|  |
| --- |
| 3GPP TR 33.757 V0.1.0 (2024-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security for PLMN hosting a NPN(Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

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

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Overview 7

5 Security assumptions 8

6 Key issues 8

6.1 Key Issue #1: Security for dedicated UPF interacting with PLMN through N4 interface 9

6.1.1 Key issue details 9

6.1.2 Security threats 9

6.1.3 Potential security requirements 9

6.2 Key Issue #2: Dedicated NFs interacting with PLMN through SBA interface 9

6.2.1 Key issue details 9

6.2.2 Security threats 10

6.2.3 Potential security requirements 10

6.3 Key issue #3: SUPI privacy issue in PLMN hosting NPN scenario 10

6.3.1 Key issue details 10

6.3.2 Security Threats 11

6.3.3 Potential security requirements 11

6.X Key Issue #X: <Key Issue Name> 11

6.X.1 Key issue details 11

6.X.2 Security threats 11

6.X.3 Potential security requirements 11

7 Solutions 11

7.Y Solution #Y: <Solution Name> 11

7.Y.1 Introduction 11

7.Y.2 Solution details 12

7.Y.3 Evaluation 12

8 Conclusions 12

Annex <X> (informative): Change history 13

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# 1 Scope

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

More specifically, this document:

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

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

# 2 References

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

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

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

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

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

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

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

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

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

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

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

<ABBREVIATION> <Expansion>

# 4 Overview

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

The focus of the study is divided into two parts:

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

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

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

The creation, modification, and termination of a Network Slice Instance (NSI) are supported by Management Services provided by the 5G management systems. Therefore, NFs which provide NSI Management Services may cross the operational domains between PNI-NPNs and PLMNs.

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.

Editor’s Note: Whether interface between customer’s AFs and 5G core network of this study is FFS,

Editor’s Note: Whether the management interface is in scope of this study is FFS.

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 premise is SBA interface. Examples of dedicated CP functions that are likely to be hosted by NPN in the customer premises are as below:

- AMF.

- SMF.

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

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

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

# 5 Security assumptions

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

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

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

# 6 Key issues

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

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

### 6.1.1 Key issue details

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

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

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

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

### 6.1.2 Security threats

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

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

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

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

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

### 6.1.3 Potential security requirements

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

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

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

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

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

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

### 6.2.1 Key issue details

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

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

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

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

### 6.2.2 Security threats

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

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

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

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

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

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

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

### 6.2.3 Potential security requirements

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

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

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

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

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

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

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

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

### 6.3.1 Key issue details

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

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

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

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

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

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

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

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

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

### 6.3.2 Security Threats

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

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

### 6.3.3 Potential security requirements

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

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

### 6.X.1 Key issue details

### 6.X.2 Security threats

### 6.X.3 Potential security requirements

# 7 Solutions

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

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

### 7.Y.1 Introduction

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

### 7.Y.2 Solution details

### 7.Y.3 Evaluation

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

# 8 Conclusions

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 |  | S3-240411 |  |  |  | Skeleton | 0.0.0 |
| 2024-03 | SA3#115 | S3-240977 |  |  |  | S3-240976, S3-240978, S3-240979, S3-240980, S3-240981, S3-241006, S3-241007 implemented | 0.1.0 |