

Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 19, 2018

X. de Foy
A. Rahman
InterDigital Communications, LLC
October 16, 2017

**Network Slicing - 3GPP Use Case
draft-defoy-netslices-3gpp-network-slicing-02**

Abstract

This document describes work conducted at the 3GPP standard organization on 5G Network Slicing. Its goal is to provide detailed use cases, and help better define requirements, for Internet Protocols supporting Network Slicing.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 19, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Background	3
1.2.	NS Work in 3GPP Prior to 5G Phase 1	3
2.	Network Slicing Requirements in 3GPP	3
3.	Network Slicing in Logical 5G Architecture in 3GPP	4
3.1.	Early Work on RAN Slicing	7
4.	Management Aspect of Network Slicing in 3GPP	8
5.	5G Virtual Infrastructure Management in 3GPP	8
6.	Security for Network Slicing in 3GPP	10
7.	Analysis and Input to IETF NETSLICES	12
7.1.	Use Cases	12
7.1.1.	Management Use Case: Create or Terminate a 3GPP Network Slice Subnet	12
7.1.2.	Management Use Case: Create or Terminate a Complete 3GPP Network Slice	13
7.1.3.	Management Use Case: Activate or Deactivate a Complete 3GPP Network Slice	14
7.1.4.	Management Use Case: Update a Complete 3GPP Network Slice	14
7.1.5.	Management Use Case: Monitor Network Slices	15
7.1.6.	Management Use Case: Slice Management Exposure	15
7.1.7.	Management Use Case: Support for Multi-Domain Network Slice	16
7.1.8.	Operational Use Case: Select Network Slices for a Device	16
7.1.9.	Operational Use Case: Create or Terminate a PDU Session	16
7.2.	Additional Discussion on Security Related Requirements	17
8.	Security Considerations	18
9.	IANA Considerations	18
10.	Acknowledgements	18
11.	Informative References	18
	Authors' Addresses	19

[1.](#) Introduction

This document describes work conducted at the 3GPP standard organization on 5G Network Slicing. Its goal is to provide detailed use cases, and help better define requirements, for Internet Protocols supporting Network Slicing.

The concept of Network Slicing (NS) is considered a key mechanism for 5G networks to serve vertical industries with widely different service needs, in term of latency, reliability, capacity, and domain specific extra functionalities. It does so by exposing isolated partitions of network resources and services. The IETF Bar-BoF

NETSLICES activity studies the need for supporting protocols. In particular, [[I-D.gdmb-netslices-intro-and-ps](#)] defines NS in a broad context and suggests related problems and work areas. It also identifies the need to provide use cases such as, for example, ultra-low latency and massive-connectivity machine communication services. We propose to review ongoing NS work in 3GPP within the present document. This constitutes in our view another valid type of use case, since 3GPP architecture may ultimately use or integrate with NS solutions defined in IETF.

Sections [2](#) to [6](#) aim to represent the current state of NS and related aspects in 3GPP. We attempted to leave our own analysis out of these sections and present it into [section 7](#). For simplicity, 3GPP-specific acronyms are defined in the section they are used, which is mostly [section 3](#).

[1.1](#). Background

The 3GPP standard organization is in the process of developing 5G system architecture, which includes NS. In the present document we will use information collected from 3GPP Release 15 specifications (as well as preliminary studies from Release 14 when specifications are not yet available). This release aims to address a more urgent subset of commercial needs in "5G Phase 1", with expected deployments in 2020. Work on NS is split between different working and study groups, reviewed here in separate sections.

[1.2](#). NS Work in 3GPP Prior to 5G Phase 1

While the present document will only focus on NS in 5G Phase 1, an early form of NS was introduced in Release 13, with the Dedicated Core Network (DCN) or DECOR feature, where dedicated core network nodes are forming a DCN serving subscribers or devices with a certain "usage type" (e.g. machine-to-machine or enterprise). In the Release 14 eDECOR feature, the DCN selection mechanism was extended to be assisted by the device, which can now send its usage type to the RAN. This is specified in [[3GPP.23.401](#)]. Deployments are expected in 2017 and 2018.

[2](#). Network Slicing Requirements in 3GPP

NS requirements are included in [[3GPP.22.261](#)]. There are requirements related to:

- o Provisioning: create/modify/delete Network Slices, provision network functions to be used in Network Slices, define network services and capabilities supported by a network slice.

- o Managing association to slices: configure association of devices and services to Network Slices, move/remove user between/from slices.
- o Interoperating: support roaming and non-roaming using the same home slice, support devices simultaneously connected to multiple slices.
- o Supporting performance and isolation: support dynamic slice elasticity, ensure performance isolation during normal and elastic slice operation and during slice creation or deletion, enable operators to differentiate performance and functionalities between slices.

