|  |  |
| --- | --- |
| 3GPP TR 33.757 V0.5.0 (2024-10) | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® 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

7.0 Mapping solutions to key issues 14

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

7.1.1 Introduction 14

7.1.2 Solution details 15

7.1.2.1 Topology information hiding 15

7.1.2.2 Signalling inspection and message filtration 15

7.1.2.3 Security between the dedicated UPF and the Security Gateway 16

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 17

7.2.1 Introduction 17

7.2.2 Solution details 17

7.2.2.1 General 17

7.2.2.2 Procedure for CIWF deployed only in the PLMN operational domain 18

7.2.2.3 Procedure for CIWF deployed in the PLMN and PNI-NPN operational domain 19

7.2.2.4 Procedure for CIWF deployed only in the PNI-NPN operational domain 20

7.2.3 Evaluation 21

7.3 Solution #3: A perimeter security gateway for N4 and SBI interface. 21

7.3.1 Introduction 21

7.3.2 Solution details 22

7.3.2.1 Authentication and Authorization between HNSPP and NFs 23

7.3.2.2 Authentication and Authorization between HNSPPs 23

7.3.2.3 Authentication between NFs and Authorization of NF service access 23

7.3.3 Evaluation 23

7.4 Solution #4: Security protection to avoid UE information disclosure 23

7.4.1 Introduction 23

7.4.2 Solution details 24

7.4.3 Evaluation 25

7.5 Solution #5: Secure SBA interface with Security Gateway 25

7.5.1 Introduction 25

7.5.2 Solution details 25

7.5.2.1 Topology information hiding 26

7.5.2.2 Signalling inspection and message filtration 26

7.5.2.3 Security between the NF in customer premise and the Security Gateway 27

7.5.2.3.1 Authentication 27

7.5.2.3.2 Authorization 27

7.5.2.3.3 Transport protection between the Security Gateway and the NF in PLMN 27

7.5.2.4 Security between the Security Gateway and the NF in PLMN 27

7.5.2.5 Access control 28

7.5.3 Evaluation 28

7.6 Solution #6: CIWF as a gateway for SBA interface 28

7.6.1 Introduction 28

7.6.2 Solution details 28

7.6.2.1 General 28

7.6.2.2 Procedure for CIWF deployed only in the PLMN operational domain 30

7.6.2.3 Procedure for CIWF deployed in the PLMN and PNI-NPN operational domain 32

7.6.2.4 Procedure for CIWF deployed only in the PNI-NPN operational domain 33

7.6.3 Evaluation 35

7.7 Solution #7: CIWF as a delegate for SBA interface 35

7.7.1 Introduction 35

7.7.2 Solution details 35

7.7.2.1 General 35

7.7.2.2 Procedure for CIWF deployed only in the PLMN operational domain 37

7.7.2.3 Procedure for CIWF deployed in the PLMN and PNI-NPN operational domain 38

7.7.2.4 Procedure for CIWF deployed only in the PNI-NPN operational domain 40

7.7.3 Evaluation 41

7.8 Solution #8: NRF based service and information exchange restriction 42

7.8.1 Introduction 42

7.8.2 Solution details 42

7.8.2.1 NF Service Producer registration with NRF 42

7.8.2.2 NF Service Consumer obtaining access token 42

7.8.2.3 NF Service Consumer requesting service access with an access token 43

7.8.3 Evaluation 44

7.9 Solution #9: DNS Security in PLMN hosting NPN scenario 45

7.9.1 Introduction 45

7.9.2 Solution details 45

7.9.3 Evaluation 45

7.10 Solution #10: SCP based topology hiding and message handling 45

7.10.1 Introduction 45

7.10.2 Solution details 46

7.10.3 Evaluation 47

7.11 Solution #11: SUPI privacy protection in hosted NPN 48

7.11.1 Introduction 48

7.11.2 Solution details 48

7.11.3 Evaluation 49

7.12 Solution #12: Secure sensitive data with secure environment 49

7.12.1 Introduction 49

7.12.2 Solution details 50

7.12.3 Evaluation 50

7.13 Solution #13: Extended SEG to support topology hiding and message inspection 50

7.13.1 Introduction 50

7.13.2 Solution details 51

7.13.3 Evaluation 51

7.14 Solution #14: Extended SCP 51

7.14.1 Introduction 51

7.14.2 Solution details 51

7.14.3 Evaluation 55

7.15 Solution #15: SUPI privacy protection based on AMF register with UDM 55

7.15.1 Introduction 55

7.15.2 Solution details 55

7.15.3 Evaluation 55

7.16 Solution #16: Use a new PLMNNPN UE ID to resolve the SUPI privacy issue 56

7.16.1 Introduction 56

7.16.2 Solution details 56

7.16.3 Evaluation 57

7.17 Solution #17: SUPI privacy protection 57

7.17.1 Introduction 57

7.17.2 Solution details 58

7.17.3   Evaluation 59

7.18 Solution #18: Enforcing policy checks for NF Consumer in PNI-NPN 60

7.18.1 Introduction 60

7.18.2 Solution details 60

7.18.2.1 Determining the domain of the NF Consumer 60

7.18.2.2 Enforcing security checks 60

7.18.2.3 Policy checks to be enforced 62

7.18.3 Evaluation 62

7.19 Solution #19: Re-use of existing SMF/UPF/SEG functionality 62

7.19.1 Introduction 62

7.19.2 Solution details 62

7.19.3 Evaluation 62

7.20 Solution #20: SEAF in PLMN operational domain for SUPI privacy protection 63

7.20.1 Introduction 63

7.20.2 Solution details 63

7.20.3 Evaluation 63

7.Y Solution #Y: <Solution Name> 63

7.Y.1 Introduction 63

7.Y.2 Solution details 63

7.Y.3 Evaluation 63

8 Conclusions 63

8.1 Conclusions for KI#1: Security for dedicated UPF interacting with PLMN through N4 interface 64

8.2 Conclusion for KI#2: Dedicated NFs interacting with PLMN through SBA interface 64

Annex <X> (informative): Change history 65

# 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 third-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"

[11] 3GPP TS 33.126: " Lawful Interception requirements"

[12] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security"

[13] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes".

# 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:** Dedicated network entities of a NPN that are outside of the PLMN operator’s security domain and are deployed with the support of a PLMN operator as defined in TS 22.261 [2].

**PLMN Operational domain:** Network entities of NPN that can be deployed in PLMN operator premises 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 addition, 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.

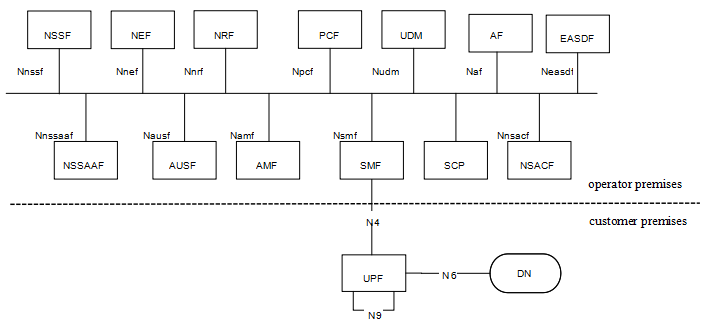


Figure 4-1 PNI-NPN with dedicated UPF deployed in the customer premises

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.

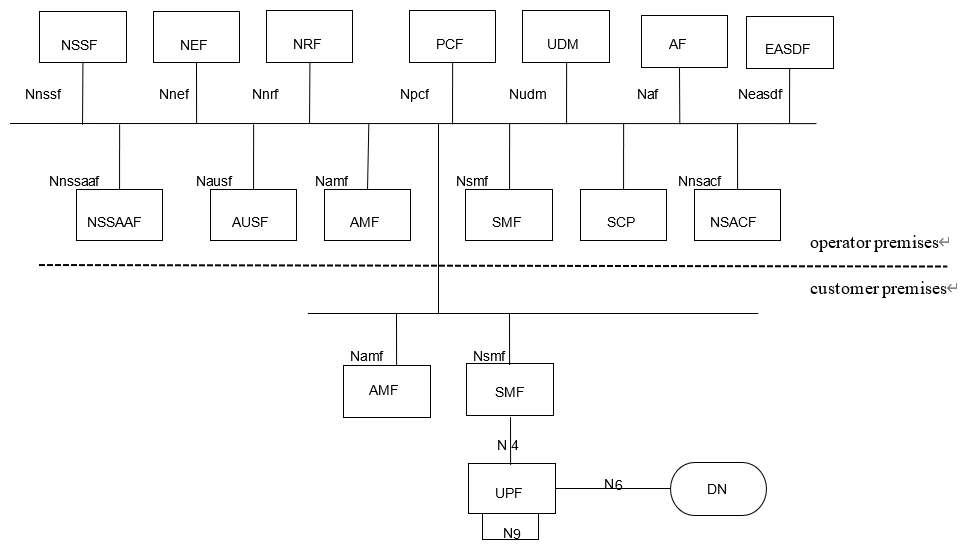


Figure 4-2 PNI-NPN with dedicated UPF and part of CP functions deployed in the customer premises

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 signalling 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 signalling 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 signalling messages to NFs in operator premises or customer premises to degrade NFs’ ability to process normal signalling 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.

- The attacker can send association and session related messages to induce service unavailability condition in the operator or the PNI-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 signalling 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.

Note: The mitigation of DoS by massive signalling attempted by compromised NF in 5GS is left for implementation.

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

The 5G system shall provide the capability for the LI functions in the SMF (CC-TF) in the operator premises to communicate with LI functions in the UPF (CC-POI) in the customer 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 signalling 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 signalling messages to NFs to degrade NFs’ ability to process normal signalling 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 signalling 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.

Note: The mitigation of DoS by compromised NF in 5GS is left for implementation.

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).

1. Lawful interception also applies for PNINPN networks. The solution addressing KI#3 needs the capability to comply with local regulation and the related LI identification requirements defined in TS 33.126 [11] clause 6.2.

### 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.

The 5G system shall provide the capability to comply with lawful interception requirements specified in TS 33.126 [11] clause 6.2.

## 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.

## 7.0 Mapping solutions to key issues

**Table 7.0-1: Mapping of solutions to key issues**

|  |  |  |  |
| --- | --- | --- | --- |
| **Solutions** | **KI#1** | **KI#2** | **KI#3** |
| **1** | **X** |  |  |
| **2** | **X** |  |  |
| **3** | **X** | **X** |  |
| **4** |  | **X** |  |
| **5** |  | **X** |  |
| **6** |  | **X** |  |
| **7** |  | **X** |  |
| **8** |  | **X** |  |
| **9** |  | **X** |  |
| **10** |  | **X** |  |
| **11** |  |  | **X** |
| **12** |  |  | **X** |
| **13** | **X** |  |  |
| **14** |  | **X** |  |
| **15** |  |  | **X** |
| **16** |  |  | **X** |
| **17** |  |  | **X** |
| **18** |  | **X** |  |
| **19** | **X** |  |  |
| **20** |  |  | **X** |

## 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.

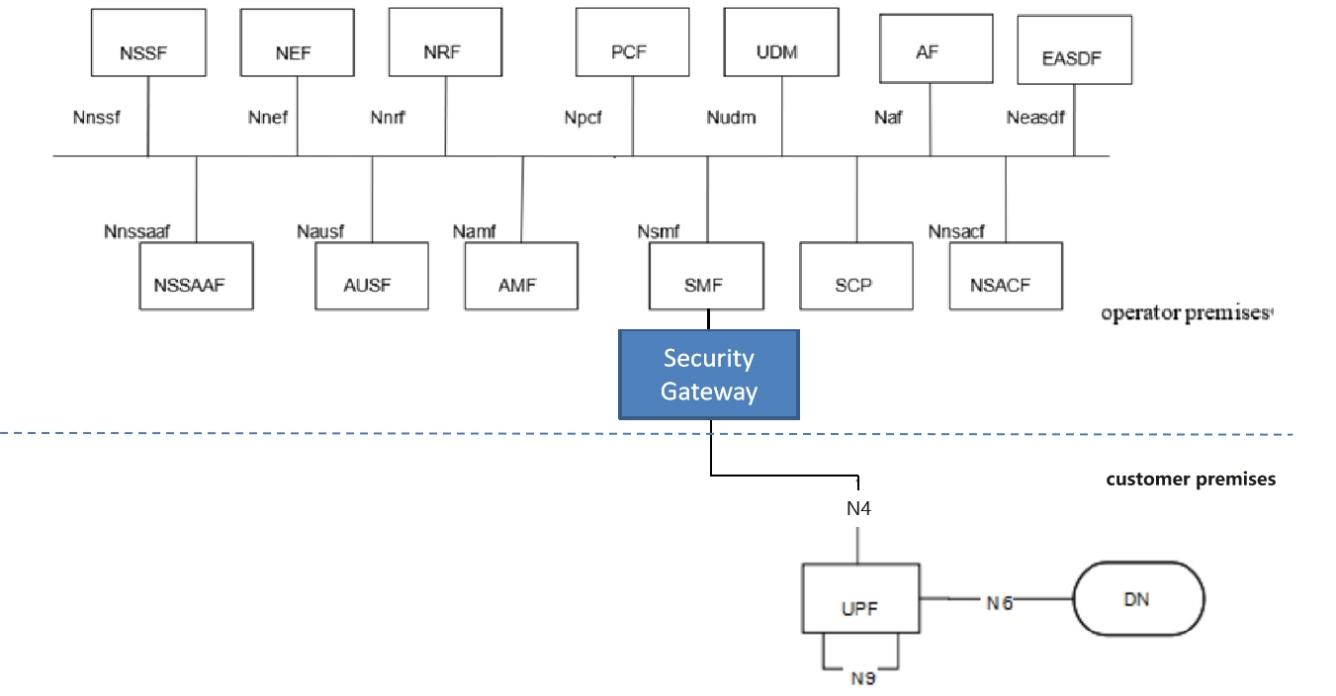


Figure 7.1-1: System architecture for Security Gateway

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;

- Signalling 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 signalling, 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 vice 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.

NOTE: This solution assumes NPN can trust the operator in terms of the topology information, since PNI-NPN is hosted by an PLMN and can be deployed with the support of a public network operator.

#### 7.1.2.2 Signalling 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 signalling 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 signalling.

In addition, as the Security Gateway provides a single point of entry for the signalling 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 signalling by analyzing the signalling 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

The solution can provide topology information hiding, signalling inspection, message filtration, security protection between the dedicated UPF and the Security Gateway and access control, that addresses the requirement of key issue 1.

The solution relies on the deployment of a Security Gateway to secure the traffic through N4 interface over the trust boundary. This solution requires the NFs in the PNI-NPN Customer’s network to trust the Security Gateway deployed in the PLMN Operator’s domain.

