ETSI GR NFV-EVE 012 V3.1.1 (2017-12)

Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/NFV-EVE012

Keywords
network, NFV, slicing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document analyses use cases related to network slicing as defined in SDOs and industry fora. Furthermore, the present document describes how these use cases could be mapped to the current NFV concepts and supported by the ETSI NFV architectural framework [i.2] and by NFV-MANO [i.10].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR NFV 001 (V1.2.1) (05-2017): "Network Functions Virtualisation (NFV); Use Cases".

[i.2] ETSI GS NFV 002 (V1.2.1) (12-2014): "Network Functions Virtualisation (NFV); Architectural Framework".

[i.3] ETSI GS NFV 003 (V1.2.1) (12-2014): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.4] ETSI GS NFV-EVE 005 (V1.1.1) (12-2015): "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework".

[i.5] ETSI GS NFV-IFA 009: "Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options".

[i.6] ETSI GS NFV-IFA 013 (V2.1.1) (10-2016): "Network Functions Virtualisation (NFV); Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification".

[i.7] ETSI GS NFV-IFA 014 (V2.3.1) (08-2017): "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Network Service Templates Specification".

[i.8] ETSI GR NFV-IFA 022 (V0.8.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services".

[i.9] ETSI GR NFV-IFA 028 (V0.13.0): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains".

[i.10] ETSI GS NFV-MAN 001 (V1.1.1) (12-2014): "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.11] ETSI GR NFV-REL 007 (V1.1.1) (09-2017): "Network Functions Virtualisation (NFV); Reliability; Report on the resilience of NFV-MANO critical capabilities".

[i.12] ETSI GS NFV-SEC 009 (V1.2.1) (12-2016): "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.13] ETSI GS NFV-SEC 012 (V3.1.1) (01-2017): "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.14] NGMN Alliance: "Description of Network Slicing Concept", January 2016.

[i.15] NGMN Alliance: "5G security recommendations; Package #2: Network Slicing", April, 2016.

[i.16] ONF TR-521: "SDN Architecture", Issue 1.1, February 2016.

[i.17] ONF TR-526: "Applying SDN architecture to 5G slicing", Issue 1, April 2016.

[i.18] ONF TR 527: "Functional Requirements for Transport API", June 2016.

[i.19] ONF TR-540: "Orchestration: A More Holistic View", January 2017.

[i.20] 3GPP TS 22.261 (V15.2.0) (09-2017): "Service requirements for next generation new services and markets".

[i.21] 3GPP TR 28.801 (V15.0.0) (09-2017): "Telecommunication management; Study on management and orchestration of network slicing for next generation network".

[i.22] ETSI GS NGP 001: "Next Generation Protocol (NGP); Scenario Definitions".

[i.23] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.24] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV); Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[i.25] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV); Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.26] ETSI GS NFV-IFA 012: "Network Functions Virtualization (NFV) Release 3; Management and Orchestration; Os-Ma-Nfvo reference point - Application and Service Management Interface and Information Model Specification".

[i.27] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV); Management and Orchestration; Functional requirements specification".

[i.28] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV); Management and Orchestration; VNF Packaging Specification".

[i.29] 3GPP TR 23.799: "Study on Architecture for Next Generation System".

[i.30] 3GPP TS 23.501: "System Architecture for the 5G System".

[i.31] 3GPP TS 23.502: "Procedures for the 5G System".

[i.32] 3GPP TR 33.899: "Study on the security aspects of the next generation system".

[i.33] 3GPP TS 28.531: "Provisioning of network slicing for 5G networks and services".

[i.34] 3GPP TS 28.530: "Management of network slicing in mobile networks; Concepts, use cases and requirements".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.3] and the following apply:

3GPP	3rd Generation Partnership Project
5G	Fifth Generation
AN	Access Network
CN	Core Network
CSMF	Communication Service Management Function
HMEE	Hardware-Mediated Execution Enclave
NF	Network Function
NGMN	Next Generation Mobile Networks
NGP	Network Generation Protocols
NS	Network Service
NSI	Network Slice Instance
NSM	Network Slice Manager
NSMF	Network Slice Management Function
NSSI	Network Slice Subnet Instance
NSSMF	Network Slice Subnet Management Function
NST	Network Slice Template
OAM	Operations and Management
ONF	Open Networking Foundation
QoS	Quality of Service
SDN	Software Defined Networking
SDO	Standards Development Organisation
TN	Transport Network

4 Overview of network slicing

4.1 Introduction

Network slicing is defined by multiple SDOs and Fora. However, the meaning and understanding of the network slicing concept are different from each other and there is no common definition. The present document does not define network slicing use cases or features but references external SDOs and Fora's definition and concept of network slicing within the context of each individual SDO/Fora.

Clause 4.2 shows relevant external body's documents which introduce and define network slicing, and describes related details provided in NGMN, 3GPP, and ONF. It also describes the possible relationship with the NFV constructs. Clause 4.3 describes NFV and SDN relation in a multi-tenant and multi-domain environment in term of network slice deployment.

4.2 Concepts defined by SDOs and Fora and NFV architectural framework mapping

4.2.1 Potential relevant SDOs and Fora

Table 4.2.1-1 describes relevant SDOs and Fora and their documentation which introduce and define the concept of network slicing.

Table 4.2.1-1: Relevant external bodies' documents

External Body (Upstream, User, or Both)	Title of Document or Activity	Area	Scope	Current Status	Relation to Network Slicing	Relation to NFV ISG support to Network Slicing
NGMN	5G white paper	High level requirements	5G white paper from NGMN	Published	Introduces network slicing, named as 5G slicing in 5G white paper, for purposes of flexibility, management and orchestration. Needs standardization phase to support those motivations and requirements.	
NGMN	White paper description of network slicing	High level requirements	NGMN white paper for network slicing	Published	NGMN white paper describing network slicing for service provider networks.	
ONF	Applying SDN Architecture to 5G Slicing (ONF TR-526 [i.17])	SDNizing network slicing for 5G services	Network slice abstraction for sustainability and business agility	Published	Generic requirements for SDN-based network slicing for 5G services including orchestration for holistic operations [i.19].	
3GPP SA2	Study on Architecture for Next Generation System (3GPP TR 23.799 [i.29])	High level requirements	Network slice related functionality	Published	Network architecture including network entity and UE. Key issues identified by 3GPP SA2 to address network slicing selection, isolation, roaming and security as well as some examples. 3GPP SA2 specifies network slicing concept and network architecture and does not have direct relation to virtualisation and MANO work in ISG NFV.	
3GPP SA2	System Architecture for the 5G System (3GPP TS 23.501 [i.30])	Architectural requirements	Network slice related functionality	Work in progress	Definition, identification, selection, subscription, configuration and storage aspects of network slicing. High level functionality for network slicing, and network slicing supported by the architecture including roaming and non-roaming scenarios.	

External Body (Upstream, User, or Both)	Title of Document or Activity	Area	Scope	Current Status	Relation to Network Slicing	Relation to NFV ISG support to Network Slicing
3GPP SA2	Procedures for the 5G System (3GPP TS 23.502 [i.31])	Procedures and flows of the architectural elements	Network slice related procedures	Work in progress	Procedures description and aspects of supporting network slicing in the 5G system.	
3GPP SA3	Study on the security aspects of the next generation system (3GPP TR 33.899 [i.32])	High level requirements	Network slice related security	Work in progress	Study work in 3GPP SA3 including security areas and high level security requirements related to network slicing.	
3GPP SA5	Study on management and orchestration of network slicing (3GPP TR 28.801 [i.21])	High level requirements	Network slice management	Published	Study work in 3GPP SA5 on management and orchestration of network slicing in mobile networks.	May be relevant to ETSI GS NFV-IFA 008 [i.25], ETSI GS NFV-IFA 013 [i.6], and ETSI GS NFV-IFA 014 [i.7].
3GPP SA5	Provisioning of network slicing for 5G networks and services (3GPP TS 28.531 [i.33])	Detailed specification of network slice provisioning	Network slice management	Work in progress	Work item in 3GPP SA5 on network slice provisioning which includes service provisioning related information model and NST specification.	May be relevant to ETSI GS NFV-IFA 013 [i.6] and ETSI GS NFV-IFA 014 [i.7].
3GPP SA5	Management of network slicing in mobile networks - concepts, use cases and requirements (3GPP TS 28.530 [i.34])	Detailed specification of network slice requirements	Network slice management	Work in progress	Work item in 3GPP SA5 on network slice management which specifies the management related use cases and requirements of 3GPP TR 28.801 [i.21].	May be relevant to ETSI GS NFV-IFA 013 [i.6], ETSI GR NFV-IFA 022 [i.8]
ETSI ISG NGP	Next Generation Protocols (NGP); Scenarios Definitions (ETSI GS NGP 001 [i.22])	High level requirements	Key scenarios for the NGP	Frozen	Specify the key scenarios for the NGP, including the network slicing use case of network virtualisation.	

4.2.2 NGMN

4.2.2.1 Network slicing as defined by NGMN

According to clause 4 of the NGMN's White Paper [i.14], a Network Slice Instance (NSI) may be composed by none, one or more Network Slice Subnet Instance (NSSI), which may be shared by another NSI. Similarly, the NSSI is formed of a set of Network Functions, which can be either VNFs or PNFs.

