NFV RG
Internet-Draft
Intended status: Informational
Expires: March 7, 2019

CJ. Bernardos, Ed.
UC3M
LM. Contreras
TID
I. Vaishnavi
Huawei
R. Szabo
Ericsson
J. Mangues
CTTC
X. Li
NEC
F. Paolucci
A. Sgambelluri
B. Martini
L. Valcarenghi
SSSA
G. Landi
Nextworks
D. Andrushko
MIRANTIS
A. Mourad
InterDigital

September 3, 2018

# Multi-domain Network Virtualization
# draft-bernardos-nfvrg-multidomain-05

## Abstract

This document analyzes the problem of multi-provider multi-domain orchestration, by first scoping the problem, then looking into potential architectural approaches, and finally describing the solutions being developed by the European 5GEx and 5G-TRANSFORMER projects.

## Status of This Memo

## Copyright Notice

## Table of Contents

## 1. Introduction

The telecommunications sector is experiencing a major revolution that will shape the way networks and services are designed and deployed for the next decade. We are witnessing an explosion in the number of applications and services demanded by users, which are now really capable of accessing them on the move. In order to cope with such a demand, some network operators are looking at the cloud computing paradigm, which enables a potential reduction of the overall costs by outsourcing communication services from specific hardware in the operator’s core to server farms scattered in datacenters. These services have different characteristics if compared with conventional IT services that have to be taken into account in this cloudification process. Also the transport network is affected in that it is evolving to a more sophisticated form of IP architecture with trends like separation of control and data plane traffic, and more fine-grained forwarding of packets (beyond looking at the destination IP address) in the network to fulfill new business and service goals.

Virtualization of functions also provides operators with tools to deploy new services much faster, as compared to the traditional use of monolithic and tightly integrated dedicated machinery. As a natural next step, mobile network operators need to re-think how to evolve their existing network infrastructures and how to deploy new ones to address the challenges posed by the increasing customers’ demands, as well as by the huge competition among operators. All these changes are triggering the need for a modification in the way operators and infrastructure providers operate their networks, as they need to significantly reduce the costs incurred in deploying a new service and operating it. Some of the mechanisms that are being considered and already adopted by operators include: sharing of network infrastructure to reduce costs, virtualization of core servers running in data centers as a way of supporting their load-aware elastic dimensioning, and dynamic energy policies to reduce the monthly electricity bill. However, this has proved to be tough to put in practice, and not enough. Indeed, it is not easy to deploy new mechanisms in a running operational network due to the high dependency on proprietary (and sometime obscure) protocols and interfaces, which are complex to manage and often require configuring multiple devices in a decentralized way.

Furthermore, 5G networks are being designed to be capable of fulfilling the needs of a plethora of vertical industries (e.g., automotive, eHealth, media), which have a wide variety of requirements [ngmn_5g_whitepaper]. The slicing concept tries to make the network of the provider aware of the business needs of tenants (e.g., vertical industries) by customizing the share of the network assigned to them. The term network slice was coined to refer to a complete logical network composed of network functions and the resources to run them [ngmn_slicing]. These resources include network, storage, and computing. The way in which services requested by customers of the provider are assigned to slices depends on customer needs and provider policies. The system must be flexible to accommodate a variety of options.

Another characteristic of current and future telecommunication networks is complexity. It comes from three main aspects. First, heterogeneous technologies are often separated in multiple domains under the supervision of different network managers, which exchange provisioning orders that are manually handled. This does not only happen between different operators, but also inside the network of the same operator. Second, the different regional scope of each operator requires peering with others to extend their reach. And third, the increasing variety of interaction among specialized providers (e.g., mobile operator, cloud service provider, transport network provider) that complement each other to satisfy the service requests from customers. In conclusion, realizing the slicing vision to adapt the network to needs of verticals will require handling multi-provider and multi-domain aspects.

Additionally, Network Function Virtualization (NFV) and Software Defined Networking (SDN) are changing the way the telecommunications sector will deploy, extend and operate its networks. Together, they bring the required programmability and flexibility. Moreover, these concepts and network slicing are tightly related. In fact, slices may be implemented as NFV network services. However, building a complete end-to-end logical network will likely require stitching services offered by multiple domains from multiple providers. This is why multi-domain network virtualization is crucial in 5G networks.

## 2. Terminology

The following terms used in this document are defined by the ETSI NVF ISG, and the ONF and the IETF:

NFV Infrastructure (NFVI): totality of all hardware and software components which build up the environment in which VNFs are deployed

NFV Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, and VIM.

NFV Orchestrator (NFVO): functional block that manages the Network Service (NS) lifecycle and coordinates the management of NS lifecycle, VNF lifecycle (supported by the VNFM) and NFVI resources (supported by the VIM) to ensure an optimized allocation of the necessary resources and connectivity.

Network Service Orchestration (NSO): function responsible for the Network Service lifecycle management, including operations such as: On-board Network Service, Instantiate Network Service, Scale Network Service, Update Network Service, etc.

OpenFlow protocol (OFP): allowing vendor independent programming of control functions in network nodes.

Resource Orchestration (RO): subset of NFV Orchestrator functions that are responsible for global resource management governance.

Service Function Chain (SFC): for a given service, the abstracted view of the required service functions and the order in which they are to be applied.  This is somehow equivalent to the Network Function Forwarding Graph (NF-FG) at ETSI.

Service Function Path (SFP): the selection of specific service function instances on specific network nodes to form a service graph through which an SFC is instantiated.

Virtualized Infrastructure Manager (VIM): functional block that is responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator’s Infrastructure Domain.

Virtualized Network Function (VNF): implementation of a Network Function that can be deployed on a Network Function Virtualization Infrastructure (NFVI).

Virtualized Network Function Manager (VNFM): functional block that is responsible for the lifecycle management of VNF.

## 3.  Background: the ETSI NFV architecture

The ETSI ISG NFV is a working group which, since 2012, aims to evolve quasi-standard IT virtualization technology to consolidate many network equipment types into industry standard high volume servers, switches, and storage.  It enables implementing network functions in software that can run on a range of industry standard server hardware and can be moved to, or loaded in, various locations in the network as required, without the need to install new equipment.  To date, ETSI NFV is by far the most accepted NFV reference framework and architectural footprint [etsi_nvf_whitepaper].  The ETSI NFV framework architecture framework is composed of three domains (Figure 1):

- o Virtualized Network Function, running over the NFVI.

- o NFV Infrastructure (NFVI), including the diversity of physical resources and how these can be virtualized. NFVI supports the execution of the VNFs.

- o NFV Management and Orchestration, which covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs. NFV Management and Orchestration focuses on all virtualization specific management tasks necessary in the NFV framework.

```
   +-------------------------------------------+  +---------------+
   |   Virtualized Network Functions (VNFs)    |  |               |
   |  -------   -------   -------   -------    |  |               |
   |  |     |   |     |   |     |   |     |    |  |               |
   |  | VNF |   | VNF |   | VNF |   | VNF |    |  |               |
   |  |     |   |     |   |     |   |     |    |  |               |
   |  -------   -------   -------   -------    |  |               |
   +-------------------------------------------+  |               |
                                                  |               |
   +-------------------------------------------+  |               |
   |         NFV Infrastructure (NFVI)         |  |      NFV      |
   | -----------    -----------    ----------- |  |  Management   |
   | | Virtual |    | Virtual |    | Virtual | |  |      and      |
   | | Compute |    | Storage |    | Network | |  | Orchestration |
   | -----------    -----------    ----------- |  |               |
   | +-------------------------------------+ |  |               |
   | |         Virtualization Layer        | |  |               |
   | +-------------------------------------+ |  |               |
   | +-------------------------------------+ |  |               |
   | | -----------  -----------  ----------- | |  |               |
   | | | Compute |  | Storage |  | Network | | |  |               |
   | | -----------  -----------  ----------- | |  |               |
   | |          Hardware resources         | |  |               |
   | +-------------------------------------+ |  |               |
   +-------------------------------------------+  +---------------+
```

Figure 1: ETSI NFV framework

The NFV architectural framework identifies functional blocks and the main reference points between such blocks. Some of these are already present in current deployments, whilst others might be necessary additions in order to support the virtualization process and consequent operation. The functional blocks are (Figure 2):

- o Virtualized Network Function (VNF).

