ETSI GR NFV-IFA 028 V3.1.1 (2018-01)

Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains

Disclaimer

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

Reference
DGR/NFV-IFA028

Keywords
architecture, management, MANO, NFV, orchestration

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document reports on potential architecture options to support the offering of NFV-MANO services across multiple administrative domains.

A set of use cases is described and analysed. The use case analysis includes:

- Interactions between functional blocks belonging to different administrative domains.
- Identification of the need for extensions and/or enhancements to NFV-MANO architecture to fulfil the use cases.

Recommendations for normative work are identified.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] ETSI GS NFV 001 (V1.1.1): "Network Functions Virtualisation (NFV); Use Cases".

[i.2] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for main concepts in NFV".

[i.3] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.4] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.5] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV); Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[i.6] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.7] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV); Management and Orchestration; Functional Requirements Specification".

[i.8] ETSI GS NFV-IFA 012: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Os-Ma-Nfvo reference point - Application and Service Management Interface and Information Model Specification".

[i.9] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV); Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification".

[i.10] ETSI GR NFV-IFA 022: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services".

[i.11] ETSI GR NFV-IFA 021: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on management of NFV-MANO and automated deployment of EM and other OSS functions".

[i.12] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification".

[i.13] ETSI GS NFV-IFA 027: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Performance Measurements Specification".

[i.14] ETSI GS NFV-SEC 004 (V1.1.1): "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications".

[i.15] ETSI GS NFV-SEC 010 (V1.1.1): "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".

[i.16] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.17] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.2] and the following apply.

An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GS NFV 003 [i.2].

LCM	LifeCycle Management
MLPOC	Multiple Logical Points Of Contact
NFVIaaS	NFVI as a Service
SLPOC	Single Logical Point Of Contact

4 Overview

4.1 Introduction

NFV-MANO services can be offered and consumed by different organizations, e.g. by different network operators or by different departments within the same network operator. Administrative domains as defined in ETSI GS NFV-IFA 010 [i.7] can be mapped to such different organizations.

Examples of use cases for NFV-MANO service offerings across multiple administrative domains are described in ETSI GS NFV 001 [i.1], e.g. NFVI as a Service (NFVIaaS) in which a service provider is able to run VNF instances inside an NFVI which is operated by a different service provider. Another use case example is Network Services (NS) offered by multiple administrative domains, in which an organization uses NS(s) offered by another organization, e.g. by a different network operator. This use case utilizes the concept of composite NS and nested NSs, as documented in ETSI GS NFV-IFA 012 [i.8].

Although the concept of administrative domains has already been described in ETSI GS NFV-MAN 001 [i.3], a more detailed study is required to identify, clarify and document the implications for the NFV-MANO architectural framework in order to support the offering of NFV-MANO services across multiple administrative domains.

Based on use cases, the present document analyses architecture options to support such NFV-MANO services offerings. Several architectural options can exist for a particular use case.

Implications to NS lifecycle management, VNF lifecycle management, and resource management for the different architecture options are studied and described, where applicable for a particular use case.

Simplified operational flows of the main operations for the different architecture options are documented when necessary in order to illustrate the different architectural options.

The study follows the guiding principles given below:

- Backwards compatibility with the existing NFV-MANO architectural framework is ensured.
- Existing NFV-MANO reference points and interfaces are reused as far as possible.

The following use cases are analysed in the present document:

- NFVIaaS.
- Network Services provided using multiple administrative domains.

The present document provides recommendations for enhancements of the NFV-MANO architecture framework resulting from the use case analysis.

4.2 Multi-domain operation

There are different options to enable the multi-domain operation as described in the present document. This basically defines how the providers become logically interconnected. The interconnection of administrative domains implies that some information is to be shared, like the IP address of the distinct functional blocks to be interconnected, the identifier of administrative domains to be interconnected, the administrative organization they pertain to, etc. The options are:

i) Configuration driven. In this option, the different functional blocks to be interconnected are statically configured with the necessary information to form the relation with the other parties.

ii) Auto-discovery. In this option, the different functional blocks advertise their own information and prepare the information to be used to form the relation. This form of interconnection assumes the implementation of a discovery mechanism in the NFV-MANO functional blocks.

All the options described before have security implications that have to be taken into account for the interaction between NFV-MANO functional blocks of different administrative domains. Security aspects are studied in ETSI GS NFV-IFA 026 [i.12].

In a general way, the logical interconnection among administrative domains assumes that the sessions established between NFV-MANO functional blocks counterparts can be maintained in order to ensure proper operation, e.g. by means of keep alive messages or any other mechanisms helpful to detect problems in the entities connected across administrative domains. Furthermore, the functional blocks detecting problems in the interconnection sessions can incorporate logic to react to such situation in order to increase system robustness. Monitoring and failure detection of NFV-MANO functional blocks is considered in ETSI GR NFV-IFA 021 [i.11].

It is also common in multi-domain operation to interchange information about the usage of resources in the different administrative domains, including monitoring information to ensure proper operation of the system. This kind of transactions should also be supported between NFV-MANO functional blocks involved, in order to ensure the SLAs defined between domains and to keep record of the resource utilization in external domains.
ETSI GR NFV-IFA 021 [i.11] presents cases for collecting performance data from NFV-MANO functional blocks.

Finally, interconnection option ii) requires the consideration of protocols for auto-discovery of NFV-MANO functional blocks from other administrative domains. These protocols would have to be supported on the interfaces between the functional blocks, but also the functional blocks would need to incorporate the logic for handling the auto-discovery procedures. The retrieval of information from NFV-MANO functional blocks is also studied in ETSI GR NFV-IFA 021 [i.11].

NOTE: The options described before are independent of the commercial relationship among providers.

5 Use case analysis: NFVI as a Service (NFVIaaS)

5.1 Use case description

This use case addresses a network operator offering of NFVI services. These NFVI services can be used to remotely deploy and run VNFs inside an NFVI provided as a service.

As described in ETSI GS NFV 001 [i.1] use case #1, NFVIaaS, a service provider (acts as NFVIaaS consumer) might want to be able to run VNF instances inside an NFVI which is provided as a service by a different service provider (acts as NFVIaaS provider). The NFVIaaS provider offers computing, storage, and networking resources to the NFVIaaS consumer. The NFVIaaS consumer can use the provided resources to run applications on which he has the control. The NFVIaaS consumer does not control the underlying infrastructure.

The NFVIaaS provider and the NFVIaaS consumer can be different network operators or different departments within the same network operator.

In this use case the NFVIaaS provider and the NFVIaaS consumer belong to different administrative domains, refer to figure 5.1-1. The NFVIaaS provider's administrative domain is regarded to be composed of one or more NFVI-PoPs and associated VIM management entities, providing an abstracted view of the resources hosted in it. The NFVIaaS consumer's administrative domain is regarded to be composed of one or more NSs and VNFs managed by the NFVO and its corresponding VNFMs, which consume the resources provided by NFVIaaS provider's administrative domain.

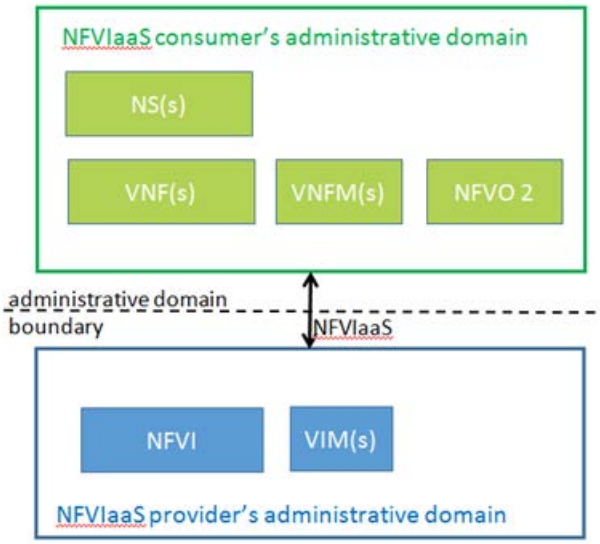

Figure 5.1-1: NFVIaaS use case

NOTE 1: This use case focuses on the interactions between the NFVIaaS provider and the NFVIaaS consumer and does not explore whether their administrative domains are further divided.

When crossing administrative domains interoperability and multi-vendor aspects need to be addressed, e.g. the involved functional blocks should have well-defined sets of responsibilities, reference points and interfaces.

The main split of responsibilities for NFVIaaS is as follows:

- The NFVIaaS provider controls the resources in his administrative domain. This includes:
  - Offer interfaces for resource management requests from NFVIaaS consumer(s).
  - Select NFVI resources according to NFVIaaS consumer's resource requests:
    - Placement decisions taking into account resource requirements and constraints from the NFVIaaS consumer, including topological information if needed.
    - It is expected that an SLA is in place between NFVIaaS provider and NFVIaaS consumer and that appropriate monitoring of resource usage is performed to enable SLA supervision. Capacity constraints and other limits can apply to resource allocation decisions.
  - Manage NFVI resources for use of several NFVIaaS consumers. This includes resource management, resource reservation, quota management, fault management and performance management.
  - Provide an overall view of the NFVI resources, like resource capabilities (e.g. capacity) and monitoring information (including usage). Each NFVIaaS consumer only gets information on NFVI resources related to his NFVI service.
  - Manage SW images for VNFs deployed on the NFVI based on input from NFVIaaS consumer.
- The NFVIaaS consumer controls the VNFs and NSs in his administrative domain and requests resources from the NFVIaaS provider to run VNFs and connect them to NSs. This includes:
  - Manage the lifecycle of VNFs and NSs. This includes management of VNF Packages, NSDs and granting of VNF LCM operations.
  - Request resources from the NFVIaaS provider to run VNFs and connect them to NSs. If applicable set NFVI quotas and/or reserve resources. Capacity constraints and other limits can apply to resource requests, quotas and resource reservations. It is expected that an SLA is in place between NFVIaaS provider and NFVIaaS consumer, addressing such capacity constraints and other limits.
  - Get information from the NFVIaaS provider about NFVI resources, e.g. capacity information, usage information, fault information, performance information. Each NFVIaaS consumer will only get information on NFVI resources related to his NFVI service.
  - Distribute SW images to the NFVIaaS provider for VNFs that will run on his NFVI.

Beside the pure NFVIaaS scenario where the NFVIaaS consumer deploys his VNFs and NSs on the NFVI of the NFVIaaS provider additional hosting scenarios are possible. This includes e.g. the following scenarios:

- An actor playing the NFVIaaS provider role can own VNFs and NSs that run on the same NFVI that is used for NFVIaaS consumers in different administrative domains. In that case, it also plays an NFVIaaS consumer role.
- An actor playing the role of NFVIaaS consumer can own an NFVI to run his VNFs and NSs. In that case, it also plays an NFVIaaS provider role. A NS can be combined from VNFs running on the own NFVI and VNFs running on another NFVIaaS provider's NFVI.

In the above cases the same actor plays both the role of an NFVIaaS consumer and the role of an NFVIaaS provider.

Different architecture options are possible with respect to which functional blocks and interfaces are exposed to NFVIaaS consumers in other administrative domains, e.g. having a single entry point for other administrative domains, allowing direct access to all VIMs, etc. In any case existing NFV environments need to be supported, e.g. VNFM using VNF-related resource management in direct mode or in indirect mode should be usable. The following clause elaborates on architecture options to support this use case.

NOTE 2: The use case description does not exclude scenarios in which a functional block can play a role in multiple administrative domains. However, those scenarios are not further addressed in the present document.

5.2 Potential architecture options

5.2.1 Overview

The NFV-MANO architecture framework as described in ETSI GS NFV-MAN 001 [i.3] builds the basis for the potential architecture options analysed in this clause in order to support the NFVIaaS use case.

In case of NFVIaaS interactions take place between the NFVIaaS provider and the NFVIaaS consumer and are supported via interfaces exposed by NFVIaaS provider and consumed by NFVIaaS consumer which are located in different administrative domains.

Multiple NFVIaaS consumers can use NFVIaaS of an NFVIaaS provider, multi-tenancy aspects need to be considered. Access to the NFVIaaS interfaces need to be controlled and NFVIaaS consumers need to be isolated from each other.

The NFVIaaS consumer issues NFVIaaS service requests towards the NFVIaaS provider in order to run his VNFs on the NFVIaaS provider's infrastructure and connect them to NSs. NFVIaaS service requests include, e.g. resource management, SW image management.

In the NFVIaaS use case multi-site connectivity and its management needs to be considered. Such multi-site connectivity aspects are studied and described in ETSI GR NFV-IFA 022 [i.10].

The NFVIaaS provider offers interfaces for the NFVIaaS service requests to the NFVIaaS consumer(s). Multiple interworking options are possible:

1) Access to Multiple Logical Points of Contacts (MLPOC) in the NFVIaaS provider's administrative domain is allowed for NFVIaaS service requests.

   In this case the NFVIaaS consumer has visibility of the NFVIaaS provider's VIMs and might need to interface with different VIM implementations and versions.

   Variants are:

   a) VNF-related resource management in direct mode is used.

   b) VNF-related resource management in indirect mode is used.

2) A Single Logical Point of Contact (SLPOC) to the NFVIaaS provider's administrative domain is used for NFVIaaS service requests.

   In this case the NFVIaaS provider's VIMs are hidden from the NFVIaaS consumer and unified interfaces are exposed by the SLPOC and offered to the NFVIaaS consumer.

   Variants are:

   a) VNF-related resource management in direct mode is used.

   b) VNF-related resource management in indirect mode is used.

NOTE: The MLPOC and SLPOC functions are not intended to create new functional blocks but are used for the purpose to describe the functionality. As described in clauses 5.2.2 and 5.2.3 the MLPOC functionality is provided by VIM. Refer to clause 5.2.7 for an analysis of integration options of SLPOC into NFV-MANO functional blocks.

The architecture options related to the different interworking options are described in clauses 5.2.2-5.2.5. Combinations of the architecture options are possible and are considered in clause 7.

5.2.2 Architecture option 1.a: Multiple logical points of contact, VNF related resource management in direct mode

This architecture option describes the case that the NFVIaaS provider allows access to multiple logical points of contact in his administrative domain. The NFVIaaS consumer issues NFVIaaS service requests using interfaces provided by the VIMs.

In this architecture option it is assumed that VIMs provide logical points of contact for virtualised resource management requests.

It is further assumed that NFVIaaS provider and NFVIaaS consumer have a business relationship. Before NFVIaaS requests can be issued, the NFVIaaS provider and the NFVIaaS consumer exchange information about infrastructure tenants, resource groups, and access to the VIMs.

VNF related resource management in direct mode is used in this architecture option, i.e. the VNFM invokes virtualised resource management operations on the VIM(s).

It is assumed that the existing interfaces of the reference points Or-Vi and Vi-Vnfm can be reused in this architecture option, refer to ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5]. Figure 5.2.2-1 illustrates this architecture option by focusing on the interactions between functional blocks belonging to different administrative domains.

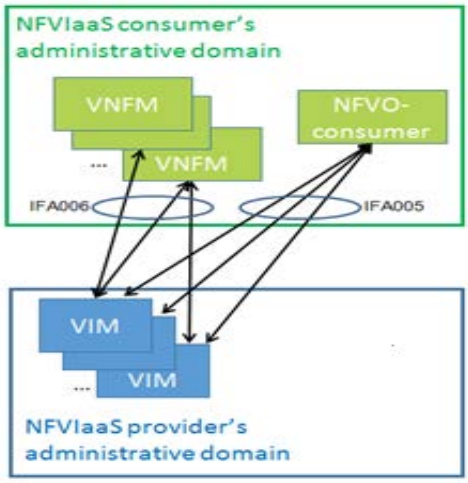

Figure 5.2.2-1: Illustration of NFVIaaS architecture option 1.a

NS management:

NFVO-consumer is responsible for NS lifecycle management, including the management of NSDs and VNF packages. NFVO-consumer manages the VNFFGs and VLs for NSs and issues network resource management operations towards the respective VIM(s).

VNF management:

The VNFMs are responsible for the VNF lifecycle management. Before executing the VNF lifecycle operation the VNFM requests an operation granting from NFVO-consumer. The granting decision can depend on e.g. operator policies, VNF dependencies and resource information. In the grant response NFVO-consumer provides the VNFM with information to enable the access to the VIM for VNF related resource management. The VNFMs request resource management operations needed for VNF LCM from the identified VIM(s).

The NFVO-consumer collects information on consumable resource and virtualised resources capacity from the VIMs. NFVO-consumer uses such information for identifying and selecting the target VIM(s) from which the virtualised resources will be provided for the VNF.

When an allowance model is used, the NFVO-consumer maintains and enforces permitted allowance at various granularity levels (VNFM, VNF, NS, etc.) in order to control resource consumption by VNFMs in relation with VNF lifecycle operation granting.

The NFVO-consumer cannot guarantee resource availability during the granting of a VNF lifecycle request if the resources needed to accommodate such lifecycle operation have not been reserved in the VIM.

NFVO-consumer performs VNF Package management and distributes the SW images of VNFs to the VIM(s) on which they will be deployed.

Virtualised resource management:

The VIMs are responsible for the management of the virtualised resources and provide interfaces to VNFMs and NFVO-consumer so that they can request operations for virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, and NFP management.

The VIMs manage infrastructure tenants and infrastructure resource groups and limit the scope of operations to the requesting infrastructure tenant (refer to ETSI GS NFV-IFA 010 [i.7]). This includes:

- The infrastructure tenant gets only information related to the infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only initiate virtualised resource management related to the infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only request quota related to infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only reserve virtualised resources belonging to infrastructure resource groups that are assigned to this infrastructure tenant.

5.2.3 Architecture option 1.b: Multiple logical points of contact, VNF related resource management in indirect mode

This architecture option describes the case that the NFVIaaS provider allows access to multiple logical points of contact in his administrative domain. The NFVIaaS consumer issues NFVIaaS service requests using interfaces provided by the VIMs.

In this architecture option it is assumed that VIMs provide logical points of contact for virtualised resource management requests.

It is further assumed that NFVIaaS provider and NFVIaaS consumer have a business relationship. Before NFVIaaS requests can be issued, the NFVIaaS provider and the NFVIaaS consumer exchange information about infrastructure tenants, resource groups, and access to the VIMs.

VNF related resource management in indirect mode is used in this architecture option, i.e. the VNFM invokes virtualised resource management operations on the NFVO-consumer and the NFVO-consumer in turn invokes them towards the VIM(s), refer to ETSI GS NFV-IFA 010 [i.7].

It is assumed that the existing interfaces of the reference points Or-Vi and Or-Vnfm can be reused in this architecture option, refer to ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 007 [i.6]. Figure 5.2.3-1 illustrates this architecture option.

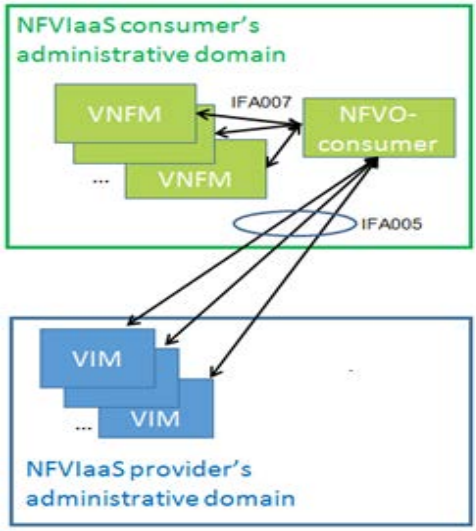

Figure 5.2.3-1: Illustration of NFVIaaS architecture option 1.b

NS management:

NFVO-consumer is responsible for NS lifecycle management, including the management of NSDs and VNF packages. NFVO-consumer manages the VNFFGs and VLs for NSs and issues network resource management operations towards the respective VIM(s).

VNF management:

The VNFMs are responsible for the VNF lifecycle management. Before executing the VNF lifecycle operation the VNFM requests an operation granting from NFVO-consumer. The granting decision can depend on e.g. operator policies, VNF dependencies and resource information. The VNFMs request resource management operations needed for VNF LCM from NFVO-consumer which issue the requests towards the VIM(s).

The NFVO-consumer collects information on consumable resource and virtualised resources capacity from the VIMs. NFVO-consumer uses such information for identifying and selecting the target VIM(s) from which the virtualised resources will be provided for the VNF.

When an allowance model is used the NFVO-consumer maintains and enforces permitted allowance at various granularity levels (VNFM, VNF, NS, etc.) in order to control resource consumption by VNFMs in relation with VNF lifecycle operation granting.

The NFVO-consumer cannot guarantee resource availability during the granting of a VNF lifecycle request if the resources needed to accommodate such lifecycle operation have not been reserved in the VIM.

NFVO-consumer performs VNF Package management and distributes the SW images of VNFs to the VIM(s) on which the VNF(s) will be deployed.

Virtualised resource management:

The VIMs are responsible for the management of the virtualised resources and provide interfaces to NFVO-consumer for requesting operations for virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, and NFP management.

The VIMs manage infrastructure tenants and infrastructure resource groups and limit the scope of operations to the requesting infrastructure tenant (refer to ETSI GS NFV-IFA 010 [i.7]). This includes:

- The infrastructure tenant gets only information related to the infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only initiate virtualised resource management related to the infrastructure resource groups that are assigned to this infrastructure tenant.

- The infrastructure tenant can only request quota related to infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only reserve virtualised resources belonging to infrastructure resource groups that are assigned to this infrastructure tenant.

5.2.4 Architecture option 2.a: Single logical point of contact, VNF related resource management in direct mode

This architecture option describes the case that the NFVIaaS provider allows access to a single logical point of contact (SLPOC) in his administrative domain. The NFVIaaS provider's VIMs are hidden from the NFVIaaS consumer and unified interfaces are exposed by the SLPOC and offered to the NFVIaaS consumer. The NFVIaaS consumer issues NFVIaaS service requests using interfaces provided by the SLPOC.

NOTE 1: The SLPOC function is not intended to create a new functional block but is used for the purpose to describe its functionality. Refer to clause 5.2.7 for an analysis of integration options of SLPOC into NFV-MANO functional blocks.

It is further assumed that NFVIaaS provider and NFVIaaS consumer have a business relationship. Before NFVIaaS requests can be issued, the NFVIaaS provider and the NFVIaaS consumer exchange information about infrastructure tenants, resource groups, and access to the SLPOC.

VNF related resource management in direct mode is used in this architecture option, i.e. the VNFM invokes virtualised resource management operations on the SLPOC.

It is assumed that the existing interfaces of the reference points Or-Vi and Vi-Vnfm can be reused in this architecture option, refer to ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5]. Figure 5.2.4-1 illustrates this architecture option by focusing on the interactions between functional blocks belonging to different administrative domains.

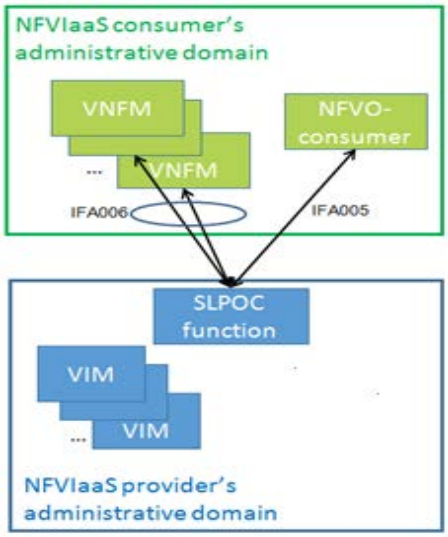

Figure 5.2.4-1: Illustration of NFVIaaS architecture option 2.a

NS management:

NFVO-consumer is responsible for NS lifecycle management, including the management of NSDs and VNF packages. NFVO-consumer manages the VNFFGs and VLs for NSs and issues network resource management operations towards the SLPOC.

VNF management:

The VNFMs are responsible for the VNF lifecycle management. Before executing the VNF lifecycle operation the VNFM requests an operation granting from NFVO-consumer. The granting decision can depend on e.g. operator policies, VNF dependencies and resource information. In the grant response NFVO-consumer provides the VNFM with information to enable the access to the SLPOC for VNF related resource management. The VNFMs request resource management operations needed for VNF LCM from the identified SLPOC.

The NFVO-consumer collects information on consumable resource and virtualised resources capacity from the SLPOC. NFVO-consumer uses such information for VNF lifecycle management decisions.

When an allowance model is used the NFVO-consumer maintains and enforces permitted allowance at various granularity levels (VNFM, VNF, NS, etc.) in order to control resource consumption by VNFMs in relation with VNF lifecycle operation granting.

The NFVO-consumer cannot guarantee resource availability during the granting of a VNF lifecycle request if the resources needed to accommodate such lifecycle operation have not been reserved by the SLPOC.

NFVO-consumer performs VNF Package management and distributes the SW images of VNFs to the SLPOC which forwards them to the VIM(s).

Virtualised resource management:

The SLPOC hides the VIM interfaces. The SLPOC maintains information about infrastructure resources organization, availability and utilization from the various VIMs in the infrastructure domain, refer to ETSI GS NFV-IFA 010 [i.7] for the definition of infrastructure domain. All virtualised resource management requests from the NFVIaaS consumer go to the SLPOC which forwards them to the VIM(s).

NOTE 2: In the context of this use case, infrastructure domain is the same as NFVIaaS provider's administrative domain.

It is assumed that the existing interfaces of the Or-Vi reference point can be reused for the interfaces between SLPOC and VIMs, refer to ETSI GS NFV-IFA 005 [i.4]. Figure 5.2.4-2 illustrates these interfaces.

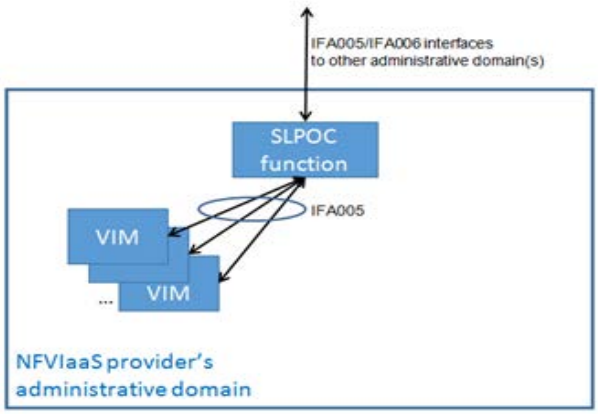

Figure 5.2.4-2: Illustration of SLPOC interfaces

The VIMs are responsible for the management of the virtualised resources and provide interfaces to SLPOC which in turn interfaces with VNFMs and NFVO-consumer so that they can request operations for virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, and NFP management.

The SLPOC manages infrastructure tenants and infrastructure resource groups and limits the scope of operations to the requesting infrastructure tenant (refer to ETSI GS NFV-IFA 010 [i.7]). This includes:

- The infrastructure tenant gets only information related to the infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only initiate virtualised resource management related to the infrastructure resource groups that are assigned to this infrastructure tenant.

- The infrastructure tenant can only request quota related to infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only reserve virtualised resources belonging to infrastructure resource groups that are assigned to this infrastructure tenant.

5.2.5 Architecture option 2.b: Single logical point of contact, VNF related resource management in indirect mode

This architecture option describes the case that the NFVIaaS provider allows access to a single logical point of contact in his administrative domain. The NFVIaaS provider's VIMs are hidden from the NFVIaaS consumer and unified interfaces are exposed by the SLPOC and offered to the NFVIaaS consumer. The NFVIaaS consumer issues NFVIaaS service requests using interfaces provided by the SLPOC.

NOTE: The SLPOC function is not intended to create a new functional block but is used for the purpose to describe its functionality. Refer to clause 5.2.7 for an analysis of integration options of SLPOC into NFV-MANO functional blocks.

It is further assumed that NFVIaaS provider and NFVIaaS consumer have a business relationship. Before NFVIaaS requests can be issued, the NFVIaaS provider and the NFVIaaS consumer exchange information about infrastructure tenants, resource groups, and access to the SLPOC.

VNF related resource management in indirect mode is used in this architecture option, i.e. the VNFM invokes virtualised resource management operations on the NFVO-consumer and the NFVO-consumer in turn invokes them towards the SLPOC.

It is assumed that the existing interfaces of the reference points Or-Vi and Or-Vnfm can be reused in this architecture option, refer to ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 007 [i.6]. Figure 5.2.5-1 illustrates this architecture option.

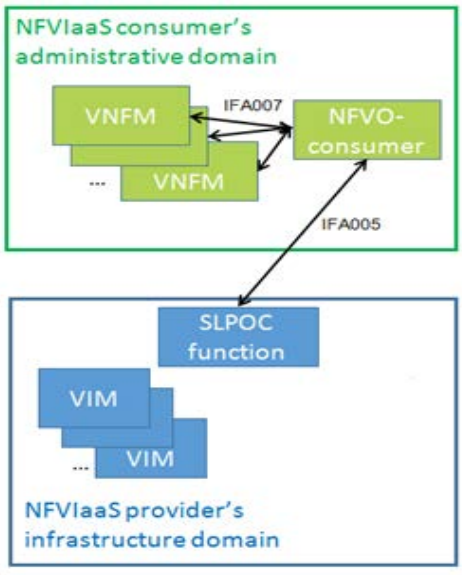

Figure 5.2.5-1: Illustration of NFVIaaS architecture option 2.b

NS management:

NFVO-consumer is responsible for NS lifecycle management, including the management of NSDs and VNF packages. NFVO-consumer manages the VNFFGs and VLs for NSs and issues network resource management operations towards the SLPOC.

VNF management:

The VNFMs are responsible for the VNF lifecycle management. Before executing the VNF lifecycle operation the VNFM requests an operation granting from NFVO-consumer. The granting decision can depend on e.g. operator policies, VNF dependencies and resource information. The VNFMs request resource management operations needed for VNF LCM from NFVO-consumer which issue the requests towards the SLPOC.

The NFVO-consumer collects information on consumable resource and virtualised resources capacity from the SLPOC. NFVO-consumer uses such information for VNF lifecycle management decisions.

When an allowance model is used the NFVO-consumer maintains and enforces permitted allowance at various granularity levels (VNFM, VNF, NS, etc.) in order to control resource consumption by VNFMs in relation with VNF lifecycle operation granting.

The NFVO-consumer cannot guarantee resource availability during the granting of a VNF lifecycle request if the resources needed to accommodate such lifecycle operation have not been reserved in the SLPOC.

NFVO-consumer performs VNF Package management and distributes the SW images of VNFs to the SLPOC which forwards them to the VIM(s).

Virtualised resource management:

The SLPOC hides the VIM interfaces. The SLPOC maintains information about infrastructure resources organization, availability and utilization from the various VIMs in the infrastructure domain. All virtualised resource management requests from the NFVIaaS consumer go to the SLPOC which forwards them to the VIM(s).

It is assumed that the existing interfaces of the Or-Vi reference point can be reused for the interfaces between SLPOC and VIMs, refer to ETSI GS NFV-IFA 005 [i.4]. Figure 5.2.5-2 illustrates these interfaces.

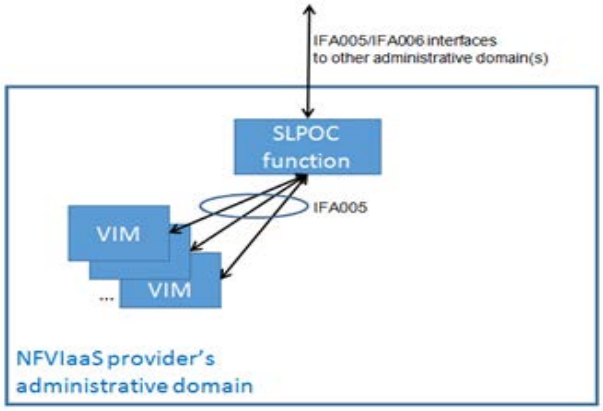

Figure 5.2.5-2: Illustration of SLPOC interfaces

The VIMs are responsible for the management of the virtualised resources and provide interfaces to SLPOC which in turn interfaces with NFVO-consumer for requesting operations for virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, and NFP management.

The SLPOC manages infrastructure tenants and infrastructure resource groups and limits the scope of operations to the requesting infrastructure tenant (refer to ETSI GS NFV-IFA 010 [i.7]). This includes:

- The infrastructure tenant gets only information related to the infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only initiate virtualised resource management related to the infrastructure resource groups that are assigned to this infrastructure tenant.
- The infrastructure tenant can only request quota related to infrastructure resource groups that are assigned to this infrastructure tenant.

- The infrastructure tenant can only reserve virtualised resources belonging to infrastructure resource groups that are assigned to this infrastructure tenant.

5.2.6 Summary of the differences of the NFVIaaS architecture options

The main differentiator between the architecture options described in clauses 5.2.2, 5.2.3, 5.2.4 and 5.2.5 is whether the NFVIaaS provider offers interfaces specified in ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] to an SLPOC or to the MLPOCs in his administrative domain.

The NFVIaaS consumer needs to know how to access the interfaces for NFVIaaS requests:

- In case of architecture options with MLPOC the NFVIaaS provider allows direct access to the VIMs in his administrative domain and provides the NFVIaaS consumer with information that enables the access to all VIMs.

- In case of architecture options with SLPOC the multiple VIMs in the NFVIaaS provider's administrative domain are hidden from the NFVIaaS consumer. The NFVIaaS provider provides the NFVIaaS consumer with information that enables the access to the SLPOC.

Depending on the mode of VNF-related resource management either the NFVO or the VNFM invokes virtualised resources management operations for VNF lifecycle management. The consumer sees the interfaces specified in ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] regardless of whether the MLPOC or SLPOC option is used.

Table 5.2.6-1 summarizes the differences related to virtualised resource management, table 5.2.6-2 summarizes the differences related to NS and VNF management, and table 5.2.6-3 summarizes the differences related to the management of infrastructure tenants and resource groups.

Table 5.2.6-1: Differences related to virtualised resource management

Function	Architecture options with MLPOC (1.a, 1.b)	Architecture options with SLPOC (2.a, 2.b)
Virtualised resource management	The VIMs provide resource management interfaces to VNFMs and NFVO-consumer. The NFVO-consumer maintains the overview of virtualised resources across the VIMs.	The SLPOC provides resource management interfaces to VNFMs and NFVO-consumer. The SLPOC maintains the overview of virtualised resources across the VIMs and provides it to NFVO-consumer.
Capacity management	The VIMs provide capacity management interfaces to NFVO-consumer. The NFVO-consumer maintains the capacity information across the VIMs.	The SLPOC provides capacity management interfaces to NFVO-consumer. The SLPOC maintains the capacity information across the VIMs and provides it to NFVO-consumer.
Quota management	The VIMs provide quota management interfaces to NFVO-consumer. The NFVO-consumer breaks down the quota to the respective VIMs and maintains the quota information across the VIMs.	The SLPOC provides quota management interfaces to NFVO-consumer. The SLPOC coordinates the quota across the VIMs and maintains the quota information across the VIMs.
Resource reservation	The VIMs provide resource reservation management interfaces to NFVO-consumer. The NFVO-consumer breaks down the resource reservations to the respective VIMs and maintains the resource reservation information across the VIMs.	The SLPOC provides resource reservation management interfaces to NFVO-consumer. The SLPOC coordinates the resource reservations across the VIMs and maintains the resource reservation information across the VIMs.

Table 5.2.6-2: Differences related to NS and VNF management

Function	Architecture options with MLPOC (1.a, 1.b)	Architecture options with SLPOC (2.a, 2.b)
Granting	The NFVO-consumer collects information on consumable resources and resource capacity from the VIMs and uses this information for the granting procedure. The NFVO-consumer selects the VIM(s) for the VNF related resource management. In case of VNF-related resource management in direct mode the NFVO-consumer provides the VNFM with information that enables the VNFM to access the VIM(s).	The NFVO-consumer collects information on consumable resources and resource capacity from SLPOC and uses this information for the granting procedure. In case of VNF-related resource management in direct mode the NFVO-consumer provides the VNFM with information that enables the VNFM to access the SLPOC.
NS related resource management	The NFVO-consumer issues network resource management operations towards the relevant VIM(s).	The NFVO-consumer issues network resource management operations towards SLPOC. The SLPOC forwards the operations to the relevant VIMs.
VNF related resource management	Direct mode: VNFM issues resource management operations towards the relevant VIM(s). Indirect mode: VNFM issues resource management operations towards NFVO-Consumer which in turn forwards them to the selected VIM(s).	Direct mode: VNFM issues resource management operations towards the SLPOC. Indirect mode: VNFM issues resource management operations towards NFVO-Consumer which in turn forwards them to the SLPOC. In either case SLPOC forwards the operations to the relevant VIMs.
VNF package management	NFVO-consumer distributes the SW images to the VIMs.	NFVO-consumer distributes the SW images to the SLPOC which in turn forwards them the VIMs.

Table 5.2.6-3: Differences related to the management of infrastructure tenants and resource groups

Function	Architecture options with MLPOC (1.a, 1.b)	Architecture options with SLPOC (2.a, 2.b)
Tenant management	Infrastructure tenants are managed in each VIM of the infrastructure domain.	Infrastructure tenants are managed in the SLPOC, see note 1.
Resource Group management	Infrastructure resource groups are managed in each VIM of the infrastructure domain.	Infrastructure resource groups are managed in the SLPOC.
Limitation of operations for infrastructure tenants	Each VIM controls the access of infrastructure tenants and limits the scope of operations to the infrastructure resource groups that are assigned to this infrastructure tenant.	The SLPOC controls the access of infrastructure tenants and limits the scope of operations to the infrastructure resource groups that are assigned to this infrastructure tenant, see note 2.
NOTE 1: The knowledge of infrastructure tenants can be propagated to the VIMs below the SLPOC. NOTE 2: The SLPOC has the responsibility to limit the scope of operations to the requesting infrastructure tenant. However, the VIMs below the SLPOC can also check and limit the scope of operations to the infrastructure resource groups that are assigned to this infrastructure tenant within the scope of their responsibility.		

5.2.7 Integration of MLPOC and SLPOC into NFV-MANO functional blocks

As described in clause 5.2.6, the NFVIaaS consumer's NFVO and VNFMs use the interfaces specified in ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] to issue NFVIaaS requests regardless of whether the MLPOC or SLPOC option is used. That is, from an NFVIaaS consumer's NFVO and VNFMs perspective, the MLPOC and SLPOC look like a VIM.

For the architecture options utilizing the NFVIaaS provider's VIMs providing the MLPOC functionality, refer to the summary in clause 5.2.6. No new reference points are needed for these options.

For the architecture options utilizing an SLPOC there are two integration options: The SLPOC can be integrated into an NFVIaaS provider's VIM (see figure 5.2.7-1) or into the NFVIaaS provider's NFVO (see figure 5.2.7-2). Therefore new reference points are introduced and the interfaces specified in ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] are reused at the new reference points. Due to the integration of SLPOC, the NFVIaaS provider's NFVO or VIM(s) include additional functionality.