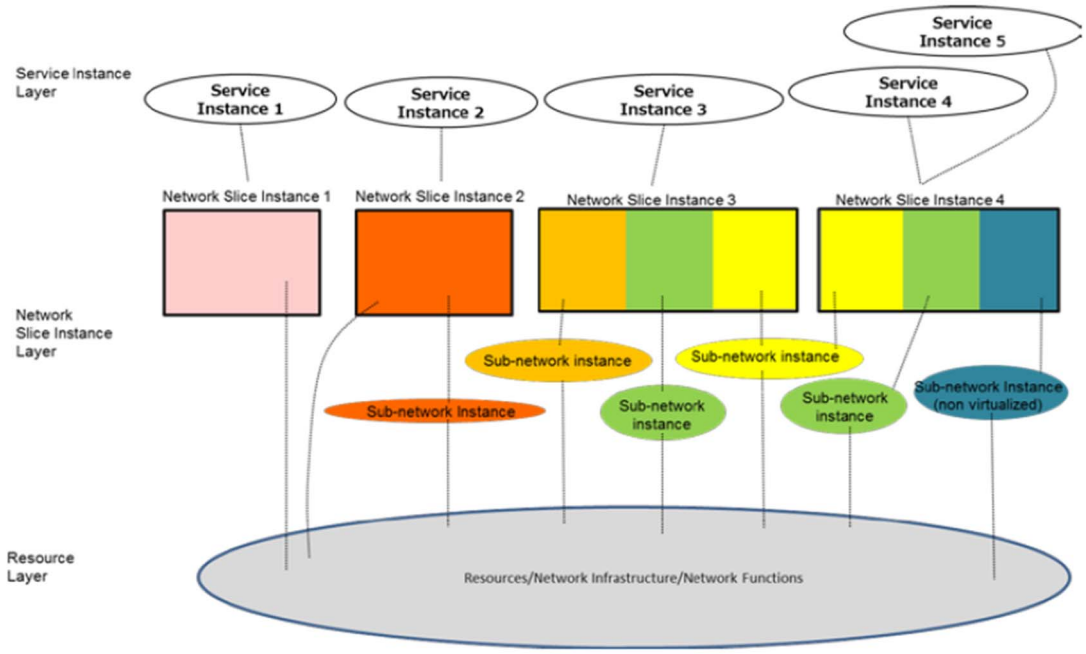

Figure 4.2.2.1-1: Network slice conceptual outline (figure 1 in NGMN White Paper [i.14])

4.2.3 3GPP

4.2.3.1 Network slicing as defined by 3GPP

According to clause 4.2.1 of 3GPP TR 28.801 [i.21], the network slice concept includes the following aspects:

1) Completeness of an NSI:

   - An NSI is complete in the sense that it includes all functionalities and resources necessary to support certain set of communication services thus serving certain business purpose.

2) Components of an NSI:

   - The NSI contains NFs (e.g. belonging to AN and CN).

   - If the NFs are interconnected, the 3GPP management system contains the information relevant to the connections between these NFs such as topology of connections, individual link requirements (e.g. QoS attributes), etc.

   - For the part of the TN (Transport Network) supporting connectivity between the NFs, the 3GPP management system provides link requirements (e.g. topology, QoS attributes) to the management system that handles the part of the TN supporting connectivity between the NFs.

3) Resources used by the NSI:

   - The NSI is realized via the required physical and logical resources.

4) Network Slice Template:

   - The network slice is described by a Network Slice Template (NST). The NSI is created using the NST and instance-specific information.

5) NSI policies and configurations:

   - Instance-specific policies and configurations are required when creating an NSI.

   - Network characteristics examples are ultra-low-latency, ultra-reliability, etc.

- NSI contains a Core Network part and an Access Network part.

6) Isolation of NSIs:

- A NSI may be fully or partly, logically and/or physically, isolated from another NSI.

4.2.3.2 Mapping NFV and 3GPP network slicing concepts

4.2.3.2.1 Network slice vs. Network service

3GPP TR 28.801 [i.21] describes an information model where a network slice contains one or more network slice subnets, each of which in turn contains one or more network functions and can also contain other network slice subnets (see left-hand side of figure 4.2.3.2-1). These network functions can be managed as VNFs and/or PNFs. An NFV Network Service (NS) can thus be regarded as a resource-centric view of a network slice, for the cases where a Network Slice Instance (NSI) would contain at least one virtualised network function.

According to 3GPP TR 28.801 [i.21], a network slice subnet instance (NSSI) can be shared by multiple NSIs. The virtualised resources for the slice subnet and their connectivity to physical resources can be represented by the nested NS concept defined in ETSI GS NFV-IFA 014 [i.7] (see right-hand side of figure 4.2.3.2-1), or one or more VNFs and PNFs directly attached to the NS used by the network slice. The dotted arrows in figure 4.2.3.2-1 illustrate this correspondence from a resource point of view.

NOTE: ETSI ISG NFV does not handle the:

- Application-aware NS configuration and management; and
- VNF application layer configuration and management; and
- Management and deployment of PNFs, or their application layer configuration and management.

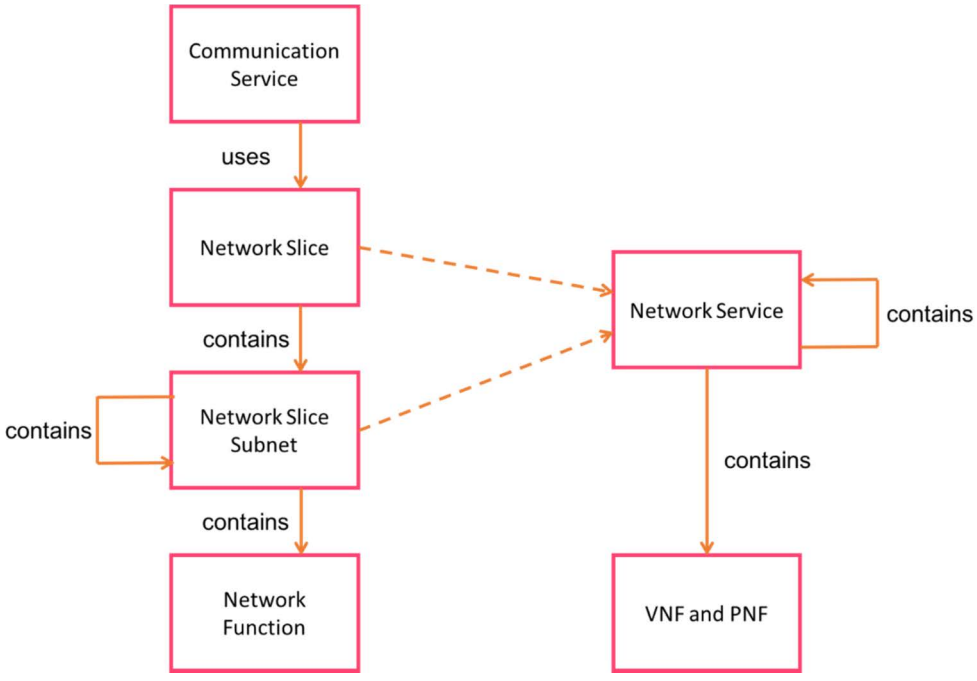

Figure 4.2.3.2-1: Relating the information models

4.2.3.2.2 Architecture

3GPP TR 28.801 [i.21] identifies 3 management functions related to network slicing management:

- Communication Service Management Function (CSMF): this function is responsible for translating the communication service related requirement to network slice related requirements. The CSMF communicates with the Network Slice Management Function (NSMF).

- Network Slice Management Function (NSMF): this function is responsible for the management (including lifecycle) of NSIs. It derives network slice subnet related requirements from the network slice related requirements. NSMF communicates with the NSSMF and the CSMF.

- Network Slice Subnet Management Function (NSSMF). This function is responsible for the management (including lifecycle) of NSSIs. The NSSMF communicates with the NSMF.

As shown in figure 4.2.3.2.2-1, the Os-Ma reference point can be used for the interaction between 3GPP slicing related management functions and NFV-MANO. To properly interface with NFV-MANO, the NSMF and/or NSSMF need to determine the type of NS or set of NSs, VNF and PNF that can support the resource requirements for a NSI or NSSI, and whether new instances of these NSs, VNFs and the connectivity to the PNFs need to be created or existing instances can be re-used.

NOTE 1: In order to use the NS, the NSMF and/or NSSMF would have to maintain an association between Network Slice Templates (NSTs), and NFV Network Service Descriptors (NSDs) with applicable deployment flavour identifiers, as well as an association between NSI identifiers and NS instance identifiers.

NOTE 2: The 3GPP slice-related management functions are still under definition in 3GPP SA5 and future updates might require further analysis about the interaction between 3GPP slicing related management functions and NFV-MANO.

