|  |  |
| --- | --- |
| 3GPP TR 33.857 V0.1.0 (2020-08) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on enhanced security support for Non-Public Networks;  (Release 17) | |
|  | |
|  |  |
|  | |
| 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.  © 2020, 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 4

Introduction 5

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 6

4 Architectural and security assumptions 7

4.1 Architectural requirements 7

5 Key issues 7

5.1 Key Issue #1 Credentials owned by an external entity 7

5.1.1 Key issue details 7

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key Issue #2 Provisioning of Credentials 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 9

5.3 Key Issue #3 Security impacts from supporting IMS voice and IMS services in SNPNs 9

5.3.1 Key issue details 9

3.2.2 Security threats 9

3.3.3 Potential security requirements 9

5.X Key Issue #X: <Key Issue Name> 9

5.X.1 Key issue details 9

5.X.2 Security threats 9

5.X.3 Potential security requirements 9

6 Solutions 9

6.0 Mapping of Solutions to Key Issues 9

6.Y Solution #Y: <Solution Name> 10

6.Y.1 Introduction 10

6.Y.2 Solution details 10

6.Y.3 System impact 10

6.Y.4 Evaluation 10

7 Conclusions 10

Annex A (informative): 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

The 5GS already supports certain specific features for Non-Public Networks, these are evolved in the architectural study documented in 3GPP TR 23.700-07[3], considering new functionality for Non-Public Networks. One of the main architectural changes in need of security enhancements are the allowance of credentials owned by a separate entity than a Standalone Non-Public Network. The other is onboarding and remote provisioning of non-USIM credentials to allow for a seamless setup of Non-Public Networks.

# 1 Scope

The present document …

# 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 33.501: "Security architecture and procedures for 5G System"

[3] 3GPP TR 23.700-07: "Study on enhanced support of non-public networks (Release 17)"

…

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

# 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].

**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> <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 Architectural and security assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

## 4.1 Architectural requirements

- Solutions are built on the 5G System security architectural principles as in TS 33.501 [2] and conclusions drawn in TR 23.700-07 [3], including flexibility and modularity for newly introduced functionalities.

# 5 Key issues

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

## 5.1 Key Issue #1 Credentials owned by an external entity

### 5.1.1 Key issue details

This Key Issue aims at addressing security implications introduced in solutions related to Key Issue #1 Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN in TR 23.700-07 [3].

TR 23.700-07 [3] contains numerous solutions addressing Key Issue #1, where some solutions rely on a AAA-S external to the SNPN, depicted in 5.Y.1-2, and others on an AUSF separated from the SNPN the UE is attempting to access, depicted in 5.Y.1-1. These architectural changes may have an impact on security architecture, for instance, primary authentication.

Editor’s note: The solutions depicted are preliminary and might expand or reduce based on SA2 conclusion.

Figure 5.Y.1-1: SNPN + PLMN

Figure 5.Y.1-2: SNPN + non-PLMN

The solution are to describe how authentication is done with credentials owned by an entity separate from the SNPN and how keys may be shared between an entity separate from the SNPN and the SNPN, considering trust relationship between the SNPN and the separate entity owing the credentials.

### 5.1.2 Security threats

Weak authentication procedures may allow attackers to impersonate the UE towards the SNPN or vice versa.

Sharing of keying material between the SNPN and an entity separate from the SNPN during the key establishment procedure where authentication and key agreement is the same, may imply that a third party can derive keys on its own.

### 5.1.3 Potential security requirements

- The UE and SNPN shall support network access authentication procedure with credentials owned by an entity separate from the SNPN.

## 5.2 Key Issue #2 Provisioning of Credentials

### 5.2.1 Key issue details

This Key Issue aims at addressing security implications introduced in solutions related to Key Issue #4 in TR 23.700-07 [3].

The objective of Key Issue #4 in TR 23.700-07 [3] is twofold, UE onboarding and then remote provisioning of non USIM credentials for SNPN. This Key Issue aims at treating the security implications related to the provisioning part.

Designing completely new protocols is not in scope of this key issue.

Editor’s note: other details are FFS.

### 5.2.2 Security threats

Unprotected provisioning of SNPN credentials may cause the SNPN credentials to be obtained or manipulated by on-boarding network.

### 5.2.3 Potential security requirements

FFS

## 5.3 Key Issue #3 Security impacts from supporting IMS voice and IMS services in SNPNs

### 5.3.1 Key issue details

This key issue aims to analyse the potential security impacts from supporting IMS voice and IMS services in SNPNs. In Rel-16 SNPNs do not support IMS emergency services but for Rel-17 its expected that the enabling of IMS and IMS services for SNPNs is to be studied.

UEs that are to be used in SNPN are currently not required to have IMS credentials. It needs to be studied especially how these UEs can authenticate with the network. This means that solutions that address UEs without IMS credentials are in scope of this key issue.

Architectural requirement: Solutions to this key issue need to describe how the security, especially authentication, of supporting IMS voice and IMS services in SNPN is to be addressed.

### 3.2.2 Security threats

If the UE and the network do not mutually authenticate, an attacker could either impersonate the network towards the UE or the UE towards the network.

### 3.3.3 Potential security requirements

The UE and the network shall mutually authenticate before granting access to IMS and IMS services.

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |
| --- | --- | --- | --- |
|  | Key Issues | | |
| Solutions | X | Y | Z |
| 1 |  |  |  |
| 2 |  |  |  |

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

### 6.Y.1 Introduction

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

### 6.Y.2 Solution details

### 6.Y.3 System impact

Editor’s Note: Each solution should clearly list which entities need new functionality and what functionality they need for the provided solution to work.

### 6.Y.4 Evaluation

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

# 7 Conclusions

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

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100-e | S3-201582 |  |  |  | TR Skeleton | 0.0.0 |
| 2020-08 | Sa3#100-e | S3-202068 |  |  |  | Version after incorporating changes from S3-202089, S3-202091, S3-202092, S3-202093 and S3-201925 | 0.1.0 |