Network Functions Virtualisation (NFV)

Network Operator Perspectives on NFV priorities for 5G

OBJECTIVES

The objectives for this white paper are to provide network operator perspectives on NFV priorities for 5G and to identify common technical features in terms of NFV.

This is a non-proprietary white paper authored by network operators who are participating in the ETSI NFV Industry Specification Group (NFV ISG). It has been produced independently of the NFV ISG; it is not an NFV ISG document and claims no endorsement by the NFV ISG.

CONTRIBUTING ORGANISATIONS & AUTHORS

Bell Canada:	Javan Erfanian, Brian Smith.
BT:	Peter Willis, Phil Eardley, Alex Leadbeater.
CableLabs:	Tetsuya Nakamura, Don Clarke, Steve Goeringer.
CenturyLink:	Michael Bugenhagen.
China Mobile:	Chih-Lin I, Jinri Huang, Rongwei Ren, Peng Zhao, Lingli Deng.
China Unicom:	Xiaoyan Pei, Jie Miao, Gang He.
Colt:	Javier Benitez.
Deutsche Telekom:	Klaus Martiny.
KDDI:	Keisuke Kuroki.
KT:	Kisang Ok, Youngwook Woo, Eunkyoung Paik.
NTT:	Takashi Shimizu, Atsushi Taniguchi.
NTT DOCOMO:	Kazuaki Obana, Ashiq Khan, Joan Triay Marques.
Orange:	Bruno Chatras, Chidung Lac.
Portugal Telecom:	António Gamelas, Jorge Carapinha.
Rogers:	Alex Markman.
SK Telecom:	DK Lee, Wooyong Choi, Keunhyun Kim.
Sprint:	Serge Manning.
STC:	Anwar I. Alsubhi, Samer S. Mahmoud.
Swisscom:	Markus Brunner.
Telecom Italia:	Cecilia Corbi, Elena Demaria.
Telefonica:	Diego López, Francisco Javier Ramón Salguero, Antonio Elizondo Armengol.
Telenor:	Pål Grønsund, Patrick Waldemar.
Vodafone:	Susana Sabater, Adrian Neal.

PUBLICATION DATE

February 21st, 2017 at the NFV#17 Plenary meeting, Bilbao, Spain

This white paper is available at the following link:
http://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

Executive Summary

This white paper provides network operator perspectives on priorities for NFV to deliver the industry vision for 5G systems and identifies common technical features in terms of NFV that should be adopted to accelerate progress and avoid duplication of specification effort across the industry.

Network operators believe NFV is a key technology enabler for 5G. While what "5G" exactly means is still to be defined, the evolved 5G network will be characterised by agile resilient converged fixed/mobile networks based on NFV and SDN technologies and capable of supporting network functions and applications encompassing different domains, including serving remote areas and inside buildings. This requires integration with existing network systems, efficiently extending the network and backhaul support and implementing end-to-end service management.

The breadth of foreseen 5G use cases and environments implies high scalability, ultra-low latency, ability to support a massive number of concurrent sessions and ultra-high reliability and security, while each 5G use case has significantly different characteristics and combinations of these requirements. To achieve these goals, Network Slicing, Edge Computing, Security, Reliability, and Scalability should be taken into account in the context of virtualisation. Moreover, given that the goal of NFV is to decouple network functions from hardware, and virtualised network functions are designed to run in a generic IT cloud environment, cloud-native design principles and cloud-friendly licensing models are critical matters.

The NFV ISG already provides foundational specifications for many 5G technologies and supporting network operations. Therefore, the authors of this paper recommend that the NFV specifications are referenced and used as the basis for 5G specification work in the relevant industry bodies, and that these bodies are pro-active to provide feedback to the NFV ISG on gaps or capabilities that need to be addressed by NFV technologies to support the evolution of 5G systems.

Contents

1 Introduction

The emergence of Network Functions Virtualisation (NFV) as the foundation for telecommunications networks of the future was heralded in our first white paper published in October 2012 [1]. The paper called for international collaboration to accelerate development and deployment of interoperable solutions for NFV based on high volume industry standard servers. The formation of the ETSI NFV Industry Specification Group (NFV ISG) in November 2012 was the specific action taken to achieve the goals.

Over the past four years, the NFV ISG has grown to over 290 organisations including 38 network operators, which provides an unparalleled collective service provider view of business requirements and strategic direction. The intensity of work remains undiminished and the NFV ISG periodically evolved its internal structure to deal with a very high workload and to accommodate the expansion of scope resulting from greater technical awareness of the topic. The NFV specifications are being widely used across the industry in bodies and forums as a key input.

Since the first meeting of the NFV ISG in January 2013, the key Standards Development Organisations (SDOs) for telecommunications networks have established relationships with the NFV ISG and have evolved their work to take into account the emergence of NFV as a foundation technology. The NFV ISG recently completed and published the second release of documents to guide industry implementation of NFV solutions and work on a third release of documents is well underway and scheduled for completion in the second half of 2017.

We believe NFV will realise its full potential as the basis for the next significant wave of telecommunications infrastructure deployment - 5G. While what "5G" exactly encompasses is still under discussion in the wider industry, 5G is being defined in relevant SDOs (the reason we do not seek to define it here) and standardisation work is progressing at pace. Re-use of existing wireless infrastructure, e.g. LTE, is anticipated and important for early deployments. We believe the evolved 5G system will be characterised by an agile resilient converged fixed/mobile core network based on NFV and SDN technologies and capable of supporting network functions and applications from different domains (i.e. beyond a domain-specific focus of a particular industry body). Hence the NFV ISG has a key role to ensure that an NFV-based infrastructure for 5G will not only enable 5G, but also support the myriad of new network functions and applications that will undoubtedly be spawned as a result of 5G deployments, and the evolution of existing networks.

The NFV ISG already provides foundational specifications for many 5G technologies including support for agile network operations. In addition, the group has consistently sought to work collaboratively with other bodies to identify and address gaps for NFV to support their domain-specific requirements. This needs to be a two-way street and we will act to ensure that the whole industry works together to realise the 5G vision.

This white paper provides directional feedback from the perspective of multiple network operators on NFV priorities for 5G in order to identify and encourage re-use of the common technical NFV features to avoid wasteful duplication of industry effort.

2 NFV Key Features for 5G

This section describes key NFV features that network operators in the NFV ISG as well as the wider industry are addressing in order to realise 5G use cases. These features include Network Slicing, Cloud-native design principles, End-to-end Service Management, Edge Computing, Cloudification of the Radio Access Network (RAN), Multi-site/domain Services, NFV License Management, Security, Reliability, and Scalability.

2.1 Network Slicing

From a network operator viewpoint, Network Slicing is a service-oriented network construct providing network-on-demand to concurrent applications. In other words, Network Slicing can be seen as an implementation of the "Network as a Service" paradigm, where a common network is able to provide and expose concurrent, partitioned and self-contained “slices” to support different services in an efficient way and provide the required Quality of Service (QoS).

From a standards definition view point, domain-specific standards bodies and open source communities are using “slicing” in contextually different ways. This is a barrier to convergence of requirements, potentially leading to increased complexity to implement network slicing in a converged (i.e. common) core infrastructure supporting 5G and other evolved network services.

Although standardisation bodies and industry forums have produced their own definitions of network slicing, available definitions in different SDOs and industry forums seem to have one thing in common: all of them refer to the creation of multiple logical network instances (i.e. slices) on the same underlying network. The parameters for each “slice” are optimised according to different criteria and possibly used by different tenants/organisations. This is reminiscent of the way NFV is typically used to support use cases such as creating on-demand enterprise customer networks (e.g. virtual enterprise CPE). Indeed, network slices can be viewed as on-demand networks. In NFV parlance, a slice would typically be deployed as one or more NFV Network Service instances. NFV technology thus provides a solid platform to support 5G network slicing.

