MEF

MEF White Paper

Standardized VNF License Management Framework White Paper

April 2020

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and MEF Forum (MEF) is not responsible for any errors. MEF does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by MEF concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by MEF as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. MEF is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any MEF member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any MEF members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

c) any form of relationship between any MEF member and the recipient or user of this document.

Implementation or use of specific MEF standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in MEF Forum. MEF is a non-profit international organization to enable the development and worldwide adoption of agile, assured and orchestrated network services. MEF does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

1 Abstract ... 1

2 Introduction ... 1

3 Industry Standardization Background ... 4

3.1 TM Forum ... 4
3.2 ETSI-IFA ... 6

4 Proposed Standardized Constructs and Terminology ... 6

4.1 Virtual Network Function ... 6
4.2 VNF Instance ... 7
4.3 VNF License ... 8
4.4 VNF License Policy ... 9
4.5 VNF License Key ... 10
4.6 VNF License Manager ... 11
4.7 VNF License Management System ... 13
4.8 VNF Ledger ... 14

5 VNF License Management Architecture ... 16

6 VNF Ecosystem ... 17

6.1 VNF Vendors ... 18
6.2 Service Providers ... 18
6.3 Third Parties ... 19

7 VNF Business and Trust Models ... 19

7.1 VNF Business Models ... 20
7.2 VNF Ecosystem Trust Model ... 20

8 Summary ... 21

9 About MEF ... 22

10 Terminology ... 22

11 References ... 23

12 Acknowledgements ... 24

List of Figures

Figure 1: Large scale of VNF instances and license keys in Service Providers 3
Figure 2: SDO approaches to VNF License Management.. 4
Figure 3: Proposed TM Forum VNF License Management Architecture 5
Figure 4: Ongoing work in ETSI-IFA 6
Figure 5: VNFs and VNF instances 7
Figure 6: VNF and VNF license 8
Figure 7: VNF instances and VNF policies 9
Figure 8: VNF license keys... 11
Figure 9: VNF Vendor and its VNF license manager.. 12
Figure 10: VNF license management system 14
Figure 11: VNF ledger and VNF license management system.. 15
Figure 12: VNF Licensing Reference Architecture for single Service Provider domain 16
Figure 13: VNF Licensing Reference Architecture for multiple Service Provider domains........ 17

1 Abstract

This White Paper is aimed at Communications Service Providers (CSPs) and their VNF vendors who are currently challenged with introducing large numbers of VNFs into the Service Provider's environment due to high overhead involved in agreeing and managing VNF licenses. Today's non-standardized VNF licensing environment is holding back the rapid introduction of innovative new VNF products into the telecom environment and is a barrier to entry for many smaller VNF vendors. This problem will become increasingly acute with the growing deployment of SD-WAN managed services, 5G and Edge Compute by CSPs.

This paper explains the current state of lack of adoption of even initial attempts at standards for VNF licensing. Proposals are made by the authors to address the lack of scalability of VNF licensing and deployment through standardized terminology, constructs and a scalable VNF Licensing Management architecture aligned with that of MEF's LSO (Lifecycle Service Orchestration) framework.

2 Introduction

Communications Service Providers (CSPs) or 'Service Providers' are increasingly using Virtual Network Functions (VNFs) to enhance their product offerings – for example SD-WAN managed services – as well as to enable deployments of 5G and Edge Compute.

VNFs are pure software entities that can be deployed in a compute environment anywhere in the network and can be cloned and deployed extremely quickly. However, VNF vendors have to realize return on their development investments in the technology and therefore need to have intellectual property rights associated with them. Just as with any other networking product, VNFs therefore have rules and conditions for their use set by the VNF vendor. The intellectual property rights (IPR) associated with the VNF may also include IPR for components from third parties that have been used in the development of the VNF. For these reasons, among others, Service Providers using VNFs have to negotiate the use of VNF products with their vendors and mechanisms for monitoring adherence to rules and conditions of use have to be agreed and implemented.

Aspects of such rules and conditions for use of VNFs include:

- Conditions of VNF use: What are the conditions in which a VNF can be used or not used by the Service Provider?
- Duration of VNF use: What is the timeframe for usage by the Service Provider (single use, annual, in perpetuity, other)?
- Changes to VNF: What modification permissions (if any) does the software owners grant to the Service Provider user of the VNFs?
- Business model for VNF use: How will the license users pay the software owners as they use a VNF license over the course of business?

The term 'license' is typically used as shorthand for these rules and conditions of use of a VNF, and we would say that a Service Provider has a license to use the VNF as long as it adheres to the rules and conditions set by the VNF vendor. Some Service Providers have not yet fully understood the challenges associated with VNF licensing from multiple VNF vendors. VNF license negotiation between Service Providers and VNF vendors is very often a cumbersome and expensive legal and commercial exercise that can last several months and it can drastically slow down the introduction of new VNF products into Service Provider environments acting as a major barrier to innovation by large and small VNF vendors alike. Even when the challenge is understood in the commercial and business parts of the Service Provider, there is often a significant barrier for those groups in the Service Provider to articulate and achieve implementations of their requirements from the counterparts in the operational departments of the Service Provider.

Enforcement of the terms of the VNF license is very central to the use of VNFs. The nature of software makes it very easy to copy and reuse - and therefore also easy to abuse the terms of the software licence. To help counter this possibility, VNF Vendors often use a mechanism in which the VNF software itself enforces the terms of the license and also measures the VNF’s usage. Enforcement is the responsibility of the VNF Vendor and for that reason, enforcement is implemented by the VNF Vendor. This can be done in a proprietary manner and there is no intention to standardize the mechanism for enforcement.

However, enforcement as it is typically implemented today requires the ability either to send reports to the VNF Vendor directly over the Internet or to implement very expensive audits. This is where there is a need to standardize the tracking and reporting around the usage of the VNF. This ties directly into having a more effective trust model between the Service Provider and the VNF Vendor and is also central to the need for standardization (see Section 7).

Also, due to lack of operational standardization of the management of licenses, Service Providers often have great difficulty introducing VNF-oriented mechanisms into their existing BSS/OSS environments, acting as an additional barrier to the use of VNFs in Service Provider products. Examples of causes of lack of progress in this area appear to include the required costly changes to the Service Provider’s legacy OSS/BSS in order to accommodate proposed VNF license management approaches, concerns about sharing information on the usage of the VNF by the Service Provider with the VNF vendor (usage monitoring), as well as architectural requirements on the part of both Service Providers and VNF vendors.

This contrasts starkly with the apparent ease of using VNFs in the hyperscale cloud provider environment. There is indeed much that can be learned from the cloud service providers’ implementation of “charging and billing” and could be used for the possible standardization of **VNFaaS** (VNF as a service). However operationally there is a fundamental difference between the CSP context and that of the cloud provider. In the CSP case of, the vendor provides the VNF (**VNF instance)** but the run time is managed by the CSP.