Figures 5.2.7-1 and 5.2.7-2 illustrate the SLPOC integration options, focusing on the interfaces utilized for this use case. Other interfaces of VIMs, VNFMs, and NFVOs are preserved independently of the SLPOC integration option (not shown in the figures).

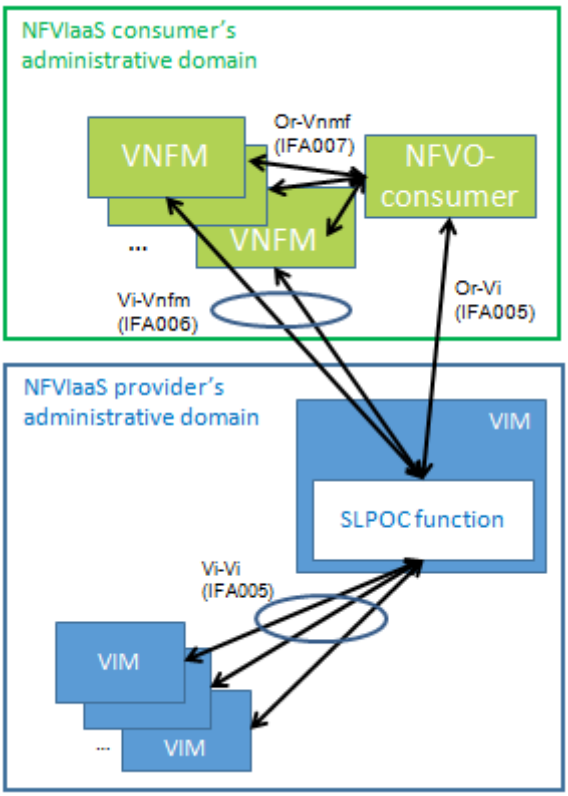

Figure 5.2.7-1: Illustration of SLPOC function integrated into VIM

Figure 5.2.7-1 shows the functional relationship of the SLPOC function to other NFV-MANO functional blocks. The VIM integrating the SLPOC function is endpoint of the interfaces over the reference points towards NFVO, VNFMs and VIMs.

If the SLPOC is integrated into VIM, the VIM needs to support the SLPOC functionality and interfaces. This includes the following enhancements:

- Forwarding requests from NFVIaaS consumer's NFVO and VNFM(s) to the respective VIMs.
- Maintaining the overview over virtualised resources, quotas, reservations, and capacity per tenant / infrastructure resource group (currently only supported in the context of a VIM being responsible for multiple NFVI-PoPs).

A new Vi-Vi reference point would need to be introduced to support this integration option. ETSI GS NFV-IFA 005 [i.4] interfaces are reused for this reference point.

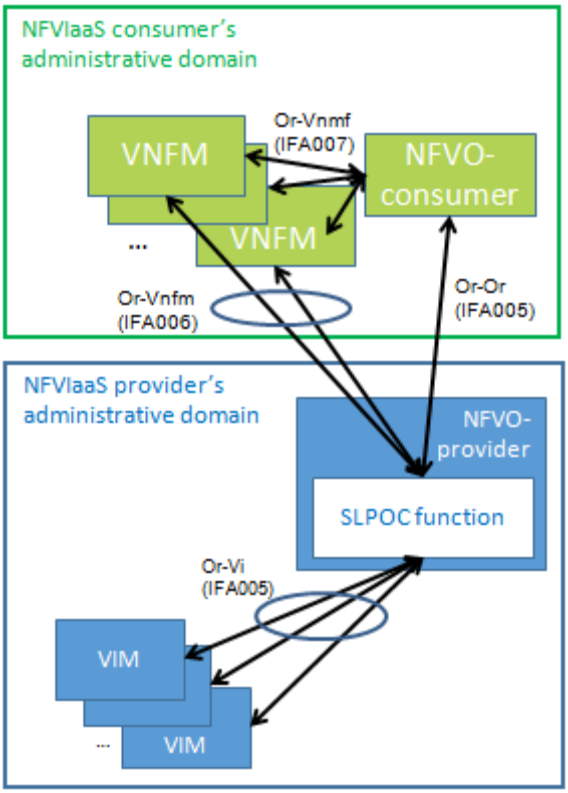

Figure 5.2.7-2: Illustration of SLPOC function integrated into NFVO

Figure 5.2.7-2 shows the functional relationship of the SLPOC function to other NFV-MANO functional blocks. The NFVO integrating the SLPOC function is endpoint of the interfaces over the reference points towards NFVO, VNFMs and VIMs.

NOTE: This scenario assumes that an NFVO (NFVO-provider) exists in the NFVIaaS's provider administrative domain. In this case the NFVIaaS provider operates its own NSs and is therefore performing functions beyond the NFVIaaS role.

If the SLPOC is integrated into NFVO-provider, the NFVO-provider needs to support the SLPOC functionality and interfaces. This includes the following enhancements:

- Management of infrastructure resource groups and infrastructure tenants (currently only supported in case of indirect mode).
- Providing the interfaces specified in ETSI GS NFV-IFA 005 [i.4] towards the NFVIaaS consumer's NFVO and forward the requests to the respective VIM(s).
- Providing the interfaces specified in ETSI GS NFV-IFA 006 [i.5] towards the NFVIaaS consumer's VNFM(s) and forward the requests to the respective VIM(s).
- Limiting the scope of operations to the infrastructure resource groups assigned to the requesting infrastructure tenant (currently only supported in case of indirect mode).
- Maintaining the overview over virtualised resources, quotas, reservations, and capacity per infrastructure tenant / infrastructure resource group (currently supported in case of indirect mode only).

For this integration option the NFVIaaS consumer's NFVO and VNFMs interface with the NFVO-provider instead of VIM(s) for NFVIaaS requests. However, as the interfaces specified in ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] are used, this does not imply functional differences for the NFVIaaS consumer's NFVO and VNFMs.

The following enhancements to the NFV architectural framework would be needed to support this integration option:

- The Or-Vnfm reference point would have to be enhanced with the interfaces specified in ETSI GS NFV-IFA 006 [i.5].

- A new Or-Or reference point would have to be introduced for this integration option. The interfaces specified in ETSI GS NFV-IFA 005 [i.4] would be reused for this reference point.

5.3 Enhancements to NFV-MANO architecture

The NFV-MANO architecture framework and reference points are reused for the NFVIaaS use case. This clause describes potential enhancements of NFV-MANO functional blocks and reference points based on the use case analysis. Refer to clause 5.2.6 for a summary of the differences of the NFVIaaS architecture options. Integration of the MLPOC and SLPOC into NFV-MANO functional blocks is described in clause 5.2.7.

While the functional requirements for multi-tenancy are already specified in ETSI GS NFV-IFA 010 [i.7] and partly covered in the interface specifications, some enhancements are necessary to fully enable limiting the scope of operations to the requesting infrastructure tenant.

Table 5.3-1 lists the reference points specified in NFV-MANO architectural framework specifications, maps it to the reference points applied for this use case and summarizes the changes due to the use case.

Table 5.3-1: Mapping of reference points

NFV-MANO Reference Point	Reference Points in this Use Case	Changes due to the use case
Os-Ma-nfvo	Os-Ma-nfvo	Unchanged
Or-Vnfm	Or-Vnfm	For the option where SLPOC is integrated in NFVO this reference point needs to be enhanced with ETSI GS NFV-IFA 006 [i.5] interfaces. In addition ETSI GS NFV-IFA 006 [i.5] enhancements as described for the Vi-Vnfm reference point are necessary.
Or-Vi	Or-Vi	In addition to the operations specified in ETSI GS NFV-IFA 005 [i.4], operations for the management of infrastructure tenants and infrastructure resource groups are necessary. Enhancements are necessary to use the infrastructure resource group as input parameter in ETSI GS NFV-IFA 005 [i.4] operations, e.g. it is currently missing in query and update operations (see note 2 and note 3).
Vi-Vnfm	Vi-Vnfm	Enhancements are necessary to use the infrastructure resource group as input parameter in ETSI GS NFV-IFA 006 [i.5] operations, e.g. it is currently missing in query operations (see note 2 and note 3).
Ve-Vnfm	Ve-Vnfm	Unchanged.
-	Vi-Vi	New reference point between VIMs, used if SLPOC is integrated in VIM. ETSI GS NFV-IFA 005 [i.4] interfaces are reused for this reference point, including the enhancements described for the Or-Vi reference point.
-	Or-Or	New reference point between NFVOs, used if SLPOC is integrated in NFVO. ETSI GS NFV-IFA 005 [i.4] interfaces are reused for this reference point, including the enhancements described for the Or-Vi reference point (see note 1, note 2 and note 3).

NOTE 1: This reference point is also used for use case "Network Services provided using multiple administrative domains", refer to clause 6.3.

NOTE 2: Monitoring and failure detection of MANO functional blocks are studied in ETSI GR NFV-IFA 021 [i.11]. From an operational perspective, enhancements for the maintenance of the session between the NFVO and the VIM (for Or-Vi reference point), the VNFM and the VIM (for Vi-Vnfm), or between NFVOs (for Or-Or) in different administrative domains are required, in order to increase the robustness of the system. This becomes especially critical when SLPOC option is followed.

NOTE 3: For the logical interconnection of domains, discovery mechanisms can be required for auto-discovery of the NFVO and the VIM (for Or-Vi reference point), the VNFM and the VIM (for Vi-Vnfm in direct mode of operation), or between NFVOs (for Or-Or reference point) functional blocks of the different administrative domains.

Table 5.3-2 summarizes the functional enhancements of the NFV-MANO functional blocks.

Table 5.3-2: NFV-MANO functional blocks

NFV-MANO Functional Block	Changes
NFVO	The NFVO needs to consider the interface changes as described in table 5.3-1. If the SLPOC is integrated into NFVO, the NFVO needs to support the SLPOC functionality and interfaces. This includes the following enhancements: • Management of infrastructure resource groups and infrastructure tenants (currently only supported in case of indirect mode). • Providing ETSI GS NFV-IFA 005 [i.4] interfaces towards the NFVIaaS. consumer's NFVO and forward the requests to the respective VIM(s). • Providing ETSI GS NFV-IFA 006 [i.5] interfaces towards the NFVIaaS consumer's VNFM(s) and forward the requests to the respective VIM(s.) • Limiting the scope of operations to the infrastructure resource groups assigned to the requesting infrastructure tenant (currently only supported in case of indirect mode). • Maintaining the overview over virtualised resources, quotas, reservations, and capacity per infrastructure tenant / infrastructure resource group (currently supported in case of indirect mode only).
VNFM	The VNFM needs to consider the interface changes described in table 5.3-1.
VIM	The VIM needs to consider the interface changes as described in table 5.3-1. If the SLPOC is integrated into VIM, the VIM needs to support the SLPOC functionality and interfaces. This includes the following enhancements: • Forwarding requests from NFVIaaS consumer's NFVO and VNFM(s) to the respective VIMs. • Maintaining the overview over virtualised resources, quotas, reservations, and capacity per tenant / infrastructure resource group (currently only supported in the context of a VIM being responsible for multiple NFVI-PoPs).
NOTE 1: Monitoring and failure detection of NFV-MANO functional blocks are studied in ETSI GR NFV-IFA 021 [i.11]. For operational purposes, the different functional blocks (NFVO, VNFM and VIM) need to consider resiliency procedures to increase the robustness of the system by reacting to failures in the logical interconnection among administrative domains. This is especially critical in SLPOC case. For each case (i.e. NFVO, VNFM and VIM), the functional block requires to play the role of MANO Monitor of the corresponding entity on the remote domain, as described in ETSI GR NFV-IFA 021 [i.11]. NOTE 2: In case of using auto-discovery procedures for the logical interconnection of the functional blocks of different administrative domains, the functional blocks involved in the process need to consider the logic required for the auto-discovery mechanisms used. Information like the IP address of the distinct functional blocks to be interconnected, the identifier of administrative domain, the administrative organization it pertains, etc. should be handled during the process.	

6 Use case analysis: Network Services provided using multiple administrative domains

6.1 Use case description

This use case describes a network operator offering Network Services (NS) to different departments within the same operator, as well as facilitating the offering of these NSs to another network operator.

In this use case, an administrative domain is regarded as one or more NFVI PoPs, VIMs, VNFMs (together with their related VNFs). Each administrative domain includes an NFVO, allowing distinct specific sets of NSs to be hosted and offered on each administrative domain.

NOTE 1: A single NFVO can support multiple administrative domains however this use case focuses on the example when there is an NFVO per administrative domain.

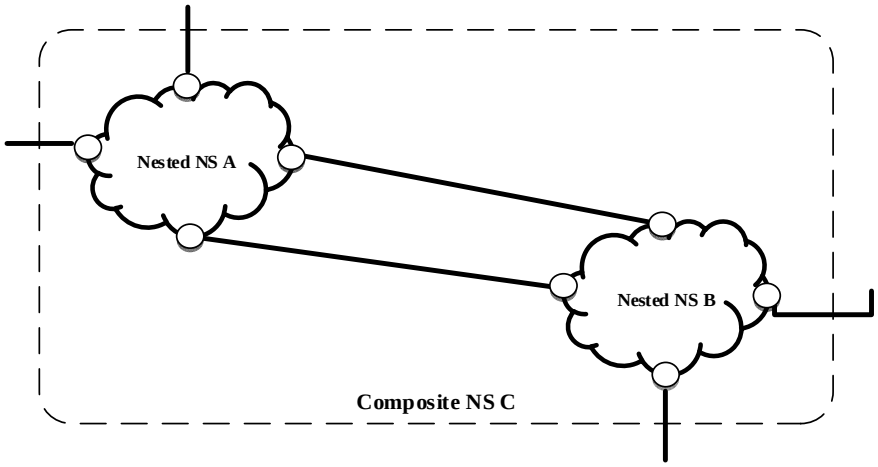

Figure 6.1-1: Composite NS and nested NSs example

Figure 6.1-1 provides an example of composite NS and nested NSs. In this example, the two constituent nested NSs which build up the composite NS are offered by administrative domains different than the one offering the composite NS itself. As shown in figure 6.1-1, the composite NS C offered by Administrative Domain C contains the nested NS A and B which are offered by Administrative Domains A and B respectively. Nested NS A or B can also be shared by other composite NS(s) than composite NS C (in the same administrative domain or in another administrative domain). For the management of the NS hierarchy shown in figure 6.1-2, NFVO-1 in Administrative Domain C is on-top, meaning that it manages the composite NS C. NFVO-2 in Administrative Domain A and NFVO-3 in Administrative Domain B manage the nested NS A and nested NS B respectively and expose the nested NSs to NFVO-1 in Administrative Domain C.

NOTE 2: NFVO-1, NFVO-2 and NFVO-3 are just NFVO roles and the example above neither prevents the NFVO-1 to manage nested NS, nor prevents NFVO-2 or NFVO-3 to manage composite NS for another NS hierarchy.

It is expected that an SLA is in place between the providers of the constituent nested NSs in Administrative Domain A or B and the provider of the composite NS in Administrative Domain C. Monitoring related to resource usage of the constituent nested NSs is needed for SLA supervision.

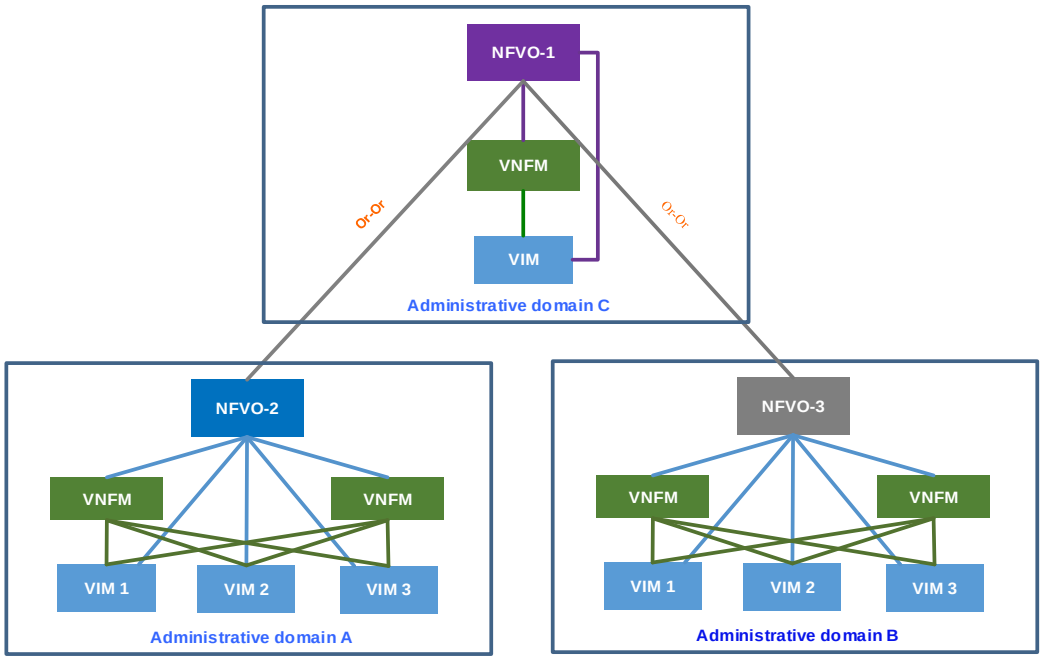

Figure 6.1-2: NSs provided using multiple administrative domains

Figure 6.1-2 gives an example of multiple administrative domains, each one offering a set of NSs. This use case does not create any new functional block out of the NFVO, as NFVO-1, NFVO-2 and NFVO-3 are just NFVO roles, but introduces the new reference point Or-Or between NFVOs for interoperability purpose.

6.2 Potential architecture options

6.2.1 NFVO roles

To further facilitate the use case study, the NFVO roles applied in this use case are abstracted to NFVO-1 and NFVO-2 respectively. NFVO-1 and NFVO-2 possess the functionality of the NFVO. NFVO-1 is responsible for lifecycle management of the composite NS and NFVO-2 is responsible for lifecycle management of the nested NSs (NFVO-2 and NFVO-3 in the examples of figure 6.1-2).

NOTE: A single NFVO can simultaneously play both roles described in this clause.

NFVO-1 is responsible for performing the instantiation of the composite NS. As this composite NS includes nested NSs, NFVO-1 also triggers, if needed, the instantiation of those nested NSs to corresponding NFVO-2. After the instantiation of the nested NSs, NFVO-1 is also responsible for initiating other lifecycle management operations like scaling or healing of the nested NSs, in collaboration with NFVO-2. If a nested NS is offered by the administrative domain that NFVO-1 belongs to, NFVO-2 and NFVO-1 can be played by the same NFVO.

For this use case, NFVO-1 is unaware of virtualised resources in the administrative domain of NFVO-2.

NFVO-2 provides NFVO functionalities for the nested NSs. The scope also includes the VNFs and resources that are part of those nested NSs.

NFVO-2 receives NS LCM request from NFVO-1 and provides NS LCM for the nested NSs.

Granting is applied for nested NS LCM operation with regards to the guarantee of composite NS consistency (see clause A.1.6).

NFVO-2 manages NS tenants and service resource groups and their association for the nested NSs, refer to ETSI GS NFV-IFA 010 [i.7] for the definition and description of service resource group and NS tenant. NFVO-2 limits the scope of operations to the requesting NS tenant (based on the association to NS resource group).

NFVO-2 provides NFVO-1 with information about the nested NSs belonging to service resource groups assigned to the related NS tenants. Such information includes e.g. fault information, performance information, capacity information, etc. NFVO-1 uses the nested NS information to derive information of the composite NS (performance, faults, etc.).

