|  |
| --- |
| 3GPP TR 33.757 V0.2.0 (2024-04) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security for PLMN hosting a NPN(Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 9

3.3 Abbreviations 9

4 Overview 9

5 Security assumptions 11

6 Key issues 11

6.1 Key Issue #1: Security for dedicated UPF interacting with PLMN through N4 interface 11

6.1.1 Key issue details 11

6.1.2 Security threats 11

6.1.3 Potential security requirements 11

6.2 Key Issue #2: Dedicated NFs interacting with PLMN through SBA interface 12

6.2.1 Key issue details 12

6.2.2 Security threats 12

6.2.3 Potential security requirements 12

6.3 Key issue #3: SUPI privacy issue in PLMN hosting NPN scenario 13

6.3.1 Key issue details 13

6.3.2 Security Threats 13

6.3.3 Potential security requirements 13

6.X Key Issue #X: <Key Issue Name> 14

6.X.1 Key issue details 14

6.X.2 Security threats 14

6.X.3 Potential security requirements 14

7 Solutions 14

7.1 Solution #1: Secure N4 interface with Security Gateway 14

7.1.1 Introduction 14

7.1.2 Solution details 14

7.1.2.1 Topology information hiding 15

7.1.2.2 Signaling inspection and message filtration 15

7.1.2.3 Security between the dedicated UPF and the Security Gateway 15

7.1.2.3.1 Authentication 16

7.1.2.3.2 Transport protection between the dedicated UPF and the Security Gateway 16

7.1.2.4 Access control 16

7.1.3 Evaluation 16

7.2 Solution #2: CIWF for N4 interface 16

7.2.1 Introduction 16

7.2.2 Solution details 16

7.2.2.1 General 16

7.2.2.2 Procedure 17

7.2.3 Evaluation 18

7.3 Solution #3: A perimeter security gateway for N4 and SBI interface. 18

7.3.1 Introduction 18

7.3.2 Solution details 18

7.3.3 Evaluation 19

7.4 Solution #4: Security protection to avoid UE information disclosure 19

7.4.1 Introduction 19

7.4.2 Solution details 20

7.4.3 Evaluation 21

7.5 Solution #5: Secure SBA interface with Security Gateway 21

7.5.1 Introduction 21

7.5.2 Solution details 21

7.5.2.1 Topology information hiding 22

7.5.2.2 Signaling inspection and message filtration 22

7.5.2.3 Security between the NF in customer premise and the Security Gateway 23

7.5.2.3.1 Authentication 23

7.5.2.3.2 Authorization 23

7.5.2.3.3 Transport protection between the Security Gateway and the NF in PLMN 23

7.5.2.4 Security between the Security Gateway and the NF in PLMN 23

7.5.2.5 Access control 23

7.5.3 Evaluation 23

7.6 Solution #6: CIWF as a gateway for SBA interface 23

7.6.1 Introduction 23

7.6.2 Solution details 24

7.6.2.1 General 24

7.6.2.2 Procedure 24

7.6.3 Evaluation 26

7.7 Solution #7: CIWF as a delegate for SBA interface 26

7.7.1 Introduction 26

7.7.2 Solution details 26

7.7.2.1 General 26

7.7.2.2 Procedure 27

7.7.3 Evaluation 28

7.8 Solution #8: NRF based service and information exchange restriction 28

7.8.1 Introduction 28

7.8.2 Solution details 28

7.8.2.1 NF Service Producer registration with NRF 28

7.8.2.2 NF Service Consumer obtaining access token 28

7.8.2.3 NF Service Consumer requesting service access with an access token 30

7.8.3 Evaluation 30

7.9 Solution #9: DNS Security in PLMN hosting NPN scenario 31

7.9.1 Introduction 31

7.9.2 Solution details 31

7.9.3 Evaluation 31

7.10 Solution #10: SCP based topology hiding 31

7.10.1 Introduction 31

7.10.2 Solution details 32

7.10.3 Evaluation 33

7.11 Solution #11: SUPI privacy protection in hosted NPN 33

7.11.1 Introduction 33

7.11.2 Solution details 33

7.11.3 Evaluation 34

7.12 Solution #12: Secure sensitive data with secure environment 34

7.12.1 Introduction 34

7.12.2 Solution details 34

7.12.3 Evaluation 35

7.Y Solution #Y: <Solution Name> 35

7.Y.1 Introduction 35

7.Y.2 Solution details 35

7.Y.3 Evaluation 35

8 Conclusions 35

Annex <X> (informative): Change history 36

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the security when a PLMN hosts an NPN with dedicated NFs deployed in the customer domain. A NPN customer may deploy on-premises NFs, or hosted NFs which reside in thrid-party premises, or both. A PLMN hosting an NPN is an example of a Public Network Integrated NPN (PNI-NPN). The term PNI-NPN applies to this study of a PLMN hosting an NPN.

More specifically, this document:

- identifies key issues and potential security requirements for the scenarios of PLMN hosting an NPN with dedicated NFs deployed in the customer domain. Related dedicated NFs may be described in the key issues.

- when necessary, develops solutions to address the identified requirements.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for the 5G system;Stage 1".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[4] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[5] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes"

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)"

[7] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)"

[8] 3GPP TS 23.273: " 5G System (5GS) Location Services (LCS); Stage 2"

[9] 3GPP TS 23.501: " System architecture for the 5G System (5GS); Stage 2"

[10] 3GPP TS 29.500: "Technical Realization of Service Based Architecture"

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**PNI-NPN Operational domain:** a network located within a premise (e.g. a residence, office or shop), which is owned, installed and/or (at least partially) configured by the customer of a public network operator as defined in TS 22.261[2] . Dedicated network entities of NPN that can be deployed in NPN operator premises that are outside the control of the PLMN operator.

**PLMN Operational domain:** Network entities of NPN that can be deployed in PLMN operator premises that are under the control of the PLMN operator.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

NSI Network Slice Instance

PNI-NPN Public Network Integrated NPN

# 4 Overview

NPN can be hosted by a PLMN. NPN customers can request dedicated NFs to be deployed in the customer premises for performance and privacy reasons.

The focus of the study is divided into two parts:

- Provide security to the PLMN from the attacks that may be initiated by the PNI-NPN.

- Provide security to PNI-NPN functions from attacks that may be initiated by the PLMN.

Public Network Integrated NPNs are NPNs made available via PLMNs e.g. by means of dedicated DNNs, or by one (or more) Network Slice instances allocated for the NPN. Therefore, NFs which may reside within PNI-NPN Network Slice instances may require interfaces which cross the operational domains between PNI-NPNs and PLMNs. In addtion, AFs which reside within a PNI-NPN DNNs operational domain may require interfaces which cross the operational domains between PNI-NPNs and PLMNs.

The creation, modification, and termination of a Network Slice Instance (NSI) are supported by Management Services provided by the 5G management systems. Therefore, NFs which provide NSI Management Services may cross the operational domains between PNI-NPNs and PLMNs. The security of management interface is not in the scope of this study.

NFs which reside in the PNI-NPN operational domain may require interfaces which cross the trust boundary between PNI-NPN and PLMN. Therefore, these interfaces require security controls to mutually protect the NFs which reside in the PLMN operational domain and in the PNI-NPN operational domain.

Figure 4-1 and Figure 4-2 demonstrate two example PNI-NPNs with dedicated NFs deployed in the the customer premises.



Figure 4-1 PNI-NPN with dedicated UPF deployed in the customer premises

For scenario 1, as depicted in Figure4-1, dedicated UPF is deployed in the customer premises, the other NFs are deployed in the operator premises. The interface between the dedicated UPF in the customer premises and NFs in the operator premises is N4.



Figure 4-2 PNI-NPN with dedicated UPF and part of CP functions deployed in the customer premises

For scenario 2, as depicted in Figure 4-2, dedicated UPF and part of CP functions are deployed in the customer premises. The interface between the dedicated NFs in the customer premises and the NFs in the operator premises is SBA interface. Examples of dedicated CP functions that are likely to be hosted by NPN in the customer premises are as below:

- AMF.

- SMF.

SA1 has captured the scenarios and added requirements in clause 8.2 of TS 22.261[2], which is:

*“The 5G system shall enable a PLMN to host an NPN without compromising the security of that PLMN.*

*NOTE: Dedicated network entities of NPN can be deployed in customer premises that are outside the control of the PLMN operator.”*

# 5 Security assumptions

To meet the requirement stated in TS 22.261[2] that the 5G system shall enable a PLMN to host an NPN without compromising the security of that PLMN or NPN, this document is based on the following assumptions:

- This document assumes that mutual trust between PLMN and the dedicated Network functions at the PNI\_NPN is not in place.

- This document assumes that attacks happen from NPN to PLMN and PLMN to NPN.

# 6 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 6.1 Key Issue #1: Security for dedicated UPF interacting with PLMN through N4 interface

### 6.1.1 Key issue details

In the scenario where the dedicated UPFs are deployed in NPN customer premise, the compromised UPF might launch signaling attacks towards the SMF in PLMN 5GC network.

If the dedicated UPF is compromised, attackers may utilize compromised dedicated UPF to collect PLMN’s topology, send malformed messages or launch DoS attacks to PLMN etc.

For this scenario, NDS/IP shall be supported to ensure confidentiality, integrity and replay protection as described in clause 9.9 in TS 33.501[3].

However, existing NDS/IP cannot protect PLMN or NPN from attacks from a compromised dedicated UPF or SMF, such as DoS, malformed signaling messages, topology information exposure etc.

### 6.1.2 Security threats

If a dedicated UPF in customer premises, is compromised by an attacker, the following problems may occur:

- The attacker may collect topology information from the PLMN or NPN and use the information to direct further attacks at the PLMN or NPN.

- The attacker may send malformed signaling messages to NFs in operator premises or customer premises to degrade NFs’ ability to process normal signaling messages.

- The attacker may send messages to the NFs in the operator premises or customer premises with wrong NF types according to 3GPP specifications. For example, a comprised dedicated UPF may send messages to the SMF in the operator premises to discover vulnerabilities of the SMF.

- The attacker may launch DoS attacks to flood and disrupt the PLMN or NPN.

### 6.1.3 Potential security requirements

5GS shall support mutual topology information hiding of the PLMN and the NPN customer premises network.

5GS shall support the means to block malformed signaling messages sent from dedicated UPF in the customer premises and compromised SMF in the operator premises.

5GS shall support the means to block messages with wrong NF types sent from dedicated UPF in the customer premises or SMF in the operator premises according to 3GPP specifications.

Editor’s Note: Whether the 5GS should support mitigation of DoS by compromised NF are FFS.

5GS shall support the means to authenticate and authorize the dedicated NFs in the customer premises and operator premises.

## 6.2 Key Issue #2: Dedicated NFs interacting with PLMN through SBA interface

### 6.2.1 Key issue details

When dedicated UPF and part of CP functions are deployed in the customer premises, the interface between the dedicated NFs in the customer premises and NFs in the operator premises is SBA interface.

If NFs are compromised, attackers may utilize compromised NFs to collect topology, send malformed messages or launch DoS attacks.

For this scenario, SBA security shall be supported to ensure confidentiality, integrity and replay protection as described in clause 13 in TS 33.501[3].

However, existing SBA security cannot protect PLMN nor NPN from attacks from a compromised NFs, such as DoS, malformed signaling messages, topology information exposure etc. via the intersection between the MNO and customer domain.

### 6.2.2 Security threats

If a NF is compromised by an attacker, the following problems may occur:

- The attacker may collect topology information of the PLMN or NPN and use the information to direct further attacks at the PLMN or NPN.

- The attacker may send malformed signaling messages to NFs to degrade NFs’ ability to process normal signaling messages.

- The attacker may send messages to the NFs in the opposite domain with wrong NF types according to 3GPP specifications.

- The attacker may launch DoS attacks to flood and disrupt the availability of NFs in the operator domain and vice versa.

- The attacker may initiate unauthorized service operations. Safeguarding access tokens from an attacker is challenging when it crosses the security/trust boundary between the operator premises and the customer premises.

- A compromised NF in the customer premises may request the NF(s) in a PLMN to consume a service that are not allowed in the customer premises, and vice versa.

### 6.2.3 Potential security requirements

5GS should support mutual topology information hiding of the PLMN and the customer premises network.

5GS should support the means to block malformed signaling messages sent from NFs in the customer premises or operator premises over trust boundary.

5GS should support the means to block messages with wrong NF types sent from NFs in the customer premises or operator premises over the trust boundary according to 3GPP specifications.

Editors Note: Whether the 5GS should support mitigation of DoS by compromised NF are FFS.

5GS should support the means to authenticate and authorize the NFs in the customer premises and operator premises over the trust boundary.

The 5G system shall support a mechanism for secure exchange of DNS queries/answers, when the dedicated NFs are in customer premises.

5GS should support the means to restrict access to services and information exchanged between customer and operator premises and vice versa.

## 6.3 Key issue #3: SUPI privacy issue in PLMN hosting NPN scenario

### 6.3.1 Key issue details

SA1 has captured the scenario for NPN security considerations in clause 8.2 of TS 22.261 [2], which is:

|  |
| --- |
| *The 5G system shall enable a PLMN to host an NPN without compromising the security of that PLMN.**NOTE: Dedicated network entities of NPN can be deployed in customer premises that are outside the control of the PLMN operator.* |

When NPN is hosted by a PLMN, there are two possible deployment scenarios as below:

 - For scenario 1, dedicated UPF is deployed in customer premises, with N4 interface (non-SBA interface) with the operator premises.

- For scenario 2, dedicated UPF and part of CP functions are deployed in customer premises with SBA interface with operator premises.

Considering the primary authentication and authorization procedure specified in the clause in TS 33.501 [3], if a Subscription Permanent Identifier (SUPI) is available in clear text to the NFs in customer premises then it may potentially lead to security threats, privacy breaches, UE location tracking and targeted attacks.

Further, with the evolution of the roaming architectures (Roaming Hub) and Core Network (NPN, Edge computing), distributed CN (multi-site CN), as there is no direct trust relationship between HN and SN/VPLMN/Edge network (i.e., between the different security domains), in this case HN need to consider exposing of permanent and/or sensitive identifiers/ parameter to the NFs in different security domain.

The privacy-sensitive SUPI is the home network operator-provided identifier used exclusively to identify its subscribers and related subscription information to handle the related services.

This key issue is to study how to avoid exposure of the sensitive parameters (specifically, permanent identifiers) to the entities outside the MNO premises (in other security domains).

### 6.3.2 Security Threats

An attacker can compromise NFs in customer premises and can retrieve the SUPI to launch targeted attacks.

An NF can be compromised in customer premises, then a Subscription Permanent Identifier (SUPI) is available to the attacker, it can potentially lead to security threats, like privacy breaches, UE location tracking, mapping of the user to the identifiers, and targeted DoS.

### 6.3.3 Potential security requirements

The 5G system shall support a mechanism to ensure the protection of the sensitive parameters against the risk caused by PLMN hosting NPN and vice versa.

## 6.X Key Issue #X: <Key Issue Name>

### 6.X.1 Key issue details

### 6.X.2 Security threats

### 6.X.3 Potential security requirements

# 7 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 7.1 Solution #1: Secure N4 interface with Security Gateway

### 7.1.1 Introduction

This solution addresses key issue #1.

Considering the nature that the dedicated NF locates outside of operator’s controlled network and interact with PLMN through N4 interface, which leads to the exposure threats to the operator’s core network, this solution proposes to introduce an Security Gateway at the border of operator’s core network to prevent operator’s core network against the attacks through N4 interface. The Security Gateway should be the first contact node when the dedicated UPF interacting with PLMN. All N4 related input/output traffic over the trust boundary should be delegated and protected by Security Gateway.

### 7.1.2 Solution details

The assumed architecture with the Security Gateway deployed over the trust boundary for SBA interface is shown in Figure 7.1-1.



Figure 7.1-1: System architecture for Security Gateway

The NFs in the PNI-NPN Customer’s network trust the Security Gateway deployed in the PLMN. Security protections provided by the Security Gateway for the traffic through N4 interface over the trust boundary can be categorized in the following way:

- Topology information hiding of the PLMN and the customer premises network;

- Signaling inspection and message filtration;

- Security between the dedicated UPF and the Security Gateway;

- Access control etc.

#### 7.1.2.1 Topology information hiding

The Security Gateway delegates every Control Plane message in inter-domain signaling, acting as a service relay between the dedicated UPF and SMF. The Security Gateway can handle topology hiding by limiting the PLMN network topology information visible to the dedicated network in customer premises and vise versa (e.g IP address of SMF/UPF at IP layer, SEID in PFCP message etc.).

Based on the local policy provided by the operator, the appropriate topology hiding mechanisms can be performed based on the security requirements.

Editor's note: It is FFS this solution requires PLMN Operator’s to know the topology information of PNI-NPN Customer’s network. The Security Gateway deployed in the PLMN Operator domain is not intended to protect the NFs in the PNI-NPN Customer’s domain.

#### 7.1.2.2 Signaling inspection and message filtration

The Security Gateway supports to protect the Control Plane messages, it receives all messages through N4 interface over the trust boundary and forwards them to the appropriate NF after verifying security, where present.

Editor's note: It is FFS this solution requires the Security Gateway to interpret all application layer messages passing the trust boundary between PLMN Operator’s domain and the PNI-NPN Customer’s domain.

The Security Gateway supports to discard malformed signaling messages sent from dedicated UPF through N4 interface over the trust boundary according to 3GPP specifications. If an N4 message violates the specified input or output, that message can be considered as malformed message.

NOTE 1: 3GPP specifications specifies N4 message inputs and outputs described in TS 23.502 [4] and TS 29.244 [5] can be considered as normal messages.

NOTE 2: An example for such mechanism is the following: discard PFCP message with unknown/inappropriate message type, discard PFCP message with illegal length, discard the illegal IE which does not belong to the PFCP message, etc.

The Security Gateway supports the means to block messages with wrong NF types sent from NFs in the customer premises or operator premises over the trust boundary according to 3GPP specifications.

The Security Gateway supports anti-spoofing mechanisms that enable cross-layer validation of source and destination address.

NOTE: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the Security Gateway’s PLMN, the message is discarded.

The Security Gateway supports the rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling.

In addition, as the Security Gateway provides a single point of entry for the signaling messages through N4 interface, this gives it the global view on all the NFs connecting with it, which makes it be capable to inspect and filter more advanced behavioral and logical attacks against signaling by analyzing the signaling messages received from multiple NFs.

#### 7.1.2.3 Security between the dedicated UPF and the Security Gateway

The Security Gateway is a network function at the border of a security domain of the operator. After successful mutual authentication between the dedicated UPF and the Security Gateway, the Security Gateway connects the dedicated UPF to the operator’s security domain.

##### 7.1.2.3.1 Authentication

The Security Gateway allows the dedicated UPF access to the core network only after successful completion of all required authentications.

Any unauthenticated traffic from the NF in customer premise is filtered out at the Security Gateway.

IKEv2 with certificates or PSK used for authentication is run between the dedicated UPF and the Security Gateway to mutually authenticate the dedicated UPF and the Security Gateway. The certificate handling and profiles adheres to 3GPP TS 33.310 [6].

##### 7.1.2.3.2 Transport protection between the dedicated UPF and the Security Gateway

The Security Gateway uses IKEv2 protocol to set up IPsec tunnel to protect the traffic with the dedicated UPF. All control plane and user plane traffic over the interface between the dedicated UPF and the Security Gateway are sent through an IPsec ESP tunnel that is established as a result of the authentication procedure, which provides the confidentiality, integrity and replay protections. The IPsec ESP adheres to 3GPP TS 33.310 [6] and IETF RFC 4303[7].

#### 7.1.2.4 Access control

The Security Gateway supports access control:

- The ACL (Access Control List) based access control mechanism for the dedicated UPF accessing the SMF in PLMN and vice versa (e.g. based on NF’s address).

### 7.1.3 Evaluation

Editor's note: evaluation is ffs

## 7.2 Solution #2: CIWF for N4 interface

### 7.2.1 Introduction

This solution addresses key issue 1 to provide security to the PLMN from the attacks that may be initiated by the dedicated UPF. The solution presents a Customer InterWoking Function henceforth referred to as CIWF. The CIWF is deployed in the PLMN operational domain.

This solution assumes that the PNI-NPN customer trusts the PLMN operator to have its topology information and to update/maintain the PNI-NPN topology information.

This solution assumes that the PNI-NPN customer trusts the PLMN operator to have access to and content of messages exchanged with the NF’s residing in the PNI-NPN customer’s operational domain.

### 7.2.2 Solution details

#### 7.2.2.1 General

Figure 7.2-1 illustrates CIWF deployed in PLMN operational domain when dedicated UPF is deployed in PNI-NPN operational domain. Dedicated UPF connects to the PLMN through CIWF. The CIWF may connect dedicated UPFs from different PNI-NPN operational domains simultaneously. CIWF protects the PLMN from the attacks that may be initiated by the dedicated UPF.



Figure 7.2-1 CIWF deployed in PLMN operational domain to protect PLMN through N4 interface

#### 7.2.2.2 Procedure

IPsec ESP and IKEv2 certificate-based authentication are used to provide confidentiality, integrity and replay protection between UPF in PNI-NPN operational domain and CIWF.

IPsec ESP and IKEv2 certificate-based authentication are used to provide confidentiality, integrity and replay protection between SMF in PLMN operational domain and CIWF.

The CIWF does topology hiding, malformed and wrong type message blocking between PLMN operational domain and PNI-NPN operational domain.

Note: The CIWF can support topology hiding and message filtering for messages sent from PLMN to NPN and from NPN to PLMN. However, since the CIWF resides in the PLMN operator’s domain, the PLMN operator will configure the CIWF and therefore the PLMN operator will know the topology and content of messages exchanged with the NF’s residing in the PNI-NPN customer’s operational domain.

Figure 7.2-2 illustrates an example of the procedure.



Figure 7.2-2 Example of procedure

1. SMF sends an N4 Session Establishment Request to CIWF.

2. CIWF checks if it is malformed message or wrong type message. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards the message.

3. CIWF forwards the N4 Session Establishment Request to UPF1.

4. UPF1 sends an N4 Session Establishment Response to CIWF.

5. CIWF checks if it is malformed message or wrong type message. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards the message.

6. CIWF forwards the N4 Session Establishment Response to UPF1.

### 7.2.3 Evaluation

TBD.

## 7.3 Solution #3: A perimeter security gateway for N4 and SBI interface.

### 7.3.1 Introduction

This solution addresses KI#1 "Security for dedicated UPF interacting with PLMN through N4 interface" and KI#2 " Dedicated NFs interacting with PLMN through SBA interface".

### 7.3.2 Solution details

To protect messages that are sent over the N4 and SBI interface, it is proposed to deploy a Hosted NPN Security Protection Proxy (HNSPP) as an entity sitting at the border between the PLMN and customer premise, as shown in Figures 7.3-1 and 7.3-2.

Based on the security level assumption of the operator and customer premises, the deployment options of the HNSPP are as follows:

- Option 1. The HNSPP is only deployed in the operator premise. HNSPP has the ability to filter malformed message, hide topology, and verify the NF type based on the messages sent from both sides of the premises.

- Option 2. The HNSPP is only deployed in the customer premise. HNSPP has the ability to filter malformed message, hide topology, and verify the NF type based on the messages sent from both sides of the premises.

- Option 3. The HNSPP is deployed in each operator and customer premise. HNSPP in the operator premise has the ability to filter malformed message, hide topology, and verify the NF type based on the messages sent from the operator premise. HNSPP in the customer premise has the ability to filter malformed message, hide topology, and verify the NF type based on the messages sent from the customer premise.

It depends on the operator and the PNI-NPN Customer to decide the deployment option of HNSPP.

Editor’s Note: For the scenario where AMF/SMF/UPF are deployed in customer premises, it needs to be explained how procedures involving the NRF, including discovery, registration and access token requests, are affected by the introduction of an HNSPP.

Editor’s Note: Whether the HNSSP can be a SEG with additional security gateway functionality is ffs.

Editor’s Note: What security capabilities and features makes HNSPP more secure than rest of other 3GPP NFs is FFS.

Editor’s Note: What features and mechanisms make HNSPP capable to process the malformed message without any security threats to HNSPP is FFS.

Editor’s Note: Impacts to the NF producer due to HNSPP is for FFS.

Editor’s Note: Impacts due to HNSPP and SCP is for FFS



Figure 7.3-1 Deployment of HNSPP in Hosted NPN with dedicated UPF deployed in the customer premises



Figure 7.3-2 Deployment of HNSPP in Hosted NPN with dedicated UPF and part of CP functions deployed in the customer premises

### 7.3.3 Evaluation

TBD

## 7.4 Solution #4: Security protection to avoid UE information disclosure

### 7.4.1 Introduction

This solution addresses KI#2: Dedicated NFs interacting with PLMN through SBA interface.

A misbehaving NF in the customer premises may request the NF(s) in a PLMN to consume a service that are not allowed by the customer premises.

In case of the customer opting to extend the NF service to GMLC, there could be a possibility to build an attack where an NF in the customer premises may get unauthorized UE’s location using the LCS service. As specified in TS 23.273[8], the Gateway Mobile Location Centre (GMLC) is the first node an external LCS client accesses in a PLMN. After performing authorization of an external LCS Client or AF and verifying target UE privacy, a GMLC forwards a location request to a serving AMF using Namf interface. However, it is assumed that the LCS system deployed in the customer premises shall only provide service to a certain number of UE based on the Customer’s requirement. For example, the LCS system shall provide location service for some UEs belonging to the hosted NPN users. If the home network does not check the relation between the customer premises and the target UE, location information of the target UE (e.g. UEs belonging to the home network) will be leaked.

The solution is proposed to prevent the NFs in the customer premise from requesting the UE's privacy information (e.g., location information) in the operator premise.

The security proxy does not change the authorization flow. OAuth 2.0 framework is still supported, and the producer NF can still decide whether to provide the service.

Editor’s Note: It is ffs whether the scenario where GMLC is deployed in the customer premises is relevant.

### 7.4.2 Solution details

The solution proposes to deploy a security proxy at the border between the operator premise and customer premise. The security proxy is owned by the operator. The security proxy is able to check whether the service is allowed for the specific PNI-NPN domain, when it receives the request from such domain. The security proxy prevents the leakage of UE privacy information in the operator premise by checking the PNI-NPN ID and the UE ID (e.g., SUPI and GPSI) in the service request from the NF consumer in the customer premise. Unlike the NFs in the operator and customer premise, the security proxy does not need to register to the NRF. The security proxy is more like a SEPP or SCP, instead of the NEF.

The solution reuses PNI-NPN IDs (e.g. dedicated DNNs, S-NSSAIs) to identify the services sent from the customer premises. As specified in TS 23.501[9], " Public Network Integrated NPNs are NPNs made available via PLMNs e.g. by means of dedicated DNNs, or by one (or more) Network Slice instances allocated for the NPN." A security proxy deployed in operator premises shall check the authorization of the service request based on the PNI-NPN IDs and a pre-configured local policy. As an example, the pre-configured local policy may include a list of UE’s ID and service range. When the security proxy receives a service request from the PNI-NPN, it checks whether the target UE and service request are in the pre-configured local policy. The security proxy forwards the service request to the corresponding NF in the operator premises only after successful verification.

NOTE: For this solution it is assumed that hosted NPN NFs are provisioned with either DNN or S-NSSAI.



Figure 7.4-1: Security protection to avoid UE privacy information disclosure.

1. Once an NF consumer in the customer premises, denoted by NF-CP, sends a service request to operator premises, it sends the service request to a security proxy firstly. If the service request is used to request some information and services of a UE, the service request shall include a dedicated DNN or S-NSSAI and a SUPI or a GPSI for the target UE.
2. The security proxy checks the authorization based on dedicated DNN or S-NSSAI and a pre-configured local policy. If the target UE is not allowed to exposure the information or invoke a service to the customer premises, the security proxy shall reject the service request received in step 1.

Editor’s Note: Details, provisioning and management of local policy is FFS.

1. If the authorization is successful, the security proxy sends the service request to the corresponding NF producer in the operator premises, denoted by NF-OP.

4-5 After receiving a service response, the security proxy shall send it to the NF-CP directly.

### 7.4.3 Evaluation

Evaluation is FFS.

## 7.5 Solution #5: Secure SBA interface with Security Gateway

### 7.5.1 Introduction

This solution addresses key issue #2.

Considering the nature that the dedicated NF locates outside of operator’s controlled network and interact with PLMN through SBA interface, which leads to the exposure threats to the operator’s core network, this solution proposes to introduce an Security Gateway at the border of operator’s core network to prevent operator’s core network against the attacks through SBA interface. The Security Gateway should be the first contact node when the dedicated NFs interacting with PLMN. All SBA related input/output traffic over the trust boundary should be delegated and protected by the Security Gateway.

Editor’s Note: whether the Security Gateway can be an SCP with additional security gateway functionality is FFS.

### 7.5.2 Solution details

The assumed architecture with the Security Gateway deployed over the trust boundary for SBA interface is shown in Figure 7.5-1.



Figure 7.5-1: System architecture for Security Gateway

The NFs in the PNI-NPN Customer’s network trust the Security Gateway deployed in the PLMN. Security protections provided by Security Gateway for the traffic through SBA interface over the trust boundary can be categorized in the following way:

- Topology information hiding of the PLMN and the customer premises network,

- Signaling inspection and message filtration

- Security between the NF in customer premise and the Security Gateway

- Security between the Security Gateway and the NF in PLMN

- Access control etc.

#### 7.5.2.1 Topology information hiding

The Security Gateway delegates every Control Plane message in inter-domain signaling, acting as a service relay between the actual Service Producer and the actual Service Consumer. For both Service Producer and Consumer, the result of the service relaying is equivalent to a direct service interaction. The Security Gateway handles topology hiding by limiting the PLMN network topology information visible to the dedicated network in customer premises and vise versa.

Editor's note: It is FFS this solution requires PLMN Operator’s to know the topology information of PNI-NPN Customer’s network. The Security Gateway deployed in the PLMN Operator domain is not intended to protect the NFs in the PNI-NPN Customer’s domain.

For SBA interface, the following address information in the message may need to hide IP address or FQDN of the NF in the incoming/outgoing message including in the fields such as CallbackUri, link, Location etc.

Based on the local policy provided by the operator, the appropriate topology hiding mechanisms can be performed based on the security requirements.

#### 7.5.2.2 Signaling inspection and message filtration

The Security Gateway supports to protect application layer Control Plane messages, it receives all messages through SBA interface over the trust boundary and forwards them to the appropriate NF after verifying security, where present.

Editor's note: It is FFS this solution requires the Security Gateway to interpret all application layer messages passing the trust boundary between PLMN Operator’s domain and the PNI-NPN Customer’s domain.

The Security Gateway supports to discard malformed signaling messages sent from NFs in the customer premises or operator premises through SBA interface over the trust boundary according to 3GPP specifications. If an SBI message violates the specified input or output (i.e., SBI message violation), that message can be considered as malformed message.

NOTE: 3GPP specifications specifies N4 message inputs and outputs described in TS 23.502 [4] and TS 29.500 [10] can be considered as normal messages.

The Security Gateway supports the means to block messages with wrong NF types sent from NFs in the customer premises or operator premises over the trust boundary according to 3GPP specifications.

The Security Gateway supports anti-spoofing mechanisms that enable cross-layer validation of source and destination address.

NOTE: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the Security Gateway’s PLMN, the message is discarded.

The Security Gateway supports the rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling.

In addition, as the Security Gateway provides a single point of entry for the signaling messages through SBA interface, this gives it the global view on all the NFs connecting with it, which makes it be capable to inspect and filter more advanced behavioral and logical attacks against signaling by analyzing the signaling messages received from multiple NFs.

#### 7.5.2.3 Security between the NF in customer premise and the Security Gateway

The Security Gateway is a network function at the border of a security domain of the operator. After successful mutual authentication between the NF in the customer premise and the Security Gateway, the Security Gateway connects the NF to the operator’s security domain.

##### 7.5.2.3.1 Authentication

Authentication between the NF in customer premise and the Security Gateway can use one of the following methods:

- If the dedicated network uses protection at the transport layer, authentication provided by the transport layer protection solution for the SBA interface specified in TS 33.501 [3] can be used for authentication between the NF in customer premise and the Security Gateway.

- If the dedicated network does not use protection at the transport layer, authentication between the NF in customer premise and the Security Gateway may be implicit by NDS/IP or physical security.

##### 7.5.2.3.2 Authorization

Authorization between the NF in customer premise and the Security Gateway is based on local authorization policy.

##### 7.5.2.3.3 Transport protection between the Security Gateway and the NF in PLMN

TLS is used for transport protection between the NF in customer premise and the Security Gateway unless network security is provided by other means.

#### 7.5.2.4 Security between the Security Gateway and the NF in PLMN

As a network function locating at the border of the security domain of the operator, the authentication, authorization of the Security Gateway, and the transport protection between the Security Gateway and the NF in PLMN can reused the existing mechanisms on SBA interface.

#### 7.5.2.5 Access control

The Security Gateway supports access control:

- The Security Gateway allows the NF in customer premise access to the core network only after successful completion of all required authentications.

- Any unauthenticated traffic from the NF in customer premise is filtered out at the Security Gateway.

- The ACL (Access Control List) based access control mechanism for the NF in customer premise accessing the service of the NF in PLMN and vice versa (e.g. the accessible service based on NF’s address, the accessible service based on the SBA interface type, the accessible data scope based on SUPI).

Editor's note: It is FFS this solution may overlap with OAuth 2.0 authorization.

### 7.5.3 Evaluation

Editor's note: evaluation is ffs

## 7.6 Solution #6: CIWF as a gateway for SBA interface

### 7.6.1 Introduction

This solution addresses key issue 2 to provide security to the PLMN from the attacks that may be initiated by the dedicated NFs in the PNI-NPN operational domain. The solution presents a Customer InterWoking Function henceforth referred to as CIWF. The CIWF is deployed in the PLMN operational domain.

This solution assumes that the PNI-NPN customer trusts the PLMN operator to have its topology information and to update/maintain the PNI-NPN topology information.

This solution assumes that the PNI-NPN customer trusts the PLMN operator to have access to and content of messages exchanged with the NF’s residing in the PNI-NPN customer’s operational domain.

### 7.6.2 Solution details

#### 7.6.2.1 General

Figure 7.6-1 illustrates CIWF deployed in PLMN operational domain when dedicated NFs is deployed in PNI-NPN operational domain. Dedicated NFs connect to the PLMN through CIWF. The CIWF may connect dedicated NFs from different PNI-NPN operational domains simultaneously. CIWF acts as a gateway to protect the PLMN from the attacks that may be initiated by the dedicated NFs.



Figure 7.6-1 CIWF deployed in PLMN operational domain to protect PLMN through SBA interface

#### 7.6.2.2 Procedure

The CIWF does topology hiding between PLMN operational domain and PNI-NPN operational domain.

Note: The CIWF can support topology hiding and message filtering for messages sent from PLMN to NPN and from NPN to PLMN. However, since the CIWF resides in the PLMN operator’s domain, the PLMN operator will configure the CIWF and therefore the PLMN operator will know the topology and content of messages exchanged with the NF’s residing in the PNI-NPN customer’s operational domain.

Mutual authentication between NFs in the PNI-NPN operational domain and CIWF can be provided by TLS. Mutual authentication between NFs in the PLMN operational domain and CIWF can also be provided by TLS. There is no mutual authentication between NFs in the PNI-NPN operational domain and NFs in the PLMN operational domain.

SBA authorization framework can be used to authorize the service requests between NFs in the PNI-NPN operational domain and NFs in the PLMN operational domain. CIWF forwards the access token request/response between PNI-NPN operational domain and PLMN operational domain.

The CIWF does malformed and wrong type message blocking between PLMN operational domain and PNI-NPN operational domain. CIWF maintains a restriction list of services/operations that NFs in the PNI-NPN operational domain are not allowed to request from NFs in the PLMN operational domain. CIWF also maintains a restriction list of information that NFs in the PNI-NPN operational domain are not allowed to access from NFs in the PLMN operational domain. When CIWF forwards messages between PNI-NPN operational domain and PLMN operational domain:

1. CIWF checks if the message is malformed or wrong type message. If yes, CIWF drops the message.

2. CIWF checks if the service request from PNI-NPN operational domain to PLMN operational domain is in the restriction list of services/operations. If yes, CIWF drops the service request.

3. CIWF checks if the message from PLMN operational domain to PNI-NPN operational domain contains information in the restriction list of information. If yes, CIWF drops the message.

Figure 7.6-2 illustrates an example of the procedure.



Figure 7.6-2 Example of procedure

1. SMF1 in the PNI-NPN operational domain sends Nnrf\_NFDiscovery\_Request to CIWF.

2. CIWF checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Nnrf\_NFDiscovery\_Request to the NRF in the PLMN operational domain.

3. NRF sends Nnrf\_NFDiscovery\_Response to CIWF.

4. CIWF checks if the message is malformed, or wrong type message, or contains information in the restriction list of informaion. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Nnrf\_NFDiscovery\_Response to SMF1.

5. SMF1 sends Nnrf\_AccessToken\_Get\_Request to CIWF.

6. CIWF checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Nnrf\_AccessToken\_Get Request to NRF.

7. NRF issues an access token. NRF sends the access token to the CIWF in Nnrf\_AccessToken\_Get\_ Response.

8. CIWF checks if the message is malformed, or wrong type message, or contains information in the restriction list of information. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Nnrf\_AccessToken\_Get\_Response to SMF1.

9. SMF1 sends Npcf\_SMPolicyControl\_Create\_Request to CIWF. The service request includes the access token received in Step 8.

10. CIWF checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Npcf\_SMPolicyControl\_Create\_Request to PCF.

11. PCF validates the access token.

12. PCF sends Npcf\_SMPolicyControl\_Create\_Response to CIWF.

13. CIWF checks if the message is malformed, or wrong type message, or contains information in the restriction list of informaion. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Npcf\_SMPolicyControl\_Create\_Response to SMF1.

### 7.6.3 Evaluation

TBD.

## 7.7 Solution #7: CIWF as a delegate for SBA interface

### 7.7.1 Introduction

This solution addresses key issue 2 to provide security to the PLMN from the attacks that may be initiated by the dedicated NFs in the PNI-NPN operational domain. The solution presents a Customer InterWoking Function henceforth referred to as CIWF. The CIWF is deployed in the PLMN operational domain.

This solution assumes that the PNI-NPN customer trusts the PLMN operator to have its topology information and to update/maintain the PNI-NPN topology information.

This solution assumes that the PNI-NPN customer trusts the PLMN operator to have access to and content of messages exchanged with the NF’s residing in the PNI-NPN customer’s operational domain.

### 7.7.2 Solution details

#### 7.7.2.1 General

Figure 7.7-1 illustrates CIWF deployed in PLMN operational domain when dedicated NFs is deployed in PNI-NPN operational domain. Dedicated NFs connect to the PLMN through CIWF. The CIWF may connect dedicated NFs from different PNI-NPN operational domains simultaneously. CIWF acts as a delegate to protect the PLMN from the attacks that may be initiated by the dedicated NFs.



Figure 7.7-1 CIWF deployed in PLMN operational domain to protect PLMN through SBA interface

#### 7.7.2.2 Procedure

The CIWF does topology hiding between PLMN operational domain and PNI-NPN operational domain.

Note: The CIWF can support topology hiding and message filtering for messages sent from PLMN to NPN and from NPN to PLMN. However, since the CIWF resides in the PLMN operator’s domain, the PLMN operator will configure the CIWF and therefore the PLMN operator will know the topology and content of messages exchanged with the NF’s residing in the PNI-NPN customer’s operational domain.

Mutual authentication between NFs in the PNI-NPN operational domain and CIWF can be provided by TLS. Mutual authentication between NFs in the PLMN operational domain and CIWF can also be provided by TLS. Client credentials assertion (CCA) based authentication is optionally used between NFs in the PNI-NPN operational domain and NFs in the PLMN operational domain.

SBA authorization framework can be used to authorize the service requests between NFs in the PNI-NPN operational domain and NFs in the PLMN operational domain. CIWF requests access tokens on behalf of NF service consumers in the PNI-NPN operational domain.

The CIWF does malformed and wrong type message blocking between PLMN operational domain and PNI-NPN operational domain. CIWF maintains a restriction list of services/operations that NFs in the PNI-NPN operational domain are not allowed to request from NFs in the PLMN operational domain. CIWF also maintains a restriction list of information that NFs in the PNI-NPN operational domain are not allowed to access from NFs in the PLMN operational domain. When CIWF forwards messages between PNI-NPN operational domain and PLMN operational domain:

1. CIWF checks if the message is malformed or wrong type message. If yes, CIWF drops the message.

2. CIWF checks if the service request from PNI-NPN operational domain to PLMN operational domain is in the restriction list of services/operations. If yes, CIWF drops the service request.

3. CIWF checks if the message from PLMN operational domain to PNI-NPN operational domain contains information in the restriction list of information. If yes, CIWF drops the message.

Figure 7.7-2 illustrates an example of the procedure.



Figure 7.7-2 Example of procedure

1. SMF1 in the PNI-NPN operational domain sends Npcf\_SMPolicyControl\_Create\_Request to CIWF. The service request may include SMF1's CCA.

2. CIWF checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF drops the message. If no, CIWF may performs a service discovery with the NRF in the PLMN operational domain. If SMF1 has included an access token in step 1, or if the CIWF has a cached granted access token, then CIWF may reuse the access token, do topology hiding and proceeds to step 6.

3. CIWF sends Nnrf\_AccessToken\_Get\_Request to the NRF. The access token request may include SMF1's CCA if received in Step 1.

4. If CCA is included, NRF validates SMF1’s CCA. NRF issues an access token.

5. The NRF sends the access token to CIWF in Nnrf\_AccessToken\_Get\_Response.

6. CIWF sends Npcf\_SMPolicyControl\_Create\_Request to the PCF in the PLMN operational domain. The service request includes an access token received in Step 5, and may include the SMF1's CCA if received in Step 1.

7. If CCA is included, PCF validates SMF1’s CCA. PCF validates access token.

8. PCF sends Npcf\_SMPolicyControl\_Create\_Response to CIWF.

9. CIWF checks if the message is malformed, or wrong type message, or contains information in the restriction list of informaion. If yes, CIWF drops the message. If no, CIWF does topology hiding and forwards Npcf\_SMPolicyControl\_Create\_Response to SMF1.

### 7.7.3 Evaluation

TBD.

## 7.8 Solution #8: NRF based service and information exchange restriction

### 7.8.1 Introduction

This solution addresses the service and information exchange restriction issue of KI#2.

In this solution, NRF deployed in PLMN/PLMN hosting NPN domain will do the service and information exchange restriction.

### 7.8.2 Solution details

#### 7.8.2.1 NF Service Producer registration with NRF

During NF Service registration procedure, the NF profile configuration data of the NF Service Producer may include the "additional scope". The "additional scope" information indicates the services/resources that are allowed for the NF Service Consumer of a specific PLMN hosting NPN.

#### 7.8.2.2 NF Service Consumer obtaining access token

The following procedure describes how the NF Service Consumer obtains an access token before service access to NF Service Producers of a specific NF type.

Figure 7.8-1: NF Service Consumer obtaining access token before NF Service access

1. The NF Service Consumer shall request an access token from the NRF in the same PLMN using the Nnrf\_AccessToken\_Get request operation.

The message may also include the information about the NPN served by the NF Service Consumer.

Note: The NPN information can be the location information of the NF profile that is defined in clause 6.3.1.2 of 3GPP TS 23.501 [x]. The location information can indicate the location (e.g., the data centre of a specific company) of the NF instance.

2. The NRF shall verify that the input parameters NF Instance ID, information about the NPN served by the NF Service Consumer, and NF type as well as PLMN ID(s), if available, in the access token request match with the corresponding ones in the public key certificate of the NF Service Consumer or those in the NF profile of the NF Service Consumer or those in CCA of the NF Service Consumer.

 The NRF do the authorization based on the NF profile of NF service producer.

3. If the authorization is successful, the NRF shall send access token to the NF Service Consumer in the Nnrf\_AccessToken\_Get response operation, otherwise it shall reply based on Oauth 2.0 error response. The claims in the token may include information about the NPN served by the NF Service Consumer.

#### 7.8.2.3 NF Service Consumer requesting service access with an access token

Figure 7.8-2: NF Service Consumer requesting service access with an access token

Pre-requisite: The NF Service Consumer is in possession of a valid access token before requesting service access from the NF Service Producer.

1. The NF Service Consumer requests service from the NF Service Producer. The NF Service Consumer shall include the access token.

2. The NF Service Producer shall verify the token as follows:

- The NF Service Producer ensures the integrity of the token by verifying the signature using NRF’s public key or checking the MAC value using the shared secret.

- If the token includes the NPN information and the requested service operation is for requesting/provisioning information/resources (e.g., location information) related to a specific UE:

The NF Service Producer then may check whether the resource to be triggered by the NPN NF service consumer is allowed by the UE.

- The NF Service Producer may leverage the UE ID (e.g., SUPI, GPSI, SUCI) to retrieve the information about the NPN that serves the UE from the UDM/UDR. If the NPN information in the token is identical to the one related to the UE, the verifications should be continued. Otherwise, the verification fails.

- If NPN information is not reflected in UE’s subscription or the NF Service Producer cannot interact with the UDM, the list of UEs associated with the NPNs configured in the local profile can be used.

3. If the verification is successful, the NF Service Producer shall execute the requested service and responds back to the NF Service Consumer. Otherwise, it shall reply based on Oauth 2.0 error.

NOTE: UDM is assumed not to provide the wrong NPN information.

### 7.8.3 Evaluation

TBD

## 7.9 Solution #9: DNS Security in PLMN hosting NPN scenario

### 7.9.1 Introduction

This solution addresses the security requirement of key issue#2. The solution assumes that one or more than one NFs are located in the customer premises.

NFs in the PLMN network and in the PNI-NPN Customer network can resolve/discover NFs in each other’s network through DNS servers hosted in either or both domains. This creates a need to prevent unauthorized entities in either network from querying the associated DNS servers. As such, DNS messages which cross the trust boundary must be protected.

NOTE: This solution does not mandate any DNS security mechanism. It is optional for the network to use the solution defined for providing the DNS security information to the NFs.

### 7.9.2 Solution details

Consider the scenario where the dedicated NF located in the customer premises communicates with the NF in the operator premises over the SBA interface. Based on the FQDN returned by the service discovery mechanism, the DNS exchanges between the dedicated NF and the DNS server in the operator premises are protected. NFs deployed in the customer premises are configured with a DNS server security configuration.

NOTE: Security configuration and profiling of DNS servers should be left to implementation.

### 7.9.3 Evaluation

TBD

## 7.10 Solution #10: SCP based topology hiding

### 7.10.1 Introduction

This solution addresses the topology hiding issue of KI#2.

In this solution, SCP deployed in PLMN domain and SCP deployed in NPN domain will do the topology hiding.

### 7.10.2 Solution details

Figure 7.10-1 SCP based topology hiding

If domain A represents PLMN hosting NPN domain, domain B indicates PLMN domain.

If domain A is PLMN domain, domain B is PLMN hosting NPN domain.

1. To discover the NF services provided in domain B, the NF service consumer in the domain A sends Nnrf\_NFDiscovery\_Request to SCP-A (i.e. the SCP deployed in domain A).

2.SCP-A forwards the NF discovery request to the SCP-B (the SCP deployed in domain B).

3. SCP-B forwards the NF discovery request to the NRF that is deployed in domain B.

4. The NRF checks if the Nnrf\_NFDiscovery\_Request is allowed.

 If allowed, the NRF sends the required parameters (e.g., FQDN, IP address of the NF service provider) to the SCP-B via Nnrf\_NFDiscovery\_Response message.

5. The SCP-B does the topology hiding for the address information of NF service producer (e.g., FQDN, IP address of the NF service provider). The SCP-B forwards the modified NF service producer address information to the SCP-A.

6. SCP-A sends the modified NF service producer address information to the NF service consumer.

7. To request/subscribe information from the NF service producer, the NF service consumer sends request to the SCP-A. The request includes the modified NF service producer address information. To do the subscription, the request includes its own address information (e.g., FQDN, IP address).

8. If SCP-A forwards the request to SCP-B.

If the request includes the NF service consumer address information, SCP-A does the topology hiding to the NF service consumer address information. The SCP-A forwards the modified NF service consumer address information to the SCP-B.

9. SCP-B forwards the request to the NF service producer. The subscription related request includes the modified NF service consumer address information. SCP-B identifies the true NF service producer address information via the modified NF service producer address information.

10. The response message sent by the NF service producer is sent to the SCP-B. The NF service producer may also send the notification message to the SCP-B along with the modified NF service consumer address information.

11. The SCP-B forwards the message to the SCP-A.

12. The SCP-A forwards the message to the NF service consumer. The SCP-A identifies the true NF service consumer address information via the modified NF service consumer address information.

In summary, this solution proposes to use an SCP at the customer premises and an SCP at the operator premises as security gateway functions.

### 7.10.3 Evaluation

TBD

## 7.11 Solution #11: SUPI privacy protection in hosted NPN

### 7.11.1 Introduction

This Solution address KI#3.

### 7.11.2 Solution details

The solution uses the Primary authentication procedure described in TS 33.501 [3] Clause 6.1 as the baseline with the following adaptations as shown in Figure 7.11-1.



Figure 7.11-1: GPSI usage for UE context management in hosted NPN which is external to Operator’s Security Domain

1. The authentication initiation steps are same as in TS 33.501 Clause 6.1.2.

2. The UDM following the SUCI de-concealment and authentication method selection, based on Operator managed SUPI usage restriction policy, UDM/UDR fetches a privacy protected identifier related to the SUPI assigned by the operator based on operator’s local policy, which can be an existing identifier like GPSI containing external identifier defined in TS 23.003. A SUPI usage restriction policy can indicate if a SUPI usage is allowed/not for the UE context management external to operator’s security domain/network domain during a hosted NPNs or serving network access.

3. The UDM provides GPSI additionally along with SUPI usage restriction indication to the AUSF in authentication response.

NOTE: For secure transfer of SUPI across different security domains to facilitate kamf generation and to not impact UE, suitable transport security can be applied as described in Solution#X in this present document.

4. The AUSF and UE exchange selected method specific authentication message based on TS 33.501 [3].

5. Following a successful verification of the response, the AUSF sends received GPSI along with SUPI and SUPI usage restriction indication to the SEAF.

6. The SEAF following a successful Kamf derivation, it deletes SUPI and uses GPSI instead of SUPI for further UE context and subscription data management (e.g., for any Nudm service operation). If the AMF/SEAF wants to initiate primary authentication, it follows TS 33.501 [3] clause 6.12.4 and clause 6.1.2.

### 7.11.3 Evaluation

Editor’s Note: Evaluation is FFS.

Editor’s Note: The impact on UE is FFS.

Editor’ Note: Whether the privacy issue is completely mitigated with this solution is FFS

## 7.12 Solution #12: Secure sensitive data with secure environment

### 7.12.1 Introduction

The solution addresses key issue #3. It is proposed that a Secure Environment is used for the execution of sensitive functions and the storage of sensitive data in the NFs deployed in customer premise.

### 7.12.2 Solution details

A Secure Environment (SeE) is a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the SeE is unknowable to unauthorized external entities, which protects data it holds from unauthorized access and tampering.

The SeE is built from an irremovable, HW-based root of trust by way of a secure boot process, which occurs whenever an NF in customer premises is turned on or goes through a hard reset. The root of trust is physically bound to the NF. The secure boot process includes checks of the integrity of the SeE performed by the root of trust. Only successfully verified components shall be loaded or started. The SeE, after having been successfully started, shall proceed to verify other components of the hosting NF (e.g. operating system and further programs) that are necessary for trusted operation of the NF.

The SeE is used to provide the following protections to secure the sensitive data in customer premise:

- Sensitive data such as SUPI and security context in UE context should be stored in the SeE of the NF in customer premise.

- Sensitive functions such as key derivation functions should be performed within SeE.

- All signaling messages should be confidentiality, integrity and replay protected while being transmitted in the customer premise.

- The following attributes should additionally be confidentiality protected when being sent between the NF in dedicated network and 5GC:

- SUPI.

In summary, this solution proposes that the customer has appropriate physical and other security measures in place to protect the SUPI.

### 7.12.3 Evaluation

Editor's note: evaluation is ffs

## 7.Y Solution #Y: <Solution Name>

### 7.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 7.Y.2 Solution details

### 7.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 8 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 |  | S3-240411 |  |  |  | Skeleton | 0.0.0 |
| 2024-03 | SA3#115 | S3-240977 |  |  |  | S3-240976, S3-240978, S3-240979, S3-240980, S3-240981, S3-241006, S3-241007 implemented | 0.1.0 |
| 2024-04 | SA3#115 e ad-hoc  | S3-241595 |  |  |  | S3-241550, S3-241596, S3-241597, S3-241598, S3-241560, S3-241579, S3-241561, S3-241571, S3-241157 implemented (more Tdoc number to be added) |  |