Editor's note: Evaluation is ffs.

## 7.2 Solution #2: CIWF for N4 interface

### 7.2.1 Introduction

This solution addresses key issue 1. The solution presents a Customer InterWoking Function henceforth referred to as CIWF.

When the NPN trusts the PLMN and the PLMN does not trust the NPN, the CIWF is deployed only in the PLMN operational domain.

When the NPN does not trust the PLMN and the PLMN does not trust the NPN either, the CIWFs are deployed both in the PLMN operational domain and the PNI-NPN operational domain. The CIWF deployed in the PLMN operational domain is named as CIWF-PLMN. The CIWF deployed in the PNI-NPN operational domain is named as CIWF-NPN.

When the NPN does not trust the PLMN and the PLMN trusts the NPN, the CIWF is deployed only in the PNI-NPN operational domain.

### 7.2.2 Solution details

#### 7.2.2.1 General

Figure 7.2-1 illustrates CIWF deployed only 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.

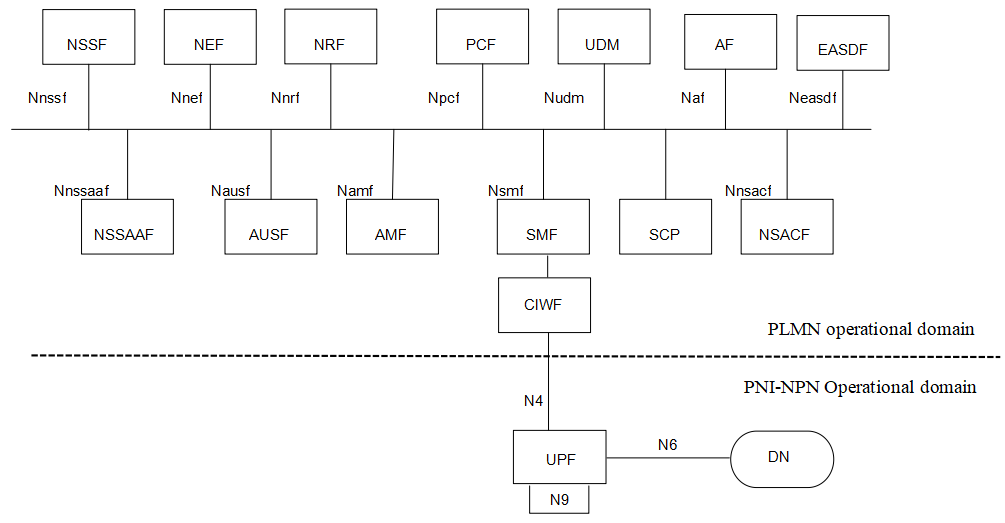


Figure 7.2-1 CIWF deployed only in PLMN operational domain to protect PLMN through N4 interface

Figure 7.2-2 illustrates CIWFs deployed in PLMN and PNI-NPN operational domain for N4 interface. The CIWF-PLMN may connect CIWF-NPNs in different PNI-NPN operational domains simultaneously.

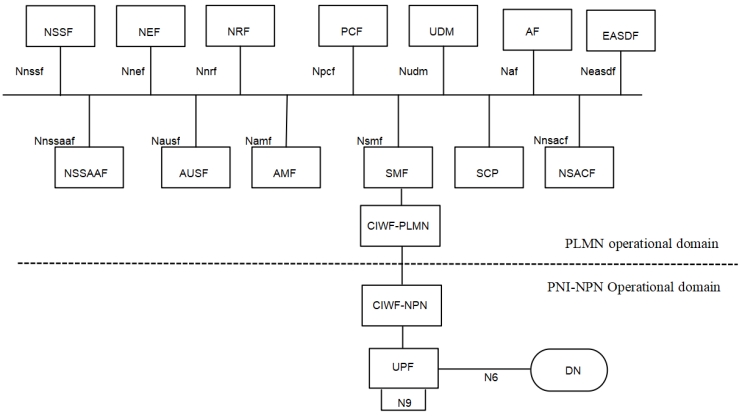


Figure 7.2-2 CIWFs deployed in PLMN and PNI-NPN operational domain for N4 interface

Figure 7.2-3 illustrates CIWF deployed only in PNI-NPN operational domain for N4 interface.

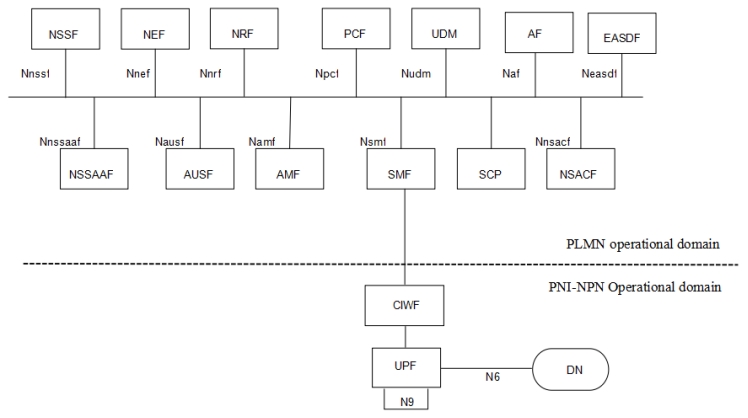


Figure 7.2-3 CIWF deployed only in the PNI-NPN operational domain for N4 interface

#### 7.2.2.2 Procedure for CIWF deployed only in the PLMN operational domain

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 7.2-4 illustrates an example of the procedure.

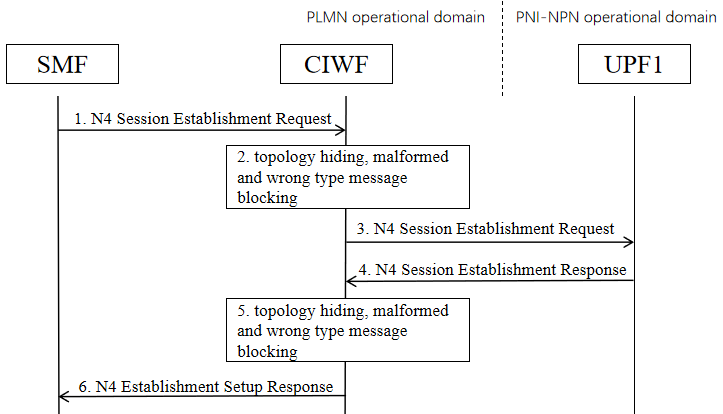


Figure 7.2-4 Example of procedure

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 to SMF’s address 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 to UPF1’s address and forwards the message.

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

#### 7.2.2.3 Procedure for CIWF deployed in the PLMN and PNI-NPN operational domain

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-NPN.

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

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

The CIWF-PLMN does topology hiding for the PLMN. The CIWF-NPN does topology hiding for the PNI-NPN.

The CIWF-PLMN does malformed and wrong type message blocking for messages sending to the PLMN. The CIWF-NPN does malformed and wrong type message blocking for messages sending to the PNI-NPN.

Figure 7.2-5 illustrates an example of the procedure.

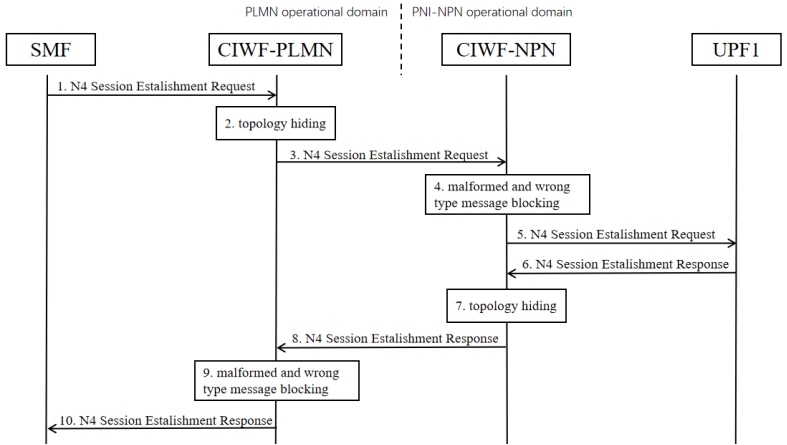


Figure 7.2-5 Example of procedure for CIWF deployed in PLMN and PNI-NPN operational domain

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

2. CIWF-PLMN does topology hiding to SMF’s address.

3. CIWF-PLMN forwards the N4 Session Establishment Request to CIWF-NPN.

4. CIWF-NPN checks if it is malformed message or wrong type message. If yes, CIWF drops the message. If no, CIWF-NPN forwards the message.

5. CIWF-NPN forwards the N4 Session Establishment Request to UPF1.

6. UPF1 sends an N4 Session Establishment Response to CIWF-NPN.

7. CIWF-NPN does topology hiding to UPF1’s address.

8. CIWF-NPN forwards the N4 Session Establishment Response to CIWF-PLMN.

9. CIWF-PLMN checks if it is malformed message or wrong type message. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards the message.

10. CIWF-PLMN forwards the N4 Session Establishment Response to SMF.

#### 7.2.2.4 Procedure for CIWF deployed only in the PNI-NPN operational domain

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 for PNI-NPN operational domain.

Figure 7.2-6 illustrates an example of the procedure.

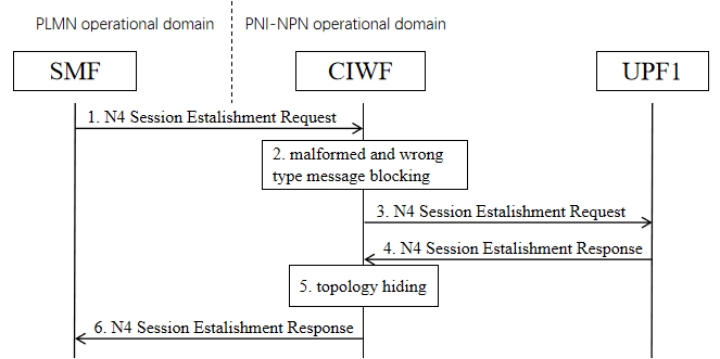


Figure 7.2-6 Example of procedure for CIWF deployed only in the PNI-NPN operational domain

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 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 does topology hiding to UPF1’s address.

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

### 7.2.3 Evaluation

The solution addresses KI#1 by introducing Customer InterWoking Function (CIWF). The CIWF can be deployed only in the PLMN operational domain, or both in the PLMN operational domain and the PNI-NPN operational domain, or only in the PNI-NPN operational domain.

IPsec ESP and IKEv2 certificate-based authentication are used between UPF in PNI-NPN operational domain and CIWF, SMF in PLMN operational domain and CIWF, CIWF-PLMN and CIWF-NPN.

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

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

Editor’s Note: Compliance with LI requirements is FFS.

Editor’s Note: Further evaluation is FFS.

## 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 through 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. HNSPP is deployed to protect both N4 and SBI interface.

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 inspect and 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 inspect and 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 inspect and 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 inspect and 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.

The HNSPP discards malformed signalling messages sent through the N4 and SBI interface.

The HNSPP implements rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signalling. This includes HNSPP-to-HNSPP signalling messages if Option3 is deployed.

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

#### 7.3.2.1 Authentication and Authorization between HNSPP and NFs

The authentication and authorization between HNSPP and NFs can reuse the procedure defined in clause 13.3.6, TS 33.501 [3],

#### 7.3.2.2 Authentication and Authorization between HNSPPs

The authentication and authorization between HNSPPs can reuse the procedure defined in clause 13.3.7, TS 33.501 [3]

#### 7.3.2.3 Authentication between NFs and Authorization of NF service access

The authentication between NFs can reuse the procedure defined in clause 13.3.2, TS 33.501 [3].

The authorization of NF service access can reuse the procedure defined in clause 13.4.1.3, TS 33.501 [3].,

Note: The certificate pre-configuration or certificate management for PNI-NPN is not in the scope of this solution.

### 7.3.3 Evaluation

This solution addresses the requirements of KI#1 and KI#2 i.e mutual topology hiding, handling malformed messages, message inspection and filtering both at SBA and N4, NF type verification, provides rate limiting capability, authentication and authorization of the dedicated NFs.

This solution proposes to deploy a new security proxy named Hosted NPN Security Protection Proxy (HNSPP) to secure both the SBA and N4 interface. The HNSPP can be deployed only in the operator premise in the customer premise, or in both operator and customer premises, based on the operator and the PNI-NPN Customer's decision.

Editor’s Note: Evaluation is FFS.

## 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.

Note: Details, provisioning and management of local policy is left to implementation.

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

The solution addresses the requirement of KI#2 related to restrict access to services and information exchanged between customer and operator premises. The procedure proposes to use a PNI-NPN ID to bind the authorized UE range for each hosted NPN. The PNI-NPN ID may be a dedicated DNN or S-NSSAI or a standalone PNI-NPN ID.

The solution requires the security proxy deployed in operator premises preconfigure a local policy and check the authorization of the service request based on the PNI-NPN IDs. Specifically, the solution checks whether the NF consumer in the customer premise can obtain the information and service of a UE by checking whether the UE id and PNI-NPN ID correspond to that pre-configured in the security proxy. The solution also requires all service request with a UE id needs to add the PNI-NPN ID for authorization check.

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.

NOTE: How to deploy the Security Gateway could be left to the implementation.

