ETSI GS NFV 004 V1.1.1 (2013-10)

Network Functions Virtualisation (NFV); Virtualisation Requirements

Disclaimer

This 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
DGS/NFV-0012

Keywords
NFV, requirements

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

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 (http://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.

Foreword

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

1 Scope

The present document specifies the requirements that Telecommunications operations put on Network Functions Virtualisation in order to consolidate network equipment, belonging to fixed and mobile networks, onto industry standard high volume servers, switches and storage, which could be located in N-PoPs, Network Nodes and in end user premises.

The present document addresses the requirements in the following areas:

- Portability/Interoperability
- Performance
- Management and Orchestration
- Elasticity
- Security
- Resiliency
- Network Stability
- Service Continuity
- Operations
- Energy Efficiency
- Migration and co-existence with existing platforms

2 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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[2] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

2.2 Informative references

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] NFV White paper: "Network Functions Virtualisation, An Introduction, Benefits, Enablers, Challenges & Call for Action. Issue 1".

[i.2] IEEE 1588-2008: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in GS NFV 003 [2] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
BSS	Business Support System
CMS	Cloud Management System
CPE	Customer Premises Equipment
IMS	IP Multimedia Subsystem
NF	Network Function
NFV	Network Functions Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NIC	Network Interface Card
NID	Network Interface Device
NOC	Network Operations Centre
N-PoP	Network Point of Presence
OSS	Operations Support System
PNF	Physical Network Function
SLA	Service Level Agreement
SPoF	Single Point of Failure
SW	Software
VM	Virtual Machine
VNF	Virtual Network Function
VNPaaS	Virtual Network Platform as a Service

4 General Description

4.1 Introduction

Virtualisation aims to transform the way that network operators architect networks by evolving existing IT virtualisation technology and making use of cloud computing techniques in order to consolidate network equipment onto industry standard high volume servers, switches and storage, which could be located in N-PoPs, Network Nodes and in the end user premises.

Virtualisation involves the implementation of network functions in software that can run on a range of industry standard hardware, enabling ubiquitous, convenient and on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

4.2 Objectives

Virtualisation brings specific benefits on efficient resource usage, resiliency and redundancy, as well as faster management of operations (e.g. SW upgrades) and enhanced time to market (e.g. to deploy new functionality less hardware dependant). However, the specific nature of the Telco environment (i.e. carrier grade requirements) imply technical challenges that the present document aims to address in order to facilitate interoperability and seamless evolution towards fully virtualised networks.

The present document addresses the requirements to facilitate the assignment of infrastructure resources to virtual network functions. Specific NFV requirements will focus primarily on the differences introduced by the Network Functions Virtualisation (NFV) process, and not on aspects of the Network Functions (NF) interfaces, protocols and management that are identical whether the implementation is physical or virtual.

5 High level requirements

5.1 General

[**Gen.1**] The NFV framework shall be able to permit Service Providers/Network Operators to *partially* or *fully* virtualise the network functions needed to create, deploy and operate the services they provide.

NOTE: Partial refers to virtualisation of a specific set of functions (e.g. based on similar characteristics) within a network system/subsystem, and used for creation of certain service. For example, virtuali sation of network functions in the control plane but not the ones in the data plane.

[**Gen.2**] In case of partial virtualisation, any impact on the performance or operation of non-virtualised network functions shall be manageable, predictable, and within the acceptable limits.

[**Gen.3**] In case of partial virtualisation, there shall be manageable impact on the legacy management systems of the network functions that have not been virtualised.

[**Gen.4**] The NFV framework shall be able to support a network service composed of Physical Network Functions (PNFs) and Virtual Network Functions (NFs) as a VNF Forwarding Graph implemented across N-PoP multivendor environments that may be instantiated in a single operator or in cooperating inter-operator environments. The following areas are in or out of scope:

Scenario/NF Composition	All Physical NFs	Physical/Virtual NFs	All Virtual NFs
Intra-Operator	Out-of-Scope	In-Scope	In-Scope
Inter-Operator Cooperation	Out-of-Scope	In-Scope	In-Scope

5.2 Portability

[**Port.1**] The NFV framework shall be able to provide the capability to load, execute and move Virtualised Network Functions (VNFs) across different but standard N-PoP multivendor environments.

[**Port.2**] The NFV framework shall support an interface to decouple VNF associated software instances from the underlying infrastructure.