The concepts of NFV Network Services and deployment flavours can be leveraged in a quite straightforward manner to deploy and manage network slices in an automated and flexible way. To enable full automation of network slice management, NFV Management & Orchestration functions (NFV-MANO) need to be complemented and interwork with slice management functions. These slice management functions can consume the Application Programming Interfaces (APIs) exposed by the NFV Orchestrator (NFVO) for Network Service and Virtual Network Function (VNF) lifecycle management, as well as other APIs exposed by other management entities enabling Fault, Configuration, Accounting, Performance and Security management (FCAPS) of the network functions involved in a slice instance. As a result, slice management can be regarded as a particular Operations Support System (OSS) functional area which needs to be standardised on top of NFV. This includes specifying a mechanism for mapping network slice requirements onto Network Services capabilities.

With regard to NFV-MANO, we believe that most features required to enable network slicing are already incorporated in the NFV Architectural Framework and specified in the relevant deliverables published by the NFV ISG over the past four years. Hence, support for network slicing is unlikely to bring fundamentally new requirements to an NFV system. However, a few areas do deserve further attention and standardisation work, in particular in the fields of multi-site/multi-tenant

orchestration, isolation of resources at different layers, and security enforcement. Multi-Operator inter-working will require model harmonisation in order for relevant data from one operator to be viewable in the NFV / Cloud Graphical User Interfaces (GUIs, sometimes called dashboards) of another operator. Some groups have identified this common top down model as an industry business requirement.

2.2 Cloud-native Network Functions

Cloud-native network functions are network functions implemented using generic IT cloud techniques beyond virtualisation (e.g. functions composed from re-usable components rather than monolithic implementations of functions). The goal is to maximise efficient use of resources through a finer-grained multiplexing on the infrastructure, and to be amenable to advanced cloud orchestration techniques as used in IT environments while offering the deterministic performance deriving from the NFV requirements specified by the NFV ISG. This is in contrast to virtualised network functions that are re-purposed software coming from existing Physical Network Functions/Appliances (PNFs).

It is important to support VNFs which follow cloud-native design principles. Assumptions are that such VNFs

- can be decomposed into many lightweight components and common platform services,
- are designed following a component-based software engineering style (e.g. Micro-services), and
- are built for quick restoration under failure conditions.

Enhancements to the NFV ISG defined interfaces (MANO and NFVI) to provide flexible choices for the designers of VNFs may thus be needed, for example, in the area of provisioning common platform services, management of many dependent VNF components, and communication between many VNF components.

Virtualised implementations of 5G network functions may be instantiated, terminated and version updated more rapidly than traditional physical implementations [2], for example to support the on-demand nature of network slicing. Hence, 5G network functions should consider the following factors for efficient deployment and operation of elastic and dynamically evolving end-to-end network slices [2,3]:

1. 5G architecture, interfaces, and protocol stacks should be designed taking into account the opportunities offered by cloud-native VNFs.
2. Data storage (e.g. user profiles, traffic identification data or firewall rules) should be separated from processing/logic (e.g. moving data to a shared data layer) for easy and massive scale-out of the functionality, if compatible with performance requirements. Typically, this is relatively easy to achieve for control and management related functionality, but harder to achieve for data/user plane functionality.
3. Reduce the need for maintaining state in the components of network functions as much as possible, so as to facilitate flexible scale-in/out or migration with no or short service

interruption. The recommendation to reduce the need to maintain state can also apply to the VNF level, by considering functional architectures that minimise the number of functional entities having to maintain state.

4. Define functional components that can be independently scaled, re-used, composed, and migrated. This applies both at the VNF level (e.g. design small VNFs that can be easily re-used to compose various Network Services and nested Network Services) and on the VNF Component (VNFC) level.

5. Techniques to tradeoff data storage versus compute should be considered to optimise resource utilisation and performance at run time. Potential gains identified when using one technique versus another (e.g. local disks versus separate servers) should be assessed.

6. Identification of VNF instances in a location independent manner in order to automatically support load-balance and switch-over (as required) across locations during lifecycle operations or under failure conditions.

7. Customisation of VNFs by applications is required. This can happen through inter-VNF communication or configuration changes. For example, an IoT application wants to change certain settings of the firewall VNF of the connectivity service.