### 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.

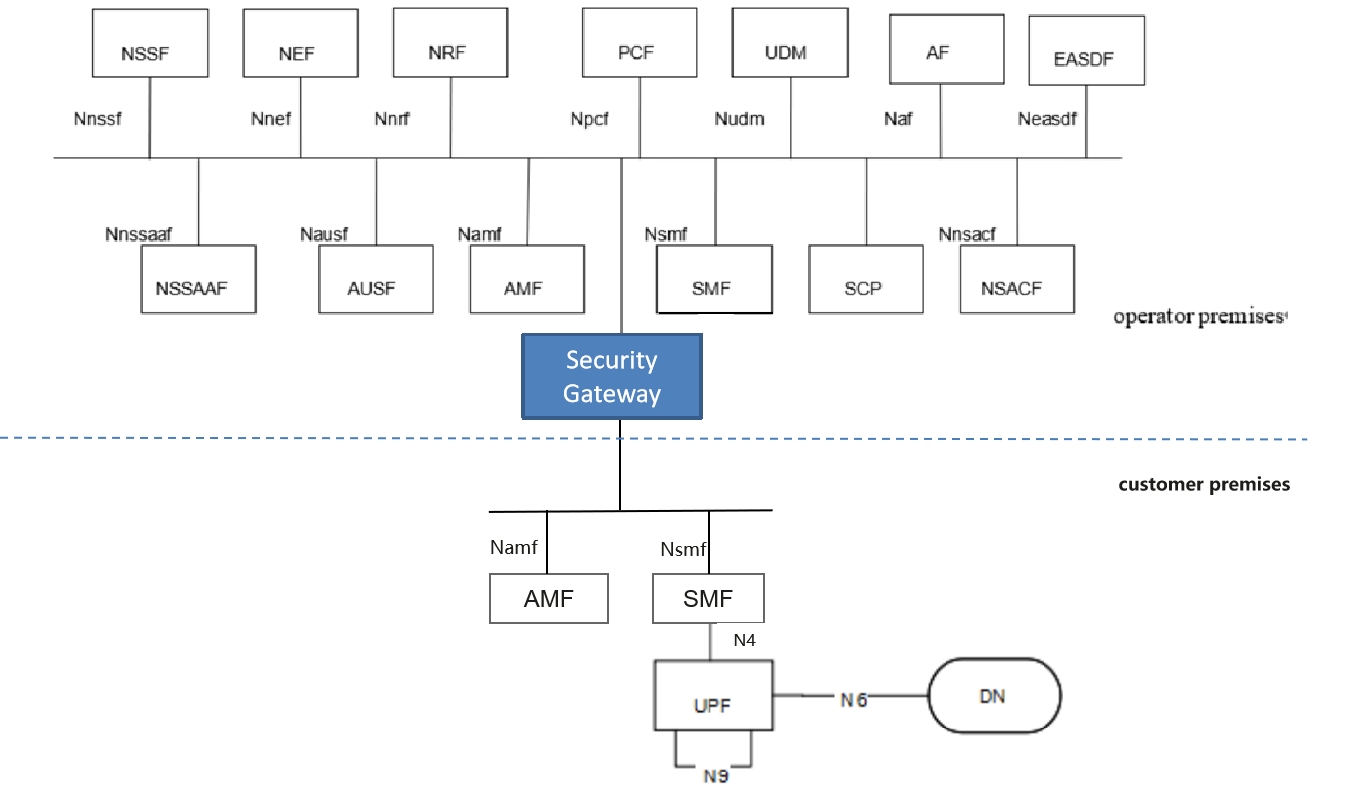


Figure 7.5-1: System architecture for Security Gateway

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,

- Signalling 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 signalling, 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 vice versa.

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.

NOTE: This solution assumes NPN can trust the operator in terms of the topology information, since PNI-NPN is hosted by an PLMN and can be deployed with the support of a public network operator.

#### 7.5.2.2 Signalling 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 signalling 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 signalling.

In addition, as the Security Gateway provides a single point of entry for the signalling 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 signalling by analyzing the signalling 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

The solution can provide topology information hiding, signalling inspection, message filtration, security protection between Security Gateway and NF in each side, and access control, that addresses the requirement of key issue 2.

The solution relies on the deployment of a Security Gateway to secure the traffic through SBA interface over the trust boundary. This solution requires the NFs in the PNI-NPN Customer’s network to trust the Security Gateway deployed in the PLMN Operator’s domain.

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. The solution presents a Customer InterWoking Function henceforth referred to as CIWF. The CIWF acts as a gateway.

When the NPN trusts the PLMN and the PLMN does not trust the NPN, the CIWF is deployed only in the PLMN operational domain.

When the NPN does not trust the PLMN and the PLMN does not trust the NPN either, the CIWFs are deployed both in the PLMN operational domain and the PNI-NPN operational domain. The CIWF deployed in the PLMN operational domain is named as CIWF-PLMN. The CIWF deployed in the PNI-NPN operational domain is named as CIWF-NPN.

When the NPN does not trust the PLMN and the PLMN trusts the NPN, the CIWF is deployed only in the PNI-NPN operational domain.

### 7.6.2 Solution details

#### 7.6.2.1 General

Figure 7.6-1 illustrates CIWF deployed only 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.

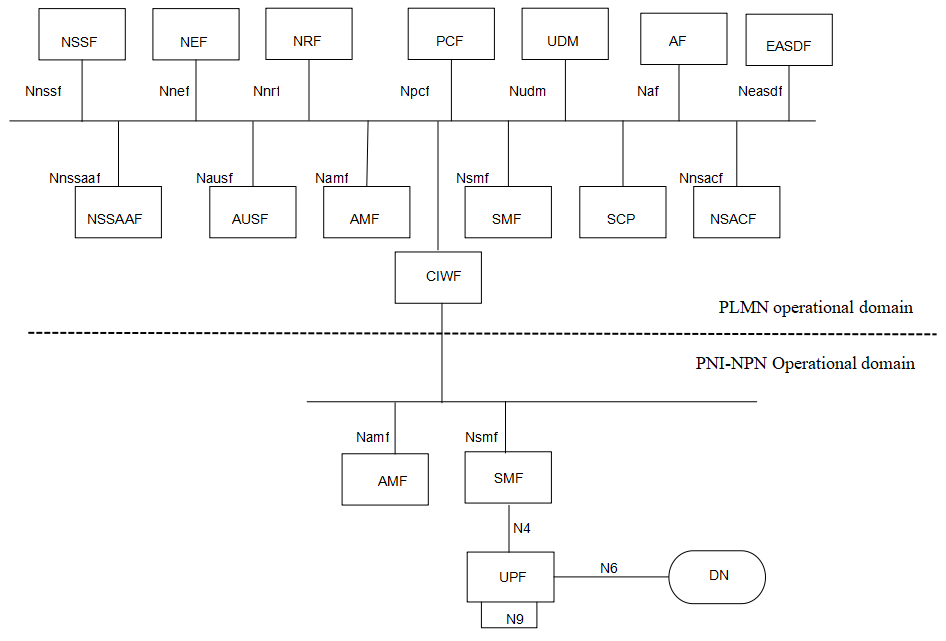


Figure 7.6-1 CIWF deployed only in PLMN operational domain to protect PLMN through SBA interface

Figure 7.6-2 illustrates CIWFs deployed in PLMN and PNI-NPN operational domain for SBA interface. The CIWF-PLMN may connect CIWF-NPNs in different PNI-NPN operational domains simultaneously.

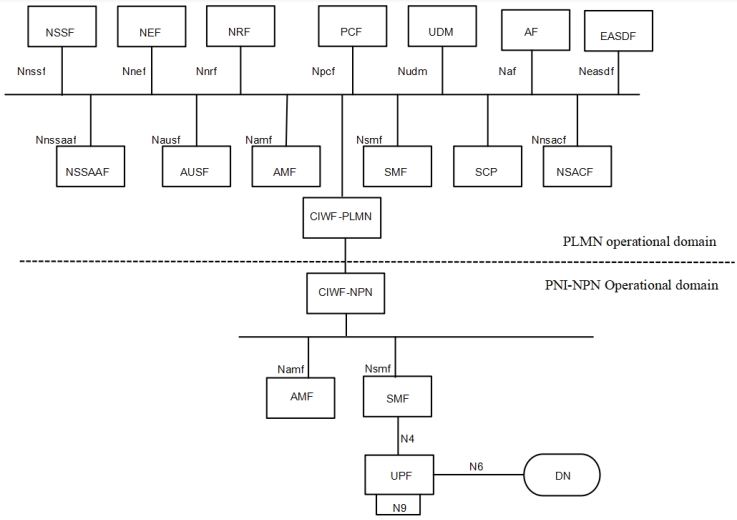


Figure 7.6-2 CIWFs deployed in PLMN and PNI-NPN operational domain for SBA interface

Figure 7.6-3 illustrates CIWF deployed only in PNI-NPN operational domain for SBA interface.

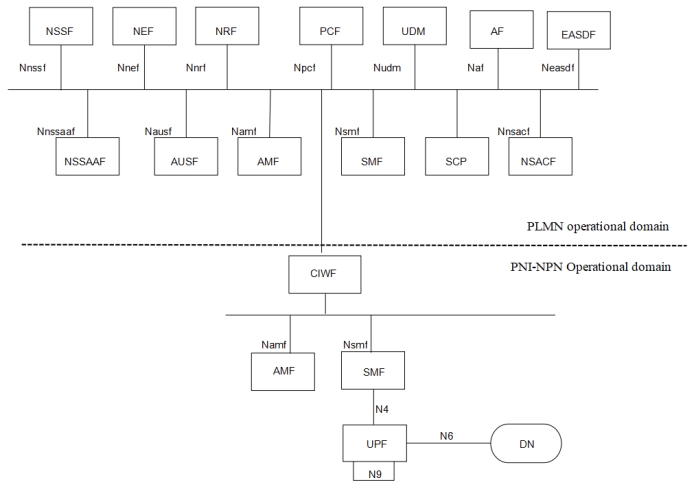


Figure 7.6-3 CIWF deployed only in the PNI-NPN operational domain for SBA interface

#### 7.6.2.2 Procedure for CIWF deployed only in the PLMN operational domain

The CIWF does topology hiding for target NFs in the discovery response, Callback URI in the payload of the messages, IP address or FQDN of the messages etc. 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 7.6-4 illustrates an example of the procedure.

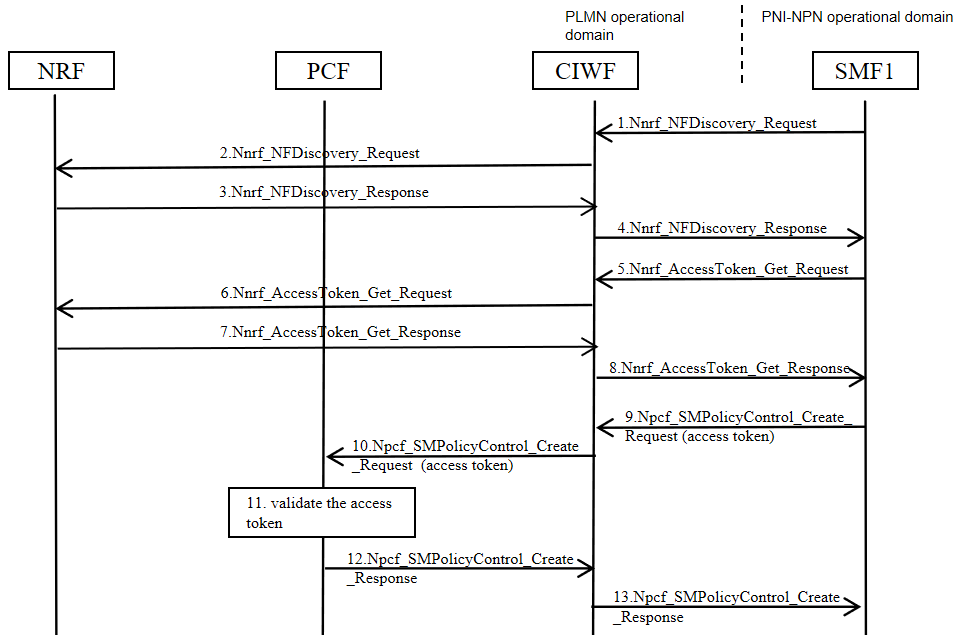


Figure 7.6-4 Example of procedure

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 to SMF1’s address 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 information. If yes, CIWF drops the message. If no, CIWF does topology hiding to modify the address information of NF service provider in the Nnrf\_NFDiscovery\_Response 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 to SMF1’s address 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 to NRF’s address 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 to SMF1’s address 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 information. If yes, CIWF drops the message. If no, CIWF does topology hiding to PCF’s address and forwards Npcf\_SMPolicyControl\_Create\_Response to SMF1.

#### 7.6.2.3 Procedure for CIWF deployed in the PLMN and PNI-NPN operational domain

Mutual authentication between NFs in the PNI-NPN operational domain and the CIWF-NPN can be provided by TLS. Mutual authentication between NFs in the PLMN operational domain and the CIWF-PLMN can also be provided by TLS. Mutual authentication between the CIWF-PLMN and the CIWF-NPN 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-PLMN and CIWF-NPN forward the access token request/response between PNI-NPN operational domain and PLMN operational domain.

CIWFs do topology hiding for target NFs in the discovery response, Callback URI in the payload of the messages, IP address or FQDN of the messages etc. The CIWF-PLMN does topology hiding for the PLMN. The CIWF-NPN does topology hiding for the PNI-NPN.

The CIWF-PLMN does malformed and wrong type message blocking for messages sending to the PLMN. The CIWF-NPN does malformed and wrong type message blocking for messages sending to the PNI-NPN.

CIWF-PLMN 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-PLMN checks messages sending to the PLMN according to the restriction list of services/operations. CIWF-PLMN 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. CIWF-PLMN checks messages sending from the PLMN according to the restriction list of information.

CIWF-NPN maintains a restriction list of services/operations that NFs in the PLMN operational domain are not allowed to request from NFs in the PNI-NPN operational domain. CIWF-NPN checks messages sending to the PNI-NPN according to the restriction list of services/operations. CIWF-NPN also maintains a restriction list of information that NFs in the PLMN operational domain are not allowed to access from NFs in the PNI-NPN operational domain. CIWF-NPN checks messages sending from the PNI-NPN according to the restriction list of information.

Figure 7.6-5 illustrates an example of the procedure.

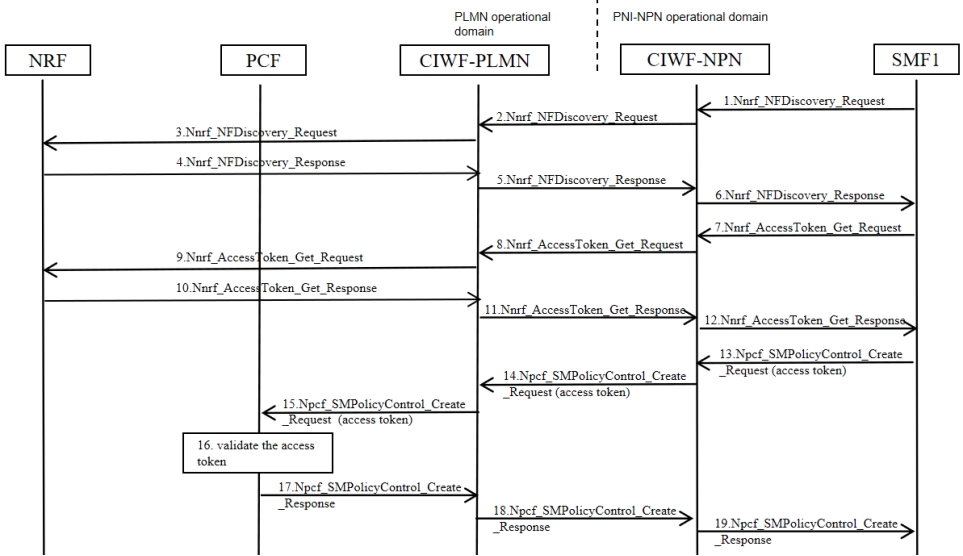


Figure 7.6-5 Example of procedure

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

2. The CIWF-NPN checks if the message contains information in the restriction list of information. If yes, CIWF-NPN drops the message. If no, CIWF-NPN does topology hiding to SMF1’s address and forwards the message to the CIWF-PLMN.