The problem is only growing in complexity. A Service Provider will typically have many potential sources for VNF products, and each VNF vendor has its own approach to licensing and monitoring. Furthermore, Service Providers may be using wholesale network services from partners to complete the footprint of a given service for a customer and may need to trigger the use of VNFs not only in its own network, but also in the network of the wholesale partner (e.g. service chaining on an offnet uCPE).

The scale of the challenge of managing VNF licenses for the Service Provider is illustrated in Figure 1. A Service Provider can expect to work with tens of VNF vendor partners. Each VNF vendor comes with at least one VNF license manager for its VNF products. Each VNF license manager will be handling at least tens of VNF policies and thousands of VNF instances. Multiply this out, and each Service Provider could well face the task of managing millions of associations between VNF instances and VNF policies.

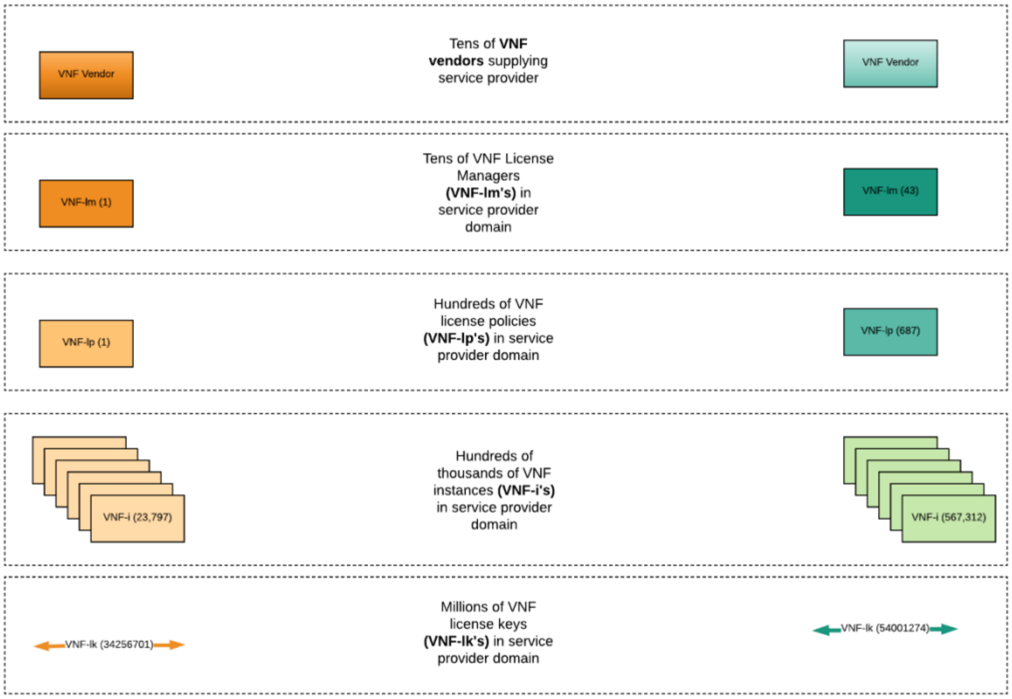
VNF Vendor
Tens of VNF vendors supplying service provider
VNF Vendor
VNF-lm (1)
Tens of VNF License Managers (VNF-lm's) in service provider domain
VNF-lm (43)
VNF-lp (1)
Hundreds of VNF license policies (VNF-lp's) in service provider domain
VNF-lp (687)
VNF-i (23,797)
Hundreds of thousands of VNF instances (VNF-i's) in service provider domain
VNF-i (567,312)
VNF-lk (34256701)
Millions of VNF license keys (VNF-lk's) in service provider domain
VNF-lk (54001274)

Figure 1: Large scale of VNF instances and license keys in Service Providers

Even standardizing terminology around VNF licensing appears to be a challenge, also confusing and fragmenting the market to the detriment of market growth and innovation.

Looking to the future, the ability to rapidly clone VNFs and deploy them means that automation of VNF lifecycle management is absolutely essential. Automation can only occur when terminology, constructs, architecture and interfaces for license management have also been standardized.

This White Paper proposes standardized terminology and an architecture aligned with the MEF Lifecycle Service Orchestration (LSO) architecture for standardized VNF license management.

The goal of standardized license management is to minimize commercial, business and operational friction experienced by both CSPs and VNF vendors.

3 Industry Standardization Background

Standardization work related to VNF licensing has already taken place in organizations such as TM Forum and ETSI. It is instructive to understand at a high level the results of that work in order to understand how using MEF standardization paradigms help the service providers and VNF vendors eliminate, or at least greatly reduce, the commercial and business friction they currently experience.

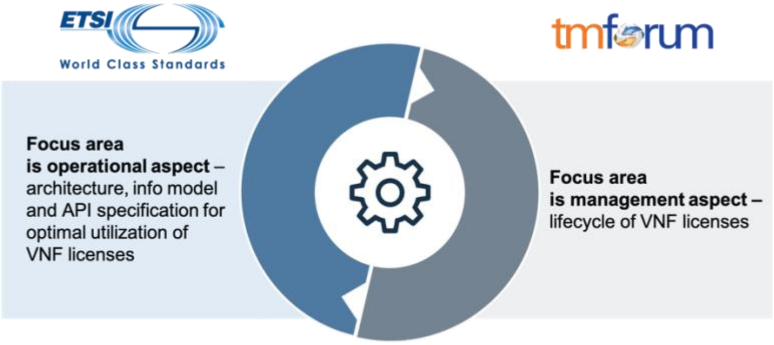
ETSI
World Class Standards
tmforum
Focus area
is operational aspect – architecture, info model and API specification for optimal utilization of VNF licenses
Focus area
is management aspect – lifecycle of VNF licenses

Figure 2: SDO approaches to VNF License Management

3.1 TM Forum

In March 2017, TM Forum released it Frameworx Exploratory Report on License Management [1] covering the challenges and requirements of VNF licensing, as well as the use cases and functional architecture and interfaces relating to VNF license management.

The resulting TM Forum work highlighted the need for standardized industry taxonomy in this area which should be used for communications between business and operations teams, and between vendors and suppliers.

3.1.1 Architecture Proposed in TMF IG1143

TM Forum proposed the following architecture to be used for reference, analysis and validation of current and future requirements.

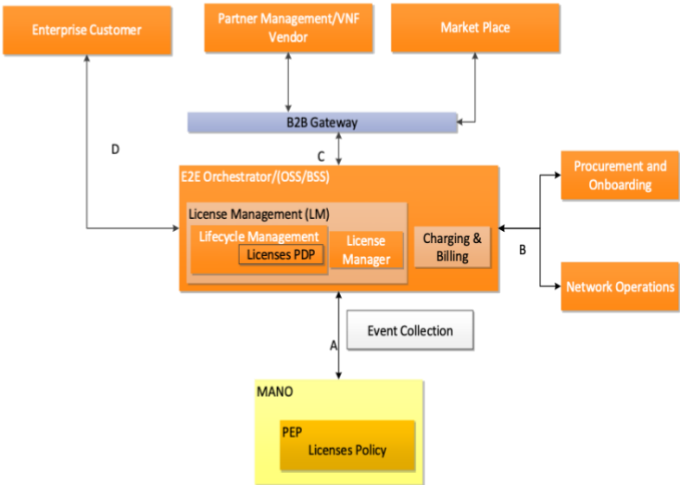

Figure 3: Proposed TM Forum VNF License Management Architecture

3.1.2 License Management

TM Forum also introduced the concept of 'license management' (cf. 'license manager' - see below) License Management would be the centralized entity in a service provider domain for management of all the VNF licenses in that domain irrespective of VNF type, VNF vendor etc. The License Management would comprise the respective License Managers supplied by either the VNF vendor, or a 3rd party managing the VNF on behalf of the VNF vendor. Externally, the License Management interacts with all instance of MANO, and internally provides vendor and technology agnostic APIs for interacting with the individual License Managers. Protection of VNF Licenses is not in the purview of License Management system.

3.1.3 License Manager

Finally, TM Forum introduced the concept of 'license manager' as an application provided by the VNF vendor or a 3rd party for protecting in an implementation specific way against use of VNF's outside the scope of the license.
The License Manager would be a gateway between Service Provider and VNF vendor/3rd party and would be separate from the MANO to ensure that the application wouldn't interfere with MANO operations.
All License Managers from the various vendors would be registered in the License Management system.

These TM Forum concepts have not yet been adopted in the industry.

3.2 ETSI-IFA

Since the TM Forum finished its work in this area, ETSI-IFA [2] has been exploring VNF licensing issues including

- License management architectural considerations and architecture
- Interface requirements for license management
- Information model requirements for VNF licenses
- Security requirements for VNF licenses

Discussions in ETSI-IFA are ongoing, but ETSI's focus is in the operation and management areas relating to VNFs, however VNF Licenses will be managed in the domain of BSS/OSS. In addition, license related information will be made by BSS/OSS (VNF License Management functional block) to NFV-MANO.

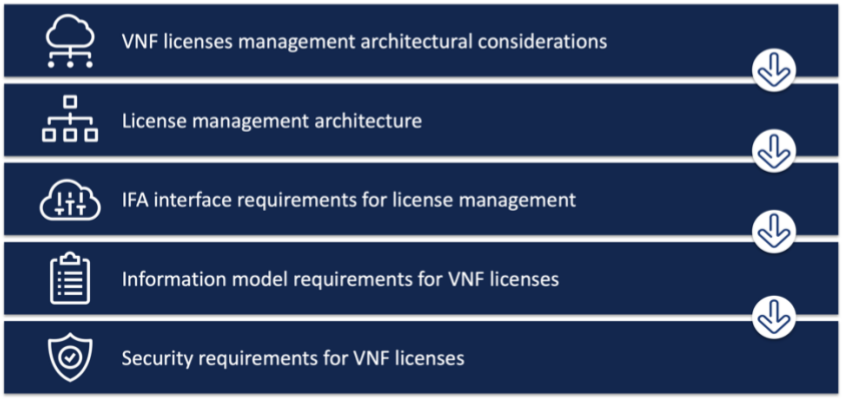
VNF licenses management architectural considerations
License management architecture
IFA interface requirements for license management
Information model requirements for VNF licenses
Security requirements for VNF licenses

Figure 4: Ongoing work in ETSI-IFA

4 Proposed Standardized Constructs and Terminology

The authors of this paper propose that the work of ETSI-NFV and TM Forum described above needs to be enhanced and completed in alignment with MEF's Lifecycle Service Orchestration (LSO) Reference Architecture [3] so that Service Providers will be able to handle VNF licensing in an automated and scalable way. In this section, we describe the various pieces in the VNF license operational environment, and where required propose new terms and definitions.

4.1 Virtual Network Function

The basis for all VNF licensing is the **Virtual Network Function** or '**VNF**' itself. The VNF is executable software which is a product with its own product lifecycle. It is developed and delivered to the market as a product by VNF vendors. The VNF can be used by a range of entities including Service Providers.

There are a huge number of examples of VNF products including:

- Edge Devices: SD-WAN Edge, vCPE, IP Edge
- Switching: BNG, CG-NAT, routers
- Tunnelling gateway elements: IPSec/SSL VPN gateways
- Traffic analysis: DPI, QoE measurement
- Signalling: SBCs, IMS
- Application-level optimisation: CDNs, load Balancers
- Home routers and set top boxes
- Mobile network nodes: HLR/HSS, MME, SGSN, GGSN/PDN-GW, RNC
- Network-wide functions: AAA server's policy control, charging platforms
- Security functions: Firewalls, intrusion detection systems, virus scanners, spam protection

4.2 VNF Instance

The **VNF Instance** or '**VNF-i**' is a live copy of the VNF running in a live environment. There can be any number of VNF-i's for a given VNF. Each VNF-i must have its own unique identifier which is generated by NFV MANO. The VNF-i itself is also instantiated and operated by the NFV MANO. However, the related license information is provided and managed by the VNF License Manager in turn supplied by the VNF Vendor. Note that when referring to VNF-i's, it is important to distinguish between the VNF product and the instance of a VNF product.

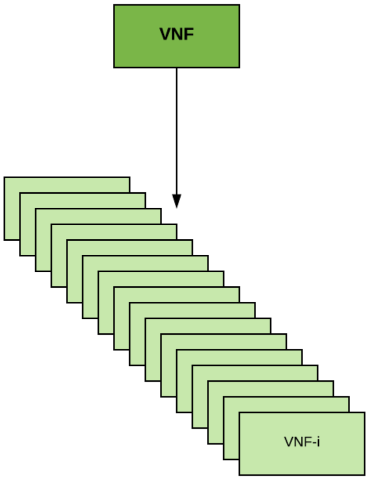

Figure 5: VNFs and VNF instances

Example

A VNF might be a pure software firewall product that can be used at the edges of an SD-WAN service on a uCPE. The actual instance of the firewall on a given uCPE at a specific customer site is the VNF-i. If the service using the VNF has say 100 edges, there may be 100 VNF-i's or instances of the VNF firewall product.

It is also important to note that the service provider may have agreed a price with the vendor for which the service provider can use up to a total 500 instances of the VNF product in different customer deployments at any given moment. The service provider may then activate and deactivate VNF-i's rapidly in order to ensure that it gets the maximum use of the 'pool' of 500 VNF-i's at any given time. The VNF vendor in this case has licensed the service provider to use its VNF product (the firewall), but on condition that it uses no more than 500 live copies, or VNF-i's. of the VNF product at any given moment. It is important for the VNF vendor, as well as the service provider, to know how many VNF-i's are being used at any given moment by the service provider. More on this later.

4.3 VNF License

A **VNF License** or '**VNF-li**' is a logical entity with a unique identifier which is associated with a VNF product. It expresses the agreement of the owner of the VNF product to have it used by one or more users. In simple language, the VNF user may say "I have the license to use this VNF from the VNF Vendor". The VNF License does not have to include commercial terms.

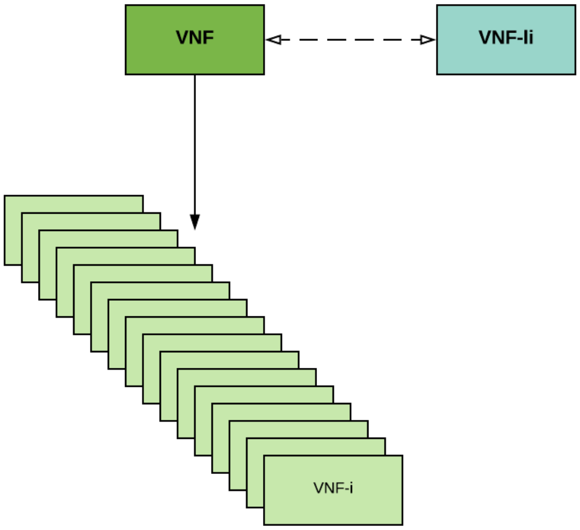

Figure 6: VNF and VNF license

4.4 VNF License Policy

A **VNF License Policy** or '**VNF-lp**' is the set of rules and conditions constraining the use of one or more VNF instances. For example, the vendor may want to limit the use of its VNF product to a specific country or set of countries, or it may want to limit the number of simultaneous instances of its VNF product. Similarly, it may want to limit the duration of use of the VNF and often, there is a limit applied to the number of concurrent users of a VNF.
All of these rules and conditions are captured in a VNF-lp.

Explicitly, an attribute of VNF-lp is a rule or condition. Examples of VNF-lp attributes include:

- Number of simultaneous users of VNF-i
- Location of use of VNF-i
- Modification permission for VNF-i
- Number of cores running VNF-i

As an example, a VNF-lp may limit the use of a VNF product to 100 instances. If the Service Provider wants to deploy another, say, 50 instances beyond the 100 limit, then the VNF License would enable the creation of VNF-lp that would apply to the usage of the additional 50 VNF-i's.

The VNF-lp resides in the VNF License Management System as a configuration file (e.g. .txt format). The implementation of the VNF-lp is enforced by the VNF vendor's VNF License Manager.

The VNF-lp is generated and supplied by the VNF vendor for review by the Service Provider before deployment in the VNF License Management System.

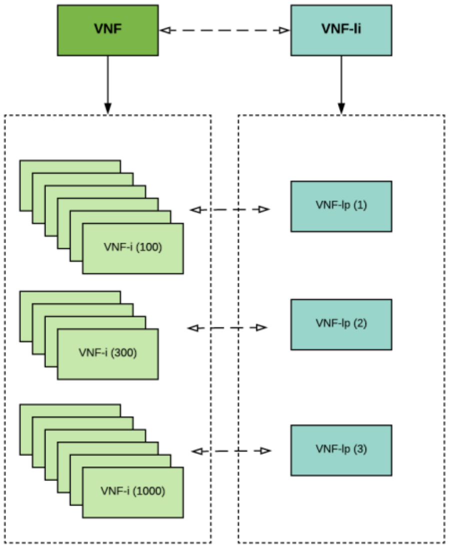

Figure 7: VNF instances and VNF policies

4.5 VNF License Key

The terms VNF License and VNF License Key tend to be used interchangeably in the industry, and quite often mean different things to different stakeholders. Agreeing on a definition of the VNF License Key will reduce confusion and promote progress in achieving scalability for VNF deployments. The VNF License should not be confused with the VNF License Key. The former is a contractual construct and the latter is an operational identifier.

The authors propose the following definition: A **VNF License Key** or '**VNF-lk**' is a unique identifier for each association at a given time of VNF-i and VNF-lp. There can be an unlimited number of VNF-i's associated with a given VNF-lp and conversely, there can be an unlimited number of VNF-lp's associated with a given VNF-i. In other words, there can be an unlimited number of VNF-lk's which uniquely identify each such association of VNF-i and VNF-lp.

The VNF-lk has two distinct roles:

1. Enabling the operational lifecycle of the VNF-i
2. Enabling the tracking of usage of the VNF-i

4.5.1 Tracking of Usage

The VNF-lk can be recorded in a VNF Ledger and is visible to all stakeholders that have appropriate access permissions. Stakeholders other than the VNF vendor (e.g. the service provider) need to be able to monitor the usage of VNF-i's and their associated VNF-lp's. The VNF-lk is the unique identifier for each association of VNF-i and VNF-lp. Therefore, it is important that the VNF-lk can be used in a look-up in the VNF Ledger to find a VNF-i and its associated VNF-lp.

4.5.2 Operational Lifecycle

The VNF-i can only become operational if the terms and conditions described in the VNF-i's associated VNF-lp are fulfilled. Therefore, the VNF-lm (vendor specific) that controls the VNF-i is the only element in the ecosystem that is allowed by the vendor to communicate with the VNF-i for the purposes of licensing the VNF-i. It does this using the VNF-lk in a proprietary closed communication between the VNF-lm and the VFN-i, for example, using a public key or dual key approach. In other words, the VNF-lk will be visible for a range of stakeholders for usage tracking purposes, but at the same time, cannot be used by stakeholders other than the VNF vendor to activate a VNF-i.

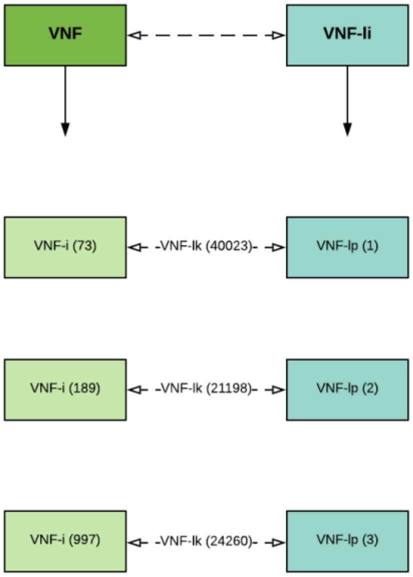

Figure 8: VNF license keys

4.6 VNF License Manager

The VNF License Manager or 'VNF-lm' is the specific vendor implementation solution for managing that vendor's VNF licenses associated with the VNFs provided by the VNF Vendor in a given Service Provider's domain.