2.3 End-to-end Service Management

Virtualisation is one of the basic transformation pillars for next generation networks. However, an end-to-end vision is necessary to implement NFV use cases in general, and 5G-related ones in particular in order to realise the benefits of an NFV-based architecture in a production network.

One of the key concepts underpinning the business decisions to invest in future systems is to enable different service offerings for different customers. Moreover, customers may be able to compose their proprietary service by selecting basic network service components in order to meet their specific needs. This is what we mean when we talk about 5G network slices that are composed of capabilities from multiple network segments that span the network from access to core, as well as service components. This end-to-end perspective is needed to meet the needs of diverse services, use cases, and business models.

To make this model work appropriately, it appears clear that different deployment interworking scenarios, including those related to interworking with legacy networks, must be taken into account. Moreover, existing networks and systems (e.g. OSS/BSS) must be able to work with the new models to form an end-to-end service delivery and service assurance solution.

One of the key challenges that must be addressed is the definition of a complete management and orchestration framework. Such a framework should exploit and leverage NFV features (e.g. on-demand instantiation and scaling of VNFs) together with additional automated network capabilities for guaranteeing reliability and service assurance. Coordination among a) resource-oriented management tasks performed by MANO, and b) FCAPS management of network application is needed.

We believe that the design of procedures such as selection and reselection (e.g. selection of mobility management entities) must take into account the potential dynamic nature of VNF

placement. Lifecycle operations performed over a specific VNF are essentially of a dynamic nature [4,5] and may introduce variations regarding the placement and deployment of VNFs. In the NFV ISG architecture, it is the NFV Orchestrator (NFVO) that keeps a map of the NFVI Points of Presence (PoPs) where specific VNFs are deployed, and introduces dynamic VNF allocation within the deployed networks according to diverse policies and requirements related to global resource and capacity management, resilience considerations, etc.

The classical FCAPS functions are still needed but the processes and implementations will change. Complexity will increase, requiring a higher degree of automation for OAM functions. The network will run more autonomously and the production of services will become more automated and more often on a real time basis. Hence, management of changes in VNFs or clouds will be more dynamic than the management of static network elements.

Historically, Network Management has been based on Element Management supported by intelligent strategies such as alarm filtering and correlation. The new approach should be more focused on services management and based on real-time Service & Network Management.

2.4 Edge Computing

Support of services with ultra-low latency requirements is one of the key differentiators for 5G over previous technologies. This implies deploying 5G networks as highly distributed systems, where network functions that are the most sensitive to latency run on servers located as close as possible to end-user devices or even within such devices. The ETSI Mobile Edge Computing Industry Specification Group (MEC ISG) architecture is an incarnation of this. The MEC ISG and NFV ISG are working together to understand how the architecture defined by the former can be implemented using the framework specified by the later. It is advantageous that many of the same players are involved in both forums, but joint effort is still needed to ensure alignment.

Ultimately, what the industry is looking for is a single distributed NFVI with associated management and orchestration functions which accommodates all aspects of 5G and the mainstream NFV use cases.

2.5 RAN Cloudification

NFV should be applied to 5G networks end-to-end, i.e. including both core networks and Radio Access Networks (RAN), as well as network management systems. Network virtualisation to date has focused on the core network to underpin growth of existing systems. After showing enough success in the core network, virtualisation is now also moving into the RAN area. As 5G approaches, it is timely to accelerate RAN cloudification, and radio functions virtualisation is one of the key use cases documented by the NFV ISG [6]. In addition, several concepts in the realm of RAN cloudification, including C-RAN [7], elastic RAN, virtualised RAN [8], etc. have been proposed and widely accepted as essential for 5G RAN architectures.

RAN cloudification is expected to provide operators with unprecedented capability in terms of flexibility, agility, resource/service management and orchestration, etc. Due to unique characteristics of radio signal processing, including the strict latency requirements of the order of 1ms or less for new 5G air interfaces, and high-volume computation, RAN cloudification is more

challenging than other features of the wireless networks. Some challenges have been identified as follows:

- RAN function split and the functional definition of RAN VNFs. Even though not all RAN functions may be amenable to virtualisation and run on general-purpose processors or centralised in data centers, it is crucial to assess the most suitable targets for virtualisation and define a RAN architecture with clear identification of both VNFs and PNFs, and the related standard interfaces,
- potential new requirements imposed by RAN-VNFs on the NFVI due to unique features of RAN function processing should be specified,
- potential RAN requirements for acceleration [9], in particular interface definition and management should be specified,
- RAN-related management and orchestration functions, including Self-Organising Networks (SON), should evolve to interwork with the NFV-MANO framework,
- whether RAN-oriented functions extension of MANO are necessary should be investigated by taking into account RAN specific features and requirements such as the need for site backup, connection restriction between central unit and distributed units, etc.

2.6 Multi-site/domain Services

The support of Infrastructure as a Service (IaaS), NFV as a Service (NFVaaS) and Network Service (NS) composition in different administrative domains is critical for the 5G work, for example roaming scenarios in wireless networks.

Within the 5G context, scenarios where the NS supporting a network slice is itself a composition of nested or concatenated NSs, each provided by different operators, may become more common than with today's mainstream NFV use cases. Thus, NFVO hierarchies may need to be deployed where a top-level NFVO responsible for a parent NS would delegate to lower-level NFVOs the management of nested NSs. The NFV ISG is working on such multi-domain scenarios as a part of the natural evolution of NFV technology, and as a consequence of new business models which are enabled by a software-intensive approach [10].

Furthermore, Network Services can involve network functions deployed at different sites, thereby requiring virtual network connectivity to be established across sites, possibly through a Wide Area Network (WAN). Network slicing in the context of 5G is likely to make this scenario more common, considering the support of roaming, e.g. when a VNF to support home users/services is made available in the visiting network, and to ensure efficient use of legacy resources. In such cases, the NFVO will typically rely on a WAN Infrastructure Manager (WIM). As this functionality has been underspecified so far, the NFV ISG has started a study within the framework of the NFV release 3 specifications to identify potential new connectivity requirements for multi-site Network Services which could impact NFV management and orchestration functions [11].

2.7 NFV License Management

Providers of NFV software components currently offer proprietary license management mechanisms which make service provisioning and license acquisition/renewal operations complex and error prone. It also makes it difficult to deal with VNF license usage information to ensure that the contract between the service provider and software provider can be implemented and managed correctly. Moreover, the dynamic nature of NFV-based 5G systems with rapid reconfiguration of the infrastructure to respond to on demand changes imposes requirements that are very difficult to meet with licensing mechanisms available today. Therefore, to alleviate the compounding complexity of licensing interactions in such a dynamic NFV-based 5G system, underlying license management mechanisms need to be standardised.

To help solve this problem, the NFV ISG has initiated a study on the features needed within the NFV Architectural Framework to support NFV License Management functionality implemented in higher layer systems. The intent is to enable any service provider commercial licensing arrangement to be supported by standardised mechanisms.

2.8 Security

Network operators and developers of the 5G network functions have been considering the security implications of deployments on virtualised infrastructures. The core goal of ensuring security for 5G deployments using NFV will be extendibility of identity management, attestation, authentication, and encryption solutions across all aspects of 5G deployments.

The NGMN Alliance 5G white paper [12] introduces multiple use cases, which have unique security requirements. Meanwhile, migration to an NFV platform naturally modifies the threat surface, introducing new challenges - as well as some unique opportunities to improve security - as outlined in the NFV ISG Security Problem Statement [13].

The NGMN 5G Security Recommendations white paper [14] cites the network operator as the partner for state-of-the art data security using recognised security practices for all levels of communication, connectivity, and storage purposes. Telecommunications networks are considered Critical National Infrastructure (CNI) in many countries as they underpin economic success and support every aspect of public and private life of their citizens. The NFV ISG is addressing several key security areas in order to address 5G needs, beginning by ensuring that security-by-design can be achieved. Specific examples of these are the architecture for lawful interception, along with a more general architecture for the execution of sensitive components, pervasive security monitoring and management, as well as remote attestation.

Furthermore, recognising that “running” open source code is being used in the current implementation base, the NFV ISG has undertaken detailed study of *OpenStack* security [15], which includes recommendations for its evolution, particularly in the area of identity management. This work constitutes a valuable reference if the usage of open source software in implementing a 5G system is considered.

While the NFV ISG has addressed the solutions ([16]-[19]) to the problems identified in [12] and [15], there are still significant challenges that remain when envisaging 5G networks which the security experts are addressing. For example:

- a comprehensive identity management capability that comprises not only roaming or home-network users, but also the methods of pinpointing hardware and software components,
- a set of security-related guidelines for addressing network slicing both through establishing the common security base and through network slice isolation, and the identification and blocking of malicious traffic,
- the ability to disable the use of memory inspection by unauthorised sources and at the same time harness memory inspection capabilities to improve security of virtualised network functions,
- a better understanding of the impact of security controls such as authentication, authorisation, latency and other performance metrics, in order to provide sufficient security while satisfying user experience and business goals, and
- the incorporation of security management, attestation, and sensitive component control (e.g. lawful interception or other CNI functions), into the operations and management system. This would provide the ability to dynamically chain security services and automate the deployment of secure configurations compliant with validated and consistent operator policies, pervasive and responsible encryption, and computable attestation.

2.9 Reliability

There are unique challenges and opportunities to ensure service availability and resiliency in 5G systems which are expected to be required to support critical services. The topic of reliability has been extensively studied within the NFV ISG and the findings brought together in a number of documents which are informative to the design of 5G systems to support high availability services.

The Resiliency Requirements document [20] describes the resiliency problem, use case analysis, resiliency principles, requirements, and deployment, as well as engineering guidelines for NFV. The resiliency requirements cover service availability, fault management and failure prevention, detection, and recovery. The use cases considered include: resiliency of stateless and stateful services, network transparency of the location of the VNFs, regression and pre-emption, spatial distribution of the VNFs, service chaining, and service continuity. These use cases and the resiliency guidelines apply to the development of all VNFs including those that will support 5G networks.

The Resiliency Requirements document is the starting point for a number of detailed NFV reliability studies within the NFV ISG. These studies ([21]-[24]) include: (i) robust design architectures; (ii) end-to-end network service resilience assessment; (iii) impact on availability of software modification; (iv) active monitoring for anomalies detection; (v) NFV resilience metrics; (vi) roles and responsibilities leading to demarcation points in a quality accountability framework. It is noteworthy that a theme tackled in those studies is related to service availability level and grade of service allowing to deliver different SLAs based on a single pool of resources. Subject to adaptation, this concept is applicable to 5G slices that may be characterised by a diversity of QoS requirements.

These studies have strongly influenced the MANO specifications and led directly to the creation of the OPNFV 'Doctor' project [25] which itself has influenced key upstream open source projects, notably OpenStack.

5G is likely to increase the occurrence of complex deployment scenarios, thereby making resilience mechanisms more complex as well, e.g.:

- the coexistence of VNFs and physical network functions (e.g. for certain RAN functions) in some 5G systems, potentially coupled under the control of SDN elements, increases the complexity of end-to-end resilience-by-design,
- the traceability of fault propagation across nested and concatenated network services involved in the realisation of a network slice is rendered challenging, and
- coordination between multiple orchestrators might be required.

Network functions following cloud-native design principles such as software componentisation increase the overall fault tolerance of the network services from an end-to-end perspective.

When hardware or software failures occur, the cloud-native approach helps to make it easier to re-start small and lightweight components. This is more efficient and has quicker restoration times than re-launching large monolithic VNFs. High-availability mechanisms such as redundancy also need to have fast detection capabilities. Furthermore, a VNF can be componentised in a way enabling it to continue fulfilling its role, in a degraded mode, in case of failure of some of its non-critical components, although there should be a mechanism to report such events to the fault management system.

2.10 Scalability

5G use cases and Edge Computing drive a need to make the NFV architecture massively scalable. 5G networks will be composed of thousands, perhaps millions or even billions, of distributed compute nodes, e.g. it is entirely feasible each home could host a compute node running 5G VNFs and applications. This degree of scalability and distribution is not possible with today's Virtual Infrastructure Managers (VIMs). A key challenge is therefore to develop a VIM architecture and implementations that are massively scalable whilst at the same time open and flexible enough to address future unknown 5G applications. The NFV ISG can help define the scalability requirements but it is most likely VIMs will be developed through open source initiatives elsewhere.

3 Conclusions

Network operators recognise NFV as a key technology enabler for 5G. The evolved 5G network will be characterised by agile resilient converged fixed/mobile networks based on NFV and SDN technologies and capable of supporting end-to-end service management across heterogeneous environments. The breadth of foreseen 5G use cases and environments implies massive scalability, ultra-low latency, ability to support a huge number of concurrent sessions, ultra-high reliability and strong security, while each 5G use case has significantly different characteristics and combinations of these requirements. To achieve these goals, the requirements for Network Slicing, Edge Computing, Security, Reliability, Scalability, and RAN Cloudification outlined in this paper should be taken into account in the context of virtualisation of 5G systems. Moreover, given that the goal of NFV is to

decouple network functions from hardware, and to enable virtualised network functions to run in a generic IT cloud environment when required, cloud-native design principles and cloud friendly licensing models are critical matters.

The ETSI NFV Industry Specification Group has provided and will maintain foundational specifications which support both mainstream use cases, and the emerging 5G technologies, as well as the required network management operations. Therefore, the authors of this paper recommend that the NFV specifications are referenced and used as a basis for 5G specification work in the relevant industry bodies, and that these bodies are pro-active to provide feedback to the NFV ISG on gaps or capabilities that need to be addressed by NFV technologies to support the evolution of 5G systems. Meanwhile, the NFV ISG has itself identified gaps or capabilities that will be handled in the very near future.

4 References

1. Network Functions Virtualisation - Introductory White Paper, October, 2012: http://portal.etsi.org/NFV/NFV_White_Paper.pdf
2. ETSI GS NFV SWA 001 V1.1.1 (2014-12): Network Functions Virtualisation (NFV); Virtual Network Functions Architecture
3. ETSI GS NFV IFA 011 V2.1.1 (2016-10): Network Functions Virtualisation (NFV); Management and Orchestration; VNF Packaging Specification
4. ETSI GS NFV IFA 007 V2.1.1 (2016-10): Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification
5. ETSI GS NFV IFA 008 V2.1.1 (2016-10): Network Functions Virtualisation (NFV); Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification
6. ETSI GS NFV 001 V1.1.1 (2013-10): Network Functions Virtualisation (NFV); Use Cases
7. NGMN Alliance, “General Requirements for C-RAN”, 2012
8. NGMN Alliance, “Further Study on Critical C-RAN Technologies”, March, 2015
9. ETSI GS NFV IFA 001 V1.1.1 (2015-12): Network Functions Virtualisation (NFV); Acceleration Technologies; Report on Acceleration Technologies & Use Cases
10. Draft ETSI GR NFV IFA 028 V0.2.0 (2017-01): Network Functions Virtualisation (NFV); Management and Orchestration; Report on architecture options to support multiple administrative domains
11. Draft ETSI GR NFV IFA 022 V0.4.0 (2016-12): Network Functions Virtualisation (NFV); Management and Orchestration; Report on Management and Connectivity for Multi-Site Services
12. NGMN Alliance, "NGMN 5G White Paper v1.0", February, 2015
13. ETSI GS NFV SEC 001 V1.1.1 (2014-10): Network Function Virtualisation (NFV); NFV Security; Problem Statement
14. NGMN Alliance, “5G Security Recommendations - Package #2: Network Slicing”, April, 2016
15. ETSI GS NFV SEC 002 V1.1.1 (2015-08): Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software
16. ETSI GS NFV SEC 003 V1.2.1 (2014-12): Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance
17. ETSI GS NFV SEC 009 V1.1.1 (2015-12): Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration
18. Draft ETSI GS NFV SEC 012 V0.0.13 (2016-11): Network Functions Virtualisation (NFV); NFV Security; System architecture specification for execution of sensitive NFV components

19. Draft ETSI GS NFV SEC 007 V0.0.6 (2016-12): Network Functions Virtualisation (NFV); NFV Security; Trust; Report on Attestation Technologies and Practices for Secure Deployments
20. ETSI GS NFV REL 001 V1.1.1 (2015-09): Network Functions Virtualisation (NFV); Resiliency Requirements
21. ETSI GS NFV REL 003 V1.1.2 (2016-07): Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability
22. ETSI GS NFV REL 004 V1.1.1 (2016-04): Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection
23. ETSI GS NFV REL 005 V1.1.1 (2016-01): Network Functions Virtualisation (NFV); Accountability; Report on Quality Accountability Framework
24. ETSI GS NFV INF 010 V1.1.1 (2014-12): Network Functions Virtualisation (NFV); Service Quality Metrics
25. OPNFV Doctor Project: https://wiki.opnfv.org/display/doctor/Doctor+Home

5 Contact Information

If your organisation has any comment on the contents of this white paper, please contact any of the following:

Bell Canada: Javan Erfanian, javan.erfanian@bell.ca
BT: Peter Willis, peter.j.willis@bt.com
CableLabs: Tetsuya Nakamura, t.nakamura@cablelabs.com
CenturyLink: Michael Bugenhagen, michael.k.bugenhagen@centurylink.com
China Mobile: Jinri Huang, huangjinri@chinamobile.com
China Unicom: Jie Miao, miaojie9@chinaunicom.cn
Colt: Javier Benitez, javier.benitez@colt.net
Deutsche Telekom: Klaus Martiny, klaus.martiny@telekom.de
KDDI: Keisuke Kuroki, ke-kuroki@kddi.com
KT: Kisang Ok, ksok@kt.com
NTT: Takashi Shimizu, shimizu.takashi@lab.ntt.co.jp
NTT DOCOMO: Kazuaki Obana, kazuaki.obana.uz@nttdocomo.com
Orange: Bruno Chatras, bruno.chatras@orange.com
Portugal Telecom: António Gamelas, agamelas@alticelabs.com
Rogers: Alex Markman, alexander.markman@rci.rogers.com
SK Telecom: DK Lee, dongkee.lee@sk.com
Sprint: Serge Manning, serge.manning@sprint.com
STC: Samer Salah Mahmoud, sasmahmoud.c@stc.com.sa
Swisscom: Markus Brunner, markus.brunner3@swisscom.com
Telecom Italia: Cecilia Corbi, ceciliamaria.corbi@telecomitalia.it
Telefonica: Diego López, diego.r.lopez@telefonica.com
Telenor: Patrick Waldemar, patrick.waldemar@telenor.com
Vodafone: Susana Sabater, susana.sabater@vodafone.com

6 Glossary

API	Application Programming Interface
BSS	Business Support System
CNI	Critical National Infrastructure
C-RAN	Centralised, Cooperative, Cloud and Clean Radio Access Network

CPE	Customer Premises Equipment
DC	Data Center
DPI	Deep Packet Inspection
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, Configuration, Accounting, Performance & Security
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
IoT	Internet of Things
ISG	Industry Specification Group.
IT	Information Technology
LTE	Long Term Evolution
MEC	Mobile Edge Computing
MANO	Management and Orchestration
NFV	Network Functions Virtualisation
NFVaaS	NFV as a Service
NFVI	Network Functions Virtualisation Infrastructure
NFVO	NFV Orchestrator
NGMN	Next Generation Mobile Networks
NS	Network Service
OAM	Operations, Administration & Maintenance
OPNFV	Open Platform for NFV
OSS	Operations Support System
QoS	Quality of Service
PNF	Physical Network Function
PoP	Point of Presence
SDN	Software-Defined Networking
SDO	Standards Development Organisation
SLA	Service Level Agreement
SON	Self-Organising Network
VIM	Virtualised Infrastructure Manager
VNF	Virtualised Network Function
VNFC	VNF Component
WAN	Wide Area Network
WIM	WAN Infrastructure Manager