3GPP TR 33.807 V16.0.1 (2019-10)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on the security of the wireless and wireline convergence for the 5G system architecture

(Release 16)

** 

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 Report 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.

Keywords

5G, 5WWC, Wireless, Wireline, Convergence

***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.

© 2019, 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 [6](#__RefHeading___Toc22558912)

1 Scope [8](#__RefHeading___Toc22558913)

2 References [8](#__RefHeading___Toc22558914)

3 Definitions of terms, symbols and abbreviations [8](#__RefHeading___Toc22558915)

3.1 Terms [8](#__RefHeading___Toc22558916)

3.2 Symbols [9](#__RefHeading___Toc22558917)

3.3 Abbreviations [9](#__RefHeading___Toc22558918)

4 Security aspects of the 5WWC features in the 5G System [9](#__RefHeading___Toc22558919)

4.1 General [9](#__RefHeading___Toc22558920)

5 Key issues [9](#__RefHeading___Toc22558921)

5.1 Key Issue #1: security of 5G-RG [9](#__RefHeading___Toc22558922)

5.1.1 Key issue details [9](#__RefHeading___Toc22558923)

5.1.2 Security threats [9](#__RefHeading___Toc22558924)

5.1.3 Potential Security requirements [9](#__RefHeading___Toc22558925)

5.2 Key Issue #2: FN-RG authentication and authorization [10](#__RefHeading___Toc22558926)

5.2.1 Key issue details [10](#__RefHeading___Toc22558927)

5.2.2 Security threats [10](#__RefHeading___Toc22558928)

5.2.3 Potential security requirements [10](#__RefHeading___Toc22558929)

5.3 Key Issue #3: Transport security for the interfaces between W-5GAN and 5GC [10](#__RefHeading___Toc22558930)

5.3.1 Key issue details [10](#__RefHeading___Toc22558931)

5.3.2 Security threats [10](#__RefHeading___Toc22558932)

5.3.3 Potential security requirements [10](#__RefHeading___Toc22558933)

5.4 Key Issue #4: Security for the interface between 5G-RG and W-5GAN [11](#__RefHeading___Toc22558934)

5.4.1 Key issue details [11](#__RefHeading___Toc22558935)

5.4.2 Security threats [11](#__RefHeading___Toc22558936)

5.4.3 Potential security requirements [11](#__RefHeading___Toc22558937)

5.5 Key Issue #5: Registration and NAS transport for trusted non-3GPP access [11](#__RefHeading___Toc22558938)

5.5.1 Key Issue Details [11](#__RefHeading___Toc22558939)

5.5.2 Security threats [11](#__RefHeading___Toc22558940)

5.5.3 Potential security requirements [11](#__RefHeading___Toc22558941)

5.6 Key Issue #6: Access to 5GC from WLAN UEs that do not support NAS [11](#__RefHeading___Toc22558942)

5.6.1 Key Issue Description [11](#__RefHeading___Toc22558943)

5.6.2 Security threats [12](#__RefHeading___Toc22558944)

5.6.3 Potential security requirements [12](#__RefHeading___Toc22558945)

5.7 Key Issue #7: Authentication of 5G capable UE behind a RG [12](#__RefHeading___Toc22558946)

5.7.1 Key Issue details [12](#__RefHeading___Toc22558947)

5.7.2 Security Threats [12](#__RefHeading___Toc22558948)

5.7.3 Potential security requirements [12](#__RefHeading___Toc22558949)

5.8 Key Issue #8: User plane data handling for 5G capable UE behind a RG [12](#__RefHeading___Toc22558950)

5.8.1 Key issue details [12](#__RefHeading___Toc22558951)

5.8.2 Security Threats [12](#__RefHeading___Toc22558952)

5.8.3 Potential security requirements [13](#__RefHeading___Toc22558953)

5.9 Key Issue #9: User plane security for 5G-RG or FN-RG to 5GC [13](#__RefHeading___Toc22558954)

5.9.1 Issue details [13](#__RefHeading___Toc22558955)

5.9.2 Security Threats [13](#__RefHeading___Toc22558956)

5.9.3 Potential security requirements [13](#__RefHeading___Toc22558957)

5.10 Key Issue #10: NAS termination in Trusted WLAN Interworking Function (TWIF) [13](#__RefHeading___Toc22558958)

5.10.1 Key issue details [13](#__RefHeading___Toc22558959)

5.10.2 Security threats [14](#__RefHeading___Toc22558960)

5.10.3 Potential Security requirements [14](#__RefHeading___Toc22558961)

5.11 Key Issue #11: NAS termination for FN-RG [14](#__RefHeading___Toc22558962)

5.11.1 Key issue details [14](#__RefHeading___Toc22558963)

5.11.2 Security threats [14](#__RefHeading___Toc22558964)

5.11.3 Potential Security requirements [14](#__RefHeading___Toc22558965)

5.12 Key Issue #12: Protection of Line Id [14](#__RefHeading___Toc22558966)

5.12.1 Key Issue details [14](#__RefHeading___Toc22558967)

5.12.2 Security Threats [15](#__RefHeading___Toc22558968)

5.12.3 Potential security requirements [15](#__RefHeading___Toc22558969)

5.13 Key Issue 13: Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN) [15](#__RefHeading___Toc22558970)

5.13.1 Key issue details [15](#__RefHeading___Toc22558971)

5.13.2 Security threats [15](#__RefHeading___Toc22558972)

5.13.3 Potential Architecture requirements [15](#__RefHeading___Toc22558973)

5.14 Key Issue #14: Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN) [15](#__RefHeading___Toc22558974)

5.14.1 Key issue details [15](#__RefHeading___Toc22558975)

5.14.2 Security threats [16](#__RefHeading___Toc22558976)

5.14.3 Potential security requirements [16](#__RefHeading___Toc22558977)

5.15 Key Issue #15: N3GPP Key Separation [16](#__RefHeading___Toc22558978)

5.15.1 Key issue details [16](#__RefHeading___Toc22558979)

5.15.2 Security threats [17](#__RefHeading___Toc22558980)

5.15.3 Potential security requirements [17](#__RefHeading___Toc22558981)

5.16 Key Issue #16: Missing SUCI-to-SUPI mapping for the FN-RG [17](#__RefHeading___Toc22558982)

5.16.1 Key issue details [17](#__RefHeading___Toc22558983)

5.16.2 Security threats [17](#__RefHeading___Toc22558984)

5.16.3 Potential architectural requirements [17](#__RefHeading___Toc22558985)

6 Solutions [17](#__RefHeading___Toc22558986)

6.1 Solution #1: Solution for trusted non-3GPP access [17](#__RefHeading___Toc22558987)

6.1.1 Definitions [17](#__RefHeading___Toc22558988)

6.1.2 Abbreviations [17](#__RefHeading___Toc22558989)

6.1.3 Introduction [18](#__RefHeading___Toc22558990)

6.1.4 Solution details [18](#__RefHeading___Toc22558991)

6.1.5 Evaluation [20](#__RefHeading___Toc22558992)

6.2 Solution #2: 5GC-capable UEs behind 5G-RG/FN-RG using N3GPP-access solutions [21](#__RefHeading___Toc22558993)

6.2.1 Introduction [21](#__RefHeading___Toc22558994)

6.2.2 Solution details [21](#__RefHeading___Toc22558995)

6.2.3 Evaluation [21](#__RefHeading___Toc22558996)

6.2.3.1 Key issue #7 [21](#__RefHeading___Toc22558997)

6.2.3.1 Key issue #8 [21](#__RefHeading___Toc22558998)

6.3 Solution #3: 5G-RG connecting to 5GC via W-5GAN [22](#__RefHeading___Toc22558999)

6.3.1 Introduction [22](#__RefHeading___Toc22559000)

6.3.2 Solution details [22](#__RefHeading___Toc22559001)

6.3.3 Evaluation [22](#__RefHeading___Toc22559002)

6.4 Solution #4: FN-RG registration to 5GC [23](#__RefHeading___Toc22559003)

6.4.1 Introduction [23](#__RefHeading___Toc22559004)

6.4.2 Solution details [23](#__RefHeading___Toc22559005)

6.4.3 Evaluation [24](#__RefHeading___Toc22559006)

6.5 Solution #5: 5G-RG connecting to 5GC via NG-RAN (FWA) [24](#__RefHeading___Toc22559007)

6.5.1 Introduction [24](#__RefHeading___Toc22559008)

6.5.2 Solution details [24](#__RefHeading___Toc22559009)

6.5.3 Evaluation [25](#__RefHeading___Toc22559010)

6.6 Solution #6: Solution for 5GC access from WLAN UEs that do not support NAS [25](#__RefHeading___Toc22559011)

6.6.1 Introduction [25](#__RefHeading___Toc22559012)

6.6.2 Solution details [25](#__RefHeading___Toc22559013)

6.6.2.1 Definitions [25](#__RefHeading___Toc22559014)

6.6.2.2 Initial Registration & PDU Session Establishment [25](#__RefHeading___Toc22559015)

6.6.3 Evaluation [27](#__RefHeading___Toc22559016)

6.7 Solution #7: Key separation for untrusted and trusted access [28](#__RefHeading___Toc22559017)

6.7.1 Introduction [28](#__RefHeading___Toc22559018)

6.7.2 Solution details [28](#__RefHeading___Toc22559019)

6.7.2.0 General [28](#__RefHeading___Toc22559020)

6.7.2.1 Keys for trusted access [28](#__RefHeading___Toc22559021)

6.7.3 Evaluation [29](#__RefHeading___Toc22559022)

6.8 Solution #8: Transport security for the interfaces between W-5GAN and 5GC [29](#__RefHeading___Toc22559023)

6.8.1 Introduction [29](#__RefHeading___Toc22559024)

6.8.2 Solution details [29](#__RefHeading___Toc22559025)

6.8.3 Evaluation [30](#__RefHeading___Toc22559026)

6.9 Solution #9: Solution on Line ID protection [30](#__RefHeading___Toc22559027)

6.9.1 Introduction [30](#__RefHeading___Toc22559028)

6.9.2 Solution details [30](#__RefHeading___Toc22559029)

6.9.3 Evaluation [30](#__RefHeading___Toc22559030)

7 Conclusions [30](#__RefHeading___Toc22559031)

7.1 Conclusion on KI #1 [30](#__RefHeading___Toc22559032)

7.2 Conclusion on KI #2 [30](#__RefHeading___Toc22559033)

7.3 Conclusion on KI #3 [31](#__RefHeading___Toc22559034)

7.4 Conclusion on KI #4 [31](#__RefHeading___Toc22559035)

7.5 Conclusion on KI #5 [31](#__RefHeading___Toc22559036)

7.6 Conclusion on KI #6 [31](#__RefHeading___Toc22559037)

7.7 Conclusion on KI #7 [31](#__RefHeading___Toc22559038)

7.8 Conclusion on KI #10 [31](#__RefHeading___Toc22559039)

7.9 Conclusion on KI #11 [31](#__RefHeading___Toc22559040)

7.10 Conclusion on KI #12 [32](#__RefHeading___Toc22559041)

7.11 Conclusion on KI #14 [32](#__RefHeading___Toc22559042)

7.12 Conclusion on KI#15 [32](#__RefHeading___Toc22559043)

7.13 Conclusion on KI #16 [32](#__RefHeading___Toc22559044)

Annex A: Change history [33](#__RefHeading___Toc22559045)

# 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.

# 1 Scope

The scope of the present document is:

- Study for security between a 5G-RG and 5GC.

- Study for security for a 3GPP UE and non 3GPP UE behind a 5G-RG or a FN RG.

- Study for security for supporting legacy RG. The scope is limited based on the conclusion of the study in TR 23.716 [2].

- Study for security for trusted non-3GPP access.

- The privacy issues in the convergence architecture, if any.

# 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 23.716: "Study on the Wireless and Wireline Convergence for the 5G system architecture"

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[4] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[5] IETF RFC 2410: "The NULL Encryption Algorithm and Its Use With IPsec".

[6] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System"

[7] 3GPP TS 23.501: "System Architecture for the 5G System".

[8] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[9] IEEE 802.11i-2004: "Amendment 6: Medium Access Control (MAC) Security Enhancement".

# 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], TR 23.716 [2] 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].

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], TR 23.716 [2] 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].

# 4 Security aspects of the 5WWC features in the 5G System

## 4.1 General

To support Wireless and Wireline Convergence for the 5G system, two new network entities, 5G-RG and FN-RG, are introduced in the architecture.

5G-RG acts as a 5G UE in order to access 5GC reusing security procedure defined in TS 33.501 [3]. The scenario of UE behind 5G-RG accesses to the 5GC is also captured in the present document.

The security of FN-RG accessing to 5GC is studied in the present document. The scenario of UE behind FN-RG accesses to the 5GC is also captured in the present document.

For trusted non-3GPP access, the unified authentication framework is reused. Any potential security enhancements in addition to the security procedures defined in TS 33.501 [3] are captured in the present document.

# 5 Key issues

## 5.1 Key Issue #1: security of 5G-RG

### 5.1.1 Key issue details

5G RG is a new introduced entity in TR 23.716 [2] for 5WWC service. According to the definition of 5G RG, it is both a RG connecting to 5GC and some kind of relay for forwarding the messages from a 5GC capable UE behind it. Therefor the 5G RG has different functions in different scenarios.

This KI aims to define the security of 5G RG for adapting to different roles, such as how to run the authentication procedure, and how to make it secure

### 5.1.2 Security threats

5G RG is the critical part in 5WWC, if it is a faked, all the devices behind it could be hijack, and all the information is unsafe. From the core network point of view, a fake 5G RG connects to a 5GC, the resource of 5GC is wasted and could potentially be misused.

### 5.1.3 Potential Security requirements

5G RG shall be authenticated by the 5GC.

## 5.2 Key Issue #2: FN-RG authentication and authorization

### 5.2.1 Key issue details

Scenario 2 in TR 23.716 [2] describes how a legacy FN-RG without support of 3GPP procedures is connected to the 5GC via the W-5GAN. This key issue studies authentication and authorization aspects related to the FN-RG:

- The FN-RG does not support 3GPP protocols, so it cannot authenticate to the 5GC by EAP-AKA' or 5G AKA. It needs to be studied which entity authenticates the FN-RG and whether 3GPP nodes need to support further authentication methods.

- The Interworking function of the W-5GAN interfaces the 5GC using the 3GPP reference points N1, N2 and N3. Expressed differently, the W-5GAN sends NAS messages on behalf of the FN-RG. Authorization of the FN-RG by the W-5GAN may hence be needed.

- The FN-RG will use identifiers not specified in 3GPP, e.g. the line ID. It needs to be studied how these identifiers interplay with 3GPP identifiers such as SUPI, SUCI and PEI, especially in relation to authentication.

### 5.2.2 Security threats

If the FN-RG is not authenticated, an attacker may impersonate the FN-RG and hence gain access to the 5GC.

If the 5GC does not know whether the FN-RG is authenticated or not, the 5GC may provide service to an unauthenticated FN-RG which is a waste of resource. Besides, it is against on the 3GPP trust model if FN-RG connects to 5GC without checking the authentication result.

### 5.2.3 Potential security requirements

5GS shall have the knowledge whether the FN-RGs has been successfully authenticated by the wireline network.