3. Network Slicing in Logical 5G Architecture in 3GPP

5G network architecture is entering its normative stage in 2017 with a "5G System - Phase 1" Release 15 work item, which is in the process of producing two technical specifications: 23.501 "System Architecture for the 5G System" and 23.502 "Procedures for the 5G System". At this early stage, though, we will still need to refer to the earlier technical report [[3GPP.23.799](#)]. The following text summarizes what has been agreed about NS (refer to [section 8.1](#) of that report for more details).

A Network Slice is a complete logical network including Radio Access Network (RAN) and Core Network (CN). It provides telecommunication services and network capabilities, which may vary (or not) from slice to slice. Distinct RAN and Core Network Slices will exist. A device may access multiple Network Slices simultaneously through a single RAN.

The device may provide Network Slice Selection Assistance Information (NSSAI) parameters to the network to help it select a RAN and a core network part of a slice instance for the device. A single NSSAI may lead to the selection of several slices. The network may also use device capabilities, subscription information and local operator policies to do the selection.

A NSSAI is a collection of smaller components, Session Management NSSAIs (SM-NSSAI), which each include a Slice Service Type (SST) and possibly a Slice Differentiator (SD). Slice service type refers to an expected network behavior in terms of features and services (e.g. specialized for broadband or massive IoT), while the slice differentiator can help selecting among several Network Slice instances of the same type, e.g. to isolate traffic related to different services into different slices.

A PDU session is a 5G concept for an association between the device and a data network, which can be IP, Ethernet or Unstructured (i.e. transparent to the 5G system). The device will associate an application with one out of multiple parallel PDU sessions, each PDU session correspond to one core Network Slice and one RAN slice. Different PDU sessions may belong to different slices. More precisely, an application will be associated with a SM-NSSAI (as mentioned above, this includes a slice service type and may also include a slice differentiator), and data for this application will be routed to a PDU session associated to this SM-NSSAI.

Part of the control plane, the Common Control Network Function (CCNF), is common to all or several slices. It includes the Access and mobility Management Function (AMF) as well as the Network Slice Selection Function (NSSF), which is in charge of selecting core Network Slice instances. Besides those shared functions, different Network Slices may also have dedicated control plane functions such as the Session Management Function (SMF), which manages PDU sessions. User plane functions are dedicated to each slice. The RAN selects a CCNF for a new PDU session. CCNF may initiate the redirection of service for a device towards another CCNF, initially at session setup, or later on.

In figures 1 and 2 we attempt to represent the use of NS in 3GPP logical architecture (those figures are our interpretation and are not directly adapted from the report). Figure 1 represents the role of NSSAI in network selection. Figure 2 represents the major network functions and interfaces in the context of RAN and Core Network Slicing. The terms used in these diagrams were introduced earlier. System description and diagrams in section 4 of [[3GPP.23.501](#)] can provide additional context.