6.2.2 Architecture option proposal

The NFV-MANO architecture framework as described in ETSI GS NFV-MAN 001 [i.3] builds the basis for the potential architecture option analysed in this clause in order to support the use case of NS provided using multiple administrative domains.

In this use case, a new reference point between NFVO-1 and NFVO-2 (named Or-Or) is added in the NFV-MANO architecture framework to support the NS LCM procedures which are provided using multiple administrative domains. The VNFMs in each administrative domain interact with the NFVO (either NFVO-1 or NFVO-2) of the same administrative domain. The functionality over Or-Vnfm reference point is unchanged in each administrative domain. NFVO-1 is not aware of the constituent VNF instances of the nested NS instance, and hence NFVO-1 does not interact with the VNFMs in the administrative domain of NFVO-2. Similarly, NFVO-2 is not aware of the constituent VNF instances of the composite NS instance, and so NFVO-2 does not interact with the VNFMs in the administrative domain of NFVO-1. The VIM is not relevant for this use case.

Figure 6.2.2-1 illustrates the architecture option for this use case.

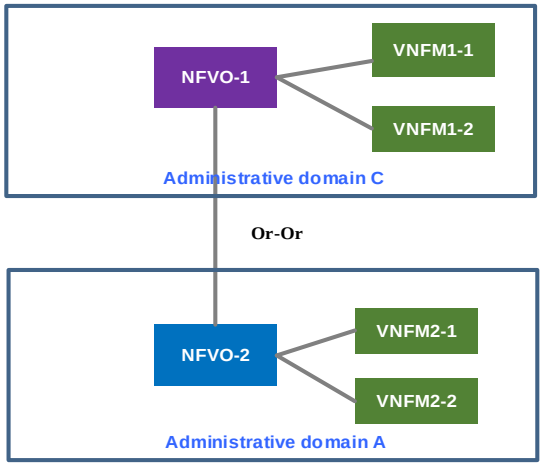

Figure 6.2.2-1: Illustration of use case architecture option

6.3 Enhancements to NFV-MANO architecture

Table 6.3-1 lists the mapping between the reference points defined in NFV-MANO stage 2 specifications and the reference points applied in use case.

Table 6.3-1: Mapping of the reference points

NFV-MANO Reference Point	Reference Points in this Use Case	Note
Os-Ma-nfvo	Os-Ma-nfvo	Unchanged
Or-Vnfm	Or-Vnfm	Unchanged
Or-Vi	Or-Vi	Unchanged (see note)
Vi-Vnfm	Vi-Vnfm	Unchanged
Ve-Vnfm	Ve-Vnfm	Unchanged
-	Or-Or	This is a new reference point between NFVOs introduced by the use case. Interfaces for NS lifecycle management (see clause A.1), NSD management, fault management (see clause 6.2.1), and performance management (see clause 6.2.1) from ETSI GS NFV-IFA 013 [i.9] are reused for this reference point. An interface for NS lifecycle operation granting is added for this reference point (see clause A.1.6). From an operational perspective, enhancements for the maintenance of the session between NFVOs in different administrative domains are required, in order to increase the robustness of the system. The NFVO need to play the role of MANO Monitor as described in ETSI GR NFV-IFA 021 [i.11]. Similarly, for the logical interconnection of domains, discovery mechanisms (as presented in ETSI GR NFV-IFA 021 [i.11]) can be required for auto-discovery of NFVOs of the different administrative domains.
NOTE: In the study of management and connectivity for multi-site services ETSI GR NFV-IFA 022 [i.10], a new reference point other than Or-Vi is used for the interaction between the NFVO and the WIM. Therefore, the Or-Vi reference point is located in a certain administrative domain and not impacted by this use case.		

All the functionality over the existing NFV-MANO reference points is unchanged when this use case is introduced. However, a reference point between NFVO-1 and NFVO-2 which belong to different administrative domains is introduced. The new reference point only applies between the NVFO that play the role of managing nested NSs and the NFVO that play the role of managing composite NSs. That is to say, between the NFVOs playing different roles. This new reference point provides (1) the ability to query NSDs of nested NS for their identification and selection when a composite NS is created, and (2) the interfaces of lifecycle management for nested NS managed by NFVO-2 which is necessary to compose composite NS managed by NFVO-1 in a different administrative domain. Clause A.1 provides the operational flows for NS LCM and NSD management by using the new reference point Or-Or in this use case.

Based on the analysis to the operational flows in clause A.1, Table 6.3-2 summarizes the functional enhancements to the NFV-MANO functional blocks.

Table 6.3-2: NFV-MANO functional blocks impact

NFV-MANO Functional Block	Changes
NFVO	The provider NFVO needs to provide a subset of the NS LCM interface over the Or-Or reference point, which includes the following operations (see notes 1 and 3): • NS Identifier Creation • NS instantiation • NS scaling • NS healing • NS query • NS lifecycle change notification The provider NFVO needs to provide a subset of the NSD management interface over Or-Or reference point which includes the following operation: • NSD query (see notes 2, 3). The provider NFVO needs to provide NS performance management interface over Or-Or reference point (see note 3). The provider NFVO needs to provide NS fault management interface over Or-Or reference point (see note 3). The consumer NFVO needs to provide NS lifecycle operation granting interface over Or-Or reference point (see note 4). The consumer NFVO needs to provide NS instance usage notification interface over the Or-Or reference point (see note 4). For operational purposes, the NFVO needs to consider resiliency procedures to increase the robustness of the system by reacting to failures in the logical interconnection among domains, in the same way as presented in ETSI GR NFV-IFA 021 [i.11] for single domain case. NFVO should act as MANO Monitor. In case of using auto-discovery procedures for the logical interconnection of the functional blocks of different administrative domains, the NFVO needs to consider the logic required for the auto-discovery mechanisms used. Information like the IP address of the distinct functional blocks to be interconnected, the identifier of administrative domain, the administrative organization it pertains, etc. should be handled during the process. This is studied in ETSI GR NFV-IFA 021 [i.11] with focus on single administrative domain operation.
VNFM	Not impacted by this use case.
VIM	Not impacted by this use case.
NOTE 1: (nested) NS termination or (nested) NS update operation is not explicitly derived in the procedure of (composite) NS termination or (composite) NS update operation. Instead, the association of nested NS and composite NS is established or released inside NFVO-1. NOTE 2: NSD on-board procedure follows a bottom-up approach in which the Sender initiates the NSD on-boarding of each nested NS before NSD on-boarding of composite NS. The NFVO does not initiate NSD on-boarding operation over Or-Or reference point thereby. NOTE 3: The provider-NFVO refers to the NFVO role which provides the necessary NS LCM and NSD management functionality to the consumer over Or-Or reference point. NOTE 4: The consumer NFVO refers to the NFVO role which consumes NS LCM, NSD management, NS performance management and NS fault management functionality provided by the provider NFVO over Or-Or reference point. On the other hand, the consumer NFVO provides NS lifecycle operation granting and NS instance usage notification functionality to the provider NFVO over Or-Or reference point.	

7 Conclusions and recommendations

7.1 Conclusions

The present document studies two use cases to support the offering of NFV-MANO services across multiple administrative domains and describes related architecture options:

1) For the NFVIaaS use case, clause 5.2 identifies and describes 4 architecture options:

   - Architecture options utilizing the NFVIaaS provider's VIMs providing the MLPOC functionality:

     - Architecture option 1.a: Multiple logical point of contact VNF related resource management in direct mode (see clause 5.2.2).

     - Architecture option 1.b: Multiple logical point of contact VNF related resource management in indirect mode (see clause 5.2.3).

     The NFVIaaS provider allows direct access to the VIMs in his administrative domain.No new reference point is needed, but enhancements of ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] interfaces are needed.

   - Architecture options utilizing an SLPOC which can be either integrated into VIM or NFVO.

     - Architecture option 2.a: Single logical point of contact VNF related resource management in direct mode (see clause 5.2.4).

     - Architecture option 2.b: Single logical point of contact VNF related resource management in indirect mode (see clause 5.2.5).

     The NFVIaaS provider offers single entry point for other administrative domains, the VIMs in his administrative domain are hidden from the NFVIaaS consumer. New reference points are needed and ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5] interfaces are reused at the new reference points. Due to the integration of SLPOC, the NFVIaaS provider's NFVO or VIM(s) includes additional functionality.From NFVIaaS consumer's NFVO and VNFMs perspective the SLPOC looks like a VIM.

2) For the use case "NSs provided using multiple administrative domains", clause 6.2 describes the architecture option: A new reference point between two NFVOs playing different roles is introduced for this use case.

Table 7.1-1 summarizes the proposed changes related to the architecture options analysed in clauses 5 and 6.

Table 7.1-1: Changes related to the architecture options

Topic	Use case, architecture option	Reference
Changes of NFV-MANO functional blocks	• NFVO: – NFVIaaS, architecture options 2.a and 2.b: Optional integration of SLPOC functionality into NFVO-provider. – In this case the NFVO-provider looks like a VIM to NFVIaaS consumer's NFVO and VNFMs. – NSs provided using multiple administrative domains: Support NS LCM provided over the new Or-Or reference • VNFM: No functional change identified. • VIM: NFVIaaS, architecture options 2.a and 2.b: – Optional integration of SLPOC functionality into the VIM.	table 5.3-2 table 6.3-2 table 5.3-2
Changes of NFV-MANO reference points	• New Or-Or reference point: – NFVIaaS, architecture options 2.a and 2.b: Provide ETSI GS NFV-IFA 005 [i.4] interfaces between NFVOs if SLPOC functionality is integrated in NFVO-provider. – NSs provided using multiple administrative domains: Provide NS LCM interface between NFVOs. • New Vi-Vi reference point: NFVIaaS, architecture options 2.a and 2.b: Provide ETSI GS NFV-IFA 005 [i.4] interfaces between VIMs if SLPOC functionality is integrated in VIM. • Or-Vi: New interface for management of infrastructure tenants and infrastructure resource groups. • Or-Vnfm: Provide interfaces for virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, and SW image management between the NFVO-provider and the NFVIaaS consumer's VNFMs if SLPOC functionality is integrated in NFVO-provider. See note. The remaining reference points are unchanged.	table 5.3-1 table 6.3-1 table 5.3-1 table 5.3-1 table 5.3-1
Interface changes	• ETSI GS NFV-IFA 005 [i.4] interfaces: NFVIaaS, all architecture options: Enhance operations to use infrastructure resource groups as input parameter, e.g. it is currently missing in query and update operations. • ETSI GS NFV-IFA 006 [i.5] interfaces: NFVIaaS, all architecture options: Enhance operations to use infrastructure resource groups as input parameter, e.g. it is currently missing in query operations.	table 5.3-1
Changes of Information Model	No changes identified.	
NOTE: The enhancements needed for Or-Vnfm virtualised resource management purpose need to consider and analyse the already available support of virtualised resource management available on this reference point.		

Recommendations for normative work are identified in clause 7.2 based on the use case analysis in clauses 5 and 6.

7.2 Recommendations

This clause provides recommendations for normative work focusing on NFV-MANO functional blocks and reference points.

Table 7.2-1 lists the recommendations related to NFV-MANO reference points.

Table 7.2-1: Recommendations for NFV-MANO reference points

Identifier	Recommendation	Comments
Or-Or.Mad.001	It is recommended that a new Or-Or reference point between NFVOs be specified. Interfaces of the new Or-Or reference point are used: - Between NFVOs in different administrative domains for management of composite/nested NSs. - Between NFVOs in different administrative domains if SLPOC is integrated in NFVO.	see clauses 5.3 and 6.3
Or-Or.Mad.002	It is recommended that the new Or-Or reference point reuses ETSI GS NFV-IFA 005 [i.4] interfaces for NFVIaaS service requests between NFVOs in different administrative domains. These requests include virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, NFP management, and SW image management. Management of infrastructure tenants and infrastructure resource groups needs to be covered over this interface as well.	see clauses 5.1 and 5.3
Or-Or.Mad.003	It is recommended that the new Or-Or reference point reuses ETSI GS NFV-IFA 013 [i.9] interfaces for NS lifecycle management between NFVOs in different administrative domains.	see clause 6.3
Or-Or.Mad.004	It is recommended that the new Or-Or reference point reuses ETSI GS NFV-IFA 013 [i.9] interfaces for NSD management between NFVOs in different administrative domains.	see clause 6.3
Or-Or.Mad.005	It is recommended that NS lifecycle management interface over Or-Or reference point includes a subset of operations (i.e. NS identifier creation, NS instantiation, NS scale, NS heal, NS query and NS lifecycle change notification) which are derived from ETSI GS NFV IFA 013 [i.9] NS lifecycle management interface.	see clause 6.3
Or-Or.Mad.006	It is recommended that NSD management interface over Or-Or reference point includes a subset of operations (i.e. NSD query) which are derived from ETSI GS NFV-IFA 013 [i.9] NSD management interface.	see clause 6.3
Or-Or.Mad.007	It is recommended that the new Or-Or reference point reuses ETSI GS NFV-IFA 013 [i.9] interfaces for NS performance management between NFVOs in different administrative domains.	see clause 6.3
Or-Or.Mad.008	It is recommended that the new Or-Or reference point reuses ETSI GS NFV-IFA 013 [i.9] interfaces for NS fault management between NFVOs in different administrative domains.	see clause 6.3
Or-Or.Mad.009	It is recommended that the new Or-Or reference point specifies an interface for NS lifecycle operation granting between NFVOs in different administrative domains.	see clause 6.3
Or-Or.Mad.010	It is recommended that the new Or-Or reference point specifies an interface for NS instance usage notification between NFVOs in different administrative domains.	see clause A.1.2b, clause A.1.4 and clause A.1.8
Or-Or.Mad.011	It is recommended that Or-Or reference point is enhanced with NS state handling to include the information on whether the NS is shared.	see clause A.1.2b
Or-Vi.Mad.001	It is recommended that the ETSI GS NFV-IFA 005 [i.4] interface requirements on Or-Vi reference point are enhanced to include operations for the management of infrastructure tenants and infrastructure resource groups and the association between those.	see clause 5.3. The functional requirements for multi-tenancy support in VIM are specified in ETSI GS NFV-IFA 010 [i.7] clause 8.7, but the related interface requirements are missing in ETSI GS NFV-IFA 005 [i.4]

Identifier	Recommendation	Comments
Or-Vi.Mad.002	It is recommended that the ETSI GS NFV-IFA 005 [i.4] interface requirements on the Or-Vi reference point are enhanced in order to consider infrastructure resource group as input parameter in IFA 005 operations, e.g. it is currently missing in query and update operations.	see clause 5.3
Or-Vnfm.Mad.001	It is recommended that the Or-Vnfm reference point provides interfaces for NFVIaaS service requests between the NFVO-provider and the NFVIaaS consumer's VNFMs. These requests include virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, and SW image management. Such interfaces are used if SLPOC is integrated in NFVO and correspond to VIM northbound interfaces. See note.	see clauses 5.2.7 and 5.3
Vi-Vnfm.Mad.001	It is recommended that the ETSI GS NFV-IFA 006 [i.5] interface requirements on Vi-Vnfm reference point are enhanced in order to consider infrastructure resource group as input parameter in ETSI GS NFV-IFA 005 [i.4] operations, e.g. it is currently missing in query operations.	see clause 5.3
Vi-Vi.Mad.001	It is recommended that a new Vi-Vi reference point between VIMs be specified. Interfaces of the new Vi-Vi reference point are used between VIMs in the NFVIaaS provider's administrative domain if SLPOC is integrated in VIM. ETSI GS NFV-IFA 005 [i.4] interfaces are recommended to be reused at this Vi-Vi reference point, including the enhancements described in Or-Vi.Mad.002.	see clause 5.3
Vi-Vi.Mad.002	It is recommended that the new Vi-Vi reference point reuses all ETSI GS NFV-IFA 005 [i.4] interfaces for infrastructure management operations between VIMs. These operations include virtualised resource management, resource reservation, quota management, capacity management, performance management, fault management, NFP management, and SW image management. Operations for management of infrastructure tenants and infrastructure resource groups can be supported over this reference point as well.	see clauses 5.1 and 5.3
NOTE: The enhancements needed for Or-Vnfm virtualised resource management purpose need to consider and analyse the already available support of virtualised resource management available on this reference point.		

Table 7.2-2 lists the recommendations related to NFV-MANO functional blocks.

Table 7.2-2: Recommendations for NFV-MANO functional blocks

Identifier	Recommendation	Comments
VIM.SLPOC.001	It is recommended that an optional requirement be specified for the VIM to support the integration of SLPOC functionality.	see clause 5.3
VIM.SLPOC.002	It is recommended that an optional requirement be specified for the VIM to support the new Vi-Vi reference point for the cases where SLPOC is integrated in VIM.	see clause 5.3
NFVO.SLPOC.001	It is recommended that an optional requirement be specified for the NFVO to support the integration of SLPOC functionality. In this case the NFVO-provider looks like a VIM to NFVIaaS consumer's NFVO and VNFMs, so that the NFVIaaS consumer's VNFMs do not need to distinguish which MLPOC and SLPOC option is used in the NFVIaaS provider's administrative domain.	see clause 5.3
NFVO.SLPOC.002	It is recommended that an optional requirement be specified for the NFVO to support the new Or-Or reference point for the cases where SLPOC is integrated in NFVO.	see clause 5.3
NFVO.001	It is recommended that a requirement be specified for the NFVO to support the capability to invoke NS lifecycle management operations towards the NFVO in another administrative domain.	see clause 6.3
NFVO.002	It is recommended that a requirement be specified for the NFVO to support the capability to invoke NSD management operations towards the NFVO in another administrative domain.	see clause 6.3
NFVO.003	It is recommended that a requirement be specified for the NFVO to support the capability to invoke NS performance management operations towards the NFVO in another administrative domain.	see clause 6.3
NFVO.004	It is recommended that a requirement be specified for the NFVO to support the capability to invoke NS fault management operations towards the NFVO in another administrative domain.	see clause 6.3
NFVO.005	It is recommended that a requirement be specified for the NFVO to support the capability to invoke NS lifecycle operation granting towards the NFVO in another administrative domain.	see clause 6.3
NFVO.006	It is recommended that a requirement be specified for the NFVO to support the capability to receive invocations of NS lifecycle operation granting from the NFVO in another administrative domain.	see clause 6.3
NFVO.007	It is recommended that a requirement be specified for the NFVO to support the capability to provide notifications of NS instance usage towards the NFVO in another administrative domain.	see clause 6.3
NFVO.008	It is recommended that a requirement be specified for the NFVO to support the capability to receive notifications of NS instance usage from the NFVO in another administrative domain.	see clause 6.3
NFVO.009	It is recommended to address in normative specifications mechanisms facilitating discovery of the NFVOs responsible for specific network services in one domain by an NFVO in a different administrative domain.	see clause 6.3

Certain monitoring parameters can be considered sensitive and should not be shared in multiple administrative domain environments. How to determine monitoring parameters applied in multi-domain environment will be resolved either in a separate study or as part of the future normative work (which will take guidance from ETSI GR NFV-IFA 021 [i.11] and ETSI GS NFV-IFA 027 [i.13]).

7.3 Information exchange between administrative domains

As a generic statement, some level of information should be exchanged between administrative domains to permit a correct and proper operation of the final service. A non-exhaustive list is the following:

- Monitoring parameters information, in order to facilitate service assurance in the multi-domain environment and to track the usage of resources instantiated in other administrative domains (see clause 4.2).
- Topology view (up to L3) in order to assist on the decision of multi-domain service orchestration, e.g. to select the appropriate NFVI PoP in case of NFVIaaS requests (see clause 5.1).
- Resource capabilities, applicable to both IT (computing and storage) and networking resources participant of the multi-domain service, to assist on the decision of VNF placement in case of NFVIaaS requests (not applied in case of composite NS requests), (see clause 5.1).
- Descriptors, enabling the right selection of services (and/or functions) when providers offer multiple choices (composite NS), (see clause 6.1).
- Access information (e.g. URL) to the MLPOCs endpoints of the different NFVI PoPs (NFVIaaS MLPOC), to the SLPOC single endpoint for the provider's administrative domain (NFVIaaS SLPOC), or to the provider domain NFVO (composite NS), (see clauses 5.2 and 6.2).
- (Optional) notifications from provider to consumer administrative domains about incurred changes in the offered network service descriptors (see clause A.1.1 hereafter).

The information to be exchanged, and the detail or granularity of such information, will depend in some cases on the specific multi-domain service under analysis. In any case, the provider's administrative domain (unless explicitly stated in the acting inter-domain business agreements) can discretionally decide what of his resources and topologies it intends to expose towards other administrative domains, and accordingly commit to provision in the event of actual requests.

In particular, the topology view information set can include:

- Geographical location of the NFVI PoPs hosting the offered NS (composite NS use case) or available to allocate VNFs (NFVIaaS use case), at a granularity defined according to commercial and regulatory constraints (as first assumption, country identification), (see clauses 5.1 and 6.1).
- Abstract description (endpoints and assured bandwidth/throughput) of available external connectivity links towards the provider domain; these describe the connectivity to a NS endpoint (composite NS use case) or to individual NFVI PoPs (NFVIaaS use case), (see clauses 5.1 and 6.1).

The assessment of the impact on NFV-MANO architecture of the mechanisms required for interchanging and processing the referenced information is not addressed in the present document.

7.4 Recommendations related to security

This clause provides recommendations for normative work related to security aspects in accordance with the risk analysis and assessment in annex B.

Table 7.4-1: Recommendations related to security

Identifier	Recommendation	Comments
SEC.001	It is recommended that a requirement be specified for the reference points across administrative domains to verify the authenticity of the consumer and provider of the interfaces in that reference point.	
SEC.002	It is recommended that a requirement be specified to provide means that allow an NFVIaaS consumer to verify that a SW image is not tampered after having been distributed to another administrative domain.	see table 5.2.6-2
SEC.003	It is recommended that a requirement be specified to provide means that prevent the unauthorized usage of SW images in an administrative domain different to the one to which the NFVIaaS consumer has distributed the SW image.	see table 5.2.6-2
SEC.004	It is recommended that a requirement be specified to provide means that ensure the authenticity and integrity of information related to tenant and infrastructure resource groups when this is conveyed in the interfaces across multiple administrative domains.	see table 5.3-1

Annex A:
Operational Flows

A.1 Operational Flows for Network Services provided using multiple administrative domains

A.1.0 Introduction

This clause provides the operational flows of NSD management and network service lifecycle management initiated by the Sender (i.e. OSS/BSS) for managing composite NS in Use Case "Network Services provided using multiple administrative domains" (see clause 6), and corresponding management procedures (related to the management of nested NS) over the reference point Or-Or. It is allowed that the Sender communicating with NFVO-1 in one administrative domain is different from the one communicating with NFVO-2 in another administrative domain (see clause A.1.1).

A.1.1 Composite NSD on-boarding flow

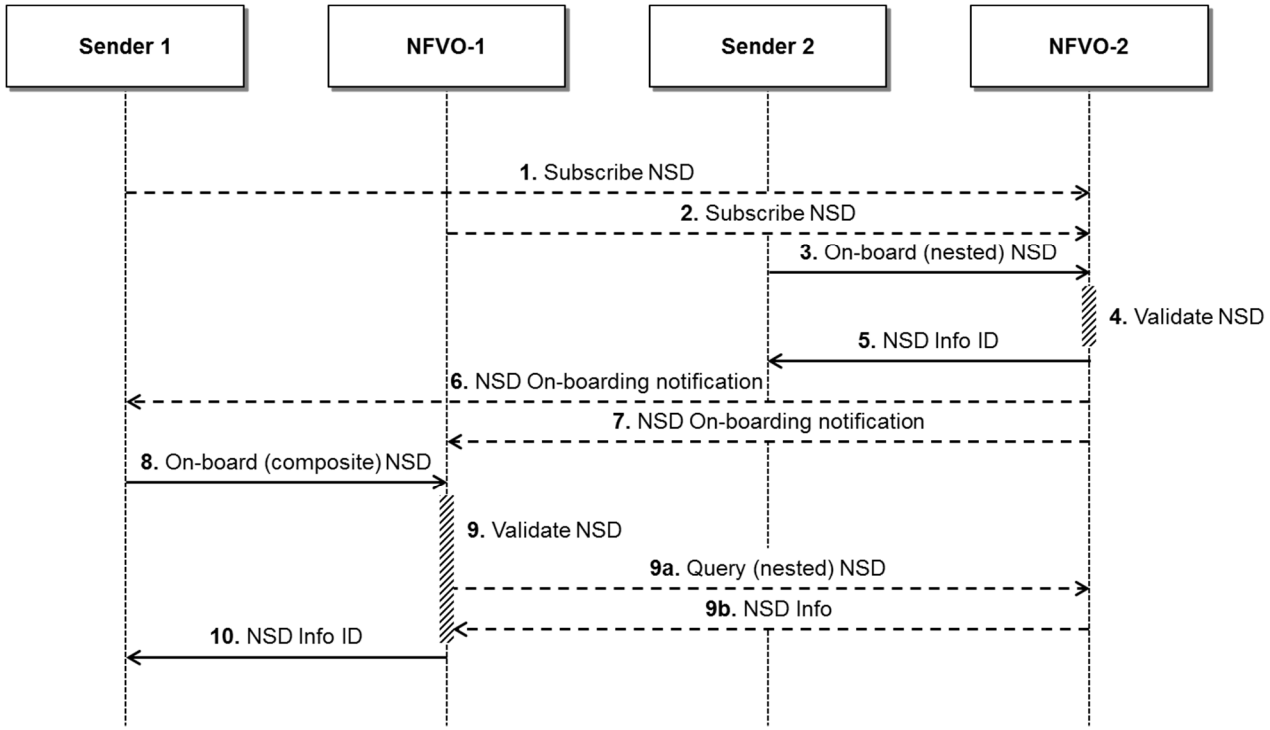

Figure A.1.1-1: Composite NSD on-boarding flow

The following clause describes the on-boarding process applicable to the use case of network services provided using multiple administrative domains. On-boarding flows are asynchronous: i.e. no timing constraints exist between two consecutive on-boarding calls.

NOTE 1: The process below is not the only scenario for composite NSD on-boarding in this use case.

With respect to the message flow depicted in figure A.1.1-1, the following assumptions apply:

- The NSD submitted to NFVO-2 in step 3 does not have any nested NSD.
- The NSD submitted to NFVO-1 in step 8 is a composite NSD which references the NSD submitted to NFVO-2 in step 3.

However, scenarios where NFVO-2 manages composite NSs as well as scenarios where NFVO-1 manages nested NSs are not prevented.

In the following, optionality only refers to a given step of the on-boarding flow and not to any of the capabilities exposed by involved functional blocks.

The main steps are:

1. Optional. Sender 1 subscribes to the NSD notifications (see ETSI GS NFV-IFA 013 [i.9], clause 7.2.12) produced by NFVO-2.

2. Optional. NFVO-1 subscribes to the NSD notifications produced by NFVO-2.

NOTE 2: The way a given NFVO chooses the set of NFVOs whose notifications it needs to subscribe depends on the particular scenario. For example, a suitable approach would be subscribing to the notifications provided by each other "known" NFVO.

NOTE 3: The way a given NFVO chooses the set of notifications produced by another NFVO to subscribe depends on the particular scenario as well. For example, a suitable approach would be subscribing to every produced NSD notification. Alternatively, the filter supported by the subscribe message can be leveraged in order to restrict the amount of received notifications. The selection behaviour might be controlled either via pre-configuration or policy.

3. Sender 2 requests NFVO-2 to on-board a new NSD (see ETSI GS NFV-IFA 013 [i.9], clause 7.2.2).

4. NFVO-2 processes the NSD provided in step 3. As part of this processing, NFVO-2 (non-exhaustive list):

   a) Validates the integrity and authenticity of the NSD.

   b) Checks the existence of mandatory attributes.

   c) Checks whether the VNF Package for every VNF that is part of the NS has been already on-boarded or not.

   d) Checks whether the PNFD for every PNF (if any) that is part of the NS has been already on-boarded or not.

   If any of the above is not satisfied, NFVO-2 is expected to reject the on-boarding request.

5. In case of successful on-boarding, NFVO-2 returns to Sender 2 the ID of the NsdInfo IE.

6. Optional. If Sender 1 has previously subscribed (see step 1), NFVO-2 notifies Sender 1 about the on-boarding of a new NSD (see ETSI GS NFV-IFA 013 [i.9], clause 7.2.13).

NOTE 4: The combination of steps 1 and 6 allows Sender 1 to learn the correct NSD ID by which the NSD provided in step 3 needs to be referenced by the NSD provided in step 8. The present description does not prevent such information to be provided by other means (e.g. pre-configuration).

7. Optional. If NFVO-1 has previously subscribed (see step 2), NFVO-2 notifies NFVO-1 about the on-boarding of a new NSD.

NOTE 5: The combination of steps 2 and 7 allows NFVO-1 to infer the mapping <NSD, Nested NS NFVO>. The present description does not prevent such information to be provided by other means (e.g. pre-configuration).

8. Sender 1 requests NFVO-1 to on-board a new composite NSD referencing the NSD previously submitted to NFVO-2 (see step 3).

9. NFVO-1 processes the NSD provided in step 8. As part of this processing, NFVO-1 (non-exhaustive list):

   - 9a. Validates the integrity and authenticity of the NSD.
   - 9b. Checks the existence of mandatory attributes.
   - 9c. Checks whether the VNF Package for every VNF (if any) that is part of the NS have been already on-boarded or not.
   - 9d. Checks whether the PNFD for every PNF (if any) that is part of the NS have been already on-boarded or not.
   - 9e. Checks whether the NSD for every NS that is part of the NS have been already on-boarded or not.

NOTE 6: NFVO-1 is expected to consult both its own catalogue and the mapping mentioned in note 4 in order to search for the referenced nested NSDs. If no matching NSD is found, NFVO-1 might query other "known" NFVOs (step 9a; see ETSI GS NFV-IFA 013 [i.9], clause 7.2.7) receiving, in case of success, the corresponding NsdInfo IE (step 9b).

If any of the above is not satisfied, NFVO-1 is expected to reject the on-boarding request.

10. In case of successful on-boarding, NFVO-1 returns the ID of the NsdInfo IE.

A.1.2a Top-down Composite NS instantiation

Figure A.1.2a-1 provides the process of a composite NS instantiation by using a top-down method, in which NFVO-1 initiates the instantiation of each nested NS. The process focuses on the interactions over the reference point Or-Or.

The assumptions are:

1. The mapping information <NSD, NFVO-2> is available to NFVO-1 after the composite NSD is on-boarded.
2. There is not an existing nested NS instance which can be directly used by the composite NS for instantiation.
3. Each nested NS instance is not shared by other composite NS.

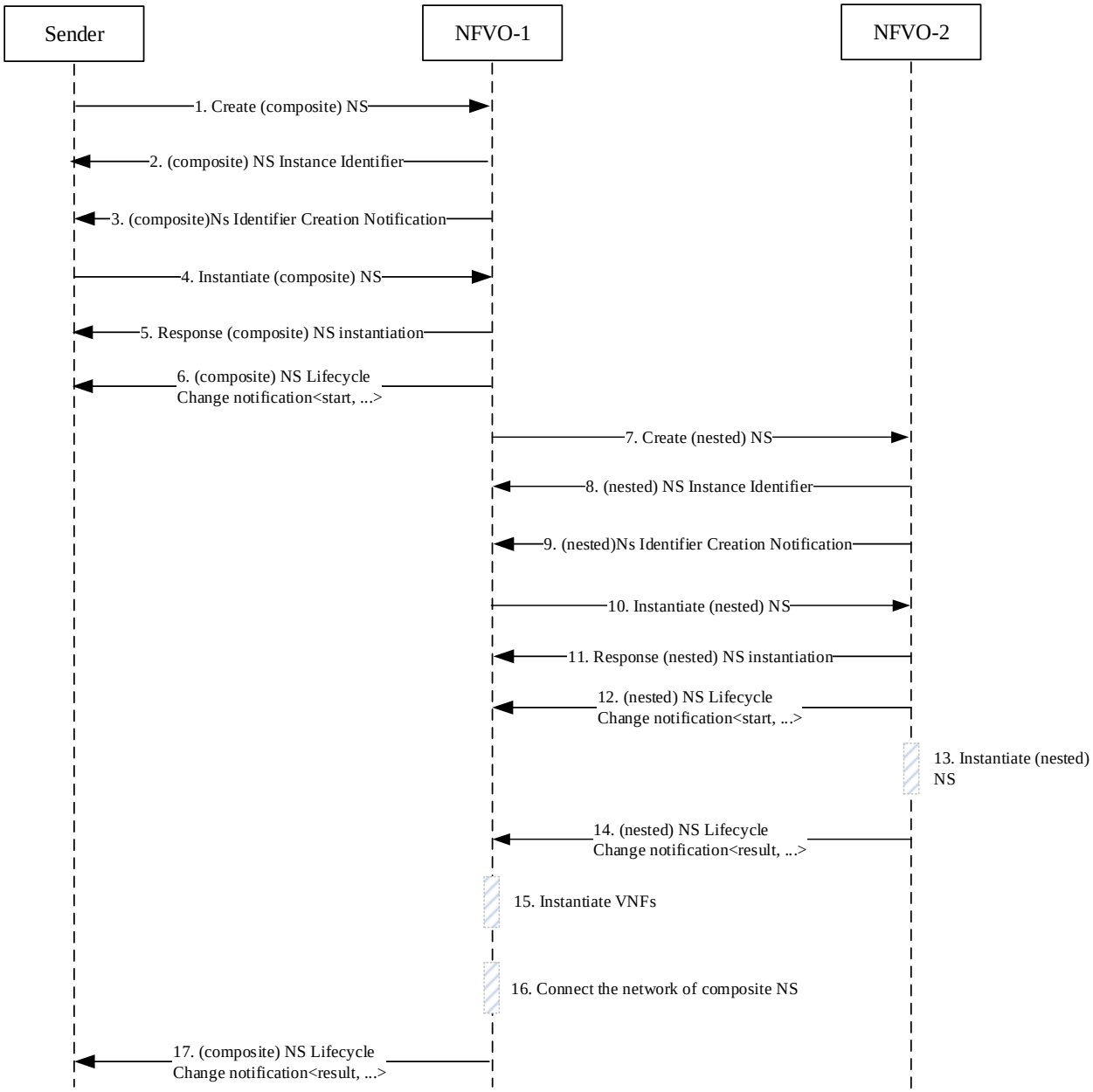

Figure A.1.2a-1: Top-down Composite NS instantiation

1. The Sender sends a request to NFVO-1 for creating an instance ID of the composite NS (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.2).

2. NFVO-1 returns a composite NS Instance ID to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.2).

3. NFVO-1 sends the composite NS Identifier Creation notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.9).

4. The Sender requests NFVO-1 to instantiate the composite NS (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.3).

5. NFVO-1 returns a response to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.3).

6. NFVO-1 obtains the composite NSD, and sends the "instantiation start" Lifecycle Change Notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

7. NFVO-1 finds the corresponding NFVO-2 from the mapping <NSD, NFVO-2> for each nested NSD which constitutes the composite NSD.

   For each constituent nested NS, NFVO-1 requests NFVO-2 to create an instance ID for the nested NS.

8. NFVO-2 processes the operation and returns a nested NS Instance ID to NFVO-1.
9. NFVO-2 sends the nested NS Identifier Creation notification to NFVO-1.
10. NFVO-1 requests NFVO-2 to instantiate the nested NS with the nested NS instance ID.
11. NFVO-2 returns a response of the nested NS instantiation to the Sender.
12. NFVO-2 sends the "instantiation start" Lifecycle Change Notification of the nested NS to NFVO-1.
13. NFVO-2 performs NS instantiation procedure for the nested NS.
14. In case of successful nested NS instantiation, NFVO-2 sends the "result" Lifecycle Change Notification to NFVO-1 (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).
15. If the composite NS includes VNFs that are directly part of the composite NS, NFVO-1 performs VNF instantiation procedure for each VNF.
16. Once all the constituent VNF instances and nested NS instances are available, NFVO-1 connects the constituent VNF instances and nested NS instances of the composite NS instance.
17. In case of successful instantiation for the composite NS, NFVO-1 sends the "result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

A.1.2b Composite NS instantiation in sharing scenario

The operational flow in this clause provides a variant scenario of composite NS instantiation (see clause A.1.2a) in which the nested NS instance of the instantiated composite NS instance is an already existing NS instance used by other composite NS instances. As a result, the nested NS instance is shared by multiple composite NS instances which can be provided in different administrative domains.

There are some assumptions in this flow (as shown in figure A.1.2b-1):

1. The mapping information <(nested) NSD, NFVO-2> is available to NFVO-1 after the composite NSD is on-boarded.
2. There is an existing nested NS instance that is managed by NFVO-2 and can be directly used by the instantiated composite NS.
3. It is the decision of NFVO-1 whether to use the existing NS instance for composing the instantiated composited NS.

With assistance of the mapping information< (nested) NSD, NFVO-2>, NFVO-1 can subscribe to the notification from NFVO-2, on capturing the status change of certain NS instances which are associated with the NSD in the administrative domain that NFVO-2 is located in. The status of NS instance includes for example: created but not instantiated, instantiated but not shared, instantiated and shared, etc. NFVO-1 can further use the status information of the nested NS instance (e.g. instantiated and shared) in that administrative domain for instantiating composite NS (e.g. determine if the existing nested NS instance can be used in the new composite NS).

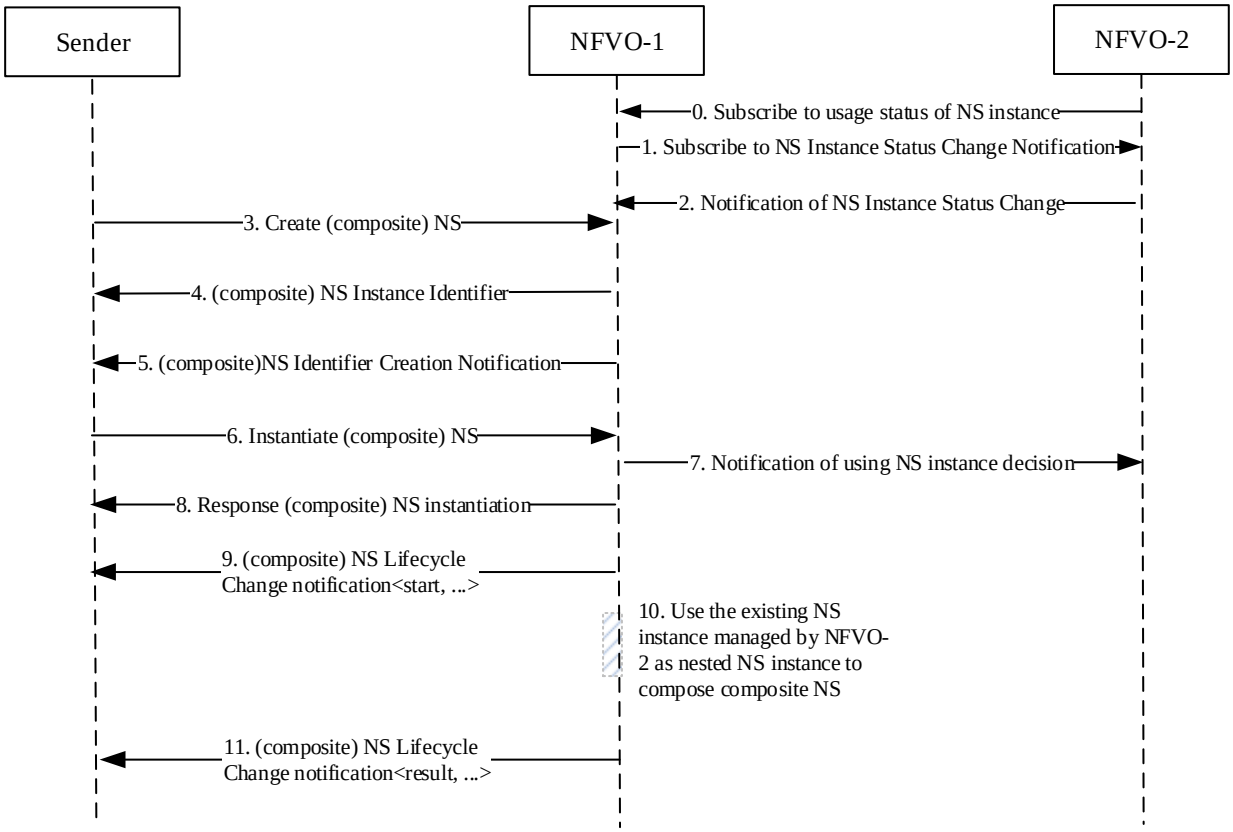

Figure A.1.2b-1: Composite NS instantiation in sharing scenario

0. NFVO-2 subscribes to the notification of NS instance (managed by NFVO-2) usage status from all of the relevant NFVOs (including NFVO-1) who interact with NFVO-2 via Or-Or reference point.

NOTE: The way a given NFVO chooses (e.g. NFVO-2 in this case) the set of NFVOs (e.g. NFVO-1 in this case) whose notifications it needs to subscribe depends on the particular scenario. For example, a suitable approach would be subscribing to the notifications provided by each other "known" NFVO.

1. NFVO-1 subscribes to the notification from NFVO-2 on the status change of certain NS instances (which are associated with a NSD or are directly indicated by NFVO-1) provided in administrative domain that NFVO-2 is located in. The status of NS instance includes: created and not instantiated, instantiated but not shared, instantiated and shared.

2. NFVO-2 sends to NFVO-1 the notification on the NS instance status change with the identifier of NS instance and its new status, when corresponding event occurs.

Step 3 to step 6 execute the same flow as in step 1 to step 4 of clause A.1.2a for the Sender initiates a request to NFVO-1 to instantiate a composite NS.

7. NFVO-1 sends a notification to NFVO-2 for notifying its decision of using an existing NS instance (nested NS) managed by NFVO-2 for instantiating a NS instance (composite NS), based on the status of the existing NS instance (e.g. instantiated and shared) and other constraints like the capacity limitation of the NS instance. NFVO-2 therefore establishes the usage relationship of the existing NS instance (nested NS) and NFVO-1.

8. NFVO-1 returns a response of NS instantiation to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.3).

9. NFVO-1 sends the "instantiation start" Lifecycle Change Notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

10. NFVO-1 uses the existing NS instance managed by NFVO-2 to compose the instantiated composite NS.

11. In case of successful instantiation for the composite NS, NFVO-1 sends the "result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

A.1.3a Composite NS scaling

Figure A.1.3a-1 provides the process of a composite NS, in which NFVO-1 initiates the scaling of each nested NS. The process focuses on the interactions over the reference point Or-Or. The assumption is that each nested NS instance is not shared by other composite NS.

In this case the composite NS scaling operation is requested by OSS/BSS via the Os-Ma-nfvo reference point. The OSS/BSS can provide explicit guidance to NFVO-1 what to scale and in what way, e.g. the OSS/BSS tells NFVO-1 to scale a specific nested NS to a specific scale level.

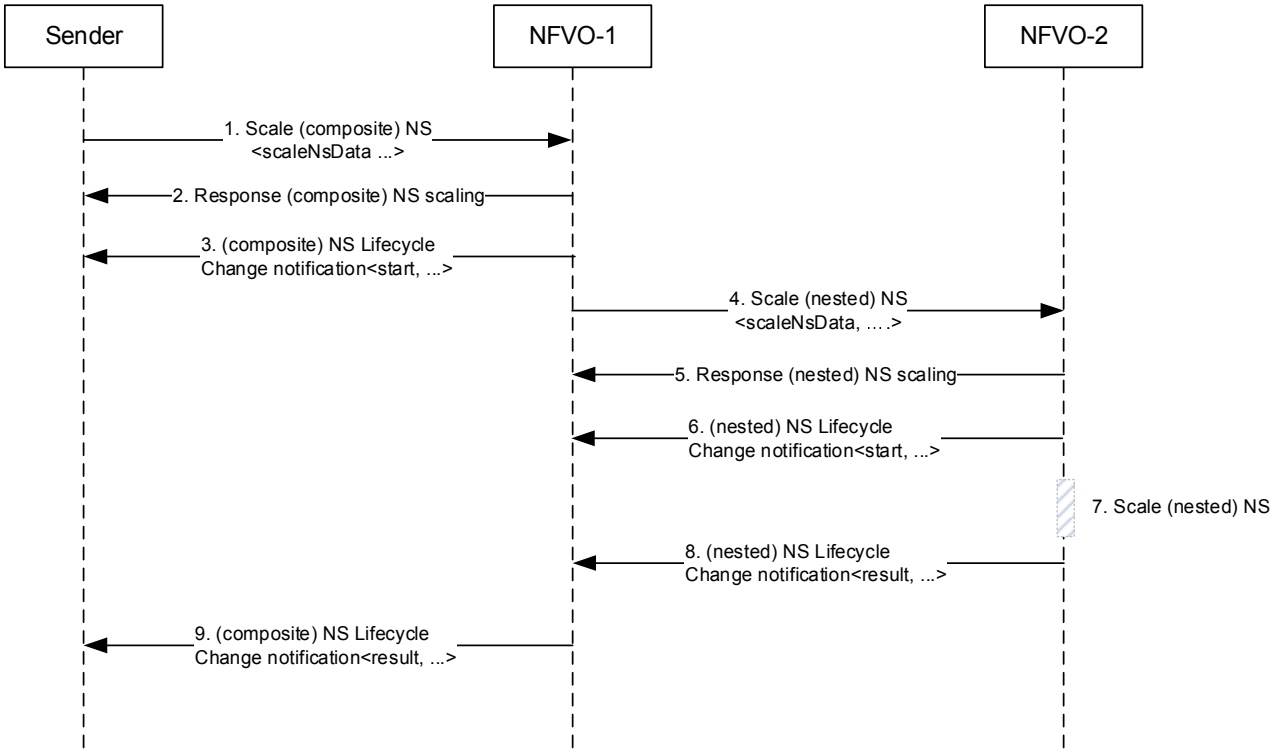

Figure A.1.3a-1: Composite NS scaling

1. The Sender requests NFVO-1 to scale the composite NS including scaleNsData in the request. The scaleNsData indicates the information to scale the referenced nested NS instance.

NOTE: The parameters included in ScaleNS request of the present flow just provide an example of input for a typical NS scaling scenario.

2. NFVO-1 returns a response of scaling composite NS to the Sender.

3. NFVO-1 sends the "scaling start" Lifecycle Change Notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

4. NFVO-1 gets scaleNsData for the constituent nested NS instances and scaleVnfData for the constituent VNFs from the request, and then sends a scaling NS request to the corresponding NFVO-2 to scale the nested NS instance.

5. NFVO-2 returns a response of the nested NS scaling to NFVO-1.

6. NFVO-2 sends the "scaling start" Lifecycle Change Notification of the nested NS to NFVO-1.

7. NFVO-2 performs NS scaling procedure for the nested NS instance according to the scaling data of the nested NS.

8. In case of successful nested NS scaling, NFVO-2 sends the "result" Lifecycle Change Notification to NFVO-1.

9. In case of successful composite NS scaling, NFVO-1 sends the "result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

A.1.3b Composite NS scaling in sharing scenario

The operational flow in this clause provides a variant scenario of composite NS scaling (see clause A.1.3a) in which the nested NS instance composing the composite NS instance is shared by other composite NS instances. In this scenario, when NFVO-2 receives the Scale NS request from NFVO-1, NFVO-2 further initiates corresponding granting procedure to the NFVO who manages the composite NS instance using the shared nested NS instance.

NOTE 1: It is possible that scaling on multiple layers of nested NSs can propagate across multiple administrative domains. For simplicity purpose, it is assumed that only one layer of nested NS is applied in this use case.

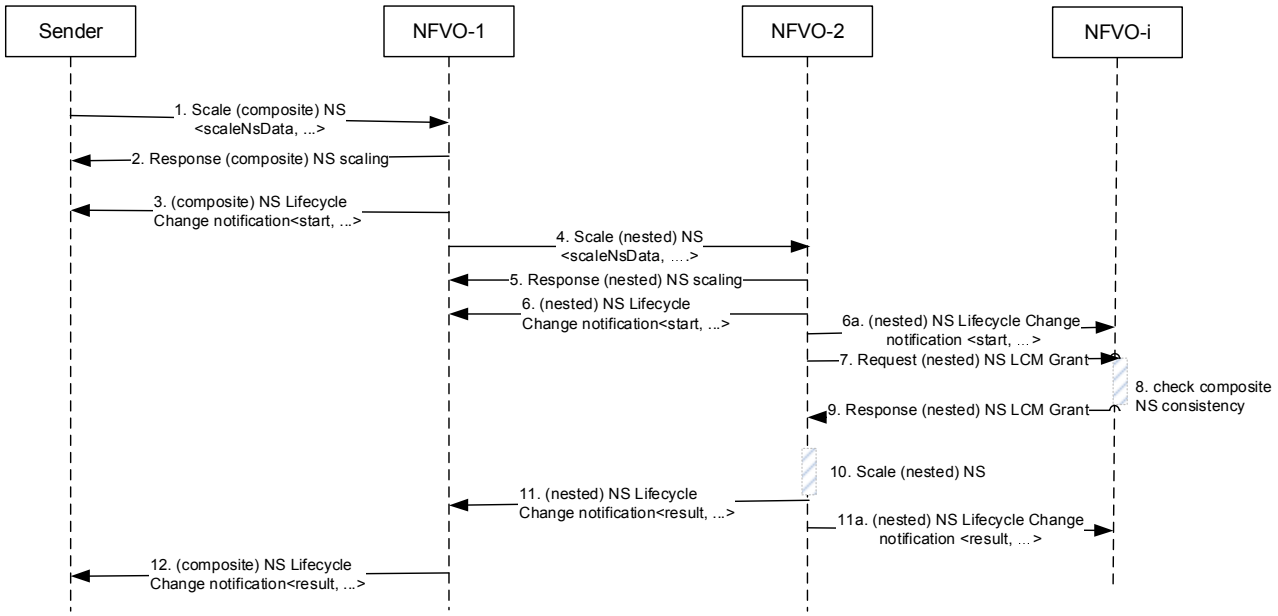

Figure A.1.3b-1: Composite NS scaling in sharing scenario

As shown in figure A.1.3b-1, step 1 to step 6 execute the same flow as in step 1 to step 6 of clause A.1.3a for the Sender initiates a request to NFVO-1 to scale a composite NS and subsequently NFVO-1 sends a ScaleNS request to NFVO-2 for scaling the nested NS instance belonging to that composite NS. NFVO-2 also sends a NS Lifecycle Change notification with the indication of the start and the end to NFVO-i in step 6a and step 11a respectively.

NOTE 2: In step 4, a more generic request could be used (as an alternative to "scale") because NFVO-2 may decide not to scale the (nested) NS but just reconfigure some parameters.

7. NFVO-2 sends a NS LCM Grant request to NFVO-i for requesting a grant of authorization of the nested NS scaling operation. Here NFVO-i manages the composite NS instance(s) which use the nested NS instance to be scaled as well.

8. NFVO-i checks the composite NS consistency (e.g. dependency between the nested NS instance and other constituent of the composite NS instance it manages) which might be impacted by the nested NS scaling operation. If the composite NS consistency is guaranteed by this scaling operation, then NFVO-i approves the grant request. Otherwise, NFVO-i rejects the grant request.

9. NFVO-i returns a NS LCM Grant response to NFVO-2 with indicating the approval or rejection of the grant.

NOTE 3: Step 7 to step 9 follows step 5 to step 7 in the operational flow of clause A.1.6 on granting nested NS lifecycle operation.

NOTE 4: NFVO-i can be one or more NFVOs which manage the composite NS(s) using the shared nested NS. NFVO-1 can act as NFVO-i as well in some cases.

Step 10 to step 12 execute the same flow as in step 7 to step 10 of clause A.1.3a for completing the remaining steps in the composite NS scaling process.

A.1.4 Composite NS termination

Figure A.1.4-1 provides the process of terminating a composite NS instance, in which NFVO-1 further disassociates the nested NS instance (managed by NFVO-2) from the terminated composite NS instance and sends a notification to NFVO-2.

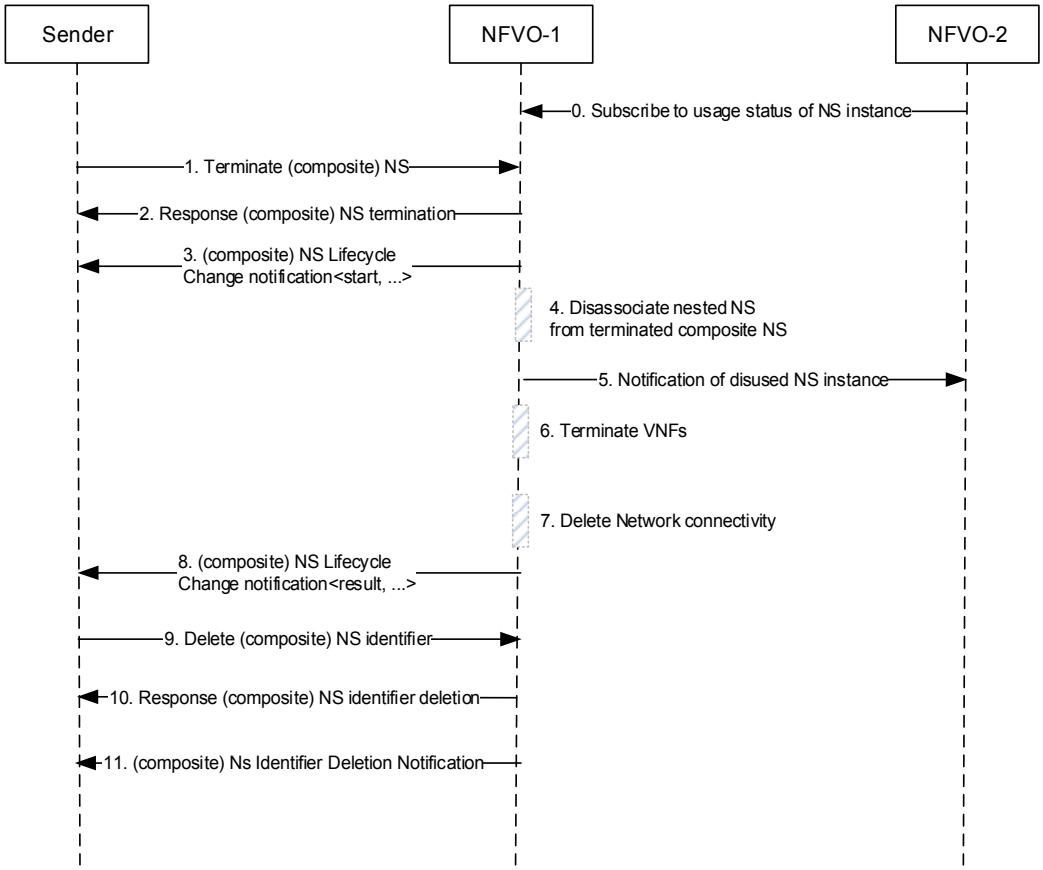

Figure A.1.4-1: Composite NS termination

0. NFVO-2 subscribes to the notification of NS instance (managed by NFVO-2) usage status from all of the relevant NFVOs (including NFVO-1) who interact with NFVO-2 via Or-Or reference point.

NOTE 1: The way a given NFVO chooses (e.g. NFVO-2 in this case) the set of NFVOs (e.g. NFVO-1 in this case) whose notifications it needs to subscribe depends on the particular scenario. For example, a suitable approach would be subscribing to the notifications provided by each other "known" NFVO.

1. The Sender sends a request to NFVO-1 to terminate an instance of a composite NS (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.7).

2. NFVO-1 returns a response of the composite NS termination to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.7).

3. NFVO-1 sends the "termination start" Lifecycle Change Notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

4. NFVO-1 disassociates nested NS instance (managed by NFVO-2) from the terminated composite NS instance.

NOTE 2: There is no difference in this step for the case of whether or not the nested NS instance is shared by other composite NS instance(s) since the nested NS instance is just released (not used by the terminated NS instance) but not terminated.

5. NFVO-1 sends a notification to NFVO-2 for notifying the disuse of the nested NS instance managed by NFVO-2. NFVO-2 therefore releases the usage relationship of the nested NS instance and NFVO-1.

6. If the composite NS includes VNFs that are directly part of the composite NS, NFVO-1 performs VNF termination procedure to terminate these VNF instances.

7. Once all the constituent VNF instances and nested NS instances are terminated, NFVO-1 deletes the connections of the composite NS instance.

8. In case of successful composite NS termination, NFVO-1 sends the "result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

9. The Sender sends a request to NFVO-1 to delete the composite NS instance identifier (see ETSI GS NFV-IFA 013 [i.9], clause7.3.8).

10. NFVO-1 returns a response of the composite NS identifier deletion to the Sender.

11. In case of successful deletion, NFVO-1 sends the composite NS Identifier Deletion notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.10).

A.1.5 Bottom-up Composite NS instantiation

Figure A.1.5-1 provides the process of a composite NS by using a bottom-up method, in which the Sender initiates the instantiation of each nested NS before instantiation of the composite NS. The process focuses on the interactions over the reference point Or-Or.

The assumptions are:

1. The mapping information <nestedNsdId, NFVO-2> is available to NFVO-1 after the composite NSD is on-boarded.

2. Each nested NS instance is not shared by other composite NS.

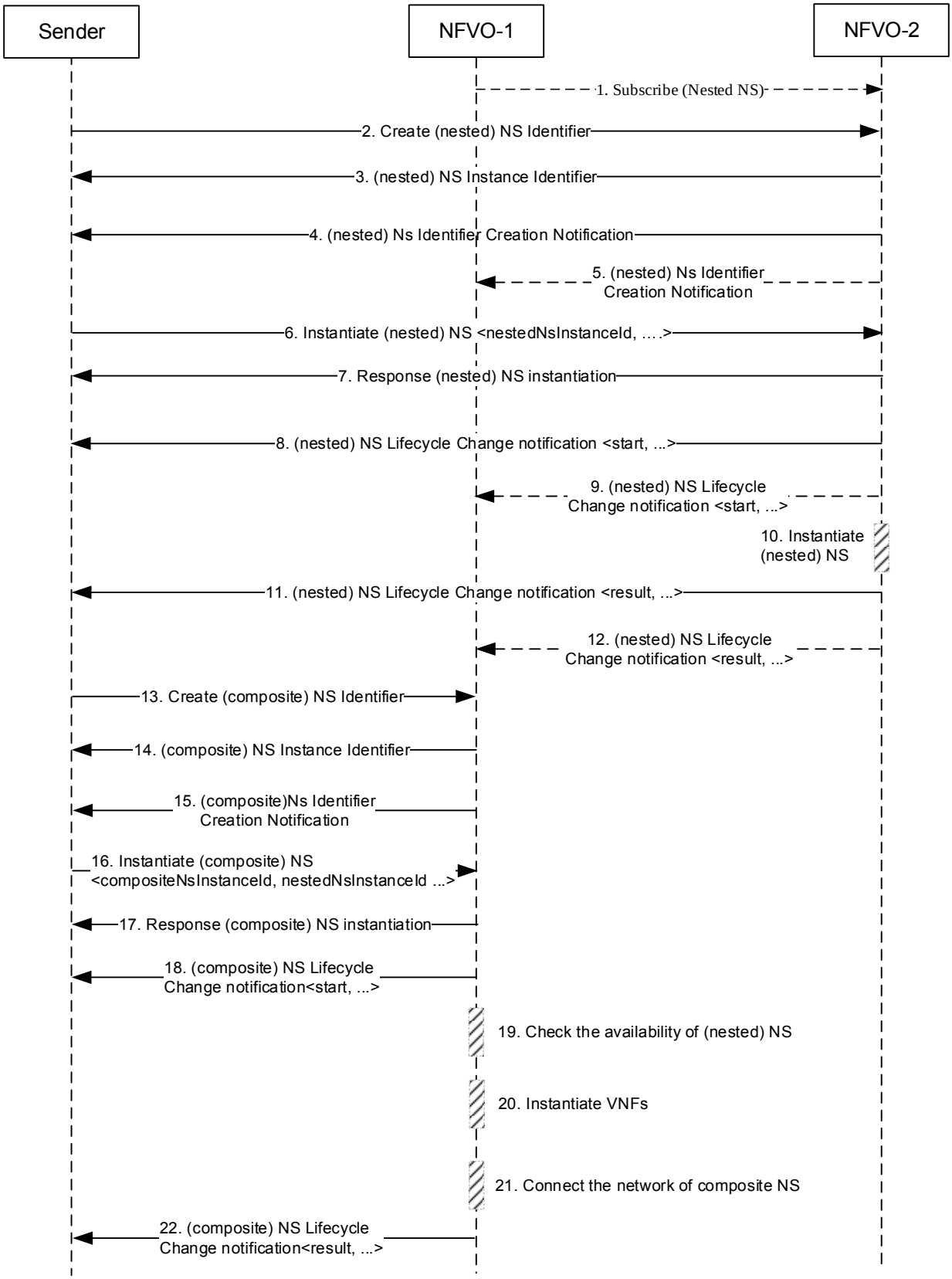

Figure A.1.5-1: Bottom-up Composite NS instantiation

1. NFVO-1 subscribes to the nested NS notifications about NS lifecycle changes (see ETSI GS NFV-IFA 013 [i.9], clause 7.4) produced by NFVO-2.

2. The Sender sends a request to NFVO-2 for creating an instance ID of the nested NS (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.2).

3. NFVO-2 returns a nested NS instance ID to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.2).

4. NFVO-2 sends a nested NS Identifier Creation notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.4.3 and clause 8.3.2.9).

5. If NFVO-1 has previously subscribed (see step 1), NFVO-2 notifies NFVO-1 about the creation of the nested NS instance identifier (see ETSI GS NFV-IFA 013 [i.9], clause 7.4.3 and clause 8.3.2.9).

6. The Sender requests NFVO-2 to instantiate the nested NS with the nested NS instance ID (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.3).

7. NFVO-2 returns a response to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.3).

8. NFVO-2 sends the "instantiation start" Lifecycle Change Notification of the nested NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.4.3 and clause 8.3.2.2).

9. If NFVO-1 has previously subscribed (see step 1), NFVO-2 notifies NFVO-1 about the "instantiation start" lifecycle change of the nested NS instance (see ETSI GS NFV-IFA 013 [i.9], clause 7.4.3 and clause 8.3.2.2).

10. NFVO-2 performs NS instantiation procedure to instantiate the nested NS.

11. In case of successful nested NS instantiation, NFVO-2 sends the "instantiation result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.4.3 and clause 8.3.2.2).

12. If NFVO-1 has previously subscribed (see step 1), NFVO-2 notifies NFVO-1 about the "instantiation result" lifecycle change of the nested NS instance (see ETSI GS NFV-IFA 013 [i.9], clause 7.4.3 and clause 8.3.2.2).

13. Once all nested NSs are instantiated, the Sender sends a request to NFVO-1 for creating an instance ID of the composite NS (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.2).

14. NFVO-1 returns a composite NS Instance ID to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.2).

15. NFVO-1 sends a composite NS Identifier Creation notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.9).

16. The Sender requests NFVO-1 to instantiate the composite NS with the composite NS instance ID and the nested NS Instance ID as parameter.

17. NFVO-1 returns a response to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.3).

18. NFVO-1 sends the "instantiation start" Lifecycle Change Notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

19. NFVO-1 checks the available of the required nested NS instances according to the notification of step 11.

20. If the Composite NS includes VNFs that are directly part of the composite NS, NFVO-1 performs VNF instantiation procedure to instantiate these VNF instances.

21. Once all the constituent VNF instances and nested NS instances are available, NFVO-1 connects the constituent VNF instances and nested NS instances of the composite NS instance.

22. In case of successful composite NS instantiation, NFVO-1 sends the "instantiation result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

A.1.6 Granting nested NS lifecycle operation

Granting is generally applied for the permission to perform a VNF lifecycle management operation and the resource management operations necessary to complete it. In this use case, considering the nested NS lifecycle operations, NFVO-1 is unaware of the resource status of administrative domain in which nested NS is provided, and cannot provide to NFVO-2 the information where the virtualised resources are allocated to nested NS instance. But it is still necessary for NFVO-1 to check the composite NS consistency which can be potentially impacted by the nested NS lifecycle operation performed by NFVO-2. Therefore, granting mechanism is applied for nested NS lifecycle operations over the Or-Or reference point.

Figure A.1.6-1 provides the process of applying granting in nested NS lifecycle operation, in which NFVO-2 requests a grant for authorization of a nested NS lifecycle operation, and NFVO-1 approves or rejects the request by checking composite NS consistency impacted by the nested NS lifecycle operation. According to the operational flow analysis for NS LCM in this study, the NS lifecycle operations applying granting include: NS scaling and NS healing.

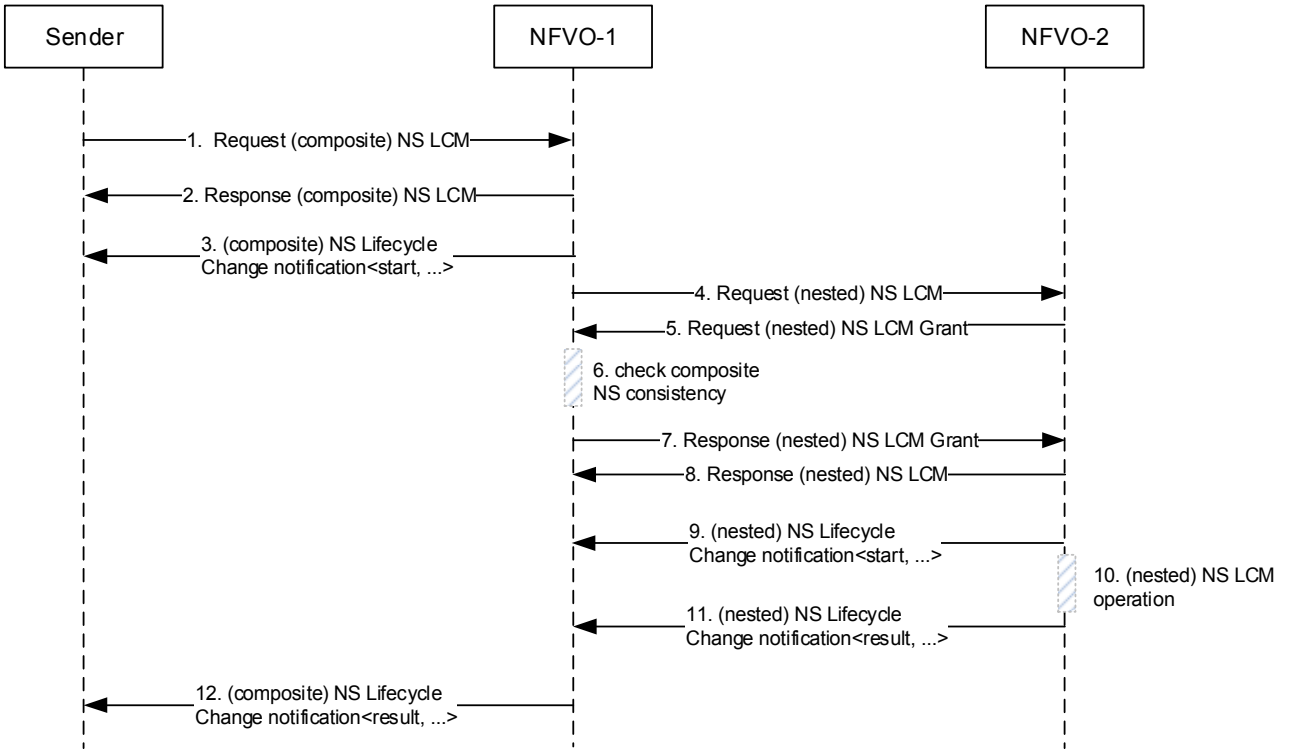

Figure A.1.6-1: Granting nested NS lifecycle operation

1. The Sender sends a NS LCM request to NFVO-1 for performing a LCM operation for the composite NS.
2. NFVO-1 returns a NS LCM response to the Sender.
3. NFVO-1 sends the "LCM operation start" Lifecycle Change Notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).
4. NFVO-1 creates a NS LCM request for performing a LCM operation for the nested NS, and then sends the NS LCM request to the corresponding NFVO-2 to perform the LCM operation for the nested NS instance.
5. NFVO-2 sends a NS LCM Grant request to NFVO-1 for requesting a grant of authorization of the nested NS LCM operation.
6. NFVO-1 checks the composite NS consistency (e.g. dependency between the nested NS instance and other constituent of the composite NS instance) which can be impacted by the nested NS lifecycle operation. If the composite NS consistency is guaranteed by this operation, then NFVO-1 approves the grant request. Otherwise, NFVO-1 rejects the grant request.
7. NFVO-1 returns a NS LCM Grant response to NFVO-2 with indicating the approval or rejection of the grant.

8. In case of grant approval, NFVO-2 returns a NS LCM response to NFVO-1 with including the success indication.

9. NFVO-2 sends the "LCM operation start" Lifecycle Change Notification of the nested NS to NFVO-1.

10. NFVO-2 performs NS LCM operation for the nested NS instance.

11. In case of successful nested NS LCM operation, NFVO-2 sends the "result" Lifecycle Change Notification to NFVO-1 (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

12. In case of successful composite NS LCM operation, NFVO-1 sends the "result" Lifecycle Change Notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

A.1.7a Composite NS healing

Figure A.1.7a-1 provides the process of a composite NS healing, in which NFVO-1 initiates the healing of each nested NS. The assumption is that each nested NS instance is not shared by other composite NS.

In this case the composite NS healing operation is requested by the Sender (i.e. OSS/BSS) via the Os-Ma-nfvo reference point. The Sender can provide explicit guidance to NFVO-1 on what constituent nested NS or VNFs within this composite NS to be healed and in what way to heal, e.g. the OSS/BSS tells NFVO-1 to heal a specific nested NS following healNsData information included in the request message. NFVO-1 further initiates NS healing request to NFVO-2 for healing the nested NS in the corresponding administrative domain.

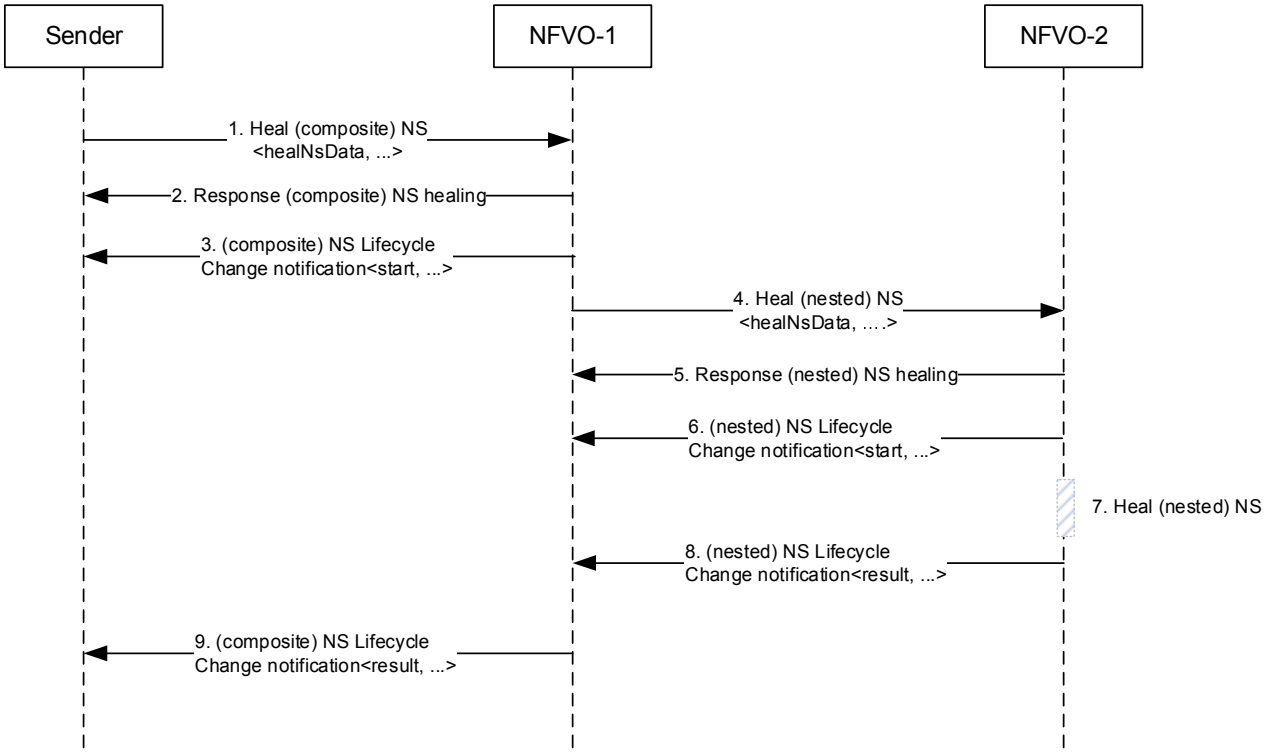

Figure A.1.7a-1: Composite NS healing

The flow of composite NS healing is similar to the one of composite NS scaling (see clause A.1.3a), with the replacement of ScaleNS operation to HealNS operation, and corresponding adaptation of input parameters (e.g. change scaleNsData to healNsData) in request messages.

A.1.7b Composite NS heal in sharing scenario

The operational flow in this clause provides a variant scenario of composite NS healing (see clause A.1.7a) in which the nested NS instance composing the composite NS instance is shared by other composite NS instances. In this scenario, when NFVO-2 receives the Heal NS request from NFVO-1, NFVO-2 further initiates corresponding granting procedure to the NFVO who manages the composite NS instance using the shared nested NS instance.

NOTE: It is possible that healing on multiple layers of nested NSs can propagate across multiple administrative domains. For simplicity purpose, it is assumed that only one layer of nested NS is applied in this use case.

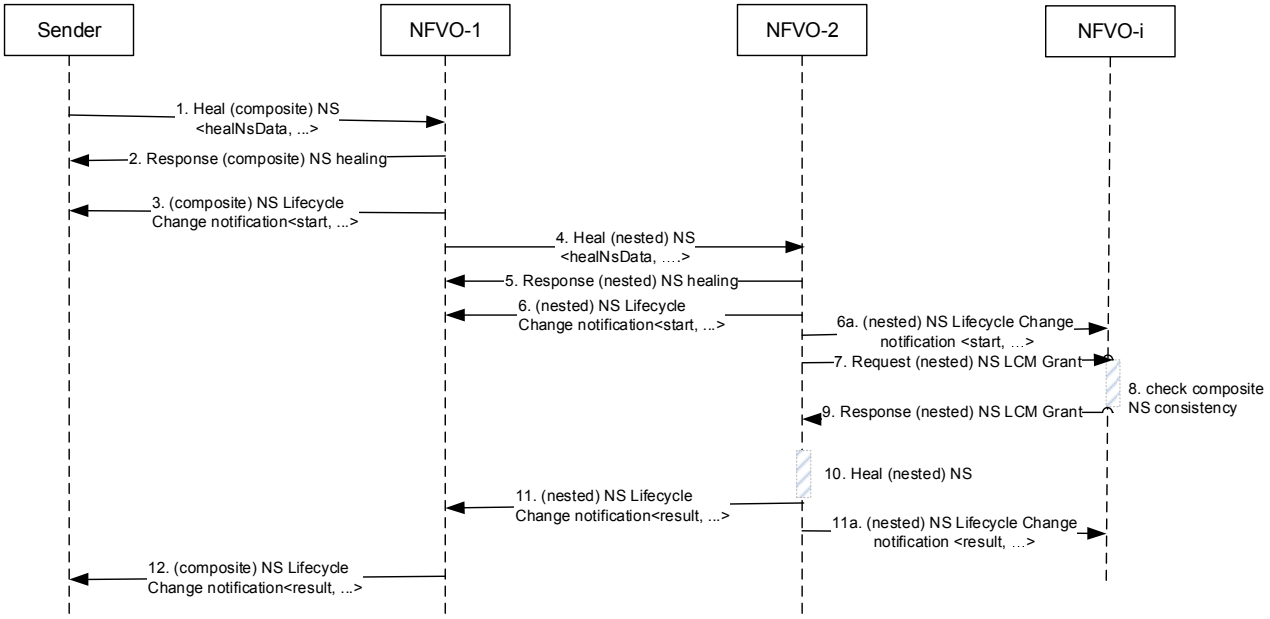

Figure A.1.7b-1: Composite NS healing in sharing scenario

The flow of composite NS healing is similar to the one of composite NS scaling (see clause A.1.3b) in the nested NS sharing scenario, with the replacement of Scale NS operation to Heal NS operation, and corresponding adaptation of input parameters (e.g. change scaleNsData to healNsData) in request messages.

A.1.8 Composite NS update

Figure A.1.8-1 provides the process of a composite NS update, in which the composite NS managed by NFVO-1 has a nested NS managed by NFVO-2. The process focuses on the interactions over the reference point Or-Or. The case of nested NS sharing does not apply to this process.

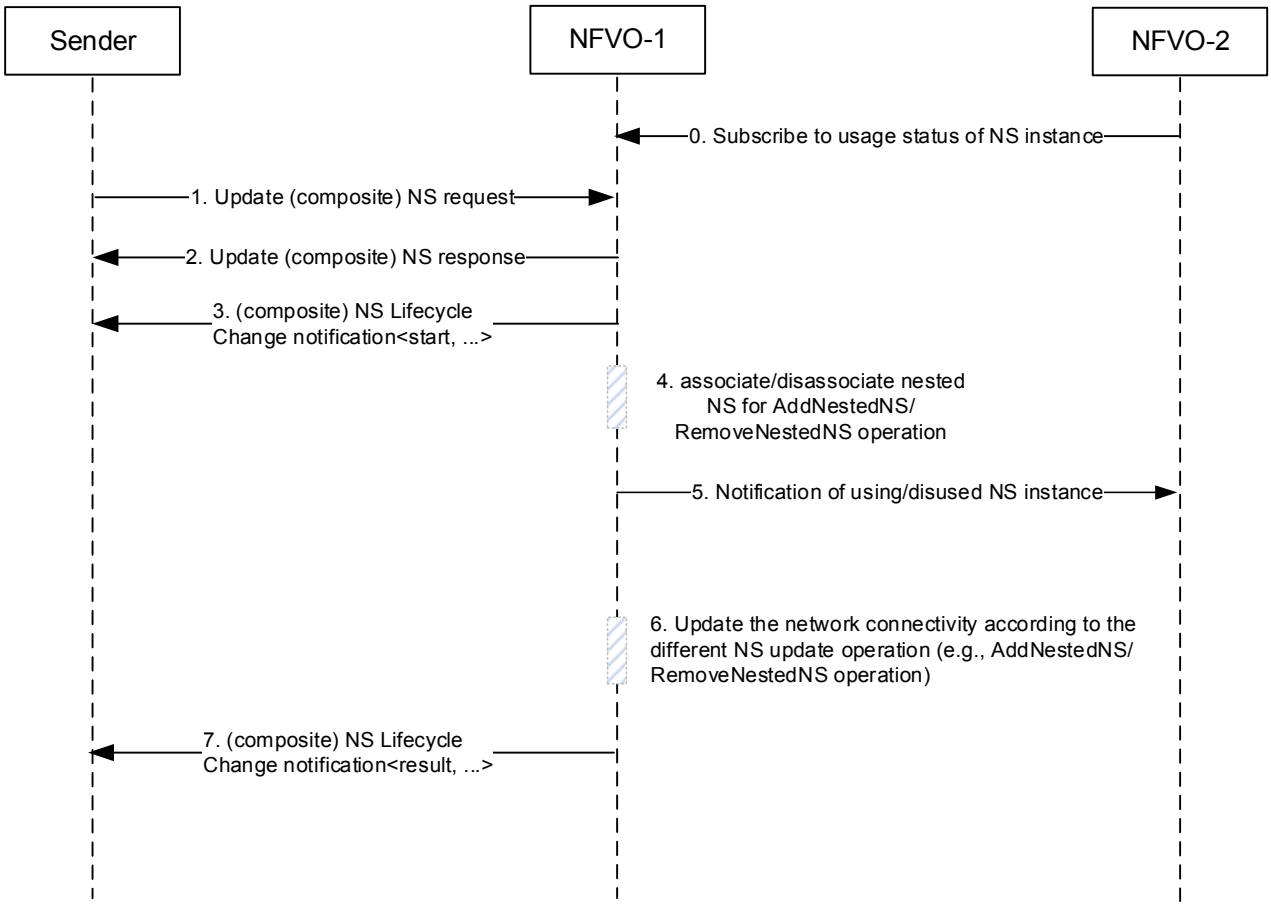

Figure A.1.8-1: Composite NS update

0. NFVO-2 subscribes to the notification of NS instance (managed by NFVO-2) usage status from all of the relevant NFVOs (including NFVO-1) who interact with NFVO-2 via Or-Or reference point.

NOTE 1: The way a given NFVO chooses (e.g. NFVO-2 in this case) the set of NFVOs (e.g. NFVO-1 in this case) whose notifications it needs to subscribe depends on the particular scenario. For example, a suitable approach would be subscribing to the notifications provided by each other "known" NFVO.

1. The Sender sends a NS Update request to NFVO-1 for performing an update operation (e.g. AddNestedNS, RemoveNestedNS) for the composite NS (see ETSI GS NFV-IFA 013 [i.9], clause 7.3.5).

2. NFVO-1 returns a NS Update response to the Sender.

3. NFVO-1 sends the "update start" NS Lifecycle Change notification of the composite NS to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

4. If the update operation acts directly on the nested NS instances, NFVO-1 performs the following process:

   a) If the operation is AddNestedNS, NFVO-1 associates the nested NS instance (managed by NFVO-2) with the updated composite NS instance.

   b) If the operation is RemoveNestedNS, NFVO-1 disassociates nested NS instance (managed by NFVO-2) from the updated composite NS instance.

NOTE 2: The Update NS operation does not allow to add and remove nested NS instances in the same operation.

5. NFVO-1 sends a notification to NFVO-2 for notifying the usage/disuse of the nested NS instance managed by NFVO-2. NFVO-2 therefore creates/releases the usage relationship of the nested NS instance and NFVO-1.

6. In case of successful update for all the nested NSs and the constituent VNF instances, NFVO-1 performs the update operation for the network connectivity of the composite NS. For example:

a) If the operation is AddNestedNS, NFVO-1 establishes a new network connectivity between the composite NS and the nested NS.

b) If the operation is RemoveNestedNS, NFVO-1 releases the network connectivity between the composite NS and the nested NS.

7. In case of successful update for the composite NS, NFVO-1 sends the "result" NS Lifecycle Change notification to the Sender (see ETSI GS NFV-IFA 013 [i.9], clause 8.3.2.2).

Annex B:
Pro forma of Security and Regulatory Concerns for use in ETSI ISG NFV GSs

B.1 Risk analysis and assessment

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the pro forma in this clause so that it can be used for its intended purposes.

A Security Environment		
a.1 Assumptions		
a.1.1	The use "Network Services provided using multiple administrative domains" described in the present document relies on functionality specified in ETSI GS NFV-IFA 013. Hence, many of the assets, threats, threat agents, security objectives, etc. are common to those derived from ETSI GS NFV-IFA 013. The present risk analysis and assessment only considers those that are specific to this use case and not common to ETSI GS NFV-IFA 013.	*Citation for full text*
a.1.2	The use case "NFVIaaS" described in the present document relies on functionality specified in ETSI GS NFV-IFA 005 and ETSI GS NFV-IFA 006. Hence, many of the assets, threats, threat agents, security objectives, etc. are common to those derived from ETSI GS NFV-IFA 005 and ETSI GS NFV IFA 006. The present risk analysis and assessment only considers those that are specific to this use case and not common to ETSI GS NFV-IFA 005 and ETSI GS NFV-IFA 006.	
GUIDANCE: *to be added by reference to ETSI TS 102 165-1*		
a.2 Assets		
a.2.1	NS instances	see clause 6 and annex A. Vulnerable to attacks from threat agents: a.3.1 > a.3.2 > a.3.3 >
a.2.2	NSDs	see annex A. Vulnerable to attacks from threat agents: a.3.2
a.2.3	Infrastructure resource groups	see clauses 5.2.2, 5.2.3, 5.2.4 and 5.2.5. Vulnerable to attacks from threat agents: a.3.3 a.3.5
a.2.4	SW images	see clauses 5.2.2, 5.2.3, 5.2.4 and 5.2.5. Vulnerable to attacks from threat agents: a.3.2 a.3.3 a.3.4

A Security Environment		
a.3 Threat agents		
a.3.1	Unauthorized user of NSs in other administrative domain	see clause A.1.2b Threats: a.4.1.1
a.3.2	Industrial espionage agent	Threats: a.4.1.5 a.4.1.7 a.4.1.10
a.3.3	Sabotage agent	Threats: a.4.1.2 a.4.1.4 a.4.1.6 a.4.1.9
a.3.4	Internal threat agent, e.g. disgruntled, corrupt employee, etc.	Threats: a.4.1.9 a.4.1.10
a.3.5	Illegal or abusive NFVIaaS tenant	Threats: a.4.1.3 a.4.1.8
a.4 Threats		
a.4.1.1	Unauthorized use of existing NS instances in other administrative domain. For example, fraudulent use of nested NS to offer a composite NS to end-users	see clause A.1.2b Related security objectives: b.1.1 b.1.2 b.1.7
a.4.1.2	Exhaustion of NS resources by illegal and excessive use	Related security objectives: b.1.1 b.1.2
a.4.1.3	Profit loss by unauthorized or hidden use of infrastructure resources	Related security objectives: b.1.4
a.4.1.4	Exhaustion of infrastructure resources by illegal and excessive use	Related security objectives: b.1.4
a.4.1.5	Inappropriate information disclosure: illegal interception in the Or-Or reference point	see clause 7 and annex A. Related security objectives: b.1.8
a.4.1.6	Denial of service: refusal of grant requests (for scaling and healing nested NS instances)	see clauses A.1.3b and A.1.7b Related security objective: b.1.9
a.4.1.7	Inappropriate information disclosure: illegal query of NSDs	see clause A.1.1 Related security objectives: b.1.3
a.4.1.8	Breach in data isolation: infrastructure tenant performing management related to an infrastructure resource group assigned to another tenant. This includes creating, reserving, terminating virtualised resources, getting information of them, performing quota management, etc.	see clauses 5.2.2, 5.2.3, 5.2.4 and 5.2.5 Related security objectives: b.1.3
a.4.1.9	Tampering of SW images	see clauses 5.2.2, 5.2.3, 5.2.4 and 5.2.5 Related security objectives: b.1.5

A Security Environment			
a.4.1.10	Illegal use or copy of SW images		see clauses 5.2.2, 5.2.3, 5.2.4 and 5.2.5 Related security objectives: b.1.6
a.5 Security policies (OPTIONAL)			
a.5.1	*Short text describing security policy*		*Citation for full text*
a.5.2			
B Security Objectives			
b.1 Security objectives for the asset			
b.1.1	NS instances can only be used by authorized users		*Citation for full text*
b.1.2	LCM of NS instances can only be requested by authorized users		
b.1.3	NSDs can only be retrieved by authorized users		
b.1.4	An infrastructure tenant can only request LCM of virtualised resources and quota management related to the infrastructure resource group that has been assigned to it		
b.1.5	The integrity of the NFVIaaS consumer's SW images, once distributed to the NFVIaaS provider, is ensured		
b.1.6	The illegal use of NFVIaaS consumer's SW images is prevented		
b.1.7	The NFVO is able to isolate data originated from different administrative domains when required. Note: sharing of data among administrative domains (e.g. NSDs, data belonging to NS instances, etc.) may also be allowed as shown in annex A		
b.1.8	It is ensured that interception is possible where required to support regulatory requirements (such as Lawful Interception ETSI GS NFV-SEC 004 [i.14] and Retained Data ETSI GS NFV-SEC 010 [i.15]) and not possible otherwise		
b.1.9	The authenticity of the provider of the NS lifecycle operation granting interface is ensured		
b.2 Security objectives for the environment			
b.2.1	*Short text describing objective for the requirement*		*Citation for full text*
b.2.2			
C IT Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	*Short text describing security functional requirement*	*ISO15408 class*	*Citation for full text*
c.1.1.2			
c.1.2 asset security assurance requirements			
c.1.2.1	*Short text describing security assurance requirement*	*ISO15408 class*	*Citation for full text*
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	*Short text describing security environment requirement*	*ISO15408 class*	*Citation for full text*
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
The TVRA should define the full rational, if this is true only a citation (reference) to the full text is required.			

In completing the pro forma above it has been shown in best practice from a number of applications in ETSI projects (including TISPAN, RRS and ITS) that the table can be built using specially crafted bookmarks and document automation although if the table scans multiple documents this is obviously more difficult.

Annex C:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Xia Haitao, Huawei Technologies

Previous Rapporteur:
Astrid Mann, Huawei Technologies (version 0.1.0 to 0.11.0)

Other contributors:
Anatoly Adriano, Nokia

Arturo Martin De Nicolas, Ericsson

Balasz Peter Gero, Ericsson

Bhumip Khasnabish, ZTE

Bruno Chatras, ORANGE

Carlos J. Bernardos, Universidad Carlos III de Madrid

Diego López, Telefonica

Feng Aijuan, Huawei Technologies

Gang He, China Unicom

Janusz Pieczerak, ORANGE

Jie Miao, China Unicom

Luis M. Contreras, Telefonica

Marco Di Girolamo, Hewlett Packard Enterprise

Annex D: Change history

Date	Version	Information about changes
16.01.2017	0.1.0	Early draft implementing the following contributions: • NFVIFA(16)0001454r1: ToC • NFVIFA(16)0001455r3: Scope • NFVIFA(17)00001r1: clause 4, Overview
24.01.2017	0.2.0	Contributions implemented in v0.2.0: • NFVIFA(17)000009r3: NFVIaaS description • NFVIFA(17)000017r1: Use case of network services provided using multiple administrative domains The placeholder clause for use case analysis is moved to the end, i.e. is now clause 7. Further editorial fixes.
27.02.2017	0.3.0	Contributions implemented in v0.3.0: • NFVIFA(17)000051r3: NFVIaaS description enhancements • NFVIFA(17)000078r2: clause 5.2: NFVIaaS architecture options overview • NFVIFA(17)000079r2: clause 5.2: NFVIaaS architecture option 1.a • NFVIFA(17)000107r4: Composite NSD on boarding flow • NFVIFA(17)000108r1: Composite NS instantiation Editorial fixes.
29.03.2017	0.4.0	Contributions implemented in v0.4.0: • NFVIFA(17)000202r1: A.1.3 composite NS scaling • NFVIFA(17)000203r1: A.1.4 composite NS termination • NFVIFA(17)000204r2: A.1.5 Bottom-up instantiation of composite NS • NFVIFA(17)000208r1: 6.2 Potential architectural option on use case #2 • NFVIFA(17)000209r1: 6.3 Analysis on enhancement to MANO architecture MLPOC and SLPOC added to the abbreviation clause (rapporteur's action). Editorial fixes.
20.04.2017	0.5.0	Contributions implemented in v0.5.0: NFVIFA(17)000263r1: IFA028, clause 5.2.3: NFVIaaS architecture option 1.b NFVIFA(17)000264r1: IFA028, clause 5.2.4: NFVIaaS architecture option 2.a NFVIFA(17)000265r1: IFA028, clause 5.2.5: NFVIaaS architecture option 2.b NFVIaaS added to the abbreviation clause (rapporteur's action) Editorial fixes.
03.05.2017	0.6.0	Contributions implemented in v0.6.0: • NFVIFA(17)000321r1: IFA028, clause 5.2: Resolve EN • NFVIFA(17)000322r1: IFA028, clause 5.2: Clarification on limiting the scope of operations • NFVIFA(17)000327r2: IFA028, A.1.x Add nested NS lifecycle operation granting operational flow in use case #2 Editorial fixes.
08.06.2017	0.7.0	Contributions implemented in v0.7.0: • NFVIFA(17)000323r2: IFA028, clause 5.2: Comparison of architecture options • NFVIFA(17)000396r2: IFA028 A.1.2b Composite NS instantiation by using the existing nested NS instance • NFVIFA(17)000397r3: IFA028 A.1.3b Composite NS scaling in case of shared nested NS • NFVIFA(17)000398r1: IFA028 A.1.4b Composite NS termination in case of shared nested NS • NFVIFA(17)000490r3: IFA028, clause 5.2.7: MLPOC, SLPOC integration • NFVIFA(17)000491r2: IFA028, clause 5.3: Architecture enhancements Editorial fixes.

Date	Version	Information about changes
03.08.2017	0.8.0	Contributions implemented in v0.8.0: • NFVIFA(17)000587r1: IFA028, clause 6: Multi-tenancy • NFVIFA(17)000584r1: IFA028, NFVIaaS: Resolve editor's notes (1) • NFVIFA(17)000585: IFA028, NFVIaaS: Resolve editor's notes (2) • NFVIFA(17)000646r1: IFA028 A.1.x Add composite NS healing operational flows in use case #2 • NFVIFA(17)000647: IFA028 A.1.3 Editor's note removal on scaleNestedNSData • NFVIFA(17)000661: IFA028, clause 5.1 clarification of FB relation • NFVIFA(17)000663r1: IFA028, clause 8: Conclusions and recommendations As rapporteur's actions: • "please refer to" replaced by "refer to" • Additional contributors added. • LCM added to the abbreviations • Editorial fixes.
17.08.2017	0.9.0	Contributions implemented in v0.9.0: • NFVIFA(17)000586r2: IFA028, clause 5.2.7: Clarification on SLPOC integration • NFVIFA(17)000667r1: IFA028 A.1.x Composite NS update operational flow • NFVIFA(17)000684r1: IFA028 6.3 Add impact analysis on MANO functional blocks • NFVIFA(17)000685: IFA028 clause A.1 step description improvement • NFVIFA(17)000700r1: IFA028 Consistency correction in clause 6 • NFVIFA(17)000707: IFA028, clause 5.2.7: Introduce note for figure 5.2.7-2
30.08.2017	0.10.0	Contributions implemented in v0.10.0: • NFVIFA(17)000698r1: Conclusions and recommendations for use case #2 • NFVIFA(17)000699r1: IFA028 Editor's note removal proposal for use case #2 • NFVIFA(17)000702r1: clause 8.1 enhancements • NFVIFA(17)000703r2: clause 8.2: Enhancements
18.09.2017	0.11.0	Contributions implemented in v0.11.0: • NFVIFA(17)000583r2: IFA028, Remove empty clause 7. Subsequent clauses are renumbered. • NFVIFA(17)000758r1: IFA028 6.3, 8.2, A.1.6 Add recommendation related to NS LCM grant • NFVIFA(17)000759r1: IFA028 6.3, 8.2 Add recommendation on NS PM and NS FM • NFVIFA(17)000792r1: IFA028 5.1 5.2.1 Add illustration on NFVIaaS consumer's administrative domain • NFVIFA(17)000793r1: IFA028 6.3 A Editor's note removal proposal • NFVIFA(17)000794: IFA028 Minor editorial improvement for use case #2 • NFVIFA(17)000795: IFA028 Add clarification on infrastructure domain • NFVIFA(17)000811r1: IFA028 6.3 Alignment on NSD management • NFVIFA(17)000674r4: IFA028 - clause on Multi-domain operation • NFVIFA(17)000675r4: IFA028 - clause on Information exchange between providers
10.11.2017	0.12.0	Contributions implemented in v0.12.0: • NFVIFA(17)000846r1: IFA028 review, clause 7.1 and 7.2: fix inconsistencies for Or-Vnfm • NFVIFA(17)000864r1: IFA028 Rapporteur edits part 1 • NFVIFA(17)000865r1: IFA028 Rapporteur edits part 2 • NFVIFA(17)000866r1: IFA028 final handling of editor's note • NFVIFA(17)0000902: IFA028 NS Composite flows corrections • NFVIFA(17)000905r1: IFA028 NFVO impacts and recommendations • NFVIFA(17)000910r1: IFA028 Editorial improvements • NFVIFA(17)000927: IFA028 - clause 5- Clarification on the NFVO-provider role • NFVIFA(17)000972: IFA028 6.3 Add clarification to auto-discovery of MANO functional blocks • NFVIFA(17)0001028r1: IFA028 7.2 Add recommendation for NFVO discovery
05.12.2017	0.13.0	Contributions implemented in v0.13.0: NFVIFA(17)000951r3: IFA028 Security Proforma clause
01.2018	0.13.0	Publication

History

Document history		
V3.1.1	January 2018	Publication