## 5.3 Key Issue #3: Transport security for the interfaces between W-5GAN and 5GC

### 5.3.1 Key issue details

The scenarios described in clause 4.2.2 of TR 23.716 [2] introduce changes to existing interfaces (e.g. N2, N3), whose security implications need to be studied. This key issue studies the transport security, i.e. confidentiality, integrity and replay-protection, for the interfaces between W-5GAN and 5GC:

- W-5GAN – AMF (N2, in Scenario 2 also N1)

- W-5GAN – UPF (N3)

### 5.3.2 Security threats

Without protection, an attacker may eavesdrop on or manipulate or replay the communication on the interface.

### 5.3.3 Potential security requirements

Confidentiality protection, integrity protection and replay-protection shall be supported on the W-5GAN – AMF interface and the W-5GAN – UPF interface.

## 5.4 Key Issue #4: Security for the interface between 5G-RG and W-5GAN

### 5.4.1 Key issue details

The scenarios described in clause 4.2.2 of TR 23.716 [2] introduce a new interface between 5G-RG and W-5GAN. It is understood that this interface seems to be under the responsibility of BBF. However, the traffic via the W-5GAN is destined to 5GC and therefore can have a security impact to the 5GC.

This key issue studies the security, i.e. confidentiality, integrity and replay-protection, for the interface between 5G-RG and W-5GAN.

### 5.4.2 Security threats

Without protection, an attacker may eavesdrop on or manipulate or replay the communication on the interface. Lack of security measures may also have an impact on 5GC.

### 5.4.3 Potential security requirements

void

Note: he description of the interface is out of the scope of the present document.

## 5.5 Key Issue #5: Registration and NAS transport for trusted non-3GPP access

### 5.5.1 Key Issue Details

The following security aspects need to be investigated to enable trusted non-3GPP access to 5G Core Network:

- authentication procedures associated with the registration procedure for trusted non-3GPP access and the impact on the security procedures as applicable in the scope of SA WG3.

### 5.5.2 Security threats

Unauthenticated UEs shall not be able to register for normal service and access to the 5G core network, else several attacks are possible e.g. it could lead to issues on binding the subscription profile to the session and all related issues on charging/billing, access rights, QoS profile and slicing, etc. The UE could spoof any ID to hijack a subscription or UEs could try DoS attacks since the network would accept all UEs via the trusted non-3GPP connection.

### 5.5.3 Potential security requirements

A UE connecting to the 5G Core network via trusted non-3GPP access shall be authenticated.

## 5.6 Key Issue #6: Access to 5GC from WLAN UEs that do not support NAS

### 5.6.1 Key Issue Description

The following security aspects need to be investigated to enable UEs that do not support NAS to access via trusted non-3GPP (WLAN) access to the 5G Core Network:

Wireline access is not considered.

### 5.6.2 Security threats

Access of unauthenticated UEs to the 5G Core Network would allow several attacks, since the network does not know which UE is actually connecting to its core network, which leads to issues on binding the subscription profile to the session leading to all related issues on charging/billing, access rights, QoS profile and slicing. The UE could spoof any ID to hijack a subscription, or, UEs could try DoS attacks since the network would accept all UEs via the trusted non-3GPP connection.

### 5.6.3 Potential security requirements

UEs that do not support NAS over WLAN access and access to the 5G Core Network via trusted non-3GPP access shall be authenticated.

## 5.7 Key Issue #7: Authentication of 5G capable UE behind a RG

### 5.7.1 Key Issue details

Scenarios 3 and 5 in TR 23.716 [2] describe how a 5G capable UE behind a residential gateway (5G-RG or FN-RG) is connected to the 5GC. This key issue studies authentication aspects for 5G capable UEs behind residential gateways.

A 5G capable UE behind a RG (FN-RG or 5G-RG) can authenticate to the 5GC using 5G subscription credentials. It needs to be studied whether the authentication procedure needs to be adapted when the access is via a residential gateway (FN-RG or 5G-RG).

### 5.7.2 Security Threats

If authentication via a RG is not properly defined, there might be security flaws that enable an attacker to impersonate a UE.

### 5.7.3 Potential security requirements

A 5G capable UE behind a RG (FN-RG or 5G-RG) shall be able to authenticate to the 5GC.

NOTE: Any solution to this Key Issue different from usual 5G authentication needs strong motivation.

## 5.8 Key Issue #8: User plane data handling for 5G capable UE behind a RG

### 5.8.1 Key issue details

Scenarios 3 and 5 in TR 23.716 [2] describe how a 5G capable UE behind a residential gateway (5G-RG or FN-RG) is connected to the 5GC. This key issue studies user plane data handling for 5G capable UEs behind residential gateways.

For a UE behind a residential gateway (5G-RG or FN-RG), the user data may pass additional nodes compared to the situation for a usual 5G UE connected to 5GC. It needs to be studied whether different or additional security measures need to be taken.

### 5.8.2 Security Threats

Without confidentiality, integrity and replay protection, an attacker may eavesdrop on or manipulate or replay the user plane data.

### 5.8.3 Potential security requirements

User plane data of a 5G-capable UE behind a RG (FN-RG or 5G-RG) shall be forwarded via the RG in a manner that preserves data confidentiality, integrity and replay-protection.

For a *5G-capable* UE connecting to the 5G core network via a FN-RG or a 5G-RG, the 5GS shall provide a level of user plane security that is at least equal to the level provided to a UE connected via NG RAN.

The solution for user plane protection shall be compatible with local regulations.

## 5.9 Key Issue #9: User plane security for 5G-RG or FN-RG to 5GC

### 5.9.1 Issue details

In 5G, security of the user plane is provided from the 5G-capable UE to the 5GC by providing protection over the air interface between the UE and the gNB and using IPsec from the gNB to the core network. The user plane of a 5G-RG or a FN-RG that connects to a 5G core should therefore be protected equally well. Otherwise, UEs switching from the cellular network to the local WiFi network provided by the RG would suddenly be exposed to new threats.

Providing security at least equal to 4G was one of the main design goals of 5G security and should therefore be applied to 5WWC.

### 5.9.2 Security Threats

If the user plane from a RG to the 5GC is unprotected, the user plane is subject to the following threats:

- If not confidentiality protected, the user plane can be eavesdropped by an attacker.

- If not integrity protected, the user plane can be modified by an attacker.

### 5.9.3 Potential security requirements

- The user plane of a FN-RG or a 5G-RG to the 5GC shall provide a level of user plane security that is at least equal to the level provided to a UE connected via a gNB.

- The solution for user plane protection shall be compatible with local regulations.

## 5.10 Key Issue #10: NAS termination in Trusted WLAN Interworking Function (TWIF)

### 5.10.1 Key issue details

Solution #3 in clause 7.3 of TR 23.716 [2], is endorsed as a basis for normative specification for the scenario of connecting UEs, which do not support 5G NAS signalling over WLAN, to the 5GC via a trusted WLAN access network. This solution covers two types of UEs – 5G UEs that are not capable to operate as 5G UEs over a WLAN network and non-3GPP devices without any NAS capability.

In this solution, the responsibility of registering these UE's, terminating N1/NAS messages, enforcing NAS security etc. lies with the Trusted WLAN Interworking Function (TWIF). The TWIF function implements the NAS protocol stack and exchanges protected NAS messages with the AMF on behalf of the UEs.

The solution #3 specifies EAP framework as the basis for authenticating the UE over the trusted WLAN. After a successful authentication of the UE, the AMF receives the KAMF key from the SEAF and derives NAS signalling keys. It then goes on to activate the NAS security context with the TWIF.

The aim of this key issue is to study whether NAS security is required for this scenario, and if so, how NAS keys are generated in TWIF specific to the registering device (i.e. based on the identity of the device), and what, if any, changes are required in AMF.

### 5.10.2 Security threats

Not applicable.

### 5.10.3 Potential Security requirements

The NAS security to protect the UE, which do not support 5G NAS signalling over WLAN, shall be terminated between TWIF and AMF.

