|  |
| --- |
| 3GPP TR 33.858 V0.2.0 (2022-10) |
| 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 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Assumptions 8

5 Key issues 8

5.1 Key issue #1: Security of non-3GPP access for SNPN 8

5.1.1 Key issue details 8

5.1.2 Threats 8

5.1.3 Potential security requirements 9

5.2 Key issue #2: Authentication for UE access to hosting network 9

5.2.1 Key issue details 9

5.2.2 Threats 9

5.2.3 Potential security requirements 9

5.X Key issue #X: <Title> 9

5.X.1 Key issue details 9

5.X.2 Threats 9

5.X.3 Potential security requirements 9

6 Proposed solutions 10

6.0 Mapping of solutions to key issues 10

6.1 Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios 10

6.1.1 Introduction 10

6.1.2 Solution details 10

6.1.3 System impact 11

6.1.4 Evaluation 11

6.2 Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios 11

6.2.1 Introduction 11

6.2.2 Solution details 11

6.2.3 System impact 12

6.2.4 Evaluation 12

6.3 Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN 12

6.3.1 Introduction 12

6.3.2 Solution details 12

6.3.3 System impact 12

6.3.4 Evaluation 13

6.4 Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios 13

6.4.1 Introduction 13

6.4.2 Solution details 13

6.4.3 System impact 13

6.4.4 Evaluation 13

6.A Solution #A: <Title> 14

6.A.1 Introduction 14

6.A.2 Solution details 14

6.A.3 System impact 14

6.A.4 Evaluation 14

7 Conclusions 14

Annex <A>: <Informative annex title for a Technical Report> 15

Annex X: Change history 15

# 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".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[5] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"

…

[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].

For the purposes of the present document, the following terms and definitions given in TR 23.700-08 [2] apply:

**Local service, Localized service:** Service, which is localized (i.e. provided at specific/limited area) and/or can be bounded in time. The service can be realized via applications (e.g. live or on-demand audio/video stream, electric game, IMS, etc), or connectivity (e.g. UE to UE, UE to Data Network, etc.).

**Hosting network:** A network providing access to Local/Localized services.

## 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.

## 5.2 Key issue #2: Authentication for UE access to hosting network

### 5.2.1 Key issue details

The terms "localized service" and "hosting network" are explained in clause 3.1 of this document.

TR 23.700-08 [2] studies "Key Issue #3: Enabling NPN as hosting network for providing access to localized services" and "Key Issue #4: Enabling UE to discover, select and access NPN as hosting network and receive localized services".

The intention of this key issue is to study authentication of UE access to a hosting network, if existing security mechanisms can be reused or new security mechanisms are needed.

### 5.2.2 Threats

If the UE is not authenticated towards the network, it is possible to impersonate the UE.

If the network is not authenticated towards the UE, it is possible to impersonate the network.

### 5.2.3 Potential security requirements

The UE and the hosting network shall support mutual authentication between the UE and the network.

## 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

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |
| --- | --- | --- |
| Solutions | KI#1: Security of non-3GPP access for SNPN | KI#2: Authentication for UE access to hosting network |
| Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios | X |  |
| Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios | X |  |
| Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN | X |  |
| Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios | X |  |
|  |  |  |

##

## 6.1 Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios

### 6.1.1 Introduction

This solution addresses key issue #1.

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.*"

To access to SNPN via no-3GPP access, on the one hand, the UE may need to handle the new identity (e.g., onboarding SUCI/onboarding SUPI) and the new Registration Type (i.e. SNPN Onboarding) to N3IWF. On the other hand, the UE may use anonymous value SUCI during the registration procedure, which will result in N3IWF failing to locate KN3IWF to authenticate the identity of UE.

This solution is proposed to address the aforementioned problem and enables the UE to access SNPN via an untrusted non-3GPP access network.