3. The CIWF-PLMN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards the message to the NRF in the PLMN operational domain.

4. NRF sends Nnrf\_NFDiscovery\_Response to CIWF-PLMN.

5. CIWF-PLMN checks if the message contains information in the restriction list of information. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN does topology hiding to modify the address information of NF service provider in the Nnrf\_NFDiscovery\_Response. Then CIWF-PLMN forwards the message to CIWF-NPN.

6. The CIWF-NPN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-NPN drops the message. If no, CIWF-NPN forwards the message to the SMF1.

7. SMF1 sends Nnrf\_AccessToken\_Get\_Request to CIWF-NPN.

8. The CIWF-NPN checks if the message contains information in the restriction list of information. If yes, CIWF-NPN drops the message. If no, CIWF-NPN does topology hiding to SMF1’s address and forwards Nnrf\_AccessToken\_Get\_Request to CIWF-PLMN.

9. The CIWF-PLMN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards Nnrf\_AccessToken\_Get\_Request to NRF.

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

11. CIWF-PLMN checks if the message contains information in the restriction list of information. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN does topology hiding to NRF’s address and forwards the message to CIWF-NPN.

12. The CIWF-NPN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-NPN drops the message. If no, CIWF-NPN forwards Nnrf\_AccessToken\_Get\_ Response to SMF1.

13. SMF1 sends Npcf\_SMPolicyControl\_Create\_Request to CIWF-NPN. The service request includes the access token received in Step 12.

14. The CIWF-NPN checks if the message contains information in the restriction list of information. If yes, CIWF-NPN drops the message. If no, CIWF-NPN does topology hiding to SMF1’s address and forwards Npcf\_SMPolicyControl\_Create\_Request to CIWF-PLMN.

15. The CIWF-PLMN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards Npcf\_SMPolicyControl\_Create\_Request to the PCF in the PLMN operational domain.

16. PCF validates the access token.

17. PCF sends Npcf\_SMPolicyControl\_Create\_Response to CIWF-PLMN.

18. CIWF-PLMN checks if the message contains information in the restriction list of information. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN does topology hiding to PCF’s address and forwards Npcf\_SMPolicyControl\_Create\_Response to CIWF-NPN.

19. The CIWF-NPN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-NPN drops the message. If no, CIWF-NPN forwards tNpcf\_SMPolicyControl\_Create\_Response to SMF1.

#### 7.6.2.4 Procedure for CIWF deployed only in the PNI-NPN operational domain

Mutual authentication between NFs in the PNI-NPN operational domain and the CIWF can be provided by TLS. Mutual authentication between NFs in the PLMN operational domain and the 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.

CIWF does topology hiding for Callback URI in the payload of the messages, IP address or FQDN of the messages etc.

The CIWF does malformed and wrong type message blocking for messages sending to the PNI-NPN.

CIWF maintains a restriction list of services/operations that NFs in the PLMN operational domain are not allowed to request from NFs in the PNI-NPN operational domain. CIWF checks messages sending to the PNI-NPN according to the restriction list of services/operations. CIWF also maintains a restriction list of information that NFs in the PLMN operational domain are not allowed to access from NFs in the PNI-NPN operational domain. CIWF checks messages sending from the PNI-NPN according to the restriction list of information.

Figure 7.6-6 illustrates an example of the procedure.

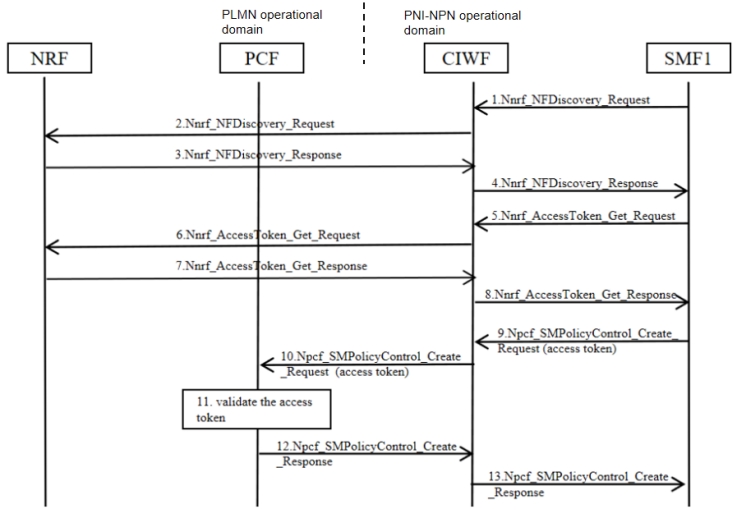


Figure 7.6-6 Example of procedure for CIWF deployed only in the PNI-NPN operational domain

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

2. The CIWF checks if the message contains information in the restriction list of information. If yes, CIWF drops the message. If no, CIWF does topology hiding to SMF1’s address and forwards the message to the CIWF.

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

4. The 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 forwards the message to the SMF1.

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

6. The CIWF checks if the message contains information in the restriction list of information. If yes, CIWF drops the message. If no, CIWF does topology hiding to SMF1’s address 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 in the restriction list of services/operations. If yes, CIWF drops the message. If no, CIWF 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 contains information in the restriction list of information. If yes, CIWF drops the message. If no, CIWF does topology hiding to SMF1’s address 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 in the restriction list of services/operations. If yes, CIWF drops the message. If no, CIWF forwards Npcf\_SMPolicyControl\_Create\_Response to SMF1.

### 7.6.3 Evaluation

The solution addresses KI#2 by introducing Customer InterWoking Function (CIWF) acting as a gateway. The CIWF can be deployed only in the PLMN operational domain, or both in the PLMN operational domain and the PNI-NPN operational domain, or only in the PNI-NPN operational domain.

Authentication provided by the transport layer protection solution are reused for mutual authentication, as defined in TS 33.501 clause 13.3, between NFs in PNI-NPN operational domain and CIWF-NPN, NFs in PLMN operational domain and CIWF-PLMN, the CIWF-NPN and the CIWF-PLMN. 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 topology hiding, malformed and wrong type message blocking between PLMN operational domain and PNI-NPN operational domain.

CIWF maintains a restriction list of services/operations and a restriction list of information. CIWF also blocks messages according to the lists.

Editor’s Note: Further evaluation is FFS.

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

### 7.7.1 Introduction

This solution addresses key issue 2. The solution presents a Customer InterWoking Function henceforth referred to as CIWF. The CIWF acts as a delegate.

When the NPN trusts the PLMN and the PLMN does not trust the NPN, the CIWF is deployed only in the PLMN operational domain.

When the NPN does not trust the PLMN and the PLMN does not trust the NPN either, the CIWFs are deployed both in the PLMN operational domain and the PNI-NPN operational domain. The CIWF deployed in the PLMN operational domain is named as CIWF-PLMN. The CIWF deployed in the PNI-NPN operational domain is named as CIWF-NPN.

When the NPN does not trust the PLMN and the PLMN trusts the NPN, the CIWF is deployed only in the PNI-NPN operational domain.

### 7.7.2 Solution details

#### 7.7.2.1 General

Figure 7.7-1 illustrates CIWF deployed only 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.

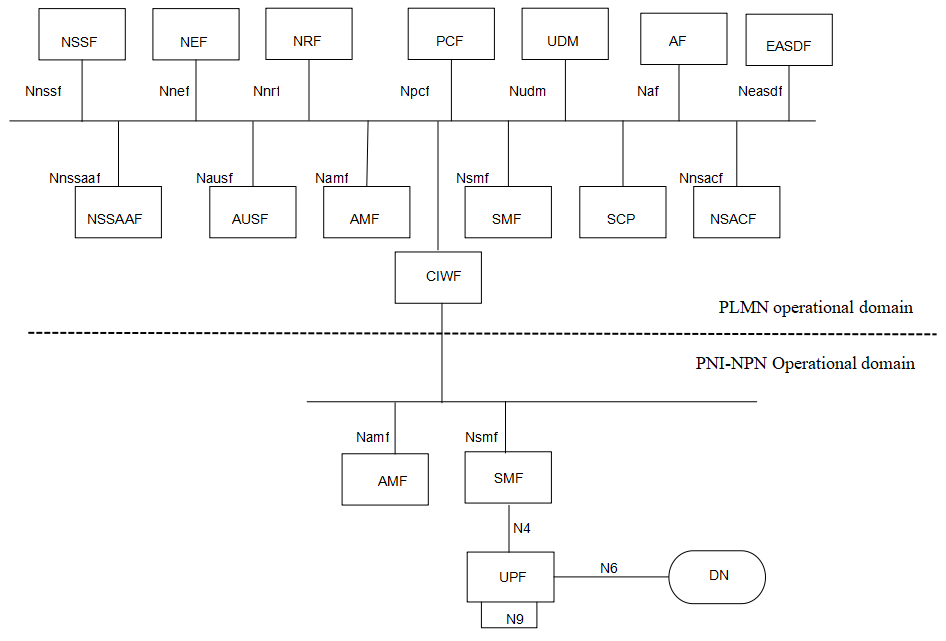


Figure 7.7-1 CIWF deployed only in PLMN operational domain to protect PLMN through SBA interface

Figure 7.7-2 illustrates CIWFs deployed in PLMN and PNI-NPN operational domain for SBA interface. The CIWF-PLMN may connect CIWF-NPNs in different PNI-NPN operational domains simultaneously.

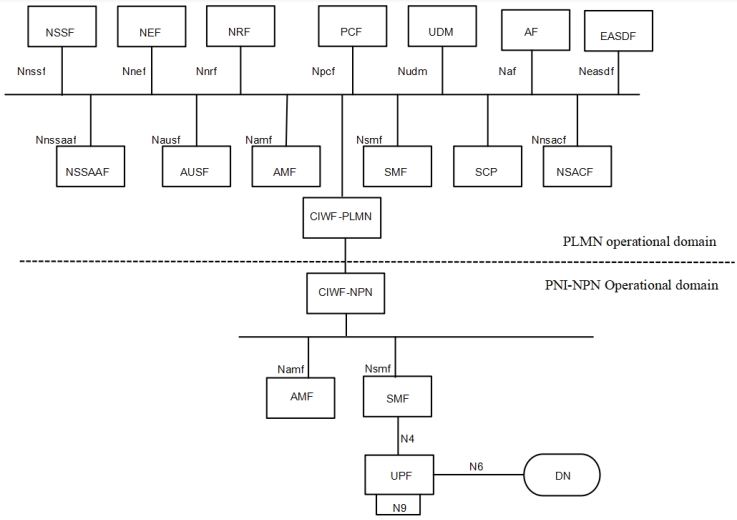


Figure 7.7-2 CIWFs deployed in PLMN and PNI-NPN operational domain for SBA interface

Figure 7.7-3 illustrates CIWF deployed only in PNI-NPN operational domain for SBA interface.

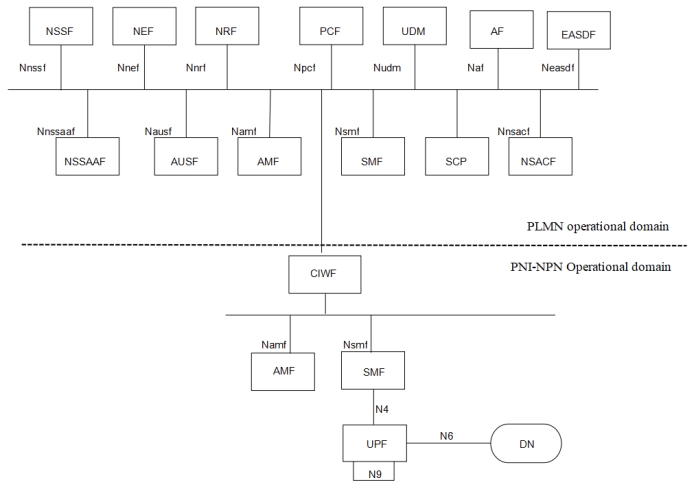


Figure 7.7-3 CIWF deployed only in the PNI-NPN operational domain for SBA interface

#### 7.7.2.2 Procedure for CIWF deployed only in the PLMN operational domain

The CIWF does topology hiding for target NFs in the discovery response, Callback URI in the payload of the messages, IP address or FQDN of the messages etc. 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 7.7-4 illustrates an example of the procedure.

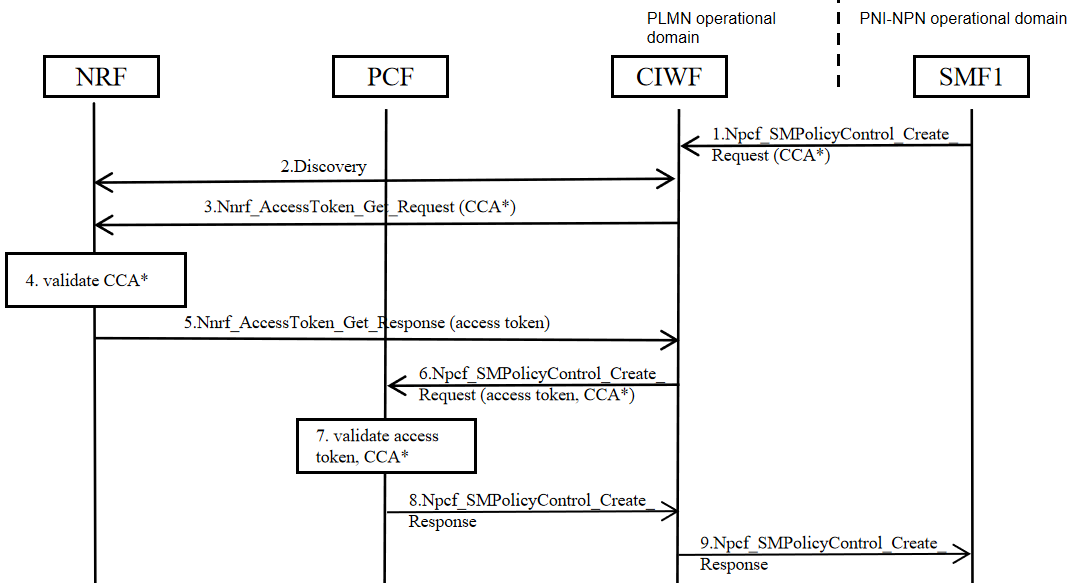


Figure 7.7-4 Example of procedure

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 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 information. If yes, CIWF drops the message. If no, CIWF does topology hiding to PCF’s address and forwards Npcf\_SMPolicyControl\_Create\_Response to SMF1.

#### 7.7.2.3 Procedure for CIWF deployed in the PLMN and PNI-NPN operational domain

Mutual authentication between NFs in the PNI-NPN operational domain and the CIWF-NPN can be provided by TLS. Mutual authentication between NFs in the PLMN operational domain and the CIWF-PLMN can also be provided by TLS. Mutual authentication between the CIWF-PLMN and the CIWF-NPN 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-NPN requests access tokens on behalf of NF service consumers in the PNI-NPN operational domain.

CIWFs do topology hiding for target NFs in the discovery response, Callback URI in the payload of the messages, IP address or FQDN of the messages etc. The CIWF-PLMN does topology hiding for the PLMN. The CIWF-NPN does topology hiding for the PNI-NPN.

The CIWF-PLMN does malformed and wrong type message blocking for messages sending to the PLMN. The CIWF-NPN does malformed and wrong type message blocking for messages sending to the PNI-NPN.

CIWF-PLMN 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-PLMN checks messages sending to the PLMN according to the restriction list of services/operations. CIWF-PLMN 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. CIWF-PLMN checks messages sending from the PLMN according to the restriction list of information.

CIWF-NPN maintains a restriction list of services/operations that NFs in the PLMN operational domain are not allowed to request from NFs in the PNI-NPN operational domain. CIWF-NPN checks messages sending to the PNI-NPN according to the restriction list of services/operations. CIWF-NPN also maintains a restriction list of information that NFs in the PLMN operational domain are not allowed to access from NFs in the PNI-NPN operational domain. CIWF-NPN checks messages sending from the PNI-NPN according to the restriction list of information.

Figure 7.7-5 illustrates an example of the procedure.

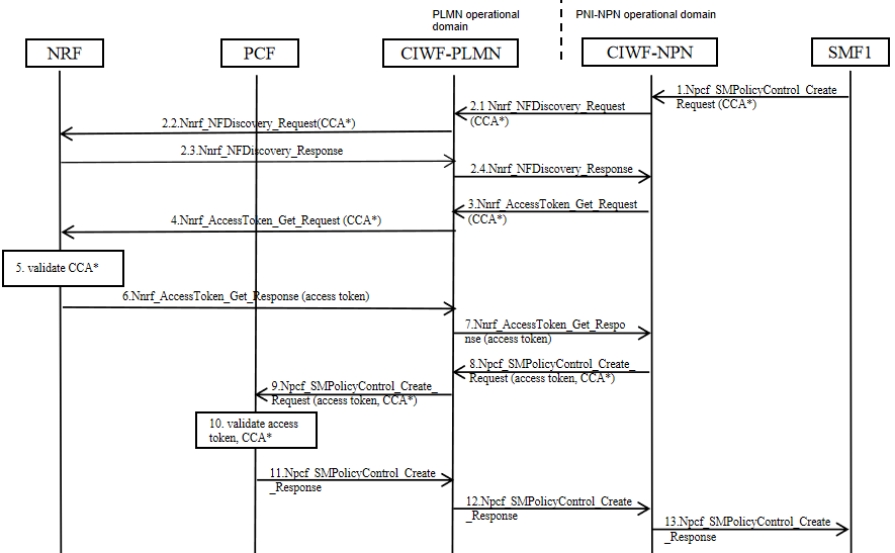


Figure 7.7-5 Example of procedure

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

2. The CIWF-NPN checks if the message contains information in the restriction list of information. If yes, CIWF-NPN drops the message. If no, CIWF-NPN may performs a service discovery with the NRF in the PLMN operational domain.

2.1 CIWF-NPN sends Nnrf\_NFDiscovery\_Request to CIWF-PLMN, SMF1's CCA may be included if received in step 1.

2.2 The CIWF-PLMN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards the message to the NRF.

2.3 If CCA is included, NRF validates SMF1’s CCA. NRF sends Nnrf\_NFDiscovery\_Response to CIWF-PLMN.

2.4 The CIWF-PLMN checks if the message contains information in the restriction list of information. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN does topology hiding to modify the address information of NF service provider in the Nnrf\_NFDiscovery\_Response. Then CIWF-PLMN forwards the message to CIWF-NPN.

2.5 If SMF1 has included an access token in step 1, or if the CIWF-NPN has a cached granted access token, then CIWF-NPN may reuse the access token and proceeds to step 8.

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

4. The CIWF-PLMN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards the message to the NRF.

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

6. The NRF sends the access token to CIWF-PLMN in Nnrf\_AccessToken\_Get\_Response.

7. CIWF-PLMN checks if the message contains information in the restriction list of information. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN does topology hiding to NRF’s address and forwards the message to CIWF-NPN.

8. CIWF-NPN sends Npcf\_SMPolicyControl\_Create\_Request to the CIWF-PLMN. The service request includes an access token received in Step 7, and may include the SMF1's CCA if received in Step 1.

9. The CIWF-PLMN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN forwards the message to the PCF.

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

11. PCF sends Npcf\_SMPolicyControl\_Create\_Response to CIWF-PLMN.

12. CIWF-PLMN checks if the message contains information in the restriction list of information. If yes, CIWF-PLMN drops the message. If no, CIWF-PLMN does topology hiding to PCF’s address and forwards the message to CIWF-NPN.

13. The CIWF-NPN checks if the message is malformed, or wrong type message, or in the restriction list of services/operations. If yes, CIWF-NPN drops the message. If no, CIWF-NPN forwards the message to the SMF1.

#### 7.7.2.4 Procedure for CIWF deployed only in the PNI-NPN operational domain

Mutual authentication between NFs in the PNI-NPN operational domain and the CIWF can be provided by TLS. Mutual authentication between NFs in the PLMN operational domain and the CIW 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.

CIWF does topology hiding for Callback URI in the payload of the messages, IP address or FQDN of the messages etc.

The CIWF does malformed and wrong type message blocking for messages sending to the PNI-NPN.

CIWF maintains a restriction list of services/operations that NFs in the PLMN operational domain are not allowed to request from NFs in the PNI-NPN operational domain. CIWF checks messages sending to the PNI-NPN according to the restriction list of services/operations. CIWF also maintains a restriction list of information that NFs in the PLMN operational domain are not allowed to access from NFs in the PNI-NPN operational domain. CIWF checks messages sending from the PNI-NPN according to the restriction list of information.

Figure 7.7-6 illustrates an example of the procedure.

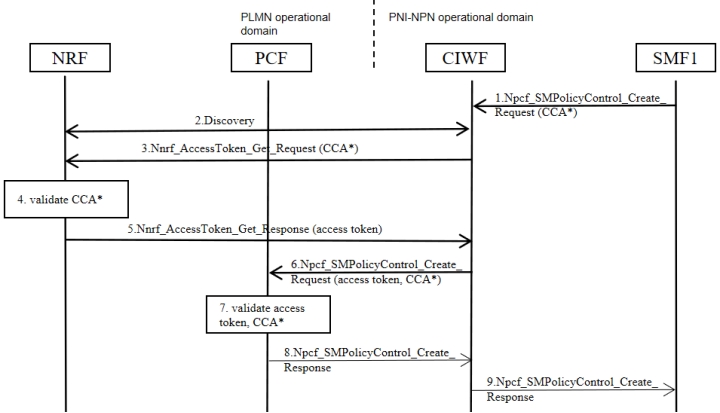


Figure 7.7-6 Example of procedure for CIWF deployed only in the PNI-NPN operational domain

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

2. The CIWF checks if the message contains information in the restriction list of information. If yes, CIWF-NPN 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 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 information. If yes, CIWF drops the message. If no, CIWF does topology hiding to PCF’s address and forwards Npcf\_SMPolicyControl\_Create\_Response to SMF1.

NOTE: The certificate pre configuration or certificate management for PNI-NPN is not in the scope of the solution.

### 7.7.3 Evaluation

The solution addresses KI#2 by introducing Customer InterWoking Function (CIWF) acting as a delegate. The CIWF can be deployed only in the PLMN operational domain, or both in the PLMN operational domain and the PNI-NPN operational domain, or only in the PNI-NPN operational domain.

Authentication provided by the transport layer protection solution are reused for mutual authentication, as defined in TS 33.501 clause 13.3, between NFs in PNI-NPN operational domain and CIWF-NPN, NFs in PLMN operational domain and CIWF-PLMN, the CIWF-NPN and the CIWF-PLMN. 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 topology hiding, malformed and wrong type message blocking between PLMN operational domain and PNI-NPN operational domain.

CIWF maintains a restriction list of services/operations and a restriction list of information. CIWF also blocks messages according to the lists.

Editor’s Note: Further evaluation is FFS.

## 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.

In this solution, NRF deployed in PLMN/PLMN hosting NPN domain will do the wrong NF type handling.

### 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.

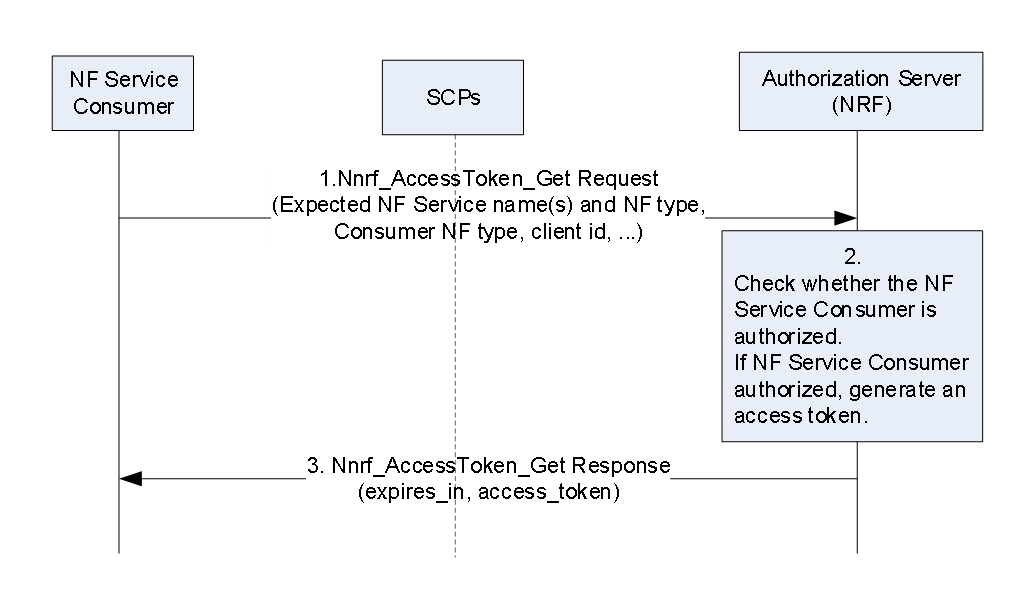
****

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 [9]. 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.

Compared with using the entity deployed at the boundary to handle wrong NF type messages, the NRF needs to verify NF service consumer's NF type for every token request as defined in clause 13 of TS 33.501 [3].The NRF shall use the NF service producer's NF profile to realize the access control and wrong NF type handling.

For the access control part, NRF uses the NF service producer's NF profile to authorize the NF service consumer.

Details of using NRF to handle the wrong NF type are as follows.

The NRF should reject the request if the NF service consumer's NF type is not allowed according to the NF service producer's NF profile (i.e., the wrong NF type is used in the service request).

If the NF service consumer provides the wrong NF type, the NRF shall reject the request. The NRF can check whether the NF service consumer provides the wrong NF type or not. Specifically, the NRF can obtain the NF service consumer's NF Instance ID via reusing the CCA-based mechanism defined in clause 13.3.8 of TS 33.501 [3] to authenticate the NF service consumer. Then the NRF can get the NF service consumer's NF profile via the authenticated ID. The NF profile contains the NF type of the NF service consumer. 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

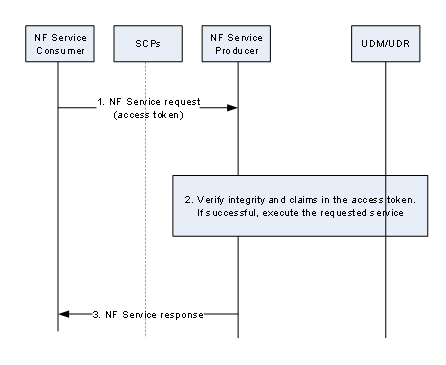


Figure 7.8-2: NF Service Consumer requesting service access with an access token

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 requestingresources related to the 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.

NOTE: The certificate pre configuration or certificate management for PNI-NPN is not in the scope of the solution.

### 7.8.3 Evaluation

This solution reuses the existing NRF and NF service producer's NF profile to realize the wrong NF type handling.

Compared with using the entity deployed at the boundary to handle wrong NF type messages, the NRF needs to verify NF service consumer's NF type for every token request as defined in clause 13 of TS 33.501 [3].This solution addresses the service and information exchange restriction requirement of KI#2 by

- Nnrf\_AccessToken\_Get request message may include the information about the NPN served by the NF Service Consumer.

- NRF authorizes the Nnrf\_AccessToken\_Get request based on NF profile of the network function producer, which includes information about the services/resources that are allowed for the NF Service Consumer of a specific NPN.

- If the token includes NPN information and the service request is related to a specific UE ID, the network function service producer in PLMN checks if the UE ID can be served by the NPN via UDM/UDR/its local profile.

This solution has impacts on NF consumer in NPN domain.

The Nnrf\_AccessToken\_Get sent by NF consumer in NPN also needs to include the information about the NPN served by the NF Service Consumer.

This solution has impacts on NF producer in PLMN domain.

The NF profile of NF producer in PLMN domain needs to indicate the specific PLMN hosting NPN whose services/resources are allowed for the NF Service Consumer.

If the token includes the NPN information and the requested service operation is for requesting information/resources related to a specific UE:

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

- The NF Service Producer needs to 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 by the NF Service Producer.

## 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 (DNS client) and the DNS server in the operator premises are protected. NFs deployed in the customer premises are configured with a DNS security configuration.

The DNS security configuration consists of at least one of the following:

* Security mechanism: Type of DNS Security mechanism (for example, DNS over TLS (RFC 7858) or DNS over DTLS (RFC 8310) or any other mechanism)
* Security credentials: Protocol relevant security parameters (for example, Root Certificate of CA for server certificate verification or Raw Public key)
* Security parameters: Protocol relevant security parameters (for example, Subject Public Key Info (SPKI) or authentication domain name or Security profile)

The dedicated NF is provisioned with the DNS security configuration using one of the following methods:

* Pre-configuring the DNS security configuration in the dedicated NF.
* Updating the DNS security configuration in the dedicated NF during NF instantiation via the OAM.

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

### 7.9.3 Evaluation

This solution enables the NFs in the PLMN network and in the PNI-NPN Customer network to securely resolve/discover NFs in each other’s network through DNS servers hosted in either or both domains.

This prevents unauthorized entities in either network from querying the associated DNS servers.

This solution, therefore, addresses the security requirement related to mutual topology information hiding and for secure exchange of DNS queries/answers in KI #2.

This solution requires the NF service consumer in the PNI-NPN customer network to support one of the DNS security mechanisms that is proposed to be used by the PLMN network.

## 7.10 Solution #10: SCP based topology hiding and message handling

### 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, message inspection, message filtering, and malformed messages handling.

The solution doesn’t address other aspect of KI2 i.e. access control, wrong NF types, unauthorized service operations, and DoS attack.

Editor's Note: Whether to use SCP for message inspection, message filtering, and malformed messages handling is FFS.

### 7.10.2 Solution details

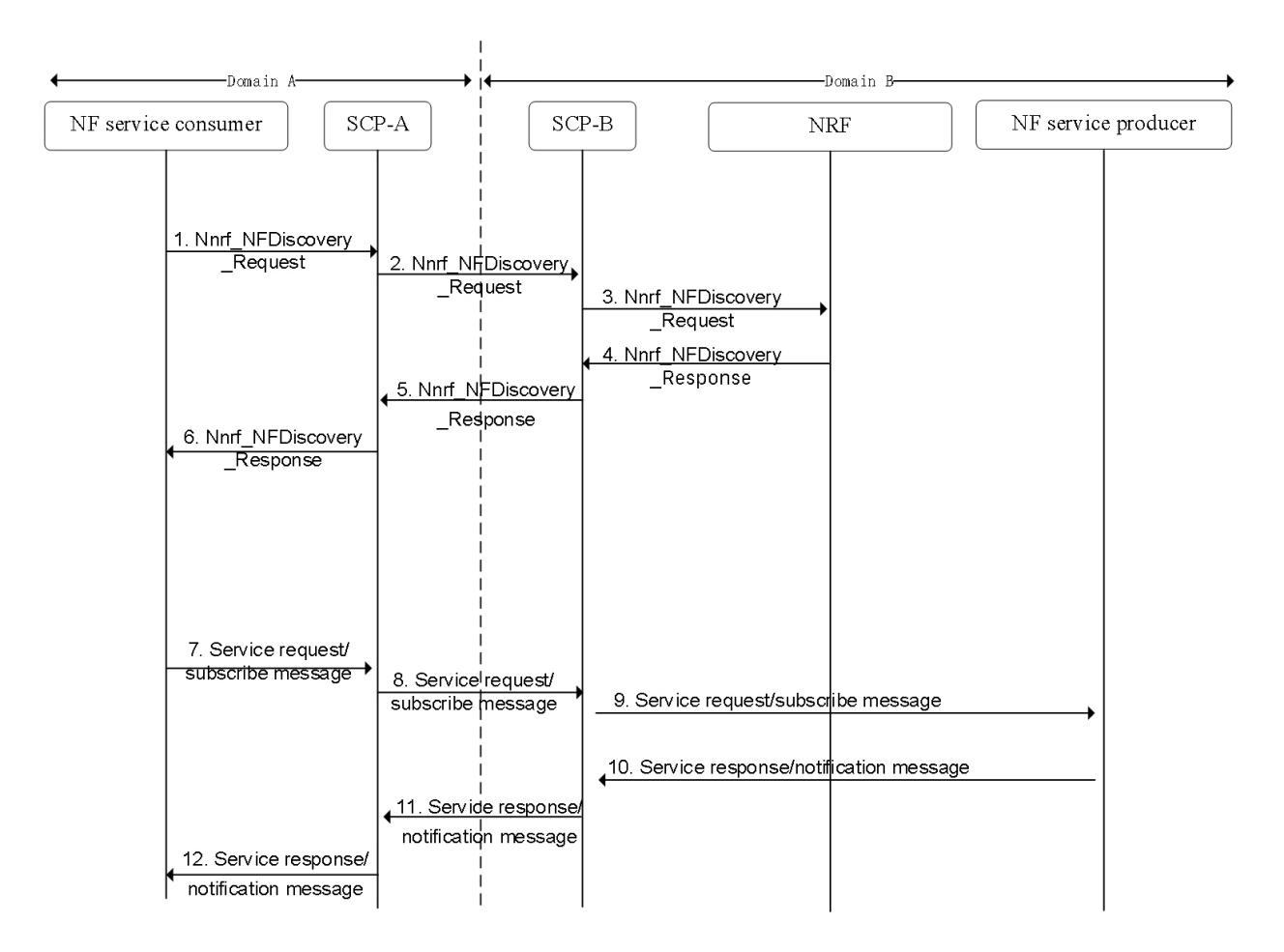


Figure 7.10-1: SCP based topology hiding

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.

The deployment of SCP is flexible. If SCP is only deployed on one domain, then the topology hiding, message inspection, message filtering, and malformed messages handling are only workable for domain deployed with the SCP.

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.

Before SCP-B forwards the discovery request to the NRF, the SCP shall do message inspection, message filtering, and malformed messages handling SCP supports to identify and block malformed messages sent from NF service consumer to NF service producer.

For instance, the SCP can check if the message sent by the NRF is aligned with TS 23.502 [4] clause 5.2.7. If they are not aligned, the SCP regards the message as the malformed message and blocks the message.

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.

Before SCP-A forwards the discovery response to the NF service consumer, the SCP shall do message inspection, message filtering, and malformed messages handling SCP supports to identify and block malformed messages sent from NF service consumer to NF service producer.

For instance, the SCP can check if the message sent by the NF service consumer is aligned with TS 23.502 [4] clause 5.2.7. If they are not aligned, the SCP regards the message as the malformed message and blocks the message.

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.

Before SCP-B forwards the service request to the NF service producer, the SCP shall do message inspection, message filtering, and malformed messages handling SCP supports to identify and block malformed messages sent from NF service consumer to NF service producer.

For instance, the SCP can check if the message sent by the NF service consumer is aligned with TS 23.502 [4] clause 5.2. If they are not aligned, the SCP regards the message as the malformed message and blocks the message.

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.

Before SCP-A forwards the service response to the NF service consumer, the SCP shall do message inspection, message filtering, and malformed messages handling SCP supports to identify and block malformed messages sent from NF service consumer to NF service producer.

For instance, the SCP can check if the message sent by the NF service producer is aligned with TS 23.502 [4] clause 5.2. If they are not aligned, the SCP regards the message as the malformed message and blocks the message.

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

The SCP deployed at the NPN/PLMN in this solution provides IP and FQDN level topology hiding, message inspection, message filtering, and malformed messages handling.

The deployment of SCP is flexible. If SCP is only deployed on one domain, then the topology hiding, message inspection, message filtering, and malformed messages handling are only workable for domain deployed with the SCP.

For SCP deployed in one domain, SCP should be able to do message inspection, message filtering, and malformed messages handling before it forwards the SBA-related message of another domain to NFs in its own domain.

This solution addresses the topology hiding requirement of KI#2 by:

- The SCP deployed in the NPN domain is used to do topology hiding for NF in the NPN domain.

- The SCP deployed in the PLMN domain is used to do topology hiding for NF in the PLMN domain.

- The SCP is used for service discovery/request/response between the NPN domain and the PLMN domain.

## 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. Alternatively, if there is a LI requirement for the UE, then SUPI is provided i.e., authentication process is executed as in TS 33.501 Clause 6.1.3. and none of the following step is executed in that case.

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#12 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.

As an alternative option: To support complete UE privacy for the hosted NPN scenario, a SEAF instance can be collocated with AUSF for Kamf derivation and Kamf is sent to AMF/SEAF in the hosted NPN in step 4 (in this case, SUPI is not sent to hosted NPN, where SEAF collocated with AMF receives and forwards Kamf to AMF and ignores anchor key).

**SUPI based LI:**

The AMF, when there is a LI requirement for a UE with target identity SUPI and if the SUPI is not stored in the available UE contexts, the AMF requests the UDM (e.g., in any suitable Nudm service operation) by sending the target identifier and LI required indication and receives in response the SUPI and GPSI mapping information. This helps the AMF to store the SUPI as part of the right UE Context and performs the necessary LI operations.

### 7.11.3 Evaluation

The solution has the following impacts.

UDM: Operator-managed SUPI usage restriction policy is stored in UDM/UDR and if SUPI usage restriction indication available, it is provided to AUSF along with GPSI. If there is a LI requirement for a UE, then SUPI is provided to the AUSF and SUPI usage restriction does not apply in that case for such UEs.

AUSF: Provides AMF/SEAF with GPSI inaddition to SUPI based on SUPI usage restriction indication from UDM.

SEAF: Deletes SUPI following a successful Kamf derivation and uses GPSI instead of SUPI for UE context.

The solution tries to achieve a better trade off with no UE impact to address KI#3 by reducing the SUPI associated security risks. If the AMF/SEAF is already compromised or if an insider attacker is already present, the security risk is not addressed.

The SUPI based LI can be done.

AMF: In the hosted NPN scenario, if the AMF finds that there is a LI requirement for a UE with target identity SUPI and if the SUPI is not stored in the available UE context, the AMF requests the UDM and fetches the SUPI and GPSI mapping information.

Impacts specific to Complete UE privacy option:

AUSF: Supports co-located SEAF, which perform Kamf key derivation as in TS 33.501.

AMF/SEAF: SEAF collocated with AMF receives and forwards Kamf to AMF and ignores anchor key.

Editor’s Note: The co-location of SEAF in HPLMN and further evaluation if any 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 signalling 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

The solution can prevent unauthorized data retrieval from Trust Environment that addresses the requirement of key issue 3. It’s left for implementation how the SUPI is exchanged from the PLMN to the NPN SeE without disclosure.

The solution relies on the implementation of Secure Environment to secure the execution of sensitive functions and the storage of sensitive data in the NFs deployed in customer premise.

Editor's note: evaluation is ffs

## 7.13 Solution #13: Extended SEG to support topology hiding and message inspection

### 7.13.1 Introduction

TS 33.210 [12] clause 4.5 specifies the SEG as the border component to which all IP traffic shall pass through when leaving or entering a security domain. As the NPN and PLNM domains are perceived as separate security domains this solution proposes to extend the SEG to support topology hiding and message inspection. As described in TS 33.501 [3] clause 9.9 the N4 interface already support IPsec ESP and IKE-v2 certificate-based authentication.

As SEG fulfils most of the requirements for KI#1, its proposed to reuse the SEG and extend the functionality to include message inspection and topology hiding.

### 7.13.2 Solution details

Figure 7.13-1 shows the architecture as described in TS 33.501 [3] clause 9.9 and TS 33.210 [12] clause 4.5. 

Figure 7.13-1: Architecture

The solution proposes to utilise the IPsec ESP for confidentiality protection between the SEG’s in their respective domain – The Za interface defined in TS 33.210 [4]. Mutual authentication and authorisation are enabled by IKE-v2 certificate-based authentication. In addition, message filtering can be supported. This is already specified in TS 33.210 [12] and TS 33.501 [3].

As the SEG’s terminates the IPsec tunnel, messages on the N4 interface are in plaintext between the SMF and SEG and SEG and UPF, which enables the SEG to enforce bi-directional topology hiding and message inspection. The message inspection and filtering are achieved by PFCP message inspection by the SEG – The inspection possibilities and corresponding errors can be found in TS 29.244 [13] clause 7.6. Therefore, it’s proposed to use the already specified architecture, define in TS 33.210 [4], to protect the N4 interface but extend the feature set of the SEG to include topology hiding and message inspection. The enablement of feature set is based on configuration.

To support message inspection besides message filtering the SEG needs to be extended to be N4 message content aware.

Editor’s note: Further clarification on topology hiding is FFS.

### 7.13.3 Evaluation

The solution has the following impacts.

SEG: Extension of SEG to support message filtering and topology hiding.

The solution reuses and extends the SEG with the feature sets required according to KI#1. The solution enables configurability according to domain owner preference and bi-directional protection in the sense that the SEG deployed in each domain can be configured according to preference for message inspection and filtering. Message inspection and filtering is performed, when configured, according to TS 29.244 [5] clause 7.6 which holds the corresponding error codes – Further details concerning the message inspection algorithm is left for deployment.

Editor’s note: Assessment of LI requirements is FFS.

## 7.14 Solution #14: Extended SCP

### 7.14.1 Introduction

This solution proposes to extend the SCP to include topology hiding and message inspection. The precondition of the SCP configuration is communication type C or D where the SCP acts as an intermediate function and the network functions indirectly communicates through the SCP. The communication types C and D differs in the fact that D provides delegate discovery. TS 23.501 Annex G.2 provides an example of communicating over a boundary using the SCP and how the topology information is not known to each side. More information concerning the communication types can be found in TS 23.501 [9] Annex E and G.

### 7.14.2 Solution details

The solution extends the SCP functionality to include topology hiding and message inspection based on policy. The solution is explained through a simplified procedure, subscribe/notify from NPN to PLNM, but the solution also applies to requests from the PLNM to NPN, but in this case the NRF and SCP in the customer domain applies the topology hiding and message inspection. Figures 7.14-1 show the high-level procedure for the case of subscribe notify.

Malformed message inspection applies to all messages that crosses the intersection between the NPN and PLMN and vice versa. The message inspection algorithms are deployed as part of the SCP and the specific algorithm/method deployed is left for implementation.

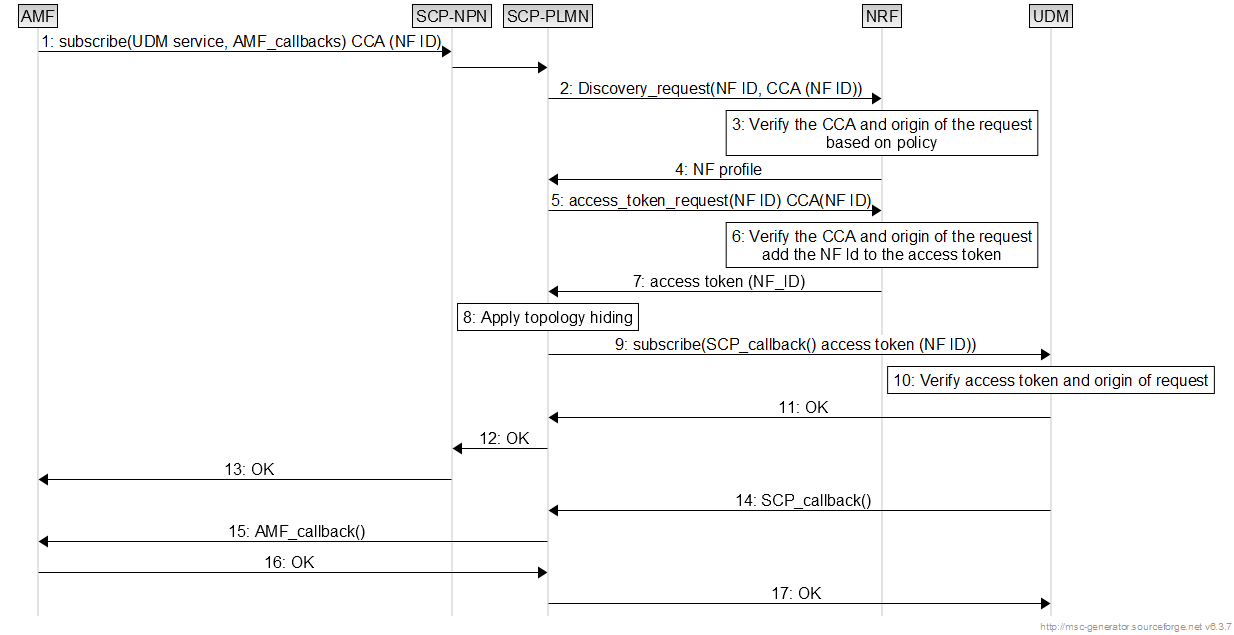


Figure 7.14-1: SCP based topology hiding for the case of subscribe notify.