- Element Management (EM).

- NFV Infrastructure, including: Hardware and virtualized resources, and Virtualization Layer.

- Virtualized Infrastructure Manager(s) (VIM).

- NFV Orchestrator.

- VNF Manager(s).

- Service, VNF and Infrastructure Description.

- Operations and Business Support Systems (OSS/BSS).

```
                                                  +--------------------+
   +-------------------------------------------+  | ----------------   |
   |                 OSS/BSS                   |  | | NFV          |   |
   +-------------------------------------------+  | | Orchestrator +-- |
                                                  | ---+------------ | |
   +-------------------------------------------+  |    |             | |
   |  ---------     ---------     ---------    |  |    |             | |
   |  | EM 1  |     | EM 2  |     | EM 3  |    |  |    |             | |
   |  ----+----     ----+----     ----+----    |  | ---+----------   | |
   |      |             |             |        |--|-|    VNF     |   | |
   |  ----+----     ----+----     ----+----    |  | | manager(s) |   | |
   |  | VNF 1 |     | VNF 2 |     | VNF 3 |    |  | ---+----------   | |
   |  ----+----     ----+----     ----+----    |  |    |             | |
   +------|-------------|-------------|--------+  |    |             | |
          |             |             |           |    |             | |
   +------+-------------+-------------+--------+  |    |             | |
   |         NFV Infrastructure (NFVI)         |  |    |             | |
   | -----------    -----------    ----------- |  |    |             | |
   | | Virtual |    | Virtual |    | Virtual | |  |    |             | |
   | | Compute |    | Storage |    | Network | |  |    |             | |
   | -----------    -----------    ----------- |  | ---+------       | |
   | +---------------------------------------+ |  | |        |       | |
   | |         Virtualization Layer          | |--|-| VIM(s) +-------- |
   | +---------------------------------------+ |  | |        |         |
   | +---------------------------------------+ |  | ----------         |
   | | -----------  -----------  ----------- | |  |                    |
   | | | Compute |  | Storage |  | Network | | |  |                    |
   | | | hardware|  | hardware|  | hardware| | |  |                    |
   | | -----------  -----------  ----------- | |  |                    |
   | |          Hardware resources           | |  |  NFV Management    |
   | +---------------------------------------+ |  | and Orchestration  |
   +-------------------------------------------+  +--------------------+
```

Figure 2: ETSI NFV reference architecture

## 4. Multi-domain problem statement

Market fragmentation results from having a multitude of telecommunications network and cloud operators each with a footprint focused to a specific region. This makes it difficult to deploy cost effective infrastructure services, such as virtual connectivity or compute resources, spanning multiple countries as no single operator has a big enough footprint. Even if operators largely aim to provide the same infrastructure services (VPN connectivity, compute resources based on virtual machines and block storage), inter-operator collaboration tools for providing a service spanning several administrative boundaries are very limited and cumbersome. This makes service development and provisioning very time consuming. For example, having a VPN with end-points in several countries, in order to connect multiple sites of a business (such as a hotel chain), requires contacting several network operators. Such an approach is possible only with significant effort and integration work from the side of the business. This is not only slow, but also inefficient and expensive, since the business also needs to employ networking specialists to do the integration instead of focusing on its core business

Technology fragmentation also represents a major bottleneck internally for an operator. Different networks and different parts of a network may be built as different domains using separate technologies, such as optical or packet switched (with different packet switching paradigms included); having equipment from different vendors; having different control paradigms, etc. Managing and integrating these separate technology domains requires substantial amount of effort, expertise, and time. The associated costs are paid by both network operators and vendors alike, who need to design equipment and develop complex integration features. In addition to technology domains, there are other reasons for having multiple domains within an operator, such as, different geographies, different performance characteristics, scalability, policy or simply historic (e.g., result of a merge or an acquisition). Multiple domains in a network are a necessary and permanent feature however, these should not be a roadblock towards service development and provisioning, which should be fast and efficient.

A solution is needed to deal with both the multi-operator collaboration issue, and address the multi-domain problem within a single network operator. While these two problems are quite different, they also share a lot of common aspects and can benefit from having a number of common tools to solve them.

## 5. Multi-domain architectural approaches

This section summarizes different architectural options that can be considered to tackle the multi-domain orchestration problem.

### 5.1. ETSI NFV approaches

Recently, the ETSI NFV ISG has started to look into viable architectural options supporting the placement of functions in different administrative domains. In the document [etsi_nvf_ifa009], different approaches are considered, which we summarize next.

The first option (shown in Figure 3) is based on a split of the NFVO into Network Service Orchestrator (NSO) and Resource Orchestrator (RO). A use case that this separation could enable is the following:

a network operator offering its infrastructure to different departments within the same operator, as well as to a different network operator like in cases of network sharing agreements.  In this scenario, an administrative domain can be defined as one or more data centers and VIMs, providing an abstracted view of the resources hosted in it.

A service is orchestrated out of VNFs that can run on infrastructure provided and managed by another Service Provider.  The NSO manages the lifecycle of network services, while the RO provides an overall view of the resources present in the administrative domain to which it provides access and hides the interfaces of the VIMs present below it.

```
                             -------
                             | NSO |
                            /-------\
                           /         \
               --------   /  -------- \    --------
               | VNFM |   |  | VNFM |  |   | VNFM |
               --------  /   --------   \  --------
                  / ____/      /  \      \____ \
                 / / _________/    \_________ \ \
                / / /                        \ \ \
   +-----------/-/-/---------+     +----------\-\-\----------+
   |        ---------        |     |        ---------        |
   |        |  RO   |        |     |        |  RO   |        |
   |        ---------        |     |        ---------        |
   |       /    |    \       |     |       /    |    \       |
   |      /     |     \      |     |      /     |     \      |
   |     /      |      \     |     |     /      |      \     |
   | ------- ------- ------- |     | ------- ------- ------- |
   | |VIM 1| |VIM 2| |VIM 3| |     | |VIM 1| |VIM 2| |VIM 3| |
   | ------- ------- ------- |     | ------- ------- ------- |
   | Administrative domain A |     | Administrative domain B |
   +-------------------------+     +-------------------------+
```

Figure 3: Infrastructure provided using multiple administrative domains (from ETSI GS NFV-IFA 009 V1.1.1)

The second option (shown in Figure 4) is based on having an umbrella NFVO.  A use case enabled by this is the following: a Network Operator offers Network Services to different departments within the same operator, as well as to a different network operator like in cases of network sharing agreements.  In this scenario, an administrative domain is compose of one or more Datacentres, VIMs, VNFMs (together with their related VNFs) and NFVO, allowing distinct specific sets of network services to be hosted and offered on each.

