Technical Paper

5G slice orchestration and lifecycle automation

Envisioning zero-touch 5G slice operations
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who is afraid of the big 5G slice orchestration?</td>
<td>3</td>
</tr>
<tr>
<td>It is not that bad</td>
<td>3</td>
</tr>
<tr>
<td>An architecture made of bricks</td>
<td>4</td>
</tr>
<tr>
<td>Tell me the story</td>
<td>4</td>
</tr>
<tr>
<td>A knock on the door</td>
<td>4</td>
</tr>
<tr>
<td>A minute of orchestration</td>
<td>4</td>
</tr>
<tr>
<td>How do you build it?</td>
<td>5</td>
</tr>
<tr>
<td>I’ll huff, and I’ll puff</td>
<td>6</td>
</tr>
<tr>
<td>Is my house made of bricks?</td>
<td>6</td>
</tr>
<tr>
<td>NFVO role in network slicing per 3GPP</td>
<td>7</td>
</tr>
<tr>
<td>What does it mean for lifecycle management?</td>
<td>8</td>
</tr>
<tr>
<td>Secure the chimney</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>10</td>
</tr>
<tr>
<td>Further reading</td>
<td>10</td>
</tr>
<tr>
<td>Acronyms</td>
<td>11</td>
</tr>
</tbody>
</table>
Who is afraid of the big 5G slice orchestration?

It is not that bad

As the 5G era comes into being, it is bringing about a set of profound changes to network operations as we know them. It is also promising a wealth of new and exciting business opportunities. Indeed, as network slicing becomes a key component of networks, it poses a key question: How can the extra complexity of 5G network slice management be managed?

For the digital service provider, network slicing has become a fundamental enabler for generating new value. It offers a platform for agile network service creation in response to the specific requirements of a variety of customer segments.

A network slice is an end-to-end “virtual private service,” which extends from an end device to an application and includes all intermediate functions and domains. Initially defined in the context of 5G, the concept has evolved to include fixed access, transport, and application domains.

A network slice comprises virtual and physical network functions, cloud resources, connectivity, and augmented services, as well as application functions. All of these are orchestrated to form a service-specific virtual network in order to meet service requirements, such as latency, reliability, coverage and security in addition to capacity and cost targets (See Figure 1).

Figure 1. Slicing across radio, transport, core and central clouds

As the request for network slices grows from a few occurrences to the basis of new business models in 5G, lifecycle management of network slices will need to be fully automated. Automation does not just apply to instantiation and initial configuration; rather, it includes all aspects of Fault, Configuration, Accounting, Performance, Security (FCAPS) management functions that will need to work without human intervention. This will enable the creation and optimization of new slices for specific market segments with minimal effort. As a result, communications service providers (CSPs) will be able to offer hundreds of new services just as cloud providers are able to offer hundreds of on-demand managed cloud services, using entirely automated business and lifecycle management approaches.
An architecture made of bricks

The good news is that network slicing capabilities are embedded in the solutions and end-to-end portfolio offered by Nokia, which are designed for digital transformation. In other words, the same architecture and products offered by Nokia, which are based on AI-driven operations, closed-loop lifecycle management, as well as domain orchestration and new business models can natively accommodate the slicing use cases. That means they are capable of managing different types of services, including those classified as network slicing services.

For the service provider that is a great benefit because there is no requirement for a dedicated software stack/layer/solution specifically designed to deal with network slicing. This would only add more complexity and cost to the service provider’s network—both economically and architecturally.

Implementing the Nokia software components ensures that the network slices can be delivered and managed like any other service in the network. This can be done simply with the unique attributes defining the service. A slice can be orchestrated, provisioned, assured and analyzed by the same set of components comprising the entire network because the specific attributes of the slices are supported by all the elements in the fulfillment and assurance chains.

Tell me the story

To demonstrate how the existing Service Orchestrator (SO) and NFV Orchestrator (NFVO) can be used in the context of 5G network slicing, this paper explains the interactions between, as well as the roles of the NFVO (responsible for network orchestration), and the SO (end-to-end Service Orchestration) layers in the context of 5G network slicing. It also shows that current security practices can be extended to the context of 5G network slicing and how, from the viewpoint of Nokia, this can lead to the operational transformation of digital networks.

A knock on the door

A minute of orchestration

In the context of communications networks, including software-defined networks (SDN) and network functions virtualization (NFV), orchestration refers to the automation of order fulfillment, service assurance, as well as other business processes in a software-controlled environment. Orchestration—preferably closed-loop orchestration of previously manual processes—is key to unlocking the level of automation expected for slicing management.

In our domain of networking, an orchestrator or, better, a set of orchestrators issues the tasks for a set of agents. These include management systems, controllers, and network functions. The domain of networking can be divided into sub-domains, such as LAN connectivity, WAN connectivity, network services, virtualized network functions (VNFs), and virtualized infrastructure. Each has its own well-defined types of resources and operations best practices. Orchestration in the networking domain can be simplified by using a hierarchy of domain-specific orchestrators, managers, and controllers. Each orchestrator decomposes and automates services, resources, and tasks in their respective domains cooperatively. The orchestrators, managers, and controllers cooperate and rely on each other.
While this document focuses on slicing fulfillment, slicing assurance also needs to be orchestrated and is converged with fulfillment as an integral part of the hierarchical orchestration architecture. Due to the dynamic software-controlled resource allocation during fulfillment, meaningful service assurance is only possible if it has access to the service descriptions at different levels and to the mappings between the services and resources created by fulfillment.

The Nokia orchestration solution simplifies slicing operations through automation. The solution lowers the complexities related to managing network slices from deployments to service assurance in multi-site, multi-vendor, and multi-technology environments. It provides NFVO functionality as specified by ETSI NFV and end-to-end service orchestration functionality.

**How do you build it?**

Below are possible steps, which describe the instantiation of a network slice and the components involved:

1. Decompose customer service to a set of network services
2. Increase RAN capacity using closed loop optimization
3. Configure the new slice in cloud RAN
4. Create a new customer and subscriber profile in the subscriber database
5. Select VIM (Virtualized Infrastructure Manager) for core network deployment
6. Create connectivity between VIMs.

**And for each core network service:**

7. Set up the networking endpoints for each VNF
8. Deploy configuration templates for the solution
9. Create VNFs as part of network slice solution
10. Auto-integrate VNFs into the next generation network management system (NG NMS)
11. Auto-configure slice
12. Deploy correlation rules
13. Deploy pre-defined reports and Key Performance Indicators
14. Deploy operation automation rules and action components
15. Deploy Key Quality Indicator definitions
16. Instantiate the customer management portal.

To become automated in an end-to-end orchestration, these tasks can be mapped onto the network architecture as shown in Figure 3, which also illustrates the components of the Nokia solution.
I’ll huff, and I’ll puff

Is my house made of bricks?

Few requirements are needed to ensure that the next-generation architecture and solutions, especially the NFVO and SO layers, are capable of supporting slicing services. These requirements include:

- Adjustable and strong APIs:
  - To enable vertical customer businesses to automate their service management within the limits of an SLA so that the vertical service provider can provision, modify, and monitor the network capacity used for different services over the APIs
  - To secure multi-tenancy in all operations over the APIs so that the network service provider can manage the APIs in order to meet the SLAs.

- Lifecycle management of network slices to plan, instantiate, and delete network slices for vertical customer businesses.

The requirement for adjustable and strong APIs is common to the variety of services enabled on the network. However, this requirement is not the focus of this paper. Instead, the paper focuses on the requirement for lifecycle management of network slices.
NFVO role in network slicing per 3GPP

If it is assumed that an NFV orchestrator is already in the network and that the network configuration has been prepared already for 5G, the NFVO can be used to implement the network slicing tasks required by the 3GPP. To begin with, the concept of the 3GPP network slice can be compared to the NFV network service. Figure 3 compares the 3GPP and ESTI NFV information models.

Figure 3. 3GPP and ETSI NFV information models

The 3GPP information model can be mapped to the ETSI NFV information model:

<table>
<thead>
<tr>
<th>3GPP concept</th>
<th>NFV concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>The network slice includes all functionalities and resources necessary to support a certain set of communication services. The slice contains one or more network slice subnets, each of which in turn contains one or more network functions and which can also contain other network slice subnets.</td>
<td>An NFV network service can be regarded as a resource-centric view of a network slice.</td>
</tr>
<tr>
<td>A network slice subnet contains one or more network functions or other network slice subnets. A network slice subnet can be shared by multiple network slice instances (NSIs).</td>
<td>The virtualized resources for the slice subnet and their connectivity to physical resources can be represented by the nested network service (NS) concept or one or more VNFs and PNFs directly attached to the NS used by the network slice.</td>
</tr>
<tr>
<td>The network slice template (NST) describes the network slice. The network slice instance (NSI) is created using the NST and instance-specific information</td>
<td>The network service descriptor templates describe the requirements, structure, and implementation of a service.</td>
</tr>
</tbody>
</table>

Similarly, the SO contains the management function layers related to slicing (See Figure 4).

Figure 4. 3GPP slice management interface ETSI Management and Orchestration (MANO)

From the perspective of resource management, network slice instances (NSIs) can be mapped to an instance of a simple or composite network service (NS), or to a concatenation of such NS instances.
Different NSIs can use instances of the same type of NS (that is, instantiated from the same NSD) with the same or different deployment flavors. Alternatively, different NSIs can use instances of different types of NSs. The first approach can be used if the NSIs share the same types of network functions (or a large common subset) but differ in terms of the performance expected from these network functions (and from the virtual links connecting them) and/or the number of instances to be deployed for each of them. If the slices differ more significantly, mapping to different NSs, each with its own NSD, can be considered. The same mapping principles might also apply to NSSIs.

**What does it mean for lifecycle management?**

3GPP TR 28.801 [i.21] describes the lifecycle of a network slice, which comprises the following four phases:

- Preparation
- Instantiation, configuration, and activation
- Run-time
- Decommissioning.

These phases can now be described in relation to the NFV MANO:

**The preparation phase** includes the creation and verification of NST(s). From an NFV perspective, the resource requirement for an NST can be realized by one or more existing NSDs, which have been on-boarded previously on the NFVO. The creation of a new NST can require the update of an existing NSD or the generation of a new NSD followed by on-boarding the new NSD if the slice requirements do not map to an NSD that is already on-boarded (that is, available in the NSD catalogue). Indeed, the NS for the multiple NSIs may be instantiated with the same NSD. This is to deliver the same optimizations and features but dedicated to different enterprise customers. On the other hand, a network slice intended to support totally new customer facing services is likely to require a new NS and thus the generation of a new NSD.

**The network slice instantiation** step in the second phase triggers the instantiation of the underlying NSs. NFV-MANO functions are only involved in the network slice configuration phase if the configuration of virtualization-related parameters is required on one or more of the constituent VNF instances. Configuration of the network applications embedded in the constituent network functions involves the network slice management function (NSMF) or network slice subnet management function (NSSMF) and/or other parts of the operations support system/business support system (OSS/BSS), and the element managers (if any) associated to these functions. NFV-MANO functions can be triggered during the network slice activation step. If explicit activation of VNFs is required, the NSMF or the NSSMF can change the operational state of those VNFs through an update NS operation.

The involvement of NFV-MANO “in the run-time” phase is limited to the operations related to performance management, fault management, and lifecycle management of virtualized resources (for example, scaling an underlying NS to expand an NSI).

The decommissioning phase triggers the termination of the underlying network service instances. As a result, the existing NFV MANO, as well as the NFVO and SO, in particular, can be used to implement 5G slicing.
Secure the chimney

The parallels drawn in this paper to the tale of The Three Little Pigs would not be complete without a look at the chimney used by the wolf to enter the house. This parallel naturally raises the question: What about security in a 5G slicing environment?

When slicing a network, the typical intention is that a slice not affect the other slices that exist in parallel on the same infrastructure. When the business model requires slice isolation, slices should be isolated from other slices, except for well-defined interfaces between slices which allow interaction, where required. If network multi-tenancy is assumed (that is, where different parties operate different slices, for example multiple verticals operating multiple slices created and rented out by a mobile network operator) network slice isolation becomes the crucial aspect of security. Security isolation refers to the property that information in one slice cannot be accessed or modified by other slices sharing the same infrastructure.

In its role as an isolated logical network or network part, each slice clearly needs state-of-the-art network security measures. These might include perimeter security and network zoning by means of firewalls (typically not firewall appliances, but virtual firewalls), separation of different traffic types, intrusion and anomaly detection, as well as cryptographic traffic protection. Slices enable the adaption of these security measures to the individual needs of the application(s) supported by this slice. For example, an IoT slice may provide a different choice of authentication and/or encryption mechanisms than an enhanced mobile broadband (eMBB) slice.

Differences in the security setup of different slices also relate to the degree of security assurance provided for the individual VNFs that form the slice. Obviously, the security assurance for a slice can never be higher than the security assurance of the infrastructure it runs on. Consequently, a highly secure infrastructure is a prerequisite for getting the high security assurance required for certain mission-critical applications handled in a slice.

Slicing a network means increasing its complexity, and thus increasing the attack surface. For example, attackers might target new procedures, such as slice selection or slice-specific authentication and authorization procedures. Furthermore, any interfaces created to allow management access to slices for third parties, such as industry verticals that operate their own slices, might be attacked. Similarly, when common network functions interface to slice specific functions in third-party slices, they need to be protected against erroneous or malicious usage by third-party network functions. This might be caused by the third party operating the slice and configuring its network functions in an erroneous or malicious way. All of these attacks can be mitigated by state-of-the-art security measures provided by a modern identity and access management (IAM) system, such as the Nokia NetGuard 5G Security Suite. The suite can be applied to all new slice-specific procedures and interfaces.

One specific attack that can compromise slice isolation is malicious traffic routing between slices. This can be done with user equipment (UE) that is connected to more than one slice simultaneously. However, a network or network slice must always be protected in any case against erroneous or malicious behavior of UEs. As a result, it might not represent a major difference for these defenses if an attack that uses a UE is triggered by another slice or by local malware installed on the UE. To mitigate the risk, the Nokia NetGuard 5G Security solution provides multi-dimensional security analytics that correlate data from multiple domains and sources to identify anomalies that might be suspicious, malicious or inadvertent. In addition, the solution provides contextual intelligence about the nature of the threat, the threat vectors used, in addition to the associated business risks and recommended mitigation steps.
To summarize, network slices can be secured by careful isolation facilitated by a sound implementation of the virtualization layer and the cloud stack. This is achieved by applying well-known network security measures to each of the logical networks implemented by a slice, as well as by securing all interfaces provided or used by the slices, especially management interfaces.

**Conclusion**

This paper has shown how the existing orchestration layers offered by Nokia can be used to implement 5G network slicing without adding extra complexity while, at the same time, enabling a path towards zero-touch 5G slice operations through orchestration. It has also been shown that the defense mechanism that ought to be implemented with network slicing is not fundamentally different from the security measures in current modern networks, provided that the defence mechanism is implemented soundly across the entire network architecture.

**Why Nokia**

Nokia provides the network components (including the orchestration layers shown in Figure 2) to offer the full network and service orchestration stacks without the requirement for an additional 5G slicing stack.

Security is handled by the Nokia NetGuard 5G Security Suite.

Nokia has a global practice to assist in operationalizing the digital transformation and to evolve legacy networks to the efficiency expected in a 5G context.

**Further reading**

[04/2018] “CSPs need a new approach for cloud and 5G security”  

[04/2018] “Network slicing – solid business case or commercial non-starter?”  

NFV insight series: “Scalable orchestration with a hierarchy of domain-focused orchestrators”  
https://resources.nokia.com/asset/200613

Additional information on the network slicing business case and on the improvement in total cost of ownership (TCO) to expect from network slicing can be provided by Nokia Bell Labs research and consulting.
About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2018 Nokia

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1809028662EN (September) CID 205631

Acronyms

API Application Programming Interface
BSS Business Support System
CBND CloudBand Network Director (Nokia’s NFVO)
CBAM CloudBand Application Manager (Nokia’s VNFM)
eMBB Enhanced Mobile Broadband
FCAPS Fault, Configuration, Accounting, Performance, Security
KQI Key Quality Indicator
MANO Management and Orchestration
OSS Operations Support System
NFVO Network Functions Virtualization Orchestrator
NS Network Service
NSD Network Service Descriptor
NSI Network Slice Instance
NSMF Network Slice Management Function
NSSMF Network Slice Subnet Management Function
NST Network Slice Template
SDN Software-Defined Networks
VIM Virtualized Infrastructure Manager
VNF Virtual Network Function