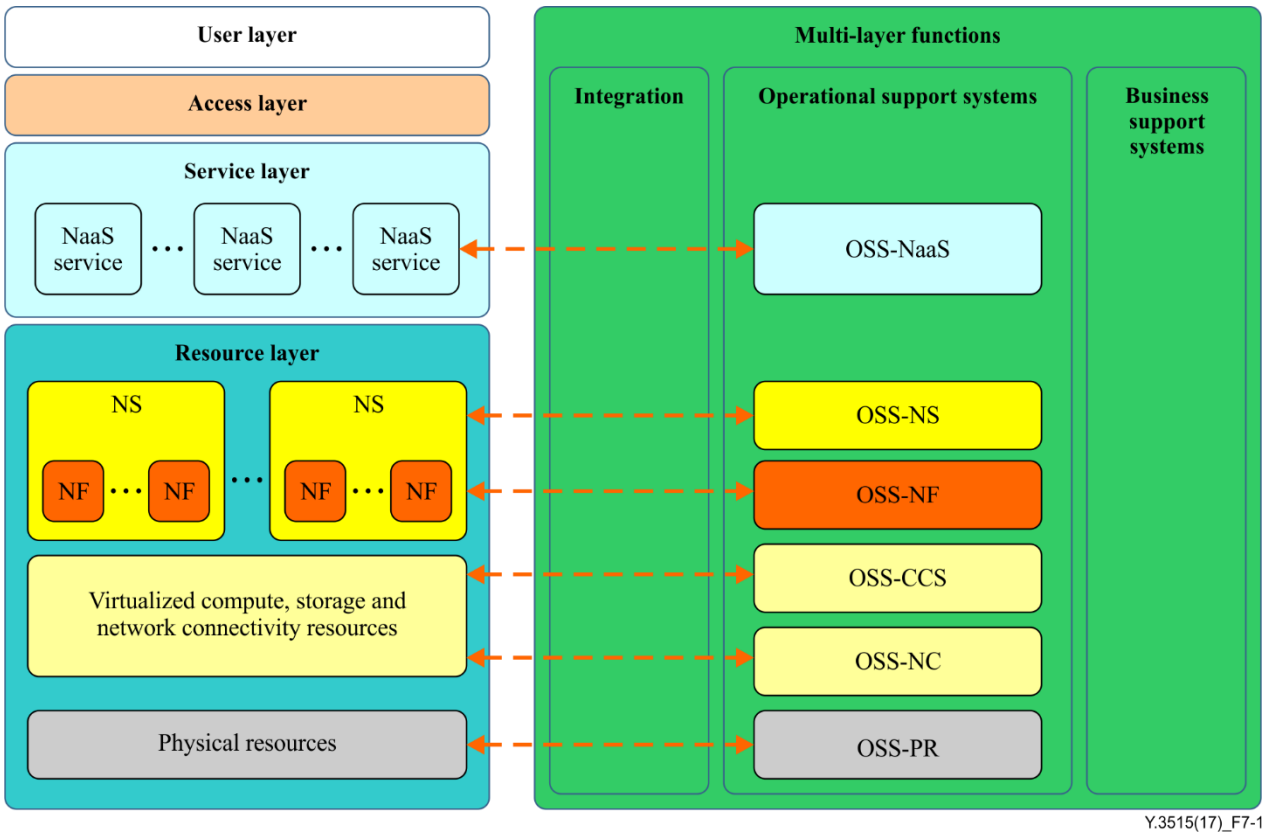

Figure 7-1 – OSS functionalities for NaaS

From the perspective of the management layers described in [ITU-T Y.3521], the OSS functionalities described in this clause cover the service management layer and resource management layer aspects (see Figure 8-3 of [ITU-T Y.3521]). The service management layer takes care of the management of NaaS services offered to NaaS CSCs, i.e., OSS-NaaS services functionalities described in clause 7.8.1. Regarding resource management layer aspects, they cover the management of the different NaaS resources (see clause 6.3) that are involved in the support of NaaS services, i.e., network services, network functions, cloud compute and storage resources, network connectivity resources and physical resources. These management functionalities are described in more detail in clause 7.8.2.

7.8.1 Service management layer functionalities

The OSS-NaaS services (OSS-NaaS) functionalities are responsible for the management of NaaS services (covering their deployment and operation), i.e., including service fulfilment, service assurance and service repositories [ITU-T Y.3521].

In accordance with clause 10.3 of [ITU-T Y.3521], these functionalities include:

– Catalogue management of NaaS services (e.g., connectivity as a service, network function as a service, network service as a service), with their relevant descriptions in terms of required network functions and their interconnectivity;

– NaaS service order management functionalities including NaaS service order orchestration and distribution decomposing the NaaS service order into resource order requests towards the relevant OSS functionalities described in clause 7.8.2;

– NaaS service assurance functionalities such as performance management, problem management and quality management of NaaS services instances;

– Inventory management of NaaS services instances;

– Usage management of NaaS services instances.

7.8.2 Resource management layer functionalities

This clause describes the resource management layer functionalities (see clause 10.4 of [ITU-T Y.3521]) for the support of NaaS services. These functionalities cover the management functionalities related to NaaS resources, i.e., network services, network functions, cloud compute and storage resources, network connectivity resources and physical resources.

7.8.2.1 OSS-network services

The OSS-network services (OSS-NS) functionalities are responsible for the management (including the deployment and operation) of network services.

In accordance with clause 10.4 of [ITU-T Y.3521], these functionalities include:

– Catalogue management of network services with their relevant descriptions in terms of required network functions and their interconnectivity;

– Network services' order management functionalities including the automated creation, modification and termination of network services instances (following NaaS service order requests received from OSS-NaaS);

– Network services' assurance functions such as performance monitoring, fault management of network services' instances; These functions include monitoring of network services' instances, calculating and performing restoration activities when monitoring detects one or more faulty network service instances as well as reporting status of network services' instances to clients of OSS-NS, e.g., OSS-NaaS functionalities;

– Inventory management of network services' instances (including availability and performance of network services' instances and the resources used to support the network services' instances);

– Usage collection and distribution of network services' instances.

The OSS-NS will handle the management of network service chains including the automated deployment, policy management and profile management of network service chains. By routing traffic flows according to a 'service graph', service chains address the requirement for optimization of the network through the provisioning of network services that are tailored to the customer context.

7.8.2.2 OSS-network functions

The OSS-network functions (OSS-NF) functionalities are responsible for the management of network functions such as instantiation, update, query, scaling, and termination of network functions. The services provided by the OSS-NF can be consumed by other functionalities such as the OSS-NS (see clause 7.8.2.1).

In accordance with clause 10.4 of [ITU-T Y.3521], the OSS-NF include functionalities such as:

– Catalogue management of network functions with their relevant descriptions and software;

– Network functions' order management functionalities including the automated creation, modification and termination of network functions' instances (including instances of network functions' components and their inter-connectivity);

– Network functions' assurance functions such as performance management and, fault management of network functions instances; These functions include monitoring of network functions' instances, calculating and performing restoration activities when monitoring detects one or more faulty network functions' instances as well as reporting status of network functions' instances to clients of OSS-NF, e.g., OSS-NS functionalities;

– Inventory management of network functions instances;

– Usage collection and distribution of network functions instances.

7.8.2.3 OSS-cloud compute and storage

The OSS-cloud compute and storage (OSS-CCS) functionalities are responsible for the management of virtual compute and storage resources. The functionalities provided by the OSS-CCS can be used by other OSS functionalities such as the OSS-NS (see clause 7.8.2.1) or the OSS-NF (see clause 7.8.2.2).

In accordance with clause 10.4 of [ITU-T Y.3521], the OSS-CCS includes functionalities such as:

– Catalogue management of cloud compute and storage resources;

– Resource order management functionalities such as the allocation, modification and termination of virtual compute and storage resources;

– Resource assurance functions such as performance management and fault management of allocated virtual compute and storage resources;

– Inventory management of allocated virtual compute and storage resources;

– Usage collection and distribution of virtual compute and storage resources.

7.8.2.4 OSS-network connectivity

The OSS-network connectivity (OSS-NC) functionalities are responsible for the management of network connectivity resources. The OSS-NC functionalities can be used by other OSS functionalities such as the OSS-NS (see clause 7.8.2.1) the OSS-NF (see clause 7.8.2.2) or the OSS-CCS (see clause 7.8.2.3).

In accordance with clause 10.4 of [ITU-T Y.3521], the OSS-NC includes functionalities such as:

– Resource order management functionalities such as allocation, modification and termination of virtualized network connectivity resources such as virtualized networks, links, sub-networks;

– Resource assurance functionalities such as performance management and fault management of allocated virtualized network connectivity resources;

– Inventory management of allocated virtualized network connectivity resources;

– Usage management of virtualized network connectivity resources.

The OSS-NC functionalities can be consumed by other NaaS functionalities such as OSS-NS (see clause 7.8.2.1) or OSS-NaaS functionalities (see clause 7.8.1). Control plane functions are topology and device detection, virtual partitioning, traffic isolation, reachability, traffic engineering and path computation, flow management, failure detection, path convergence, QoS control and management, as well as policy control and management. The configuration of virtualized networks requires interfaces to all relevant components, including network elements (physical switches and physical routers) in the infrastructure network domains, virtual switches (vSwitchs) as well as virtual routers (vRouters) in hypervisors, and embedded switches as well as routers in computing platforms.

The OSS-NC functionalities are basically responsible to manage network connectivity in a given infrastructure network domain (e.g., access, core). This functionality provides on-demand network service through northbound interfaces to the higher layer functions, abstracts the various southbound interfaces, and invokes the underlying infrastructure network interfaces. Several OSS-NC functionalities may exist in a given NaaS CSP each responsible for a particular network domain with overall end-to-end network connectivity through multiple network domains being handled by e.g., the functionalities for NaaS service orchestration (see clause 7.3) and/or OSS-NaaS functionalities (see clause 7.8.1).

7.8.2.5 OSS-physical resources

The OSS-physical resources (OSS-PR) are functionalities responsible for the management of physical resources such as compute, storage and networking physical resources. The functionalities provided

by the OSS-PR can be used by other OSS functionalities such as the OSS-CCS (see clause 7.8.2.3) or the OSS-NC (see clause 7.8.2.4).