1. The AMF in customer domain requestion to subscribe to a service in the UDM in the PLMN domain. In the CCA a distinct identifier of the AMF in customer premise is applied.

2. The SCP discovers the UDM and includes the CCA in the request. This is delegated discovery which is part of communication model D.

3-4. The NRF verifies the CCA and according to policy, if the NF ID belongs to another domain verifies that the discovery request origins from the SCP. The authentication and authorization of the consumer to access the producer is accomplished in this step by the NRF according to the procedures described in TS 33.501 [3] clause 13.3.

5. The SCP requests an access token from the NRF.

6-7. The NRF reverifies the CCA according to the same steps as described in step 3. If Valid, the NRF include the NF ID in the access token.

8. The SCP applies topology hiding by substituting the callbacks provided by the AMF with callbacks local to the SCP. The SCP stores the mapping between the local callback and AMF callback. As the SCP uses communication model D (indirect communication with delegate discovery) the topology of the PLNM is not exposes over the boundary between the domains. In this step message inspection can be applied.

9. The SCP registers with the local callbacks at the UDM services. It includes the access token in the request.

10-13. The UDM verifies the access token and according to policy, verifies that the origin of the request is from the SCP if the NF ID belongs to an external domain.

14-16. The UDM triggers the notification of the AMF. The initial callback terminates in SCP which based on translating triggers the callback provided by the AMF.

In all cases the SCP can apply message inspection before forwarding messages to the NRF or service producer.

Similarly, the procedure for request/reply using indirect communication with delegated discovery is shown in figure

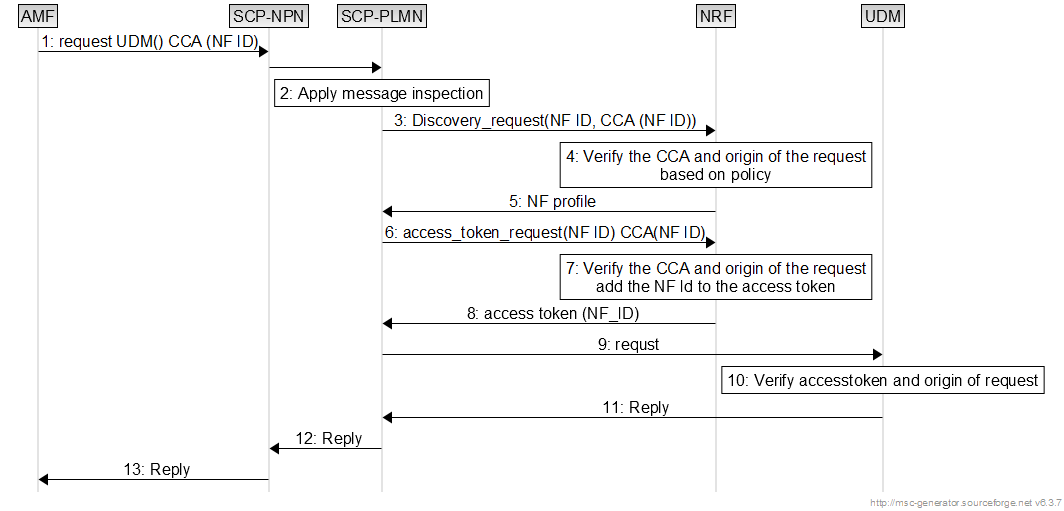


Figure 7.14-2: SCP based topology hiding for the case of request/reply.

1. The AMF in customer domain request a service in the UDM in the PLMN domain. In the CCA a distinct identifier, which is NF ID, of the AMF in customer premise is applied.
2. The SCP applies message inspection/filtering. If the inspection fails, the procedure terminates.

3. The SCP discovers the UDM and includes the CCA in the request. This is delegated discovery which is part of communication model D.

4-5. The NRF verifies the CCA and according to policy, if the NF ID belongs to another domain verifies that the discovery request origins from the SCP. The authentication and authorization of the consumer to access the producer is accomplished in this step by the NRF according to the procedures described in TS 33.501 [3] clause 13.3.

6. The SCP requests an access token from the NRF.

7-8. The NRF reverifies the CCA according to the same steps as described in step 3. If Valid, the NRF include the NF ID in the access token.

9. Request is forwarded to the producer (UDM)

10. The UDM verifies the access token according to policy and verifies that the origin of the request is from the SCP if the NF ID belongs to an external domain.

11-13. The UDM provides the reply to the AMF

Another example of the usage of the solution is the case where the PLNM subscribes to a service in the NPN.

Figure 7.14-3: SCP based topology hiding for the case of subscribe/notify by NF in PLMN.

0. An AMF in NPN registers to NRF in PLMN

1. If a NWDAF in PLMN subscribes notification from NF, e.g. AMF, in NPN, communication model D is applied and NWDAF in PLMN sends request to SCP-PLMN for subscription service in NPN for notification from AMF in NPN, the NWDAF includes target AMF and its domain in the request.

2. The SCP-PLMN send discovery request to NRF on behalf of the NWDAF.

3. After received request, NRF authenticates and authorizes the request target AMF and its DN in the request and local policies, selects and returns NF profile of selected AMF instance(s) to the SCP-PLMN.

4. SCP-PLMN sends request to NRF for access token to subscribe notification of the AMF.

5. NRF authenticates and authorizes the request based on local policies, generated token returns to the SCP-PLMN.

6. SCP-PLMN applies topology hiding, e.g. map callback URI of the original subscription request from address of NWDAF to address of SCP-PLMN.

7. The SCP-PLMN forwards subscription request to AMF in NPN.

8. AMF in NPN validates the token in the request, accepts the request based on local policies, then sends response to SCP-PLMN, and SCP-PLMN forwards the response to the NWDAF.

9. The AMF sends notifications to SCP-PLMN according to subscription information.

10. The SCP-PLMN inspects the notification.

11. If inspection is successful, the SCP-PLMN gets NWDAF address from local mapping table created in step 6, and forwards the notification to the NWDAF.

### 7.14.3 Evaluation

The solution has the following impacts.

SCP: Extension of feature set to support message inspection/filtering and topology hiding.

NRF: Verification of CCA NF ID and the origin of the request (ensure delegated discovery when request is sent from non-trusted domain)

NF: Verification of origin of request when access token sub ID (NF consumer ID) is from the non-trusted domain. (ensure indirect communication through SCP)

The solution reuses the SCP and extends the feature set by message inspection/filtering and topology hiding. The solution inherits already specified features like indirect communication with delegated discovery to authorise the consumer. Authentication is achieved through the client credentials assertion-based authentication. Due to the configurability of SCP deployments (one in each domain or a single in the operator domain), the solution fulfils the requirement for bi-directional protection.

## 7.15 Solution #15: SUPI privacy protection based on AMF register with UDM

### 7.15.1 Introduction

This solution addresses the key issue#3 SUPI privacy issue in PLMN hosting NPN scenario.

### 7.15.2 Solution details

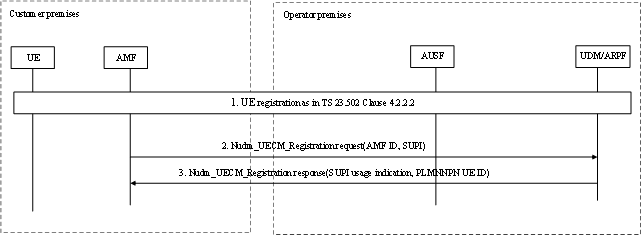


Figure 7.15-1: Procedure

1.UE perform the general registration as specified in TS 23.502 clause 4.2.2.2

2. The new AMF registers with the UDM using Nudm\_UECM\_Registration for the access to be registered. The message includes AMF ID, SUPI.

3. The UDM response a PLMNNPN UE ID, and UDM decide whether the AMF can use SUPI based on the AMF ID. If the AMF can use SUPI (e.g due to LI concern), the UDM sends a SUPI usage indication to AMF to indicate the AMF to keep SUPI. Otherwise, the UDM sends a SUPI usage indication to AMF to indicate the AMF to remove SUPI. The AMF will use PLMNNPN UE ID instead of SUPI for further UE context and subscription data management.

### 7.15.3 Evaluation

This solution needs to secure transfer of SUPI across different security domains, the AMF in the PNI-NPN Operational domain gets the SUPI during the registration procedure. The AMF in the PNI-NPN Operational domain gets a PLMNNPN UE ID instead of SUPI after AMF registration. It does not fully address the SUPI privacy issue due to the LI obligations.

## 7.16 Solution #16: Use a new PLMNNPN UE ID to resolve the SUPI privacy issue

### 7.16.1 Introduction

This solution addresses the key issue#3 SUPI privacy issue in PLMN hosting NPN scenario. A Security for PLMNNPN Network Function (SPNF) is designed to conceal/de-conceal PLMNNPN UE ID.

### 7.16.2 Solution details

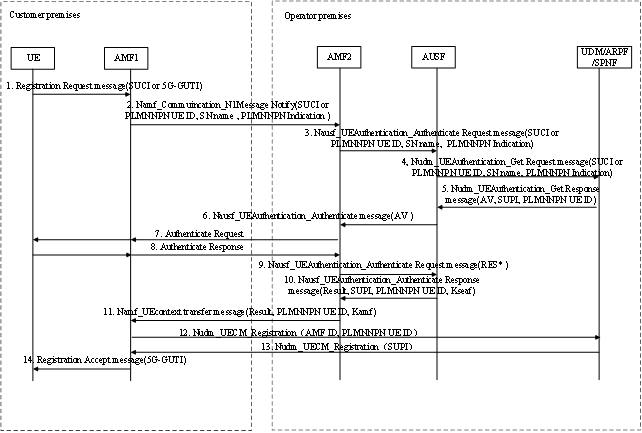


Figure 7.16-1: Procedure

1. The AMF/SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the AMF/SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

2. The AMF/SEAF in the customer premises invoke the Namf\_Commuincation\_N1Message Notify service by sending a Namf\_Commuincation\_N1Message Notify message to an AMF which is located in the operator premises. If AMF/SEAF in the customer premises has the UE context, the AMF/SEAF in the customer premises replace the 5G-GUTI to PLMNNPN UE ID. The Namf\_Commuincation\_N1Message Notify message at least include SUCI or PLMNNPN UE ID, SN name, PLMNNPN service indication.

3. Based on the PLMNNPN service indication, the AMF/SEAF in the operator premises knows the AMF/SEAF in the customer premises wants to trigger the primary authentication. The AMF/SEAF in the operator premises shall invoke the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF when receive the Namf\_Commuincation\_N1Message Notify message in the step 2.

4. The Nausf\_UEAuthentication\_Authenticate Request message shall contain either SUCI or PLMNNPN UE ID. Nausf\_UEAuthentication\_Authenticate Request message may further contain the serving network name. Nausf\_UEAuthentication\_Authenticate Request message may further contain a PLMNNPN service indication.

5. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. UDM shall invoke Security for PLMNNPN Network Function (SPNF) if a UE ID which is used in a customer premises is received. Security for PLMNNPN Network Function (SPNF) shall return SUPI. Based on the PLMNNPN UE ID generation method, the SPNF de-conceal PLMNNPN UE ID or find the mapping (SUPI, PLMNNPN UE ID). For each Nudm\_Authenticate\_Get Request, the UDM/ARPF shall create an authentication vector. If a SUCI is received, Nudm\_Authenticate\_Get Response may further contain a new PLMNNPN UE ID.

6. The AUSF sends an AV in Nausf\_UEAuthentication\_UEAuthentication message to the AMF in the operator premises.

7. The AMF/SEAF in the operator premises forward the Nausf\_UEAuthentication\_UEAuthentication message in step 6 to the AMF in the customer premises, then the AMF/SEAF in the customer premises sends the Authentication request message to UE.

8. UE response an authentication response message with RES\*, then the AMF/SEAF in the customer premises sends an authentication response message to the AMF in the operator premises.

9. The AMF/SEAF in the operator premises sends a Nausf\_UEAuthentication\_Authenticate Request message with RES\* to AUSF.

10. The AUSF shall indicate to the AMF/SEAF in the Nausf\_UEAuthentication\_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the KSEAF shall be sent to the AMF/SEAF in the Nausf\_UEAuthentication\_Authenticate Response. In case the AUSF received a SUCI or PLMNNPN UE ID from the AMF/SEAF in the authentication request, and if the authentication was successful, then the AUSF shall also include the PLMNNPN UE ID in the Nausf\_UEAuthentication\_Authenticate Response message if received from UDM.

11. The AMF/SEAF in the operator premises generate the Kamf and deleted the SUPI in Nausf\_UEAuthentication\_Authenticate Response message then sends an Namf\_UEcontext transfer message to the AMF in the customer premises. The message at least includes one of the followings: Result, PLMNNPN UE ID, Kamf, Result, etc.

12. The AMF in the customer premises registers with the UDM using Nudm\_UECM\_Registration for the access to be registered. The message includes the PLMNNPN UE ID, AMF ID.

13. The UDM decide whether the AMF can use SUPI based on the AMF ID. If the AMF can use SUPI (e.g due to LI concern), the UDM sends a SUPI to AMF.

14. The AMF/SEAF in the customer premises sends UE a registration accept message to UE if the authentication is passed. The AMF/SEAF assign a new 5G-GUTI for the UE.