A top Network Service can include another Network Service. A Network Service containing other Network Services might also contain VNFs. The NFVO in each admin domain provides visibility of the Network Services specific to this admin domain. The umbrella NFVO is providing the lifecycle management of umbrella network services defined in this NFVO. In each admin domain, the NFVO is providing standard NFVO functionalities, with a scope limited to the network services, VNFs and resources that are part of its admin domain.

```
                           ------------
                           | Umbrella |
                           |   NFVO   |
                           ------------
                              / |  \
                            /   |    \
                           / -------- \
                          /  | VNFM |  \
                        /    --------    \
                       /        |         \
                     /       -------        \
                    /        |VIM 1|         \
                  /          -------           \
   --------------/------------     -------------\-------------
   |        --------          |    |        --------          |
   |        | NFVO |          |    |        | NFVO |          |
   |        --------          |    |        --------          |
   |           | | |          |    |           | | |          |
   | -------- | | | -------- |     | -------- | | | -------- |
   | | VNFM | | | | | VNFM | |     | | VNFM | | | | | VNFM | |
   | -------- | | | -------- |     | -------- | | | -------- |
   |   |  \__/__|__\_/_   |  |     |   |  \__/__|__\_/_   |  |
   |   |  __/___|___/\ \  |  |     |   |  __/___|___/\ \  |  |
   |   | / /    |     \ \ |  |     |   | / /    |     \ \ |  |
   | ------- ------- ------- |     | ------- ------- ------- |
   | |VIM 1| |VIM 2| |VIM 3| |     | |VIM 1| |VIM 2| |VIM 3| |
   | ------- ------- ------- |     | ------- ------- ------- |
   | Administrative domain A |     | Administrative domain B |
   +-------------------------+     +-------------------------+
```

Figure 4: Network services provided using multiple administrative domains (from ETSI GS NFV-IFA 009 V1.1.1)

More recently, ETSI NFV has released a new whitepaper, titled "Network Operator Perspectives on NFV priorities for 5G" [etsi_nvf_whitepaper_5g], which provides network operator perspectives on NFV priorities for 5G and identifies common technical features in terms of NFV. This whitepaper identifies multi-site/ multi-tenant orchestration as one key priority. ETSI highlights the support of Infrastructure as a Service (IaaS), NFV as a Service (NFVaaS) and Network Service (NS) composition in different administrative domains (for example roaming scenarios in wireless networks) as critical for the 5G work.

In January 2018 ETSI NFV released a report about NFV MANO architectural options to support multiple administrative domains [etsi_nvf_ifa028]. This report presents two use cases: the NFVI as a Service (NFVIaaS) case, where a service provider runs VNFs inside an NFVI operated by a different service provider, and the case of Network Services (NS) offered by multiple administrative domains, where an organization uses NS(s) offered by another organization.

In the NFVIaaS use case, the NFVIaaS consumer runs VNF instances inside an NFVI provided by a different service provider, called NFVIaaS provider, that offers computing, storage, and networking resources to the NFVIaaS consumer. Therefore, the NFVIaaS consumer has the control on the applications that run on the virtual resources, but has not the control of the underlying infrastructure, which is instead managed by the NFVIaaS provider. In this scenario, the NFVIaaS provider’s domain is composed of one or more NFVI-PoPs and VIMs, while the NFVIaaS consumer’s domain includes one or more NSs and VNFs managed by its own NFVO and VNFMs, as depicted in Figure 5.

```
   +------------------------------------------------+
   |    NFVIaaS consumer’s administrative domain    |
   |                                                |
   |  +----------+                                  |
   |  |   NS(s)  |                                  |
   |  +----------+                                  |
   |                                                |
   |  +----------+   +----------+   +----------+    |
   |  |  VNF(s)  |   | VNFM(s)  |   |   NFVO   |    |
   |  +----------+   +----------+   +----------+    |
   |                                                |
   +-------------------------+----------------------+
                             +
    Administrative domain    +
   ++++++++++++++++++++++++++++++++++++++++++++++++++
    boundary                 + NFVIaaS
                             +
   +-------------------------+----------------------+
   |                                                |
   |  +----------+   +-----------+                  |
   |  |  NFVI    |   |   VIM(s)  |                  |
   |  +----------+   +-----------+                  |
   |                                                |
   +------------------------------------------------+
```

Figure 5: NFVI use case

The ETSI IFA 028 defines two main options to model the interfaces between NFVIaaS provider and consumer for NFVIaaS service requests, as follows:

1. Access to Multiple Logical Points of Contacts (MLPOC) in the NFVIaaS provider’s administrative domain. In this case the NFVIaaS consumer has visibility of the NFVIaaS provider’s VIMs and it interacts with each of them to issue NFVIaaS service requests, through Or-Vi (IFA 005) or Vi-Vnfm (IFA 006) reference points.

2. Access to a Single Logical Point of Contact (SLPOC) in the NFVIaaS provider’s administrative domain. In this case the NFVIaaS provider’s VIMs are hidden from the NFVIaaS consumer and a single unified interface is exposed by the SLPOC to the NFVIaaS consumer. The SLPOC manages the information about the organization, the availability and the utilization of the infrastructure resources, forwarding the requests from the NFVIaaS consumer to the VIMs. The interaction between SLPOC and NFVIaaS consumer is based on IFA 005 or IFA 006 interfaces, while

the interface between the SLPOC and the underlying VIMs is based on the IFA 005.

The two options are shown in Figure 6 and Figure 7 respectively, where we assume the direct mode for the management of VNF resources. In addition, the ETSI IFA 028 includes the possibility of an indirect management mode of the VNF resources through the consumer NFVIaaS NFVO and the IFA 007 interface.  In this latter case between the consumer NFVIaaS NFVO and the provider NFVIaaS NFVO only the IFA 005 interface is utilized.

```
        +------------------------------------------------+
        |    NFVIaaS consumer’s administrative domain    |
        |                                                |
        |  +-----------+               +------------+    |
        |  |   VNFM    |---+           |   NFVO     |    |
        |  +-+---------+   |---+       +-+--+-------+    |
        |    + +-+---------+   |        +   +            |
        |    +   + +----+----+-+       +    +            |
        |    +   +     +     +        +    +             |
        +----+---+----+------+-------+----+--------------+
             +   +    +      +      +    +
   IFA 006 --+---+---+-------+--  --+----+-- IFA 005
             +   +  +        +     +    +
        +----+---+--+--------+----+----+-----------------+
        |    +   +  +   ++++++++++    +                  |
        |  +-+---+--+-+ +    +       +                   |
        |  |   VIM    |-+-+  +      +                    |
        |  +----------+   |--+-+   +                     |
        |      +----------+    ++++                      |
        |          |    VIM    |                         |
        |          +-----------+                         |
        |    NFVIaaS provider’s administrative domain    |
        +------------------------------------------------+
```