## 5.11 Key Issue #11: NAS termination for FN-RG

### 5.11.1 Key issue details

According to Solution #23 in clause #23 of TR 23.716 [2], which is endorsed as a basis for normative specification for the scenario of connecting FN-RG to the 5G core, the FAGF function in W-5GAN authenticates the FN-RG when a connection is established between FN-RG and the FAGF before registering FN-RG to 5GC on behalf of the FN-RG. In addition, the FAGF indicates to the AMF that it has authenticated the FN-RG and therefore no authentication is to be performed by the 5GC during registration of the FN-RG.

In 5G, the AMF receives the UE-specific KAMF key at the end of a successful authentication run. The KAMF key then forms the basis for derivation of the keys required for NAS signalling. Since authentication is skipped for FN-RG, there the current procedure needs an update to trigger derivation of NAS keys in the AMF. Similar issue exists for generation of NAS signalling keys in the FAGF.

This key issue is to study whether NAS security is needed for this scenario, and if so .how it is established between the AMF and the FAGF, given the constraints described above.

### 5.11.2 Security threats

Not applicable

### 5.11.3 Potential Security requirements

The NAS security shall be terminated between W-AGF and AMF.

## 5.12 Key Issue #12: Protection of Line Id

### 5.12.1 Key Issue details

SA2 has endorsed Solution #23 and Solution #28 in clauses 6.23 and 6.28 respectively of TR 23.716 [2] as the basis for normative work for the scenario of connecting legacy RG (FN-RG) to the 5G core (clause 8.2.11 of TR 23.716 [2]).

In TR 23.716 [2], the Line Id has been suggested as a possible identifier for legacy gateways (FN-RGs).

Solution #23 specifies a procedure for registration and session management of FN-RG via W-5GAN. Solution #28 specifies the use of Line ID as an input to generate a SUPI/SUCI for the given FN-RG. The SUCI, thus generated, is sent by the FAGF to the AMF in the NAS registration request it builds on behalf of the RG. The SUCI is also expected to include other parameters such as Home Network Identifier of the operator owning the FN-RG.

According to Solution#28 in TR 23.716 [2]:

"In case of FN-RG the AGF provides the Line Id within the SUCI put in the NAS registration request it builds on behalf of the RG and it sends to the AMF. This solution assumes that the AGF ensures that the Line Id information it provides to the AMF is accurate" (The AGF is part of the W-5GAN.)

However, the format of the SUCI based on Line Id is not specified nor is it specified if the Line Id is to be concealed (like the SUPI).

This key issue studies whether the Line Id needs to be concealed. The following aspects could be considered:

a) SUPI concealment, introduced in Rel-15, is a privacy mechanism for mitigating traceability of subscribers by using SUCI over-the-air. For the FN-RG the Line Id is transferred from the W-5GAN to the AMF over a backhaul interface (i.e., not over-the-air).

b) Alignment of non-IMSI identifiers with the SUPI/SUCI solution.

c) Protection of the interface between W-5GAN and 5GC, see Key issue #3 "Transport security for the interfaces between W-5GAN and 5GC".

d) Possible threats regarding Line Id tampering on the interface between W-5GAN and 5GC.

e) User privacy effects on human users behind FN-RG.

### 5.12.2 Security Threats

Not applicable.

### 5.12.3 Potential security requirements

Not applicable.

NOTE: This interface is already protected by other means.

## 5.13 Key Issue 13: Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN)

### 5.13.1 Key issue details

In TR 23.716 [2], it has been concluded that mobility between TNAPs within the same Trusted Non-3GPP Access Network Gateway Function (TNGF-CP) is supported. The purpose of this key issue is to study:

a) The security protocol needed for intra-TNGF mobility.

b) How to generate the keys needed for mobility.

### 5.13.2 Security threats

Not applicable.

### 5.13.3 Potential Architecture requirements

Security for intra-TNGF mobility shall be supported.

## 5.14 Key Issue #14: Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN)

### 5.14.1 Key issue details

To facilitate inter-TNGF mobility within the TNAN, Tn interface is introduced between TNGFs in Solution #1 in clause 7.1 of TR 23.716 [1]. This is used for mobility between TNGFs.

When the inter-TNGF mobility procedure is executed, Tn interface is used to transfer the UE context and the NWt connections to a new TNFG-CP (the target TNGF-CP). The UE context includes the GUAMI of the serving AMF, the EAP re-authentication root key (used for intra-TNGF mobility), information about the established PDU sessions, etc.

Note: This scenario is out of scope in the present document.

### 5.14.2 Security threats

Without protection of the Tn interface, an attacker may eavesdrop on Tn to obtain sensitive information such as ERP key or manipulate data on the interface for malicious purposes.

### 5.14.3 Potential security requirements

Confidentiality protection, integrity protection and replay-protection shall be supported on the Tn interface between two TNGFs within the TNAN.

## 5.15 Key Issue #15: N3GPP Key Separation

### 5.15.1 Key issue details

This Key Issue addresses aspects in scope of 3GPP. Aspects in scope of BBF are not addressed.

In 5G Rel-15, security for untrusted N3GPP access was specified. For Rel-16, two more variants of N3GPP access are endorsed for normative work in TR 23.716 [2]:

1) Trusted non-3GPP access, similar to the untrusted case, but not identical. The solution concluded for normative work is described in clause 7.1.3.3 of TR 23.716 [2].

2) 5G-RG connecting to a W-5GAN, where the 5G-RG acts as a UE and the W-5GAN acts as non-3GPP access.

Untrusted N3GPP access as specified in 5G Rel-15 uses an access node key, KN3IWF. The new types of N3GPP accesses may need similar keys.

In the Rel-15 solution for untrusted N3GPP access, the key KN3IWF is used to setup IPSec SAs. The key relations (not a key hierarchy) for untrusted access is illustrated in Figure 5.15.1-1. The KN3IWF is used to setup the IP Sec SA used for Control plane data (encryption and integrity). From this SA, further Child SAs are derived for user plane protection (encryption and integrity).

Note that the key KN3IWF is used to authenticate the UE and N3IWF during the IP Sec SA setup. The actual keys used for CP-signalling and UP-data are negotiated using Diffie-Hellman and not derived from KN3IWF.



Figure 5.15.1-1: Rel-15 Key relations for untrusted N3GPP access. Note that this is not a key hierarchy. Instead the key negotiation for the IPSec SA is authenticated using the key KN3IWF.

According to the solution endorsed in TR 23.716 [2] for trusted N3GPP access, the access node key KTNGF is derived by the AMF and sent to the TNGF (similar to the solutions for KN3IWF). This key is used to setup IPSec SAs in a similar way as for untrusted access, with the exception that no encryption is used, only integrity protection. According to the solution, another type of keys for WLAN encryption (TNAP keys) are also derived from the KTNGF.

### 5.15.2 Security threats

If one access node key is used for different purposes i.e. the key used for IPsec protection and the key used between UE and AP, there is a risk that one node type can pose as another.

### 5.15.3 Potential security requirements

The key used for IPsec protection and between UE and TNAP shall be cryptographic separated.

## 5.16 Key Issue #16: Missing SUCI-to-SUPI mapping for the FN-RG

### 5.16.1 Key issue details

During registration of an FN-RG, the home network may need to map the SUCI of the FN-RG to the corresponding SUPI. A procedure how to perform this mapping needs to be specified.

Architectural requirement: Solutions to this key issue should describe how the home network performs mapping of the SUCI of an FN-RG to the corresponding SUPI.

### 5.16.2 Security threats

Not applicable

### 5.16.3 Potential architectural requirements

The 5G system shall support mapping of the FN-RG's SUCI to SUPI by the home network.

# 6 Solutions

## 6.1 Solution #1: Solution for trusted non-3GPP access

### 6.1.1 Definitions

**- Trusted Non-3GPP Access Network (TNAN):** a TNAN is an access network that employs an access technology not specified by 3GPP (e.g. WLAN) and can connect to 5GC by exposing north-bound interfaces compliant with N2/N3. Is deployed and managed either (a) by a 5G mobile operator or (b) by a third-party who is trusted by the 5G mobile operator. How trust is established between a third-party and a 5G mobile operator is currently not considered in the present document.