Functionalities provided by the OSS-PR include:

– Catalogue management of physical resources (compute, storage, networking);

– Resource order management of physical resources;

– Resource assurance functionalities such as performance management and fault management of physical resources;

– Inventory management of available physical resources.

7.9 Functionalities for the development of NaaS products and NaaS services

Development functionalities for NaaS enable the design, building and testing of NaaS products, NaaS services (offered by NaaS products) as well as the design, building and testing of resources including NSs and NFs that are used for the support of the designed NaaS services. The design of NaaS products, NaaS services and NaaS resources is realized using model-driven engineering techniques providing the ability to create and manage NaaS products, NaaS services and NaaS resources in terms of models (refer to NaaS service models, NaaS resource models, NaaS service operational policy models as described in clause 7.2.2).

Once designed, built and tested, the resulting models for NaaS products, respectively for NaaS services, will be made available in the product catalogue, respectively service catalogue, by the NaaS CSP. Similarly network service models and network function models will also made available in NaaS resource catalogues for further instantiation as needed by the relevant OSS functionalities.

Development functionalities for NFs allow for the design and build of NFs according to the following cases:

− Features and capability required by the NFs are provided by elementary NFs;

− Composite NF provided by mixing NFs.

Development functionalities for NSs allow for the design and build of NSs taking into account the following cases:

− NS that includes NFs and/or composite NFs;

− Composite NS provided by mixing NSs.

According to [ITU-T Y.3502], the design includes the creation of configuration metadata relating to NaaS services, NFs and NSs being developed and also supports the creation of scripts and related artefacts that are then used by the provider's operational support systems to provision and configure the NaaS services, NFs or NSs.

In addition, the development functionalities include the building of generated and ready-to-deploy software packages for NaaS services, NFs and NSs which can be then passed on-boarded for deployment in a cloud infrastructure. The software package consists of both the implementation software and also the configuration metadata and scripts.

8 Functional components

This clause presents NaaS functional components definition and description based on NaaS functionalities identified in clause 7. NaaS functional components include instantiated functional components defined in [ITU-T Y.3502] and functional components defined in this Recommendation.

The functional components in a functional architecture represent sets of functions that are required to perform the cloud computing activities for various roles and sub-roles involved in cloud computing. The functional architecture of NaaS complies with CCRA [ITU-T Y.3502], where dependencies between functions are defined in the functional architecture.

8.1 Business support system functional components for NaaS products

The functional components for NaaS products (BSS-NaaS products) are shown in Figure 8-1.

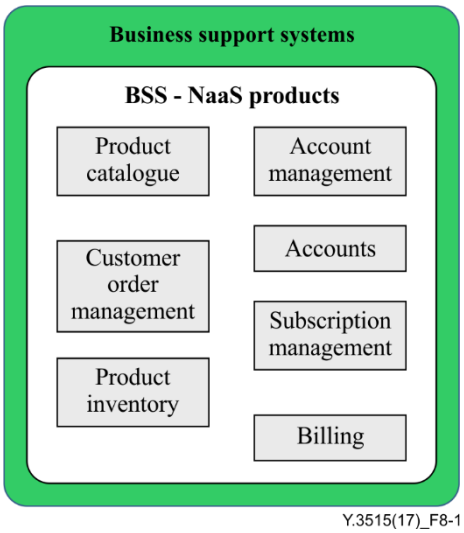

Figure 8-1 – Functional components for BSS-NaaS products

Functional components for BSS-NaaS products include the business support system (BSS) functional components described in clause 9.2.5.4 of [ITU-T Y.3502], i.e., product catalogue functional component, account management functional component, subscription functional component, billing functional component and accounts functional component.

These components are used to support NaaS business related functionalities of the NaaS CSP as described in clause 7.1. In particular:

– The product catalogue functional component provides capabilities for NaaS CSCs to browse the list of available NaaS service offerings which they can purchase, plus a set of capabilities for the management of the content of the catalogue which are available to the staff of the NaaS CSP. Product catalogue entries consist of technical information about each of the NaaS service offerings (capabilities provided by the NaaS service, interface definitions for the NaaS service), plus related business information such as pricing or rating;

– The subscription management functional component handles subscriptions from NaaS CSCs to particular NaaS services, aiming to record new or changed subscription information from the NaaS CSC and ensure the delivery of the subscribed NaaS service(s) to the NaaS CSC;

– Billing functional component. The billing functional component has capabilities for the metering and rating of the use of NaaS services by NaaS CSCs and the generation of invoices based on the charges for the use of NaaS services created by the metering and rating function, and the transmission of the invoices to the NaaS CSCs.

In addition to BSS components defined in [ITU-T Y.3502], the following functional components are added (see Figure 8-1):

– The customer order management functional component is responsible of the lifecycle management of a NaaS CSCs' requests for NaaS products (and NaaS services offered by these NaaS products). This includes customer order establishment (step guiding, data collection and validation), customer order orchestration and overall customer order lifecycle management (see [ITU-T Y.3521] and [ITU-T Y.3522]). Orders from NaaS CSCs may be for new NaaS products and NaaS services, or may be for updating or terminating of an existing NaaS service;

– The product inventory functional component holds information of NaaS products' instances ordered by NaaS CSCs. This information is updated during the lifecycle of the NaaS products instances, reflecting changes resulting from execution of management operations on these NaaS product instances.

8.2 Service layer functional components for NaaS

Figure 8-2 shows the service layer functional components used for NaaS services instantiation and also when a NaaS service is instantiated by the NaaS CSP.

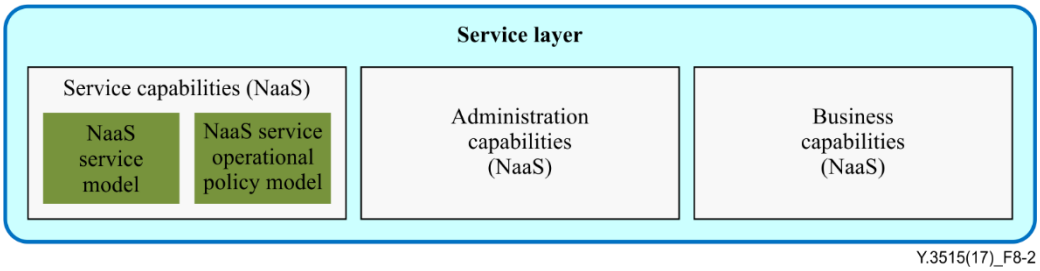

Figure 8-2 – Service layer functional components for NaaS

8.2.1 Business capabilities (NaaS)

The business capabilities (NaaS) functional component provides a set of capabilities for accessing the NaaS business related functionalities (see clause 7.1) related to the provision of NaaS services. The business functionalities are contained within the business support systems (BSS) functional components (see clause 8.1).

In particular, the business capabilities (NaaS) functional component provide access means for the NaaS CSC to select and purchase a NaaS product (and associated NaaS services with associated NaaS service models and NaaS service operational policy models) available in the product catalogue functional component (see clause 8.1). Once validated by the NaaS CSP, the requested NaaS service is instantiated by the NaaS CSP, i.e., a corresponding service capabilities (NaaS) functional component is made available in the service layer allowing for further NaaS service interactions between the NaaS CSC and the NaaS CSP. If not already instantiated an administration capabilities (NaaS) functional component is also made available in the service layer allowing for NaaS service-related management interactions between the NaaS CSC and the NaaS CSP.

Interactions through the business capabilities (NaaS) functional component also allow for the NaaS CSC to access the billing information related to the usage of instantiated NaaS services. Using BSS and OSS functional components, the NaaS CSP collects relevant usage measurements and usage events in order to generate and provide a bill to the NaaS CSC.

8.2.2 Administration capabilities (NaaS)

The administration capabilities (NaaS) functional component provides a set of capabilities for accessing the OSS-NaaS functionalities (see clause 7.8.1) related to the management of instantiated NaaS services. This includes functionalities contained within the OSS-NaaS functional components. For example, the administration capabilities (NaaS) functional component allows the NaaS CSC to view performance and fault information related to instantiated NaaS services. The NaaS CSP will collect information requested by the NaaS CSC and make it available through reporting to the NaaS CSC via the administration capabilities (NaaS) functional component.

8.2.3 Service capabilities (NaaS)

The service capabilities (NaaS) functional component consists of the necessary software required to implement the NaaS service offered to the NaaS CSC and implements the functionality defined by

the NaaS service interface, i.e., the interface offered to the NaaS CSC, independent of the service implementation.

As shown in Figure 8-2, the service capabilities (NaaS) functional component provides capabilities exposed to the NaaS CSC according to the NaaS service model and NaaS service operational policy model selected by the NaaS CSC through business level interactions with the NaaS CSP. Refer to clause 8.3.1 for the description of these two NaaS-related service models.

Using the NaaS service exposed API provided by the service capabilities (NaaS) functional component, the NaaS CSC can trigger NaaS service specific on-demand behaviours (made possible by the NaaS CSP according to the selected NaaS service model). These on-demand requests are validated by the NaaS CSP according to the NaaS service specific policies that govern such on-demand behaviour. The on-demand behaviours (and associated constraints) are defined in the NaaS service operational policy model selected by the NaaS CSC at NaaS instantiation time. For example, a NaaS service operational policy model may describe the range of bandwidth in which the NaaS CSC is permitted to send traffic to the NaaS CSP or the range of computing resources that a specific NF instance is allowed to be allocated in the NaaS CSP infrastructure.

8.3 OSS functional components

The OSSs functional components encompass the set of operational-related management capabilities of the NaaS functional architecture in order to manage and control aspects from NaaS services down to the NaaS CSP infrastructure resources including cloud compute and storage, network connectivity and physical resources.

The OSS components described in this clause are intended to support the functionalities for an evolved real-time OSS described in clause 7.8. The description of OSS components follows the structure of the OSS as shown in Figure 7-1.

Annex A describes reference points related to OSS functional components.

8.3.1 OSS-NaaS functional components

The OSS-NaaS functional components encompass the set of operational-related management functionalities that are required in order to manage and control NaaS services offered to customers (refer to clause 7.8.1).

NOTE – These functional components are not meant to be specific to NaaS and are applicable to other cloud service categories provided by NaaS CSPs.