Every VNF Vendor will want to have some interface with its VNF-i's to monitor the utilization of VNFs. In order to achieve this, there is a need for a solution which can be deployed in the Service Provider domain by the VNF Vendors without impacting the functioning and security of the VNF-i's. Also, every VNF Vendor needs to prevent exposure of its VNF-lm implementation so as to prevent misuse of its VNFs and exposure of its intellectual property. This is achieved by having vendor-specific VNF-lm.

While the VNF-lm implementation and its interface with the VNF-i are specific to a given vendor (i.e. proprietary), the VNF-lm and VNF software lifecycles should be manageable independently. In addition, the data exchange between the VNF Vendor and VNF-lm should be visible to the service provider to ensure that only relevant information related to a VNF-i is exchanged between the VNF Vendor and VNF-lm.

License management of a VNF-i does not have to be implemented using the vendor-specific VFN-lm. In those scenarios where there is established trust between the Service Provider and the VNF Vendor, the vendor-specific VNF-lm implementation can be bypassed. This is equivalent to not having any operational licensing enforcement but simply reporting to the VNF Vendor. This model usually implies audits.

Even though a VNF-lm solution is very straight forward, there are however many complexities that need to analyzed carefully, especially because the VNF-lm itself will be considered as overhead by Service Providers while running in the Service Provider domain.

Some of the complexities and scenarios that a VNF-lm implementation must consider are mentioned below:

1. Possibilities of having multiple VNF-lm's from a given VNF Vendor.
2. Management, deployment and execution of the VNF-lm must ensure that the VNF-lm and VNF-i lifecycles are decoupled from one another.
3. Vendor-specific (i.e. proprietary) solution for the interface between VNF-i and VNF-lm
4. Possibility of having a third party VNF-lm supporting VNFs from multiple vendors single license manager for multiple VNF Vendors.
5. Transparency of information exchanged between VNF-lm and VNF Vendor.
6. Interface of VNF-lm and VNF-le.

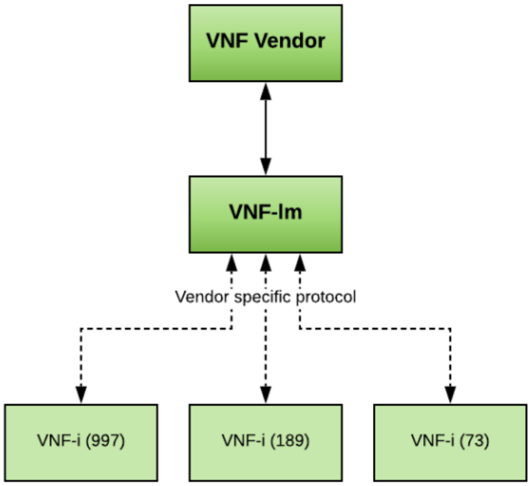

Figure 9: VNF Vendor and its VNF license manager

4.7 VNF License Management System

VNF License Management System or 'VNF-lms' is the framework for managing the inter-relationship of the various VNF-i's, VNF-lp's, and VNF-lk's in a given service provider domain, and assuring adherence to the VNF-lp's agreed to with the VNF Vendor.

It is important to note that the VNF Vendor will provide the VNFs to run in the service provider domain through MANO. The VNF Vendor needs to ensure that the VNF is not used outside the constraints of the agreed VNF-lp(s). This requires a control mechanism, which the VNF Vendor enables through the VNF-lm. The challenge of the service provider hosting multiple VNF-lm's typically are as follows:

1. Every VNF Vendor may provide multiple VNF-lm's which run in the service provider domain. Managing the runtimes of these VNF-lm's will be an overhead for the service provider.
2. There could be hundreds of VNF Vendors which will mean hundreds of VNF-lm's to be hosted and managed by the service provider.
3. The service provider needs a standard interface into the VNF-lm's to ease their management even though they operate as black boxes.
4. It is important to the service provider to have a view of what information is collected by the various VNF-lm's and how it is passed to the respective VNF Vendors.

It can be expected that additional challenges for service providers hosting and managing multiple VNF-lm's from multiple vendors in their domain will come to light.

These challenges are all addressed by having a single VNF-lms.

A VNF-lms framework provides vendor-neutral implementation for the following:

1. Centralized repository of the VNF license information for tracking and managing the VNF license usage throughout the service provider domain.
2. Vendor-agnostic interface for managing and utilizing the VNF licenses.
3. Onboarding of VNF licenses from the VNF Vendors.
4. Lifecycle management of multiple VNF-lm from various VNF Vendors.
5. Providing the interface between the VNF Vendor and the service provider domain.

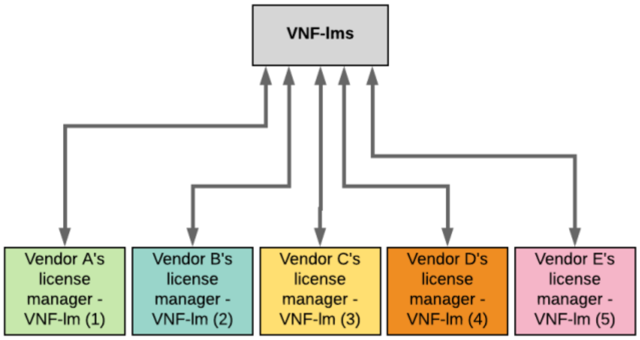
VNF-lms
Vendor A's license manager - VNF-lm (1)
Vendor B's license manager - VNF-lm (2)
Vendor C's license manager - VNF-lm (3)
Vendor D's license manager - VNF-lm (4)
Vendor E's license manager - VNF-lm (5)

Figure 10: VNF license management system

4.8 VNF Ledger

Today, VNF Vendors and CSPs both keep track of the license usage in their own respective siloed systems as it relates to billing which then have to be reconciled. There is an opportunity to transform those separate, sometimes manual ledgers, into an agreed and mutually trusted distributed ledger. We propose as a first step addressing the ledger issue with the following abstract construct.

VNF Ledger (VNF-le) is the abstract repository of VNF usage information mapped to VNF-i, VNF-lk and VNF-lp. Information contained in the VNF Ledger can be used by various stakeholders to track the VNF usage. The information in the VNF-le is updated through VNF-lms, which in turn collects information from various sources during the lifecycle of each VNF-i.

Though shown as a separate entity outside the VNF-lms in figure 11, it can also be implemented as part of the VNF-lms solution. The purpose of showing this functional block externally to the VNF-lms is to explain the interaction of this functional block with other functions in the ecoystem. The security and integrity of the data contained within the VNF-le, and its position in the service provider trust model, can be ensured by specific implementations of the VNF-lms or otherwise.

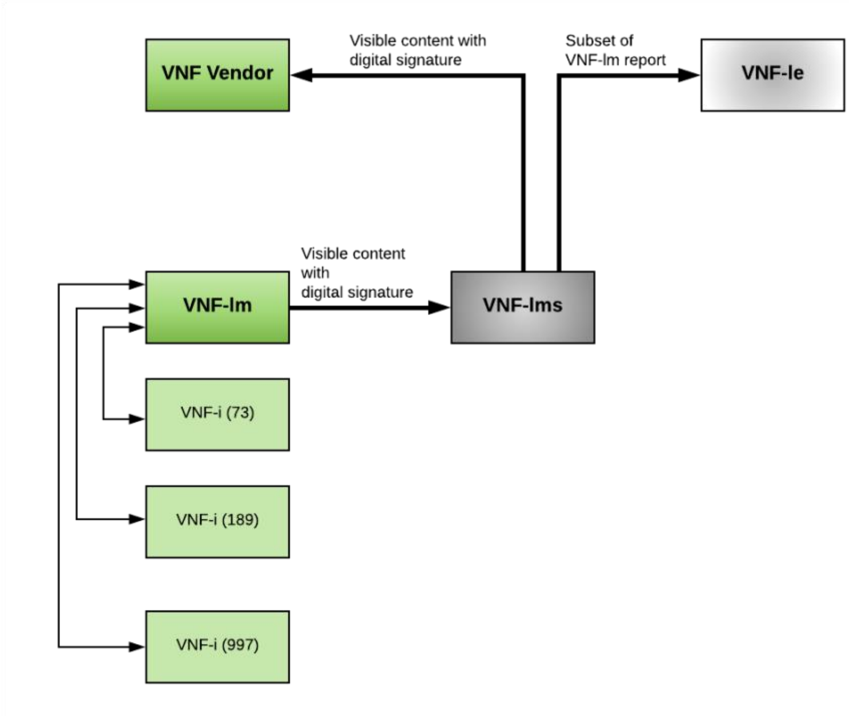

Figure 11: VNF ledger and VNF license management system

Note also that information collected by the VNF-lm needs to be communicated to the VNF Vendor outside the Service Provider domain. This needs to be done while both ensuring for the VNF Vendor that the information has not been tampered with on the one hand, and on the other ensuring for the Service Provider that is has visibility into that information. This can be achieved by applying a digital signature to information in the VNF-lm while passing that information in clear text format via the VNF-lms. A subset of the information will then be stored in the VNF Ledger by the VNF License Management System.

5 VNF License Management Architecture

Using the constructs outlined above, the authors propose an architecture for VNF License Management that:

a. Brings together these constructs together with suitable interfaces, some of which would need to be standardized
b. Aligns with the MEF's LSO Reference Architecture (MEF 55)

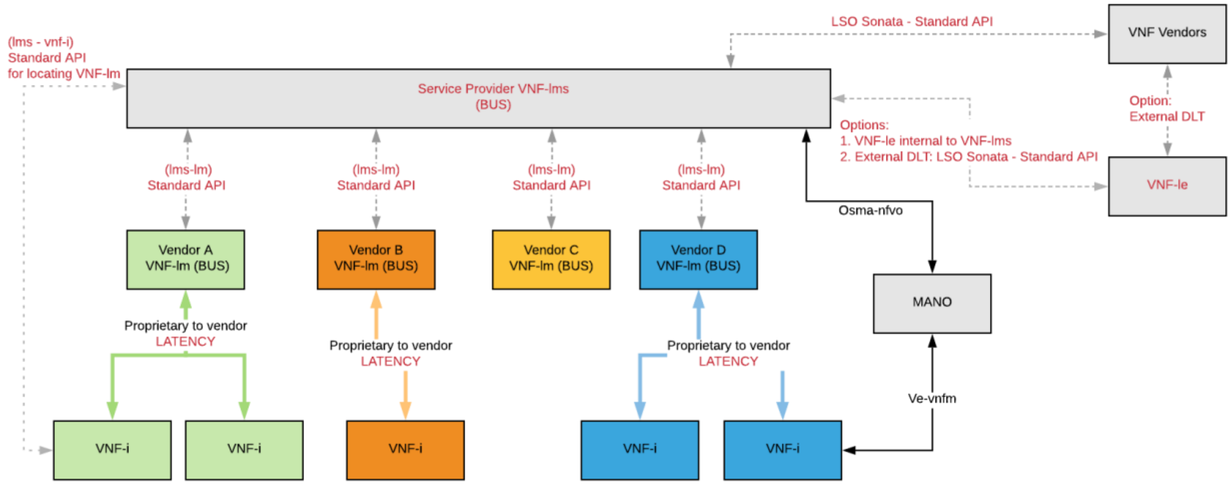

Figure 12: VNF Licensing Reference Architecture for single Service Provider domain

In figure 12, we see that the Service Provider will be hosting VNF License Managers from multiple VNF Vendors with each VNF-lm handling potentially very large numbers of instances of the vendor's VNFs. The communications between the VNF-i's and the VNF-lm (e.g. including information on how many concurrent users the VNF-i is supporting) are proprietary to the VNF Vendor. The NFV-MANO will also be communicating with the VNF-i's via the standardized NFV Ve-vnfm interface. Typically, the VNF Vendor will prefer to have the instance of its VNF-lm in the network close to the VNF-i's to reduce latency but the Service Provider will prefer not to have such a software entity embedded in its network resources due to both performance and security considerations. For that reason, we propose putting the VNF-lm in the Business Applications part of the LSO Reference Architecture together with the VNF License Management System.

This paper also proposes that the interface between a VNF Vendor's proprietary VNF-lm and the VNF License Management System be standardized for more rapid onboarding of new VNFs.

Similarly, a standardized interface will be required between each VNF-i and the VNF-lms for the simple task of locating its specific VNF-lm at the beginning of the VNF-i's lifecycle.

A standardized interface will also be required between the Service Provider's VNF License Management System and the VNF Vendor's systems external to the Service Provider domain.

Note that the interfaces between the NFV-MANO and the VNF-i's as well as between NFV-MANO and the VNF License Management System (e.g. information on memory used, cores used, network usage and runtime) are already standardized by ETSI as Ve-vnfm and Osma-nfvo respectively.

The VNF Ledger is shown in the proposed architecture as a separate logical entity which may or may not be included within the implementation of the VNF-lms. This is an operational consideration for the Service Provider. There may be use cases where use of Distributed Ledger Technology (DLT) as the basis for the VNF Ledger are justified, including the case of a data service that spans multiple operator domains as shown in figure 13.

