|  |
| --- |
| 3GPP TR 33.858 V0.1.0 (2022-07) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of enhanced support of Non-Public Networks phase 2(Release 18) |
|   |
|  |  |
|  |
| 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.© 2022, 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

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Assumptions 7

5 Key issues 7

5.1 Key issue #1: Security of non-3GPP access for SNPN 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 8

5.X Key issue #X: <Title> 8

5.X.1 Key issue details 8

5.X.2 Threats 8

5.X.3 Potential security requirements 8

6 Proposed solutions 8

6.1 Mapping of solutions to key issues 8

6.A Solution #A: <Title> 8

6.A.1 Introduction 8

6.A.2 Solution details 8

6.A.3 System impact 8

6.A.4 Evaluation 9

7 Conclusions 9

Annex <A>: <Informative annex title for a Technical Report> 10

Annex X: Change history 10

# 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.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The aim of this work is to study the security aspects for any potential enhancements to be developed based on the outcome of the study in TR 23.700-08 [2]. For each of the objectives in the scope of the study in TR 23.700-08 [2], potential security aspects that are to be covered in this study are as follows:

- Support for enhanced mobility by enabling support for idle and connected mode mobility between SNPNs without new network selection.

- Study if existing security mechanisms for mobility between PLMNs can be reused for SNPNs or if new security mechanisms are needed.

- Support for non-3GPP access for SNPN

- Study if existing security mechanisms for enabling non-3GPP access in a PLMN can be reused for enabling non-3GPP access in an SNPN or if new security mechanisms are needed.

- Address new requirements (e.g., TS 22.261 [3] requirements for Providing Access to Local Services) related to NPN

- Study the trust model for the resulting architecture for enabling Localized Services via a local hosting NPN.

- Study if existing mechanisms for a UE to access an NPN can be reused for enabling a UE to authenticate with and access the local hosting NPN and the localized services via the hosting NPN with proper authorization, or if new security mechanisms are needed.

# 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 TR 23.700-08: "Study on enhanced support of Non-Public Networks; Phase 2".

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

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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].

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

Symbol format (EW)

<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 format (EW)

<ABBREVIATION> <Expansion>

# 4 Assumptions

This clause contains assumptions for the study. If there are no assumptions at the end of the study, the clause will be removed before sending for approval.

# 5 Key issues

## 5.1 Key issue #1: Security of non-3GPP access for SNPN

### 5.1.1 Key issue details

TR 23.700-08 [2] studies "Key Issue #2: Support of Non-3GPP access for SNPN". Clause 5.2.1 of TR 23.700-08 [2] states: *"Currently the 3GPP specifications do not support direct connection to SNPN via non-3GPP access networks"* and *"One objective of this key issue is to enable the 5GS to support direct connection of non-3GPP access networks to the SNPN's 5GC."*

The intention of this key issue is to study if existing security mechanisms for enabling non-3GPP access in a PLMN can be reused for enabling non-3GPP access in an SNPN, or if new security mechanisms are needed.

### 5.1.2 Threats

If non-3GPP access in an SNPN does not provide mutual authentication between UE and SNPN, it is possible to impersonate the UE or SNPN.

If communication between UE and SNPN via non-3GPP access is not confidentiality, integrity or replay-protected, it is possible to disclose, tamper or replay the communication.

### 5.1.3 Potential security requirements

The 5G system shall provide the means for UE and SNPN to mutually authenticate if non-3GPP access is used.

The 5G system shall provide the means to confidentiality, integrity and replay protect communication between UE and SNPN, if non-3GPP access is used.

Editor's Note: Threats and requirements for devices that are not UEs (e.g. FN-RG or N5GC device behind RG) are ffs.

## 5.X Key issue #X: <Title>

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Proposed solutions

## 6.1 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.A Solution #A: <Title>

### 6.A.1 Introduction

### 6.A.2 Solution details

### 6.A.3 System impact

### 6.A.4 Evaluation

# 7 Conclusions

Annex <A>:
<Informative annex title for a Technical Report>

Annex X:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e | S3-220957 |  |  |  | Skeleton | 0.0.0 |
| 2022-07 | SA3#107e AdHoc | S3-221674 |  |  |  | Version after incorporating changes from S3-221492 and S3-221681 | 0.1.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |