|  |
| --- |
| 3GPP TR 33.xxx V1.0.0 (2021-05) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on non-seamless WLAN Offload in 5GS using 3GPP credentials;(Release 17) |
|   |
| *5G-logo_175px* | 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 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.© 2021, 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 3

Introduction 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 Architectural and security assumptions 7

5 Key issues 7

5.1 Key Issue #1: Support of EAP-AKA’ authentication for NSWO 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

6 Solutions 8

6.Y Solution #Y: <Solution Name> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 8

Annex A (informative): Change history 9

**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.

# 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

Editor’s Note: The text in this clause is not agreed, needs further alignment with feature description and background.

This document aims to study the security procedures necessary to support NSWO in 5GS maintaining security and privacy of users and 5GS network nodes.

In 4G, specifications allow Non-seamless WLAN Offload (NSWO), i.e. allow a UE to connect to a WLAN access network using SIM based access authentication via the mobile network core (as specified in TS 23.402 and in TS 33.402) and to offload selected traffic to the WLAN. This is a deployed feature in 4G networks and enables 4G UEs to connect e.g. to a Wi-Fi venue like a hotel or stadium using SIM based access authentication. This allows the use of mobile network subscription and roaming agreements for WLAN access and for offloading selected traffic to the WLAN where the selection of the traffic to offload is based on policies and where the offloaded traffic is not using 3GPP defined entities. The same feature support is missing so far in 5GS. This Rel-17 study tries to address this gap.

# 1 Scope

The scope of this study is to support Non-seamless WLAN Offload (NSWO) in 5GS. The following will be studied in this SID:

1. Solutions to support NSWO in 5GS
2. Procedures to support authentication methods for the respective solutions in objective.
3. Maintain privacy of subscription identifier similar to 3GPP/non-3GPP access to 5GC, even for NSWO authentication from WLAN.

SA2 positive feedback regarding the architectures for the selected solutions is required before they can proceed to normative phase.

# 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".

…

[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.

# 5 Key issues

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

## 5.1 Key Issue #1: Support of EAP-AKA’ authentication for NSWO5.1.1 Key issue details

For 5G access authentication, two authentication methods EAP-AKA’ and 5G AKA are supported over both 3GPP access and non-3GPP access. Currently the procedure in 3GPP TS 33.402 which are used for (4G) Non-Seamless WLAN Offload (NSWO) over trusted non-3GPP access in 23.402 foresees that the UE may send its IMSI in clear text, i.e. unencrypted, over that air interface and to the AAA server in the core network. To support NSWO for users with credentials defined in a 5GC, the NSWO authentication procedure needs to make use of credentials provided by the 5GC (i.e. by the UDM/ARPF in the 5GC). The new NSWO authentication procedures should also support the same or similar level of security and privacy as in 5GS, i.e. to never expose the IMSI/SUPI in the clear. Since the UEs may be provisioned by the operators to use EAP-AKA’, this may be the easiet authentication method to be adopted for 5G NSWO.

Currently installed WLAN APs support only EAP authentication framework over Radius or Diameter interface to an operator owned AAA. . Since the 5GC is able to support a unified authentication method, including EAP-AKA’ the same could be extended to support NSWO using the same credentials.

Reusing the same EAP-AKA’ infrastructure for the NSWO authentication can provide 5G equivalent authentication security to enterprise users as well.

### 5.1.2 Security threats

UEs need to be authenticated when they are connected to WLAN APs for availing NSWO, otherwise the NSWO could be misused by fraudulent UEs. Fraudulent UEs accessing enterprise WLAN without authentication can consume the WLAN resources and prevent the NSWO for legitimate UEs. This can cause DDoS scenarios for NSWO UEs.

If subscriber identity privacy is not available during authentication procedure, then tracking of the subscriber with “IMSI catchers” can lead to trackability and linkablity attacks.

### 5.1.3 Potential security requirements

The 5GS shall support EAP-AKA’ authentication method using 5GC credentials for NSWO.

# 6 Solutions

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

## 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 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** |
| 2021-05 | SA3#103-e | S3-211515 |  |  |  | TR Skeleton | 0.0.0 |
| 2021-05 | SA3#103-e | S3-212148, S3-212149, S3-212150 |  |  |  |  | 1.0.0 |