Figure 8-3 shows the OSS-NaaS functional components.

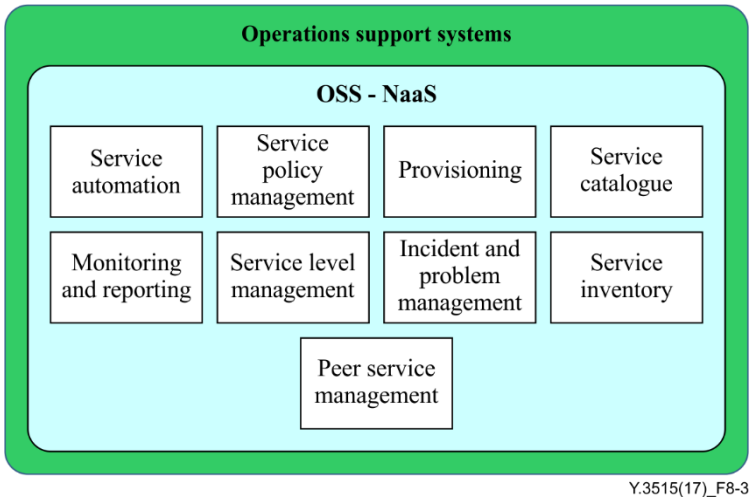

Figure 8-3 – OSS-NaaS functional components

The OSS-NaaS functional components include the following OSS functional components:

1) Service catalogue functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). This component includes a listing of all cloud services of NaaS CSPs including the relevant NaaS services;

   Modelling is needed for ensuring an efficient control and management of the NaaS services, policies, and resources by the NaaS CSP. The following models used for NaaS service instantiation (see clause 7.2.2) are needed in the service catalogue:

   – NaaS service models

     A NaaS service model provides the information model of a given NaaS service (e.g., VPN as a service (VPNaaS)) being offered by the NaaS CSP. NaaS service models are used for creating and deploying NaaS service solutions by the NaaS CSP. In a NaaS service model, a NaaS service specification is needed which includes the various interfaces related to the operations offered by a NaaS service. The NaaS service model is used when instantiating the corresponding NaaS service. For example, in case of a VPN service instance the different service attributes used to model a VPN service, such as tenant ID, VPN site IDs, VPN type and access bandwidth are part of the NaaS service model and will be subsequently used by the NaaS CSC when triggering VPN-related service requests.

   – NaaS service operational policy models

     A NaaS service operational policy model provides the information model related to network operational policies for a given NaaS service. The operational policies can be created at different levels of abstraction and can represent different types of policy rules for controlling NaaS resources managed by the NaaS CSP. The operational policies are used to control the configuration changes of NaaS resources (e.g., network elements).

     For a given NaaS service, the corresponding NaaS service model and NaaS service operational policy model always work together although loosely bound to each other. The creation, deletion, and any major state changes of a specific NaaS service instance (instantiated based on the corresponding NaaS service model selected by the NaaS CSC) usually trigger the execution of one specific NaaS service operational policy model, which is used together with the NaaS service model during the whole lifecycle of the NaaS service.

   – NaaS resource models

     A NaaS resource model reflects, in an abstract manner, NaaS CSP's resources including their associated topological view across different layers. A NaaS resource model reflects the attributes and operational parameters of given NaaS resources (e.g., NS, NF, virtualized resources, physical resources) described by the model. A NaaS resource model provides the information model of NaaS resources, e.g., the topology attributes of a physical and virtualized network such as bandwidth or latency of corresponding links, and the operational parameters needed to support the deployment of these NaaS resources.

2) Provisioning functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). This component provides the capabilities for provisioning NaaS services;

3) Monitoring and reporting functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). This component provides the capabilities for monitoring services including NaaS services provided by the NaaS CSP;

4) Service policy management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The service policy management functional component provides capabilities to define, store and retrieve policies that apply to cloud services including NaaS services;

5) Service automation functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The service automation functional component provides capabilities for service delivery including the management and execution of service templates and the orchestration of services, which include NaaS services. The service automation functional component realizes the NaaS service orchestration functionalities described in clause 7.3.

   In order to realize the functionalities for NaaS service orchestration, a unified abstract modelling of NaaS services provided to the NaaS CSC by the service layer is a must. With such modelling being defined, the NaaS service automation functional component when receiving a composite NaaS service request from the NaaS CSC will be able to decompose the request into several independent NaaS resources order requests and distribute each of these independent requests to the appropriate control or OSS functionalities of the NaaS CSP specific domains, automatically. The OSS-NaaS service automation functional component provides coordination, aggregation and composition of multiple services in order to deliver NaaS services.

   The OSS-NaaS service automation functional component provides service orchestration according to the NaaS service model and NaaS service operational policy model. The service automation functional component handles NaaS service requests received from the NaaS CSC and decomposes these NaaS service requests according to the NaaS service models and policy models, respectively.

6) Service level management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The service level management functional component provides capabilities for managing the service levels of a particular cloud service, aiming to ensure that the cloud service meets the requirements of the service level agreement (SLA) which applies to the service. This includes service level management of NaaS services;

7) Incident and problem management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The incident and problem management functional component provides capabilities for the capture of incident or problem reports and managing those reports through to resolution. Incidents and problems can be detected and reported by the NaaS CSP's systems, or they can be detected and reported by NaaS CSCs;

8) Peer service management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The peer service management functional component provides capabilities for connecting the NaaS CSP's operational support systems and business support systems to the administration capabilities and business capabilities of peer NaaS CSPs, in respect of peer cloud services that are used by the NaaS CSP;

9) Service inventory functional component. The service inventory functional component provides contains and maintains information about the instances of NaaS services deployed by the NaaS CSP.

NOTE – This component may also apply to cloud service categories different from NaaS.

8.3.2 OSS-NS functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-NS functional components encompass the set of operational-related management capabilities that are required in order to manage and control network services offered to customers as part of NaaS services. See clause 7.8.2.1 for a description of OSS-NS functionalities.

Figure 8-4 shows the OSS-NS functional components.

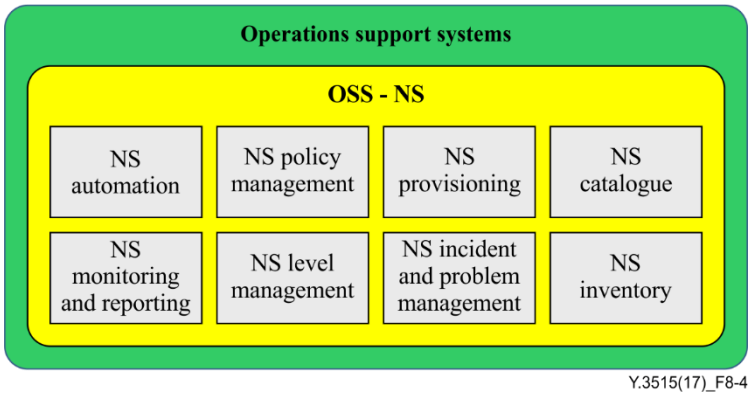

Figure 8-4 – OSS-NS functional components

The OSS-NS functional components include:

– NS catalogue;
– NS provisioning;
– NS monitoring and reporting;
– NS policy management;
– NS automation;
– NS level management;
– NS incident and problem management;
– NS inventory.

8.3.2.1 NS catalogue

The NS catalogue functional component provides a listing of all network services of the NaaS CSP. The NS catalogue contains and /or references all relevant technical information required to deploy, provision and run a network service.

8.3.2.2 NS provisioning

The NS provisioning functional component provides the capabilities for provisioning network services, both in terms of the provisioning of network service implementations and of network service access endpoints and the workflow required to ensure that elements are provisioned in the correct sequence.

8.3.2.3 NS monitoring and reporting

The NS monitoring and reporting functional component provides capabilities for:

– Monitoring the activities of other functional components throughout the NaaS CSP's system. This includes functional components involved in the support of network services, such as functional components in the OSS-NS itself like the NS automation functional component (e.g., the provisioning of a network service instance for a particular customer).
– Providing reports on the behaviour of the NaaS CSP's system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., service usage data).
– Storage and retrieval of network service monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the NS monitoring and reporting functional component. For multi-tenant cloud services, there is

also a need to design access to the records so that particular tenants can only gain access to information about their own tenancy and about no other tenancy.

8.3.2.4 NS policy management

The NS policy management functional component provides capabilities to define, store and retrieve policies that apply to network services. Policies can include business, technical, security, privacy and certification policies that apply to network services and their usage by NaaS CSCs.

Some policies can be general and apply to a network service irrespective of the customer concerned. Other policies can be specific to a particular customer.

8.3.2.5 NS automation

The NS automation functional component provides capabilities for network service delivery including the management and execution of network service templates and the orchestration of network services. The NS automation functional component holds the network service templates which define the cloud computing activities and workflows required to provision and deliver a specific entry in the NS catalogue.

Network service provisioning can be automated in order to support scalable resource operations, including configuration and charging.

Network service administration activities of NaaS CSC can be capable of being automated and need not require any intervention by NaaS CSP.

The NS automation functional component works with the NS provisioning functional component and the service integration functional component to achieve its goals.

8.3.2.6 NS level management

The NS level management functional component provides capabilities for managing the service levels of a particular network service, aiming to ensure that the network service meets the requirements of the SLA which applies to the network service.

The NS level management functional component manages the capacity and performance relating to a network service. This can involve the application of network service policies (e.g., a placement rule which aims to avoid single points of failure).

The NS level management functional component obtains monitoring information from the NS monitoring and reporting functional component in order to measure and record key performance indicators (KPIs) for the network service. Capacity of network service is allocated or de-allocated based on the basis of these KPIs.

The NS level management functional component also keeps track of the overall state of allocated and available resources. The comparison of allocated capacity against network service performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning.

8.3.2.7 NS incident and problem management

The NS incident and problem management functional component provides capabilities for the capture of network service incident or problem reports and managing those reports through to resolution.

Network service incidents and problems can be detected and reported by the NaaS CSP's systems, or they can be detected and reported by NaaS CSCs.

8.3.2.8 NS inventory

The NS inventory functional component holds information of all network service instances. This information is updated during the lifecycle of the network service instances, reflecting changes resulting from execution of management operations on these network service instances.

8.3.3 OSS-NF functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-NF functional components encompass the set of operational related management capabilities that are required in order to manage and control the network functions offered to customers as part of network services. Refer to clause 7.8.2.2 for a description of OSS-NF functionalities.

Figure 8-5 shows the OSS-NF functional components.

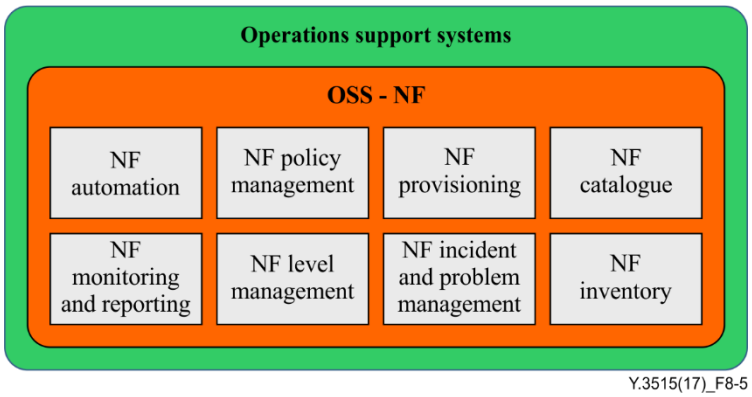

Figure 8-5 – OSS-NF functional components

The OSS-NF functional components include:

– NF catalogue;
– NF provisioning;
– NF monitoring and reporting;
– NF policy management;
– NF automation;
– NF level management;
– NF incident and problem management;
– NF inventory.

8.3.3.1 NF catalogue

The NF catalogue functional component provides a listing of all network functions of the NaaS CSP. The NF catalogue functional component contains and/or references all relevant technical information required to deploy, provision and run a network function.

8.3.3.2 NF provisioning

The NF provisioning functional component provides the capabilities for provisioning network functions, both in terms of the provisioning of network functions implementations and of network functions access endpoints and the workflow required to ensure that necessary NF elements are provisioned in the correct sequence.

8.3.3.3 NF monitoring and reporting

The NF monitoring and reporting functional component provides capabilities for:

– Monitoring the activities of other functional components throughout the NaaS CSP's system. This also includes functional components involved in the support of network functions, such

as other OSS-NF functional components like the NF automation functional component (e.g., the provisioning of a network functions instance for a particular customer);

– Providing reports on the behaviour of the NaaS CSP's system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., network function usage data);

– Storage and retrieval of network functions monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the NF monitoring and reporting functional component.

8.3.3.4 NF policy management

The NF policy management functional component provides capabilities to define, store and retrieve policies that apply to network functions. Policies can include business, technical, security, privacy and certification policies that apply to network functions and their usage by NaaS CSCs.

Some policies can be general and apply to a network function irrespective of the customer concerned. Other policies can be specific to a particular customer.

8.3.3.5 NF automation

The NF automation functional component provides capabilities for network functions' delivery including the management and execution of network functions' templates and the orchestration of network functions. The NF automation functional component holds the network functions templates which define the cloud computing activities and workflows required to provision and deliver a specific entry in the NF catalogue.

Network function provisioning can be automated in order to support scalable resource operations, including configuration and charging.

Network function administration activities of the NaaS CSC can be capable of being automated and need not require any intervention by the NaaS CSP.

The NF automation functional component works with the NF provisioning functional component to achieve its goals.

8.3.3.6 NF level management

The NF level management functional component provides capabilities for managing the service levels of a particular network function, aiming to ensure that the network function meets the requirements of the SLA which applies to the related network service.

The NF level management functional component manages the capacity and performance relating to a network function. This can involve the application of network function policies (e.g., a placement rule which aims to avoid single points of failure).

The NF level management functional component obtains monitoring information from the NF monitoring and reporting functional component in order to measure and record KPIs for the network function. Capacity of a network function can be allocated or de-allocated based on the basis of these KPIs.

The NF level management functional component also keeps track of the overall state of allocated and available resources. The comparison of allocated capacity against network function performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning.

8.3.3.7 NF incident and problem management

The NF incident and problem management functional component provides capabilities for the capture of network function incident or problem reports and managing those reports through to resolution.

Network function incidents and problems can be detected and reported by the NaaS CSP's systems, or they can be detected and reported by NaaS CSCs.

8.3.3.8 NF inventory

The NF inventory functional component holds information of all network function instances. This information is updated during the lifecycle of the network function instances, reflecting changes resulting from execution of management operations on these network function instances.

8.3.4 OSS-CCS functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-CCS functional components encompass the set of operational-related management capabilities that are required in order to manage and control the virtual resources for CCS necessary for the support of network functions instances. These virtual resources are provided in NaaS CSP's infrastructure points of presence (PoPs) (e.g., data centres) in which network functions instances are deployed. Typical virtual resources for compute include virtual machines (VMs) or containers. See clause 7.8.3 for a description of OSS-CCS functionalities.

Figure 8-6 shows the OSS-CCS functional components.

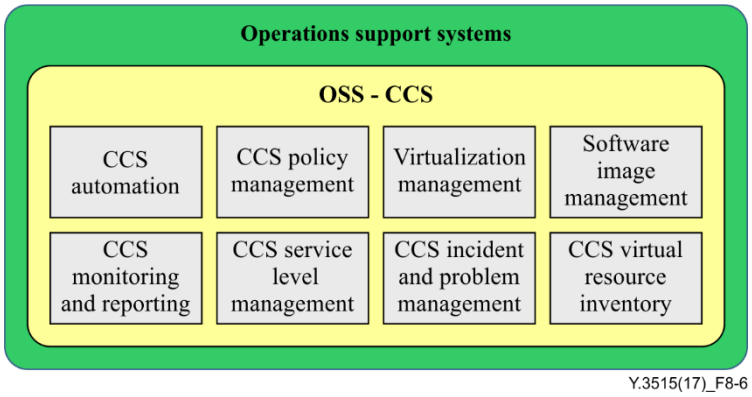

Figure 8-6 – OSS-CCS functional components

8.3.4.1 CCS automation

The CCS automation functional component provides capabilities for delivering and orchestrating virtual resources for cloud compute and storage. This includes orchestration of allocation, release, upgrade of relevant infrastructure resources including optimizing of such resources usage, as well as managing the association of the virtual resources to the physical resources. Provisioning of these virtual resources can be automated in order to support scalable resource operations, including configuration.

8.3.4.2 CCS monitoring and reporting

The CCS monitoring and reporting functional component provides capabilities for:

– Reporting on the behaviour of the NaaS CSP's system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., service usage data);

– Storing and retrieving monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the CCS monitoring and reporting functional component. For multi-tenant cloud services, there is also a need to design access to the records so that particular tenants can only gain access to information about their own tenancy and about no other tenancy.

8.3.4.3 CCS policy management

The CCS policy management functional component provides capabilities for defining, storing and retrieving policies (e.g., quotas) that apply to virtual resources for cloud compute and storage. Policies can include technical and security policies that apply to these virtual resources and their usage by their users.

8.3.4.4 CCS service level management

The CCS service level management functional component provides capabilities for managing the service levels of virtual resources for cloud compute and storage, aiming to ensure that each virtual resource meets the negotiated service level requirements.

The CCS service level management functional component manages the capacity and performance relating to virtual resources for cloud compute and storage. This can involve the application of policies (e.g., a placement deployment rule which aims to avoid single points of failure).

The CCS service level management functional component obtains monitoring information from the CCS monitoring and reporting functional component in order to measure and record KPIs for the virtual resources. Capacity of virtual resources is allocated or de-allocated based on the basis of these KPIs.

The CCS service level management functional component also keeps track of the overall state of allocated and available resources for cloud compute and storage. The comparison of allocated capacity against performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning. This includes the management of the virtual resources capacity (e.g., density of virtual resources to physical resources), and the forwarding of information related to infrastructure resources capacity and usage reporting.

8.3.4.5 CCS incident and problem management

The CCS incident and problem management functional component provides capabilities for capturing incident or problem reports related to virtual resources for CCS and managing those reports through to resolution.

8.3.4.6 Virtualization management

The virtualization management functional component provides the capabilities for managing the virtualization of the resources for CCS (e.g., realized by means of hypervisors).

8.3.4.7 CCS virtual resource inventory

The CCS virtual resource inventory functional component keeps track of the allocation of virtual resources for CCS to physical resources (e.g., server pool).

8.3.4.8 Software image management

The software image management functional component manages software images (e.g., network functions) as requested by other OSS functional components (e.g., OSS for network functions). These requests include operations on images such as add, delete, update, query and perform rollback. Once validated by the software image management functional component, software images are stored in a software image repository.

8.3.5 OSS-NC functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-NC functional components encompass the set of operational related management capabilities that are required in order to manage and control the network connectivity in NaaS CSP domains, also called NaaS CSP connectivity domains. See clause 7.8.4 for a description of the OSS-NC functionalities.

The OSS-NC functional components may be able to manage network connectivity across one or multiple NaaS CSP's domains (e.g., access, backhaul or core NaaS CSP domains) and can also manage network connectivity at one or multiple technology layers (e.g., overlay, IP, multiprotocol label switching (MPLS), optical transport network (OTN)).

Figure 8-7 shows the OSS-NC functional components.

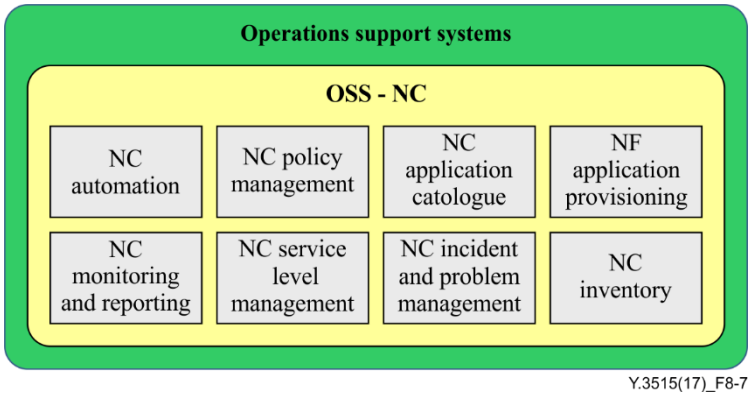

Figure 8-7 – OSS-NC functional components

8.3.5.1 NC application catalogue

The NC catalogue functional component provides a listing of all NC applications supported by the OSS-NC. A NC catalogue can contain and/or reference all relevant technical information required to deploy, provision and run a NC application.

8.3.5.2 NC application provisioning

The NC provisioning functional component provides the capabilities for provisioning NC applications, both in terms of the provisioning of NC application implementations and of access endpoints and the workflow required to ensure that elements are provisioned in the correct sequence.

8.3.5.3 NC automation

The NC automation functional component provides capabilities for the delivery of network connectivity applications and the orchestration of network connectivity across one or multiple NaaS CSP connectivity domains. This includes orchestrating the allocation, release, upgrade of network connectivity through the relevant NaaS CSP connectivity domains.

8.3.5.4 NC monitoring and reporting

The NC monitoring and reporting functional component provides capabilities for:

– Providing reports on the behaviour of the NaaS CSP's NC applications, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault on a given established NC, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., NC usage data).

– Storage and retrieval of NC related monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the NC monitoring and reporting functional component.

8.3.5.5 NC policy management

The NC management functional component provides capabilities to define, store and retrieve policies that apply to NC applications. Policies can include technical and security policies that apply to NC applications and their usage by users of these NC applications.

8.3.5.6 NC service level management

The NC service level management functional component provides capabilities for managing the service levels of NC, aiming to ensure that the negotiated NC service level requirements are met.

The NC service level management functional component manages the capacity and performance relating to NC. This can involve the application of policies (e.g., a placement rule which aims to avoid single points of failure).

The NC service level management functional component obtains monitoring information from the NC monitoring and reporting functional component in order to measure and record KPIs for the NC. NC capacity can be allocated or de-allocated based on the basis of these KPIs.

The NC service level management functional component also keeps track of the overall state of an allocated NC capacity and available network capacity. The comparison of allocated capacity against performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning. This includes the management of connectivity capacity and the forwarding of information related to NC capacity and usage reporting.

8.3.5.7 NC incident and problem management

The NC incident and problem management functional component provides capabilities for the capture of incident or problem reports related to NC and managing those reports through to resolution.

8.3.5.8 NC inventory

The NC inventory functional component keeps track of the allocated NC including the associated characteristics.

8.3.6 OSS functional components for physical resources

NOTE – This clause is out of the scope of this Recommendation.

8.4 Functional components for NaaS development support

Refer to clause 7.9 for a description of development functionalities for NaaS products and services.

The functional components for NaaS development support include the development support functional components described in clause 9.2.5.5 of [ITU-T Y.3502]:

– Developer environment functional component. Provides the capabilities to support the development of the NaaS service software implementation including the development of the following software components:
  - Network function software. A network function software can be developed in such a way that features and capability of the network function is provided by elementary network functions; It can also be provided by composition of other developed network functions;
  - Network services;
  - Network connectivity applications software (such as for SDN applications).
– The development environment functional component includes capabilities for the creation of the configuration metadata for the above software components as well as scripts and related

artefacts that are then used by the provider's operational support systems to provision and configure the network function, network service or network connectivity application.

– Build management functional component. Supports the building of a ready-to-deploy NaaS software package for network functions, network services and network connectivity applications which can be passed to the NaaS CSP for deployment into the NaaS cloud service environment. The software package consists of both the service implementation software and also the configuration metadata and scripts.

– Test management functional component. Supports the execution of test cases against any build of the NaaS service implementation. The test management functional component produces reports of the executed tests and these can be communicated to the NaaS CSP along with a build of the NaaS service implementation.

The functional components for NaaS development support (Dev-NaaS products and services) are shown in Figure 8-8.

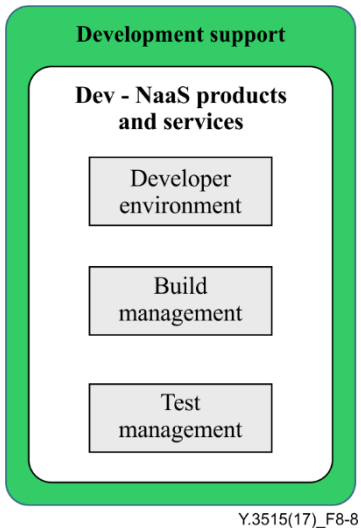

Figure 8-8 – Functional components for Dev-NaaS products and services

9 Security considerations

Security aspects for consideration within the cloud computing environment, including NaaS, are addressed by security challenges for NaaS CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

The functional components for security systems defined in clause 9.2.5.2 of [ITU-T Y.3502] are applicable in the context of the NaaS functional architecture. These components are responsible for applying security related controls to mitigate the security threats in cloud computing environments and encompass all the security facilities required to support cloud services of the NaaS cloud service category.

Annex A

OSS reference points

(This annex forms an integral part of this Recommendation.)

This annex describes reference points related to OSS whose functional components are described in clause 8.3 of the NaaS functional architecture.

Figure A.1 identifies the reference points internal to the OSS (reference points labelled as "oss") as well as reference points between the OSS and external entities.

For a NaaS service that involves either a "legacy" (i.e., non-virtualized) network functions (i.e., PNFs), the "OSS for NaaS services" will interact with the OSS (called "legacy OSS" in Figure A.1) responsible for the management of these "legacy" network functions. The "OSS legacy" system typically includes management systems such as network management systems (NMSs) or element management systems (EMSs).

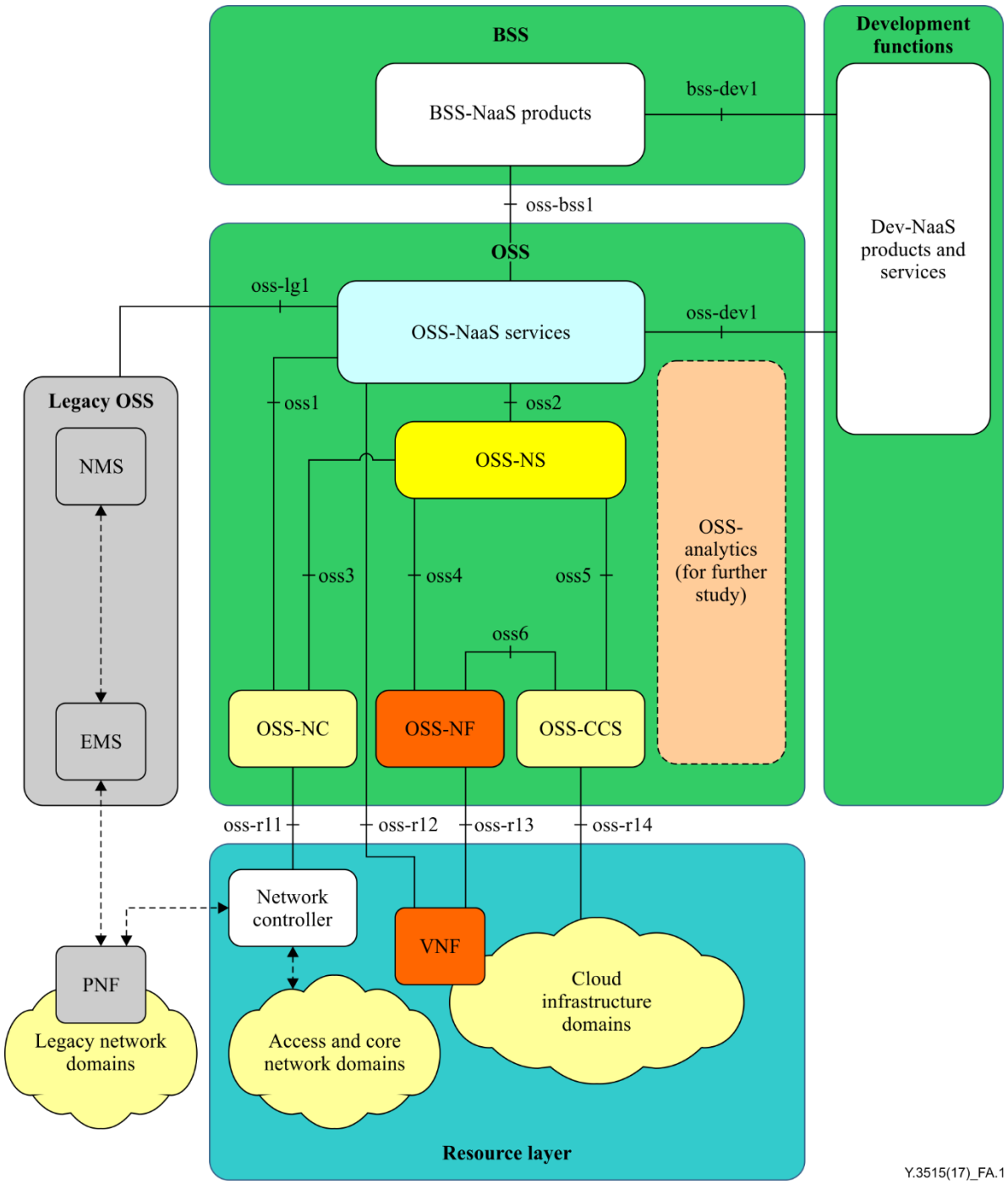

Figure A.1 – OSS-related reference points

The internal reference points illustrated in Figure A.1 are listed as follows:

– **oss1**: This reference point covers interactions between the OSS-NaaS and OSS-NC, e.g., for wide area network (WAN) connectivity management.

– **oss2**: This reference point covers interactions between the OSS-NaaS and the OSS-NS. This includes interactions related to network service lifecycle management, network service fault and performance management, network service usage management and network service inventory management.

– **oss3**: This reference point covers interactions between the OSS-NS and OSS-NC, e.g., for WAN connectivity management, as required by a given network service orchestrated by the OSS-NS.

– **oss4**: This reference point covers interactions between the OSS-NS and OSS-NF. This includes interactions related to network functions lifecycle management, network functions fault and performance management, network functions usage management and network functions inventory management.

– **oss5**: This reference point covers interactions between the OSS-NS and OSS-CCS. This includes interactions related to virtual resources life cycle management, virtual resources fault and performance management, virtual resources usage management and virtual resources inventory management.