[**Port.3**] The NFV framework shall be able to provide the capability to optimize the location, reservation and allocation of the required resources of the Virtualised Network Functions (VNFs).

NOTE: The portability requirements expose gaps such as binary compatibility, integration/interworking and meeting SLA requirements during porting that the industry needs to resolve. To move the industry forward in resolving these gaps, portability can be achieved through phases. For example, a first step could be de-coupling of software instances from the hardware enabling porting VNFs on other instances of the same architectural type and drive performance to meet various SLAs.

The NFV target is to achieve portability across multi-vendors, hypervisors, hardware and meet SLA requirements.

Reference is made to the technical challenges clause on Portability/Interoperability from [i.1].

5.3 Performance

[Per.1] The NFV framework shall be able to instantiate and configure any given VNF over the underlying infrastructure so that the behaviour of the resulting VNF instance in terms of performance is conforming to the requirements expressed in the VNF information model provided by the VNF vendor for such a type of infrastructure.

[Per.2] The NFV framework shall be able to describe the underlying infrastructure requirements of a VNF so that it can be sized for a given performance target while the corresponding resources are allocated and isolated/shared in the infrastructure accordingly.

[**Perf.3**] For any running VNF instance, the NFV framework shall be able to collect performance related information regarding the usage of compute, storage and networking resources by that VNF instance.

[**Perf.4**] The NFV framework shall be able to collect performance related information concerning the resource usage at the infrastructure level (e.g. hypervisor, NIC, virtual switch).

NOTE: VNF instance is a run-time copy of the VNF software, resulting from completing the deployment and instantiation of the VNF components and the connectivity between them, by using the VNF deployment and behaviour information model, as well as additional run-time instance-specific information and constraints.

5.4 Elasticity

The following requirements apply when a VNF or its components can be parallelised to realize elasticity:

[**Elas.1**] The VNF vendor shall describe in an information model for each component capable of parallel operation the minimum and maximum range of such instances it can support as well as additional information such as the required compute, packet throughput, storage, memory and cache requirements for each component.

[**Elas.2**] The NFV framework shall be able to provide the necessary mechanisms to allow virtualised network functions to be scaled with SLA requirements. Different mechanisms shall be supported: e.g. on-demand scaling, automatic scaling.

NOTE 1: On-demand scaling of a VNF instance may be initiated by the VNF instance itself, by another authorized entity (e.g. OSS), or by an authorized user (e.g. a NOC administrator). Automatic scaling of a VNF instance can be initiated based on some trigger, e.g. when pre-defined criteria included in the information model describing a VNF are met.

[**Elas.3**] The scaling request or automatic decision may be granted or denied depending on e.g. network-wide views, rules, policies, resource constraints or external inputs.

NOTE 2: The trigger for requesting scaling is out of the scope of the present document; e.g. how the virtual software function(s) detect a load situation. Decision criteria to grant or deny scaling requests are out of the scope of the present document.

[**Elas.4**] The VNF user, through standard information model, shall be capable of requesting, for each component capable of scaling, specific minimum and maximum limits within the range specified by the VNF vendor to fulfil individual SLA, regulatory or licensing constraints.

[**Elas.5**] The NFV framework shall provide the capability to move some or all VNF components from one compute resource onto a different compute resource while meeting the service continuity requirements for the VNF components.

NOTE 3: The timeframe required to move VNF components is dependent upon a number of factors, such as available network bandwidth and compute capacity.

NOTE 4: The movement of VNF components can be within a single administrative domain or between administrative domains.

5.5 Resiliency

[**Res.1**] The NFV framework shall be able to provide the necessary mechanisms to allow network functions to be recreated after a failure.

The relevant resiliency characteristics of a VNF or a set of VNFs shall be made available to the entities handling the network service they are involved in.

Different mechanisms shall be supported: on-demand re-creation, automatic re-creation.

NOTE 1: On-demand re-creation of a VNF instance can be initiated by another authorized entity (e.g. OSS), or by an authorized user (e.g. a NOC administrator). Automatic re-creation of a VNF instance may be initiated based on some trigger, e.g. when pre-defined criteria included in the information model describing a VNF are met.

[**Res.2**] The NFV framework shall be able to provide a means to classify (sets of) VNFs that have similar reliability/availability requirements into resiliency categories.

[**Res.3**] The NFV framework shall be able to support standard based replication of state data (synchronous and asynchronous) and preservation of data integrity with the necessary performance to fulfil the SLAs.

[**Res.4**] The NFV framework (including the orchestration and other functions necessary for service continuity) shall facilitate resiliency schemes in both the control plane and the data plane, in order to secure service availability and continuity. Orchestration functionalities and other functions necessary for managing service continuity shall not become a single point of failure (SPoF).

[**Res.5**] The SLA shall specify the "metrics" to define the value and variability of "stability".

[**Res.6**] In order to enable network stability, the NFV framework shall support mechanisms to measure the following metrics and ensure that they are met per SLA:

- Maximum non-intentional packet loss rate (e.g. packets lost due to oversubscription of the service network interconnects, not due to polices or filters).
- Maximum rate of non-intentional drops of stable calls or sessions (depending on the service).
- Maximum latency and delay variation on a per-flow basis.
- Maximum time to detect and recover from faults aligned with the service continuity requirements (zero impact or some measurable impact).
- Maximum failure rate of transactions that are valid and not made invalid by other transactions.

NOTE 2: Additional metrics necessary for defining network stability can be addressed during further phases of the NFV work.

Reference is made to the technical challenges clause on Security and Resiliency from [i.1] and Use Cases "Virtualisation of Mobile Core Network and IMS" and "Service Chains (VNF Forwarding Graphs)" from GS NFV 001 [1].

5.6 Security

[**Sec.1**] The NFV framework shall implement appropriate security countermeasures to address:

- security vulnerabilities introduced by the virtuali sation layer;
- protection of data stored on shared storage resources or transmitted via shared network resources;
- protection of new interfaces exposed by the interconnectivity among NFV end-to-end architectural components, e.g. hardware resources, VNFs, management systems;
- isolation of distinct VNF sets executing over the NFVI to ensure security and separation between these VNF sets;

- secure management of VNF sets by other third-party entities (e.g. VNPaaS, enterprise virtual CPE, and virtual consumer home gateways).

[**Sec.2**] The NFV framework shall be able to provide mechanisms for the network operator to control and verify the configuration of the elements that virtualise the hardware resource.

[**Sec.3**] Management and orchestration functionalities shall be able to use standard security mechanisms wherever applicable for authentication, authorization, encryption and validation.

[**Sec.4**] NFV Infrastructure shall be able to use standard security mechanisms wherever applicable for authentication, authorization, encryption and validation.

NOTE 1: Detailed requirements on security of shared storage (e.g. mirroring, backups) are to be addressed during further phases of the NFV work.

[**Sec.5**] The NFV framework shall be able to provide role-based information access control and rights management.

NOTE 2: Each actor, based on its associated role definition, will have access to a subset of the VNF instances and a subset of the VNF instances management functions (e.g. creation, modification, activation…). A special role will be the administrator role that is able to manage roles and rights.

[**Sec.6**] Access to NFV functions via NFV exposed APIs at all layers shall be protected using standard security mechanisms appropriate for that layer, wherever applicable for authentication, authorization, data encryption, data confidentiality and data integrity.

[**Sec.7**] The management and orchestration functionality shall provide at least two levels of privileges to API clients (e.g. root privilege and user privilege, in this case the root privilege is a higher level of privilege than the user one). Each privilege gives access to a range of differentiated APIs.

[**Sec.8**] The NFV exposed APIs should be divided into multiple subsets of APIs so that clients with different levels of privilege will only be able to use certain subsets of API functionality based on the clients' levels of privilege.

NOTE 3: A special case is that the management and orchestration functionality allow using all APIs for the highest privilege only.

[**Sec.9**] The management and orchestration functionality shall be able to authorize client's privilege for using APIs based on operator-defined criteria.

Reference is made to the technical challenges clause on Security and Resiliency from [i.1] and Use Cases "Virtual Network Platform as a Service (VNPaaS)", "Virtual Network Function as a Service (VNFaaS)" and "Virtualisation of the Home Environment" from GS NFV 001 [1].

5.7 Service Continuity

The NFV framework shall provide the following capabilities:

[**Cont. 1**] The SLA shall describe the level of service continuity required (e.g. seamless, non-seamless according to the definitions) and required attributes.

NOTE 1: There are two cases of the impact on service continuity in the events of intervening exceptions or anomalies: zero impact (seamless service continuity) and measurable impact (non-seamless service continuity).

NOTE 2: Seamless Service Continuity (with zero impact). In response to some anomaly (e.g. detected failure, commanded movement, and migration), there will be a means specified such that no observable state loss, no observable transmit queue packet loss and no observable transmit queue storage loss occurs, and any impact on latency and delay variation will be within the SLA specification for the function.

NOTE 3: Non-seamless Service Continuity. Some level of measurable service impact can be perceived by the end-user. When there is measurable service continuity impact on the function, then any impact will be described in terms of the SLA specification, to include at least a maximum value of outage duration, packet loss, latency and delay variation.

[**Cont. 2**] In the event of an anomaly that causes hardware failure or resource shortage/outage, the NFV framework shall be able to provide mechanisms such that the functionality of impacted VNF instance(s) shall be restored within the service continuity SLA requirements for the impacted VNF instance(s).

[**Cont. 3**] In the event that a VNF instance (or a subset thereof) needs to be migrated, the NFV framework shall be able to consider the impact on the service continuity during the VNF instance migration process and such impact shall be measurable and within the limits described in the SLA.

[**Cont. 4**] When a VNF instance subset (e.g. a VM) is migrated, the communication between the migrated VNF instance and other entities (e.g. VNF instance subset or physical network elements) shall be maintained regardless of its location and awareness of migration.

5.8 Service Assurance

Once many network functions are provided in virtualised form, the more ubiquitous presence of virtualisation infrastructure presents the opportunity for running virtualised instrumentation functions whenever and wherever they are needed, e.g. to remotely view a point in the network to diagnose problems, to routinely monitor performance as seen by a customer or to measure latency between two remote points.

Therefore sufficiently precise mechanisms will be needed in any circumstances where the relation between one function and another may be investigated, including when replica functions are created or functions are migrated.

[**SeA.1**] The NFV framework shall provide mechanisms for time-stamping of hardware (e.g. network interface cards, NICs, and network interface devices, NIDs, that sit beneath virtualisation infrastructure). The minimum support from hardware shall be to:

- copy packets or frames;
- accurately time-stamp the copies, using a clock synchronized to a source of appropriate precision (e.g. IEEE 1588 [i.2]); and
- forward the time-stamped copies to a configured destination. Once the precise time-stamps have been added in hardware, all other instrumentation and diagnosis functions can then proceed as virtualised functions without strict time constraints, e.g. filtering headers, removing payloads, local analysis, forwarding for remote analysis, logging, storage, etc.

[**SeA.2**] It should be possible to interrogate whether particular network interface hardware provides hardware time-stamping facilities.

NOTE 1: Detailed requirements and recommendations on how this could be economically implemented are to be addressed during further phases of the NFV work and/or referenced to a competent body.

[**SeA.3**] A (set of) VNF instance(s) and/or a management system shall be able to detect the failure of such VNF instance(s) and/or network reachability to that (set of) VNF instance(s) and take action in a way that meets the fault detection and remediation time objective of that VNF resiliency category.

NOTE 2: Detailed requirements on liveness checking of an VNF, e.g. watchdog timer or keepalive, as well as means including interface, syntax, methods for discovering, publishing, and retrieving notifications, are to be addressed during further phases of the NFV work.

[**SeA.4**] A VNF shall be able to publish means by which other entities (e.g. another VNF, the orchestration functionality and/or a management system) can determine whether the VNF is operating properly.

5.9 Operational and Management requirements

[**OaM.1**] The NFV framework shall incorporate mechanisms for automation of operational and management functions, e.g. creation, scaling and healing of VNF instances based on pre-defined criteria described in the VNF information model, network capacity adaptation to load, software upgrades and new features/nodes introduction, functions configuration and relocation and intervention on detected failures.

NOTE 1: The examples given are considered an initial set and it is expected that additional mechanisms are addressed as NFV solutions start to be deployed.

[**OaM.2**] The NFV framework shall be able to provide an management and orchestration functionality that shall be responsible for the VNF and VNF instances lifecycle management: instantiation, allocation and relocation of resources, scaling, and termination.

[**OaM.3**] The management and orchestration functionality shall be limited to the differences introduced by the Network Function Virtualisation process. The management and orchestration functionality shall be neutral with respect to the logical functions provided by the VNFs.

NOTE 2: Operational, Provisioning or Management aspects of the logical functions of the VNF are not considered part of the orchestration functionality depicted in the present document.

[**OaM.4**] As part of VNF life cycle management, monitoring and collection of information related to usage, the management and orchestration functionality shall be able to interact with other operations systems (when they exist) managing the Virtual Network Functions and/or the NFV infrastructure comprised of compute/storage machines, network software/hardware and configurations and/or software on these devices.

[**OaM.5**] The management and orchestration functionality shall be able to use standard information models that describe how to manage the VNF life cycle. Information models provide a structure of operational attributes of VNFs, as well as characteristics of the network service in terms of capacity, performance, resiliency, constraints and security, for example:

- deployment attributes and environment of a VNF e.g. VM images, required computational and storage resources and network reachability;
- operational attributes of a VNF, e.g. VNF topology as the links between the different network functions composing a specific network service, operations (initiation/tear-down), functional scripts.
- migration attributes of a VNF e.g. limitations for maximum acceptable propagation delay, scaling [Elas.2] and resiliency [Res.1] methods as defined by the SLA.

NOTE 3: The examples above are not exhaustive and can be refined during further phases of the NFV work.

[OaM.6] The management and orchestration functionality shall be able to manage the lifecycle of VNFs and VNF instances using the information models in combination with run-time information accompanying scheduled or on-demand requests regarding VNF instances and run-time policies/constraints.

[**OaM.7**] The management and orchestration functionality shall be able to manage the NFV infrastructure in coordination with other applicable management systems (e.g. CMS) and orchestrate the allocation of resources needed by the VNF instances.

[**OaM.8**] The management and orchestration functionality shall be able to maintain the integrity of each VNF instance with respect to its allocated NFV infrastructure resources.

[**OaM.9**] The management and orchestration functionality shall be able to monitor and collect NFV infrastructure resource usage and map such usage against the corresponding particular VNF instances.

[**OaM.10**] The management and orchestration functionality shall be able to monitor resources used on a per-VNF basis, and shall be made aware of receiving events that reflect NFV Infrastructure faults, correlate such events with other VNF related information, and act accordingly on the NFV Infrastructure that supports the VNF.

[**OaM.11**]: The management and orchestration functionality shall support standard APIs for all applicable functions (e.g. VNF instantiation, VNF instances allocation/release of NFV infrastructure resources, VNF instances scaling, VNF instances termination, and policy management) that it provides to other authorized entities (e.g. OSS, VNF instances, 3rd parties).

[**OaM.12**] The management and orchestration functionality shall be able to manage policies and constraints (e.g. regarding placement of VMs).

[**OaM.13**] The management and orchestration functionality shall enforce policies and constraints when allocating and/or resolving conflicts regarding NFV Infrastructure resources for VNF instances.

[**OaM.14**] The NFV framework shall be able to manage the assignment of NFVI resources to a VNF in a way that resources (compute hardware, storage, network) can be shared between VNFs.

Reference is made to the technical challenges clauses on Automation, Simplicity and Integration from [i.1].

5.10 Energy Efficiency requirements

Network infrastructures consume significant amounts of energy. Studies have indicated that NFV could potentially deliver up to 50 % energy savings compared with traditional appliance based network infrastructures. The virtualisation aspect of network functions assumes some separation of communication, storage or computing resources, which implies changes in the distribution of energy consumption. VNFs provide on-demand access to a pool of shared resources where the locus of energy consumption for components of the VNF is the virtual machine instance where the VNF is instantiated. It is expected that the NFV framework can exploit the benefits of virtualisation technologies to significantly reduce the energy consumption of large scale network infrastructures.

[**EE.1**] The NFV framework shall support the capability to place only VNF subset that can be moved or placed in a sleep state on a particular resource (compute, storage) so that resource can be placed into a power conserving state.

NOTE 1: Workload consolidation can be achieved by e.g. scaling facilities so that traffic load is concentrated on a smaller number of servers during off-peak hours so that all the other servers can be switched off or put into energy saving mode.

[**EE.2**] The NFV framework shall be able to provide mechanisms to enable an authorized entity to control and optimize energy consumption on demand, by e.g. scheduling and placing VNF instances on specific resources, including hardware and/or hypervisors, placing unused resources in energy saving mode, and managing power states as needed.

NOTE 2: Energy efficiency mechanisms could consider maintaining service continuity requirements and network stability requirements.

[**EE.3**] The NFV framework shall provide an information model that includes attributes defining the timeframe required for a compute resource, hypervisor and/or VNF (e.g. VM) to return to a normal operating mode after leaving a specific power-saving mode.

NOTE 3: This information is necessary to determine when to power on resources and software sufficiently in advance of the time when such assets would be needed to meet expected future workloads.

5.11 Coexistence with existing networks - Transition

[**Mig.1**] The NFV framework shall co-exist with legacy network equipment. I.e., the NFV framework shall be able to work in a hybrid network composed of classical physical network and virtual network functions as defined by a VNF Forwarding Graph.

[**Mig.2**] The NFV framework shall support a transition path from today's Physical Network Functions (PNFs) based solutions, to a more open standards based virtual networks functions solutions.

NOTE 1: For example, the NFV migration could allow a true "mix&match" deployment scenario by integrating multiple virtual and physical network functions from different vendors without incurring significant integration complexity and facilitate multi-vendor ecosystem.

[**Mig.3**] The NFV framework in conjunction with legacy management system shall support the same service capability and acceptable performance impact within service SLA when transitioning from Physical Network Functions (PNFs) to Virtual Network Functions (and vice versa).

[**Mig.4**] The NFV framework shall be able to interwork with legacy management systems with minimal impact on existing network nodes and interfaces.

NOTE 2: Example of legacy management systems are Operational Support System (OSS), Business Support System (BSS), Cloud Management System or load balancing control systems that could exist in the operators' networks.

[**Mig.5**] During the transition from physical to virtual the NFV framework shall be able to ensure security of VNF instances from various security threats, without disrupting or negatively impacting existent physical network functions (PNFs) and associated network elements and interfaces.

Reference is made to the technical challenges clause on Coexistence with existing networks - migration, from [i.1].

6 Service Models

6.1 General

In order to meet network service performance objectives (e.g. latency, reliability), or create value-added services for global customer or enterprises, it may be desirable for a Service Provider to be able to run VNF instances on NFV Infrastructure (including infrastructure elements common with cloud computing services) which is operated by a different Service Provider.

The ability to remotely deploy and run Virtualised Network Functions on NFV Infrastructure provided by another Service Provider permits a Service Provider to more efficiently serve its global customers. The ability for a Service Provider to offer its NFV Infrastructure as a Service (e.g. to other Service Providers) enables an additional commercial service offer (in addition to a Service Providers existing catalogue of network services that may be supported by VNFs) to directly support, and accelerate, the deployment of NFV Infrastructure. The infrastructure may also be offered as a Service from one department to another within a single Service Provider.

The commercial and deployment aspects of those agreements are out of the scope of the present document and only the technical requirements to facilitate these models will be depicted.

Maintenance for NFV framework and hosted VNFs will be different to non-virtuali sed network functions. Especially in deployments, where not only the vendors of framework and VNFs but also the providers of framework and VNFs are different, it needs to be assured that all necessary service and maintenance tasks on the resources, the framework and the VNFs can be executed. There will be new interactions in such a multivendor - multi-operator environment. More details are provided in the maintenance clause.

6.2 Deployment models

[**Mod.1**] The NFV framework shall provide the necessary mechanisms to achieve the same level of service availability for fully and partially virtualised scenarios as for existing non-virtualised networks.

[**Mod.2**] Services (i.e. "User" services) making use of network functions shall be agnostic with regards to the actual implementation of it as virtual or non-virtual network function.

[**Mod.3**] The NFV framework shall permit identification and management of two types of traffic flows: services traffic over Virtualised Network Functions, in addition to identifying traffic flows specific to resource facing operations (e.g. management, portability, scaling, etc.).

Reference is made to the Use Case "Virtualisation of Mobile Core Network and IMS" from GS NFV 001 [1].

6.3 Service models

[**Mod.5**] The NFV framework shall provide the appropriate mechanisms to facilitate network operators to consume NFV infrastructure resources operated by a different infrastructure provider, via standard APIs, and without degraded capabilities (e.g. scaling, performance, etc.) compared to consuming self -operated infrastructure resources.

[**Mod.6**] The NFV framework shall permit Virtual Network Functions from different Service Providers to coexist within the same infrastructure while facilitating the appropriate isolation between the resources allocated to the different service providers.

[**Mod.7**] The NFV framework should permit a Service Provider to fulfil, assure and bill for services delivered to end users across infrastructures that are independently administered.

[**Mod.8**] The NFV framework shall be able to provide the necessary mechanisms to instantiate different subsets of VNF (e.g. VMs) of the same VNF on infrastructure resources managed by different administrative domains.

[**Mod.9**] Appropriate mechanisms shall exist for:

- Authentication and authorization to control access in a way that only authorized VNF instances from authorized Service Providers are allowed to be executed.

- Failure notification and diagnostics and measurement of SLA related parameters, so that VNF instance failures or resource demands from one Service Provider do not degrade the operation of other Service Provider's VNF instances.

- Maintaining the relationships between each virtual network function/application, the service making use of it and the resources allocated to it.

[Mod.10] The NFV framework shall support different options for allocation of resources to adapt to different sets of virtual network functions/applications, e.g. pay-as-you-go, overcommitting, immediate reservation, etc.

6.4 Maintenance models

Serviceability and Maintainability describe how the necessary tasks to run an NFV framework and the hosted VNFs are supported by the system. This mostly deals with exchanging software or hardware and with diagnosis and elimination of problems, as well as monitoring the health of NFV framework and VNFs, logging of resource usage, energy consumption, irregular events, etc.

[**Maint.1**] The NFV framework shall be able to facilitate all necessary actions to assure long life cycle of the infrastructure services, such as hardware and software exchanges, live upgrades, troubleshooting, repair, logging.

[**Maint.2**] The NFV framework shall be able to provide the necessary support for providers of VNFs deployed on the framework for the troubleshooting, repair and other service tasks for the VNFs. The serviceability and maintainability for VNFs should be possible as for non virtuali sed network functions.

[**Maint.3**] The NFV framework shall provide the necessary means to exchange any piece of hardware (compute, storage, network equipment or equipment practice) without affecting service continuity of the hosted services.

[**Maint.4**] The NFV framework shall provide the necessary means to exchange any piece of firmware and software of all domains without affecting service continuity.

[**Maint.5**] The NFV framework shall provide the necessary means to verify the health of any resource it provides for the hosted VNFs.

[**Maint.6**] The NFV framework shall provide the necessary means to diagnose faults of resources, so it can be identified which unit of hardware or software needs repair.

[**Maint.7**] The NFV framework shall provide the necessary means to repair all parts of its software without affecting the service continuity of the hosted services.

[**Maint.8**] The NFV framework shall provide the necessary means to verify that a corrective process was successful and the fault is eliminated.

[**Maint.9**] The NFV framework shall provide an inventory of all units of hardware and software it consists of, including information about versions, releases, patches etc.

[**Maint.10**] The NFV framework shall monitor, log and report all changes to its inventory.

[**Maint.11**] The NFV framework shall provide the necessary means to log and report the usage of its resources.

[**Maint.12**] The NFV framework shall provide the necessary means to log and report any unexpected events on the resources.

[**Maint.13**] The NFV framework shall provide the necessary means to log and report all maintenance activity on the framework

[**Maint.14**] The NFV framework shall provide the necessary interfaces for VNFs to implement their serviceability and maintainability.

[**Maint.15**] The NFV framework shall provide the necessary interfaces for VNFs to report unexpected behaviour of resources.

[**Maint.16**] The NFV framework shall support the correlation of events between the resources and VNFs. E.g. the events shall be logged including information like exact location and time.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Susana Sabater, Vodafone Group PLC

Other contributors:

Jan Ignatius, NSN

Peter Woerndle, Ericsson

Ashiq Khan, DOCOMO

Michael Brenner, Alcatel Lucent

Don Clarke, British Telecom

Marc Flauw, Hewlett Packard

Naseem Khan, Verizon UK LTD

Olivier Le Grand, France Telecom

Dave McDysan, Verizon UK LTD

Kazuaki Obana, NTT

Parviz Yegani, Juniper Networks

Valerie Young, Intel

Tetsuya Nakamura, DOCOMO

Hidetoshi Yokota, KDDI Corportaion

Ulrich Kleber, Huawei

History

Document history		
V1.1.1	October 2013	Publication