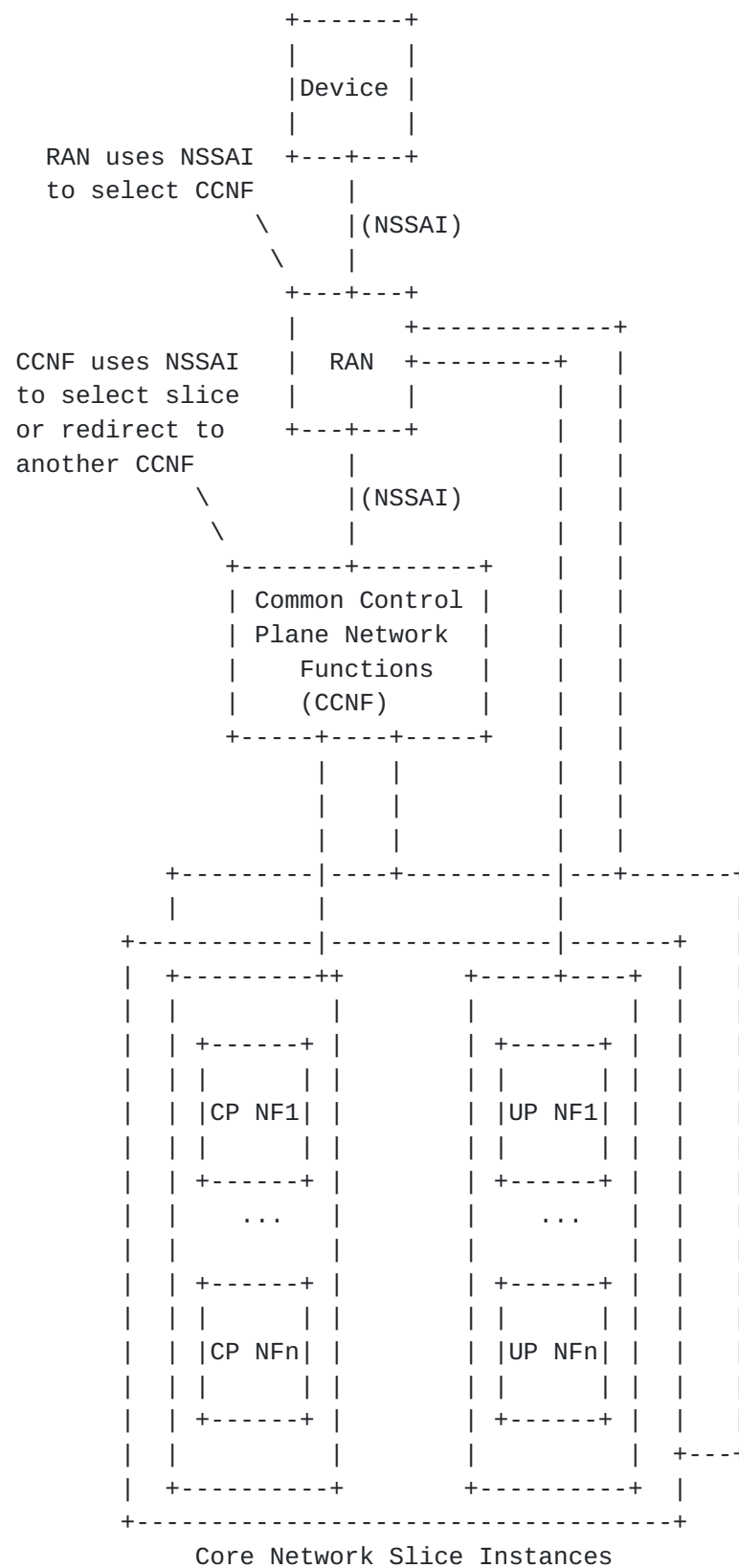


Figure 1: Network Slice Selection in 3GPP architecture

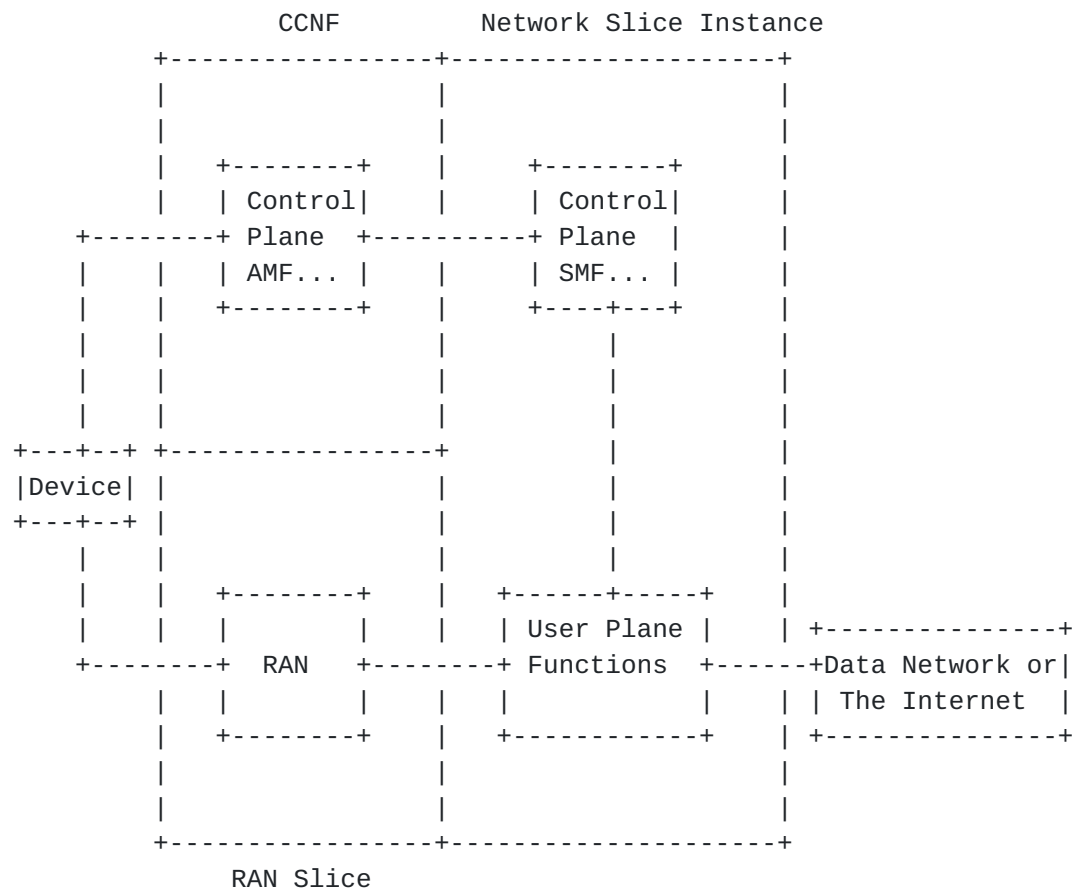


Figure 2: Network Slices in 3GPP architecture

3.1. Early Work on RAN Slicing

In line with the logical architecture described above, early work on RAN slicing is being conducted as part of the larger Release 14 "Study on New Radio Access Technology". Key principles are likely to include the following, extracted from [[3GPP.38.801](#)]:

1. RAN will support differentiated handling of traffic between pre-configured, isolated RAN slices. How to perform this is left to implementation.
2. Selection of the RAN slice will be based on IDs (which should be the slice service type and slice differentiator defined above) provided by the device or core network.
3. A RAN slice may or may not be available at a given location.
4. RAN will select the core network slice.
5. QoS differentiation within a RAN slice will be supported as well.

4. Management Aspect of Network Slicing in 3GPP

3GPP is developing a Release 14 "Study on management and orchestration of NS for next generation network" technical report [[3GPP.28.801](#)], which defines an information model where the Network Slice as well as physical and virtualized network functions belong to the network operator domain, while the virtualized resources belong to another domain operated by a virtualization infrastructure service provider.

The concept of "Network Slice Subnet" is used in the model, as defined originally in [[NGMN_Network_Slicing](#)]. Network Slice Subnet instances are comprised of physical and virtual resources, have a life cycle independent from Network Slices they belong to, can be shared between several Network Slices and may be associated with other Network Slice Subnet instances.

Multiple management use cases are described, ranging from creating and monitoring a slice instance to configuring its SLA policy, capacity and roaming support. It is also expected that some level of slice management will be exposed to customers, and that operators will have the possibility to create end-to-end Network Slices involving multiple operators' networks.

Key issues are identified, including creating a slice across multiple administrative domains, sharing a Network Slice between multiple services, moving towards a more autonomous management, as well as additional management specific key issues.

Finally, the life cycle of a slice is defined over 4 phases: preparation phase including design and pre-provisioning, an "instantiation, configuration and activation" phase, a run-time phase including supervision and reporting, as well as upgrade, reconfiguration and scaling, and a decommissioning phase.

5. 5G Virtual Infrastructure Management in 3GPP

To support the logical architecture defined earlier, some aspects of virtualization infrastructure management are also being standardized by 3GPP, through the activity "Management of mobile networks that include virtualized network functions". This includes 5 work tasks, the first of which deals with concept, architecture and requirements [[3GPP.28.500](#)], and 4 additional specialized work tasks on configuration, fault, lifecycle and performance management, are in the process of creating more detailed technical specification documents.

The new 5G management system is tied to NFV-MANO, as defined by ETSI. Its system architecture is described in [[3GPP.28.500](#)] and represented in Figure 3 (directly adapted from TS28.500). It defines interconnections between the 3GPP management system and the NFV-MANO system. NFV-MANO has the responsibility to manage NFV Infrastructure (NFVI) and VNF lifecycle, and to report performance data, fault and VNF instance information to 3GPP management system.

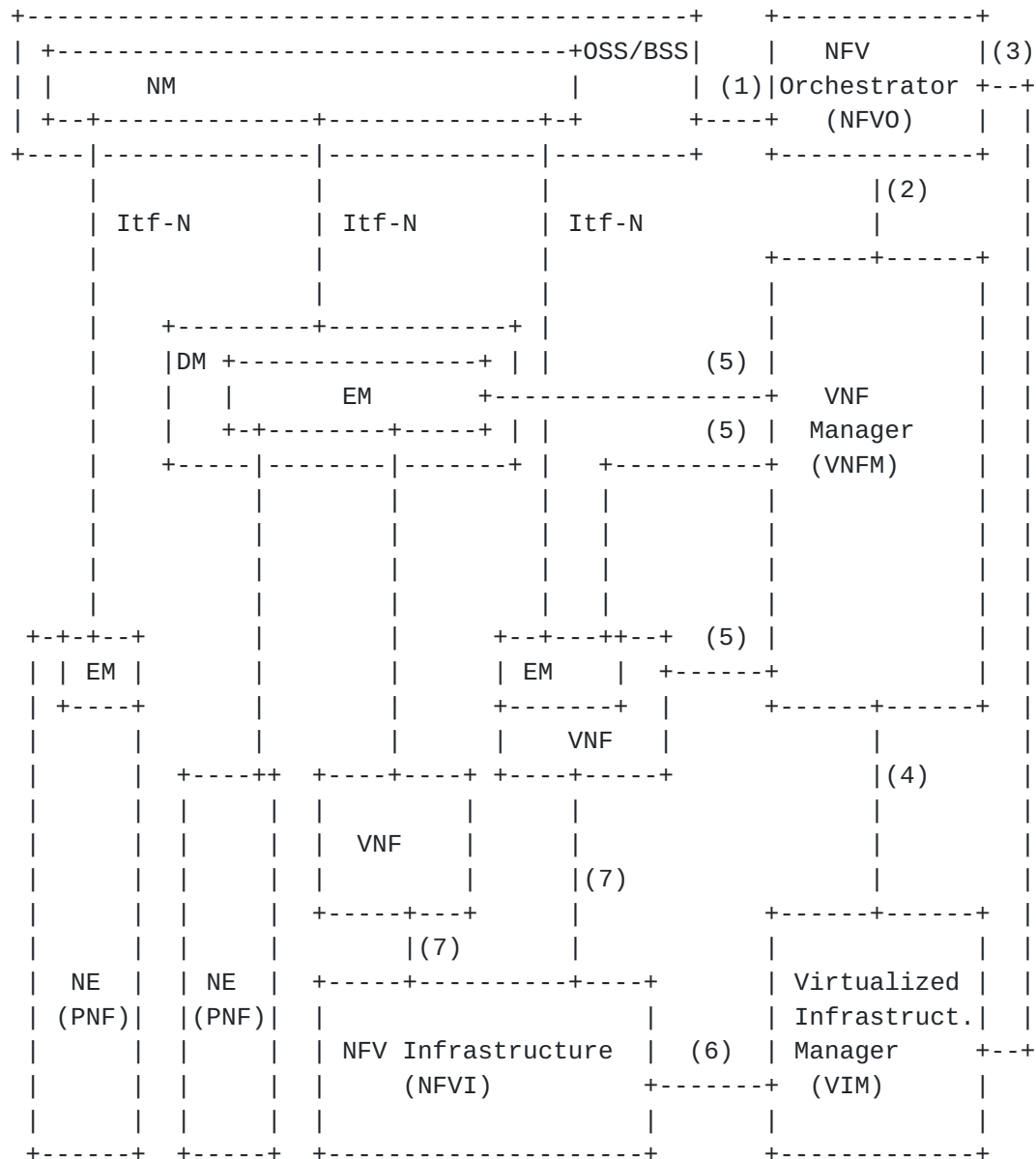


Figure 3: 3GPP Network Management Architecture

The major building blocks on the left are from pre-existing 3GPP architecture and on the right are from ETSI NFV architecture. Itf-N is the traditional 3GPP management interface between the network

manager and domain and element managers, some of which will now be collocated with VNFs. Other interfaces identified in the diagram are defined as part of the NFV architecture and described in published NFV specifications (which themselves do not make mention of NS).

- o (1) Os-Ma-nfvo enables managing Network Service Descriptors (NSD), network service lifecycle, performance, faults and VNF packages. The NSD information model is specified by ETSI NFV as well. It enables describing network connectivity topology graphs where VNFs are connected together through virtual links. An NSD also includes VNF descriptors, which include memory and CPU requirements, a link to a software image, initial setup scripts, etc.
- o (2) Or-Vnfm includes package management, VNF lifecycle/fault/configuration management, virtualized resources management (in indirect mode as seen below), and relays notifications from the VNF or EM.
- o (3) Or-Vi and (4) Vi-Vnfm are the northbound interface of the Virtual Infrastructure Manager (VIM). The orchestrator can basically use a direct interface to VIM, or indirectly go through the VNF manager over Or-Vnfm. The orchestrator can add software images, create/update/terminate virtualized compute/network/storage resources allocations, manage resource capacity, manage network virtual paths, run and query performance collection jobs, set quotas. Location/affinity constraints can be applied when creating resources.
- o (5) Ve-Vnfm is used both between VNFM and EM and between VNFM and VNFs. It includes lifecycle, performance, fault and configuration management, as well as notifications from the EM that VNFM can subscribe to.
- o (6) Nf-Vi is for assignment of virtualized resources, hardware resource configuration and state information exchange.
- o (7) Vn-Nf represents the execution environment provided to the VNF.

6. Security for Network Slicing in 3GPP

The present section on NS security is based on the "Study on Architecture and Security for Next Generation System", a Release 14 study item. Its related technical report is [[3GPP.33.899](#)], and covers, among other areas, a NS security area dealing with service access, network function sharing and isolation. Multiple key issues

are summarized here (refer to [[3GPP.33.899](#)] [section 5.8](#) for more details):

1. Isolation requirements, especially performance isolation, ask for data plane actions on one slice to have no influence on other Network Slices and for control plane actions (e.g. creation/update/deletion) to have little influence on other slices. Lack of isolation can enable DoS attacks from one slice to another, especially since some functions can be shared between slices. Moreover, a device can access multiple Network Slices, which increases the possibility for leakage/breach type of issues between Network Slices, both from the device and the service side.
2. Different Network Slices may need to implement different security policies, e.g. in term of authentication requirements (IoT vs. mobile broadband user). Authentication may be centralized and/or per-slice.
3. Security and privacy of devices' access to Network Slices is also a concern. It may be possible to forge slice selection information for a device. Slice selection information sent over the access network can also lead to confidentiality issues. The proposed key hierarchy supports having different keys for different slices. How to enable security isolation of a common control plane between different Network Slices is not addressed at this point.
4. Security of sensitive shared network elements such as the HSS (which holds customers' profiles) is identified as a key issue as well.
5. Slice management functions should be secured, since an attacker may use them, e.g. to delete a slice. Slice management capabilities exposed through APIs for 3rd parties are especially vulnerable.
6. Security on inter-slice communications is an issue in several scenarios, for example when multiple Network Slices share control plane functions, and when a RAN slice and a Core Network slice are interconnected to form a complete slice. Each slice is considered a different trusted domain.
7. A range of potential issues related to virtualization are yet to be explored further, though it is not clear if they are in the scope of 3GPP. Issues include for example isolation between VNFs hosted by the same hypervisor, authentication between VNFs, performance isolation between VNFs.

7. Analysis and Input to IETF NETSLICES

Earlier sections of this document summarized our understanding of 5G architecture and requirements for NS, as defined by 3GPP, in their current state. Our goal in these sections was to provide context to IETF NETSLICES, since a protocol or framework defined by IETF for NS may be used to implement or interoperate with 3GPP-compliant 5G systems. In reference to Figure 3, the scope of IETF involvement with NS could be within NFV Infrastructure, as well as some aspects of the control plane on the right-hand side of the figure. The concept of "Network Slice Subnet" discussed in [section 4](#) may be useful as a building block, e.g. a single-domain and composable service chain that is used to assemble a network slice. Defining the interfaces of such a component could help focusing on sharing between Network Slices and extending Network Slices across domains.

We will now attempt to derive high level use cases and requirements from this work. The goal is to serve as 3GPP-focused input to future efforts to gather use cases and requirements for IETF NETSLICES.

7.1. Use Cases

The following 3GPP-focused use cases for NS are derived from the reviewed 3GPP specifications and reports. Especially, management related use cases are derived from [[3GPP.28.801](#)] and operational use cases are derived from [[3GPP.23.501](#)].

The goal here is to describe the use cases at high level only, with the understanding that the IETF NETSLICES group may choose to define selected use cases further if needed.

In the following text we will use the terms "Complete 3GPP Network Slice" to refer to a "Network Slice Instance" used by 3GPP, and "3GPP Network Slice Subnet" to refer to "Network Slice Subnet Instance". Moreover, we consider that the (IETF) Network Slice concept is a generalization of the "3GPP Network Slice Subnet", i.e. the "3GPP Network Slice Subnet" is a particular Network Slice which happens to be part of a 3GPP network.

7.1.1. Management Use Case: Create or Terminate a 3GPP Network Slice Subnet

The operator's OSS/BSS provides a description of a Network Slice to the Orchestrator, which, through the Virtual Infrastructure Manager, configures compute and network elements to create a Network Slice holding a specific set of interconnected virtual and/or physical network functions. User plane Network Slices include one or more bidirectional paths between network functions (i.e. one or more

service function chains). Control plane Network Slices can either include a set of service function chains or alternatively can interconnect multiple network functions in a virtual network. In all cases, Network Slices are defined with a variable set of reserved KPIs, including minimum and maximum throughput, delay, packet loss, etc.

Potential requirements:

- o A Network Slice can be a service function chain or a virtual network
- o A Network Slice can be associated with a variable set of resource reservation with regards to KPIs such as minimum and maximum throughput, delay, packet loss, etc.

7.1.1.2. Management Use Case: Create or Terminate a Complete 3GPP Network Slice

The operator creates a Complete 3GPP Network Slice by composing together smaller Network Slices together, which the highest level Network Slices being: a RAN Network Slice, a Core Network slice holding user plane (UPF) and control plane (SMF) network functions, as well common Core Network functions. Those common core network functions (AMF, PCF, etc.) may be placed in multiple Network Slices since they can have different scaling properties.

The Common CN Function Network Slices (including AMF) may be shared or dedicated to a given SMF. In the shared case, there will be traffic flows terminated within a dedicated CN slice (e.g. SMF) and the shared function. RAN Slices may similarly be shared or dedicated. In the shared case, each user traffic flow passing through a shared RAN slice will then pass through one out of multiple dedicated CN slices interconnected with this shared RAN Slice. In both (RAN and CN) shared cases, there should be reserved resources within the shared Network Slice, to ensure that the whole flow has reserved resources.

NS is not a required feature in 3GPP, especially not all Core Network functions are required to belong to a slice with a specified level of service. In some cases, common network functions like AMF and PCF may be implemented outside of a Network Slice, or, equivalently, in a Network Slice with no specified QoS.

A wide variation of cases, associating "n" Network Slices with "m" network services or applications involving "p" end devices, is supported. For example: a single slice instance could be associated with multiple IoT applications, each connected to multiple devices.

In another example, an application may split its end users in 2 service categories with different SLAs, using different Network Slice instances.

Potential requirements:

- o Network Slices can be composed of smaller Network Slices which can be dedicated or shared.
- o Functions in Network Slices can interact with network functions outside of a Network Slice.

7.1.3. Management Use Case: Activate or Deactivate a Complete 3GPP Network Slice

Each Network Slice can be created in a deactivated state, and can be later switched between activated and deactivated state. This can provide multiple advantages, e.g. speeding up procedures, and enabling using a pool of unused resources. Activation or deactivation of a Complete 3GPP Network Slice can then be orchestrated as the activation (resp. deactivation) of individual Network Slices, possibly in a given order.

Potential requirement:

- o A slice can be created deactivated, and can be switched between activated and deactivated state.

7.1.4. Management Use Case: Update a Complete 3GPP Network Slice

The operator can modify the configuration (e.g. network or compute capacity or capability) of one of the Network Slices composing the Complete 3GPP Network Slice, while it is in use. Example of such operations include:

- o Increase the capacity of NFs
- o Update the configuration of NFs
- o Add, replace or remove a NFs
- o Add, replace or remove a Network Slice

Some operations affecting a shared slice may not be possible without affecting other Network Slices, and may be replaced by other operations: for example, instead of changing the configuration of a shared AMF to accommodate the needs of a SMF, another Network Slice

with an AMF may be created or activated, and replace the original AMF's slice for this SMF.

Potential requirement:

- o Ability to add, replace, remove NFs, and Network Slices without affecting service, assuming that the network service's design enables this.

7.1.5. Management Use Case: Monitor Network Slices

The 3GPP management system monitors performance of individual Network Slice level and coalesce performance data for the whole Complete 3GPP Network Slice. Individual Network Slice level performance data is also useful to decide to scale up or down services within those slices. Performance data (or events) includes user and control traffic load data. It can also include QoS/SLA data, e.g. indicating whether services were provided at expected QoS/SLA level. Alarms notifications can be individually enabled. Events and alarms from a shared Network Slice contain enough information to be attributed by the 3GPP management system to one of the Complete 3GPP Network Slices that contain this shared Network Slice.

Potential requirements:

- o Performance monitoring (measure of KPIs and alarms) occurs at Network Slice level.
- o Performance monitoring should be able to identify flows which are shared with other Network Slices, and enable matching performance data with those flows and Network Slices.

7.1.6. Management Use Case: Slice Management Exposure

3GPP networks may in some cases expose partial 3GPP Network Slice management to third party Communication Service Providers (CSP), who may in turn consume this service or provide it to their own customers. Using this management interface a third party can request the creation of a Complete 3GPP Network Slice using specifications of NFs, isolation, security, performance requirements (such as traffic demand requirements for the coverage areas, QoS for service).

When a 3GPP operator exposes management data (e.g. fault management data, performance data) about a Complete 3GPP Network Slice shared by multiple customers of a CSP, exposed management data of each customer is isolated from each other.

Potential requirement:

- o Management data should enable identification of individual flows in such a way that it can be match to different customer groups.

7.1.7. Management Use Case: Support for Multi-Domain Network Slice

To support roaming, a 3GPP operator configures one or more Complete 3GPP Network Slice to be selected to support roaming subscribers, to act as visited Complete 3GPP Network Slices. Operators configure the interconnection of a home Complete 3GPP Network Slice in one domain and a visited Complete 3GPP Network Slice in the other domain. Performance data is sent from the visited domain to the control function in the home domain.

Potential requirement:

- o Support secure inter-domain interconnection for exchanging user plan traffic and performance data.

7.1.8. Operational Use Case: Select Network Slices for a Device

A subscriber's device initially connects to the network. It sends, over a signaling path through the RAN, a message including a Network Slice Selection Assistance Information (NSSAI), which is a set of one or more tuples (slice type, slice differentiator). The RAN selects an appropriate AMF and forwards the NSSAI to this function. The AMF determines (possibly with the help of a Network Slice Selection Function) the set of allowed (slice type, slice differentiator) for this subscriber, using the NSSAI, device capabilities, subscriber's profile, and operator policy. There is no physical resource reservation at this stage.

Slice selection in this context is a preparation of control plane functions and may probably be considered out of scope for a general NS framework. Therefore no potential requirements are derived from it.

7.1.9. Operational Use Case: Create or Terminate a PDU Session

At some point, the device needs a PDU session to transport flows for a specific application. It sends, over a signaling path through the RAN, a PDU session establishment request to the AMF, typically including a tuple (slice type, slice differentiator) and a data network name. If no such tuple is provided, the AMF will determine a default one to use. The AMF will then determine which SMF (i.e. which Core Network Slice) to use, taking into consideration: the tuple (slice type, slice differentiator), data network name, subscription information, local operator policies and load conditions of the candidate SMFs. If this is a home-routed roaming case, the

AMF will select a SMF in the visited network and another SMF in the home network. The SMF selects the user plane function (UPF) that will handle the traffic, and transmits configuration information to this UPF (e.g. packet detection, QoS enforcement and reporting rules to be installed on the UPF for this PDU Session).

Potential requirement:

- o A network slice control API should enable installing new flows and associated reporting rules.

7.2. Additional Discussion on Security Related Requirements

In addition to potential requirements listed along with the use cases above, here is a list of additional discussion points related to security requirements and not directly described in a use case at this point:

1. 3GPP architecture demonstrates a requirement for authenticating users of Network Slice resources (which may or may not be within the scope of an IETF framework). There is however a need for separate per-slice security policies, e.g. having different authentication requirements between IoT and broadband.
2. Interoperation between Network Slices is a major risk factor on isolation and can occur in various scenarios:
 - * "Interoperation for extension" when data and control plane are interconnected for extending a slice between RAN and CN, or between visitor and home networks in a roaming scenario.
 - * "Interoperation through network function sharing" occurs in 3GPP when some control planes functions are performed by common functions.
 - * "Interoperation through end points" can occur on user devices connected to multiple Network Slices, or on an application server side interacting with clients over different slices.
3. There is a strict requirement for security and performance isolation from data plane and control plane actions between slices. Should Network Slices be allowed to tap into currently unused resource capacity? There is a possible tradeoff here between performance/network efficiency and isolation, since in this case, through its normal operation, a slice may influence another slice by denying it this extra capacity.

8. Security Considerations

Security aspects of NS in 3GPP are covered in [section 6](#).

9. IANA Considerations

This document requests no IANA actions.

10. Acknowledgements

The authors would like to thank Ulises Olvera-Hernandez for his contribution and comments.

11. Informative References

[_3GPP.22.261]

3GPP, "Service requirements for next generation new services and markets", 3GPP TS 22.261 1.1.0, February 2017, <<http://www.3gpp.org/ftp/Specs/html-info/22261.htm>>.

[_3GPP.23.401]

3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 14.2.0, 12 2016, <<http://www.3gpp.org/ftp/Specs/html-info/23401.htm>>.

[_3GPP.23.501]

3GPP, "System Architecture for the 5G System", 3GPP TS 23.501 0.2.0, 2 2017, <<http://www.3gpp.org/ftp/Specs/html-info/23501.htm>>.

[_3GPP.23.799]

3GPP, "Study on Architecture for Next Generation System", 3GPP TR 23.799 14.0.0, 12 2016, <<http://www.3gpp.org/ftp/Specs/html-info/23799.htm>>.

[_3GPP.28.500]

3GPP, "Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions", 3GPP TS 28.500 1.3.0, 11 2016, <<http://www.3gpp.org/ftp/Specs/html-info/28500.htm>>.

[_3GPP.28.801]

3GPP, "Study on management and orchestration of network slicing for next generation network", 3GPP TR 28.801 0.4.0, 1 2017, <<http://www.3gpp.org/ftp/Specs/html-info/28801.htm>>.

[_3GPP.33.899]

3GPP, "Study on the security aspects of the next generation system", 3GPP TR 33.899 0.6.0, 11 2016, <<http://www.3gpp.org/ftp/Specs/html-info/33899.htm>>.

[_3GPP.38.801]

3GPP, "Study on the security aspects of the next generation system", 3GPP TR 38.801 1.0.0, 12 2016, <<http://www.3gpp.org/ftp/Specs/html-info/38801.htm>>.

[I-D.gdmb-netslices-intro-and-ps]

Galis, A., Dong, J., kiran.makhijani@huawei.com, k., Bryant, S., Boucadair, M., and P. Martinez-Julia, "Network Slicing - Introductory Document and Revised Problem Statement", [draft-gdmb-netslices-intro-and-ps-02](#) (work in progress), February 2017.

[NGMN_Network_Slicing]

NGMN, "Description of Network Slicing Concept", 1 2016, <https://www.ngmn.org/uploads/media/160113_Network_Slicing_v1_0.pdf>.

Authors' Addresses

Xavier de Foy
InterDigital Communications, LLC
Montreal
Canada

Email: Xavier.Defoy@InterDigital.com

Akbar Rahman
InterDigital Communications, LLC
Montreal
Canada

Email: Akbar.Rahman@InterDigital.com