– **oss6**: This reference point covers interactions between the OSS-NF and OSS-CCS. This includes interactions related to virtual resources life cycle management, virtual resources fault and performance management, virtual resources usage management and virtual resources inventory management.

The external reference points illustrated in Figure A.1 are listed as follows:

– **oss-bss1**: This reference point covers interactions between BSS functional components for NaaS products (BSS-NaaS products) and OSS components for NaaS services (OSS-NaaS). This includes for example NaaS service order interactions between the BSS account management functional component and the OSS-NaaS following a NaaS CSC order for a NaaS product.

– **oss-rl1**: This reference point covers interactions between the OSS-NC and a network controller (e.g., a SDN controller). This includes interactions related to virtualized network connectivity life cycle management, fault and performance management, usage management and inventory management. In this case the OSS-NC can be viewed as a set of SDN applications as per [ITU-T Y.3300], [ITU-T Y.3302] and the interactions being carried over the SDN Application Control Interface (ACI) reference point.

– **oss-rl2**: This reference point covers interactions between the OSS-NaaS and a VNF. This includes interactions related to the network functions' configuration management and network functions' fault and performance management from a NaaS service perspective.

– **oss-rl3**: This reference point covers interactions between the OSS-NF and a VNF. This includes interactions related to the network functions' configuration management and network functions' fault and performance management.

– **oss-rl4**: This reference point covers interactions between the OSS-CCS with the NaaS cloud infrastructure domain. This includes interactions related to the specific assignment of virtual resources in response to resource allocation requests and the exchange of virtual resources state information.

– **oss-lg1**: This reference point covers interactions between the OSS-NaaS with a legacy OSS system that manages legacy networks including PNFs.

– **oss-dev1**: This reference point covers interactions between the OSS-NaaS with Development Functions for NaaS products and Services. This include interactions related the distribution of developed NaaS services in order to make them available in the service catalogue functional component within the OSS-NaaS.

– **bss-dev1**: This reference point covers interactions between the BSS-NaaS products with development functions for NaaS products and services. This includes interactions related to the distribution of developed NaaS products in order to make them available in the product catalogue functional component within the BSS-NaaS products.

NOTE 1 – In some cases, interaction of the OSS-NaaS with a PNF may be realized through the OSS-NC using either oss1 reference point or oss2 plus oss3 reference points. In such case the OSS-NC will typically interact with a Network Controller (e.g., a SDN controller or the NMS/EMS that controls and manages the PNF).

NOTE 2 – The OSS-Analytics box shown in Figure A.1 is for further study. Main objective of the OSS-Analytics is to support network analytics functionalities as described in clause 7.3. Interactions of the OSS-analytics with other OSS components needs further study.

Annex B

Functional components on mapping between physical and virtualized networks

(This annex forms an integral part of this Recommendation.)

This annex describes the functional components on mapping between physical and virtualized networks.

NOTE – A virtualized network can be seen as a specific realization of a NS whose resources are provided on top of physical resources that constitute a physical network.

In order to realize the functionality for mapping between physical and virtualized networks (refer to clauses 7.7.1 and I.4), specialized mapping functional components are necessary.

The resource abstraction and control functional component [ITU-T Y.3502] is used by NaaS CSPs to:

– Provide access to the physical computing resources through software abstraction;

– Ensure efficient, secure, and reliable usage of the underlying infrastructure;

– Enable a NaaS CSP to offer qualities such as rapid elasticity, resource pooling and on-demand self-service.

The resource abstraction and control functional component can include software elements such as hypervisors, virtual machines, virtual data storage, and time-sharing.

The physical resources functional component [ITU-T Y.3502] includes hardware resources, such as computer, networks (routers, firewall, switches, network links and network connectors), storage components and other physical computing infrastructure elements.

The resource abstraction and control functional component and the physical resources functional component can be instantiated to realise the functionality described in clause 7.7.1, as shown in Figure B.1.

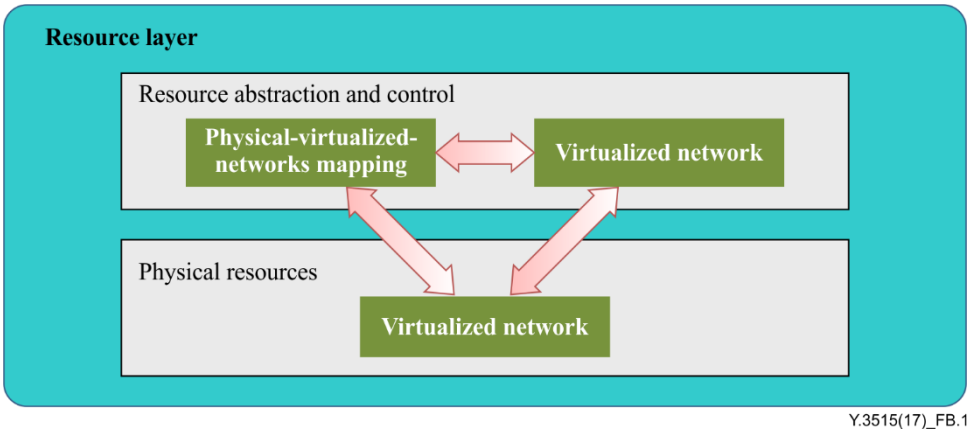

Figure B.1 – Functional components on mapping between physical and virtualized networks

B.1 Physical network

Physical network functional component provides physical agents of physical network elements, such as physical nodes, ports, switches and links.

NOTE – Physical agents are the representations of actual physical network nodes, ports, switches, links, etc.

B.2 Virtualized network

Virtualized network functional component provides virtualized network elements, such as virtual nodes, ports, switches and links. Each tenant is represented by one virtualized network and different tenants can only discover their own virtualized network. All virtualized network elements are mapped to at least one physical element and can be enabled, disabled, modified or reorganised at runtime.

NOTE – A virtualized network element is a broader concept than VNF. It can be a VNF but also can correspond to a network port or network link.

B.3 Physical-virtualized-networks mapping

Physical-virtualized-networks mapping functional component enforces the mapping between virtualized (overlay) networks and physical (underlay) networks. The mapping contents are stored in a database, which can be accessed by both physical and virtualized networks.

Appendix I

Mapping among NaaS functional requirements and functionalities

(This appendix does not form an integral part of this Recommendation.)

This appendix aims to describe the mapping among NaaS functional requirements (specified in [ITU-T Y.3512]) and functionalities. The mapping between functionalities and functional requirements of three kinds of NaaS services had been taken into account.

I.1 Mapping and derivation of functionality for NaaS service instantiation

Taking the functional requirements "elastic network reconfiguration", "dynamic and flexible network services composition and steering", and "unified network control mechanism" as the analysis example, NaaS architecture needs to satisfy dynamic configuration change requirements based on real-time network status and policy, and network resource abstraction across different layers including application layer (L7), IP layer (L3), and lower layers (L0-L2).

The traditional development and operation procedures are always separated and hardly address real-time configuration changes due to slow deployment of network functions/devices and unsatisfactory quality of experience (QoE). Therefore, it is also needed for the NaaS CSP to offer programmable ways to configure networks (so called development and operations (DevOps)), which is also mentioned in the functional requirement "programmable NaaS platform".

NOTE – DevOps is a software development method that stresses communication, collaboration (information sharing and web service usage), integration, automation and measurement of cooperation between software developers and other IT professionals. DevOps acknowledges the interdependence of software development and IT operations.

To implement network resource abstraction across different layers, it is needed to model different network resources in a unified manner, including physical and/or virtualized network nodes and links. Apart from this, network services and the corresponding deployment policies also need respective unified models. These three kinds of models should be able to share information with one another in order that the real-time configuration change demands can be transferred from the NaaS CSC to the NaaS CSP's network elements.

Moreover, regarding the requirement "optimized and fine-grained traffic engineering", its detailed description includes "collects near real-time utilization metrics and topology data from its own network equipment" and "controls the network resource allocation by reconfiguring network profiles as well as properties in response to dynamically changing traffic demands", which also require dynamic configuration changes response. Therefore, this can be grouped to derive the common functionality with the above mentioned functional requirements.

I.2 Mapping and derivation of functionality for service orchestration

Regarding "coexistence with legacy network services and functions", its detailed description includes "avoid or mitigate possible performance and flexibility impacts when introducing new network connectivity services" and "support coexistence of new network connectivity services with legacy systems", which requires NaaS architecture to provide the evolution and incremental deployment mechanism for the new paradigm of networking.

Taking the introduction of SDN as an example, during its transition, SDN-based networks should/could coexist with legacy IP networks, any SDN-based deployment should/could be able to exchange reachability information, forwarding traffic, and express routing policies with exiting IP networks.

Moreover, "interworking among different VPN solutions" is an example of networking connectivity interworking implementation requirement and can also be grouped in this functionality.

Regarding the "unified network control mechanism", "centralized control view and abstraction view of resources", "unified SLA for multiple optimized networks", and "leveraging transport networks dynamically" functional requirements, their detailed description includes "provide a unified control mechanism for the end-to-end NaaS connectivity given to a CSC", "support logically centralized management and control view of networking resources", "provide network connectivity services using unified SLA for CSC's management of multiple optimized networks in order to simplify and unify the control and management of networks", and "leverage transport networks dynamically form multiple choices of physical and virtualized networks for the purpose of providing network connectivity services", which requires NaaS architecture to provide the dedicated mechanism to present a panorama portal to the NaaS CSC, allowing a unified abstract service modelling repository to receive, parse, and transfer NaaS CSC's requirement to the control function of specific domain, which is implemented separately with other parallel control function of dedicated domains. Using this manner, it is feasible to realize the composite NaaS service, which can be decomposed automatically and dispatched to the appropriated control function.

Take the use case for dynamic transport network, specified in [ITU-T Y.3512], as an example, it is a typical composite NaaS service, which requires the service management related function to separate the requirement composition into independent service model and distribute them to the independent network control functions.

