|  |  |
| --- | --- |
| 3GPP TR 33.887 V0.2.0 (2022-08) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security aspects for 5WWC Phase 2  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| 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.  © 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 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 7

4 Assumptions 7

5 Key issues 7

5.1 Key issue #1: Authentication of AUN3 device behind RG and supporting EAP 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

5.2 Key issue #2: Security aspect of slice information exposure of N3IWF/TNGF to UE 7

5.2.1 Key issue details 7

5.2.2 Threats 8

5.2.3 Potential security requirements 8

5.3 Key issue #3: Security aspect of slice information exposure of N3IWF/TNGF 8

5.3.1 Key issue details 8

5.3.2 Threats 8

5.3.3 Potential security requirements 8

6 Proposed solutions 8

6.0 Mapping of solutions to key issues 9

6.1 Solution #Y: EAP\_AKA prime based authentication for AUN3 devices 9

6.1.1 Introduction 9

6.1.2 Solution details 9

6.1.3 Evaluation 11

6.Y Solution #Y: <Title> 11

6.Y.1 Introduction 11

6.Y.2 Solution details 11

6.Y.3 Evaluation 11

7 Conclusions 11

Annex X: Change history 12

# 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 objectives of this study are to identify key issues, potential security and privacy requirements and solutions with respect to:

* Whether and how to identify, authenticate and authorize the Authenticable Non-3GPP devices behind the Residential Gateway (RG) connecting to the network.
* Whether and how to identify, authenticate and authorize the 3GPP devices (UE or N5CW devices) behind the Residential Gateway (RG) connecting to the network.
* Security aspects of supporting slice in 5WWC.

# 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 23700-17 "Study on the support for 5WWC, Phase 2"

[3] 3GPP TR 33.316 "Wireless and wireline convergence access support for the 5G System (5GS)"

# 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: Authentication of AUN3 device behind RG and supporting EAP

### 5.1.1 Key issue details

The AUN3 device is a non-3GPP device that does not support NAS over non-3GPP access, but it can be identified and/or authenticated by 5GC. For example, an AUN3 device may support EAP-AKA’, or does not support EAP based authentication but has a subscription with the 5GC.

This key issue considers AUN3 devices supporting EAP based authentication.

AUN3 devices supporting EAP can be connected to RG via WLAN or wireline. RG is connected to 5GC via 3GPP access or W-AGF as defined in TS 23.316[3] clause 4.10. Currently, authentication of these AUN3 devices is not sufficiently defined in 3GPP.

### 5.1.2 Threats

TBD.

### 5.1.3 Potential security requirements

TBD.

## 5.2 Key issue #2: Security aspect of slice information exposure of N3IWF/TNGF to UE

### 5.2.1 Key issue details

The solutions to KI #2 enable the selection of TNGF/N3IWF that support the S-NSSAI(s) required by the UE, as defined in 3GPP TR 23700-17[2]. Many solutions are presented, and one of the categories is:

* UE is able to discover the slice of TNGF/N3IWF and select TNGF/N3IWF accordingly.

Exposing the S-NSSAI information from the network nodes (TNGF/N3IWF) to any UE will cause privacy issues and should be studied.

### 5.2.2 Threats

If UE and network node exchanges interested slice information without any protection, then the MitM will be able to intercept what slices/services UE is interested in. Therefore, it will leak the privacy information of the UE..

.

### 5.2.3 Potential security requirements

The 5G system shall provide means to protect the slice information associated with the initial UE communication with the N3IWF/TNGF node.

## 5.3 Key issue #3: Security aspect of slice information exposure of N3IWF/TNGF

### 5.3.1 Key issue details

The solutions to KI #2 enable the selection of TNGF/N3IWF that support the S-NSSAI(s) required by the UE, as defined in 3GPP TR 23700-17[2]. Many solutions are presented, and one of the categories is.

* The UE chooses the default TNGF/N3IWF, and the network selects the appropriate TNGF/N3IWF based on UE slice requirements and relocates the TNGF.

The TR 23700-17 [2] few solutions, for example, solutions 10 and 11, include the IKE v2 procedure enhancement to relocate the TNGF. Security aspects of the solutions in this category should be studied.

### 5.3.2 Threats

TBD.

### 5.3.3 Potential security requirements

TBD.

# 6 Proposed 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

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

## 6.1 Solution #Y: EAP\_AKA prime based authentication for AUN3 devices

### 6.1.1 Introduction

This solution addresses the authentication of AUN3 devices based on the EAP\_AKA prime method.

### 6.1.2 Solution details

6.1.2.1 Procedure

 Figure 6.1.2.1-1: EAP-AKA prime based AUN3 authentication

1a. The AUN3 device establishes a WLAN connection with the WLAN Access Network (AN), using procedures specified in IEEE 802.11.

1b, 1c. L2 connection and EAP identity retrieval are performed. AUN3 device sends back its Network Access Identifier (NAI) in the form of username@realm.

Editor’s Note: Privacy protection for the UE identifier is FFS.

Editor’s Note: Details of SUCI calculation is FFS.

2a, 3a, 3b, 3c. If the RG is an FN-RG, the FN-RG sends the EAP response/Identity including the NAI to the W-AGF. The W-AGF creates a registration request on behalf of the AUN3 device with a new indication that the registration is on behalf of an AUN3 device where protection is required for the interface between the AUN3 device and RG. The SUPI of the AUN3 device is the NAI as received from the device, and the W-AGF constructs the SUCI from this SUPI using the NULL scheme. The W-AGF selects the AMF/SEAF.The W-AGF sends to the AMF/SEAF a registration request on behalf of the AUN3 device. The registration request includes the NAI SUCI, wireline network name if available, and the new indication. The same message content is forwarded from AMF to AUSF and then from AUSF to UDM.

2b, 3b, 3c. If the RG is a 5G-RG, the 5G-RG constructs a SUCI from the NAI-based SUPI of the AUN3 device and sends a NAS Registration Request message to the AMF, including the SUCI and the new indicator for encryption required for AUN3 device.

Editor’s Note: The need for the 5G-RG to create a SUCI using non-null-scheme is FFS.

4. Authentication procedure for EAP-AKA' is performed as defined in the section 6.1.3.1 of TS 33.501[2].

5. Based on the indication in step 3, AMF derives the WAGF key.

6. The AMF sends NAS Security Mode Command mode and provides the WAGF key to W-AGF.

7. W-AGF/RG derive the PMK key from the WAGF key.

Note: whether the PMK is derived by RG and W-AGF is out if 3GPP scope.

8. RG and AUN3 device will derive WLAN keys from PMK.

9. The AUN3 device performs a 4-way handshake to establish a secure connection with the WLAN AN.

Editorial Note: KEY derivation is FFS.

### 6.1.3 Evaluation

TBD

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

### 6.Y.1 Introduction

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

# 7 Conclusions

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

Annex X:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-07 | SA3#107e-AdHoc | S3-221341 |  |  |  | TR Skeleton (approved at SA3#107e-AdHoc) | 0.0.0 |
| 2022-07 | SA3#107e-AdHoc | S3-221703 |  |  |  | Inclusion of the documents approved at SA3#107e-AdHoc: S3-221636, S3-221637 S3-221638 | 0.1.0 |
| 2022-07 | SA3#107e-AdHoc |  |  |  |  | It removes the revision mark version from the zip file | 0.1.1 |
| 2022-08 | SA3#108-e | S3-222399 |  |  |  | Inclusion of the documents approved at SA3#108-e: S3-221767, S3-222395 | 0.2.0 |