Figure 6: NFVIaaS architecture: MLPOC option

```
     +------------------------------------------------+
     |    NFVIaaS consumer’s administrative domain    |
     |                                                |
     |  +-----------+               +------------+    |
     |  |   VNFM    |---+           |   NFVO     |    |
     |  +-+---------+   |---+       +-+----------+    |
     |    + +-----------+   |        +                |
     |    +     |   VNFM    |        +                |
     |     +    +---------+-+       +                 |
     |      +             +        +                  |
     +-------+------------+-------+-------------------+
              +           +      +
IFA 006 -------+----------+--  --+-- IFA 005
                +         +     +
     +-----------+--------+----+----------------------+
     |            +       +   +                       |
     |         +---+------+--+--+                     |
     |         | SLPOC function |                     |
     |         +-+---+---+------+                     |
     |          +    +   +                            |
     |      ---+-----+---+--- IFA 005                 |
     |        +      +   +                            |
     |  +----+-----+ +   +                            |
     |  |   VIM    |-+-+ +                            |
     |  +----------+   |-+-+                          |
     |      +----------+   |                          |
     |          |   VIM    |                          |
     |          +----------+                          |
     |    NFVIaaS provider’s administrative domain    |
     +------------------------------------------------+
```

Figure 7: NFVIaaS architecture: SLPOC option

In the use case related to Network Services provided using multiple administrative domains, each domain includes an NFVO and one or more NFVI PoPs, VIMs and VNFMs.  The NFVO in each domain offers a catalogue of Network Services that can be used to deploy nested NSs, which in turn can be composed into composite NSs, as shown in Figure 8.  Nested NSs can be also shared among different composite NSs.

```
                |
     ***********+***************************************
     *          |                                      *
     *  +-------+------+                               *
     *  |              |                               *
   --+--+ Nested NS A  +-------+                       *
     *  |              |       +--------+              *
     *  +-------+------+                |              *
     *          |                       |              *
     *          |                 +-----+--------+     *
     *          |                 |              |     *
     *          +-----------------+ Nested NS B  +-----+---
     *                            |              |     *
     *                            +-------+------+     *
     *        Composite NS C              |            *
     *                                    |            *
     *************************************+*************
                                          |
```

Figure 8: Composite and nested NSs

The management of the NS hierarchy is handled through a hierarchy of NFVOs, with one of them responsible for the instantiation and lifecycle management of the composite NS, coordinating the actions of the other NFVOs that manage the nested NSs.  These two different kinds of NFVOs interact through a new reference point, named Or-Or, as shown in Figure 9, where NFVO-1 manages composite NSs and NFVO-2 manages nested NSs.  To build the composite NSs, the responsible NFVO consult its own catalogue and may subscribe to the NSD notifications sent by other NFVOs.

```
            +---------------------------------------------+
            |                                             |
            |                             +-------------+ |
            |                       +++++++   VNFM1-1   | |
            |    +-----------+     +      +-------------+ |
            |    |  NFVO-1   ++++++                       |
            |    +---+-------+     +      +-------------+ |
            |        +              +++++++   VNFM1-2   | |
            |        +                    +-------------+ |
            |        +    Administrative domain C         |
            +--------+------------------------------------+
                     +
                     +
                     +   Or-Or
                     +
            +--------+------------------------------------+
            |        +                                    |
            |        +                    +-------------+ |
            |        +              +++++++   VNFM2-1   | |
            |    +---+-------+     +      +-------------+ |
            |    |  NFVO-2   ++++++                       |
            |    +-----------+     +      +-------------+ |
            |                       +++++++   VNFM2-2   | |
            |                             +-------------+ |
            |             Administrative domain A         |
            +---------------------------------------------+
```

Figure 9: Architecture for management of composite and nested NS

## 5.2. Hierarchical

Considering the potential split of the NFVO into a Network Service Orchestrator (NSO) and a Resource Orchestrator (RO), multi-provider hierarchical interfaces may exist at their northbound APIs.
Figure 10 illustrates the various interconnection options, namely:

E/NSO (External NSO): an evolved NFVO northbound API based on Network Service (NS).

E/RO (External RO): VNF-FG oriented resource embedding service. A received VNF-FG that is mapped to the northbound resource view is embedded into the distributed resources collected from southbound, i.e., VNF-FG_in = VNF-FG_out_1 + VNF-FG_out_2 + ... + VNF-FG_out_N, where VNF-FG_out_j corresponds to a spatial embedding to subordinate domain "j". For example, Provider 3’s MP-NFVO/RO creates VNF-FG corresponding to its E/RO and E/VIM sub-domains.

E/VIM (External VIM): a generic VIM interface offered to an external consumer. In this case the NFVI-PoP may be shared for multiple consumers, each seeing a dedicated NFVI-PoP. This corresponds to IaaS interface.

I/NSO (Internal NSO): if a Multi-provider NSO (MP-NSO) is separated from the provider’s operational NSO, e.g., due to different operational policies, the MP-NSO may need this interface to realize its northbound E/NSO requests. Provider 1 illustrates a scenario the MP-NSO and the NSO are logically separated. Observe that Provider 1’s tenants connect to the NSO and MP-NSO corresponds to "wholesale" services.

I/RO (Internal RO): VNF-FG oriented resource embedding service. A received VNF-FG that is mapped to the northbound resource view is embedded into the distributed resources collected from southbound, i.e., VNF-FG_in = VNF-FG_out_1 + VNF-FG_out_2 + ... + VNF-FG_out_N, where VNF-FG_out_j corresponds to a spatial embedding to subordinate domain "j". For example, Provider 1’s MP-NFVO/RO creates VNF-FG corresponding to its I/RO and I/VIM sub-domains.

I/VIM (Internal VIM): a generic VIM interface at an NFVI-PoP.

Nfvo-Vim: a generic VIM interface between a (monolithic) NFVO and a VIM.

Some questions arise from this. It would be good to explore use-cases and potential benefits for the above multi-provider interfaces as well as to learn how much they may differ from their existing counterparts. For example, are (E/RO, I/RO), (E/NSO, I/NSO), (E/VIM, I/VIM) pairs different?

```
                                             Tenants
                             *    Provider      |
      *                       *   Domain 4   +--+-----------+
       *                       *             |MP-NFVO/NSO:  |
        *                       *            |Network Serv. |
         *   Provider            *           |Orchestrator  |
          *  Domain 3             *          +--+-----------+
           *              Tenants  *            |E/RO
            *                |      ************|*************
             *              ++-------------+    |
              *             |MP-NFVO/NSO:  |    |
      Provider *            |Network Serv. |    |
      Domain 1  *           |Orchestrator  |    |
                 *          +-+-----+------+    |
                  *      E/NSO|     | I/RO     /
                   *.---------'   +-+---------+--+
                   /*             |MP-NFVO/RO:   |
                  /  *            |Resource      |
   Tenants       /    *           |Orchestrator  |
   |             |     *          +--+---+-------+
   | +-----------+--+   *************|***|********************
   | |MP-NFVO/NSO:  |                |  * \          Provider
   | |Network Serv. |         E/RO  /   *  \ E/VIM    Domain 2
   | |Orchestrator  |  .-----------'    *   '-------.
   | +-+------+-----+  |                *           |
   |   |I/NSO |I/RO    |                *           |
   |   |   +--+--------+--+             *           |
   |   |   |MP-NFVO/RO:   |             *           |
   |   |   |Resource      |             *           |
    \  |   |Orchestrator  |             *    +------+-------+
     \ |   +----+---- --+-+             *    |VIM:          |
    +--+-----+  |I/RO   |I/VIM          *    |Virtualized   |
    |NFVO/NSO|  |       |               *    |Pys mapping   |
    +------+-+  |       |               *    +--------------+
       I/RO|    |       |               *
    +------+----+---+   |               *
    |    NFVO/RO    |   |               *
    ++-------------++   |               *
     |Nfvo-Vim     |    |               *
    ++-------+    ++----+--+            *
    |WIM|VIM ||   |VIM|WIM |            *
    +--------+|   +--------+            *
     +--------+                         *
```

Figure 10: NSO-RO Split: possible multi-provider APIs - an illustration

## 5.3. Cascading

Cascading is an alternative way of relationship among providers, from the network service point of view. In this case, service decomposition is implemented in a paired basis. This can be extended in a recursive manner, then allowing for a concatenation of cascaded relations between providers.

As a complement to this, from a service perspective, the cascading of two remote providers (i.e., providers not directly interconnected) could require the participation of a third provider (or more) facilitating the necessary communication among the other two. In that sense, the final service involves two providers while the connectivity imposes the participation of more parties at resource level.

## 6. Virtualization and Control for Multi-Provider Multi-Domain

Orchestration operation in multi-domain is somewhat different from that in a single domain as the assumption in single domain single provider orchestration is that the orchestrator is aware of the entire topology and resource availability within its domain as well as has complete control over those resources. This assumption of technical control cannot be made in a multi domain scenario, furthermore the assumption of the knowledge of the resources and topologies cannot be made across providers. In such a scenario solutions are required that enable the exchange of relevant information across these orchestrators. This exchange needs to be standardized as shown in Figure 11.

```
                   |                               |
                   + IF1                           +
              _____|____                       ____|_____
             |   Multi  |        IF2          |   Multi  |
             | Provider |<--------+---------->| Provider |
             |___Orch___|                     |___Orch___|
                  /\                               /\
                 /  \                             /  \
                /    \ IF3                       /    \
        _______/__   _\_________        ________/_    _\________
       |  Domain  | |  Domain  |       |  Domain  |  |  Domain  |
       |___Orch___| |___Orch___|       |___Orch___|  |___Orch___|
```

Figure 11: Multi Domain Multi Provider reference architecture

The figure shows the Multi Provider orchestrator exposing an interface 1 (IF1) to the tenant, interface 2 (IF2) to other Multi Provider Orchestrator (MPO) and an interface 3 (IF3) to individual domain orchestratrators. Each one of these interfaces could be a possible standardization candidate. Interface 1 is exposed to the tenant who could request his specific services and/or slices to be deployed. Interface 2 is between the orchestrator and is a key interface to enable multi-provider operation. Interface 3 focuses on abstracting the technology or vendor dependent implementation details to support orchestration.

The proposed operation of the MPO follows three main technical steps. First, over interface 2 various functions such as abstracted topology discovery, pricing and service details are detected. Second, once a request for deploying a service is received over interface 1 the Multi Provider Orchestrator evaluates the best orchestrators to implement parts of this request. The request to deploy these parts are sent to the different domain orchestrators over IF2 and IF3 and the acknowledgement that these are deployed in different domain are received back over those interfaces. Third, on receipt of the acknowledgement the slice specific assurance management is started within the MPO. This assurance function collects the appropriate information over IF2 and IF3 and reports the performance back to the tenant over IF1. The assurance is also responsible for detecting any failures in the service and violations in the SLA and recommending to the orchestration engine the reconfiguration of the service or slice which again needs to be performed over IF2 and IF3.

Each of the three steps is assigned to a specific block in our high level architecture shown in Figure 12.

```
                   |                                    |
                   + IF1                                +
     ______________|______________                  ____|_____
    |      Multi Provider Orch    |                |  Multi   |
    | ______   ________   _______ |<------+------->| Provider |
    ||Assur-| |        | | Catal-||      IF2      |___Orch___|
    ||-ance | |  NFVO  | | logue ||
    || Mgmt.| |        | | Topo. ||
    ||______| |________| |_Mgmt._||
    |_____________________________|
                  /\
                 /  \ IF3
```

Figure 12: Detailed MPO reference architecture

The catalogue and topology management system is responsible for step 1. It discovers the service as well as the resources exposed by the other domains both on IF2 and IF3. The combination of these services with coverage over the detected topology is provided to the user over IF1. In turn the catalogue and topology management system is also responsible for exposing the topology and service deployment capabilities to the other domain.  The exposure over interface 2 to other MPO maybe abstracted and the mapping of this abstracted view to the real view when requested by the NFVO.

The NFVO (Network Function Virtualization Orchestrator) is responsible for the second step.  It deploys the service or slice as is received from the tenant over IF2 and IF3.  It then hands over the deployment decisions to the Assurance management subsystem which use this information to collect the periodic monitoring tickets in step 3.  On the other end it is responsible for receiving the request over IF2 to deploy a part of the service, consult with the catalogue and topology management system on the translation of the abstraction to the received request and then for the actual deployment over the domains using IF3.  The result of this deployment and the management and control handles to access the deployed slice or service is then returned to the requesting MPO.

The assurance management component periodically studies the collected results to report the overall service performance to the tenant or the requesting MPO as well as to ensure that the service is functioning within the specified parameters.  In case of failures or violations the Assurance management system recommends reconfigurations to the NFVO.

## 6.1.  Interworking interfaces

In this section we provide more details on the interworking interfaces of the MPO reference architecture.  Each interface IF1, IF2 and IF3 is broken down into several sub-interfaces.  Each of them has a clear scope and functionality.

For multi provider Network Service orchestration, the Multi-domain Orchestrator (MdO) offers Network Services by exposing an OSS/BSS - NFVO interface to other MPOs belonging to other providers.  For multi-provider resource orchestration, the MPO presents a VIM-like view and exposes an extended NFVO - VIM interface to other MPOs.  The MPO exposes a northbound sub-interface (IF1-S) through which an MPO customer sends the initial request for services.  It handles command and control functions to instantiate network services.  Such functions include requesting the instantiation and interconnection of Network Functions (NFs).  A sub-interface IF2-S is defined to perform similar operations between MPOs of different administrative domains. A set of sub-interfaces -- IF3-R and IF2-R -- are used to keep an updated global view of the underlying infrastructure topology exposed by domain orchestrators.  The service catalogue exposes available services to customers on a sub-interface IF1-C and to other MPO service operators on sub-interface IF2-C.  Resource orchestration related interfaces are broken up to IF2-RC, IF2-RT, IF2-RMon to reflect resource control, resource topology and resource monitoring respectively. Furthermore, the sub-interfaces introduced before are generalised and also used for interfaces IF3 and IF1.

## 6.2. 5GEx Multi Architecture

The 5G-PPP H2020 5GEx projects addresses the proposal and the deployment of a complete Multi-Provider Orchestrator providing, besides network and service orchestration, service exposition to other providers. The main assumptions of the 5GEx functional architecture are a) a multi-operator wholesale relationship, b) a full multi-vendor inter-operability and c) technology-agnostic approach for physical resources. The proposed functional architecture of the 5GEx MPO is depicted in Figure 13.

```
                         ^                          ^
                    I1-S |                          |
                    I1-F |                     I1-C |
                    I1-RM|                          |
   +----------------------------------------------------+
   |          +-------------------------------------|--+|
   |          |          |                          |  ||     I2-S
   |          | +--------------------+              |  ||     I2-F
   |+---+     | | +-----+ +---+ IP-  |              |  ||     I2-RC
   ||OSS|<----|-| | NSO | |RO | NFVO +<-------------|--+|-------------->
   |+---+     | | +-----+ +---+      |<-------------+  ||
   |  ^       | +---^----------------+              |  ||
   |  |       |     |     ^ ^    ^^ ^               |  ||
   |  |       | +---+---+ | |    || |               |  ||
   |  +---------| VNF   | | |    || |  Multi-       |  ||
   |          | |Manager| | |    || |  Provider     |  ||
   |          | ++------+ | |    || |  Orchestrator |  ||
   |          |  ^        | |    || |  (MPO)        |  ||
   |          |  +--------+ |    || |               |  ||
   |          |  |     +-------+ || |               |  ||    I2-Mon
   |          |  |     |SLA    |<-|-|---------------|--+|-------------->
   |          |  |     |Manager| || |               |  ||
   |          |  |     +-------+ || |               |  ||
   |          |  |       ^       || +------------+  |  ||I2-RT-advertise
   |          |  |       |       || |Topology    |  |  ||I2-RT-bilateral
   |          |  |       |       || |Distribution|<-|--+|-------------->
   |          |  |       |       || |Repository  |  |  ||
   |          |  |       |       || +--------^+--+  |  ||
   |          |  |       |       ||   ^      ||     |  ||
   |          |  |       |       ||   |  +---+v-+   |  ||I2-RC-network
   |          |  |       |       |+---|--+MD-PCE|<--|--+|-------------->
   |          |  |       |       |    |  +------+   |  ||
   |          |  |       |       |    |   ^ +-------+-+||I2-C-advertise
   |          |  |       |       |    |   | |Service  |||I2-C-bilateral
   |          |  |       |       |    |   | |Catalogue+<|-------------->
   |          |  |       |       |    |   | +---------+||
   |          |  |       |       |    |   |      ^     ||
   |          +--|----- -|-------|----|---|------|-----+|
   |             |       |            |   |      |      |
   |             |I3-RC  |   I3-S|    |   |I3-RC-network|
   |          +--+--+    |   +----+   | +---+    |      |
   |          | VIM |    |   |NFVO|   | |PCE|    |      |
   |          +-----+    |   +----+   | +---+    |      |
   |                     |            |          |      |
   |                     |       I3-RT|          |I3-C  |
   |              I3-Mon |     +------+----+ +---+-----+|
   |           +---------+-+   |Topology   | |Service  ||
   |Operator   | Monitoring|   |Abstraction| |Catalogue||
   |Domain     +-----------+   +-----------+ +---------+|
   +----------------------------------------------------+
```

Figure 13: 5GEx MPO functional architecture

Providers expose MPOs service specification API allowing OSS/BSS or external business customers to perform and select their requirements for a service. Interface I1-x is exploited as a northbound API for business client requests. Peer MPO-MPO communications implementing multi-operator orchestration operate with specific interfaces referred to as I2-x interfaces. A number of I2-based interfaces are provided for communication between specific MPO modules: I2-S for service orchestration, I2-RC for network resource control, I2-F for management lifecycle, I2-Mon for inter-operator monitoring messages, I2-RT for resource advertisement, I2-C for service catalogue exchange, I2-RC-network for the QoS connectivity resource control. Some I2 interfaces are bilateral, involving direct relationship between two operators, and utilized to exchange business/SLA agreements before entering the federation of inter-operator orchestrators. Each MPO communicates through a set of southbound interface, I3-x, with local orchestrators/controllers/VIM, in order to set/modify/release resources identified by the MPO or during inter-MPO orchestration phase. A number of I3 interfaces are defined: I3-S for service orchestration towards local NFVO, I3-RC for resource orchestration towards local VIM, I3-C towards local service catalogue, I3-RT towards local abstraction topology module, I3-RC-network towards local PCE or network controller, I3-Mon towards local Resource Monitoring agent. All the considered interfaces are provided to cover either flat orchestration or layered/hierarchical orchestration. The possibility of hierarchical inter-provider MPO interaction is enabled at a functional level, e.g., in the case of operators managing a high number of large administrative domains. The main MPO modules are the following:

The Inter-provider NFVO, including the RO and the NSO, implementing the multi-provider service decomposition

the VNF/Element manager, managing VNF lifecycle, scaling and responsible for FCAPS (Fault, Configuration, Accounting, Performance and Security management)

the SLA Manager, in charge of reporting monitoring and performance alerts on the service graph

the Service Catalogue, exposing available services to external client and operators

the Topology and Resource Distribution module and Repository, exchanging operators topologies (both IT and network resources) and providing abstracted view of the own operator topology

the Multi-domain Path Computation Element (PCE implementing inter-operator path computation to allow QoS-based connectivity serving VNF-VNF link).

The Inter-provider NVFO selects providers to be involved in the service chained request, according to policy-based decisions and resorting to Inter-Provider topologies and service catalogues advertised through interfaces I2-RT-advertise and I2-C-advertise, respectively. Network/service requests are sent to other providers using the I2-RC and I2-S interfaces, respectively. Policy enforcement for authorized providers running resource orchestration and lifecycle management are exploited through interfaces I2-RC and I2-F, respectively. The VNF/Element Manager is in charge of managing the lifecycle of the VNFs part of the services. More specifically, it is in charge to perform: the configuration of the VNFs, also in terms of security aspects, the fault recovery and the scaling according to their performance. The SLA Manager collects and aggregates quality measurement reports from probes deployed by the Inter-Provider NFVO as part of the service setup. Measurements results at the Manager represent aggregated results and are computed and stored utilizing the I2-Mon interface between Inter-Provider MPOs sharing the same service. Faults and alarms are moreover correlated to raise SLA violation to remote inter-provider MPOs and, optionally, to detect the source and the location of the violation, triggering service re-computation/rerouting procedures. The Service Catalogue stores information on network services and available VNFs and uses I2-C interfaces (either bilateral or advertised) to advertise and updating such offered services to other operators. To enable inter-provider service decomposition, multi-operator topology and peering relationships need to be advertised. Providers advertise basic inter-provider topologies using the I2-RT-advertse interface including, optionally, abstracted network resources, overall IT resource capabilities, MPO entry-point and MD-PCE IP address. Basic advertisement takes place between adjacent operators. These information are collected, filtered by policy rules and propagated hop-by-hop. In 5GEx, the I2-RT-advertise interfaces utilizes BGP-LS protocol. Moreover, providers establish point-to-point bilateral (i.e., direct and exclusive) communications to exchange additional topology and business information, using the I2-RT-bilateral interface. Service decomposition may imply the instantiation of traffic-engineered multi-provider connectivity, subject to constraints such as guaranteed bandwidth, latency or minimum TE metric. The multi-domain PCE (MD-PCE) receives the connectivity request from the inter-provider NFVO and performs inter-operator path computation to instantiate QoS-based connectivity between two VNFs (e.g., Label Switched Paths). Two procedures are run sequentially:

operators/domain sequence computation, based on the topology database, provided by Topology Distribution module, and on specific policies (e.g., business, bilateral),

per-operator connectivity computation and instantiation.

In 5GEx, MD-PCE is stateful (i.e., current connectivity information is stored inside the PCE) and inter-operator detailed computation is performed resorting to the stateful Backward Recursive PCE-based computation (BRPC) [draft-stateful-BRPC], deploying a chain of PCEP sessions among adjacent operators, each one responsible of computing and deploying its segment. Backward recursive procedure allows optimal e2e constrained path computation results.

### 6.3. 5G-TRANSFORMER Architecture

5G-TRANSFORMER project proposes a flexible and adaptable SDN/NFV-based design of the next generation Mobile Transport Networks, capable of simultaneously supporting the needs of various vertical industries with diverse range of requirements by offering customized slices. In this design, multi-domain orchestration and federation are considered as the key concepts to enable end-to-end orchestration of services and resources across multiple administrative domains.

The 5G-TRANSFORMER solution consists of three novel building blocks, namely:

1. Vertical Slicer (VS) as the common entry point for all verticals into the system. The VS dynamically creates and maps the

vertical services onto network slices according to their requirements, and manages their lifecycle. It also translates the vertical and slicing requests into ETSI defined NFV network services (NFV-NS) sent towards the SO. Here a network slice is deployed as a NFV-NS instance.

2. Service Orchestrator (SO). It offers service or resource orchestration and federation, depending on the request coming from the VS. This includes all tasks related with coordinating and offering to the vertical an integrated view of services and resources from multiple administrative domains. Orchestration entails managing end-to-end services or resources that were split into multiple administrative domains based on requirements and availability. Federation entails managing administrative relations at the interface between SOs belonging to different domains and handling abstraction of services and resources.

3. Mobile Transport and Computing Platform (MTP) as the underlying unified transport stratum, responsible for providing the resources required by the NFV-NS orchestrated by the SO. This includes their instantiation over the underlying physical transport network, computing and storage infrastructure. It also may (de)abstract de MTP resources offered to the SO.

The 5G-TRANSFROMER architecture is quite in line with the general Multi Domain Multi Provider reference architecture depicted in Figure 11. Its mapping to the reference architecture is illustrated in the figure below.

```
               _________                       _________
              |         |                     |         |
              |   VS    |                     |   VS    |
              |_________|                     |_________|
                   |                               |
                   + IF1                           +
               ____|____                       ____|____
              |         |        IF2          |         |
              |   SO    |<--------+---------->|   SO    |
              |_________|                     |_________|
                  /\                               /\
                 /  \                             /  \
                /    \ IF3                       /    \
         ______/__   _\_______           _______/_    _\_______
        |   MTP   | |   MTP   |         |   MTP   |  |   MTP   |
        |_________| |_________|         |_________|  |_________|
```

Figure 14: 5G-TRANSFORMER architecture mapped to the reference architecture

The MTP would be mapped to the individual domain orchestrators, which only provides the resource orchestration for the local administrative domain.  The role of the SO is the Multi Provider orchestrator (MPO) responsible for multi-domain service or resource orchestration and federation.  The operation of the SO follows three main technical steps handled by the three function components of the MPO shown in Figure 14, namely (i) the catalogue and topology management system; (ii) the NFVO (Network Function Virtualization Orchestrator); and the assurance management component.

Correspondingly, the interface between the SO and the VS (So-Vs) is the interface 1 (IF1), through which the VS requests the instantiation and deployment of various network services to support individual vertical service slices.  The interface between the SOs (So-So) of different domains is the interface 2 (IF2), enabling multi domain orchestration and federation operations.  The interface between the SO and the MTP (So-Mtp) is the interface 3 (IF3).  It, on the one hand, provides the SO the updated global view of the underlying infrastructure topology abstraction exposed by the MTP domain orchestrators, while on the other hand it also handles command and control functions to allow the SO request each MTP domain for virtual resource allocation.

In 5G-TRANSFOMER, a set of sub-interfaces have been defined for the So-Mtp, So-So and Vs-So interfaces.

### 6.3.1.  So-Mtp Interface (IF3)

This interface is based on ETSI GS-NFV IFA 005 and ETSI GS-NFV IFA 006 for the request of virtual resource allocation, management and monitoring.  Accordingly, the 5G-TRANSFORMER identified the following sub-interfaces at the level of So-Mtp interactions (i.e., IF3-x interfaces regulating MPO-DO interactions).

So-Mtp(-RAM).  It provides the Resource Advertisement Management (RAM) functions to allow updates or reporting about virtualized resources and network topologies in the MTP that will accommodate the requested NFVO component network services.

So-Mtp(-RM).  It provides the Resource Management (RM) operations over the virtualized resources used for reserving, allocating, updating (in terms of scaling up or down) and terminating (i.e., release) the virtualized resources handled by each MTP and triggered by NFVO component (in Figure 14) to accommodate network services.

So-Mtp(-RMM).  It provides the required primitives and parameters for supporting the SO resource monitoring management (RMM) capability for the purpose of fault management and SLA assurance handled by assurance management component in Figure 14.

In the reference architecture (Fig. 6), the IF3-RC, IF3-RT, IF3-RMon sub-interface are defined for resource control, resource topology and resource monitoring respectively. The IF3-RT, IF3-RC and IF3-RMon sub-interfaces map to So-Mtp(-RAM), So-Mtp(-RM) and So-Mtp(-RMM) sub-interfaces from 5G-TRANSFORMER.

### 6.3.2. So-So Interface (IF2)

This interface is based ETSI GS-NFV IFA 013 and ETSI GS-NFV IFA 005 for the service and resource federation between the domains. The 5G-TRANSFORMER identified the following sub-interfaces at the level of So-So interactions (i.e., IF2-x interfaces regulating MPO interactions) to provide service and resource federation and enable NSaaS and NFVIaaS provision, respectively, across different administrative domains.

So-So(-LCM), for the operation of NFV network services. The reference point is used to instantiate, terminate, query, update or re-configure network services or receive notifications for federated NFV network services. The SO NFVO-NSO uses this reference point.

So-So(-MON), for the monitoring of network services through queries or subscriptions/notifications about performance metrics, VNF indicators and network service failures. The SO NFVO-NSO uses this reference point.

So-So(-CAT), for the management of Network Service Descriptors (NSDs) flavors together with VNF/VA and MEC Application Packages, including their Application Descriptors (AppDs). This reference point offers primitives for on-boarding, removal, updates, queries and enabling/disabling of descriptors and packages. The SO NFVO-NSO uses this reference point.

Furthermore, resource orchestration related operations are broken up to the following sub-interfaces to reflect resource control, resource topology and resource monitoring respectively.

So-So(-RM), for allocating, configuring, updating and releasing resources. The Resource Management reference point offers operations such as configuration of the resources, configuration of the network paths for connectivity of VNFs. These operations mainly depend of the level of abstraction applied to the actual resources. The SO NFVO-RO uses this reference point.

So-So(-RMM), for monitoring of different resources, computing power, network bandwidth or latency, storage capacity, VMs, MEC hosts provided by the peering administrative domain. The details level depends on the agreed abstraction level. The SO NFVO-RO uses this reference point.

So-So(-RAM), for advertising available resource abstractions to/from other SOs. It broadcasts available resources or resource abstractions upon capability calculation and periodic updates for near real-time availability of resources. The SO-SO Resource Advertisement uses this reference point.

So-So(-RMM), for monitoring of different resources, computing power, network bandwidth or latency, storage capacity, VMs, MEC hosts provided by the peering administrative domain. The details level depends on the agreed abstraction level. The SO NFVO-RO uses this reference point.

In the reference architecture (Figure 11), the sub-interface IF2-S and IF2-C are defined to perform network service-related operations between MPOs of different administrative domains. The IF2-RC, IF2-RT, IF2-RMon sub-interfaces are defined to regulated interactions between Catalogue and Topology Management components. Their mapping to the sub-interfaces defined in 5G-TRANSFORMER are summarized as follows:

The IF2-S sub-interface maps to So-So(-LCM) and So-So(-MON).

The IF2-C sub-interface maps to So-So(-CAT).

The IF2-RC, IF2-RT, IF2-RMon sub-interfaces map to So-So-RM, So-So-RAM, So-So-RT respectively.