I.3 Mapping and derivation of functionalities for network analytics, policy, and autonomy

Regarding the requirement "optimized and fine-grained traffic engineering" in [ITU-T Y.3512], whose detailed description includes "collect near real-time utilization metrics and topology data from its own network equipment", "provide the CSC with fine-grained view on usage of network resources", "control the network resource allocation by reconfiguring network profiles as well as properties (e.g., topology, bandwidth) in response to dynamically changing traffic demands", which requires NaaS architecture provide analytical mechanism to collect near real-time data from NaaS CSP's network environment, maintain monitoring NaaS service during its lifecycle, trigger the corresponding pre-defined action based on the matched specific condition.

In order to perform the closed analysis and control loop in NaaS service lifecycle management mentioned above, it is also needed for NaaS architecture to provide configurable policy mechanism, covering policy creation, policy distribution, and policy decision and enforcement.

Based on the analytical and policy mechanisms, autonomy at resource level of NaaS architecture can be achieved accordingly.

I.4 Mapping and derivation of functionality for mapping between physical and virtualized networks

On the one hand, the "overlay network mechanism", "logically isolated network partition", and "overlapped private IP addresses" functional requirements, whose detailed description includes "support virtualized overlay networks on top of the physical underlay network", "implement LINP", and "allows different CSCs to use their own private IP addresses even when the subnet addresses are overlapped" can be satisfied by virtualized overlay network mechanism, e.g., virtual extensible local area network (VXLAN), VPN. On the other hand, the "optimized and fine-grained traffic engineering" functional requirement asks for "NaaS CSP provides the CSC with fine-grained view on usage of network resource". If the network resource mentioned here consists of not only physical network, but also virtualized network, which are always implemented by tunnelling overlay mechanism, the NaaS CSC cannot obtain the near real-time utilization on physical networks. Because the virtualized network is overlaid over the physical networks, and shields the underlying information to the NaaS CSC, this results in possible underutilization/overutilization of resource.

Hence, NaaS architecture needs to provide the mapping between physical underlay network and virtual overlay network in order to present fine-grained view on usage of physical network resource.

I.5 Mapping and derivation of functionalities for an evolved real-time OSS

The "operation and management", "performance" and "service chain" requirements for NaaS applications described in clause 7 of [ITU-T Y.3512] imply that functionalities for performance management as well as for flexible provisioning and configuration of NaaS applications and their chaining have to be supported by the OSS.

Concerning NaaS platform related requirements described in clause 8 of [ITU-T Y.3512], "programmable NaaS platform", "isolation of service chain for tenants" and "flexible scaling of NaaS platform" requires that the OSS functionalities be flexible and efficient enough to allow for the instantiation of network services, network functions and corresponding cloud computing resources in an automated manner.

Regarding NaaS connectivity related requirements identified in clause 9 of [ITU-T Y.3512], "unified network control mechanism, "elastic network reconfiguration", "leveraging transport networks dynamically" and "seamless and end-to-end solution of bandwidth", this requires that the NaaS architecture provides OSS functionalities that support the real-time control, management and orchestration of end-to-end connectivity across the NaaS cloud computing infrastructure as well as access and core network domains.

I.6 Mapping and derivation of functionalities for NaaS products and NaaS services development

"Integration of software applications" requirements as described in clause 8.5 of [ITU-T Y.3512] implies that integration of these applications on the NaaS platform allows the building and design of combined solutions which will be tested prior to their deployment by the NaaS CSP. Functionalities for the development of NaaS services are therefore required to be supported in the NaaS architecture.

I.7 Mapping and derivation of functionalities related to NaaS business

[ITU-T Y.3512] does not explicitly address requirements related to NaaS business capabilities since the requirements in [ITU-T Y.3512] are related to the three types of NaaS services, i.e., NaaS application, NaaS platform and NaaS connectivity. However, these business capabilities have to be addressed in the NaaS architecture to support the management of NaaS service offerings by the NaaS CSP including NaaS CSC requests for selection and purchase of NaaS products and services available in the NaaS CSP product catalogue.

Appendix II

Modelling usage example of NaaS service, NaaS service operational policy and NaaS resource model

(This appendix does not form an integral part of this Recommendation.)

II.1 Introduction

In practice, a NaaS CSP can virtualize cloud resources into multiple isolated virtual private clouds (VPCs) and provide them to NaaS CSCs. A NaaS CSC can establish and manage the network easily in a typical VPC, for example: deploying or removing virtualized network devices (e.g., vRouter and vSwitch), adjusting the topology of VPC networks, specifying packet forwarding policies, and deploying or removing virtualized network services (e.g., load balancer, firewalls, databases, DNS). The NaaS functionalities that the NaaS CSC can obtain are virtualized and actually performed by VMs located on compute servers, which may be located in different geographically distributed data centres, connected through physical or overlay networks.

The manipulation of the virtualized VPC network may also affect the configuration of physical networks. For example, when two new VMs associated to a given VPC are deployed in two different data centres, the VPC control mechanism needs to generate a VPN between these two data centres for the internal VPC communications. Therefore, the control mechanism for a VPC should be able to adjust the underlying network at runtime when the NaaS CSC requests changes to the VPC network or service deployment.

When the NaaS CSC moves from one location to another, which is near to another NaaS CSP's data centre, and in the case the network load between these two data centres is low, NaaS CSC's VM(s) should be migrated to the new data centre in order to allow for a better user experience.

As illustrated by Figure II.1, a VPC corresponds to a combination of cloud computing resources with a VPN infrastructure to give NaaS CSCs the abstraction of a private set of cloud resources that are transparently and securely connected to their own infrastructure. VPCs are created by taking dynamically configurable pools of cloud resources and connecting them to enterprise sites with VPNs.

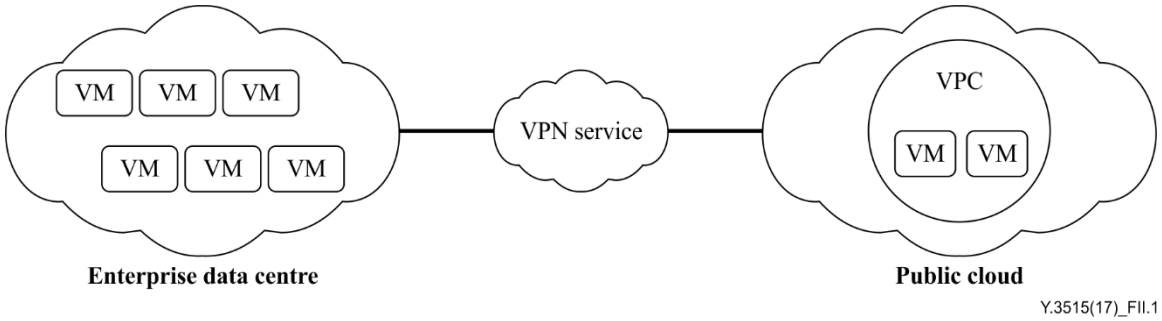

Figure II.1 – Example of VPC and VPN relationship

II.2 Modelling usage

Based on the description given in clause II.1, the VPC service can be modelled as a VPC NaaS service model based on its concrete service attributes, including service ID, tenant ID, access bandwidth, access virtualized network device, attached virtual service, etc.

The initial provisioning configuration can be generated based on the VPC NaaS service model, together with the corresponding NaaS service operational policy model, which includes the following aspects:

– The required services on data centres according to NaaS CSC's profile are allocated;
– Services located in multiple distributed data centres are interconnected via e.g., VPNs;
– The VPN associated to the services provided for NaaS CSC matches NaaS CSC's profile in terms of latency, speed, and bandwidth.

The runtime VM migration configuration can be generated based on the VPC NaaS service model, together with the corresponding NaaS service operational policy model, which includes the aspects below:

– The action is triggered by the event that an NaaS CSC's location is changed (location near to another NaaS CSP's data centre) and the network load between these two data centres is low;
– The VM is migrated to the new data centre;
– The VPN connecting an NaaS CSC's services is updated.

The above used network resources are managed by a resource abstraction and control functional component in the form of NaaS resource model, containing the network topology (physical and virtual interconnection of network elements, etc.), inventory (database of network elements, ports, device type, capabilities, etc.), protocol specific information, etc.

Appendix III

Relationship between NaaS functional architecture and SDN

(This appendix does not form an integral part of this Recommendation.)

As categorized by [ITU-T Y.3512], NaaS services are divided into NaaS application services, NaaS platform services, and NaaS connectivity services. As a kind of cloud service, based on its use cases and derived functional requirements specified in [ITU-T Y.3512], network connectivity service can be implemented by the traditional technologies and/or emerging technologies, such as SDN.

Both cloud computing and SDN have their own reference architectures, whose mapping is presented in Figure III.1. NaaS connectivity is a kind of cloud service, which is located in the services layer of the cloud reference architecture. If it is supported and implemented by SDN, a NaaS connectivity service can be regarded as one kind of SDN application in SDN architecture and seen as a bridge between the cloud computing and SDN architectures.

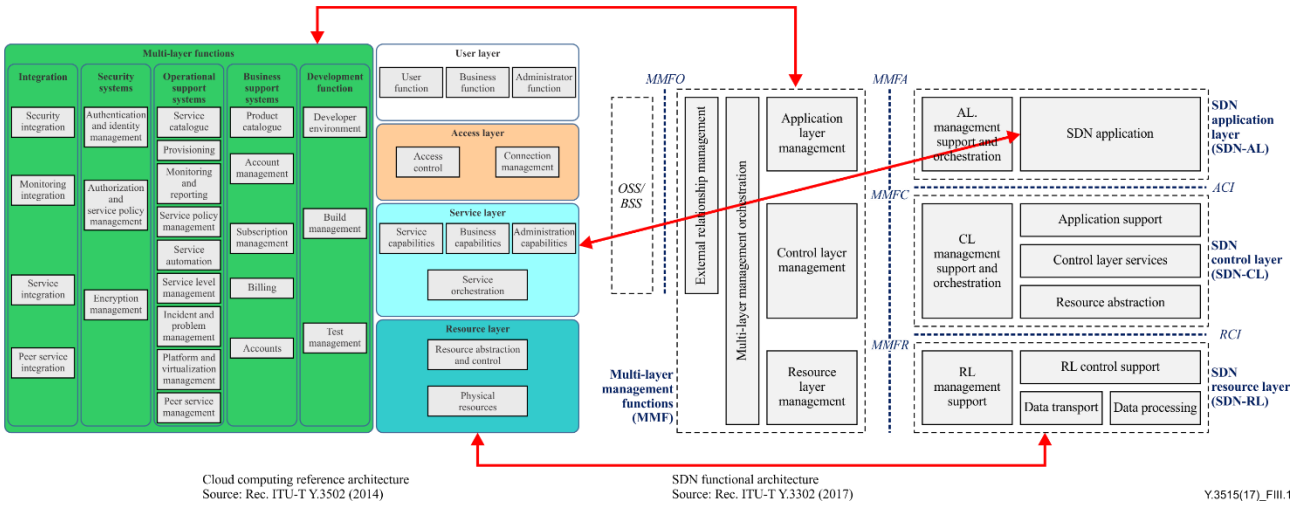

Figure III.1 – Mapping of architectures of cloud computing and SDN

Figure III.2 presents the positioning of a NaaS connectivity service as an application in the SDN architecture. Such NaaS connectivity service interacts with SDN management functionalities and SDN control layer functionalities including application support entity, orchestration entity, abstraction entity.

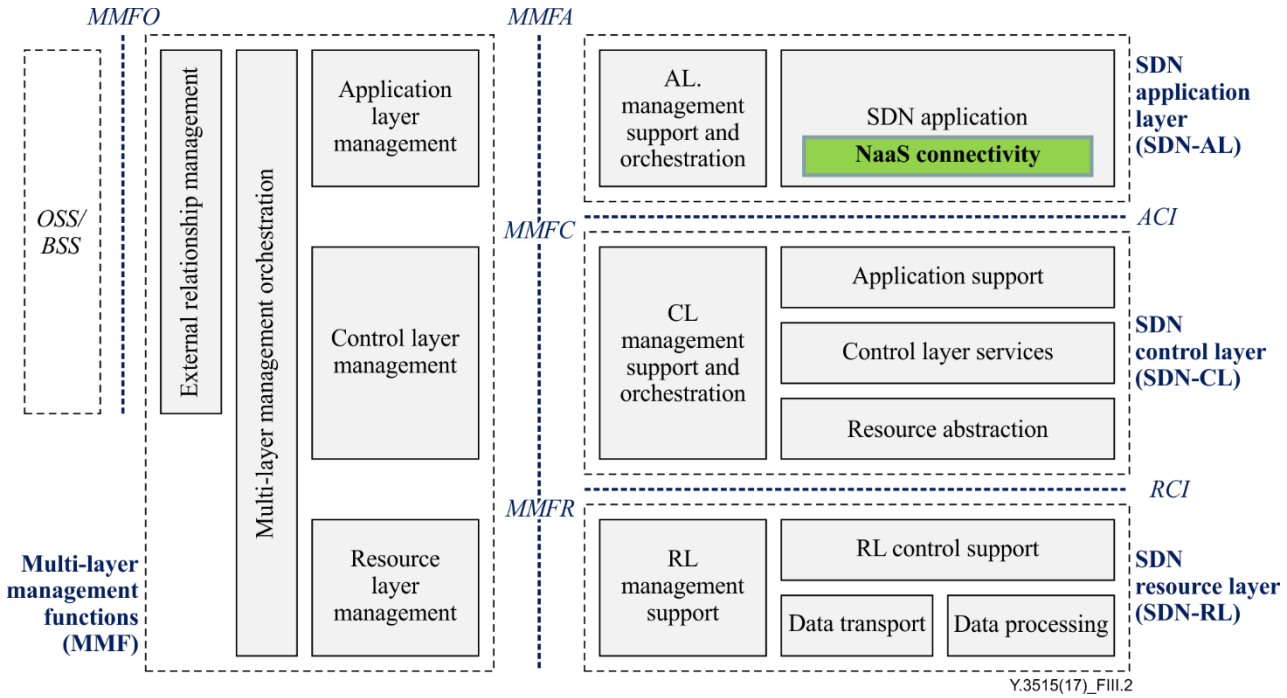

Figure III.2 – NaaS connectivity and relationships SDN functional entities

In the use cases of [ITU-T Y.3512], SDN is not mentioned, although it can be regarded as one of the implementation technologies especially in NaaS connectivity use cases.

Appendix IV

Example of NFV and SDN usage in support of NaaS architecture

(This appendix does not form an integral part of this Recommendation.)

This appendix provides an example of how NFV and SDN can be used in realizing the NaaS functional architecture.

The NFV architectural framework as defined in [b-ETSI NFV-arch] and [b-ETSI NFV-mano] provides a high-level functional architectural framework and design philosophy of virtualized network functions and of the supporting infrastructure. It identifies functional blocks and the main reference points between such blocks. In particular, the following functional blocks are described:

– VNF;
– NFV Infrastructure (NFVI), including:
  • Hardware and virtualized resources; and
  • Virtualization layer.
– Virtualized infrastructure manager (VIM);
– NFV orchestrator (NFVO);
– VNF manager (VNFM);
– WAN infrastructure manager (WIM).

[ITU-T Y.3300] describes the framework of SDN specifying fundamental aspects of SDN and providing a high-level architecture consisting of the following layers:

– SDN application layer;
– SDN control layer;
– SDN resource layer.

Figure IV.1 shows how elements of the NFV and SDN architectures (represented using dotted boxes) can be mapped to the functional components of the NaaS architecture defined in clause 8 of this Recommendation.

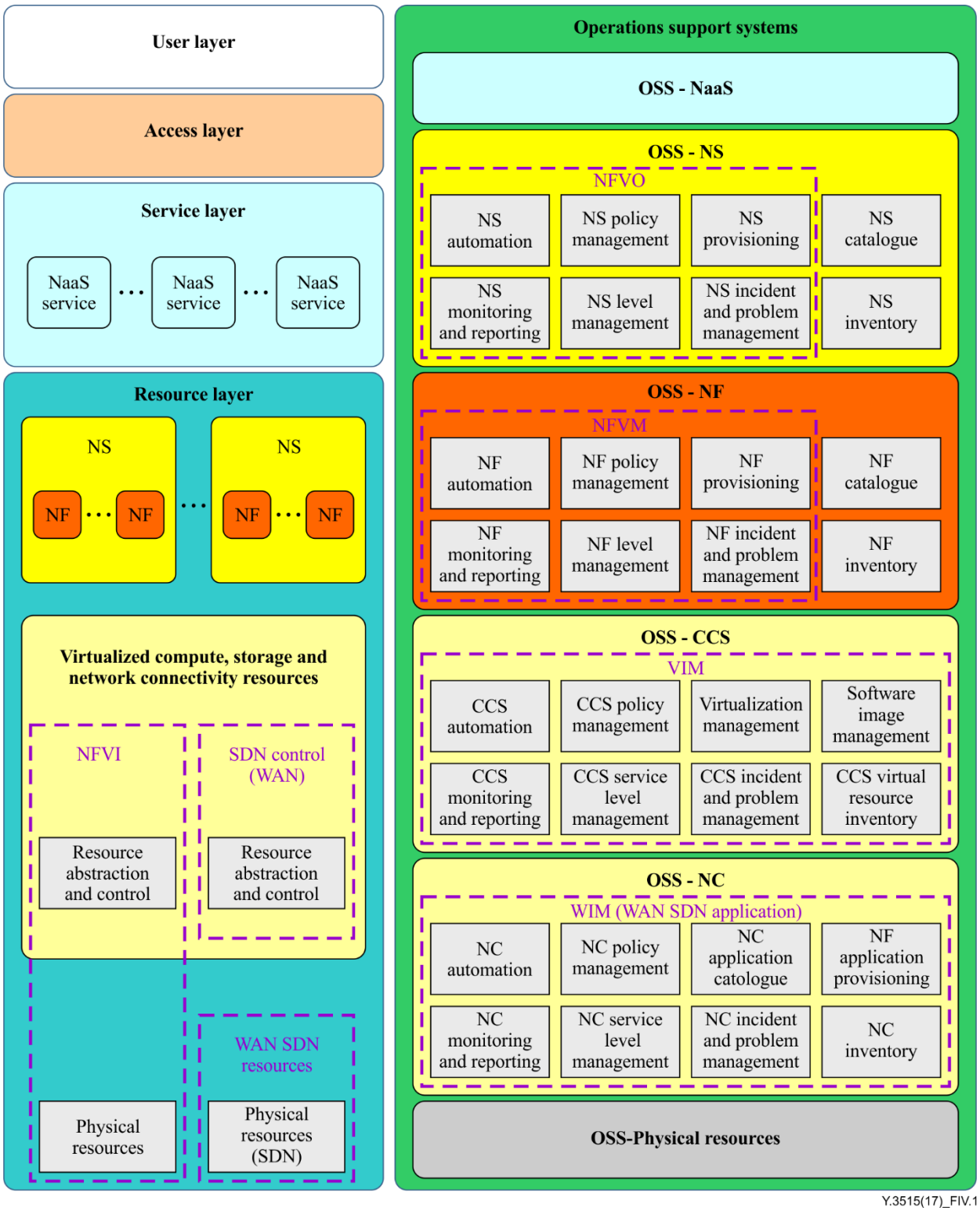

Figure IV.1 – Example of NFV and SDN usage to support NaaS

Regarding the use of SDN, the scenario illustrated in Figure IV.1 assumes that SDN is used to control network connectivity between NFVI PoPs. The resources controlled by SDN are also assumed to be physical resources in a wide area network (e.g., physical switches or routers) and therefore does not cover the case where the SDN resource layer can itself be virtualized (e.g., virtual switches or routers supported as virtualized network functions). The potential use of SDN in the NFVI is not shown in Figure IV.1. The SDN control layer (e.g., the SDN controller) and the SDN resource layer (e.g., switches and routers) can also be virtualized as well elements of the NFV architecture (e.g., VNFM).

Bibliography

[b-ETSI NFV-arch] ETSI GS NFV 002 V1.2.1 (2014), *Network Functions Virtualisation (NFV); Architectural Framework*.

[b-ETSI NFV-mano] ETSI GS NFV-MAN 001 V1.1.1 (2014), *Network Functions Virtualisation (NFV); Management and Orchestration*.

[b-ETSI NFV-term] ETSI GS NFV 003 V1.2.1 (2014), *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017