- **Trusted Non-3GPP Access Point (TNAP):** The TNAP enables UEs to access the TNAN by using a non-3GPP wireless or wired access technology. In case of an IEEE 802.11 [4] WLAN, the TNAP corresponds to a WLAN access point. A TNAP terminates the UE's IEEE 802.11 [4] link defined in IEEE Std 802.11 [4].

**- Trusted Non-3GPP Gateway Function (TNGF):** The TNGF exposes the N2/N3 interfaces and enables the UE to connect to 5GC over a non-3GPP access technology. The TNGF is functionally split into a control-plane function, referred to as TNGF-CP, and to a user-plane function, referred to as TNGF-UP. The interface between these functions is not defined.

### 6.1.2 Abbreviations

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

### 6.1.3 Introduction

The UE registers to 5GC and, at the same time, it authenticates with the TNAN by using the EAP-based procedure, which is essentially the same with the registration procedure for untrusted non-3GPP access. The link between the UE and the TNAN can be any data link (L2) that supports EAP encapsulation. The interface between the TNAP and TNGF-CP is an AAA interface. The TNGF terminates the EAP-5G signalling and behaves as authenticator when the UE attempts to register to 5GC via the TNAN. The security relies on Layer-2 security between UE and TNAP, which is a trusted entity so that no IPSec encryption would be necessary between UE and TNGF, i.e. NULL encryption is sufficient for the user plane and signalling.

Separate IPSec SAs may be used for NAS transport and PDU Sessions. At the end of the UE's registration to 5GC, an IPSec SA (NWt-cp) is established between the UE and TNGF. This is used to protect NAS messages between the UE and TNGF-CP. Later when the UE initiates a PDU session establishment, the TNGF initiates establishment of one or more IPSec child SAs per PDU session. This results in additional IPSec SA's (NWt-up) to be setup between the UE and TNGF-UP which are then for user plane transport between the two.

The main advantage of using IKEv2/IPsec is that it makes the solution for trusted non-3GPP access almost identical with the solution for untrusted non-3GPP access specified in TS 33.501 [3]. Thus, the UE can use the same protocols and procedures for both trusted and untrusted non-3GPP access and the TNGF can become very similar to N3IWF.

### 6.1.4 Solution details

The solution is the same as the specified procedure in TS 23.502 [8] clause 4.12a.2.2 "Registration procedure for trusted non-3GPP access" with the difference that here the PDU session establishment procedure (steps 16 – 19) is shown in addition.



Figure 6.1.4-1: Registration \ Authentication and PDU Session establishment for trusted non-3GPP access

1. A layer-2 connection is established between the UE and the TNAP. In case of IEEE 802.11 [4], this step corresponds to an 802.11 [4] Association. In case of PPP, this step corresponds to a PPP LCP negotiation. In other types of non-3GPP access (e.g. Ethernet), this step may not be required.

2-3. An EAP authentication procedure is initiated. EAP messages are encapsulated into layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc. The UE provides a NAI that triggers the TNAP to send an AAA request to a TNGF-CP, which operates as an AAA proxy. Between the TNAP and TNGF-CP the EAP packets are encapsulated into AAA messages.

4-10. An EAP-5G procedure is executed as specified in TS 33.501 [3], clause 7.2.1with the following modifications:

- The EAP-5G packets are not encapsulated into IKEv2 packets.

- A TNGF key and a TNAP key (instead of an N3IWF key) is created in the UE and in the AMF and TNGF-CP respectively after the successful authentication. The TNGF key is transferred from the AMF to TNGF-CP in step 10a (within the N2 Initial Context Setup Request). The TNGF-CP generates the TNAP key and transfers it from TNGF-CP to TNAP in step 10b (within an AAA message). In case of trusted WLAN access, the TNAP key corresponds to the Pairwise Master Key (PMK) and can be derived from the TNGF key, e.g. by using the first 32 bytes of the TNGF key.

- In step 9b the UE receives the "TNGF Contact Info" which includes the IP Address of TNGF-CP to which NAS signalling should be sent.

11. The common TNAP key is used by the UE and TNAP to derive security keys according to the applied non-3GPP technology and to establish a security association to protect all subsequent traffic. In case of IEEE 802.11 [4], the TNAP key is the Pairwise Master Key (PMK) and a 4-way handshake is executed (see IEEE 802.11 [4]) which establishes a security context between the WLAN AP and the UE that is used to protect unicast and multicast traffic over the air. All messages between UE and TNAP are encrypted and integrity protected from this step onwards.

12. The UE receives IP configuration from the TNAN, e.g. with DHCP.

13. The UE initiates an IKE\_INIT exchange with the TNGF. The UE has received the IP address of TNGF during the EAP-5G signalling in step 9b, subsequently, the UE initiates an IKE\_AUTH exchange and provides its SUPI or 5G-GUTI identity. The common TNGF key is used for mutual authentication. NULL encryption is negotiated as specified in RFC 2410 [5]. After step 13c, an IPsec SA is established between the UE and TNGF (i.e. a NWt-cp connection) and it is used to transfer all subsequent NAS messages. This IPsec SA does not apply encryption but only apply integrity protection.

14. After the NWt-cp connection is successfully established, the TNGF responds to AMF with an N2 Initial Context Setup Response message.

15. Finally, the NAS Registration Accept message is sent by the AMF and is forwarded to UE via the established NWt-cp connection.

16-18. The UE initiates a PDU session establishment. This is carried out exactly as specified in TS 23.502 [8] clause 4.12.5. The TNGF may establish one or more IPSec child SA's per PDU session.

19. User plane data for the established PDU session is transported between the UE and TNGF-UP inside the established IPSec child SA.

### 6.1.5 Evaluation

The solution fulfils the potential security requirements from Key Issue #5: "Registration and NAS transport for trusted non-3GPP access" and is the same as the specified procedure in TS 23.502 clause 4.12a.2.2 "Registration procedure for trusted non-3GPP access" with the difference that here the PDU session establishment procedure is shown in addition.

The security relies on Layer-2 security between UE and TNAP (security context to encrypt and integrity protect unicast and multicast traffic over the air), which is a trusted entity so that no IPSec encryption would be necessary between UE and TNGF, i.e. NULL encryption is sufficient for the user plane and signalling.

Separate IPSec SAs with NULL encryption is sufficient for NAS transport and PDU Sessions:

- At the end of the UE's registration to 5GC, an IPSec SA (NWt-cp) is established to protect NAS messages between the UE and TNGF-CP.

- At PDU session establishment, the TNGF initiates establishment of one or more IPSec child SAs per PDU session. This results in additional IPSec SA's (NWt-up) to be setup between the UE and TNGF-UP which are then for user plane transport between the two.

## 6.2 Solution #2: 5GC-capable UEs behind 5G-RG/FN-RG using N3GPP-access solutions

### 6.2.1 Introduction

This solution addresses key issues #7 and #8.

In the following, when the term RG is used, it can mean either FN-RG or 5G-RG.

### 6.2.2 Solution details

This solution aims to construct a security solution based on Solution #11 for WWC in TR 23.716 [2]. Solution #11 for WWC in TR 23.716 [2] reuses the Rel-15 solution for untrusted N3GPP access in combination with Solution#1 for trusted network in TR 23.716 [2].

The main idea of Solution #11 for WWC in TR 23.716 [2] is that the RG and W-5GAN act as untrusted/trusted N3GPP access towards 5GC-capable UEs behind the RG.

The suggested reference architecture from Solution #11 for WWC in TR 23.716 [2] is provided in Figures 6.11.1-1 and 6.11.1-2 in TR 23.716 [2].

Solution #11 for WWC in TR 23.716 [2] provides the following options:

1. A 5GC-capable UE behind an FN-RG uses Untrusted N3GPP-access as defined in Rel-15.

2. A 5GC-capable UE behind a 5G-RG can use either untrusted N3GPP-access as defined in Rel-15, or trusted N3GPP-access as studied in TR 23.716 [2]. When choosing the trusted solution, the 5G-RG needs to be be trusted.

Further, Solution #11 for WWC in TR 23.716 [2] also suggests some additional features that are out of scope for SA3 work: co-location of the W-5GAN, UPF (for W-5GAN user plane) and IWF to support different scenarios such as QoS.

The suggested solution for trusted N3GPP access, which is also adopted as preliminary conclusion in TR 23.716 [2], reuses the procedures for non-trusted N3GPP access as much as possible. The security of the solution is discussed in Solution #1 of the present document.

### 6.2.3 Evaluation

#### 6.2.3.1 Key issue #7

Key issue #7 in this study is about authentication of a UE behind a RG. This solution addresses this using either the Rel-15 procedures for untrusted N3GPP access or new Rel-16 procedures for trusted N3GPP access.

For the untrusted case, the UE authentication is already described in Rel-15.

Provided that the solution for trusted access is deemed secure, the solutions solves this key issue.

#### 6.2.3.1 Key issue #8

Key issue #8 in this study is about user plane data for a UE behind a RG. The solution addresses this by tunnelling the UE's user data through the access nodes' user data plane.

For the untrusted case, the UE user data is protected between the UE and IWF with a child SA negotiated during the authentication as specified in Rel-15.

For the trusted case, Solution #1 for trusted network in TR 23.716 [2] suggests reusing this solution (using child SAs) to align with the untrusted case and because it provides smooth management of QoS parameters. However, Solution #1 for trusted network in TR 23.716 [2] suggests using null-encryption and provide authentication/integrity protection only.

The claim to use null encryption can be justified because there is hop-by-hop protection of data between the UE and the IWF. Hop-by-hop security can be achieved by the following:

1) Between UE and 5G-RG, level-2 encryption is used (WLAN or similar).

2) The interface between 5G-RG and W-5GAN, is to be handled by solutions for key issue #4 in the present document.

3) Since the UE's user data is tunnelled over the W-5GAN user data plane, it is protected from eavesdropping and manipulation between the W-5GAN and the IWF.

Given that a solution is provided for key issue #4, either by BBF methods or 3GPP methods, hop-by-hop security is achieved, which might exclude the need for IPSec encryption between UE and IWF.

However, it can be argued that using IPSec with null-encryption does not provide a major performance gain (compared to using encryption) since authentication/integrity protection is still needed. (RFC states that both encryption and authentication cannot be nullified).

## 6.3 Solution #3: 5G-RG connecting to 5GC via W-5GAN

### 6.3.1 Introduction

This solution addresses KI #1.

### 6.3.2 Solution details

This solution captures the security aspects of Solution #3 for WWC in TR 23.716 [2]. In Solution #3, the 5G-RG acts as the 3GPP UE and supports N1. The FAGF function in the W-5GAN acts as a 5G AN and supports N2 and N3.

The Untrusted non-3GPP access procedure defined in Rel-15 is used as the basis for the registration of 5G-RG when 5G-RG is connecting to the 5GC via the W-5GAN.

As the 5G-RG is a UE from 5GC point of view, the authentication framework defined in subclause 6.1.3 of 33.501 [3] shall be used to authenticate the 5G-RG.s.

Note: Any additional security between the FAGF and 5G-RG for transport of N1 messages that is needed to bring the level of protection of N1 messages to the equivalent in 5G is outside the scope of 3GPP. However, without such protection, the security level for accessing 5GC, especially in hybrid access scenario, cannot be guaranteed.

### 6.3.3 Evaluation

The solution is to address the potential security requirement in KI #1 which is that the 5G-RG shall be authenticated by the 5GC.

The 5G-RG is a UE from the 5GC point of view and SA2 has mandated the use of the Untrusted non-3GPP access procedure defined in TS 33.501 [3] as the basis for the registration of the 5G-RG with the 5GC.

This solution proposes use of the authentication framework defined in TS 33.501 clause 6.1.3 for authenticating 5G-RG. This fulfils the requirement in KI #1.NOTE: The outstanding issue is whether a key equivalent to KN3IWF is needed and how to protect between 5G-RG and W-AGF. This needs BBF's input.

## 6.4 Solution #4: FN-RG registration to 5GC

### 6.4.1 Introduction

This solution addresses key issues #2 and #11.

This solution specifies registration procedure for FN-RG. The FN-RG connects to 5GC via W-5GAN, which has the FAGF function that provides connectivity to the 5GC via N2 and N3 reference points. Since the FN-RG is a non-wireless entity defined by the BBF, it doesn't support NAS signalling. The FAGF provides N1 connectivity on behalf of the FN-RG.

### 6.4.2 Solution details



**Figure 6.4.2-1: Registration call flow for FN-RG**

1. A layer-2 (L2) connection is established between the FN-RG and the FAGF function in the W-5GAN.

2. The FN-RG is authenticated by the W-5GAN. Authentication method used for FN-RG is defined by BBF and out of scope of 3GPP.

It is assumed that there is a trust relationship between the wireline operator that manages the W-5GAN and the PLMN operator managing the 5GC.

3-4. The FAGF performs initial registration on behalf of the FN-RG. It generates a Registration Request NAS message on and sends it the AMF in 5GC over N2. The W-5GAN sends a registration request to the AMF on behalf of the FN-RG. It contains the SUCI of the FN-RG (or rather the SUCI used by the W-5GAN to uniquely identify the FN-RG).

The message includes SUCI, and it also contains an indication that the W-5GAN has authenticated the FN-RG.

5. The AMF selects an AUSF based on the received SUCI. The AMF sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the FN-RG. It also contains an authentication indication received from the W-5GAN which means the W-5GAN has authenticated the FN-RG.

6. The AUSF sends a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the FN-RG and the indication that the W-5GAN has authenticated the FN-RG.

7. The UDM invokes the SIDF and maps the SUCI to the SUPI.

8. The UDM decides using the authentication profile of the SUPI and the indication about authentication by the W-5GAN that authentication by the home network is not required.

9. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF. It contains the SUPI of the FN-RG. It also contains an indication that authentication by the home network is not required.

10. The AUSF sends a Nausf\_UEAuthentication\_Authenticate Response to the AMF. It contains the SUPI of the FN-RG. It also contains the indication that authentication by the home network is not required from the UDM. The AUSF skips authentication and sends a Nausf\_UEAuthentication\_Authenticate Response to the AMF. This response from AUSF indicates that authentication is not required, but no Kseaf is included. The response contains the deconcealed SUPI.

11. NAS security between AMF and W-5GAN is established similar to unauthenticated emergency calls, i.e. with NULL encryption and NULL integrity protection.

12. The AMF sends Registration Accept message to the FAGF. This message contains 5G-GUTI and other parameters.

13. The FAGF sends a Registration Complete message back to the AMF. The FAGF shall stores the 5G-GUTI for use in later NAS procedures.

### 6.4.3 Evaluation

The solution fulfils the potential security requirement from Key Issue #2: "FN-RG authentication and authorization" and is the same as the specified procedure in TS 23.502 clause 7.2.1.3 "FN-RG Registration via W-5GAN.

The FAGF in the W-5GAN authenticates the FN-RG and informs AMF that authentication of the FN-RG is done when it initiates registration of FN-RG. The AMF trusts the W-5GAN based on mutual authentication executed when security is established on the interface between the two using NDS/IP or DTLS. Based on this trust, the AMF forwards the "authentication done" indication to the AUSF. AUSF skips authentication of the FN-RG.

## 6.5 Solution #5: 5G-RG connecting to 5GC via NG-RAN (FWA)

### 6.5.1 Introduction

This solution addresses KI #1 - "security of 5G-RG".

### 6.5.2 Solution details

This solution captures the security aspects of Solution #19 for WWC in TR 23.716 [2].

When a 5G-RG connects to 5GC only via NG-RAN, it plays the role of a UE with regard to the 5GC. It exchanges N1 signalling with 5GC.

The 5G-RG is assumed to be equipped with UICC where the IMSI resides. If provisioned by the home operator, the 5G-RG shall store the Home Network Public Key required for concealing the SUPI, which is based on the IMSI.

Solution #19 in TR 23.716 reuses existing registration management procedures defined in TS 23.502 [8] clause 4.2.2 to register the 5G-RG with the 5GC.

Authentication of the 5G-RG is based on the existing procedures described in TS 33.501 [3].

The 5G-RG shall support all the security requirements and features defined in TS 33.501 [3].

### 6.5.3 Evaluation

The solution fulfils the requirement of KI#1 that 5G-RG shall be authenticated by the 5GC in case of connecting to 5GC via NG-RAN.

Since 5G-RG plays the role of the UE to the 5GC, it authenticates with the 5GC based on authentication procedures defined in TS 33.501.

## 6.6 Solution #6: Solution for 5GC access from WLAN UEs that do not support NAS

### 6.6.1 Introduction

This solution addresses the key issue#6 "Access to 5GC from WLAN UEs that do not support NAS".

### 6.6.2 Solution details

#### 6.6.2.1 Definitions

**"Non-5G-capable over WLAN" UE:**

- is capable to register to 5GC and to establish 5GC connectivity via a trusted WLAN access network

- is not capable to operate as 5G UE over a WLAN access network

- may be capable to operate as a 5G UE over NG-RAN

- may be without any NAS capability at all

**Trusted WLAN Access Point (TWAP):** It provides a point-of-access to the WLAN access network. This function is outside the scope of 3GPP but mentioned for completeness.

**Trusted WLAN Interworking Function (TWIF):** It provides interworking functionality that enables connectivity with 5GC. The TWIF supports the following functions:

- Terminates the N1, N2 and N3 interfaces.

- Implements the AMF selection procedures specified in TS 23.501 [7].

- Implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the UE.

- On the user plane, it relays protocol data units (PDUs) between the Yw connection and the N3 connection. It may also steer some PDUs to a local breakout point in order to support "non-seamless WLAN offload".

- May implement a local mobility anchor within the trusted WLAN access network.

#### 6.6.2.2 Initial Registration & PDU Session Establishment

The Figure 6.6.2.2-1 illustrates how the "non-5G capable UE over WLAN" UE can simultaneously connect to a trusted WLAN access network and to a 5G core network and is similar to the call flow in TR 23.716 [2], Figure 7.3.3.2-1. A single EAP-AKA' authentication procedure is executed for connecting the UE both to the trusted WLAN access network and to the 5G core network. .

Differences to the call flow in TR 23.716 [2]:

- The connection between TWIF and AMF relies on the N2 security specified in TS 33.501 [3], clause 9.2, therefore no specific NAS security is used between the TWIF to the AMF.



Figure 6.6.2.2-1: Initial registration and PDU session establishment

Steps 1-10: Initial registration to 5GC.

1. The UE associates with the trusted WLAN network and the EAP-AKA' authentication procedure is initiated.

2. The UE provides its Network Access Identity (NAI) The Trusted WLAN Access Point (TWAP) selects a Trusted WLAN Interworking Function (TWIF), e.g. based on the received realm or based on pre-configured information possibly associated with the SSID used by the UE and sends an AAA request to the selected TWIF.

In case of a UE with 5GC capabilities, the NAI has the format of <SUCI>, where the realm indicates the home PLMN. The UE discovers the PLMNs with which the WLAN supports "5G connectivity without NAS" and selects a PLMN, by using procedure defined in clause 7.6.

If the UE has registered to 5GC over 3GPP access when the above procedure is initiated, then the NAI includes the 5G-GUTI assigned to UE over 3GPP access. This enables the TWIF in step 4a below to select the same AMF as the one serving the UE over 3GPP access.

The NAI provided by the UE in step 2b indicates that the UE wants "5G connectivity without NAS" towards a specific PLMN. For example, with NAI=<SUCI>@nai.5gc-nn.mnc123.mcc45.3gppnetwork.org, the UE indicates that it wants "5G connectivity without NAS" (5gc-nn) to the PLMN with MCC=45 and MNC=123,

3. The TWIF creates a 5GC Registration Request message on behalf of the UE. The TWIF uses default values to populate the parameters in the Registration Request message, which are the same for all UEs that do not support 5G NAS. The Registration type indicates "Initial Registration".

4. The TWIF selects an AMF (e.g. by using the 5G-GUTI in the NAI, if provided by the UE) and sends an N2 message to the AMF including the Registration Request, the User Location and an AN Type.

5. The AMF triggers an authentication procedure by sending a request to AUSF indicating the AN type.

6. EAP-AKA' takes place between the UE and AUSF. Over the N2 interface, the EAP messages are encapsulated within NAS Authentication messages, as usually.

7. After a successful authentication, the AUSF sends to AMF the EAP-Success message and the created SEAF key.

8. The N2 reference point shall be secured as described in TS 33.501 [3], clause 9.2, therefore NAS security context may not be required in this scenario. The AMF derives an AN key from the received SEAF key. NAS security between AMF and W-5GAN is established similar to unauthenticated emergency calls, i.e. with NULL encryption and NULL integrity protection.

9. The AMF sends an N2 Initial Context Setup Request and provides the AN key to TWIF. In turn, the TWIF derives a Pairwise Master Key (PMK) from the AN key and sends the PMK key and the EAP-Success message to the Trusted WLAN Access Point, which forwards the EAP-Success to the UE. The PMK is the key used to secure the WLAN air-interface communication according to IEEE 802.11i [9] (now incorporated into IEEE 802.11 4]). A layer-2 or layer-3 connection is established between the Trusted WLAN Access Point and the TWIF for transporting all user-plane traffic of the UE to TWIF. This connection is later bound to an N3 connection that is created for this UE.

10. Finally, the AMF sends a Registration Accept message to TWIF At this point, the UE is connected to the WLAN access network..

Steps 20-21: PDU Session Establishment. This procedure is compliant with TS 23.502 [3] Figure 4.3.2.2.1-1 with the TWIF acting both as the AN and as the UE.

Step 25: User plane communication.

### 6.6.3 Evaluation

This solution fulfils the key issue #6 and is providing the security analysis for the normative solution in TS 23.502 V16.1.0.

Since the N2 reference point is secured by NDS as described in TS 33.501 [3], there is no need for NAS security between AMF and TWIF. The AMF selects the NULL scheme for ciphering and integrity protection in the Security Mode Command.

Further the security on the air interface relies on Layer-2 security between UE and TNAP (security context to encrypt and integrity protect unicast and multicast traffic over the air), which is a trusted entity so that no IPSec encryption would be necessary between UE and TWIF, i.e. NULL encryption is sufficient for the user plane and signalling.

## 6.7 Solution #7: Key separation for untrusted and trusted access

### 6.7.1 Introduction

This solution addresses the key issue #15 (N3GPP Key Separation).

### 6.7.2 Solution details

#### 6.7.2.0 General

When introducing more variants of Non-3GPP accesses, and thus more types of access node keys are needed, there are different optional solutions. .

One option is to keep the values in Table A.9-1 in TS.33.501 [3] and add separation in the next layer in the hierarchy. In this case, there is one common key for N3GPP access, KN3GPP. This key would be derived as described in TS.33.501 [3], Appendix A.9. Instead key separation would be added in the next layer of the key hierarchy.

#### 6.7.2.1 Keys for trusted access

In the trusted access case, as specified in TS 23.502 [6] clause 4.12a.2.2 "Registration procedure for trusted non-3GPP access", there are two different usages for the access key KTNGF; to setup IPSec SAs between the UE and the TNGF and to create WLAN keys (TNAP keys) between the UE and the TNAP.

To separate the keys for these purposes, a key hierarchy can be setup for trusted access as illustrated in Figure 6.7.2.1-1. One key is intended to be used to setup IPSec SAs (KTIPSec) and another key is derived as root key for TNAP keys (KTNAP\_Root). Note the meaning of the different arrow types as described in the legend in Figure 6.7.2.1-1.

When deriving the KTIPSec and KTNAP\_Root from KTNGF in the UE and the TNGF, the usual procedures for separation (separate FC values or other input separation) can be used.



Figure 6.7.2.1-1: Key hierarchy with additional layer for trusted access

### 6.7.3 Evaluation

This solution addresses the key issue #15 (N3GPP Key Separation). The requirement of KI#15 states:

"The key used for IPsec protection and between UE and TNAP shall be cryptographic separated."

This solution introduces two new keys, KTIPSec and KTNAP\_Root. The key KTIPSec is used to setup the IPSec SA between the UE and TNGF while the key KTNAP\_Root is used to derive WLAN keys used between the UE and the access point, TNAP.

These two keys are separated by introducing a new key derivation (details to be specified during normative work) based on the use of separate FC values to get cryptographic separation.

Hence, the solution fulfils the requirement of KI#15.

## 6.8 Solution #8: Transport security for the interfaces between W-5GAN and 5GC

### 6.8.1 Introduction

This solution addresses Key Issue #3: Transport security for the interfaces between W-5GAN and 5GC.

### 6.8.2 Solution details

The interfaces between the W-5GAN and 5GC are the following:

- W-5GAN – AMF (N2, in Scenario 2 also N1), and

- W-5GAN – UPF (N3).

According to clauses 9.2 and 9.3 in TS 33.501 [3], the following security protocols shall be supported in Rel-15 for the N2 and N3 interfaces:

- 5GAN – AMF (N2): NDS/IP and DTLS,

- 5GAN – UPF (N3): NDS/IP.

This solution proposes that the same requirements should hold in the case that the 5GAN is a wireline 5GAN. Hence it is proposed that the following security protocols shall be supported:

- W-5GAN – AMF (N2, in Scenario 2 also N1): NDS/IP and DTLS

- W-5GAN – UPF (N3): NDS/IP

### 6.8.3 Evaluation

This solution addresses KI#3 by reusing NDS/IP defined in TS 33.501 [3].

## 6.9 Solution #9: Solution on Line ID protection

### 6.9.1 Introduction

This solution addresses KI #16.

### 6.9.2 Solution details

When the UDM receives Nudm\_UEAuthentication\_Get Request from AUSF, the UDM deconceal SUCI to obtain SUPI using the method defined in 33.501 [3], and then the UDM can get the FN-RG identifier from the username part of the SUPI.

The UDM further checks whether the FN-RG is authorized to use the 5GC. If it is authorized, the UDM will reply SUPI and an indication that the FN-RG is successfully authenticated by the UDM and the authentication is not required to the AUSF in Nudm\_UEAuthentication\_Get Response. Based on the indication, the AUSF will skip the authentication procedure and forward the SUPI and the indication to the AMF.

### 6.9.3 Evaluation

The solution fulfil the requirement of KI#15.

The solution reuses the method defined in TS 33.501 to deconceal the SUCI to gain SUPI of the FN-RG.

# 7 Conclusions

## 7.1 Conclusion on KI #1

Solution#3 and solution #5 are recommended as the basic for normative work.

## 7.2 Conclusion on KI #2

Solution#4 is recommended as the basic for normative work.

## 7.3 Conclusion on KI #3

For N2 and N3 interface, solution #8 is the basic for normative work.

In case of FN-RG, the W-5GAN acts as end point of N1 on behalf of the FN-RG, the security of N1 is concluded in subclause 7.2 of the present document.

## 7.4 Conclusion on KI #4

The security of the interface between 5G-RG and W-5GAN is outside the scope of 3GPP.

## 7.5 Conclusion on KI #5

Solution #1 is selected for normative specification.

## 7.6 Conclusion on KI #6

Solution #6 is selected for normative specification.

## 7.7 Conclusion on KI #7

Solution#2 is recommended as the basis for normative work for key issue #7.7.8 Conclusion on KI #8

Solution#2 is recommended as the basis for normative work for key issue #8.7.9 Conclusion on KI #9

KI#9 overlaps with other key issues. The related interfaces in need of user plane security are:

- FN-RG – W-5GAN (covered by KI#4, which is within BBF scope)

- 5G-RG – W-5GAN (not covered by any KI, but within BBF scope)

- W-5GAN – 5GC (covered by KI#3 which is concluded to be addressed by Solution #8)

No separate solution is needed for KI#9.

## 7.8 Conclusion on KI #10

The KI #10 is to study whether NAS security is needed when registering UEs which cannot perform 5G NAS signalling over WLAN access, to establish connectivity to 5GC via a trusted WLAN access network.

The TWIF provides interworking functionality that enables connectivity with 5GC. It terminates N1, N2 and N3 interfaces and implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the UE.

Solution #8 proposes use of security protocols defined in TS 33.501 [3] (NDS/IP or DTLS) for N2 and N3 interfaces between the W-5GAN in the wireline network and the AMF in the 5GC. This conclusion proposes to use security protocols defined in TS 33.501 [3] (NDS/IP or DTLS) for protecting the interface between the TWIF and the AMF. Since NAS messages over N1 are transported over this secure interface, it can also be concluded that no additional security is required at the NAS layer.

## 7.9 Conclusion on KI #11

The KI #11 is to study whether NAS security is needed when registering FN-RG with the 5GC.

Interface between FAGF/W-AGN and AMF is used to transport N2 messages when 5G-RG is connected to W-5GAN, and N1 NAS messages when FN-RG is connected.

Solution #8 proposes use of security protocols defined in TS 33.501 [3] to protect the interface between W-5GAN and AMF. Since NDS/IP or DTLS is proposed to protect the interface between the FAGF and the AMF, there is no need for additional security for N1 messages generated by the FAGF when registering the FN-RG to the 5GC.

Solution #4 covers security aspects during FN-RG registration.

## 7.10 Conclusion on KI #12

The Key issue #12 studies whether the Line Id, that identifies a legacy gateway (FN-RG), needs to be concealed by the FAGF when the FAGF is sending it in the Registration Request message to the AMF in the 5GC.

Solution #4 proposes that the interface between the FAGF and the AMF be protected with either NDS/IP or DTLS. The Line Id is transferred from the W-5GAN to the AMF over a mutually authenticated, protected backhaul interface between the W-5GAN and the 5GC.

It can therefore be concluded that the SUCI, which is constructed by FAGF from SUPI (that contains a Line Id), there is no need to conceal the Line Id. The construction of SUCI from Line Id is based on existing scheme in TS 33.501 and is based on NULL scheme.

## 7.11 Conclusion on KI #14

The KI#14 is not in the scope of the present document.

## 7.12 Conclusion on KI#15

Solution#7 is recommended as the basis for normative work for the key issue #15, with the following exception: It is left for decision during normative phase, whether a KTIPSec key as additional layer below KTNGF for the establishment of IPSec SAs between the UE and the TNGF is introduced.

## 7.13 Conclusion on KI #16

Solution#9 is recommended as the basic for normative work.7.X Conclusion on KI #X.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-09 | SA#85 | SP-190701 |  |  |  | Presented for information and approval | 1.0.0 |
| 2019-09 | SA#85 | SP-190785 |  |  |  | Revised given that the uploaded version was not correct | 1.0.1 |
| 2019-09 | SA#85 |  |  |  |  | Change control version | 16.0.0 |
| 2019-10 |  |  |  |  |  | EditHelp review | 16.0.1 |