### 6.1.2 Solution details

This solution reuses the untrusted non-3GPP access authentication procedure in PLMN scenarios in clause 7.2.1 of TS 33.501 [x] with the following modifications:

- In SNPN scenarios, if the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports SUPI privacy, then the UE can send an anonymous value SUCI to N3IWF based on configuration. And SNPN identifier, which consists of PLMN ID and NID, should also be included in AN parameters, which are sent to the N3IWF. Moreover, to fulfill the onboarding requirements, the UE may also send onboarding SUCI to the N3IWF.

- The AMF can choose 5G AKA, EAP-AKA', or any other key-generating EAP authentication method to authenticate UE as described in clause 6.1.3 or clause I.2.2 of TS 33.501 [4].

- If EAP-AKA' or key-generating EAP authentication method is used for authentication as described in clause 6.1.3.1 and clause I.2.2 of TS 33.501 [4], the AUSF shall include the EAP-Success in step 7.

Editor’s Note: The need for including SUPI privacy case is FFS.

### 6.1.3 System impact

TBD

### 6.1.4 Evaluation

TBD

## 6.2 Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios

### 6.2.1 Introduction

This solution addresses key issue #1.

Specifically, in SNPN scenarios, the UE may register for onboarding, therefore the UE needs to send new registration type to TNAN. Moreover, TNGF may need to leverage IDi to identify KTNGF, which can authenticate the identity of the UE. And IDi can be set as the SUCI/onboarding SUCI. However, in some cases, the UE may send anonymous value SUCI to TNGF in the registration request, making TNGF not able to locally link the identity of the UE with the corresponding KTNGF. Without the mapping between UE identity and KTNGF, TNGF cannot authenticate the identity of the UE.

To access to SNPN, on the one hand, the UE may provide the new identity (e.g. onboarding SUCI/onboarding SUPI) and the new Registration Type (i.e. SNPN Onboarding) to TNAN. On the other hand, the UE may use anonymous value SUCI during the registration procedure, which results in the consequence that TNGF cannot locate KTNGF to authenticate the identity of UE.

This solution enables the UE to access SNPN via trusted non-3GPP access network.

### 6.2.2 Solution details

This solution reuses the authentication mechanism in clause 7A.2.1 of TS 33.501 [4] with the following modifications.

- The UE may send SUCI/onboarding SUCI to the TNAP/TNGF. If the construction of SUCI as described in clause 6.12 of TS 33.501 [X] cannot be used and if the employed EAP method supports SUPI privacy, then the UE can send an anonymous value SUCI to TNAP/TNGF. If the UE indents to access SNPN, AN parameters should also include SNPN identifier, which consists of PLMN ID and NID. The authentication mechanisms could be 5G AKA, EAP-AKA’, and any other key-generating EAP authentication method as described in clause I.2 of TS 33.501 [X].

- For the IKE\_AUTH exchange part in step 13a of clause 7.2.1 of TS 33.501 [X], names in the ID payloads should correspond to the keys used to generate the AUTH payload. In case the UE utilizes the anonymous value SUCI in step 5, the UE shall initiate an IKE\_AUTH exchange and shall include the SUCI/onboarding SUCI in ID payloads rather than anonymous value SUCI. To help TNGF identify KTNGF, the AMF should send the newly generated KTNGF and the corresponding SUCI/onboarding SUCI to the TNGF. The AMF may obtain the SUCI/onboarding SUCI from the AUSF.

NOTE: The UE can only provide SUCI/Onboarding SUCI in case it is configured with SUPI privacy parameters.

Editor’s Note: The need for including SUPI privacy case is FFS.

Editor’s Note: The usage of Onboarding SUCI in step 13 for a non 3gpp access is FFS.

### 6.2.3 System impact

TBD

### 6.2.4 Evaluation

TBD

## 6.3 Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN

## 6.3.1 Introduction

This solution solves Key issue #1 in the case of using anonymous SUCI in trusted non-3GPP access.

