



# Security Aspects of Network Capabilities Exposure in 5G

next generation mobile networks



# Security Aspects of Network Capabilities Exposure in 5G

by NGMN Alliance

<b>Version:</b>	<b>1.0</b>
<b>Date:</b>	<b>21-September-2018</b>
<b>Document Type:</b>	<b>Final Deliverable (approved)</b>
<b>Confidentiality Class:</b>	<b>P - Public</b>
<b>Authorised Recipients:</b> (for CR documents only)	

<b>Project:</b>	<b>NGMN - 5G Security</b>
<b>Editor / Submitter:</b>	<b>Jovan Golic</b>
<b>Contributors:</b>	<b>Min ZUO (China Mobile), Ke WANG (China Mobile), Xiaojun ZHUANG (China Mobile), Minpeng QI (China Mobile), Charles Hartmann (Orange), Marc Kneppers (Telus), Shah Yogendra (InterDigital), D'Alessandro Rosalia (TIM), Jovan Golic (TIM)</b>
<b>Approved by / Date:</b>	<b>NGMN Board, September 21st 2018</b>

© 2018 Next Generation Mobile Networks Ltd. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from NGMN Ltd.

The information contained in this document represents the current view held by NGMN Ltd. on the issues discussed as of the date of publication. This document is provided "as is" with no warranties whatsoever including any warranty of merchantability, non-infringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein. This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based on this document.

**Commercial Address:**

**ngmn Ltd.,**

Großer Hasenpfad 30 • 60598 Frankfurt • Germany

Phone +49 69/9 07 49 98-04 • Fax +49 69/9 07 49 98-41

**Registered Office:**

**ngmn Ltd.,**

Reading Bridge House • George Street • Reading •  
Berkshire RG1 8LS • UK

Company registered in England and Wales n. 5932387,  
VAT Number: GB 918713901



## Scope and Purpose

5G network is expected to expose some of its capabilities to 3<sup>rd</sup> parties in order to catalyze the creative services based on them. The exposed network capabilities should thus create new business opportunities, but may also introduce new security risks. The security considerations depend on the exposure scenarios, the local regulation constraints, business models, and trust/liability models among the service user, the network capability provider (i.e., the network operator), and the network capability consumer (i.e., the 3<sup>rd</sup> party).

The scope of this document is:

- To identify different network capabilities exposure scenarios;
- To investigate and propose security requirements for these scenarios;
- To investigate the exposure of security capabilities and present and evaluate the corresponding use cases.

The main purpose of this document is:

- To help the network operators and their partners to find secure and beneficial ways of exposing the network capabilities;
- To influence the 5G-related standardization work in 3GPP (in particular, in SA3, SA1, SA2 and SA6) as well as in other SDOs.

## Document History

1	Date	2	Version	3	Author	4	Changes
	Jun. 2, 2017		V 0.0.1		Min ZUO (CHINA MOBILE)		Creation of the initial draft
	Jun. 18, 2017		V 0.0.2		Min ZUO (CHINA MOBILE)		Update in response to initial comments from SCT (Orange, Vodafone, DT)
	July 4, 2017		(ppt)		Min ZUO (CHINA MOBILE) Ke WANG (CHINA MOBILE)		1) Network capability exposure in NGMN 2) Network capability exposure in 3GPP 3) Scope of NECsec WI
	Sept. 21, 2017		(ppt)		Ke WANG (CHINA MOBILE)		1) Progress since July 2) Proposed Schedule of the WI
	Oct. 31, 2017		V 0.0.3		Ke WANG (CHINA MOBILE) Min ZUO (CHINA MOBILE)		1) Addition of analysis of 3GPP SA5 work, NGMN E2E architecture framework WP; some other changes in Section 1 2) Some changes in Section 2 in response to Charles' comments 3) Update of Section 3
	Nov. 15, 2017		V 0.0.4		Ke WANG (CHINA MOBILE) Min ZUO (CHINA MOBILE)		Some changes in Section 2 and 3 in response to Charles' comments
	Nov.16, 2017		(ppt)		Min ZUO (CHINA MOBILE)		Introduction and summary of the WI
	Nov. 27, 2017		V 0.0.5		Min ZUO (CHINA MOBILE) Ke WANG (CHINA MOBILE)		1) Update of Section 1 with new progress of SA1 and SA6 2) Update of Section 3

Dec. 17, 2017	V 0.0.6	Min ZUO (CHINA MOBILE) Ke WANG (CHINA MOBILE) XiaoJun Zhuang (CHINA MOBILE) Charles Hartmann (Orange) Marc Kneppers (Telus)	1) Update Section 1 with new progress of CAPIF security 2) Update Section 2 with different levels of scenarios 3) Update Section 3.2 with scenarios evaluation corresponding to exposed capabilities 4) Addition of Section 3.2.3 5) Move FFS text to APPENDIX 6) Update references
Jan. 9, 2018	V 0.0.7	Min ZUO (CHINA MOBILE) Ke WANG (CHINA MOBILE) Charles Hartmann (Orange) Xiaojun ZHUANG (CHINA MOBILE)	1) Update Section 1 by adding an overview of work in oneM2M and ETSI MEC and updating work in SA2 2) Update references and abbreviations
Jan. 18, 2018	V 0.0.8	Min ZUO (CHINA MOBILE) Ke WANG(CHINA MOBILE) Marc Kneppers (Telus)	1) Add overview, relationship and status of the SDOs' work 2) Add figures to show the scenarios for each capabilities 3) Add text on exposure of slice authorization and integrated monitoring security functions
Feb. 8, 2018	V 0.0.9	Min ZUO (CHINA MOBILE) Rosalia D'Alessandro (TIM) Ke WANG (CHINA MOBILE)	1) Update according to Rosalia's comments 2) <i>Name this version as internal TR</i>
Feb. 15, 2018		Jovan Golic (TIM)	Start working on white paper on the basis of TR 1) Initial proposal for a major revision with section restructuring and new and more detailed definitions and clarifications throughout 2) New structure: Abstract, Section 1 as short introduction (based on previous Section 1), Section 2 as basic definitions (new), Section 3 as background (part of previous Section 1), Section 4 on network capabilities exposure scenarios (previous Section 2), Section 5 on security requirements (previous Section 3.1), Section 6 on exposure of security capabilities (previous Section 3.2), Appendix A on prior and ongoing work in SDOs (previous Section 1); previous Appendix on FFS topics removed

Apr. 4, 2018	V 0.0.10	Jovan Golic (TIM) Marc Kneppers (Telus) Ke WANG (CHINA MOBILE)	1) Incorporate Jovan's proposal on abstract, introduction, definitions and section restructuring 2) Add requirements in Section 5 based on Marc's proposal
Apr. 15, 2018	V 0.0.11	Jovan Golic (TIM) Ke WANG(CHINA MOBILE) Marc Kneppers (Telus) Charles Hartmann (Orange)	1) Modify and add content in Section 4 including listing the capabilities instead of giving some examples, give a comparison table and put text of Section 4 in a concise form 2) Add some privacy-related security requirements 3) Revise text of Sections 4.2, 4.3 and 4.4 by putting it in a concise form as Jovan suggested, with only remaining examples of exposable capabilities and information flow 4) Rewrite and add figures in Section 6
Apr. 23, 2018	V 0.0.12	Jovan Golic (TIM) Marc Kneppers (Telus) Charles Hartmann (Orange) Ke WANG (CHINA MOBILE) Feifei LOU (CHINA MOBILE) Cyril Delétré (Orange) Jean-Philippe Wary (Orange) Eldad Zeira (InterDigital) <i>(SCT f2f meeting in Paris)</i>	1) Revision of Abstract, Introduction, Definitions, Scenarios for network capabilities exposure 2) Revision and completion of Security Requirements
May 2, 2018	V 0.0.13	Charles Hartmann (Orange) Marc Kneppers (Telus) Ke WANG (CHINA MOBILE) Jovan Golic (TIM)	1) Modifications and responses addressing Charles's comments
Jun. 29, 2018	V 0.0.14	Charles Hartmann (Orange) Yogendra Shah (InterDigital) Ke WANG (CHINA MOBILE) Jovan Golic (TIM)	1) Update overview of prior and ongoing work of SDOs in Appendix A, by adding FIDO, GSMA MC, GBA, and SSO 2) Add potential use cases and the shortcomings of slice authentication in Section 6.4
Aug. 01, 2018	V.0.0.15	Charles Hartmann (Orange) Ke WANG (CHINA MOBILE) Minpeng QI (CHINA MOBILE) Jovan Golic (TIM)	1) Update the overview of prior and ongoing work of SDOs in Appendices A.1 and A.2 by adding reference to TR 22.904 and TR 23.740, respectively 2) Update References and Abbreviations

			3) Update usecases, benefits and challenges in Section 6.4 according to Charles' proposals 4) Update figures in 6.4 according to Charles' comment 5) Add MEC/LADN as FFS item in Section 5
Aug. 21, 2018	V 1.0	Jovan Golic (TIM)	Final revision and editorial changes; approval at SCT call after some minor changes
Sep. 21, 2018	V 1.0	Jovan Golic (TIM)	Minor revision according to comments received in the Board's approval process

## AUTHORS

Author	Company
Min ZUO	CHINA MOBILE
Ke WANG	CHINA MOBILE
Xiaojun ZHUANG	CHINA MOBILE
Minpeng QI	CHINA MOBILE
Charles Hartmann	Orange
Marc Kneppers	Telus
Yogendra Shah	InterDigital
Rosalia D'Alessandro	TIM
Jovan Golic	TIM



**Contents**

1 INTRODUCTION..... 8

2 DEFINITIONS..... 8

3 BACKGROUND..... 9

4 SCENARIOS FOR NETWORK CAPABILITIES EXPOSURE..... 9

    4.1 Overview of Scenarios for Network Exposure..... 9

    4.2 Level 1: Passive Exposure Scenario..... 12

    4.3 Level 2: Semi-active Exposure Scenario..... 13

    4.4 Level 3: Fully-active Exposure Scenario..... 14

5 SECURITY REQUIREMENTS FOR NETWORK CAPABILITIES EXPOSURE..... 15

    5.1 General Principles..... 15

    5.2 Security Requirements..... 16

6 EXPOSURE OF SECURITY CAPABILITIES..... 17

    6.1 Exposure of Network Authentication Results..... 17

    6.2 Exposure of Authenticator..... 18

    6.3 Exposure of Derived Keys..... 20

    6.4 Exposure of Slice Authentication..... 22

    6.5 Exposure of Slice Authorization..... 24

    6.6 Exposure of Integrated Monitoring Security Functions..... 26

REFERENCES..... 28

ABBREVIATIONS..... 29

APPENDIX A: OVERVIEW OF PRIOR/ONGOING WORK..... 32

    A.1 3GPP SA1..... 32

    A.2 3GPP SA2..... 32

    A.3 3GPP SA3..... 33

    A.4 3GPP SA5..... 34

    A.5 3GPP SA6..... 34

    A.6 3GPP CT3..... 34

    A.7 NGMN 5G White Paper..... 35

    A.8 NGMN 5G E2E Architecture Framework..... 35

    A.9 OneM2M..... 35

    A.10 ETSI MEC..... 35

    A.11 FIDO Alliance..... 36

    A.12 GSMA..... 36



## 1 INTRODUCTION

A network is used to establish communication between two endpoints, where endpoints include endpoint devices (e.g., UE), network elements (e.g., network servers), and application servers providing services to other endpoints. For this, it is necessary for network operators to provide access to the network and its basic communications services. 5G network is expected to expose some of its capabilities to 3<sup>rd</sup> parties in order to promote the usage of the network functionalities and to catalyze the creative services based on them. The scenarios for exposing the network capabilities can be classified into different categories depending on the level of control granted to the 3<sup>rd</sup> parties by the network operator. This document identifies the exposure scenarios and investigates the security aspects of the scenarios from two viewpoints:

- Security requirements for network capabilities exposure;
- Exposure of security capabilities, including the use cases, benefits and their evaluation.

## 2 DEFINITIONS

<b>Network Function (NF)</b>	Processing function in a network, enabling access and communications services. This includes a variety of control plane, user plane, and service functions that span the layers of the protocol stack, e.g., radio network functions, physical layer functions, Internet Protocol (IP) routing functions, applications etc. See [25]. A network function can be implemented by a physical or virtualized resource.
<b>Network Exposure Function (NEF)</b>	Network function enabling the exposure of network capabilities (e.g., by interaction with other NFs via APIs).
<b>Network Service (NS)</b>	Service that provides network access and basic communications services within the network. It necessarily includes primary network access [4]. It may include other access and communications services.
<b>Network Service Provider (NSP)</b>	Entity that provides network service and owns related resources and functions (physical or virtualized/logical) for providing such services. The resources and functions include spectrum, mobility and access management across heterogeneous and/or composite access networks, network management and orchestration, and network elements. See [25]. Virtualized resources may also include the network traffic data. Operators/MNOs and virtual MNOs (full MVNOs) are NSPs.
<b>Network Slice Instance (NSI)</b>	A set of run-time network functions, along with physical and logical resources to run these network functions, forming a complete instantiated logical network to meet certain network characteristics required by the Service Instance(s). A network slice instance may be fully or partly, logically and/or physically, isolated from another network slice instance. See [25].
<b>Service Instance (SI)</b>	A run-time construct of an end-user service or a business service that is realized within or by a Network Slice. See [25].
<b>Service Provider (SP)</b>	Entity that provides an application layer service. The entity may be an NSP or a 3 <sup>rd</sup> party. See [25].
<b>Third party (3<sup>rd</sup> party)</b>	Entity that is allowed to provide an application layer service as an SP or network access and communications services as a 3 <sup>rd</sup> party NSP. Such services do not include the primary network access service, which is in

full control of NSPs. Unlike an NSP, a 3<sup>rd</sup> party is thus allowed to provide only a secondary access service.

**Network capability**

Functionality or resource that one or a set of network functions provide.

**Authenticator**

Entity initiating EAP authentication [26].

### 3 BACKGROUND

The overview and underlying relationships of the (network) capabilities exposure work in SDOs can be roughly shown as in Figure 3-1. The work is grouped in three layers including 3<sup>rd</sup> party, exposed entities/interfaces and exposed capabilities.

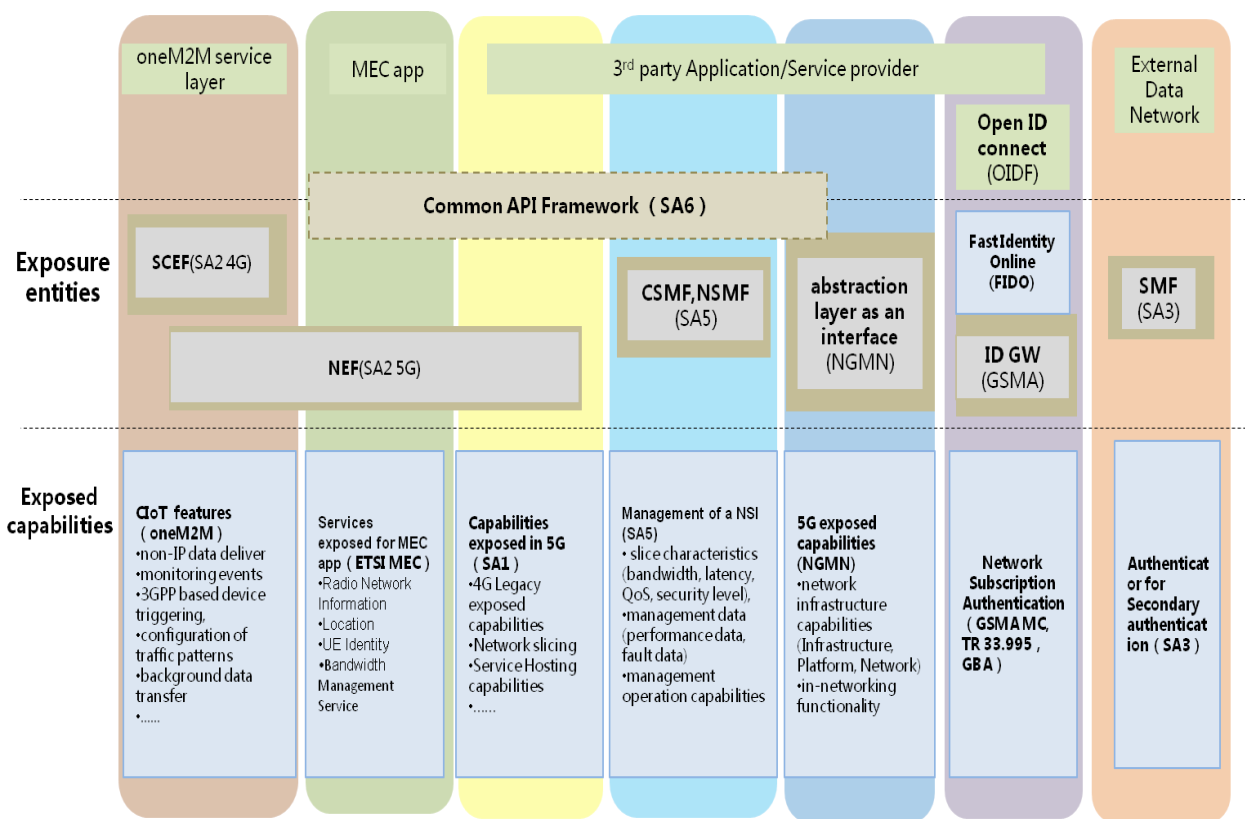


Figure 3-1. Overview of capabilities exposure work in SDOs

From the status of network capabilities exposure work shown in Figure 3-1, it follows that:

- SA1 and SA2 do not involve security capabilities exposure.
- Different SDOs define different exposed capabilities. A systematic and unified framework is still missing.

## 4 SCENARIOS FOR NETWORK CAPABILITIES EXPOSURE

### 4.1 Overview of Scenarios for Network Exposure

Network capabilities of an NSP can be classified into the following 3 categories, as depicted in Figure 4-1:

- **Network Service and Functions**, which provide access and communication services and functions to network customers. As defined in SA2 TS 23.501 [2] and TS 23.502 [3], such functions and services

include the network functions (NFs) within the 5GC control plane (CP) and user plane (UP), the NF services provided by the NFs using service-based interface, CP communications that make use of NF service operations, UP communication connections on the basis of regular UP functions and/or application layer functions, specific services such as SMS over NAS, emergency services and so on.

- **Network Infrastructure**, which provides physical or virtualized/logical resources for supporting the network service and functions. Physical resources include servers, access nodes, cloud nodes, networking nodes and associated links. Virtualized/logical resources include generic VMs, generic containers, virtualization management software, software platforms, operating system and virtual links. Data resources are here regarded as logical resources and include network traffic data, which can be separated into control plane and user plane data. These data need to be treated according to local regulations.
- **Network Management**, which provides management services and functions for other network services and functions. It translates the use cases and business models into actual network functions and slices. It defines the network slices to be used for a given application scenario, chains the relevant modular network functions, assigns the relevant performance configurations, and finally maps all of this onto the infrastructure resources. It also manages scaling of the capacity of those functions as well as their geographic distribution. In certain business models, it could also possess capabilities to allow for third parties (e.g., MVNOs and verticals) to create and manage their own network slices, through APIs.

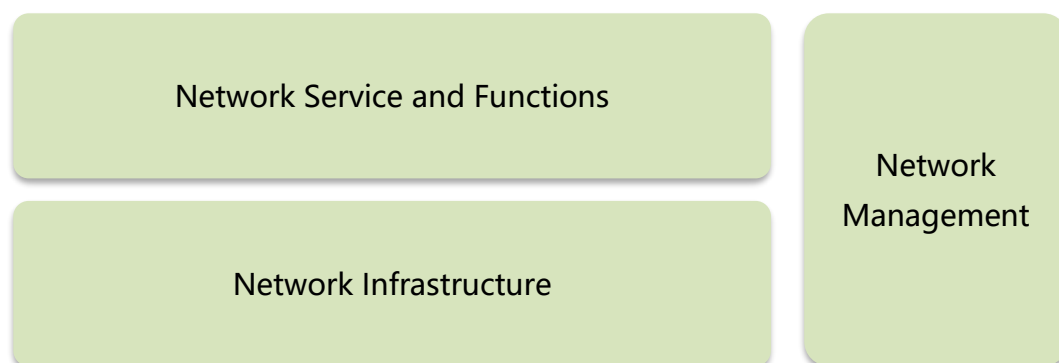


Figure 4-1. Network capabilities categories

Exposure of network capabilities of an NSP to 3<sup>rd</sup> parties means providing access to some functionality and resources of network service and functions, network infrastructure, and network management to 3<sup>rd</sup> parties in order to enable them to provide their own services according to commercial agreements with the NSP. The 3<sup>rd</sup> party can be an SP or a 3<sup>rd</sup> party NSP. The 3<sup>rd</sup> party customers are the NSP subscribers or subscribers of its roaming partners according to the roaming commercial agreements.

The scenarios for exposing the network capabilities can be classified into different categories depending on the level of access granted to the 3<sup>rd</sup> party by the network operator with respect to the degree of active exposure. At different exposure levels, the 3<sup>rd</sup> party thus has different access to exposed network capabilities with respect to the changes allowed to be performed by the 3<sup>rd</sup> party. The 3<sup>rd</sup> party will have different administrative domains and impact on the network while the capability exposure is in control of MNO all the time. In essence, we can identify the following 3 levels of exposure scenarios.

- **Level 1: Passive exposure** – The 3<sup>rd</sup> party has only passive access to exposed network service and functions. It is thus not allowed to change, control or manage the exposed network capabilities. In particular, the 3<sup>rd</sup> party can provide input data to the network and obtain the corresponding output data from the network (e.g., from the exposed network function or network access or communications service). Also, the 3<sup>rd</sup> party can request and obtain some data from the network (e.g., network traffic data). Passive access to exposure can be implemented by a NEF interacting with NFs via APIs.
- **Level 2: Semi-active exposure** – The 3<sup>rd</sup> party is allowed to customize and accordingly change, provision or manage the configuration parameters of exposed elements of the network service and

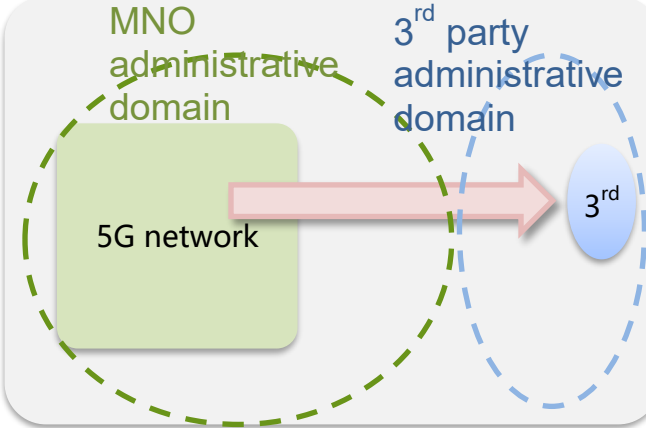
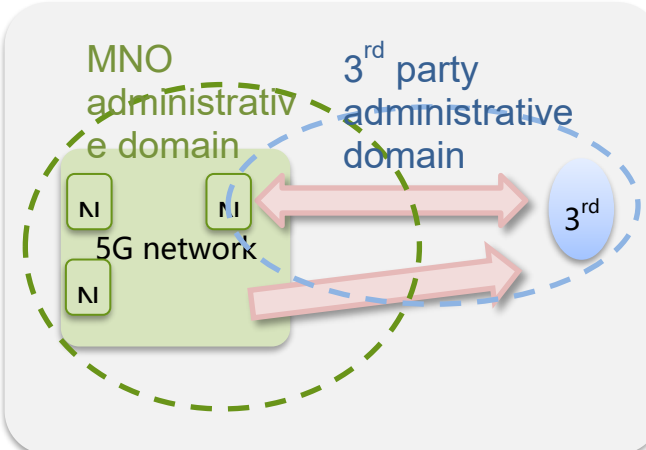
functions or network management services and functions. It is also allowed to have access to some exposed network management capabilities to accordingly customize & provision & update the configuration parameters of the network service and functions. In particular, this can relate to a closed part of the edge network. Semi-active access to exposure can be implemented by a NEF interacting with NFs via APIs or slice management interface.

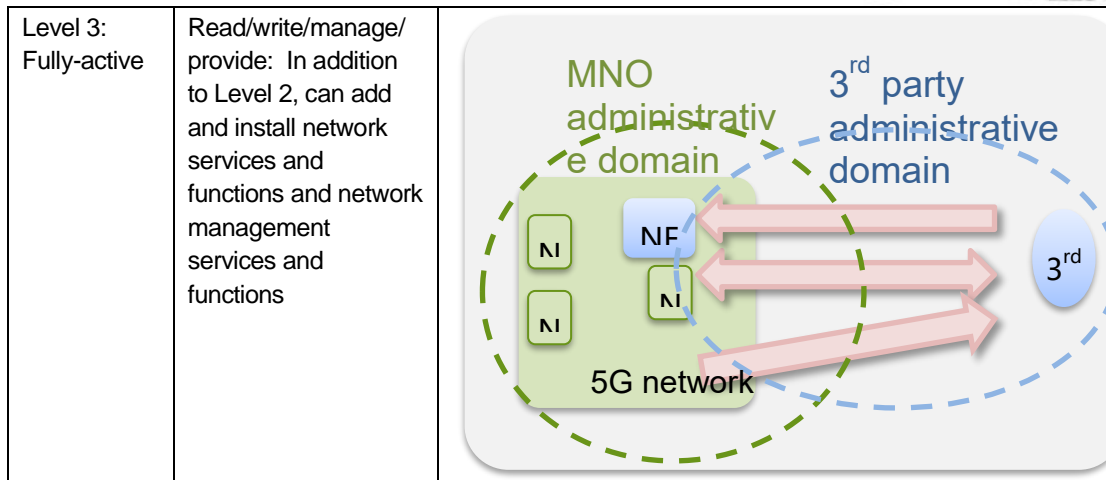
- **Level 3: Fully-active exposure** – The 3<sup>rd</sup> party is allowed to add & install & manage network access and communications services and functions and network management services and functions, on the basis of exposed network capabilities (e.g., the exposed (hosting) network infrastructure). In particular, this may relate to MEC/LADN scenarios. It is preferable that the 3<sup>rd</sup> party should not be allowed to add & install & manage new elements of the 5G core network, especially critical/sensitive network functions.

It follows that passive exposure applies to both SP and 3<sup>rd</sup> party NSP and that fully-active exposure applies only to 3<sup>rd</sup> party NSP. Semi-active exposure applies to 3<sup>rd</sup> party NSP as well as SP.

The comparison of different levels is summarized in Table 4-1 below.

Table 4-1. Comparison of different levels of exposure scenarios

Level: Degree of active access to exposure	What 3 <sup>rd</sup> party can do	Administrative domain of MNO and 3 <sup>rd</sup> party
Level 1: Passive	Read: Can passively access exposed network service and functions	
Level 2: Semi-active	Read/write/manage: In addition to Level 1, ① can configure and manage capability exposure; ② can access the network management capabilities	



It should be noted that the level of exposure is relative to the exposed network capability or capabilities, and that each level of exposure implies lower levels of exposure.

These exposure scenarios may require different business models, exposable network capabilities, trust frameworks, security features, privacy features, and liability models. Consequently, they may adapt different technical architectures and security mechanisms. Note that the 3<sup>rd</sup> party can be an external service provider (a value-added service provider, an application or content provider), an enterprise or even a roaming partner of the operator.

The operator's exposure function shall evaluate and control the legitimacy of the 3<sup>rd</sup> party requests and verify that the requests are processed in compliance with relevant national/local regulations.

#### 4.2 Level 1: Passive Exposure Scenario

Exposable capabilities in this scenario may include network monitoring capabilities, QoE response and other information capabilities that can be exposed to the 3<sup>rd</sup> party, and hence fully rely on what the operator provides.

For example, the network authentication result can be exposed to an SP portal site identifying a user. An example for the 3<sup>rd</sup> party NSP is a gaming enterprise that provides different tiers of QoS gaming services by using different QoS of network slices. The gaming enterprise can use the exposed UE roaming status to inform the visited network to provide the corresponding type of slices for continuous QoS gaming services.

The information flow of passive exposure (i.e., of passive access to exposed network capabilities) is shown in Figure 4-2. Note that passive exposure may use:

- subscribe/notify[me] method, which means that notifications are sent directly to the application that subscribed to the passive exposure event or
- request/response method.

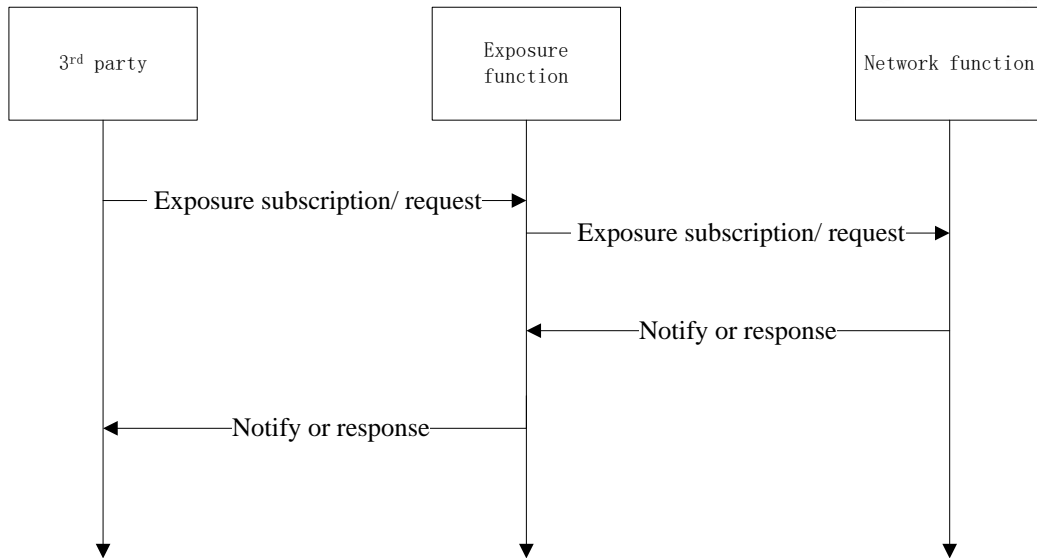


Figure 4-2. Passive exposure information flow in Level 1 scenario

1. The requesting 3<sup>rd</sup> party subscribes to or requests one or several services by sending Exposure subscription/request to the exposure function. The request is sent through the API provided by exposure functions.
2. The exposure function translates the exposure subscription/request and sends them to related network functions. This uses the reference points or RESTful API (in SBA representation) between exposure function and related NF.
3. The related network functions perform the requested network capabilities (e.g., detect occurrence of the monitored event or retrieve data) and send notification or response to the exposure function.
4. The exposure function forwards the information notified or responded to the requesting 3<sup>rd</sup> party.

### 4.3 Level 2: Semi-active Exposure Scenario

The exposable capabilities in this scenario may also include some slice management capabilities (e.g., capabilities to configure the information that associates a UE to a network slice), configuration and management of parameters of exposed elements, policy and charging capabilities, user profile provisioning and so on.

For example, an SP for this scenario can be an application server providing configuration of exposed capabilities. A 3<sup>rd</sup> party NSP for this scenario can be a vertical industry (e.g., a gaming company) that uses customized slices to provide specific services to customers.

The information flow of semi-active exposure is shown as Figure 4-3.

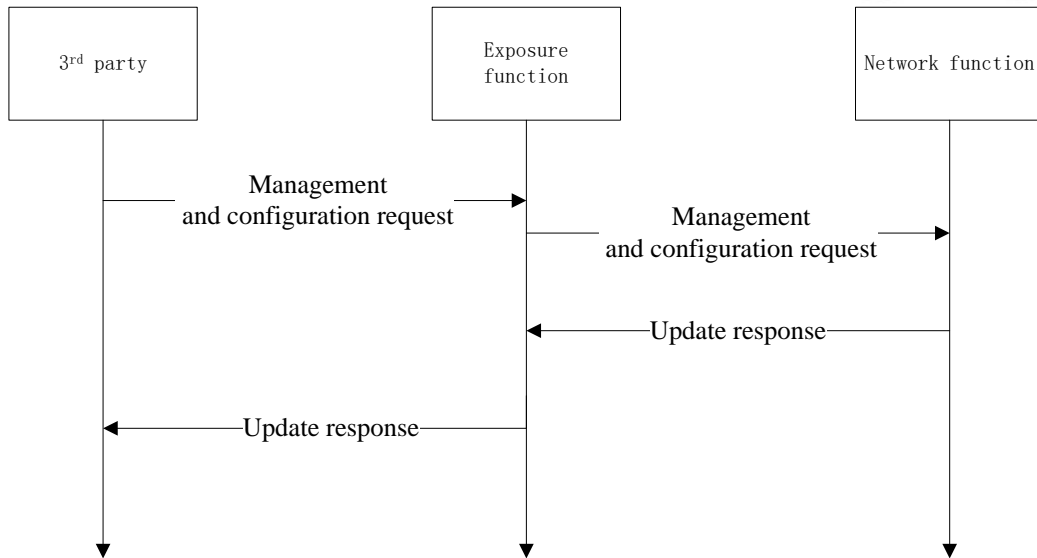


Figure 4-3. Semi-active exposure information flow in Level 2 scenario

1. The requesting 3<sup>rd</sup> party requests management and parameter configuration by sending parameter update request to the exposure function that provides API.
2. The exposure function forwards the parameter update request to related network functions.
3. The related network functions perform management and parameter configuration and send the update response to the exposure function.
4. The exposure function forwards the update response to the requesting 3<sup>rd</sup> party.

#### 4.4 Level 3: Fully-active Exposure Scenario

The exposable capabilities in this scenario may also include some service hosting capabilities (i.e., network infrastructure) to host applications provided and managed by the 3<sup>rd</sup> party in MNO's network. The 3<sup>rd</sup> party in this scenario provides network services and functions, so it can only be a 3<sup>rd</sup> party NSP.

The information flow of the fully-active (infrastructure) exposure is shown as Figure 4-4.

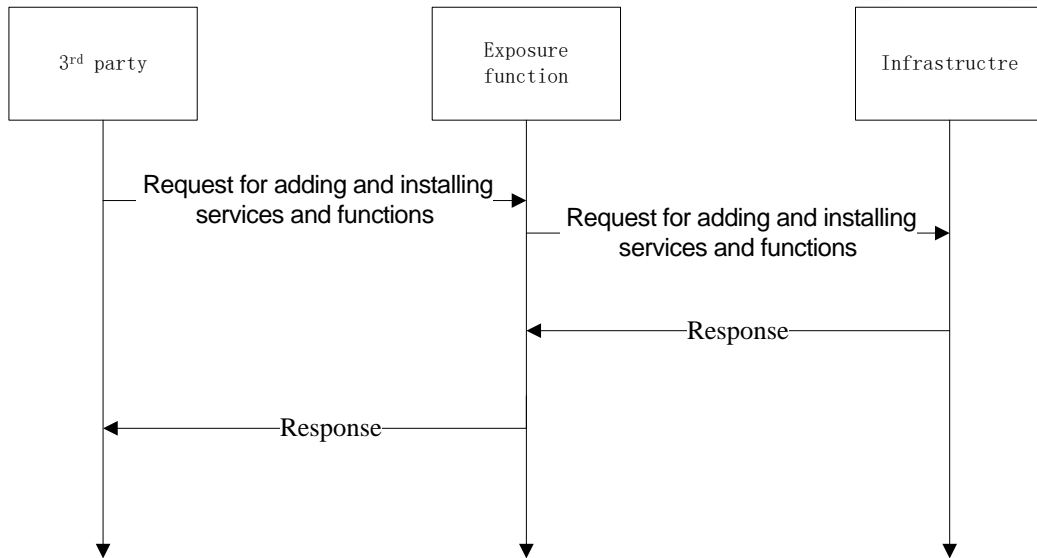


Figure 4-4. Fully-active exposure information flow in Level 3 scenario

1. The 3<sup>rd</sup> party invokes API for infrastructure as a service and requests to add and install services and functions for constructing its own network service.
2. The exposure function forwards the request to the infrastructure.
3. The requested service and functions are installed and initiated on the basis of the the (hosting) network infrastructure. The infrastructure notifies the result response.
4. The exposure function forwards the response to the 3<sup>rd</sup> party.

## 5 SECURITY REQUIREMENTS FOR NETWORK CAPABILITIES EXPOSURE

### 5.1 General Principles

A unified and general framework and infrastructure for network capability exposure providing standard, state-of-the-art, maintainable, and proven security solutions is preferable.

The framework needs to clearly delineate what is under control of the operator and what can be exposed to the 3<sup>rd</sup> party (e.g., for read-only and for read-write). It should encompass the Common API framework defined in SA6.

Network management and configuration capabilities can be exposed only in semi-active and fully-active exposure scenarios, while information capabilities can be exposed also in the passive exposure scenario.

The operator should maintain oversight of new network management functions and services introduced by the 3<sup>rd</sup> party, in semi-active or fully-active scenarios, and shall be responsible for their integration.

Exposure of API to 3<sup>rd</sup> parties is part of a commercial contract. Operators must have the capability to control - in real time - that the exposure of API is compliant to the technical terms and conditions of the contract.

For any exposure scenario, the ultimate responsibility for the exposed network capability should be determined by the legal clauses of the contract. For example, in some arrangements, the operator may take the ultimate responsibility for the exposed network capability in order to maintain the integrity of the system as a whole. On the basis of the exposed network capability, the 3<sup>rd</sup> party can be a SP providing an end-to-end service to its





customers, and the responsibility for that service is then up to the 3<sup>rd</sup> party. In any case, the contract must comply with national/local regulations (e.g., in the EU).

## 5.2 Security Requirements

The 3<sup>rd</sup> party that requires access to the exposed capabilities shall be authenticated and authorized by the operator.

Confidentiality, integrity and anti-replay protection of request and response should be ensured both in transmission and storage.

In addition, for segregation and isolation:

- Access to the NEF for ad-hoc, discrete requests (read, read/write) should be segregated from the requests for management through the NEF. This will allow for different protective measures to be applied for management;
- Management access via the NEF may be instantiated on a separate instance of the NEF;
- MEC/LADN is FFS;
- Interplay of various components of architecture SBA Rel. 16 is FFS.

New network access and communications functions and services introduced by the 3<sup>rd</sup> party should be secure and trustworthy. After their integration, the operator's network shall remain secure and should remain trustworthy. The operator shall be responsible for conducting the risk assessment of the integrated network, with special attention to critical/sensitive core network functions.

Network traffic security monitoring and anomaly detection in the integrated network should also address the new traffic introduced by the network capabilities exposure to the 3<sup>rd</sup> party. The operator should respond to security incidents in a timely manner.

The NEF should support a forensic capability to allow for the investigation of security incidents and recovery to safe state.

The exposure of security capabilities or security-related capabilities should not compromise the security of the secret keys of other parties or shared with other parties (e.g., shared symmetric keys from subscription credentials).

Without authorization, the 3<sup>rd</sup> party should not manage, configure or obtain information about slices or network functions managed by other parties.

The common parameters associated with different slice instances should not be exposed, managed or configured by 3<sup>rd</sup> parties, in order to avoid conflicts and maintain integrity.

It is important to protect the shared network resources against overload, which may be propagated over the exposed APIs. Operators are responsible for network traffic management with respect to fair use policies. Rate limiting procedures need to be applied at the API gateway. Operator may also limit the number of simultaneous active sessions and bandwidth.

When providing privacy-related (e.g., authentication-related) and other user information to the 3<sup>rd</sup> party, the operator should strictly abide by the applicable privacy protection law and regulations. In particular, privacy-sensitive information shall be securely stored and destroyed after use, and used only for legitimate purposes authorized by the user. Abuse and leakage of user information shall be prevented.

In order to ensure that APIs are not abused in an interconnected network, a transparency mechanism may be included that allows for the overall reporting of API use and inter-operator comparison. In particular, each operator must have the capability to centrally report on API metrics such as:

- Count of API call per 3<sup>rd</sup> party access, per unit time;
- Type of information queried.

In addition, 3<sup>rd</sup> parties should have unique registration numbers which allow their access to multiple operators to be tracked in a transparent and aggregated fashion. Network operators may enforce that exposed APIs use specific network ingress/egress points (applying rule-based access control at the edge of the network) and secure service access points (e.g., HTTPS reverse proxies, load balancers).

## 6 EXPOSURE OF SECURITY CAPABILITIES

This section addresses exemplary exposable security capabilities.

### 6.1 Exposure of Network Authentication Results

When a user accesses an operator's 5G network, the UE will be strongly authenticated by the network, by primary authentication based on subscription credentials. The results of this 5G network authentication can be exposed and reused for other services. Apart from the subscription-related identities (e.g., GPSI), the authentication results may also include various attributes related to the user (e.g., identity attributes), to the authentication method and others. What attributes may be offered and exposed should be defined by the contract between MNO and the 3<sup>rd</sup> party service. In this case, MNO is responsible for attribute verification, and both the MNO and the 3<sup>rd</sup> party for getting the user consent according to the respective regulation.

ITU-T X.1256 [11] recommends two types of mechanisms for sharing network authentication results with services [11]:

- *Push mode*: If the network access control entity (e.g., access control device in WLAN) understands the service's application layer protocol, it is feasible for it to insert the network authentication attributes into the application layer messages and transfer them directly to the service platform. SMF and UPF in 5G may be able to take the role of the network access control entity.
- *Pull mode*: If the network access control entity cannot parse or modify the service's application layer messages, 5G network can provide well-defined network APIs that the service applications can call to obtain authentication results from the network.

#### Scenarios evaluation:

- In passive exposure scenario, network authentication results can be exposed to the 3<sup>rd</sup> party through API. The 3<sup>rd</sup> party is not allowed to provide, install, manage or configure network authentication entities through API. See Figure 6.1-1.

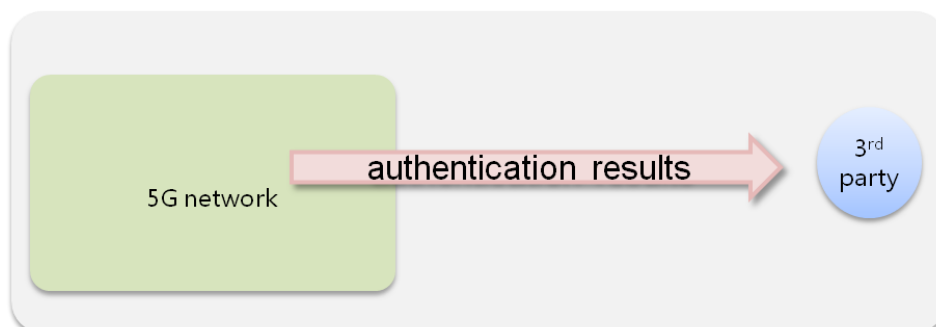


Figure 6.1-1. Exposure of network authentication results in passive exposure scenario

- In semi-active exposure scenario, network authentication results can be exposed to the 3<sup>rd</sup> party through API. The 3<sup>rd</sup> party can also configure which authentication attributes (e.g., the subscription area, authentication method and others that can be obtained from UDM) can be exposed through API, according to the contract between MNO and the 3<sup>rd</sup> party service. The authentication attributes can also include identity attributes (e.g., user-centric) associated with subscription credentials, as described above. The 3<sup>rd</sup> party is not allowed to provide or install network authentication entities related to primary authentication (through API). See Figure 6.1-2.

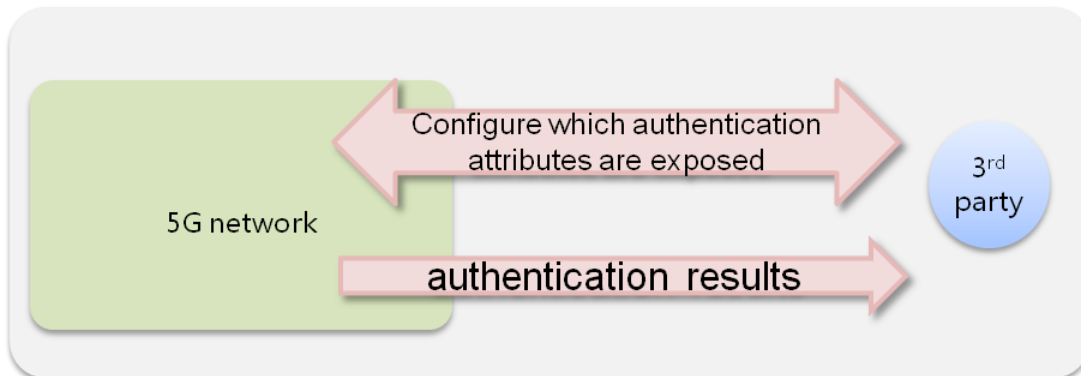


Figure 6.1-2. Exposure of network authentication results in semi-active exposure scenario

- Fully-active exposure of (primary) authentication results is not allowed, since the 3<sup>rd</sup> party is not allowed to have access to subscription credentials.

### Typical use cases:

In most cases, the end users are authenticated both in the network and in the service system. The results of 5G network authentication can be exposed and reused for customers' access to the application service through well-defined network APIs. A service application function can call these APIs to obtain authentication results from the network.

### Benefits:

- Exposure of authentication results, possibly also including the selected identity attributes, can increase influence of network operators on service platform.
- The strong and unified authentication of network layer can increase the security strength of authentication for service layer and simplify the mechanism to improve user experience.
- The service platform does not manage and store authentication credentials.

## 6.2 Exposure of Authenticator

In 5G, the authenticator, which corresponds to secondary authentication and initiates EAP authentication, can be exposed. MNO can expose one network function as an authenticator to external AAA server for the secondary access authentication. It shall rely on an external (3<sup>rd</sup> party) DN-AAA server to authenticate and authorize the UE's request for the establishment of a PDU session to external data network. This server stores the credentials for the secondary authentication. The authenticator can obtain subscription data (e.g., various user identifiers) from the UDM and check whether the UE request is compliant with the user subscription and with local policies. The authenticator also decides to trigger EAP authentication and exchange EAP messages between UE and the external AAA server. One example is the EAP based secondary authentication by an external DN-AAA server defined in SA3 TS 33.501 [4] in which SMF can perform the role of the authenticator. 5G network can also allow the 3<sup>rd</sup> party to configure the subscription profile on whether secondary authentication should be performed.

**Scenarios evaluation:**

- In passive exposure scenario, the MNO authenticator is exposed for the access authentication for external data network. The 3<sup>rd</sup> party is not allowed to provide, install, manage or configure the authenticator (through API). See Figure 6.2-1.

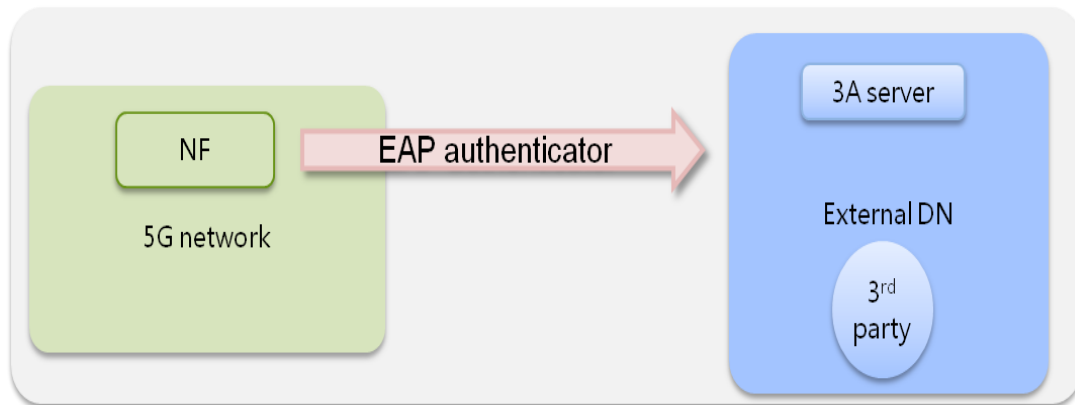


Figure 6.2-1. Exposure of authenticator in passive exposure scenario

- In semi-active exposure scenario, in addition to being exposed for the access authentication for external data network, the MNO authenticator is also exposed to be configured on whether the UE uses secondary authentication for external data network. The 3<sup>rd</sup> party is not allowed to provide or install the authenticator (through API). See Figure 6.2-2.

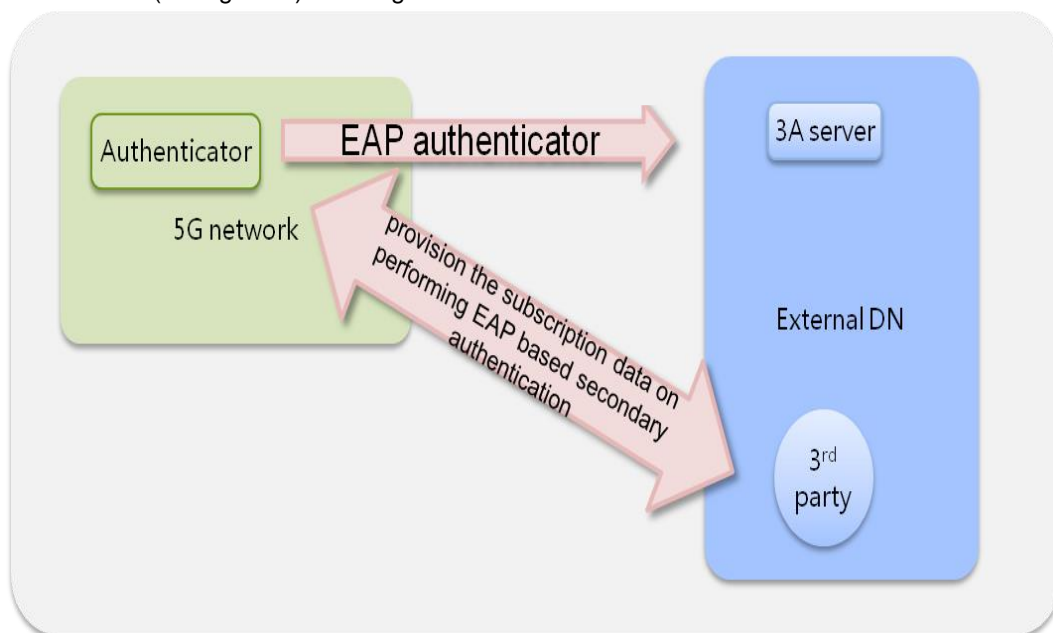


Figure 6.2-2. Exposure of authenticator in semi-active exposure scenario

- Fully-active exposure of the authenticator is allowed. For example, for a slice which is managed by the 3<sup>rd</sup> party, the authenticator in that slice can be provided or installed by the 3<sup>rd</sup> party through a dedicated SMF. See Figure 6.2-3.

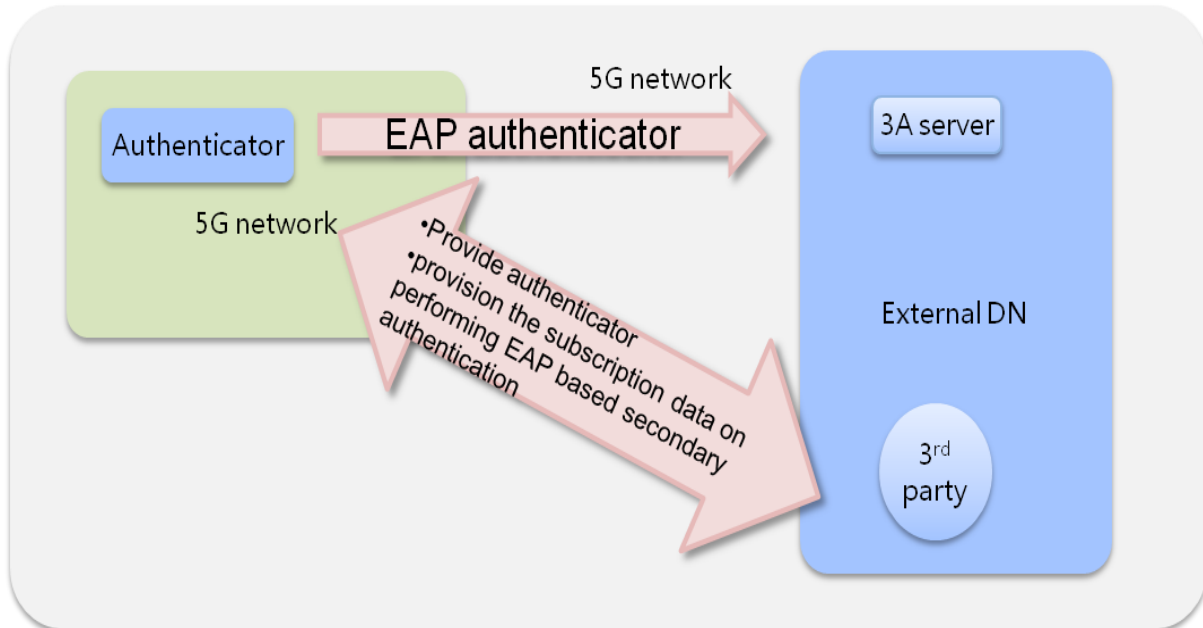


Figure 6.2-3. Exposure of authenticator in fully-active exposure scenario

### Typical use cases:

An external DN out of 5G network wishes to make sure that only those UEs which are identifiable according to its own AAA server can establish PDU sessions with that DN. Such DN may be an intranet of a global company, an industrial network, etc. 5G network can provide optional-to-use secondary authentication between UE and an external data network (DN) for their communication via the 5G network.

### Benefits:

The operator can provide access control for external network before PDU session establishment. This can reduce the security risk and burden of the server in external data network. The DN can update UEs' identifiers by operating its own AAA server which is more flexible for DN.

Exposure of slice authenticator can meet vertical industry's requirement of additional authentication.

## 6.3 Exposure of Derived Keys

4G network provides key agreement mechanisms in order to generate various shared symmetric keys between UE and the network, which can be used for a secure communication between them. GBA described in TS 33.220 [19] is an example. Analogous mechanisms and interfaces are also expected for 5G network. This can be achieved through the key derivation function by using UE subscription credentials and specified public parameters, where the shared key is computed as a function of the pre-shared secret key between UE and the network and the public input parameters. The MNO can derive keys that can be exposed to the 3<sup>rd</sup> party service platform, including its application servers. After successful exposure of the new derived keys to the service platform, the 3<sup>rd</sup> party can additionally derive new keys from additional input parameters (e.g., identifiers of the UEs on the platform), by using another or the same key derivation algorithm. On the UE side, the same new keys are generated by using the same key derivation algorithm applied to the pre-shared key and the same input parameters. Thus the UE and the application servers share the same keys, which can then be used for various security functions in the service provided, including data integrity protection, data confidentiality protection and authentication.

**Scenarios evaluation:**

- In passive exposure scenario, keys derived by the network key derivation function can be exposed to 3<sup>rd</sup> party service platform through API. The 3<sup>rd</sup> party is not allowed to provide, install, manage or configure key agreement related entities (through API). See Figure 6.3-1.

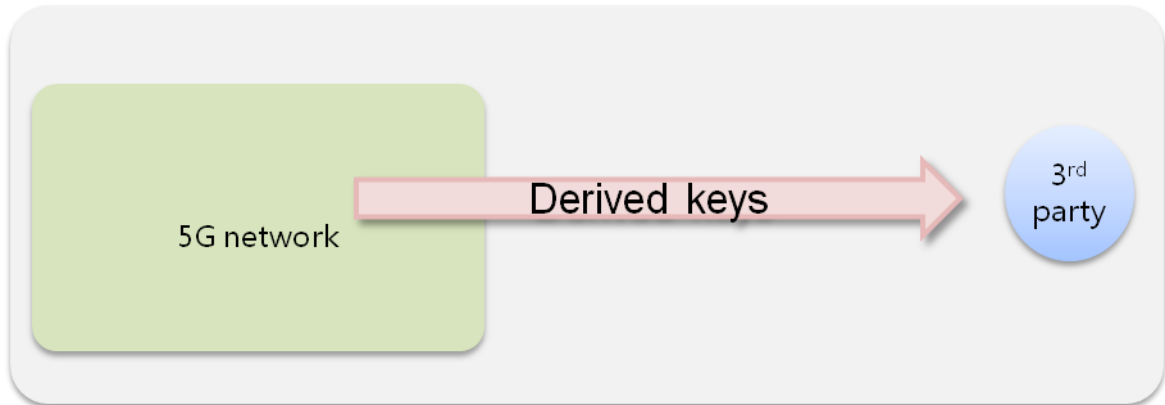


Figure 6.3-1. Exposure of derived keys in passive exposure scenario

- In semi-active exposure scenario, keys derived by the network key derivation function can be exposed to 3<sup>rd</sup> party service platform through API. The 3<sup>rd</sup> party can also configure some parameters of the key derivation function through API, not input parameters which are defined in input, but the key length and the algorithm. The 3<sup>rd</sup> party is not allowed to provide or install key agreement related entities (through API). Since the UE may negotiate with the network the key derivation parameters, it need not be exposed to being configured by the 3<sup>rd</sup> party. See Figure 6.3-2.

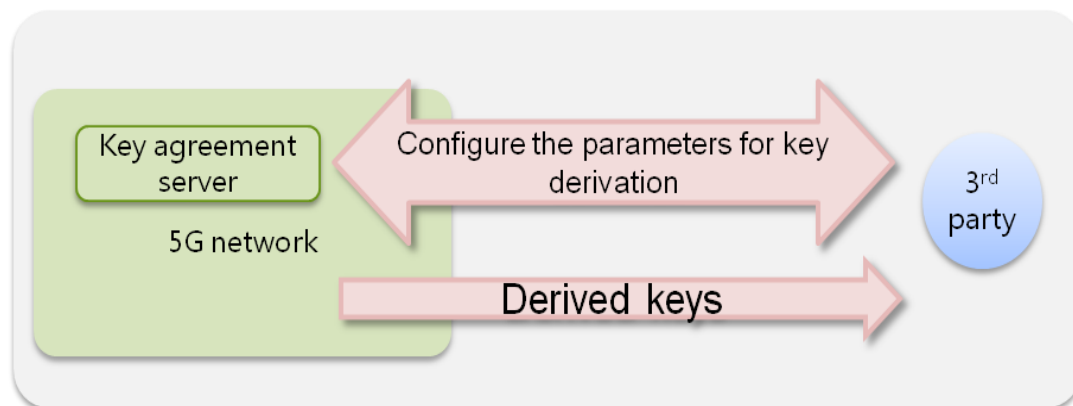


Figure 6.3-2. Exposure of derived keys in semi-active exposure scenario

- Fully-active exposure of key derivation function is not allowed, since this function makes use of the secret keys from subscription credentials, which cannot be exposed to 3<sup>rd</sup> parties. However, the 3<sup>rd</sup> party can locally install a key derivation function that makes use of the exposed derived keys obtained from the operator in the passive or semi-active exposure scenarios in order to use them on its service platform.

**Typical use cases:**

mIoT is an important scenario in 5G. When IoT devices access the IoT service platform, there may be a need for protocols such as TLS/DTLS to protect E2E communication between IoT devices and related application servers. In order to decrease the cost of computing and storage in the devices, pre-shared keys instead of public-key certificates are often adopted for establishing TLS/DTLS channels, and they are difficult to provision for massive

IoT devices. It is also difficult for the platform to manage and update the keys. Using the exposed key derivation function can make key distribution and management easier and more secure for the 3<sup>rd</sup> party platform, because it is securely based on already pre-provisioned pre-shared keys from the subscription credentials in UEs.

**Benefits:**

The capability of exposed key derivation function can help the application layer to easier distribute and manage application keys. UE and application servers do not need to store and use public-key certificates. This saves storage and computing resources and is suitable for resource-constrained UEs.

**6.4 Exposure of Slice Authentication**

Slicing is a very important feature of 5G network. For UE access to slices, UE shall be authenticated through primary authentication performed by MNO, which provides access to 5G network. When a vertical industry uses the resources of MNO network through a slice (e.g., ultra low latency), it may also be desired to additionally authenticate the UE or users via slice authentication. If the slice authentication is allowed, then the slice authentication method and user subscription can be configured and managed by the 3<sup>rd</sup> party. Even the slice authentication server can be provided by the 3<sup>rd</sup> party, for flexibility.

The network function performing this authentication can be called slice authentication server. Its level of exposure (1, 2 or 3) cannot be larger than the level of exposure of the slice (as a service) as a whole. For example, if the slice is only passively exposed to the 3<sup>rd</sup> party, then the same holds also for slice authentication.

**Scenarios evaluation:**

- Passive exposure scenario for slice authentication corresponds to passive exposure scenario for network authentication results, described in Section 6.1 or 6.2, where slice authentication results correspond to the result of primary or secondary authentication, respectively. See Figure 6.4-1.

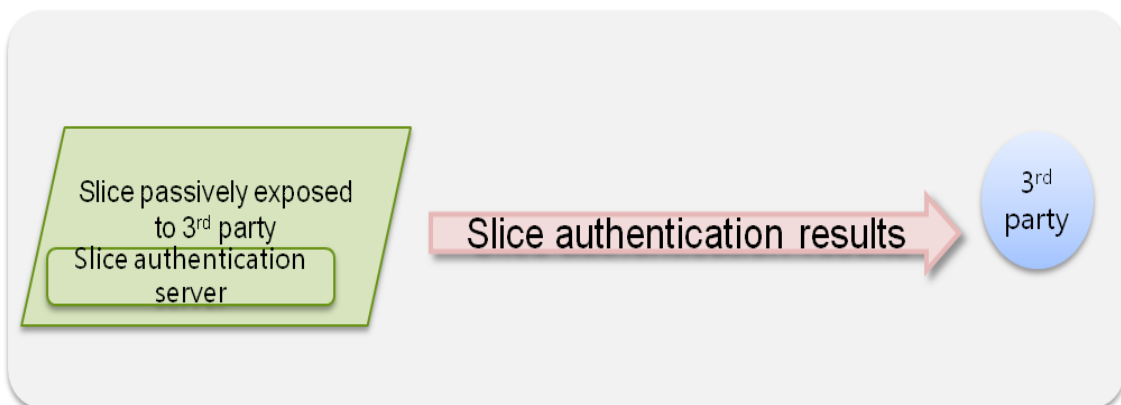


Figure 6.4-1. Exposure of slice authentication in passive exposure scenario

- In semi-active exposure scenario, the result of slice authentication is exposed to the 3<sup>rd</sup> party and the slice authentication server is exposed to be managed and configured through API (e.g., credentials, authentication method). The 3<sup>rd</sup> party is not allowed to provide or install the slice authentication related entities. See Figure 6.4-2.

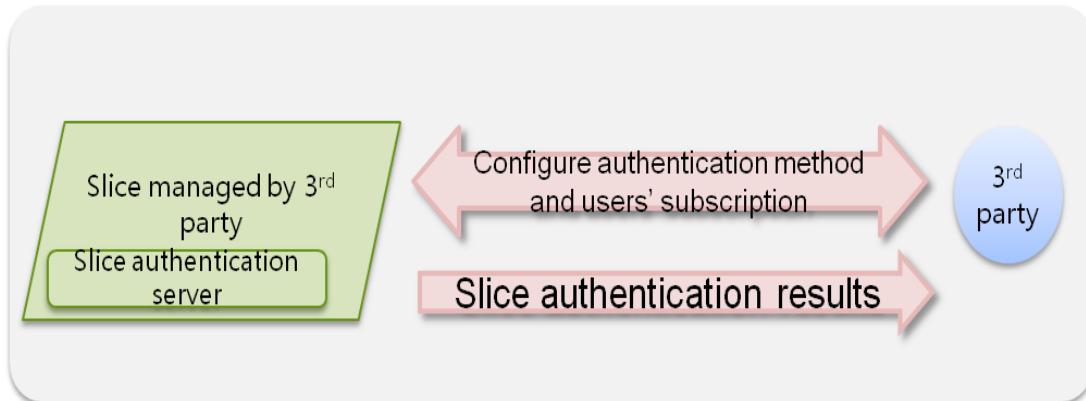


Figure 6.4-2. Exposure of slice authentication in semi-active exposure scenario

- In fully-active exposure scenario, the result of slice authentication is exposed to the 3<sup>rd</sup> party and the slice authentication server is allowed to be provided or installed by the 3<sup>rd</sup> party (through API) and also to be managed and configured through API. See Figure 6.4-3.

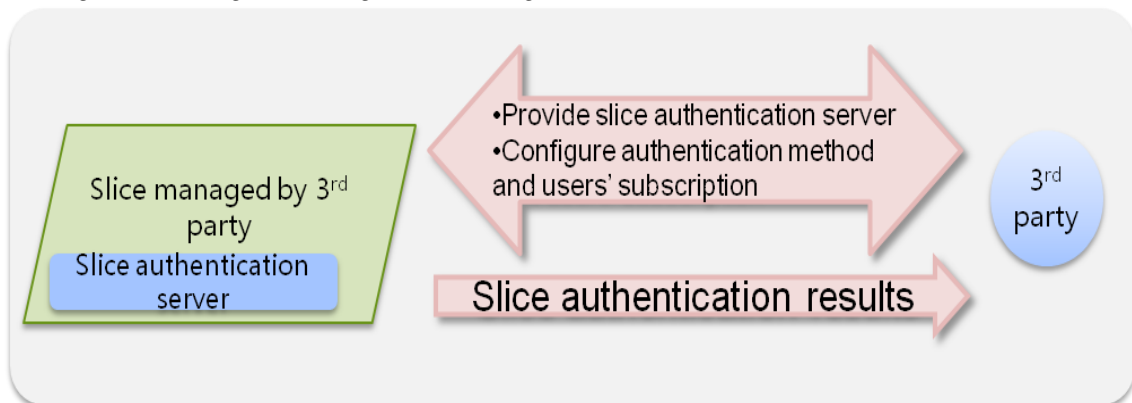


Figure 6.4-3. Exposure of slice authentication in fully-active exposure scenario

#### Illustrative use cases:

- *Access control on slice service or slice resource:* Some VR game enterprises provide VR game services to their own customers with a promise regarding a certain level of network communication services, which are bought from and provided by the MNO through network slices with specific QoS. The enterprises may need to pay for the usage of slice resource and number of active users in the data plane. The enterprise may not completely trust MNO's authentication or may have a higher degree of security requirement of authentication. So, it may wish to control the access to the specific slice services by itself in order to avoid uncontrolled access and ensure the promised QoS. Exposure of slice authentication allows the enterprises to have this ability by allowing the 3<sup>rd</sup> party to update the users' association with the slice or to perform the slice authentication. The association here refers to the subscription for the slice authentication, and not to the subscription credentials related to primary authentication, which is necessarily performed by MNO. It can also help MNO to allocate and adjust the resources in an economized way.
- *Authentication of Entity (User, Device and/or Application) associated with access subscription:* Slice authentication can support an entity authentication accompanying an access subscription authentication. There are two use cases of such authentication:
  - o Entity authentication accompanying a subscription authentication enables access to a specific slice service based on an authenticated identity of the specific entity that is authorized to access a specific slice service. For example, different entities may use the





same device to access different slice services or an entity may use different devices to gain access to the same service.

- Entity authentication can provide a second level of network access authorization based on an authenticated identity of the entity, for access to services provided by the slice.

#### **Benefits:**

As a supplement to network layer authentication, slice authentication can:

- allow the the 3<sup>rd</sup> party to be involved in slice management and, possibly, assistance in slice selection;
- control access to the specific slice service and then help MNO to allocate and adjust the resources in an economized way;
- provide access control before establishing PDU session which can reduce the security risks and burden of the application server;
- support authentication of user-centric identifiers in addition to the subscription based on MNO credential.

Exposure of slice authentication can meet vertical industry's requirement of authentication and allows new identifiers on UE. This can make update of access control more flexible and efficient.

The slice authentication feature may be of interest to 3<sup>rd</sup> party and may be requested by B2B/B2B2C marketing teams (to support service differentiation).

#### **Challenges:**

- additional complexity of managing the interaction of network, slice and application layers
- complexity of operation (e.g., troubleshooting, service management procedures, coordination between operator teams)
- completeness of device/UE management (e.g., a need to configure external DNN in UE, if this information is not available for S-NSSAI in UDM subscription)
- additional complexity for security (evolution of the threat models, incident response and mitigation, and other procedures from the security operation center perspective)
- complexity of responsibility separation between MNO and the 3<sup>rd</sup> party regarding the slice access control
- additional tests for interoperability of devices and network functions
- impact on the PDU session establishment delays (additional time)
- impact on devices (battery duration)
- lower efficiency for massive IoT: often only a few messages in a day; then network layer security and application layer security may be sufficient (i.e., the value added by slice authentication may not be significant).

## **6.5 Exposure of Slice Authorization**

It is recommended in [25] that after the necessary primary authentication, providing access to 5G network, UE should be authorized and/or authenticated to get access to each network slice.

Authorization capability can be exposed to the 3<sup>rd</sup> party to decide whether the customer can have access to the slice instance. It can be based on the primary or slice authentication (e.g., through authorization tokens). Authorization capability can be exposed as slice access control policy function.

#### **Scenarios evaluation:**

- In passive exposure scenario, slice authorization results can be exposed to the 3<sup>rd</sup> party through API. See Figure 6.5-1.

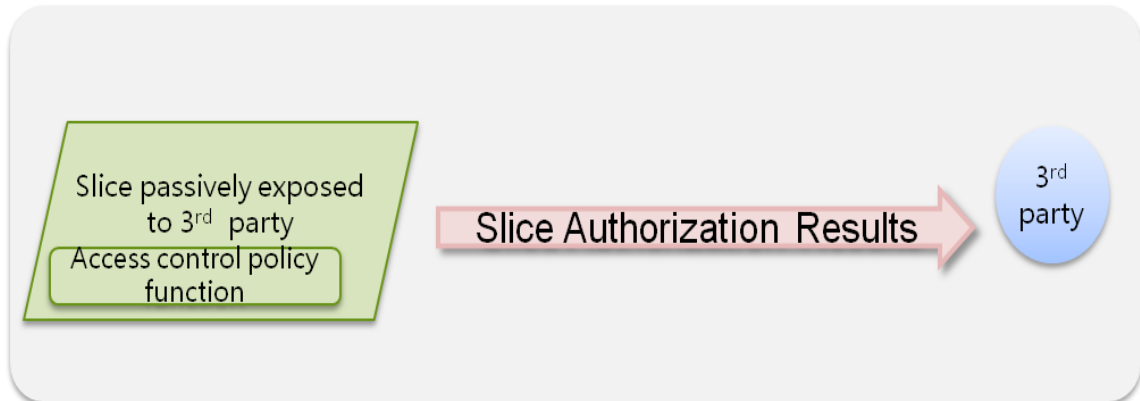


Figure 6.5-1. Exposure of slice authorization in passive exposure scenario

- In semi-active exposure scenario, the slice authorization access control policy function is exposed to the 3<sup>rd</sup> party and is exposed to be managed and configured through API (i.e., access control policy). The 3<sup>rd</sup> party is not allowed to provide or install the slice access control policy function entity. See Figure 6.5-2.

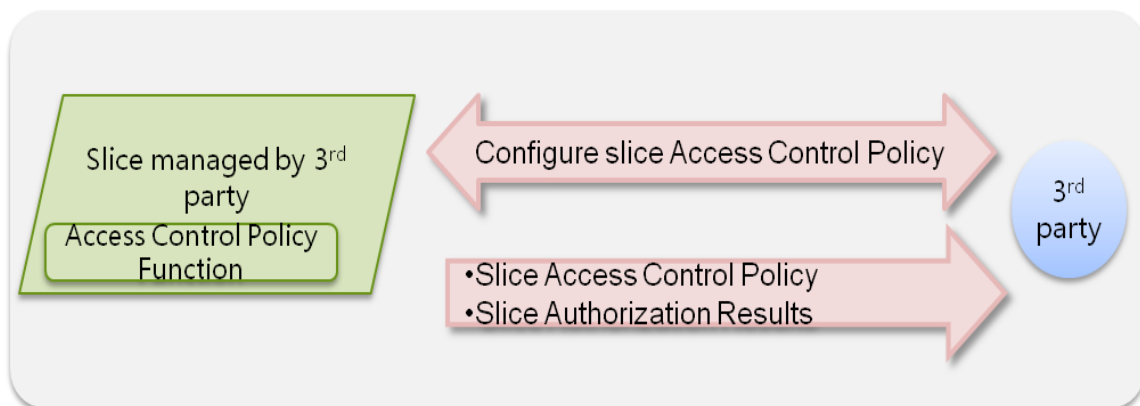


Figure 6.5-2. Exposure of slice authorization in semi-active exposure scenario

- In fully-active exposure scenario, the slice authorization access control policy function is allowed to be provided or installed by the 3<sup>rd</sup> party (e.g., through API) and also to be managed and configured through API. See Figure 6.5-3.

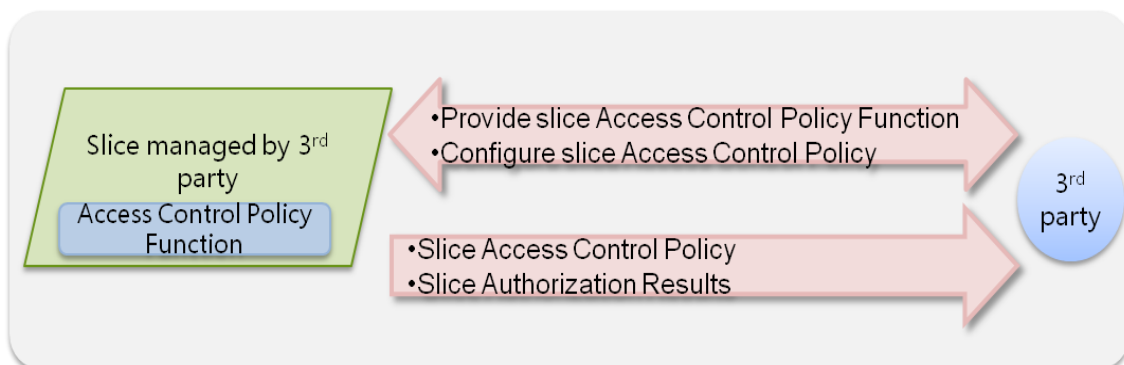


Figure 6.5-3. Exposure of slice authorization in fully-active exposure scenario

**Typical use cases:**

Assuming that 5G primary network authentication has already been performed, the 3<sup>rd</sup> party service provider who rents slices could specify which network slices a device is authorized to connect to. For example, in the case of Massive IoT, the devices may be part of a fleet, with a default network slice for Internet access, but with additional network slices for value-added services such as streaming media provided by a specific content provider.

**Benefits:**

Exposure of slice authorization can give the control of slice access to vertical industry and make update of access control policy more flexible and efficient.

**6.6 Exposure of Integrated Monitoring Security Functions**

Due to a high degree of softwarization of the 5G core network, monitoring security functions (e.g., anti-DoS, Firewall, IDS/IPS, all based on event or traffic monitoring) can be integrated in the virtualized network functions. To ensure that every single slice instance can meet the required security level, the 3<sup>rd</sup> party can be allowed to configure and use integrated monitoring security functions adapted to its needs.

**Scenarios evaluation:**

- In passive exposure scenario, MNO allows the 3<sup>rd</sup> party to have read-only access to exposable data such as performance results and security events (logs) of the integrated monitoring security functions provided by the MNO. See Figure 6.6-1.

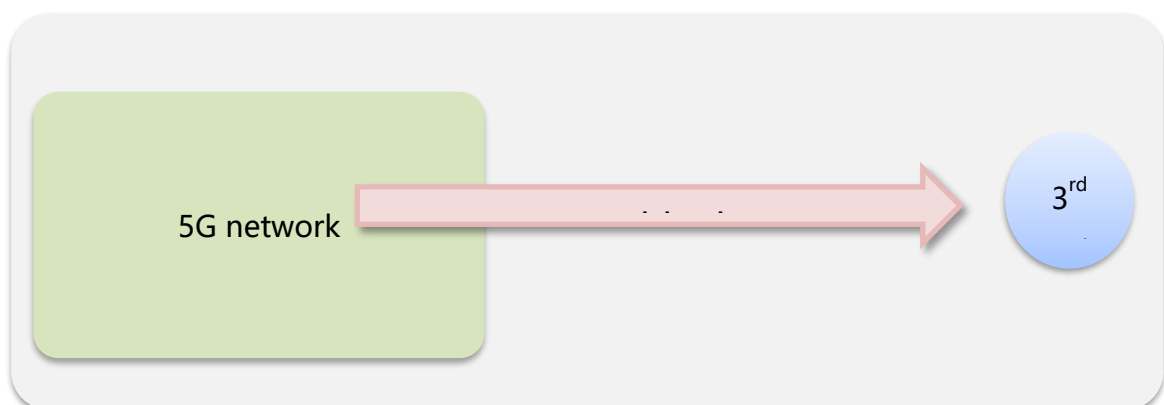


Figure 6.6-1. Exposure of integrated monitoring security functions in passive exposure scenario

- In semi-active exposure scenario, the 3<sup>rd</sup> party is also allowed to configure the integrated monitoring security functions (e.g., change filtering rules in a firewall), whose image is provided by the MNO. The 3<sup>rd</sup> party has read access to performance results and security events. See Figure 6.6-2.

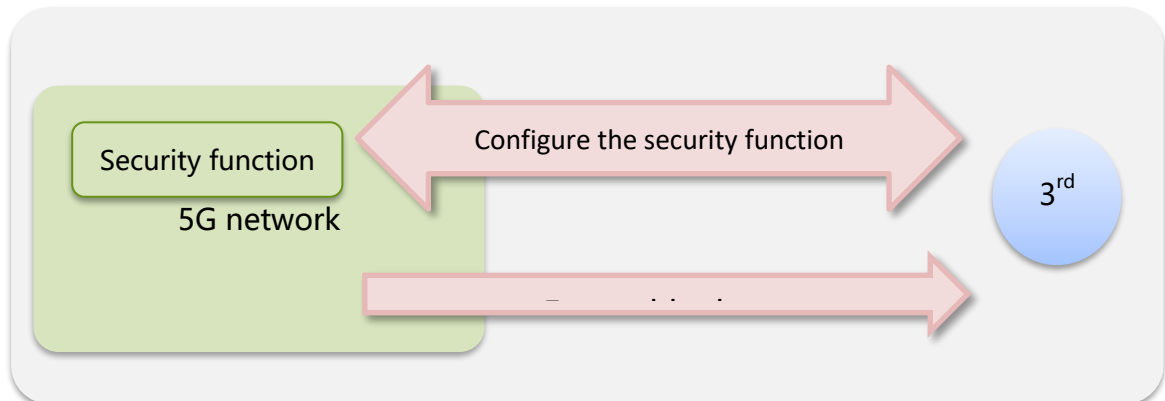


Figure 6.6-2. Exposure of integrated general security functions in semi-active exposure scenario

- In fully-active exposure scenario, MNO provides the hosting space, while the security function image is provided by the 3<sup>rd</sup> party. The MNO ensures the allocation of network paths through the security function and hosting integrity, while the 3<sup>rd</sup> party provides or installs the function and its configuration. The 3<sup>rd</sup> party has read access to performance results and security events. See Figure 6.6-3.

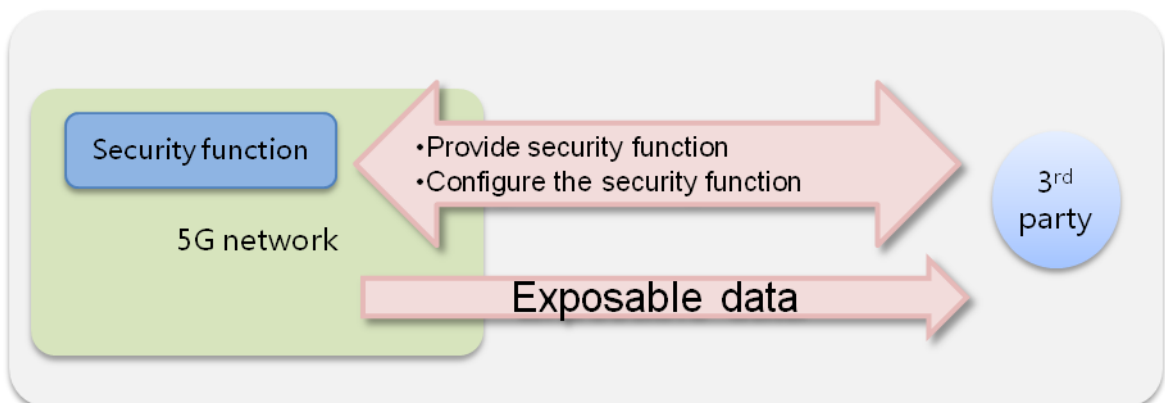


Figure 6.6-3. Exposure of integrated monitoring security functions in fully-active exposure scenario

### Typical use cases:

The exposure of integrated monitoring security functions allows for the service chaining of user plane traffic through various security functions. These services can be provided for the MNO and can also be provided as a service platform for a trusted 3<sup>rd</sup> party.

### Benefits:

The benefit is an increased ability to offer services with higher value and customized per slice, while separating and allocating the management, control and supply amongst MNO and MSP in order to maximize benefit for both. This also allows for the separation of duties between network infrastructure management (traditional MNO functions) and higher-level service management. These duties might be separated between companies (MNO and MSP) or even separated within an MNO, so that the traditional IT or security departments may control features, while the traditional mobility infrastructure ensures the availability of the 5G network.

## REFERENCES

- [1] 3GPP TS 22.261, Service requirements for the 5G system, Stage 1 (Release 15 Jul. 2018, Release 16 Jun. 2018)
- [2] 3GPP TS 23.501, System Architecture for the 5G System, Stage 2, V\_15.2.0 (Release 15 Jun. 2018)
- [3] 3GPP TS 23.502, Procedures for the 5G System, Stage 2, V\_15.2.0 (Release 15 Jun. 2018)
- [4] 3GPP TS 33.501, Security Architecture and Procedures for 5G System (Release 15 Jul. 2018)
- [5] 3GPP TR 23.722, Study on Common API Framework for 3GPP Northbound APIs V\_15.1.0 (Release 15 Mar. 2018)
- [6] 3GPP TS 29.116, Representational state transfer over xMB reference point between Content Provider and BM-SC V\_15.0.0 (Release 15 Jun. 2018)
- [7] NGMN 5G WHITE PAPER V 1.0 (Feb. 2015)
- [8] 3GPP TR 28.801, Study on management and orchestration of network slicing for next generation network V\_15.1.0 (Release 15 Jan. 2018)
- [9] 3GPP TR 33.899, Study on the security aspects of the next generation system V\_1.3.0 (Release 14 Aug. 2018)
- [10] 3GPP TR 33.811, Study on security aspects of 5G network slicing management V\_15.0.0 (Release 15 Jul. 2018)
- [11] Recommendation ITU-T X.1256: Guidelines and framework for sharing network authentication results with service applications (Mar. 2016)
- [12] 3GPP TR 22.830, Feasibility Study on Business Role Models for Network Slicing V\_1.0.0 (Release 16 May 2018)
- [13] 3GPP TS 23.222, Common API Framework for 3GPP Northbound APIs (Release 15 Jun. 2018, Release 16 Jun. 2018)
- [14] 3GPP TS 28.530, Management of network slicing in mobile networks; Concepts, use cases and requirements V\_1.2.0 (Release 15 Jul. 2018)
- [15] 3GPP TS 28.531, Provisioning of network slicing for 5G networks and services V\_1.2.0 (Release 15 Jul. 2018)
- [16] 3GPP TR 32.866, Telecommunication management; Study on a RESTful HTTP-based Solution Set (SS) V\_15.0.0 (Release 15 Jan. 2018)
- [16] 3GPP TR 22.904, Study on user centric identifiers and authentication V 16.0.0 (Release 16 Jun. 2018)
- [17] 3GPP TR 28.802, Telecommunication management; Study on management aspects of next generation network architecture and features V\_15.0.0 (Release 15 Jan. 2018)
- [18] 3GPP TR 32.899, Telecommunication management; Charging management; Study on charging aspects of 5G system architecture Phase 1 V\_15.1.0 (Release 15 Mar. 2018)
- [19] 3GPP TS 33.220, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) V\_15.2.0 (Release 15 Jun. 2018)
- [20] oneM2M TS 0026 3GPP, Interworking V 0.8.1 (Apr. 2018)
- [21] ETSI GS MEC 012 V 1.1.1, Mobile Edge Computing (MEC); Radio Network Information (Jul. 2017)
- [22] ETSI GS MEC 013 V 1.1.1, Mobile Edge Computing (MEC); Location API (Jul. 2017)
- [23] ETSI GS MEC 014 V 1.1.1, Mobile Edge Computing (MEC); UE Identity API (Feb. 2018)
- [24] ETSI GS MEC 015 V 1.1.1, Mobile Edge Computing (MEC); Bandwidth Management API (Oct. 2017)
- [25] NGMN White Paper, 5G End-to-End Architecture Framework V 2.0 (Feb. 2018)
- [26] RFC 3748, EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) KEY MANAGEMENT FRAMEWORK (Jun. 2004)
- [27] 3GPP TR 23.740, Study on Enhancement of Network Slicing V 0.4.0 (Release 16 Jun. 2018)
- [28] 3GPP SA3-182077, TR 33.cde V 0.1.0, Study on authentication and key management for applications; based on 3GPP credential in 5G (Release 16, May 2018)
- [29] 3GPP TS 33.163 Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST) V\_15.3.0 (Release 15 Mar. 2018)
- [30] 3GPP TS 33.995, Study on security aspects of integration of Single Sign-On (SSO) frameworks with 3GPP operator-controlled resources and mechanisms V\_15.0.0 (Release 15 Jun. 2018)
- [31] ETSI GS MEC 003 V 1.1.1, Mobile Edge Computing (MEC); Framework and Reference Architecture (Mar. 2016)

- [32] ETSI GS MEC 010-1 V 1.1.1, Mobile Edge Computing (MEC); Mobile Edge Management; Part 1: System host and platform management” (Oct. 2017)
- [33] ETSI GS MEC 010-2 V 1.1.1, Mobile Edge Computing (MEC); Mobile Edge Management; Part 2: Application lifecycle, rules and requirements management” (Jul. 2017)
- [34] ETSI GS MEC 011 V 1.1.1, Mobile Edge Computing (MEC); Mobile Edge Platform Application Enablement (Jul. 2017)
- [35] 3GPP TS 28.543, Management and orchestration of networks and network slicing; 5G Core Network (5GC) Network Resource Model (NRM), Stage 2 and Stage 3, V\_1.0.0 (Release 15 Jun.2018)
- [36] GSMA Network Slicing Use case requirements (Apr. 2018)
- [37] GTI 5G Network Slicing White Paper V 1.0, (Feb. 2018)
- [38] 3GPP TS 22.101, Service aspects; Service principles V\_15.5.0 (Release 15 Jun. 2018)

## ABBREVIATIONS

5G	The fifth Generation
5GC	5G Core network
5GS	5G System
AAA	Authentication Authorization and Accounting
API	Application Program Interface
AR	Advanced Reality
B2B	Business to Business
B2B2C	Business to Business to Customer
B2C	Business to Customer
CN	Core Network
CP	Control Plane
DDoS	Disitributed Denial of Service
DN	Data Network
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
E2E	End to End
FIDO	Fast IDentity Online
GBA	Generic Bootstrapping Architecture
GPSI	Generic Public Subscription Identifier
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer

IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
ITU-T	International Telecommunication Union - Telecommunication standardization sector
KYC	Know Your Customer
LADN	Local Access Data Network
MEC	Multi-access Edge Computing (from ETSI nomenclature)/Mobile Edge Computing (from NGMN nomenclature)
MNO	Mobile Network Operator
MSP	Mobile Service Provider
MVNO	Mobile Virtual Network Operator
NAS	Non-Access Stratum
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualization
NS	Network Service
NSI	Network Slice Instance
NSP	Network Service Provider
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
PDU	Protocol Data Unit
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RESTful	REpresentational State Transfer architectural constrains
S-NSSAI	Single Network Slice Selection Assistance Information
SBA	Service Based Architecture
SCEF	Service Capability Exposure Function
SD	Slice Differentiator

SDO	Standards Developing Organization
SI	Service Instance
SMF	Session Management Function
SMS	Short Message Service
SP	Service Provider
SST	Slice/Service Type
TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
VM	Virtual Machine
VR	Virtual Reality
WLAN	Wireless Local Access Network



## APPENDIX A: OVERVIEW OF PRIOR/ONGOING WORK

### A.1 3GPP SA1

According to 3GPP SA1, network capability exposure provides access to the network capabilities that are in need by 3<sup>rd</sup> party ISP/ICP. With the advent of 5G, some new network capabilities need to be considered for exposure to 3<sup>rd</sup> parties, including [1]:

- **Network slicing capabilities:**
  - o allow a trusted 3<sup>rd</sup> party to create, modify, and delete network slices used for the 3<sup>rd</sup> party
  - o allow a trusted 3<sup>rd</sup> party to monitor the network slice used for the 3<sup>rd</sup> party
  - o allow a trusted 3<sup>rd</sup> party to define and update the set of services and capabilities supported in a network slice used for the 3<sup>rd</sup> party
  - o allow a trusted 3<sup>rd</sup> party to configure the information which associates a UE to a network slice used for the 3<sup>rd</sup> party
  - o allow a trusted 3<sup>rd</sup> party to configure the information which associates a service to a network slice used for the 3<sup>rd</sup> party
  - o allow a trusted 3<sup>rd</sup> party to assign a UE to a network slice used for the 3<sup>rd</sup> party, to move a UE from one network slice used for the 3<sup>rd</sup> party to another network slice used for the 3<sup>rd</sup> party, and to remove a UE from a network slice used for the 3<sup>rd</sup> party based on subscription, UE capabilities, and services provided by the network slice
  - o allow a trusted 3<sup>rd</sup> party to scale a network slice used for the 3<sup>rd</sup> party, i.e., to adapt its capacity.
- **Service Hosting capabilities:**
  - o allow a trusted 3<sup>rd</sup> party to manage this trusted 3<sup>rd</sup> party owned application(s) in the operator's Service Hosting Environment
  - o allow a 3<sup>rd</sup> party to monitor this trusted 3<sup>rd</sup> party owned application(s) in the operator's Service Hosting Environment
  - o allow one type of traffic (from trusted 3<sup>rd</sup> party owned applications in the operator's Service Hosting Environment) to/from a UE to be offloaded to a Service Hosting Environment close to the UE's location.
- **Other capabilities:**
  - o provide a mechanism to expose broadcasting capabilities to trusted 3<sup>rd</sup> party broadcasters' management systems
  - o allow a trusted 3<sup>rd</sup> party application to request appropriate QoE from the network.

In August 2017, a new study item was initiated to examine the business role models for 5G network slicing [12]. These models are roughly classified as monitor, limited control, enhanced control, and private slice. In essence, they stand for different levels of exposing network slicing capabilities. The trust relationship between UEs, MNOs and slice tenants, and corresponding security requirements will be a main topic of that SID.

TR 22.904 [16] aims at studying the introduction of an optional, entity-centric authentication layer on top of the existing subscription authentication, supporting various authentication mechanisms and interactions with external authentication systems as well as achieving a degree of confidence in the authentication. It gives some use cases including:

- providing different Entities (user, device and/or application) using the same UE with customized services
- identifying users of devices behind a gateway with a 3GPP subscription, but without the devices having a dedicated 3GPP subscription
- using an Entity Identifier that is linked to a subscription to access 3GPP services via non-3GPP access
- using an Entity Identifier for slice authorization.

### A.2 3GPP SA2

3GPP SA2 defines NEF (Network Exposure Function) and NEF-related parameters and information flows in 5G network to support exposure of network or service provider capabilities to 3<sup>rd</sup> party, such as Monitoring capability,

Provisioning capability, and Policy/Charging capability. Exposure of other capabilities may be considered later. 5G Core Network can also provide information to edge computing application function via NEF [2][3].

A study item TR 23.740 [27] on enhancement of Network Slicing study how to provide Network Slice Access authentication and authorization specific for the Network Slice Access authorization that uses User Identities and Credentials different from the 3GPP SUPI and that takes place after the primary authentication, which is still required between the UE and the 5GS for PLMN access authorization and authentication. In a word, it will study access control to Network Slices that require additional authorization and authentication including:

- how the UE and the Network know that additional authorization and authentication is required for a Network Slice
- how the additional authorization and authentication are triggered and performed, e.g., which procedures are used and when.

### A.3 3GPP SA3

In 3GPP SA3, there are some key issues in TS 33.501 [4] related to exposure of authentication capability. It is agreed that the authentication framework of 5G network shall support optional-to-use secondary authentication between the UE and an external data network (i.e., owned by a 3<sup>rd</sup> party). One of the identified goals of this authentication framework is to provide authentication services for UE access to a 3<sup>rd</sup> party service.

TR 33.811 [10] is performing a study on the threats, potential security requirements and solutions for the features of 5G network slicing management including the management exposure interface.

There are also discussions on network slices isolation, security and protection of network resources and communications in the context of exposure to 3<sup>rd</sup> party.

SA3 has also established a work item (i.e., CAPIF\_Sec) in order to specify the security and privacy aspects of the common API Framework for 3GPP Northbound APIs defined by SA6.

3GPP specified Generic Bootstrapping Architecture (GBA) [27] to leverage MNO-owned and controlled subscription credentials for performing user authentication and key agreement with application service providers that may be located outside of the MNO domain (e.g., 3<sup>rd</sup> parties). GBA has the provisions to perform the following functionality that may be re-used or enhanced in 5G:

- Functionality to authenticate the UE to the NAF (Application Service Provider) using MNO controlled, network level authentication credentials
- Functionality to perform Key Agreement between a UE and the NAF
- Functionality for conservation of Authentication Vectors (AV), i.e., for N requests for authentication between NAF and BSF, only M AVs (where  $M \leq N$ ) will be used
- Identity Privacy Functionality, which is aimed at protecting the MNO-controlled identities (i.e., IMSIs) from being known to 3<sup>rd</sup> Party NAFs.

3GPP TR 33.995 [30] presents the results of an investigation into the security aspects for service requirements specified by SA1 in TS 22.101 clause 26 [38], on the integration of SSO frameworks with 3GPP networks for various operator authentication configurations (e.g., configurations using GBA or not using GBA). The solutions from TR 33.995 position the MNO as an Identity Provider to:

- Provide Third parties (Application/Network Service Providers) to leverage a strong and seamless network authentication capability based on the UE subscription
- Provide a capability to complement GSMA MC and/or FIDO with a strong form of automated subscription authentication and binding to a user authentication
- Cater to scenarios where the UE subscription authentication may be carried out on one device and the user authentication on another consumption device.

SA3 has also established a study item (i.e., FS\_AKMA) on authentication and key management for applications based on 3GPP credential in 5G [28]. It analyzes issues and requirements for:

- providing authentication and key management procedures to applications and 3GPP services in 5G scenarios which allow the UE to securely exchange data with an application server
- decoupling these procedures from the the transport protocol, in order to allow for the adaption to differernt application layer protocols.

This item is to study the exposure of authentication and key management for applications and will take into account new solutions as well as potential adaptations to existing ones such as GBA described in TS 33.220 [19] and BEST described in TS 33.163 [29].

#### **A.4 3GPP SA5**

SA5 [8][14][15] [35] make recommendations on the management and orchestration of network slicing for the 5G network and define slice management exposure. Customers can request and get communication service related management data from CSMF (Communication Service Management Functions) .When communication service providers offer slice as a service to their customers, the management of a NSI can also be exposed to the customers with limit and authorization, including the slice characteristics (e.g., bandwidth, latency, QoS, security level), management data (e.g., performance data, fault data) and management operation capabilities. The NSMF (Network Slice Management Function) separates certain management functionalities in NSMF according to the network slice requirements as a set of exposed slice specific management functions and access is provided to the network slice customer through CSMF.

#### **A.5 3GPP SA6**

3GPP SA6 is studying the architecture aspects necessary for the development of a common API framework within 3GPP for northbound APIs, and corresponding architectural solutions [5][12]. The common API framework can be applied to both EPS and 5GS.

The aspects of the study include identifying architecture requirements for the common API framework aspects (e.g., registration, discovery, identity management) that are applicable to any functional APIs when used by northbound entities, as well as any interactions between the common framework aspects and the functional APIs themselves.

The study also specifies the security related requirements for API invokers accessing the service APIs, including:

- Service topology hiding
- Authentication and authorization for API invokers to access the service APIs
- API invoker authorization to access service APIs
- Access control for service API
- Secure communication between functions in CAPIF
- Secure communication between the CAPIF and the API invoker
- Authorization for service APIs from the 3<sup>rd</sup> party API providers
- Data confidentiality across API providers.

The study defines the entities which perform the security related functions, for example, the CAPIF core functions and the API exposing functions. Preliminary procedures corresponding to these requirements are included in this study but the detailed security process (e.g., authentication, authorization and communication protection) will be studied in SA3.

#### **A.6 3GPP CT3**

CT3 has a clear responsibility for definition of the Nnef service-based interface exhibited by NEF:

- all the northbound/external services exposed by the NEF will be specified by CT3
- all the 5G Core Network PCC related southbound interfaces corresponding to the EPC reference points (e.g., Rx, Nt, Nu) will be specified by CT3



- all the 5G Core Network southbound interfaces related to the corresponding EPC reference points under CT3 responsibility (e.g., Ns, MB2) will be specified by CT3
- all the 5G Core Network southbound interfaces related to the corresponding EPC reference points under CT4 responsibility (e.g., S6t, T6a/T6b) will be specified by CT4.

In 4G, 3GPP CT3 defines the REST-based protocol for the xMB reference point between the Content Provider and the BM-SC (Broadcast Multicast Service Center) in the TV services system [6]. Via this reference point, the Content Provider can configure services and sessions at the BM-SC and the BM-SC can send reports to the Content Provider upon request. If a 3<sup>rd</sup> party Content Provider can access BM-SC via the xMB reference point, this can be seen as a mechanism to expose broadcasting capabilities, just like SA1 has requested. So it is possible that 5G will inherit this feature.

### **A.7 NGMN 5G white paper**

NGMN 5G white paper [7] mentions that 5G has the ability to offer to and operate for a 3<sup>rd</sup> party provider different network infrastructure capabilities (Infrastructure, Platform, Network) as a Service. It also mentions that in Partner Service Provider and XaaS Asset Provider model, 5G should provide an abstraction layer as an interface, where all types of in-networking functionality can be exposed to the application layer functions and/or service providers based on a service level agreement (also referred by E2E architecture framework white paper [25]). In this way, service providers can be able to configure and manage the service, while operators will have freedom to manage and evolve the network.

### **A.8 NGMN 5G E2E architecture framework**

This document is to provide a high-level 5G E2E architecture framework. It mentions that the application/service provider will be able to use a sub-set of the network capabilities in a flexible, configurable and programmable manner, and to use network resources depending on their service preference through an abstraction layer as an interface.

### **A.9 OneM2M**

OneM2M is making a specification named 3GPP interworking [20]. This document is to specify interworking between oneM2M service layer and 3GPP network, so that relevant 3GPP features defined by Cellular IoT can be used by oneM2M service layer for the benefit of IoT applications. It gives the architecture for 3GPP Clot interworking with oneM2M through MTC Interworking Function (MTC-IWF) and/or the Service Capability Exposure Function (SCEF). It also specifies the signalling flows and resources of the Clot network features exposed to service layer. The features exposed to oneM2M service include Cellular IoT non-IP data deliver, monitoring events, 3GPP based device triggering, configuration of traffic patterns, background data transfer and so on. This specification just revolves around 3GPP Clot features defined in Rel14, Rel13, Rel12 and Rel11. 5G Clot network can also provide Clot features to and interwork with oneM2M service layer. oneM2M is considering the issue of interworking with 5G for NEF and CAPIF.

### **A.10 ETSI MEC**

ETSI defines a series of specification on Multi-Access Edge Computing (MEC). With MEC, the edge network can be opened for authorized operators / 3<sup>rd</sup> party. MEC applications include internal applications or authorized operator (roaming-in) / 3<sup>rd</sup> party provided applications. A functional element named customer facing service portal allows operators' third-party customers (e.g., commercial enterprises) to select and order a set of mobile edge applications that meet their particular needs, and to receive back service level information from the provisioned applications.

ETSI also defines the following mobile edge services which are provided to mobile edge applications, that is:

- Radio Network Information [21]
- Location [22]
- UE Identity [23]
- Bandwidth Management Service [24].



MEC is an important feature of 5G network. The edge network can be exposed to 3<sup>rd</sup> party.

### **A.11 FIDO Alliance**

The Fast Identity Online (FIDO) Alliance paved the path for industry to migrate beyond passwords to stronger forms of user authentication <https://fidoalliance.org/>. They introduced capabilities to perform password-less single/multifactor user authentication using a variety of factors including biometric (e.g., fingerprints, facial recognition, and retina scans). Central to the FIDO specifications is the ability to perform a user authentication locally on a user device by way of FIDO Authenticators. Service providers may have access to detailed information relating to the FIDO authenticators and their security characteristics, through a FIDO certification service and a FIDO metadata discovery service. Collectively this enables risk based user authentication catering to a variety of services from simple frictionless access to online shopping sites through to secure banking transactions.

FIDO helps position the MNO as an Identity Provider to:

- Provide Third parties (Application/Network Service Providers) capabilities to leverage user authentication capabilities available on a user device
- Gain consent or transaction confirmation from a user
- Perform multi-factor user authentication using methods of authenticator capabilities discovery and user authentication.

### **A.12 GSMA**

GSMA introduced Mobile Connect (GSMA MC) which positions MNOs as Identity Providers and at the center of a universal user authentication capability with the user's mobile phone as an authenticator for access to web services and Third parties by simply using their mobile phone. GSMA MC positions the MNO as an Identity Provider to:

- o Provide Third parties (Application/Network Service Providers) access to a strong and universal network authentication capability based on a UE subscription and without a need to maintain a separate set of UE authentication credentials by the Third parties
- o Perform a Level of Assurance (LoA) and risk based combined subscription authentication and user authentication.
- o Gain consent or transaction confirmation from a user
- o Provide Third parties access to user-consent based user attribute(s) such as user personal data and location in accordance with Know Your Customer (KYC) and privacy related local regulations
- o Preserve user identifier privacy (e.g. user's MSISDN) and expose this only to trusted Third parties in accordance with KYC and privacy related local regulations.

GSMA also published Network Slicing Use case requirements in Apr. 2018 [36].