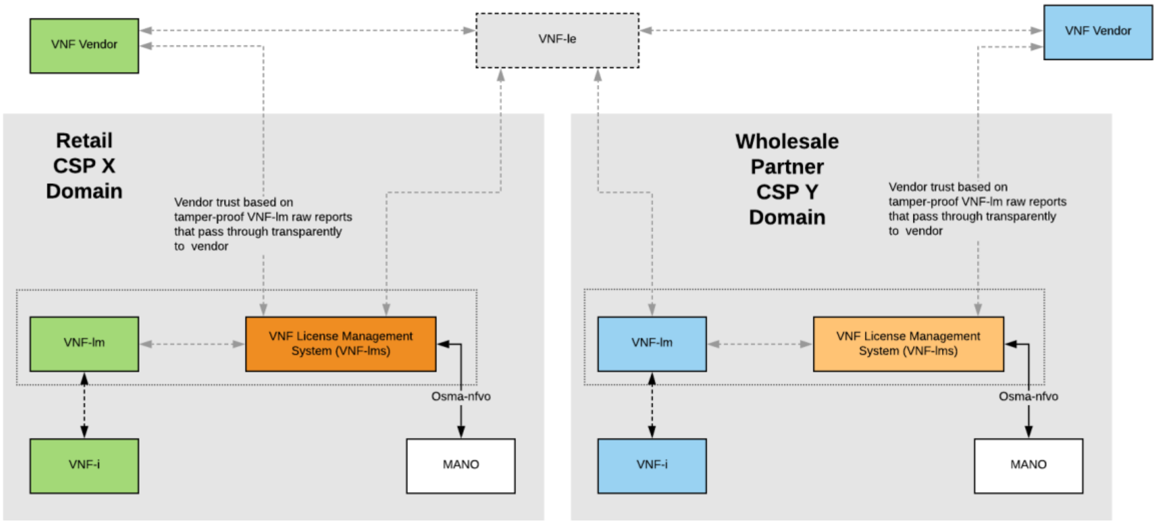
VNF Vendor
VNF-le
VNF Vendor
Retail CSP X Domain
Vendor trust based on tamper-proof VNF-lm raw reports that pass through transparently to vendor
VNF-lm
VNF License Management System (VNF-lms)
Osma-nfvo
VNF-i
MANO
Wholesale Partner CSP Y Domain
Vendor trust based on tamper-proof VNF-lm raw reports that pass through transparently to vendor
VNF-lm
VNF License Management System (VNF-lms)
Osma-nfvo
VNF-i
MANO

Figure 13: VNF Licensing Reference Architecture for multiple Service Provider domains

6 VNF Ecosystem

Having defined the standardized constructs in the area of VNF license management, it is important to understand who the key parties in the VNF ecosystem are. For this purpose, we define the term **VNF Ecosystem** as the collective name, in the context of VNF licensing, for the participants in VNF commerce and the usage of VNFs in a Service Provider domain. The following are the authors' definitions of the parties to the VNF Ecosystem for the purpose of VNF licensing.

6.1 VNF Vendors

VNF Vendors are the companies developing and selling VNFs. VNF Vendors monetize the use of their VNF products by their Service Provider partners typically in one of the following ways:

- License fee for the use of deployed VNF-i's
- Flat rate/subscription charge irrespective of the number of deployed VNF-i's
- Charge per VNF-i -specific transaction

The requirements of VNF Vendors include:

- Minimizing
  - Commercial negotiation and legal costs and time for each VNF sale
  - Pre-sales support for the integration of each VNF
  - Billing overheads for each VNF
  - Reliance on information sourced from the Service Provider partner regarding usage of the VNF
- Preventing unwanted use of VNFs by those not authorized to use them or use of the VNFs outside the terms and conditions agreed with those that are authorized to use them. To achieve this, VNF Vendors require the ability to track usage of its VNFs both offline and online.
- Placement of the vendor’s VNF License Manager (VNF-lm) in close proximity to the VNF-i’s in the infrastructure typically to minimize latency in the interactions between the VNF-lm and VNF-i. This may be a carry-over from the era of element managers needing to be close to the physical network devices for reliable control of those devices, however this often is not necessary in today’s implementations of network infrastructure.

6.2 Service Providers

Service Providers are the CSPs that use VNFs to enhance their products and services.

The requirements of the Service Providers include:

- Maximizing
  - Choice of VNFs available to them for deployment to support a functionality in a service, whether from one vendor or a range of vendors
  - Effectiveness of the VNFs in building in services in real-time (e.g. through monitoring)
- Minimizing
  - Onboarding costs and time for each VNF
  - Integration and deployment costs and time for each VNF
  - Legal, payment and dispute settlement costs and time for each VNF Vendor
  - Placement of non-VNF-i software in the network infrastructure to avoid performance impact and security vulnerabilities.
  - Service disruption due to licensing issues.

- Ensuring that tracking/monitoring of VNF usage by VNF Vendors does not introduce security vulnerabilities into the Service Provider's domain
- Enabling tracking of
  - VNF usage for optimum return on investment
  - VNF-i usage in a sufficiently granular manner to use analytics to predict future financial and resource usage, allowing the service provider to adjust its operational models to minimize future expenditure on licenses and infrastructure.

6.3 Third Parties

There is a wide range of solution providers that can deliver one or more aspects of software solutions that simplify license management for the Service Providers and/or VNF Vendors. The concepts laid out in this White Paper create new opportunities for existing and new players in the ecosystem. Examples include:

1. **3rd Party VNF License Management System Vendors**
   Suppliers of the VNF License Management System which is a specialized software solution and a key enabler for managing large numbers of VNF licenses and license policies for multiple vendors in the Service Provider domain.

2. **3rd Party VNF License Manager Vendors**
   Suppliers of the VNF License Manager which is a tool that VNF Vendors deploy in the Service Provider domain to track and manage their VNF products in their customer Service Provider's domain. Note that this creates an opportunity for commercial off-the shelf product vendors to supply the specialized software of the VNF License Manager.

3. **VNF Ledger Vendors**
   Suppliers of the VNF Ledger which will play an essential role in tracking and managing usage of VNFs in the Service Provider domain. The implementation of the VNF Ledger can be either a part of the VNF License Management System or distinct and separate (e.g. Distributed Ledger Technology implementation that is not controlled by any single participant in the ecosystem).

7 VNF Business and Trust Models

VNF license management is intrinsically connected to both enabling business between Service Providers and their VNF Partners, as well as enabling trust between them. For that reason, it is helpful to highlight the related business and trust models in the VNF space.

7.1 VNF Business Models

Once a standardized approach to VNF License Management is achieved, it is easier to quickly implement, modify and enforce business models for using VNFs. Note that while VNF business models describe the overall approach to the business between the Service Provider and the VNF Vendor, the VNF License Policies determine specific constraints and govern the actual usage of the VNFs in the context of the business model.

Examples of such business models include:

7.1.1 Flat

In the Flat model, the Service Provider pays the VNF Vendor a fixed price for a set of features of the VNFs.

7.1.2 Pay-as-you-Grow

In this model, the price varies based on the usage of the VNFs. Usage can be determined based on various parameters of the VNFs like number of instances of VNFs or the number of concurrent connections etc. VNF features can grow progressively based on requirements.

7.1.3 Subscription

The subscription model provides the Service Provider with the right to use the VNF for a fixed period of time. Renewal by the Service Provider is required to continue the use after the period.

7.1.4 Hybrid

In the hybrid model, a combination of two or more of the above models is agreed between the Service Provider and the VNF Vendor.

7.2 VNF Ecosystem Trust Model

The **VNF Ecosystem Trust Model** is the collection of rules, processes and applications which ensures that the information related to the usage of the VNFs can be trusted by the Service Providers, VNF Vendors and other relevant stakeholders. The Trust Model describes the level of transparency and integrity of all the data and applications for all the stakeholders.

Understanding in detail the Trust Model is important in the VNF ecosystem because the VNFs and VNF License Managers are supplied by the VNF Vendors but are operated in the Service Provider domain using Service Provider resources.

An unsuitable Trust Model makes it difficult to support a wide range of implementation and business scenarios. This is the typical situation currently and as a result the Trust Model today is usually underpinned by extensive legal agreements and minimal monitoring.

An effective Trust Model will ensure that all the stakeholders are coordinated in an automated, highly scalable manner regarding all aspects of the usage of VNFs in the Service Provider domain.

The Service Provider needs to trust the following artefacts and information from the VNF Vendor:

- VNF will operate as specified by the VNF Vendor
- VNF will not introduce any security threat or vulnerabilities - maliciously or accidentally - into the Service Provider domain
- Vendor's VNF License Manager will operate in an 'honest' and complete fashion in the Service Provider domain without creating significant operating overhead for the Service Provider

Conversely, the VNF Vendor needs to trust the following information from the Service Provider:

- Usage data regarding its VNF product operations (e.g. how many VNF-i's in the system; number of cores being used, number of concurrent users, geographic location etc.)

In order to maximize transparency, the Trust Model should ensure that the information exchanged between parties is visible to them and any modification to the information is also auditable and is part of the information exchanged itself.

8 Summary

There is a disconnect today in the CSP industry between business requirements and VNF technology solutions. The business people in the Service Providers are challenged in explaining to their engineering teams their requirements in terms of managing VNF licensing - a very important aspect of working with virtualized resource suppliers. Similarly, the Service Provider architects and engineering teams are challenged in designing their OSS/BSS environments with an understanding of these business requirements and how to handle them. This leads to a VNF licensing architecture with a Trust Model that requires extensive legal and commercial negotiation for each VNF and very limited business model options.

This White Paper firstly proposes that Service Providers and VNF Vendors adopt the standardized terminology and architectural framework described in this document to enable more effective trust and business models for use of VNFs. This will have the benefit of making VNF usage much more scalable, opening up the market to new and innovative VNF products from a wide variety of VNF Vendors. The authors also propose underpinning this proposed terminology and architectural framework with standardization work.

Secondly, the authors propose adopting and extending the Intent-based business language currently being developed in MEF in the context of SD-WAN service and policies specification to the area of VNF license policies. By enabling business and legal stakeholders in both Service Providers and VNF Vendors to directly create machine-readable master agreements and terms and conditions, a dramatic acceleration of the negotiation phase relating to use of VNFs can be achieved.

Finally, the authors propose that a large-scale Proof of Concept is developed to demonstrate how effective trust models and business models based on the framework proposed in this whitepaper can enable scaling for large numbers of VNFs both in a single Service Provider domain use case and in a multiple Service Providers domain(s) use case.

9 About MEF

An industry association of 200+ member companies, MEF has introduced the MEF 3.0 transformational global services framework for defining, delivering, and certifying assured services orchestrated across a global ecosystem of automated networks. MEF 3.0 services are designed to provide an on-demand, cloud-centric experience with user- and application-directed control over network resources and service capabilities. MEF 3.0 services are delivered over automated, virtualized, and interconnected networks powered by LSO, SDN, and NFV. MEF produces service specifications, LSO frameworks, open LSO APIs, software-driven reference implementations, and certification programs. MEF 3.0 work will enable automated delivery of standardized Carrier Ethernet, Optical Transport, IP, SD-WAN, Security-as-a-Service, and other Layer 4-7 services across multiple provider networks. For more information, visit https://www.mef.net and follow us on LinkedIn and Twitter @MEF_Forum.

10 Terminology

Term	Definition	Reference
Communications Service Provider	Company offering, among other services, data-oriented services to consumers and/or enterprises based on data network infrastructure. Referred to in this document as ‘Service Provider’ for easier reading.	
CSP	Communications Service Provider	
NFV	Network Function Virtualization	
License	Agreement on use of a product or service between a buyer and a seller.	
Lifecycle Service Orchestration	Standardized framework for intra-provider and inter provider orchestration of data-oriented services	MEF 55 [3]
LSO	Lifecycle Service Orchestration	
MANO	Management and Network Orchestration	www.etsi.org
Network Function Virtualization	Set of ETSI standards covering enabling the use of software running on generic compute platforms for any aspect of network functionality.	www.etsi.org
Service Provider	Used in this document instead of CSP or Communications Service Provider for easier reading.	

Trust Model	Collection of entities and processes that service providers rely on to help preserve security, safety and privacy of data.	
VNF	Virtualized Network Function	
VNF Instance	Software clone of VNF deployed on a network.	Abstract construct proposed in this White Paper
VNF Ledger	Database (DLT-based or centralized) of information pertaining to licensing, management and usage of VNF Instances.	Abstract construct proposed in this White Paper
VNF License Key	Unique operational identifier for unique association between a VNF Instance and a VNF License Policy.	Abstract construct proposed in this White Paper
VNF License Manager	Functionality that manages, monitors and polices the licensing and related usage aspects of a VNF Instance. Typically developed by the vendor that develops the VNF.	Abstract construct proposed in this White Paper
VNF License Policy	Set of rules and conditions in electronic format readable by software for use of a VNF Instance.	Abstract construct proposed in this White Paper
VNF lifecycle	Steps in the life of a VNF Instance including deployment, management and termination.	
VNF-i	VNF Instance	
VNF-le	VNF Ledger	
VNF-lk	VNF License Key	
VNF-lm	VNF License Manager	
VNF-lms	VNF License Management System	
VNF-lp	VNF License Policy	

11 References

[1] TMF IG1143 (Note: TMF members can access using their TMF credentials)

https://www.tmforum.org/resources/exploratory-report/ig1143-license-management-r16-5-1/

[2] ETSI GR NFV-EVE 010 V3.1.1 (2017-12): "Network Functions Virtualisation (NFV) Release 3; Licensing Management; Report on License Management for NFV".

https://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/010/03.01.01_60/gr_NFV-EVE010v030101p.pdf

[3] MEF LSO Reference Architecture (MEF 55)

https://wiki.mef.net/display/CESG/MEF+55+-+LSO+Reference+Architecture

12 Acknowledgements

- Abinash Vishwakarma (NetCracker) – Co-Author
- Daniel Bar-Lev (MEF) – Co-Author
- Nicolas Thomas (Fortinet)
- Peter Willis (BT)