### 6.3.3. Vs-So Interface (IF1)

This interface is based on ETSI GS-NFV IFA 013 for the VS requesting network services from the SO. Accordingly, the 5G-TRANSFORMER identified the following sub-interfaces at the level of Vs-So interactions (i.e., IF1-x interfaces regulating tenant-MPO interactions).

Vs-So(-LCM). It deals with the NFV network service lifecycle management (LCM) and it is based on the IFA 013 NS Lifecycle Management Interface. It offers primitives to instantiate, terminate, query, update or re-configure network services or receive notifications about their lifecycle.

Vs-So(-MON). It deals with the monitoring (MON) of network services and VNFs through queries or subscriptions and notifications about performance metrics, VNF indicators and network services or VNFs failures. It maps to IF1-S sub-interface of the reference architecture.

Vs-So(-CAT). It deals with the catalogue (CAT) management of Network Service Descriptors (NSDs), VNF packages, including their VNF Descriptors (VNFDs), and Application Packages, including their Application Descriptors (AppDs). It offers primitives for on-boarding, removal, updates, queries and enabling/disabling of descriptors and packages. It maps to IF1-C sub-interface of the reference architecture.

In the reference architecture (Figure 11), the sub-interface IF1-S and IF1-C are defined to build request to perform network service-related operations including requesting the instantiation, update and termination of the requested network services. The IF1-S sub-interface maps to Vs-So(-LCM) and Vs-So(-MON), while the IF1-C sub-interface maps to Vs-So(-CAT) defined in 5G-TRANSFORMER architecture.

## 7. Multi-domain orchestration and Open Source

Before reviewing current state of the open source projects it should be explicitly mentioned that term "federation" is quite ambiguous and used in multiple contexts across the industry. For example, federation is the approach used at certain software projects to achieve high availability and enable reliable non-interrupted operation and service delivery. One of the distinguishing features of this federation type is that all federated instances are managing the same piece of the infrastructure or resources set. However, this document is focused on another federation type, where multiples independent instances of the orchestration/management software establish certain relationships and expose available resources and capabilities in the particular domain to consumers at another domain. Besides sharing resource details, multi-domain federation requires various management information synchronization, such authentication/authorization data, run-time policies, connectivity details and so on. This kind of functionality and appropriate implementation approaches at the relevant open source projects are in scope of current section.

At this moment several open source industry projects were formed to develop integrated NFV orchestration platform. The most known of them are ONAP [onap], OSM [osm] and Cloudify [cloudify]. While all these projects have different drivers, motivations, implementation approach and technology stack under the hood, all of them are considering multi-VIM deployment scenario, i.e. all these software platforms are capable to deploy NFV service over different virtualized infrastructures, like public or private providers. Additionally OSM and Cloudify orchestration platforms have capabilities to manage interconnection among managed VIMs using appropriate plugins or drivers. However, despite the fact that typical Telco/Carrier infrastructure has multiple domains (both technology and administrative), none of these orchestration projects is focused on a service federation use case development.

In the meantime, as an acknowledgement of the challenges, emerged during exploitation of the federation use cases Multisite project emerged under OPNFV umbrella [opnfv]. Considering OpenStack-based VIM deployments spanned across multiple regions as a general use case, this project initially was focusing on a gaps identification in the key OpenStack projects which lacks capabilities for multi-site deployment. During several development phases of this OPNFV project, number of gaps were identified and submitted as a blueprints for the development into the appropriate OpenStack projects. Further several demo scenarios were delivered to trial OpenStack as the open source VIM which is capable to support multisite NFV clouds. While Multisite OPNFV project was focusing on a resource and VIM layer only, there are multiple viable outputs which might be considered during implementation of the federation use cases on the upper layers.

As a summary it can be stated that it is still early days for the technology implemented in a referenced NFV orchestration projects and federation use case in not on a radar for these projects for the moment. However, it is expected that upon maturity of the federation as a viable market use case appropriate feature set in the reviewed projects will be developed.

## 8. IANA Considerations

N/A.

## 9. Security Considerations

TBD.

## 10. Acknowledgments

This work is supported by 5G-PPP 5GEx, an innovation action project partially funded by the European Community under the H2020 Program (grant agreement no. 671636). This work is also supported by 5G-PPP 5G-TRANSFORMER, a research and innovation action project partially funded by the European Community under the H2020 Program (grant agreement no. 761536). The views expressed here are those of the

authors only. The European Commission is not liable for any use that may be made of the information in this presentation.

## 11. Informative References

[cloudify]
"Cloudify", <https://cloudify.co/>.

[etsi_nvf_ifa009]
"Report on Architectural Options, ETSI GS NFV-IFA 009 V1.1.1", July 2016.

[etsi_nvf_ifa028]
"Report on architecture options to support multiple administrative domains, ETSI GR NFV-IFA 028 V3.1.1", January 2018.

[etsi_nvf_whitepaper]
"Network Functions Virtualisation (NFV). White Paper 2", October 2014.

[etsi_nvf_whitepaper_5g]
"Network Functions Virtualisation (NFV). White Paper on "Network Operator Perspectives on NFV priorities for 5G"", February 2017.

[ngmn_5g_whitepaper]
"5G White Paper", February 2015.

[ngmn_slicing]
"Description of Network Slicing Concept", January 2016.

[onap] "ONAP project", <https://www.onap.org/>.

[opnfv] "OPNFV Multisite project", <https://wiki.opnfv.org/display/multisite/Multisite>.

[osm] "Open Source MANO project", <https://osm.etsi.org/>.

## Authors’ Addresses

Carlos J. Bernardos (editor)
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid  28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI:   http://www.it.uc3m.es/cjbc/

Luis M. Contreras
Telefonica I+D
Ronda de la Comunicacion, S/N
Madrid  28050
Spain

Email: luismiguel.conterasmurillo@telefonica.com

Ishan Vaishnavi
Huawei Technologies Dusseldorf GmBH
Riesstrasse 25,
Munich  80992
Germany

Email: Ishan.vaishnavi@huawei.com

Robert Szabo
Ericsson
Konyves Kaman krt. 11
Budapest, EMEA  1097
Hungary

Phone: +36703135738
Email: robert.szabo@ericsson.com

Josep Mangues-Bafalluy
CTTC
Av. Carl Friecrish Gauss, 7
Castelldefels, EMEA  08860
Spain

Email: josep.mangues@cttc.cat

Xi Li
NEC
Kurfuersten-Anlage 36
Heidelberg  69115
Germany

Email: Xi.Li@neclab.eu

Francesco Paolucci
SSSA
Via Giuseppe Moruzzi, 1
Pisa  56121
Italy

Phone: +395492124
Email: fr.paolucci@santannapisa.it

Andrea Sgambelluri
SSSA
Via Giuseppe Moruzzi, 1
Pisa  56121
Italy

Phone: +395492132
Email: a.sgambelluri@santannapisa.it

Barbara Martini
SSSA
Via Giuseppe Moruzzi, 1
Pisa  56121
Italy

Email: barbara.martini@cnit.it

Luca Valcarenghi
SSSA
Via Giuseppe Moruzzi, 1
Pisa  56121
Italy

Email: luca.valcarenghi@santannapisa.it

Giada Landi
Nextworks
Via Livornese, 1027
Pisa  56122
Italy

Email: g.landi@nextworks.it

Dmitriy Andrushko
MIRANTIS

Email: dandrushko@mirantis.com

Alain Mourad
InterDigital Europe

Email: Alain.Mourad@InterDigital.com
URI:   http://www.InterDigital.com/