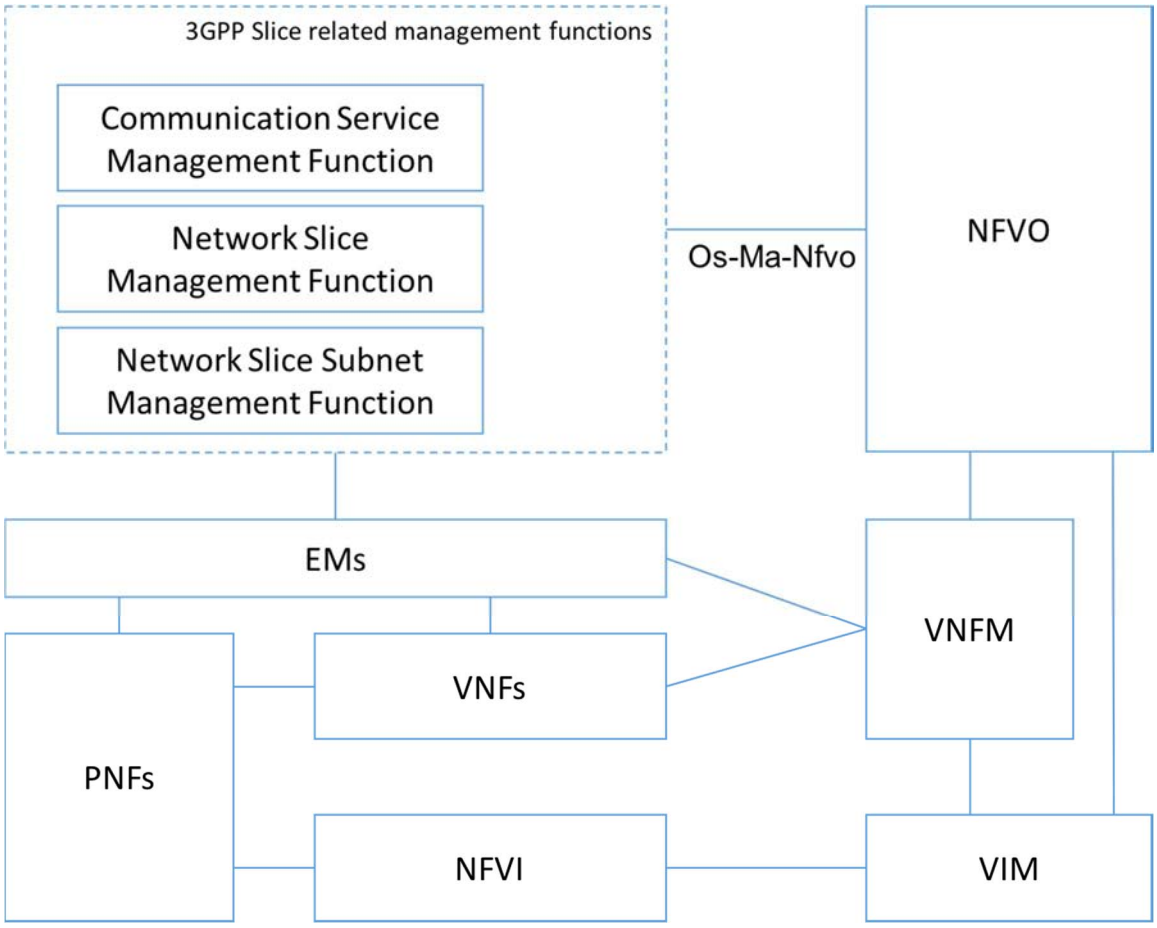

Figure 4.2.3.2.2-1: Network slice management in an NFV framework

From a resource management viewpoint, NSI can be mapped to an instance of a simple or composite NS or to a concatenation of such NS instances. From a resource management viewpoint, different NSIs can use instances of the same type of NS (i.e. they are instantiated from the same NSD) with the same or different deployment flavours. Alternatively, different NSIs can use instances of different types of NSs. The first approach can be used if the NSIs share the same types of network functions (or a large common subset) but differ in terms of the performance expected from these network functions (and from the virtual links connecting them) and/or the number of instances to be deployed for each of them. If slices differ more significantly, mapping to different NSs, each with its own NSD can be considered. The same mapping principles might apply to NSSIs.

4.2.3.2.3 Network slice lifecycle management

3GPP TR 28.801 [i.21] describes the lifecycle of a network slice, which is comprised of the four following phases:

- Preparation;
- Instantiation, Configuration and Activation;
- Run-time;
- Decommissioning.

The preparation phase includes the creation and verification of NST(s). From an NFV perspective, the resource requirement for a NST can be realized by one or more existing NSDs that have been previously on-boarded on the NFVO. The creation of a new NST can lead to requiring update of an existing NSD or generation of a new NSD followed by on-boarding the new NSD if the slice requirements do not map to an already on-boarded NSD (i.e. available in the NSD catalogue). Indeed, the NS for the multiple NSIs may be instantiated with the same NSD, in order to deliver exactly the same optimizations and features but dedicated to different enterprise customers. On the other hand, a network slice intended to support totally new customer facing services is likely to require a new NS and thus the generation of a new NSD.

The network slice instantiation step in the second phase triggers the instantiation of the underlying NSs. NFV-MANO functions are only involved in the network slice configuration phase if the configuration of virtualisation-related parameters is required on one or more of the constituent VNF instances. Configuration of the network applications embedded in the constituent network functions involves the NSMF or NSSMF and/or other parts of the OSS/BSS, and the element managers (if any) associated to these functions. NFV-MANO functions can be triggered during the network slice activation step. If explicit activation of VNFs is required, the NSMF or the NSSMF can change the operational state of those VNFs through an Update NS operation defined in ETSI GS NFV-IFA 013 [i.6].

The involvement of NFV-MANO in the run-time phase is limited to the operations related to the performance management, fault management, and lifecycle management of virtualised resources (e.g. scaling an underlying NS to expand a NSI).

The decommissioning phase triggers the termination of the underlying network service instances.

4.2.4 ONF

4.2.4.1 Network slicing abstraction and resource control from the ONF perspective

According to clause 3 of ONF TR-526 [i.17], slicing requires the partitioning and assignment of a set of resources that can be used in an isolated, disjunctive or shared manner. A set of such dedicated resources can be called a slice instance. Examples of resources to be partitioned or shared, understanding they can be physical or virtual, would be: bandwidth on a network link, forwarding tables in a network element (switch, router), processing capacity of servers, processing capacity of network elements. As it can be assumed that slice instances will often contain a combination/group of the above resources, appropriate resource abstractions as well as the exposure of abstract resources towards clients are needed for the operation of slices.

To comprehend the notion of a slice from the ONF perspective, it is important to understand the ONF SDN architecture concept in general, especially the concepts of *client context* and *server context* which are defined in ONF TR-521 [i.16].

Major components of SDN are resources and controllers. Service delivery (send, receive, transmit, transform data) makes use of resources. Provisioning, management and control of services and related resources are executed via the controller.

The controller in the SDN architecture is at the centre of a feedback loop: it mediates client requirements with resource availability, supporting policy-driven real-/run-time optimization of changes in network state, service parameters, service and traffic flow.

An SDN controller works with two major types of resource views: it interacts with its client via a (client specific) client context, and with its resources via a (server specific) server context.

The term *virtualisation* is used to describe the function of a controller to aggregate and abstract the underlying resources it manages-controls. Views onto such virtualised resources, or resource groups dedicated to particular clients, are provided to clients/applications/users via northbound interfaces.

The term *orchestration* is used to describe the responsibility of the controller to dispatch resources in a way that simultaneously satisfies service demands from all of its clients as cost-effectively as possible.

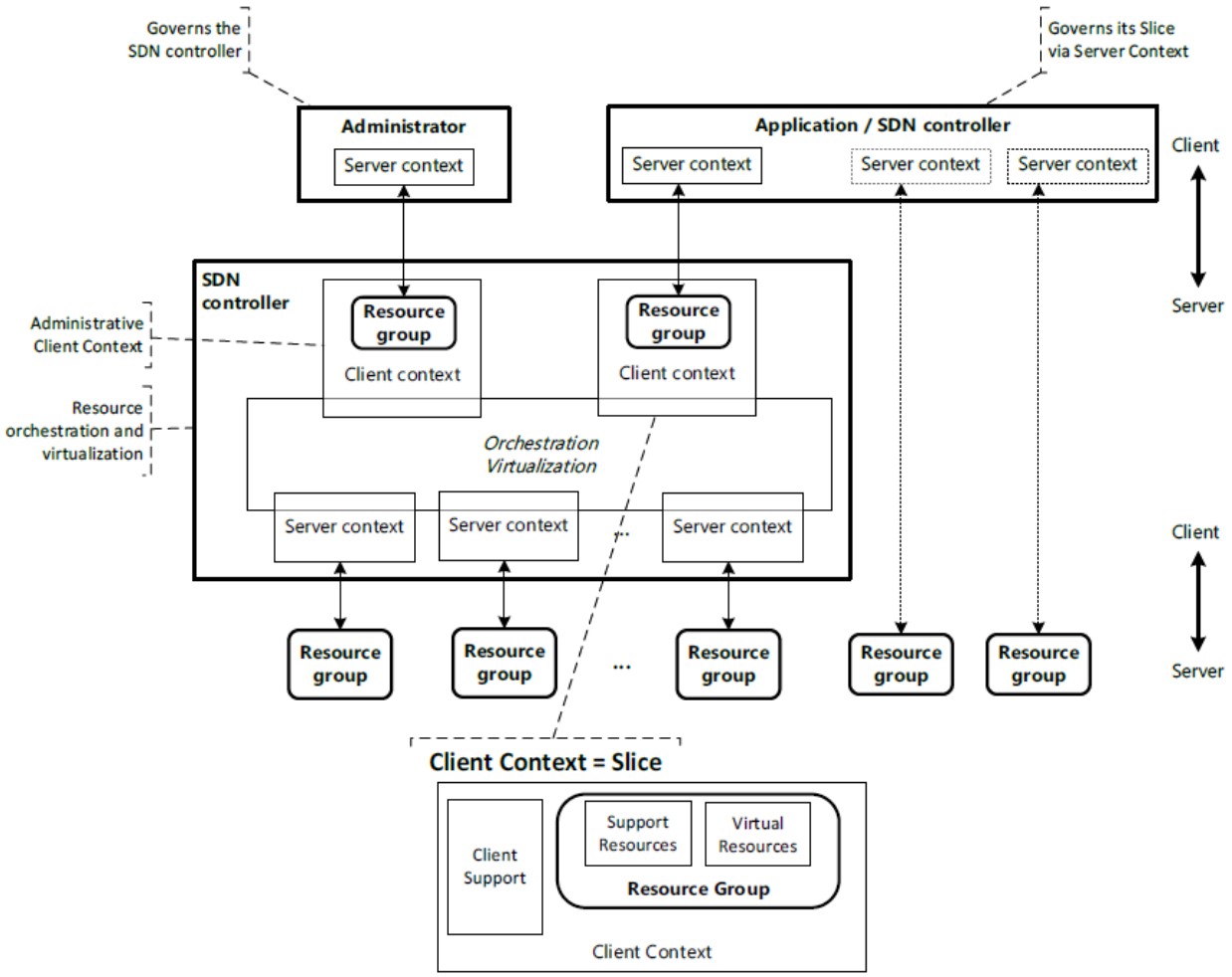

Figure 4.2.4.1-1: Core concepts of the SDN architecture and slice abstraction (figure 2 in ONF TR-526 [i.17])

An SDN controller's client context provides the complete abstract set of resources and supporting control logic for constituting a slice, including the complete collection of related client service attributes. The client context also offers to the client functions to manage-control the slice resources, including OAM related-functions, as visible by/available to the client according to administrative policy.

A *client context* represents the necessary and sufficient material in the SDN controller to support a given client, where a client may be a customer, partner, or even another entity within the same administration that owns the controller. It includes all of the attributes of a service as requested by the client, and may contain service-specific information necessary to map service attributes into the realization of the service.

The resource group in a client context defines the semantic interfaces exposed to the client. Virtual resources represent infrastructure resources that are created from the SDN controller's underlying resources through the process of virtualisation, and that are exposed to the client by way of a mapping function. Support resources, which represent functions hosted in the SDN controller itself, enable or facilitate interaction with the client. Examples for support resources are: security credentials, notifications subscription, profiles, logs, etc.

NOTE: The administrator's client context is special in that it is used for the internal configuration and management of (administrative) policies and constraints of the controller, including all client and server contexts.

A *server context* is the symmetric counterpart to a client context. It contains everything necessary and sufficient to interact with a group of underlying resources, which could be, for example, a discrete network element or the virtual resources contracted from a partner domain.

Resources fall into and may be combinations of the categories network, storage and compute, with resource capabilities therefore ranging from simple, e.g. switching between ports, to complex, e.g. firewall with DPI or a video transcoder.

The state of the resources owned by the controller is continually adapted in compliance with policies provided by the administrator. These policies include parameters to satisfy commitments to clients. For all services requested by clients, resources are provided and maintained throughout their lifecycle.

There are trust and, potentially, ownership borders across interfaces between resource group and server context. These interfaces expose views on resources available in the client context and related services. The views and services visible to each client depend on the association (business agreement) between service user and service provider, and normally include information hiding, namespace and functional mapping and translation, and service level agreements.

4.2.4.2 Mapping NFV and ONF SDN architecture network slicing concepts

According to clause 3 of ONF TR-526 [i.17], slicing requires the partitioning and assignment of a set of resources that can be used in an isolated, disjunctive or shared manner. A set of such dedicated resources can be called a slice instance.

ONF TR-526 [i.17] further states that a controller's client context provides the complete abstract set of resources and supporting control logic for constituting a slice, including the complete collection of related client service attributes. The client context also offers to the client functions to manage-control the slice resources, including OAM functions, whose visibility and availability for the client are determined by administrative policy.

A controller's server context contains everything necessary and sufficient for the controller to interact with a group of underlying resources. Resources fall into and may be combinations of the categories network, storage and compute.

ONF network slicing as defined in ONF TR-526 [i.17] has the following implications in VNF configuration, NS, NSD (affinity, anti-affinity), Virtualised resources, etc. (see figure 4.2.4.2-1):

- The concept of SDN controller's client context can be mapped to the concept of NS in NFV.
- The concept of SDN controller's server context can be mapped to the concept of NFV NFVI resources.

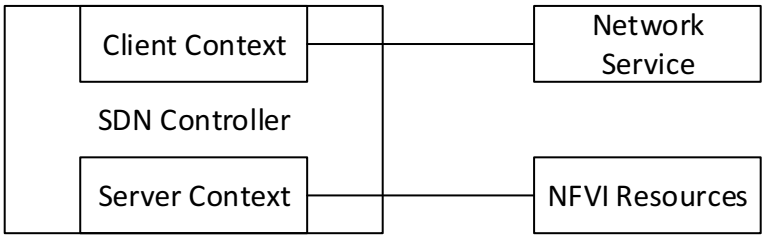

Figure 4.2.4.2-1: Mapping between ONF slicing concept with ETSI NFV elements

4.3 NFV and SDN relation in multi-tenant and multi-domain environments

Network slices are meant to be mutually isolated in the sense that they should run concurrently on top of a common shared infrastructure without (either directly or indirectly) affecting each other. This infrastructure is composed of resources that may be owned and managed by different (and potentially non-trusted) administrative domains. The shared and multi-domain nature of the infrastructure makes isolation a capital requirement for network slicing. Fulfilling each of the duly defined isolation properties (performance, resiliency, security, privacy and management isolation) is required to ensure full mutual isolation among slices. This clause analyses how the isolation properties necessary to achieve network slicing can be satisfied by applying current ETSI NFV concepts, in particular those described in ETSI GS NFV-EVE 005 [i.4], ETSI GR NFV-IFA 022 [i.8] and ETSI GR NFV-IFA 028 [i.9].

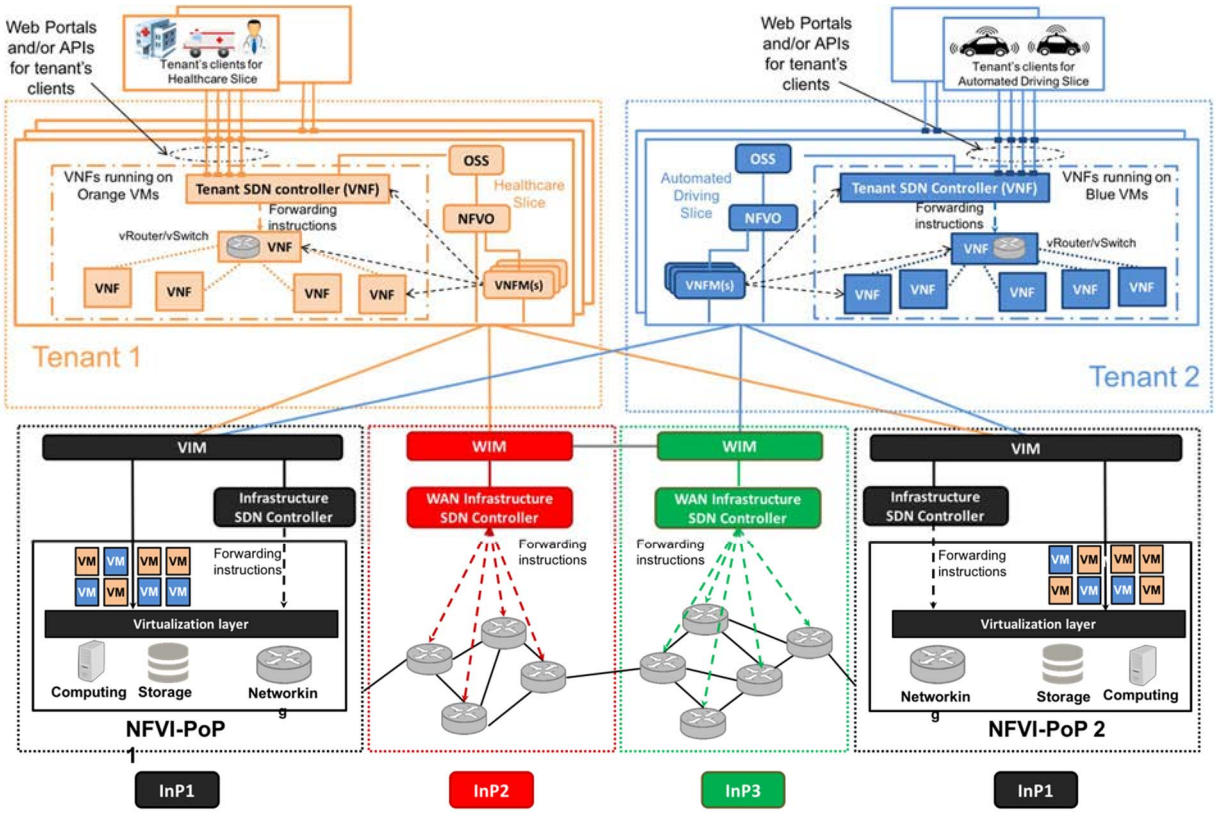

Figure 4.3-1: Network slicing deployment applying NFV concepts to achieve isolation

Figure 4.3-1 shows an example of a possible network slicing deployment illustrating the application of the concepts mentioned above to achieve isolation properties. The set of network functions, SDN and NFV-MANO functions comprising the tenancy entities is not exhaustive, and other examples are possible.

For obvious simplicity reasons, the figure shows a limited number of slice tenants and providers, but without any loss of generality. The deployment depicted in figure 4.3-1 is aligned with the interaction between SDN and NFV proposed by ETSI GS NFV-EVE 005 [i.4], and analyses the applicability of SDN in the WAN to enable multi-site network slicing deployments, in accordance with the matters discussed in ETSI GR NFV-IFA 022 [i.8] and ETSI GR NFV-IFA 028 [i.9]. In line with one of the architectural options presented in ETSI GS NFV-EVE 005 [i.4], two different types of SDN controllers are considered, namely tenant and infrastructure SDN controllers, each logically placed in different administrative domains. The tenant SDN controller dynamically configures and chains VNFs to realize network services in the tenant domain. The infrastructure SDN controller manages and controls the NFVI network resources (placed in a NFVI-PoP or a WAN) to set up the connectivity that is required for communicating the tenant VNFs in the infrastructure domain. The tenant SDN controller only controls the software applications of the VNFs for configuration and chaining purposes, but not their underlying NFVI resources. The latter is under the responsibility of the infrastructure SDN controller, in charge of managing and controlling the connectivity among the virtualisation containers that host the tenant VNFs' software applications.

The network slices graphically depicted in figure 4.3-1 run in parallel on a shared underlying NFVI. The resources of the shared underlying NFVI are owned and managed by three different infrastructure providers, each defining a different infrastructure domain. Each NFVI-PoP has a single VIM instance that directly configures and manages the virtualisation containers and their underlying hardware. Their connectivity is locally enforced by the infrastructure SDN controller, which programmatically manages the NFVI-PoP network resources under the supervision of the VIM. To enable connectivity between NFVI-PoPs, each WAN domain relies on a WAN Infrastructure Manager (WIM) instance, as proposed in the architecture model discussed in ETSI GR NFV-IFA 022 [i.8].

The NFVI resources owned and managed by the Infrastructure Providers are delivered to the tenants logically placed on top of them. Each tenant makes use of the NFVI resources supplied by the underlying Infrastructure Provider to serve the performance needs of the slices in the tenant domain. The scenario presented above is well-aligned with the NFVI as a Service (NFVIaaS) approach discussed in ETSI GR NFV-IFA 028 [i.9]. In the present case, each Infrastructure Provider takes the NFVIaaS provider's role, and each tenant acts as an NFVIaaS consumer. These tenants, each with its own set of network slices, need to be isolated from each other. To this end, both VIMs and WIMs should support multi-tenancy, offering separate NFVI resources to subscribed tenants through dedicated interfaces.

On one side, VIMs should have appropriate resource pooling mechanisms to provide subscribed tenants with isolated resource environments endowed with high availability and fault resilience features for tenant VNFs deployment. On the other side, WIMs should have mechanisms similar to those described in ONF TR 527 [i.18] to simultaneously manage a number of virtual topologies in the WAN with different levels of abstraction.

Each tenant manages the slices that are operative in its administrative domain by means of its NFVO, logically placed in the tenant domain. Tenants rely on their NFVOs to perform resource scheduling functions in the tenant domain. As these resources may be provided by different Infrastructure Providers, the NFVO should need to orchestrate resources across different administrative domains in the infrastructure. When the discussions in both ETSI GR NFV-IFA 028 [i.9] and the present document is translated into normative requirements, further alignment of roles may be required. As depicted in figure 4.3-1, each of the network slices serving a tenant comprises an NFVO, one (or several) VNFM(s), a tenant SDN controller, and an Operations Support System (OSS). The fact that each network slice has these functional blocks enables the tenant to preserve the required management isolation among slices. Other combinations of number of NFVO/VNFM are also possible depending on the level of isolation and other requirements, e.g. when an NFVO can be used to fulfil more than one slice.

The NFVO dynamically manages the lifecycle of the network slice constituent network service(s), including any associated VNFFG(s), while the VNFM(s) perform(s) lifecycle management operations over the slice VNFs. In addition to the NFVO and VNFM(s), each network slice has a tenant SDN controller. Deployed as a VNF itself, the tenant SDN controller dynamically configures the (other) inner network slice's VNFs, and properly chains them to build up the Network Service(s) that the slice needs to accommodate for a given use case. Since Network Services and VNF operations are highly correlated, once it is made aware by the NFVO that a Network Service has been instantiated, there is a need for the OSS, an SDN application from the tenant SDN controller's perspective, to interact with the controller and instruct it to perform the VNF configuration and chaining tasks. In addition to the OSS interface, the tenant SDN controller offers a set of dedicated northbound interfaces that allows slice's clients (and thus tenant's clients) to interact with the slice.

To provide trust relationships between the different actors (e.g. Infrastructure Providers, tenants, tenant's clients, etc.), each administrative domain may have its own security domain. This way, there may be one security domain for each Infrastructure Provider, one security domain for each tenant, and one (or more) security domain(s) for each slice. Since slice's clients may come from different organizations, the slice-specific management actions (resp. data) these organizations can perform (resp. access) may be potentially different. In such a situation, the definition of separate security domains in the slice is required to preserve security and privacy isolation between clients. The abstraction and isolation that the tenant SDN controller enables with its northbound interfaces helps to accomplish this.

In addition to performance, management, security and privacy isolation, this deployment enables recursion. Recursion is identified in ETSI GS NFV-IFA 009 [i.5] as one of the key features for network slicing. Recursion happens when some of the clients of a given tenant in turn can act as tenants as well. In such a case, they access the slices supplied by the tenant and use them to deploy and operate their own slices, customized to satisfy the service demands from their own clients. The recursion principle enables these two business actors (i.e. tenant and its clients) to participate in a multi-layered vertical pattern, where a client at one layer acts as a tenant at the layer immediately above. When the recursion principle is applied, a slice may recursively support new slices at higher layers.

5 Use cases analysis

5.1 Introduction

Clauses 5.2 to 5.8 introduce network slicing use cases derived from ETSI GR NFV 001 [i.1] and 3GPP and analyse these use cases to figure out potential impacts on security and reliability. Also, the relation to NFV constructs and potential impact to the NFV architectural framework are described.

5.2 Use case 1: Single operator domain network slice

5.2.1 Description

In ETSI GR NFV 001 [i.1], the concept of single operator domain network slicing is referred to as logical instantiation of the network between a set of network devices and some back end applications to deliver services for users or a set of users.

Defining a new network slice is primarily configuring a new set of policies, access control, monitoring/SLA rules, usage/charging consolidation rules and maybe new management/orchestration entity, when network is deployed with a given set of resources. Otherwise, new resources that have not been defined in the blueprint need to be deployed, and their lifecycle process needs to be developed.

It is assumed that each network slice can have its own network slice manager for automation, closed loop monitoring, and self-healing of services.

5.2.2 Security implication

New reference point(s) may be required from one or more NFV entity to the network slicing management function(s) in order to satisfy business, contractual, and operational security requirements of network slices.

Maintaining the desired level of security, including access control and policy (tenancy, geo-fence, etc.), of the reference point(s) between the network slicing management function(s) and the functional block(s) of the NFV framework may be a joint responsibility.

The required grade of entity-level and end-to-end security may be determined by the application/service-specific characteristics of the network slices.

5.2.3 Reliability implication

The network slicing management functions(s) is (are) responsible for satisfying business, contractual, and operational reliability requirements of network slices. These requirements need to be sent reliably and accurately to the entity (OSS/BSS and/or NFV-MANO) of the NFV framework with which the network slicing management function(s) is (are) interacting. The following remains open for further studies:

- Whether existing reference point(s) and/or interfaces can be effectively utilized for communications between network slicing management function(s) and NFV framework.
- Whether the parameters received from the network slicing management function(s) can be appropriately interpreted and acted upon by the NFV framework for supporting the desired level of reliability.

5.2.4 Relation to NFV constructs

A single operator domain network slice may, but need not, span multiple NFV sites within the same operator's administrative domain. Each NFV site may have its own NFVO, OSS/BSS, VIM, VNFM, etc. functionality in order to allow provisioning and management of network slices that use physical, virtual and hybrid (i.e. a combination of physical and virtual) resources from that site. However, there are scenarios where the NFVO and OSS/BSS functions may span multiple NFV sites within the same operator's administrative domain.

As discussed in the previous clauses, network slicing involves instantiation of the network between a set of network devices and some back end applications to deliver services for users or a set of users.

These instances of network slices may include physical and virtual resources, PNF(s) and VNF(s), and application/service-specific connectivity. The following may also be needed for network slices and their lifecycle management: configuring policies, access control, monitoring/SLA rules, and usage/charging consolidation rules.

The tasks of configuring, deploying, managing and scaling of VNF-based components of network slices can be performed by the NFV-MANO. In this context, the management of service quality of network slices can be achieved by using the relevant NSDs along with VNFDs via affinity/anti-affinity rules and deployment flavours of VNFs.

5.2.5 Potential impact to the NFV architectural framework

As mentioned in the previous clause, in order to fulfil the tasks of network slice instantiation and maintenance within a single operators' administrative domain, additional functionalities may be required to support configuring policies, access control, monitoring/SLA rules, and usage/charging consolidation rules.

These functionalities may be consolidated in an entity external to the NFV architectural framework. This entity may be called the Network Slice Manager (NSM), and it is involved, among others, with the following tasks:

- Determining the requirements for NSIs from the description of applications and services.

- Management of blueprint, catalogue, and lifecycle of network slices.

The NSM functional block determines, by translating or mapping or both, as appropriate, the network slices features into appropriate NSDs and VNFDs. The network slices' features are based on the requests from applications and services.

One or more new NSDs may need to be created, if translation and/or mapping cannot be done directly or any of the existing NSDs cannot satisfy the requested features of the network slices.

An NSM may need to maintain its own network slice catalogue, network slice Blueprint, and sub-network blueprint, and NSIs and NSSIs.

NOTE: The present document does not document any specific mapping/integration between NSM and the network slicing management functions that are for instance studied in 3GPP TR 28.801 [i.21].

5.3 Use case 2: Network Slice Instance creation

5.3.1 Description

This use case is derived from clause 5.1.1.1 of 3GPP TR 28.801 [i.21], when the operator decides to create a NSI.

5.3.2 Security implication

The allocated resources during NSI creation should be isolated. Also, the network slice management operations should be isolated.

5.3.3 Reliability implication

Table 7.2.2-1 of 3GPP TS 22.261 [i.20] shows low latency and high reliability 5G service scenarios and their performance requirements with an availability and reliability level varying from low to very high (i.e. from three nines to six nights). It further describes the following requirements related to availability and reliability for network slices:

- "*The 5G system shall enable the network operator to define a priority order between different network slices in case multiple network slices compete for resources on the same network.*"

- "*The 5G system shall support means by which the operator can differentiate policy control, functionality and performance provided in different network slices.*"

Those requirements imply that:

- The ability to differentiate network slices through their availability and reliability.

- The ability for the network operator to define a priority for a network slice in case of scarce resource situations (e.g. disaster recovery).

Both NGMN [i.14] **and 3GPP TR 28.801** [**i.21**] **require that** a NSI should be created by using the network slice template (NST) and certain network specific characteristics information including the reliability and priority requirements for physical and logical resources.

The reliability implications for network slice creation according to 3GPP requirements are:

- Availability, reliability, priority requirements of a network slice defined by the operators should be included into constraints for NSI creation.

- Network slice creation should enable mechanisms to support different NSIs in terms of availability, reliability and priority required by the operators.

- A created network slice should be able to adapt to changes of availability, reliability, priority requirements of this network slice.

The availability and reliability of a NSI do not depend only on the availability and reliability properties of the physical and logical resources assigned during NSI instantiation, but also on run-time operations, e.g. maintaining the assigned resources to fulfil the availability and reliability requirements during the NSI lifecycle whenever accidental or intentional anomalies occur. Also, reliability of a NSI depends on the topology of the interconnections between the assigned resources.

Since there are some gaps (see below) in current NFV specifications identified in ETSI GR NFV-REL 007 [i.11], additional NFV specifications might be needed for NS instantiation for use in the creation of a NSI:

- Support of service availability levels.
- Support of priority handling for virtual resource assignment.
- Service continuity during restoration following a failure, scaling and software (VNF, MANO, NFVI) modification.

5.3.4 Relation to NFV constructs

The NF contained in the NSI defined in 3GPP SA5 can be either a VNF or a PNF. The resources of the VNFs are managed by the NFV-MANO system. The relation to NFV constructs is analysed below:

- Whenever a VNF is in use, deployment and management of the associated virtualised resources is supported by the NFV-MANO system, including any scale operation associated with reconfigurations. About VNF management, keeping in mind that a VNF is composed by virtualized resources and a network application; according to SA5 definition, MANO takes care of the management of the virtualised resources and the 3GPP management system takes care of the 3GPP network application installed on them.
- The QoS and availability requirements for resources supporting a network slice will be dealt by including appropriate information in the NSD, and the corresponding VNFDs of the relevant VNFs (e.g. affinity and anti-affinity rules, virtual link quality of service, etc.) and/or by selecting appropriate deployment flavours at instantiation time.

5.3.5 Potential impact to the NFV architectural framework

No specific impact to the NFV architectural framework is identified other than described in clause 5.2.5.

5.4 Use case 3: Network Slice Subnet Instance creation

5.4.1 Description

This use case is derived from clause 5.2.1.1 of 3GPP TR 28.801 [i.21]: the NSSI is created by the Network Slice Subnet Management Function (NSSMF), according to the creation request received from the Network Slice Management Function (NSMF).

The concept of NSSI is further explained within clause 4.3 of 3GPP TR 28.801 [i.21]. The concept of NSSMF is further explained within clause 4.10 of 3GPP TR 28.801 [i.21].

5.4.2 Security implication

The allocated resources during NSSI creation should be isolated. Also, the network slice management operations should be isolated.

5.4.3 Reliability implication

The availability and reliability of a NSSI do not depend only on the availability and reliability properties of the physical and logical resources assigned during NSSI instantiation, but also on run-time operations, e.g. maintaining the assigned resources to fulfil the availability and reliability requirements during the NSI lifecycle whenever accidental or intentional anomalies occur. Also, reliability of a NSSI depends on the topology of the interconnections between the assigned resources.

5.4.4 Relation to NFV constructs

The NSSMF determines which network functions (NF) and resources are needed, where the NFs defined in 3GPP SA5 can be either a VNF or a PNF. The relation to NFV constructs is analysed below:

- As indicated by "The NSSMF creates and configures the NSSI constituent parts which may include both virtualised and non-virtualised NFs", when the NSSI constituent parts include VNFs, the resources of these VNFs are provided and supported by the NFV-MANO system and grouped into one (or more) NS(s) in the NFV context.

5.4.5 Potential impact to the NFV architectural framework

No specific impact to the NFV architectural framework is identified other than described in clause 5.2.5.

5.5 Use case 4: Network Slice Instance creation, configuration and activation with VNFs

5.5.1 Description

This use case is derived from clause 5.1.1.9 of 3GPP TR 28.801 [i.21], when VNFs are included during the process of NSI creation, configuration and activation.

5.5.2 Security implication

No specific security implication is identified.

5.5.3 Reliability implication

No specific reliability implication is identified other than described in clause 5.3.3.

5.5.4 Relation to NFV constructs

As described by the use case, the NSSMF configures and triggers the components of NFV-MANO to instantiate and/or configure all needed VNFs and NSs, when VNFs are included in a NSSI to compose an NSI. The components of NFV-MANO are interacting with the NSSMF, and NSSIs are composed with NSs.

5.5.5 Potential impact to the NFV architectural framework

No specific impact to the NFV architectural framework is identified other than described in clause 5.2.5.

5.6 Use case 5: Priority of NSI for re-allocating the limited resources

5.6.1 Description

This use case is derived from clause 5.1.11.1 of 3GPP TR 28.801 [i.21]. The NSIs are assigned different priorities according to different service requirements, leading the network slice management system to re-allocate the resources to high priority NSIs in case of resource shortage.

The NSM provides to NFV-MANO the policies required to be applied to the NS at instantiation time, including priority of the resources to be allocated to the NS instance. The NFV-MANO system acts as per policies in case of resources shortage, in order to properly allocate resources to the NS instances according to their assigned priority. Examples of such actions may be to terminate and/or change the resources of a NSIs with lower priority and to increase the available resources for the NSIs with higher priority.

5.6.2 Security implication

Some resources of the NSIs are isolated for security reasons, thus these resources should not be re-allocated. The network slice management system is expected to check the resource type, as well as one or more resource related security policies before re-allocating a resource.

5.6.3 Reliability implication

The reliability requirements and policies associated with a NSI are provided by the NSM and NFV-MANO should apply them throughout the lifecycle management of the NS instance.

If the network provider has enabled policies for prioritizing network slices or services supported by network slices, NFV-MANO, which manages resources used by those network slices, should provide the capability to apply the associated priority during resource assignment to network slices, recovery of resource failures in network slices, etc.

In case of scarce resources (e.g. a disaster) during the lifecycle of NS instance, the reliability of the NSI is affected if the NSI resources are partly, or totally, revoked.

5.6.4 Relation to NFV constructs

If the resources of the NSI (or part of them) are managed by the NFV-MANO, then the NFV-MANO system should provide the lifecycle management functionalities requested by the network slice management system, according to the received policies from the NSM, including priority handling. For instance, as part of the priority enforcement, the VNF instances, NS instances, or virtualised resources could be terminated or scaled down/in according to the policies provided by the NSM.

The NFV-MANO system should apply the associated reliability requirements and policies for the NSI resources that are managed by NFV-MANO.

5.6.5 Potential impact to the NFV architectural framework

There is no current support in the lifecycle management of NS instances and VNF instances for the handling of requirements on resources prioritization for the NSI. The NFV architectural framework needs to be enhanced to support reception and handling of the policies received from NSM, including resource prioritization.

Specific reliability requirements associated with the NSI should also be supported by the NFV-MANO system interfaces (e.g. communicating reliability requirements to VIM) for the lifecycle management of NSs.

5.7 Use case 6: Network Slice as a Service

5.7.1 Description

An operator proposes to service providers to build specific network slices for carrying the services of these service providers with a guaranteed QoS. This is a Network Slice as a Service functionality proposed by the operator as described in clause 4.9.2 of 3GPP TR 28.801 [i.21]. This use case is further described in clause 5.1.6.3 of 3GPP TR 28.801 [i.21].

5.7.2 Security implication

5.7.2.0 Introduction

The operator proposing a Network Slice as a Service to its customer needs to provide a network slice isolated from the other slices. The concept of isolation is described in section 1.1 of [i.15]. For some very sensitive services (e.g. mission critical services), the slice isolation is even reinforced.

A threat analysis is provided in [i.15]. The following sub-clauses detail additional security implications at the NS level and at the VNF level.

5.7.2.1 Network service level

A network slice is a graph of network functions (VNF, PNF) connected together to build an end-to-end network service with specific requirements and capabilities.

Several network functions may be common to different slices.

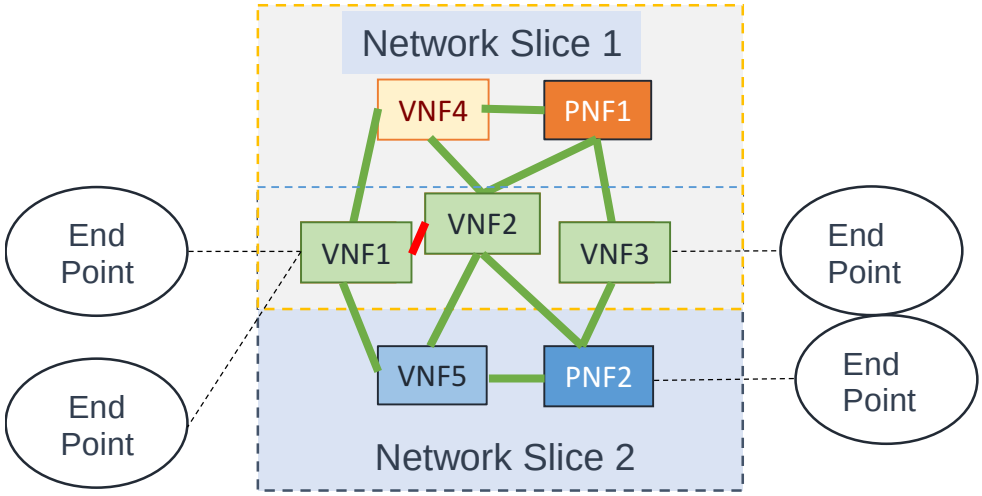

Figure 5.7.2.1-1: Network slices with common VNFs

Figure 5.7.2.1-1 shows two network slices using common functions: VNF1, VNF2 and VNF3. VNF4 and PNF1 are the dedicated network functions of the network slice 1. VNF5 and PNF2 are the dedicated network functions of the network slice 2.

Network slice isolation implies that all processes and data handled by the network slice 1 are not shared with the network slice 2. To achieve this goal, a specific care is made on the common VNFs. In these VNFs, the data flow coming from the network slice 1components is not mixed with the data flow issued from the network slice 2 components. A specific design of these VNFs and/or instantiation of these VNFs ensure this separation. For these VNFs, some security recommendations are given in clause 6.2.1.

5.7.2.2 VNF level

For some virtual functions embedding security functions, the isolation at the virtualisation container could be not sufficient.

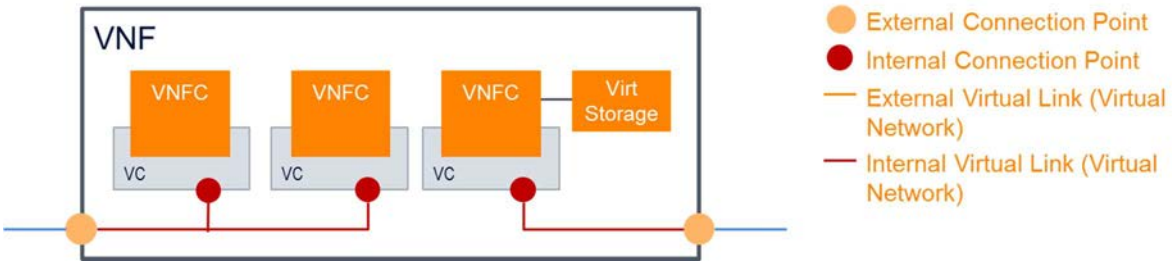

Figure 5.7.2.2-1: Virtual Network Function implemented with several components

Figure 5.7.2.2-1 shows a Virtual Network Function. The VNF Instance uses virtualised resources (e.g. compute, networking and storage). The VNF Instance is composed of VNF Components (VNFCs) that are instantiated on Virtualisation Containers (VC), e.g. in the form of Virtual Machines. The VNFC could use also optional virtual storage, which will imply further requirements on storage isolation. Each VNFC executes a part of the VNF application software. The internal connection of VNFCs in the VNF Instance is done through internal Virtual Links. The VNF Instance provides external connection points that enable the connection of the VNF to other VNFs or PNFs in the network slice.

There could be in a VNF some critical parts that need strong security and for which a strict isolation is needed. For these components, an instantiation in Hardware-Mediated Execution Enclave (HMEE), as described in ETSI GS NFV-SEC 009 [i.12], i.e. protection by hardware isolation, could be necessary.

A VNF with security requirements fulfilled with HMEE is shown below.

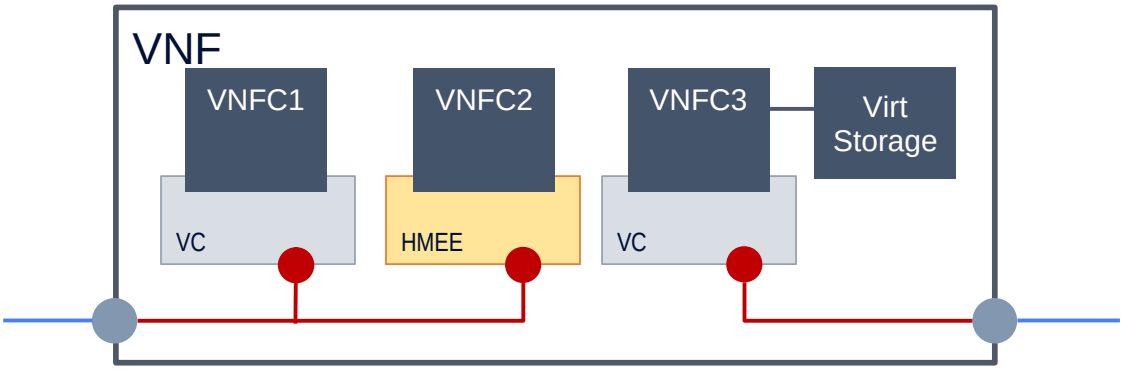

Figure 5.7.2.2-2: Virtual Network Function with critical component deployed in secure enclave

Figure 5.7.2.2-2 shows a VNF using a critical part implemented in VNFC2 for which the processing and the data are completely isolated from the other VNFCs. For this matter, the VNFC2 is deployed in a HMEE and its internal connection points correspond to the entry point and output point of the HMEE.

There could be a need to put the entire VNF in the HMEE. In this case, different possibilities are represented in figures 5.7.2.2-3 and 5.7.2.2-4.

First case:

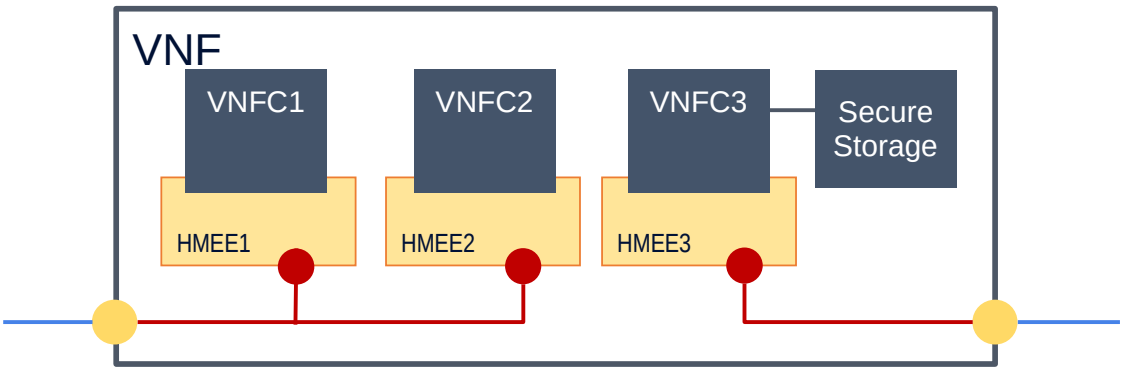

Figure 5.7.2.2-3: Virtual Network Function deployed in several HMEEs

Figure 5.7.2.2-3 shows a VNF for which there is a separation of the processes into several HMEEs. Processes and data of VNFC1 are totally isolated from those of VNFC2 and VNFC3. In this case, the virtual links connecting the VNFCs are not part of the HMEE.

Second case:

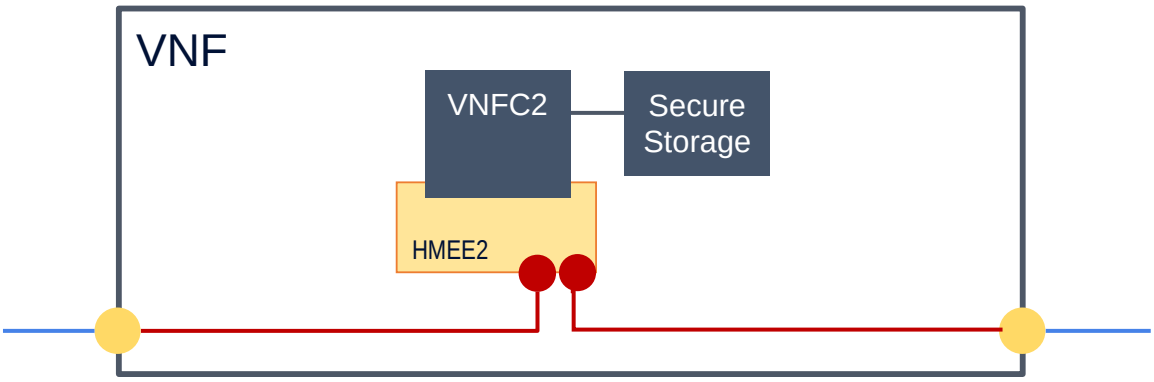

Figure 5.7.2.2-4: Virtual Network Function deployed in a HMEE

In this case, the entire VNF is designed as a single component deployed in a HMEE: the entire VNF is thus protected.

These different requirements on the VNF design and deployment result in some recommendations for the system and NFVI which are given in clause 6.2.2.

5.7.3 Reliability implication

No specific reliability implication is identified.

5.7.4 Relation to NFV constructs

As described in clause 5.1.6.3 of 3GPP TR 28.801 [i.21], the customer inputs a set of service requirements (e.g. business scenario, isolation, throughput, latency, coverage, etc.) to the operator. The network operator provides a customized network slice as a service which can serve the customer's requirements and signs an SLA with the customer.

To ensure this Network Slice as a Service's SLA, the network operator describes the service requirements in the descriptor of the network slice, which in turn could be mapped into the descriptor of a network service (NSD). The NS will be instantiated using the VNFs for which the descriptor (VNFD) requirements are fulfilled: these requirements could be, e.g. business scenario, isolation, throughput, latency, and coverage. But the requirements are not limited to this list.

It is assumed that the network slice resource requirements can be mapped to the NSD and/or VNFD.

5.7.5 Potential impact to the NFV architectural framework

This use case can lead to a requirement for NFV-MANO to manage a significantly higher number of network service instances than for more conventional use cases described in ETSI GS NFV 001 [i.1].

As described in clause 5.1.6.3 of 3GPP TR 28.801 [i.21], after activating the NSI, the network slice management system will expose part of the service-related performance data to the customer. If current performance cannot meet the SLA, some actions (e.g. scale in/out, modification, etc.) are executed to guarantee the NSI performance.

The network slice management system (which resides outside of the NFV architectural framework) includes a monitoring entity able to interpret the requirements described in the network slice descriptor (see clause 5.7.4), and interacts with the NFVO of the NFV-MANO to ensure corrective actions on resource management and guarantee the end-to-end performance. This monitoring entity interacts with the NFV-MANO to request resource-related performance data to be able to expose performance report to the network operator and /or customer of the network operator.

This performance monitoring requirement results in some recommendations for the system that are given in clause 6.1.1.

5.8 Use case 7: Network Slice Instance across multiple operators

5.8.1 Description

This use case is derived from clause 5.1.8.2 of 3GPP TR 28.801 [i.21]. Under the condition of non-management pre-requisites, such as trust and legal issues, the NSI is created across multiple operators, where each operator decomposes the service request of the NSI and provides its own NSSI to compose the NSI. One operator may provide its management data to the other operator when requested.

5.8.2 Security implication

As the sending of management data for NSSI from one operator to another operator is completed at the 3GPP, no specific security requirements for this use case is needed from the NFV-MANO perspective.

5.8.3 Reliability implication

As the service request of the NSI is decomposed for each operator, if the resource management of the NSSI is supported by the NFV-MANO system, the reliability of each NFV-MANO system is independent.

5.8.4 Relation to NFV constructs

No specific relation to NFV constructs is identified.

5.8.5 Potential impact to the NFV architectural framework

No specific impact to the NFV architectural framework is identified other than described in clause 5.2.5.

6 Support of network slicing

6.1 Recommendation: Architectural framework

6.1.0 Introduction

This clause provides recommendations in term of potential NFV-MANO evolutions resulting from the analysis performed for the use cases described in clause 5. Recommendations encompass the identification of potential new requirements, i.e. to describe that a requirement is needed to cover certain aspect or required functionality. Recommendations are categorized and elaborated as follows:

- Reference points and/or interfaces (clause 6.1.1)
- Functional (clause 6.1.2)
- Descriptors (clause 6.1.3)

6.1.1 Reference points and/or interfaces

- It is recommended that the reference point or interface between the Network Slice Management and the NFV architectural framework allows the network slice management to specify the necessary information contained in, or derived from, the network slice descriptor implementing the Network Slice requirements.
- It is recommended that the reference point or interface between a monitoring entity in the Network Slice Management and the NFV architectural framework allows the monitoring entity to collect necessary information and the network slice management to request corrective resource management actions to guarantee the performance described in the network slice descriptor.

- It is recommended that the reference point or interface between the NFV architectural framework and the Network Slice Management exposes to NSM the capabilities to provide the required NSI policies such as the priority to be applied to a NS instance.

- It is recommended that the reference point or interface between a monitoring entity in the Network Slice Management and the NFV architectural framework allows the monitoring entity to request resource performance data, including data related to the policies such as the priority requested for a NS instance, that will be exposed in a report to the network operator and /or customer of the network operator.

- It is recommended that the reference point or interface between NFV-MANO and the Network Slice Management entity enables the Network Slice Management entity to register to NFV-MANO the performance data to monitor and needed in order for the monitoring entity in the Network Slice Management entity to detect divergence against the requirements of the network slice and expose part of the service-related performance data to the customer.

- It is recommended that the reference point or interface between NFV-MANO and the Network Slice Management entity enables NFV-MANO to provide the performance data to the monitoring entity in the Network Slice Management entity for the monitoring entity in the OSS/BSS to detect a divergence against the requirements of the network slice.

- It is recommended that the reference point or interface between the Network Slice Management entity and NFV-MANO enables the Network Slice Management entity to launch the appropriate actions (e.g. scale in/out, modification, etc.) to comply with the network slice requirements when a divergence is detected.

6.1.2 Functional

- It is recommended that the prioritization of virtualised resource management is supported.

- It is recommended that a mechanism between the NFV-MANO and the Network Slice Management entity is specified to exchange with the NFV-MANO the requirements for the NS supporting the network slice.

- It is recommended that the NFV-MANO architecture be evaluated with regard to its ability to support the management of a high number of network service instances (e.g. for support the network slice as a service use case). These network service instances may span over multiple sites and multiple administrative domains.

6.1.3 Descriptors

- It is recommended that the NSD and VNFD enable conveying resource requirements derived from the network slice descriptor resource requirements.

6.2 Recommendation: Security

6.2.0 Introduction

This clause provides recommendations in term of security resulting from the analysis performed for the use cases in clause 5.

The requirements in ETSI GS NFV-SEC 012 [i.13] apply for the Network Slice as a Service use case. Security recommendations are collected in [i.15] and also apply to this use case. The following are additional recommendations for isolation at the hypervisor and OS level.

6.2.1 Network service level

As described in clause 5.6.2, the following recommendations could be made:

- It is recommended that some particular resources of the NSI are not re-allocated in case those resources are isolated for security reasons.

As described in clause 5.7.2.1, when network functions are shared between different network slices, a specific design of these VNFs and/or instantiation of these VNFs are needed to ensure the separation and isolation of network slices. For these VNFs, the following recommendations could be made:

- It is recommended to add the requirement for instantiating the VNF separately for each slice on the virtualised infrastructure, when a VNF package is used for several slices and isolation by slice is required, unless this VNF supports processes and data isolation by slice.
- It is recommended to add the requirement to use a virtualised infrastructure that ensures a separation of processes and data for the VMs used by each VNF instance.
- It is recommended to add the requirement for enabling NFV-MANO to authenticate the platform and to verify the capabilities, integrity and trustworthiness of the platform prior to the instantiation of the component of the network service.
- It is recommended to add the requirement for using PNFs physically duplicated for each slice where a PNF is used and isolation by slice is required, unless this PNF supports processes and data isolation by slice.
- It is recommended to add the requirement that the virtual link connecting the VNFs is dedicated for each slice and logically isolated even if this virtual link connects two common VNFs.

6.2.2 VNF level

As described in clause 5.7.2.2, VNF could be deployed in the NFVI using one or more HMEEs depending on the critical property of the VNF. This results in several recommendations for the system and NFVI:

- It is recommended to add the requirement for having the possibility in the NFVI to deploy one or more components of a VNF in one or more HMEEs.
- It is recommended to extend the VNFD of the VNF to add the possibility to describe the deployment of components in one or more HMEEs.
- It is recommended to add the requirement of having the possibility for a connection point of a VNFC component to be described as an entry point or output point of a HMEE.
- It is recommended to add the requirement for having the possibility for an external connection point of a VNF to be described as an entry point or output point of a HMEE.
- It is recommended to define a generic framework for the description of VNF and connection points independently of any specific underlying processor and associated HMEE technology.

6.3 Recommendation: Reliability

This clause provides recommendations in term of reliability resulting from the analysis performed for the use cases in clause 5:

- It is recommended that the parameters received from the Network Slice Management Function or the Network Subnet Slice Management Function are appropriately interpreted and acted upon by the NFV architectural framework for supporting the desired level of reliability.
- It is recommended that the NS instantiation occurs in the creation of a NSI.
- It is recommended that the NFV architectural framework applies the reliability requirements and policies associated with a NSI throughout the lifecycle management of the NS instance.

6.4 Relation with ETSI ISG NFV group specifications

Table 6.4-1 provides relation between recommendations analysed in clause 6.1 to 6.3 and ETSI ISG NFV group specifications which might need to be changed concerning the NFV architectural framework, including its security and reliability requirements, to support network slicing capabilities.

Table 6.4-1: Relation with ETSI ISG NFV group specifications

Target deliverable	Recommendation	Type	Reference
ETSI GS NFV-IFA 005 [i.23], ETSI GS NFV-IFA 006 [i.24], ETSI GS NFV-IFA 012 [i.26], ETSI GS NFV-IFA 013 [i.6]	Study whether new parameters are required to realize network slicing capabilities such as: • Determining the requirements on the lifecycle of the Network Service used as part of a network slice • Determining the requirements for the lifecycle of the Network Service used as part of a Network Slice Subnet • Determining and propagating the resource requirements for Network Service instances and VNF/C instances that are used in a Network Slice instance or Network Slice subnet instance (e.g. Communicating resource prioritization related data) • Determining the policy handling requirements for Network Service instances such as prioritization • Determining the requirements for Application and Service Management Interface and Information Model specifications • Determining the requirements for performance and fault data handling	Parameter	Clause 6.1.1 in the present document
ETSI GS NFV-IFA 010 [i.27]	Functional requirement to support network slicing which includes: Prioritization of virtualised resource management Support of multi-tenancy Support of Network Services over multi-site/multi NFVI-PoPs Study whether the NFV-MANO architecture scalability is sufficient to enable managing a high number of network service instances.	Function	Clause 4.3, 5.2.4, 6.1.2 in the present document
ETSI GS NFV-IFA 011 [i.28], ETSI GS NFV-IFA 014 [i.7]	Study whether new parameters are required in the NSD and VNFD to allow support of the network slice and network slice subnet.	Parameter	Clause 6.1.3 in the present document
SEC	Security requirement to realize the following features: • Resource isolation for security reasons and allocation policy: – At Network Service level – At VNF level – At NFVI level • Isolation of Network Service management for multiple tenants	Requirement	Clause 6.2 in the present document
REL	Reliability requirement to realize the following features: • Network Service instantiation used in the creation of a network slice instance, or in the network slice subnet instance • Maintaining the reliability of Network Services supporting the network slice instance during and after resource changes • Applying the reliability requirements and policies associated with network slice instances throughout the lifecycle management of the Network Service instances	Requirement	Clause 6.3 in the present document

7 Conclusion

The objective of the present document is to figure out a gap between the current NFV specifications and the requirements to be fulfilled by an NFV system to support network slicing use cases described by external organizations. The present document analyses a set of use cases and provides a set of recommendations on the evolution of NFV specifications to enable supporting the network slicing feature.

The set of recommendations identified in clause 6 indicates the need to perform additional normative specification work to address the network slicing feature. The aspects that require further specification work are:

- Recommendations related to reference points and/or interfaces aspects (refer to clause 6.1.1).
- Recommendations related to functional aspects (refer to clause 6.1.2).
- Recommendation related to descriptor aspects (refer to clause 6.1.3).
- Recommendations related to security aspects (refer to clause 6.2).
- Recommendations related to reliability aspects (refer to clause 6.3).

Annex A:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Tetsuya Nakamura, CableLabs

Other contributors:
Amanda Xiang, Huawei

Anatoly Andrianov, Nokia

Anne-Marie Praden, Gemalto

Baoguo Xie, ZTE

Bhumip Khasnabish, ZTE

Bruno Chatras, Orange

Cecilia Corbi, Telecom Italia

Chidung Lac, Orange

Cristina Badulescu, Ericsson

Diego Lopez, Telefonica

Dong Chen, ZTE

Fabrizio Moggio, Telecom Italia

Hui Deng, Huawei

Jesús Folgueira, Telefonica

Jinguo Zhu, ZTE

Jinhua Wu, ZTE

Joan Triay, DOCOMO Communications Labs.

Jordi Pérez-Romero, DAC-UPC

José A. Ordóñez, University of Granada

Juan J. Ramos, University of Granada

Juan M. López-Soler, University of Granada

Junyi Jiang, Huawei

Lei Zhu, Huawei

Liping Chen, ZTE

Pablo Ameigeiras, University of Granada

Olivier Le Grand, Orange

Oriol Sallent, DAC-UPC

Ramon Ferrús, DAC-UPC

Shaoji Ni, Huawei

Sibylle Schaller, NEC

Ulrich Kleber, Huawei

Zarrar Yousaf, NEC

Annex B:
Change History

Date	Version	Information about changes
March, 2017	0.0.1	ToC added
April, 2017	0.0.2	Editor's notes and clause 4.2.1 added
May, 2017	0.0.3	Clause 2.2 added and clause 4.2.1 revised
	0.0.4	Clause 2.2, clause 4.2.2, clause 5.2, clause 5.3, and clause 5.4 added
June, 2017	0.0.5	Clause 5.3 revised and clause 5.5 added
July, 2017	0.0.6	Clause 4.2.1 revised and clause 4.2.3, 4.3.1, 5.2.4 and 5.6 added
	0.0.7	Clause 5.2.5, 5.7 and 6.1 added
	0.0.8	Clause 5.8 added
	0.0.9	Clause 2.2 revised and clause 4.2.4 added
August, 2017	0.0.10	Clause 2.2 revised and clause 4.3.2, 5.2.2, and 5.3.3 added
September, 2017	0.0.11	Clause 5.6 and 6.1.1 revised and clause 5.2.3 added and clause 4 re-structured
	0.0.12	Clause 2.2 and 5.6 revised and clause 5.7 and 6.2 added and clause 4.3 added
	0.1.0	Clause 3.2, 4.2.3, 5.7.5, 6.1, 6.2 revised and Clause 6.3, 6.4, 7 added and status changed to stable
October, 2017	0.1.1	Clause 2.2 revised and clause 4.3 added
	0.1.2	Clause 4.2.3, 5.2.5, and 5.3.4 revised
November, 2017	0.1.3	Clause 5.3, 5.4, 5.5, 5.7, and 6.4 revised and editorial correction
December, 2017	3.1.1	Clause 4, 5.2, 5.3, 6.1, and 6.4 revised and editorial correction, and publish the document

History

Document history		
V3.1.1	December 2017	Publication