### 7.16.3 Evaluation

The solution addresses the key issue#3 SUPI privacy issue in PNI-NPN scenario. The solution propose to redirect the registration request to the AMF in the PLMN operator domain and propose a new PLMNNPN UE ID to avoid the SUPI pass between different security domains. The SUPI need to be passed if the LI is needed in the PNI-NPN Operational domain. It does not fully address the SUPI privacy issue due to the SA3-LI obligations.

## 7.17 Solution #17: SUPI privacy protection

### 7.17.1 Introduction

This solution addresses KI#3. In this solution, AUSF determines the UE is in customer premises and derives the KAMF and provides it to the AMF.

### 7.17.2 Solution details

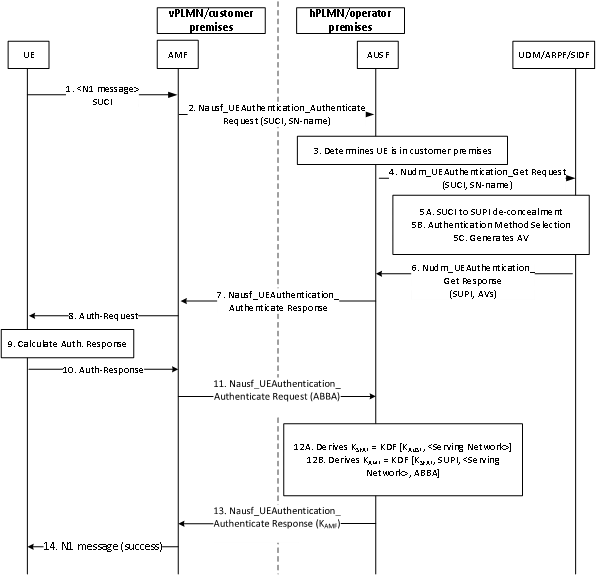


Figure 7.17-1: AUSF determines the UE is in customer premises and derives the KAMF

1. The UE is in roaming in the visited PLMN and/or in customer premises. The UE sends the Registration Request NAS message to the AMF/SEAF in the serving network, containing either a SUCI or 5G-GUTI.

2. On receiving the registration request, the AMF/SEAF invokes primary authentication by sending authentication request i.e., Nausf\_UEAuthentication\_Authenticate request to the AUSF in the home network containing the received SUCI and its serving network name.

3-4. The AUSF verifies the serving network identifier in the authentication request to check if it is the same as the expected serving network name and determines the UE is in customer premises. If the verification is successful, it sends an authentication data request i.e., Nudm\_UEAuthentication\_Get request to the UDM, including the received SUCI and SN name.

5. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF if a SUCI is received. SIDF de-conceals SUPI. The UDM/ARPF chooses the authentication method.

6. The UDM provides the authentication vectors, SUPI and other necessary parameters to the AUSF in Nudm\_UEAuthentication\_Get Response message. Additionally, the UDM derives the SUPItemp for the UE, stores it as part of subscription data and includes it in the response message to the AUSF.

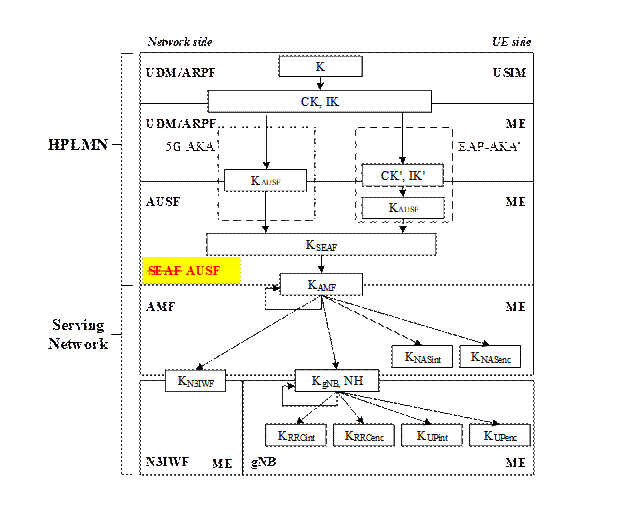
7. The AUSF sends the authentication challenge message to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response message including AV(s).

8-11. The AMF/SEAF transparently forwards the Challenge message to the UE in a NAS message Authentication Request message. On receiving the Authentication request message, the UE calculates the authentication response and sends the response to the AMF/SEAF. The AMF/SEAF provides the ABBA parameter in the Nausf\_UEAuthentication\_Authenticate Request message.

12. The procedure follows as specified in 6.1.3 of TS 33.501[3] except that the AUSF derives KAMF additionally. The derivation of KAMF includes KSEAF as the root key with inputs as: SUPI, SN ID, ABBA parameter Nausf\_UEAuthentication\_Authenticate Request message.

13. The AUSF shares the KAMF to the AMF/SEAF in customer premises as part of Nausf\_UEAuthentication\_Authenticate Response request along with the other necessary parameters. Additionally, the received SUPItemp is provided to the AMF for uniquely identification of the UE.

14. The AMF/SEAF sends N1 message to the UE with the success indication. The SUPItemp is used further as UE’s subscriber identifier as long as the UE is served by the AMF in the same customer premises.



**Figure 7.17-2: Modified key hierarchy where AUSF derives KSEAF and KAMF**

### 7.17.3   Evaluation

This solution addresses KI#3 with no UE impact.

The solution has an impact on the UDM to derive and store a SUPItemp from SUPI. The SUPI­temp is further used to identify the UE.

The solution has an impact on existing key hierarchy between AMF and the AUSF. In this solution, the AUSF derives the KAMF instead of the AMF/SEAF.

The solution has impact on the AUSF and the AMF/SEAF to support the modified key hierarchy when it determines the AMF is in customer premises. The AMF/SEAF can choose to send the ABBA parameter in the Nausf\_UEAuthentication\_Authenticate Request to the AUSF or it can be hardcoded at the AUSF as it is constant in this scenario.

Editor’s Note: Impacts on completion of the registration procedure at the AMF and how is it going to take place to build the UECM that is triggered by AMF while having access to the SUPItemp is FFS.

Editor’s Note: Further evaluation is FFS.

## 7.18 Solution #18: Enforcing policy checks for NF Consumer in PNI-NPN

### 7.18.1 Introduction

This solution addresses the requirement of key issue#2 related to restriction of access to services and information exchanged between customer and operator premises and vice versa. The solution assumes that atleast an NF consumer is in the customer premises.

The solution outlines the security requirements and mechanisms to be enforced by the NRF, SCP or the NF Producer for restricting service access if the NF Consumer is situated outside the PLMN operational domain (operator premises).

### 7.18.2 Solution details

#### 7.18.2.1 Determining the domain of the NF Consumer

To enforce policy checks, the domain of the NF Consumer has to be identified. This process can be carried out by either the NRF or by the NF Producer or by both.

The NF service consumer sends one of the following messages to the NRF: Nnrf\_NFManagement\_NFRegister Request, Nnrf\_NFDiscovery\_Request or Nnrf\_AccessToken\_Get. The NF Consumer also sends NF Service Request message to the NF Producer. The NF service consumer includes the NF instance ID in the above messages.

For an NF Consumer deployed outside the PLMN operational domain (i.e, in the customer premises), the NF instance ID contained in the request message is used by the NRF or NF Producer to identify the domain of the NF Consumer.

The NF instance ID may be included in the access token in addition to the existing parameters like "scope" including the expected NF Service name(s) and optionally "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), NF type of the expected NF Service Producer instance and NF Service Consumer, list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances.

#### 7.18.2.2 Enforcing security checks

The NF Service Consumer, NF Service Producer, and the Network Repository Function (NRF) shall follow the service access authorization procedure within the PLMN as defined in clause 13.4.1.1 of 3GPP TS 33.501 [x].

Once the domain of the NF Service Consumer is determined to be outside the PLMN operational domain (operator premises), additional security checks based on access policy can be performed by either the NRF, SCP or by the NF Producer.

**Enforcement of security checks by the NRF:**

The NRF can enforce security checks using locally configured access policy. The policies can be defined specifically to ensure the security of the externally deployed NF service consumers.

The NRF performs atleast one of the security checks based on the access policy before generating and providing the access token to the NF service consumer.



Figure 7.18-1: NRF performing additional policy checks during access token request

After performing the security checks, the NRF can indicate the SCP or the NF Producer to enforce some or all of the security checks according to the access policy. To enable this, the NRF includes the identifying information and the access policy in the additional scope of the access token.

**Enforcement of security checks by the NF Producer:**

The NF Producer can enforce security checks based on access policy by one of the two following approaches:

1. When the access policy is included in the additional scope of the access token, it can be used to enforce them.
2. When there is no accces policy available in the access token or when static authorization is used, the access policy is to be pre-configured locally.



Figure 7.18-2: NF producer performing additional policy checks during service access request

**Enforcement of security checks by the SCP:**

If an SCP is deployed at the PLMN operational domain, it can enforce the security checks based on access policy as defined in the access token or local configuration.

#### 7.18.2.3 Policy checks to be enforced

The policy checks to be enforced can include (but not limited to):

1. Enforcing mandatory transport layer protection
2. Enforcing mutual authentication between the NF service consumer and the NF service producer (if direct communication is preferred)
3. Enforcing consistency checks between NF service consumer certificate with its NF profile
4. Ensuring NF service consumer integrity
5. Enforce service access requests are routed through an SCP (if indirect communication is preferred)

### 7.18.3 Evaluation

The solution has enhancements to existing service access authorization procedures and NF service consumers in the PLMN hosted NPN domain.

The access token in the NF Service request needs to include the access policy to enforce security checks and ensure the required level of security between the PLMN operational domain and the PNI-NPN operational domain.

If there is no access policy included in the access token, the SCP or the NF service producer needs to enforce security checks based on locally configured access policy before serving the service access request to the NF service consumer.

Editor’s Note: Additional evaluation is FFS

## 7.19 Solution #19: Re-use of existing SMF/UPF/SEG functionality

### 7.19.1 Introduction

This solution addresses Key Issue #1 "Security for dedicated UPF interacting with PLMN through N4 interface". It proposes to use existing functionality of the SMF, UPF and/or SEG to address the Key Issue.

### 7.19.2 Solution details

According to clause 7.6 of TS 29.244 [5], the PFCP protocol already supports error handling that addresses the requirement of Key Issue #1 to block malformed signalling. According to the different subclauses of clause 7.6, protocol errors, different PFCP versions, invalid length of messages, unknown messages, unexpected messages, missing IEs, invalid length of IEs, semantically incorrect IEs, unknown or unexpected IEs and repeated IEs will be addressed by e.g. silent discard and/or logging. Since the SMF and UPF implement the PFCP protocol for the N4 interface, they also implement the error handling.

Authentication, authorization and transport protection (confidentiality, integrity, replay protection) are provided by using existing IPsec ESP and IKEv2 on the N4 interface, as described in TS 33.501 [3] clause 9.9.

The topology can be hidden by network configuration that only allows the UPF (among the network entities in the customer domain) to contact the SMF in the operator domain dedicated to communicating with the customer domain, and vice versa. For example, a SEG can be used to implement this network configuration.

Messages with wrong NF types can be blocked by only allowing PFCP signaling on the N4 interface. If service-based signaling is required, solutions for KI#2 can be used.

### 7.19.3 Evaluation

This solution addresses Key Issue #1 "Security for dedicated UPF interacting with PLMN through N4 interface" by using existing functionality of the SMF, UPF and/or SEG.

## 7.20 Solution #20: SEAF in PLMN operational domain for SUPI privacy protection

### 7.20.1 Introduction

This solution addresses KI#3. In this solution, if the AMF is in PNI-NPN operational domain, then the SEAF is co-located with the AUSF in the PLMN operational domain. If the SEAF is in the PLMN operational domain, then the SUPI is not sent outside the operator domain for KAMF derivation.

### 7.20.2 Solution details

The procedure follows as specified in 6.1.3 of TS 33.501[3], except the following:

* The UDM provides the authentication vectors, SUPI and other necessary parameters to the AUSF in Nudm\_UEAuthentication\_Get Response message. Additionally, the UDM derives the SUPItemp for the UE (determines based on the SN ID) , stores it as part of subscription data and includes it in the response message to the AUSF.
* SEAF is co-located with the AUSF in the PLMN operational domain, instead of co-located with the AMF in the PNI-NPN operational domain.
* The SEAF in the PLMN operational domain derives the KAMF from the KSEAF according to Annex A.7 of TS 33.501 [3] and send it to the AMF in the PNI-NPN operational domain. Additionally, the received SUPItemp from the UDM by the AUSF is provided to the AMF for uniquely identification of the UE.
* The SUPItemp is used further as UE’s subscriber identifier as long as the UE is served by the AMF in the PNI-NPN operational domain.

### 7.20.3 Evaluation

This solution addresses KI#3. According to 3GPP TS 33.501 [3], the SEAF is a logical entity that is co-located with AMF. In this solution, the SEAF is proposed to be co-located with the AUSF. If the SEAF is in the PLMN operational domain, then the SUPI is no longer needed in the PNI-NPN operational domain, as the key KAMF is derived in the PLMN operational domain.

Instead of SUPI, a pseudo SUPI (SUPItemp) is generated by the UDM and provided to the AMF for identification of the UE. The solution has impact to the UDM to generate and store the pseudo SUPI (SUPItemp).

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.

## 8.1 Conclusions for KI#1: Security for dedicated UPF interacting with PLMN through N4 interface

No normative work is endorsed.

## 8.2 Conclusion for KI#2: Dedicated NFs interacting with PLMN through SBA interface

It is proposed to use one or more entities at the border between PLMN and PNI-NPN operational domains.

Editor’s Note: Conclusion is FFS.

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, S3-241610, S3-241640, S3-241613, S3-241617, S3-241641, S3-241642 implemented | 0.2.0 |
| 2024-05 | SA3#116 | S3-242510 |  |  |  | S3-242469, S3-242470, S3-242471, S3-242472, S3-242167, S3-242473, S3-242474, S3-242178, S3-242475, S3-242476, S3-242242, S3-242477, S3-242478, S3-242479, S3-242480, S3-242481, S3-242482, S3-242483, S3-242635, S3-241911, S3-242484, S3-242554, S3-242555, S3-242556, S3-242557, S3-242558, S3-242051, S3-242667 implemented | 0.3.0 |
| 2024-08 | SA3#117 | S3-243468 |  |  |  | S3-242910, S3-243467 S3-243386, S3-243469, S3-243473, S3-243474, S3-243475, S3-243476, S3-243200, S3-243477, S3-242841, S3-243478, S3-243479, S3-243480, S3-243481, S3-243482, S3-243483, S3-243485, S3-242754 implemented | 0.4.0 |
| 2024-10 | SA3#118 | S3-242823 |  |  |  | S3-244152, S3-244149, S3-244153, S3-244204, S3-244338, S3-244492, S3-244493 | 0.5.0 |