When introducing non-3GPP access in SNPN it is assumed that most security procedures can be reused. However, the use of anonymous SUCI is only applicable to SNPNs so there are not yet any procedures specified for this case in relation to non-3GPP access.

In the current procedures for trusted non-3GPP access in clause 7A.2.1 of TS 33.501 [4], it is specified to use the SUCI/GUTI to map the user to the correct KTNGF in step 13. When using anonymous SUCI, this is not a good solution since an anonymous SUCI is not unique. Instead, another identifier is needed. This solution proposes to use a hash of the key KTNGF as identifier in case anonymous SUCI is used during the authentication towards the SNPN.

This solution defines adaptations of existing procedures needed to support the use of anonymous SUCI in trusted access for SNPN.

### 6.3.2 Solution details

Procedures in clause 7A.2.1 of TS 33.501 [4] are reused with the following exception:

- In step 13, if the construction of SUCI as described in clause 6.12 of TS 33.501 cannot be used, then a new type of identifier is used. The new identifier is proposed to be a hash of the key KTNGF. (potentially using some additional input). It is proposed to send the new identifier using the IDi payload.

It is already specified in section 3.5 of RFC 7296 [5] that the ID payload used for transport of IDi can be used to transfer a key identifier by setting the ID Type to ID\_KEY\_ID. Support of this ID Type is mandatory. The RFC does not specify how such a key identifier is generated. The proposal here is thus to use a hash of the key KTNGF potentially using some additional input to create a key identifier.

Editor's note: Use of anonymous SUCI in non-3GPP access is FFS

Editor's note: The complexity in the UE to manage two identifiers for the same non-3gpp access is FFS.

### 6.3.3 System impact

This solution has impact on UE and TNGF.

### 6.3.4 Evaluation

## 6.4 Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios

### 6.4.1 Introduction

This solution addresses key issue #1.

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*."

Devices that do not support 5GC NAS signalling over WLAN access (referred to as "Non-5G-Capable over WLAN" devices, or N5CW devices for short) may access 5GC in a SNPN via a trusted WLAN Access Network that supports a Trusted WLAN Interworking Function (TWIF).

This solution enables N5CW to access SNPN via trusted non-3GPP WLAN Access Network.

### 6.4.2 Solution details

For N5CW device in a PLMN, the authentication procedure only include EAP-AKA’, which is defined in clause 6.1.3.1 of TS 33.501 [4]. However, in SNPN scenarios, N5CW supports key-generating EAP authentication methods.

This solution reuses the authentication procedure in clause 7A.2.4 of TS 33.501 [4] with the following modifications.

- As described in clause I.2 of TS 33.501 [4], the authentication mechanisms utilized in step 8 of clause 7A.2.4 of TS 33.501 should include key-generating EAP authentication methods.

- N5CW sends UE identity (e.g. SUCI/on boarding SUCI) and AN parameters to the TWAP/TWIF. And SNPN identifier, which consists of PLMN ID and NID, should be included in AN parameters. Moreover, in SNPN scenarios, if the construction of SUCI as described in clause 6.12 of TS 33.501 cannot be used and if the employed EAP method supports SUPI privacy, the UE can send an anonymous value SUCI based on configuration.

- If the UE is accessing 5GS for Onboarding, the AN parameters sent from UE to TWAP /TWIF shall include Onboarding indication. And the Registration Type should set as "SNPN Onboarding".

- The TWIF shall create a 5GC Registration Request message on behalf of the N5CW device. The TWIF shall use UE identity, AN parameters, Registration Type that are receieved from N5CW.

Editor’s Note: Whether onboarding for N5CW devices is in scope is FFS.

Editor’s Note: The need for including SUPI privacy case is FFS.

### 6.4.3 System impact

TBD

### 6.4.4 Evaluation

TBD

## 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 |
| 2022-10 | SA3#108Adhoc-e | S3-223120 |  |  |  | Version after incorporating changes from S3-222931, S3-222965, S3-222990, S3-222931, S3-223118 | 0.2.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |