|  |
| --- |
| 3GPP TR 33.887 V0.6.0 (2023-02) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Assumptions 7

5 Key issues 8

5.1 Key issue #1: Authentication of AUN3 device behind RG and supporting EAP 8

5.1.1 Key issue details 8

5.1.2 Threats 8

5.1.3 Potential security requirements 8

5.2 Key issue #2: Security aspect of slice information exposure of N3IWF/TNGF to UE 8

5.2.1 Key issue details 8

5.2.2 Threats 9

5.2.3 Potential security requirements 9

5.3 Key issue #3: Security aspect of slice information exposure of N3IWF/TNGF 9

5.3.1 Key issue details 9

5.3.2 Threats 9

5.3.3 Potential security requirements 9

5.4 Key issue #4: Security aspect of TNAP mobility without full authentication 9

5.4.1 Key issue details 9

5.4.2 Threats 10

5.4.3 Potential security requirements 10

6 Proposed solutions 10

6.0 Mapping of solutions to key issues 11

6.1 Solution #1: EAP\_AKA prime based authentication for AUN3 devices 11

6.1.1 Introduction 11

6.1.2 Solution details 11

6.1.3 Evaluation 13

UE: derive the new keys. 14

6.2 Solution #2: EAP base authentication for AUN3 devices behind RG in PLMN 14

6.2.1 Introduction 14

6.2.2 Solution details 14

6.2.3 Evaluation 15

6.3 Solution #3: EAP base authentication for AUN3 devices behind RG in SNPN 15

6.3.1 Introduction 15

6.3.2 Solution details 16

6.3.3 Evaluation 17

6.4 Solution #4: EAP base authentication for AUN3 devices behind RG in SNPN by AAA server 17

6.4.1 Introduction 17

6.4.2 Solution details 17

6.4.3 Evaluation 18

6.5 Solution #5: TNAP mobility solution with rand 18

6.5.1 Introduction 18

6.5.2 Solution details 19

6.5.3 Evaluation 20

6.6 Solution #6: TNAP mobility solution with count 21

6.6.1 Introduction 21

6.6.2 Solution details 21

6.6.3 Evaluation 23

6.7 Solution #7: Using Fast BSS Transition for TNAP mobility 24

6.7.1 Introduction 24

6.7.2 Solution details 24

6.7.2.1 Solution overview 24

6.7.2.2 Details of FT 25

6.7.3 Evaluation 26

6.8 Solution #8: Security Establishment for TNAP Mobility 27

6.8.1 Introduction 27

6.8.2 Solution details 27

6.8.3 Evaluation 29

6.9 Solution #9: AUN3 device supporting 5G Key hierarchy (i.e. N5CW) 29

6.9.1 Introduction 29

6.9.2 Solution details 29

6.9.3 Evaluation 31

6.10 Solution #10: TNAP mobility solution without full authentication 32

6.10.1 Introduction 32

6.10.2 Solution details 32

6.10.3 Evaluation 33

6.11 Solution #11: Security of N3IWF/TNGF reallocation 33

6.11.1 Introduction 33

6.11.2 Solution details 33

6.11.3 Evaluation 35

6.13 Solution #13: TNAP mobility using modified ERP 35

6.13.1 Introduction 35

6.13.2 Solution details 36

6.13.3 Evaluation 38

6.Y Solution #Y: <Title> 38

6.Y.1 Introduction 38

6.Y.2 Solution details 39

6.Y.3 Evaluation 39

7 Conclusions 39

7.1 Key issue #1: Authentication of AUN3 device behind RG and supporting EAP 39

7.2 Key issue #2: Security aspect of slice information exposure of N3IWF/TNGF to UE 39

7.3 Key issue #3: Security aspect of slice information exposure of N3IWF/TNGF 39

7.4 Key issue #5: Authentication of UE connecting to RG using NSWO 39

Annex X: Change history 40

# 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 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.
* Whether and how the security aspects for UE TNAP mobility can be supported in the 5GS without performing the full authentication.

# 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)"

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

[5] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[6] IEEE Std 802.11™-2020 Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[7] 3GPP TS 23.502: "Procedures for the 5G System"

[8] IETF RFC 6696: "EAP Extensions for the EAP Re-authentication Protocol (ERP)".

# 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 format (EW)

<ABBREVIATION> <Expansion>

# 4 Assumptions



Figure 4.1-1 Non-roaming architecture for 5G Core Network with mobility within trusted non-3GPP access

Figure 4.1-1 shows the non roaming architecture for 5G core network for mobility use case where the target trusted non-3GPP Access Point and source Trusted Non-3GPP Access Point are connected to the same Trusted Non-3GPP Gateway Function(TNGF).

In this study, when UE switches from one TNAP(source) to another TNAP(destination) within the same TNGF, full authentication is not performed.

# 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. I.e., how AUN3 devices connected with RG over wifi are authenticated and how the interface between AUN3 devices and RG is protected.

### 5.1.2 Threats

If authentication of AUN3 device behind RG is not properly defined, an attacker may be able to impersonate an AUN3.

When AUN3 devices connect to the RG over wifi, the session between AUN3 devices and the RG is not protected. Due to this, MitM can intercept the AUN3 device's communication.

### 5.1.3 Potential security requirements

5GC should be able to authenticate the AUN3 device behind RG.

The 5GS should provide a means for the AUN3 device and RG to get a shared key that could be used to provide protection of the interface between them.

## 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] includes few solutions, for example, solutions 10 and 11, include the IKE v2 procedure enhancement to relocate the TNGF/N3IWF. Security aspects of the solutions in this category should be studied.

### 5.3.2 Threats

In case the TNGF/N3IWF relocation information is sent to the UE without protection, for example, the target SSID, the information may be tampered during the transfer. Even though the SSID is publicly known, if the target SSID is tampered, the UE may continue to connect to an unappropriated TNGF/N3IWF and the system may be in the loop to relocate the TNGF/N3IWF for the UE. In this case, the UE will suffer a DoS Attack.

.

### 5.3.3 Potential security requirements

The TNGF/N3IWF relocation information shall be securely sent to the UE.

.

## 5.4 Key issue #4: Security aspect of TNAP mobility without full authentication

### 5.4.1 Key issue details

Mobility between two TNAPs within the same trusted Non-3GPP Access Network Gateway Function(TNGF) is not supported in 3GPP currently. For example, when UE moves between two nearby or overlapping TNAP1 and TNAP2, the connectivity will break. Therefore, UE services will be interrupted. The UE needs to reconnect, go through another authentication procedure to continue the service even though the second non-3GPP access connect to the same 5GC.

There could be some potential security solutions where UE switches the TNAP1 to TNAP2 without breaking the connectivity. However, the security aspects of optimizations of inter-TNAP mobility were never studied in SA3.

### 5.4.2 Threats

TBD.

### 5.4.3 Potential security requirements

5GS should support a mechanism for communication between the UE and TNAP/TNGF to establish security with a TNAP without performing full authentication when the UE switches from another TNAP within the same TNGF.

While switching from one TNAP to another TNAP within the same TNGF, the interface between UE and the new TNAP shall be confidentiality, integrity, and replay protected.

6.5 KI #5: Authentication of UE connecting to RG using NSWO procedure

6.5.1 Key issue details

In clause 7B.4 of TS 33.501, UE behind RG can connect to 5GC via TNGF in trusted Non-3GPP access or N3IWF in untrusted Non-3GPP access procedures with the entire wireline access treated as part of the trusted or untrusted Non-3GPP access.

In TS 23.501 [2] clause 4.2.15, UE is allowed to use 5G credentials based on NSWO to authenticate to the 5GC to first obtain local IP address and then to use untrusted Non-3GPP access to register to the 5GC.

Similarly, when UE is behind RG, the UE should also be able to use NSWO to first authenticate to 5GC to obtain local IP address before using the untrusted Non-3GPP access to register with 5GC

Even when UE does not use untrusted Non-3GPP access to register, it is still beneficial for UE behind RG to use 5G credentials to authenticate to 5GC, since it allows operators to identify UE behind RG and then to offer enhanced services (e.g., WiFi speed increase) to the UE.

This key issue is to allow UE behind RG to be authenticated by 5GC using NSWO procedure.

6.5.2 Security threats

If the 5GC cannot authenticate UE connecting to RG, the 5GC may provide service to unauthorized devices behind RG.

6.5.3 Potential requirements

5GS shall support authentication of UE behind RG using NSWO procedure.

# 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 | KI#4 |
| **Solution #1: EAP\_AKA prime based authentication for AUN3 devices** | X | - |  |  |
| **Solution #2: EAP base authentication for AUN3 devices behind RG in PLMN** | X | - |  |  |
| **Solution #3: EAP base authentication for AUN3 devices behind RG in SNPN** | X | - |  |  |
| **Solution #4: EAP base authentication for AUN3 devices behind RG in SNPN by AAA server** | X | - |  |  |
| **Solution #5: TNAP mobility solution with rand** |  | - |  | X |
| **Solution #6: TNAP mobility solution with count** |  |  |  | X |
| **Solution #7: Using Fast BSS Transition for TNAP mobility** |  |  |  | X |
| **Solution #8: Security Establishment for TNAP Mobility** |  |  |  | X |

## 6.1 Solution #1: 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 EAP Response/Identity message. The AUN3 device uses SUCI in NAI format (i.e., username@realm format as specified in clause 28.7.3 of TS 23.003) or 5G-GUTI.

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 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 sends a NAS Registration Request message to the AMF, including the received SUCI and the new indicator for encryption required for AUN3 device.

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

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 (KWAGF') to W-AGF.

7. W-AGF/RG derive the KAUN3 as PMK key from the WAGF key (KWAGF').

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.

6.1.2.2 Key derivation

6.1.2.2.1 WAGF key for AUN3 device (not supporting NAS)\_

When deriving the keys KWAGF' for AUN3 device not supporting NAS, from KAMF then the following parameters should be used input S to the KDF.

- FC = 0x<to be defined>

- P0 = Device distinguisher (shall be set to 0x01 for AUN3 device, others it will be 0x00)

- L0 = length of Device distinguisher (i.e. 0x00 0x04)

- P1 = Access type distinguisher

- L1 = length of Access type distinguisher (i.e. 0x00 0x01)

The access type distinguisher shall be set to the value for 'non-3GPP (0x02) when deriving KWAGF'.

6.1.2.2.2 KAUN3 key

When deriving a KAUN3 key from KWAGF' the following parameters shall be used to form the input S to the KDF.

- FC = 0x<to be defined>

- P0 = Usage type distinguisher

- L0 = length of Usage type distinguisher (i.e. 0x00 0x01)

Usage type distinguisher value is set to 0x01.

### 6.1.3 Evaluation

This solution meets both the requirements mentioned in the KI1 for the AUN3 device that support 5G key hierarchy. i.e.

* 5GC should be able to authenticate the AUN3 device behind RG.
* The 5GS should provide a means for the AUN3 device and RG to get a shared key that could be used to provide protection of the interface between them.

**Impact on the NFs:**

AUSF/UDM: New indication received for AUN3 devices and select authentication algorithm accordingly.

AMF: generates the keys and provides the same to RG/W-AGF.

RG/W-AGF: receives new key material from AMF and then derives the PMK.

## UE: derive the new keys.

## 6.2 Solution #2: EAP base authentication for AUN3 devices behind RG in PLMN

### 6.2.1 Introduction

An AUN3 device connecting to RG in a PLMN is registered to the 5GC by the 5G-RG or W-AGF and is authenticated by 5GC using EAP-AKA’, as specified in RFC 5448 [5].

### 6.2.2 Solution details



1. The AUN3 device attempts to establish a layer 2 connection with the RG either via Ethernet or WiFi. If the layer 2 connection is based on Ethernet, steps 13-14 are skipped.

2. The RG initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer frame (e.g., EAPOL).

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm. The username part of the NAI may be encrypted if the AUN3 device supports SUPI protection

4a-4b. 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 constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. 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 an AUN3 device indicator.

5. The AMF/SEAF selects the AUSF based on the SUCI in the received registration request and sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the AUN3 device, and an AUN3 device indicator.

6. The AUSF sends a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the AUN3 device and the AUN3 device indicator.

7. The UDM invokes the SIDF to map the SUCI to the SUPI and selects an authentication method based on the SUPI. When the "username" part of the SUPI is "anonymous" or omitted, the UDM may select an authentication method based on the “realm” part of the SUPI, the AUN3 device indicator, a combination of the "realm" part and the AUN3 device indicator, or the UDM local policy.

8. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains the SUPI of the AUN3 device and an indicator of the selected EAP-AKA’.

9. The AUSF and the AUN3 device perform EAP-AKA’. Storage and procession of credentials for EAP-AKA’ is described in clause 6 of TS 33.501 [4].

10. If the EAP authentication between the AUSF and the AUN3 device is completed successfully, the AUSF sends to the AMF/SEAF an EAP-Success message along with the SUPI and the MSK in a Nausf\_UEAuthentication\_Authenticate Response message.

11a-11b. If steps 4a-4b is executed, the AMF/SEAF sends to the W-AGF the EAP-Success message and the MSK in an Authentication Result message. The W-AGF sends to the FN-RG the EAP-Success message and the MSK in AAA message.

11c. If step 4c is executed, the AMF/SEAF sends to the 5G-RG the EAP-Success message and the MSK in an Authentication Result message.

12. The RG sends to the AUN3 device the the EAP-Success message in a layer 2 frame.

13a-13b. The AUN3 device and the RG use the first 256-bit of the MSK as the PMK, from which the WLAN keys are derived.

14. The AUN3 and the RG performs four-way handshaking to establish WLAN secure connection.

### 6.2.3 Evaluation

This solution meets the requirement that an AUN3 device shall be able to authenticate to the 5GC.

## 6.3 Solution #3: EAP base authentication for AUN3 devices behind RG in SNPN

### 6.3.1 Introduction

This solution defines an authentication procedure for AUN3 devices behind RG (5G-RG or FN-RG) in SNPN. It differs from Annex O of TS 33.501 [4] in that:

1. it allows 5G-RG to register AUN3 device to 5GC on its behalf, while in Annex O, it is always the W-AGF that registers N5GC device to the 5GC.

2. it allows the AUN3 device to connect to RG via WiFi based on the MSK from the EAP authentication between the AUN3 device and the AUSF. In Annex O, the N5GC device connects to the RG via wireline (e.g., Ethernet) and MSK is not sent back by the AUSF to the RG to facilitate WiFi four-way handshaking.

### 6.3.2 Solution details



1. The AUN3 device attempts to establish a layer 2 connection with the RG either via Ethernet or WiFi. If the layer 2 connection is based on Ethernet, steps 13-14 are skipped.

2. The RG initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer frame (e.g., EAPOL).

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm. The username part of the NAI may be encrypted if the AUN3 device supports SUPI protection. Otherwise, the anonymous NAI can be used if the EAP method supports subscription identifier privacy

4a-4b. 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 constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. 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 an AUN3 device indicator.

5. The AMF/SEAF selects the AUSF based on the SUCI in the received registration request and sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the AUN3 device, and an AUN3 device indicator.

6. The AUSF sends a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the AUN3 device and the AUN3 device indicator.

7. The UDM invokes the SIDF to map the SUCI to the SUPI and selects an authentication method based on the SUPI. When the "username" part of the SUPI is "anonymous" or omitted, the UDM may select an authentication method based on the “realm” part of the SUPI, the AUN3 device indicator, a combination of the "realm" part and the AUN3 device indicator, or the UDM local policy.

8. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains the SUPI of the AUN3 device and an indicator of the selected authentication method. EAP-AKA’ as specified in RFC 5448 [5] or other key generating EAP method can be selected.

9. The AUSF and the AUN3 device perform EAP authentication based on the selected authentication method. Storage and processing of credentials for EAP authentication method is described in Annex I of TS 33.501 [4].

10. If the EAP authentication between the AUSF and the AUN3 device is completed successfully, the AUSF sends to the AMF/SEAF an EAP-Success message along with the SUPI and the MSK in a Nausf\_UEAuthentication\_Authenticate Response message.

11a-11b. If steps 4a-4b is executed, the AMF/SEAF sends to the W-AGF the EAP-Success message and the MSK in an Authentication Result message. The W-AGF sends to the FN-RG the EAP-Success message and the MSK in AAA message.

11c. If step 4c is executed, the AMF/SEAF sends to the 5G-RG the EAP-Success message and the MSK in an Authentication Result message.

12. The RG sends to the AUN3 device the the EAP-Success message in a layer 2 frame.

13a-13b. The AUN3 device and the RG use the first 256-bit of the MSK as the PMK, from which the WLAN keys are derived.

14. The AUN3 and the RG performs four-way handshaking to establish WLAN secure connection.

### 6.3.3 Evaluation

This solution meets the requirement that an AUN3 device connecting to RG shall be able to authenticate to 5GC.

## 6.4 Solution #4: EAP base authentication for AUN3 devices behind RG in SNPN by AAA server

### 6.4.1 Introduction

This solution addresses KI#1 by authenticating AUN3 devices behind RG (5G-RG or FN-RG) in SNPN using an AAA server as the credential holder.

### 6.4.2 Solution details



1. The AUN3 device attempts to establish a layer 2 connection with the RG either via Ethernet or WiFi. If the layer 2 connection is based on Ethernet, steps 13-14 are skipped.

2. The RG initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer frame (e.g., EAPOL).

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm. The username part of the NAI may be encrypted if the AUN3 device supports SUPI protection. Otherwise, the anonymous NAI can be used if the EAP method supports subscription identifier privacy.

4a-4b. 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 constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. 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 an AUN3 device indicator.

5. The AMF/SEAF selects the AUSF based on the SUCI in the received registration request and sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the AUN3 device, and an AUN3 device indicator.

6. The AUSF sends a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the AUN3 device and the AUN3 device indicator.

7. The UDM invokes the SIDF to map the SUCI to the SUPI and selects an authentication method based on the SUPI. When the "username" part of the SUPI is "anonymous" or omitted, the UDM may select an authentication method based on the “realm” part of the SUPI, the AUN3 device indicator, a combination of the "realm" part and the AUN3 device indicator, or the UDM local policy.

8. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains the SUPI of the AUN3 device and an indicator of the selected authentication method.

9. Based on the indication from the UDM, the AUSF shall select an NSSAAF as defined in TS 23.501 [2] and initiate a Nnssaaf\_AIWF\_Authenticate service operation towards that NSSAAF as defined in clause 14.4.2.

10. The NSSAAF shall select AAA Server based on the domain name corresponding to the realm part of the SUPI. The NSSAAF shall perform related protocol conversion and relay EAP messages to the AAA Server.

11. The AAA and the AUN3 device perform EAP authentication based on the selected authentication method. Storage and processing of credentials for EAP authentication method is described in Annex I of TS 33.501 [4].

12. After successful authentication, an EAP Success message, the MSK and the SUPI (i.e., the AUN3 identifier that is used for the successful EAP authentication) shall be provided from the AAA Server to the NSSAAF.

13. The NSSAAF returns the EAP Success message, the MSK and the SUPI to the AUSF using the Nnssaaf\_AIWF\_Authenticate service operation response message.

14. The AUSF sends to the AMF/SEAF the EAP-Success message along with the SUPI and the MSK in a Nausf\_UEAuthentication\_Authenticate Response message.

15a-15b. If steps 4a-4b is executed, the AMF/SEAF sends to the W-AGF the EAP-Success message and the MSK in an Authentication Result message. The W-AGF sends to the FN-RG the EAP-Success message and the MSK in AAA message.

15c. If step 4c is executed, the AMF/SEAF sends to the 5G-RG the EAP-Success message and the MSK in an Authentication Result message.

16. The RG sends to the AUN3 device the the EAP-Success message in a layer 2 frame.

17a-17b. The AUN3 device and the RG use the first 256-bit of the MSK as the PMK, from which the WLAN keys are derived.

18. The AUN3 and the RG performs four-way handshaking to establish WLAN secure connection.

### 6.4.3 Evaluation

This solution meets the requirement that an AUN3 device shall be able to authenticate to 5GC.

## 6.5 Solution #5: TNAP mobility solution with rand

### 6.5.1 Introduction

This solution addresses the security solution of TNAP mobility defined in KI#4.

### 6.5.2 Solution details

6.5.2.1 Procedure



Figure 6.5.2-1 TNAP mobility procedure

1. UE is connected to TNAP#1 via the procedure defined in TS 33.501 figure 7A.2.1-1. Once authenticated, TNGF sends the reauth Id to UE over the protected interface. Reauth Id can be a generated as <PLMNID><TNGF\_ID> <Temp Id>.

Note: TNGF Id could be TNGF address (like fqdn)already defined by SA2.

2, 3. UE decides to move from TNAP#1 to TNAP#2 and creates an L2 connection with TNAP#2.

4, 5, 6. TNAP#2 sends the L2 EAP-Request for Identity towards the UE and the UE responds back with an L2 EAP-Response with Identity and a TNAP\_Mobility\_Indication flag. The TNAP2 forwards the EAP response with reauth Id and the TNAP\_Mobility\_Indication flag towards TNGF.

7,8. Based on the reauth Id, TNFG identifies the UE and retrieves the context and TNAP\_Mobility\_Indication, the TNGF checks if the stored context in step 1 is valid and then derives the TNAP’ keys as described in section 6.5.2.2 of this document. The TNGF responds back to TNAP#2 with the generated key RAND value and MAC for the RAND value. Message Authentication Code (MAC) is derived by using the TNGF key stored in TNGF. In TNAP#2, the newly received TNAP key is considered as Pairwise Master Key (PMK).

9, 10,11. The TNAP#2 sends an EAP-notification back to the UE with the RAND value along with MAC. If MAC validation is successful then based on the RAND value, UE derives the keys. A 4-way handshake is executed (see IEEE 802.11) which establishes a security context between the WLAN AP and the UE that is used to protect unicast and multicast traffic over the air.

Once the procedure is complete, the TNGF sends the new reauth Id to UE over the secure interface that UE can use for the next interaction.

NOTE: If the UE gets the new IP configurations from TNAP2, then the UE updates the SA address using an IKE informational request "UPDATE\_SA\_ADDRESS" to TNGF for further communications.

6.5.2.2 Key derivation



Derivation of KTNAP' from KTNGF during mobility use the following input parameters.

- FC = 0xWX

- P1 = RAND,

- L1 = length of RAND (i.e. 0x00 0x04)

The input key KEY shall be KTNGF.

When KTNAP' is derived in Mobility, and RAND shall be generated and shared with UE.

### 6.5.3 Evaluation

The solution addresses KI#4.

UE and TNGF performs mutual authentication during UE TNAP mobility without performing the full authentication.

Impact on the nodes/UE:

|  |  |
| --- | --- |
| Node/UE/NF | solution |
| UE  | * Derive new TNAP keys
* receive reauth Id from TNGF and provide the same as NAI to next TNAP
 |
| TNGF | * Derive new TNAP keys
* provide reauth id and RAND to UE after authentication.
* need to find a stored UE context based on Reauth-ID
 |

## 6.6 Solution #6: TNAP mobility solution with count

### 6.6.1 Introduction

This solution addresses the security issue due to TNAP mobility defined in KI#4.

### 6.6.2 Solution details

6.6.2.1 Procedure



Figure 6.6.2-1 TNAP mobility procedure

1. UE is connected to TNAP#1 via the procedure defined in TS 33.501 figure 7A.2.1-1. Once authenticated, TNGF sends the reauth Id to UE over the protected interface. Reauth Id can be a generated as <PLMNID><TNGF\_ID> <Temp Id>.

Note: TNGF Id could be TNGF address (like fqdn)already defined by SA2.

2, 3. UE decides to move from TNAP#1 to TNAP#2 and creates an L2 connection with TNAP#2.

4, 5, 6. TNAP#2 sends the L2 EAP-Request for Identity towards the UE and the UE responds back with an L2 EAP-Response with Identity and a TNAP\_Mobility\_Indication flag. The TNAP2 forwards the EAP response with reauth Id and the TNAP\_Mobility\_Indication flag towards TNGF..

7,8. Based on the reauth Id, TNFG identifies the UE and retrieves the context and checks if the stored context in step 1 is valid and then derives the TNAP’ keys as described in section 6.6.2.2 of this document. The TNGF responds back to TNAP#2 with the generated key. In TNAP#2, the newly received TNAP key is considered as Pairwise Master Key (PMK).

9, 10,11. The TNAP#2 sends an EAP-notification back to the UE with the update flag. Based on the flag, UE updates the counter and derives the keys. A 4-way handshake is executed (see IEEE 802.11) which establishes a security context between the WLAN AP and the UE that is used to protect unicast and multicast traffic over the air.

Once the procedure is complete, the TNGF sends the new reauth Id to UE over the secure interface that UE can use for the next interaction.

NOTE: If the UE gets the new IP configurations from TNAP2, then the UE updates the SA address using IKE informational request "UPDATE\_SA\_ADDRESS" to TNGF for further communications.

6.6.2.2 Key derivation



Derivation of KTNAP' from KTNGF during mobility use the following input parameters.

- FC = 0xWX

- P1 = COUNT,

- L1 = length of COUNT (i.e. 0x00 0x04)

The input key KEY shall be KTNGF.

In this case, the COUNT shall be the downlink NAS COUNT of the Non-3GPP access.

### 6.6.3 Evaluation

TNGF and UE: Generate new keys based on the count value and handle the reauth Id.

TNAP: use updated keys for the mobility scenario

Editor's Notes: The count desynchronization issue and further evaluation are FFS.

## 6.7 Solution #7: Using Fast BSS Transition for TNAP mobility

### 6.7.1 Introduction

This solution addresses key issue #4: Security aspect of TNAP mobility

### 6.7.2 Solution details

#### 6.7.2.1 Solution overview

This solution addresses the TNAP mobility using the Fast BSS Transition protocol [6].

The Fast BSS Transition (FT) key hierarchy is established based on the Master Session Key (MSK) by the R0 Key Holder (R0KH) that is collocated with the 802.1X authenticator as specified in [aa]. To support the Fast BSS Transition, the entity that will hold the root key needs to obtain a 256 bit key (KFT) from the TNGF, which is then used as an input key to create the FT key hierarchy .

The key KFT is derived from KTNGF using fixed inputs similar to the derivation of KTNAP from KTNGF described in Annex A.22 of TS 33.501 [4] but using a new Usage type distinguisher, e.g. 0x03.

The key KFT is used to create the FT key hierarchy specified in 802.11 [6]. Specifically, KFT is used as Master PMK (MPMK) that is used as an input key for R0-Key-Data derivation. With the R0-Key-Data, the FT key hierarchy is established In effect, KFT links the 5G key hierarchy and FT key hierarchy as it is derived from a key in the 5G key hierarchy and being used to create the FT key hierarchy (see Figure 6.7.2-1 for more details).

When UE switches to a new TNAP within the same mobility domain identified by the Mobility domain identifier (MDID), the UE performs the fast BSS transition procedure as specified in [6].

The entity that has received KFT from the TNGF takes the role of PMK R0 Key Holder (R0KH) that holds the key, PMK-R0. The R0KH derives PMK-R1 from PMK-R0 and provides it to the new AP (i.e., TNAP in TNAN) during the FT procedure.

Figure 6.7.2-1 shows how the 5G and FT key hierarchies link together in this solution.



Figure 6.7.2-1: Link between the 5G and FT key hierarchies

NOTE 1: The TNGF can send both KTNAP and KFT to the entity that holds the root key of the FT key hierarchyas an MSK. The TNGF sets the MSK to KTNAP || KFT, where MSK is 512 bits and the KTNAP and KFT are 256 bits. The TNGF sends the MSK using existing mechanisms.

#### 6.7.2.2 Details of FT

This clause contains a brief overview of the FT security procedure with no attempt to give the complete details (see [6] for those details). None of the details need to be changed by the proposed solution.

The FT capability is advertised in the Beacon and Probe Response frames by including the MDIE. The MDIE is advertised in the Beacon and Probe Response frames to indicate the Mobility Domain ID (MDID), FT capability, and the FT policy.

The key PMK-R0 and PMK-R1 are identified by PMKR0Name and PMKR1Name respectively. Each AP gets a different PMK-R1 provided to it to secure the communications between the UE and AP. Finally, nonces (SNonce from UE and ANonce from the AP) are used to ensure freshness of the traffic key (PTK) between the UE and AP.

Figure 6.7.2.2-1 show a UE attaching to the first AP that results in establishing the FT key hierarchy.



Figure 6.7.2.2-1: Initial UE association

Step 1: The UE wants to connect to the AP that is advertising FT capability through inserting the MDE into Beacons and ProbeResponses. The MDE informs about that the AP is FT capable, the mobility domain ID and the potential support of FT over DS.

Step 2: The UE and AP exchange 802.11 Authentication Request and Response.

Step 3: The UE sends a (Re)association Request to the AP with a MDE included indicating that the UE wants to perform FT within the indicated mobility domain.

Step 4: The AP responds with a (Re)association Response including the MDE and both R1KH-ID and R0KH-ID, if it agrees with the proposed FT adoption

Steps 5a-c: EAP authentication is run and results in the UE and R0KH both having PMK-R0 and PMKR0Name. The AP is provided with PMK and the UE calculates PMK.

Step 6: The 4-way handshake is performed between the UE and AP.

Step 7: The UE and AP start securely exchanging data.

The important takeaway from the initial attachment is that the UE and R0KH both have PMK-R0 and the PMKR0Name and the UE has the R0KH-ID.

Figure 6.7.2.2-2 shows AP mobility using the over the air procedure.



Figure 6.7.2.2-2: AP mobility

Steps 0: The UE has connected to an AP and established the FT key hierarchy as shown in Figure 6.7.2.2-1.

Step 1: The UE finds another AP (called target AP) advertising FT capability and the same mobility domain. The UE sends an 802.11 Authentication Request to the Target AP including MDE, R0KH-ID, PMKR0Name and SNonce.

Step 2: The target AP queries the R0KH for the required PMK-R1and fetches the PMK-R1 from the R0KH using R0KH-ID and PMKR0Name.

Step 3: The target AP sends an 802.11 Authentication Response to the UE including ANonce and R1KH-ID.

Step 4: The UE calculates PMKR1Name and initiates its reassociation to the target AP continuing the establishment of a PTK for the new association

Step 5: The UE sends a Reassociation Request including PMKR1Name, ANonce, SNonce and MIC. The target AP checks the MIC and if successful installs the derived PTK for the subsequent data exchanges.

Step 6: The target AP sends a Reassociation Response including ANonce, SNonce and MIC. The UE checks the MIC and, if successful, installs likewise the PTK for the subsequent data exchanges.

Step 7: The UE and AP start securely exchanging data.

### 6.7.3 Evaluation

This solution requires new functionality of deriving a new key from an existing key in the UE and TNGF. This new key is then used to create the root key of the FT key hierarchy and hence allow the establishment of security between the UE and a new TNAP using the existing FT procedures in case of TNAP mobility. When the UE transitions from one TNAP to a new TNAP, the FT procedures enable the UE to establish a security association with the new TNAP using only 2 round trips of messages between the UE and the new TNAP.

The R0KH is part of the TNAN.

The relationship between MDID and TNGF ID will be determined in the normative phase.

The procedures in the solution are executed when the TNAN supports FT.

## 6.8 Solution #8: Security Establishment for TNAP Mobility

### 6.8.1 Introduction

The solutions address Key Issue #4.

### 6.8.2 Solution details

The solution describes to provide UE with TNGF ID and exchange freshness parameter (such as nonce to facilitate challenge and common security establishment between UE and Trusted Non-3GPP Access Network i.e., TNGF) during the Initial registration procedure (i.e., following a successful authentication for trusted non-3GPP access) as shown in Figure 6.8.2-1. Further if a UE connected to TNGF via a TNAP (i.e., say TNAP 1) decides to move to another TNAP (i.e., say TNAP 2), the solution propose to use the following Security Establishment procedure for TNAP Mobility shown in Figure 6.8.2-2 as described below.



Figure 6.8.2-1: Authentication for trusted non-3GPP access

The actual registration procedure for trusted non-3GPP access steps related to 6.8.2-1 are described in TS 23.502, clause 4.12a.2.2 and the related authentication steps are shown in TS 33.501 Clause 7A.2.1. Therefore, the necessary enhancements for steps 10b – 10e are described below.

During EAP-5G procedure (i.e., executed in steps 4-10), the additional access parameters are exchanged between the UE and the TNGF at step 10: The TNGF sends TNGF address and TNGF Nonce (TNonce) to UE in step 10b. Further the UE sends to TNGF, a UE Nonce (UNonce) in step 10c. The UE and the TNGF can derive a Reauth-ID for the UE from TNGF key using the inputs parameters such as TNGF-ID, Nonce from TNGF, Nonce from UE.



Figure 6.8.2-2: Security Establishment procedure for TNAP Mobility

The steps shown in Figure 6.8.2-2 is described as follows:

1. The UE established a layer-2 (L2) connection with TNAP2.

2. The TNAP2 initiates an EAP session as usually by requesting the UE identity.

3. The UE provides a Network Access Identifier (NAI) containing username = Reauth-ID and realm = nai.5gc.tngf<TNGF-ID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org. The Reauth-ID was derived as described for figure 6.8.2-1 and the TNGF-ID was received when the UE was first connected to TNGF, e.g. with an Initial Registration via TNGF. The UE provides username = Reauth-ID because the UE does not want to initiate NAS signaling with 5GC, but it wants to reauthenticate with the TNGF.

4. The TNAP1 selects TNGF based on the TNG1-ID in the received realm and forwards the NAI to TNGF.

5. The TNGF finds a stored UE context containing the received Reauth-ID, thus, it determines that the UE is a known UE which requests reauthentication. Therefore, it initiates the following steps. If the TNGF cannot find a stored UE context containing the received Reauth-ID, then the TNGF sends either an error response to UE, it initiates the signalling procedure related to normal authentication for trusted non-3GPP access as described in TS 33.501 Clause 7A.2.1.

 The UE context was created in the TNGF when the UE performed an initial registration (see Fig. 6.8.2-1) via TNGF.

6. The TNGF sends a 5G-Challenge packet to UE which contains a TNonce value and a Message Authentication Code1 (MAC1) derived by using the TNGF key stored in TNGF.

7. The UE derives an expected MAC1 (XMAC1) using TNGF key stored in UE, and TNonce and compares XMAC1 with the received MAC1. If they match, the TNGF is authenticated by the UE.

8. The UE generates a UNonce and derives a MAC2 using TNGF key stored in UE, and with UNonce and TNonce.

9. The UE responds with a 5G-Challenge containing UNonce, TNonce and MAC2.

10. The TNGF derives an expected MAC2 (XMAC2) using TNGF and with UNonce and TNonce. Compares XMAC2 with the received MAC2. If they match, the UE is authenticated by TNGF.

11. The TNGF derives a fresh Reauth-ID for the UE, e.g., by using TNGF key stored in TNGF, TNGF-ID, TNonce and UNonce. In addition, the TNGF derives a new TNAP key by using the TNGF key stored in TNGF, the TNGF-ID, the TNonce and UNonce values.

12. The TNGF completes the EAP-5G session by sending an EAP-Success packet to UE and the new TNAP key to TNAP2.

13. The UE derives a new Reauth-ID by using the TNGF key stored in UE, TNGF-ID, TNonce and UNonce. If the UE and the TNGF share the same TNGF key, then the Reauth-ID derived independently in the UE and in the TNGF will be the same. In addition, the UE derives also a new TNAP key similarly to the TNGF (as in step 11).

14. The new TNAP key is applied to establish over-the-air security between the UE and TNAP2. If needed, the UE may receive new IP configuration information (e.g., a new IP address).

15. The UE resumes communication with TNGF via TNAP2.

### 6.8.3 Evaluation

The solution addresses KI#4 and it enables the following aspects:

UE and TNGF performs mutual authentication during UE TNAP mobility as part of re-authentication by exchanging nonces and verifying a related MAC.

Further impacts related to the solution includes:

For UE TNAP mobility scenario, the UE and TNGF derives new TNAP key using the previously established security context (from the initial primary authentication) i.e., TNGF key and nonce(s) as a freshness parameter. The UE and TNGF need to derive a Re-auth ID, the details of the inputs is upto the normative work.UE need to construct NAI using Re-auth ID and TNGF information. The TNGF need to find a stored UE context based on Reauth-ID.

TNGF: Need to provide Nonce, TNGF ID to UE during initial registration procedure. Alternatively, an existing TNGF address can be used TNGF ID.

## 6.9 Solution #9: AUN3 device supporting 5G Key hierarchy (i.e. N5CW)

### 6.9.1 Introduction

This solution addresses the authentication of AUN3 devices supporting 5G key hierarchy(i.e. N5CW) based on the EAP\_AKA prime method.

### 6.9.2 Solution details

6.9.2.1 Procedure

 Figure 6.9.2.1-1: EAP-AKA prime based AUN3 (i.e. N5CW) 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 EAP Response/Identity message. The AUN3 device uses SUCI in NAI format (i.e., username@realm format as specified in clause 28.7.3 of TS 23.003) or 5G-GUTI.

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 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 sends a NAS Registration Request message to the AMF, including the received SUCI and the new indicator for encryption required for AUN3 device.

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

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 (KWAGF') to W-AGF.

7. W-AGF/RG derive the KRG as PMK key from the WAGF key (KWAGF').

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.

6.9.2.2 Key derivation

6.9.2.2.1 WAGF' key for AUN3 device (i.e. N5CW)

When deriving the keys KWAGF' for AUN3 from KAMF then the following parameters should be used input S to the KDF.

- FC = 0x<to be defined>

- P0 = Access type distinguisher

- L0 = length of Access type distinguisher (i.e. 0x00 0x01)

The access type distinguisher shall be set to the value for 'non-3GPP (0x02) when deriving KWAGF'.

6.9.2.2.2 KRG key

When deriving a KRG key from KWAGF' the following parameters shall be used to form the input S to the KDF.

- FC = 0x<to be defined>

- P0 = Usage type distinguisher

- L0 = length of Usage type distinguisher (i.e. 0x00 0x01)

Usage type distinguisher value is set to 0x02.

### 6.9.3 Evaluation

This solution meets both the requirements mentioned in the KI for the AUN3 device that support 5G key hierarchy. i.e.

* 5GC should be able to authenticate the AUN3 device behind RG.
* The 5GS should provide a means for the AUN3 device and RG to get a shared key that could be used to provide protection of the interface between them.

**Impact on the entities**

AUSF/UDM: New indication received for AUN3 devices and select authentication algorithm accordingly.

AMF: generates the keys and provides the same to RG/W-AGF.

RG/W-AGF: receives new key material from AMF and then derives the PMK.

UE: derive the new keys.

## 6.10 Solution #10: TNAP mobility solution without full authentication

### 6.10.1 Introduction

This solution addresses key issue #4: Security aspect of TNAP mobility

### 6.10.2 Solution details



Figure 6.10.2-1: TNAP mobility procedure

1-3. UE connected to TNAP#1 by performing the procedure defined in TS33.501 7A.2.1 step1- step19.

4. The TNGF knows the UE reconnect to the TNGF again, but via TNAP#2 by receving the same UE ID in the previous connection. The UE ID is the SUCI or 5G-GUTI used in step1.

5. TNGF finds the UE security context based on the UE ID, and determines to perform re-authentication procedure based on UE ID. The TNGF generates KTNGF’ that is equlivant to the EAP 5G reauthentication root key by using the method in A.22 of TS 33.501[xx] with the usage type distinguisher set to 0x03, with the input key KTNGF

Editor’s Note: whether the additional key is needed if FFS.

6. TNGF sends EAP-REQ message to start the re-authentication procedure, a,Nonce-TNGF and the HMAC are carried in this message. HMAC is generated by using fresh parameter and KTNGF’. TNAP#2 forwawrd this message to UE.

7. UE finds the KTNGF by using TNGF ID in step 4, and generates KTNGF’ by using the same method in step5, and verifies the HMAC. if the verification passes, perform next steps.

8. UE sends EAP-RES message, Nonce-UE and HMAC are carried in AN-Parameters of this message, HMAC is generated by using Nonce-UE parameter and KTNGF’ , TNAP#2 forward this message to TNGF.

9. TNGF verifies the HMAC, if the verification passes, TNGF generates KTNAP’ by using method defined in TS33.501 A.22.

10. TNGF sends EAP-Success message to TNAP#2, KTNAP’ generated in step 9 is carried in this message. TNAP#2 forwawrd EAP-Success message to UE.

11. After receiving EAP-Success message, UE generates KTNAP’ by using the same method in step 9.

12. UE and TNAP#2 establish security association by using the newly generated KTNAP’.

13. TS33.501 7A.2.1 step12- step19.

### 6.10.3 Evaluation

This solution addresses the requirement of KI #4 by generating a new KTNGF’.

This solution impacts UE and TNGF without affecting other NFs.

Editor’s Note: Further evaluation is FFS.

## 6.11 Solution #11: Security of N3IWF/TNGF reallocation

### 6.11.1 Introduction

This solution addresses KI#3 and is built on solution#15 in TR 23.700-17[2] v030, but only includes the N3IWF Relocation case. In this solution, an IPsec tunnel is setup before initiating the UE policy Association Establishment procedure and before the AMF sends a Registration Reject message. Please note that, according to TS 33.501[4], the NAS message is sent over IPsec tunnel. Since the conclusion in TR 23.700-17[2] has concluded that TNGF Relocation uses the same manner as N3IWF, then the solution in clause 6.11.2 can also be applied to TNGF Reallocation case.

### 6.11.2 Solution details



**Figure 6.11.2 N3IWF Relocation procedure**

NOTE: The solution can be reused to TNGF relocation case by replacing N3IWF with TNGF.

1. UE connects to S-N3IWF and sends the Registration Request message to the AMF as defined from step 1a to step 6b in clause 7.2.1 of TS 33.501[4] and as defined from step 1 to step 6b in clause 7A.2.1 of TS 33.501[4].

2. If the Registration Request contains a SUCI, AMF initiates primary authentication. If the UE contains a 5G-GUTI, and the AMF successfully verified the integrity protection of the Registration Request message, whether the AMF initiates primary authentication and NAS SMC procedure the same as what is defined in TS 33.501[4].

3. The AMF determines to use T-N3IWF as described in TR 23.700-17[2].

4. The AMF generate a KNI3WF, and sends it to the S-N3IWF for setting up the IPsec as defined from step 12 to step 15 in clause 7.2.1 of TS 33.501[4] and as defined from step 10a to step 14 in n clause 7A.2.1 of TS 33.501[4].

5. The same as step 9 described in solution#15 of TR 23.700-12[2].

6. The same as step 10a described in solution#15 of TR 23.700-12[2]. The UE and the AMF keep the security context. The AMF includes a new 5G-GUTI in the Registration Reject message.

7. After successfully verifying the integrity protection of the message in steps 5 or 6, the UE re-registered to the AMF using T-N3IWF. The Registration Request message contains the new 5G-GUTI and is protected by the security context generated in step2, or previously generated before step1.

8. If no relocation is needed again, the AMF proceeds with the rest of procedures defined in clause 7.2.1 of TS 33.501[4] and clause 7A.2.1 of TS 33.501[4]. Particularly, the AMF generates a new KNI3WF for setting up the IPsec tunnel.

9. The AMF sends NAS Registration Accept message to the UE.

### 6.11.3 Evaluation

The solution proposes to establish the IPsec tunnel before sending the redirection information (e.g. new SSID and associated Requested NSSAI) in the Registration Reject message. In this way, the security between the UE and the AMF is established and the redirection information can be protected.

6.12 Solution #12: Authentication of UE connecting to RG by NSWO

6.12.1 Introduction

This solution addresses Key Issue #5 on the authentication of UE connecting to RG, by using the NSWO procedure.

6.12.2 Solution details

A UE connecting to the 5G-RG or FN-RG via WLAN, in the case that the WLAN supports IEEE 802.1X, can use the NSWO authentication as specified in Annex S.

6.12.3 Evaluation

This solution meets the requirement that 5GS shall support authentication of UE connecting to RG using 5G credentials.

## 6.13 Solution #13: TNAP mobility using modified ERP

### 6.13.1 Introduction

This solution targets key issue #4 Security aspect of TNAP mobility without full authentication.

In earlier versions of TS 23.502 [7] it was specified that EAP re-authentication (ERP) may be used for TNAP mobility in trusted access. This would enable UEs to move from one access point to another without performing a full primary authentication. This option was removed from Rel-16 and Rel-17 since the use of ERP required this to be supported by AUSF and AMF which had not been specified in stage 3 specifications.

In short, it was specified that AUSF should generate the key rRK from EMSK and send it to the TNGF. The TNGF would then derive further keys from rRK, as specified in RFC 6696 [8] also shown below.

rRK

|

+--------+--------+

| | |

rIK rMSK1 ...rMSKn

where

**rRK** is the re-authentication Root Key, derived from the EMSK (from the EAP authentication).

**rIK** is the re-authentication Integrity Key, derived from the rRK. Used for the integrity protection of all messages between the peer and the ERP server.

**rMSK** is re-authentication MSK, derived from the rRK. There are multiple keys of this type (rMSK1, …rMSKn). These keys are derived by the ERP server and the peer.

### 6.13.2 Solution details

This solution proposes to reuse ERP for reauthentication but modify the method of how the root key (rRK) is derived. Instead of deriving the key rRK from EMSK, the rRK is derived from KTNGF.

Section 4.2 of RFC 6696 [8] specifying ERP, the properties for rRK are listed:

 The rRK has the following properties. These properties apply to the

 rRK regardless of the parent key used to derive it.

 o The length of the rRK MUST be equal to the length of the parent

 key used to derive it.

 o The rRK is to be used only as a root key for re-authentication and

 never used to directly protect any data.

 o The rRK is only used for the derivation of the rIK and rMSK as

 specified in this document.

 o The rRK MUST remain on the peer and the server that derived it and

 MUST NOT be transported to any other entity.

 o The lifetime of the rRK is never greater than that of its parent

 key. The rRK is expired when the parent key expires and MUST be

 removed from use at that time.

The above properties do not require that rRK is derived from EMSK, nor does it require that the rRK is derived by the EAP server.

To fulfil the above properties, it is possible to derive the key rRK from KTNGF as long as the other keys derived from KTNGF are separated from the rRK and that the rRK is not used for anything else than further key derivation. The current key hierarchy for trusted access is displayed in Figure 6.13.2-1. A proposal for how the key hierarchy can be made to reflect the needs is provided in Figure 6.13.2-2.

A new type of key, rRK, is derived from KTNGF. The derivation of rRK is performed according to section 4.1 of RFC 6696 [8] replacing the input key EMSK with the key KTNGF.

The difference is that no extra key needs to be transferred from the AMF and no ERP requests needs to be sent.



**Figure 6.13.2-1 Current key hierarchy for trusted non-3GPP access**



**Figure 6.13.2-2 Proposal for updated key hierarchy for trusted non-3GPP access to support TNAP mobility**

Editor's Note: Initial UE identifier between UE and target TNAP, and its protection, are ffs.

Editor's Note: Session correlation at the TNGF when the target TNAP contacts the TNGF is ffs.

Editor's Note: Further details on the key derivation are ffs.

Editor's Note: The need to modify rRK derivation in ERP is FFS.

Editor's Note: The problem with current rRK derivation specified in ERP (i.e., to use EMSK) is FFS.

Editor's Note: The steps and procedure for ERP bootstrapping and the ERP procedure are FFS.

### 6.13.3 Evaluation

Editor's Note: Evaluation is ffs.

## 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.

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

It is concluded that solutions #2, #3, and #4 are used as the basis for normative specifications for authentication of AUN3 devices behind RG, where the AUN3 devices do not support 5G key hierarchy. More specifically,

* Solution #2 is used as the basis for PLMN
* Solution #3 and #4 are used as the basis for SNPN.

The AUN3 device supporting the 5G key hierarchy is also called the N5CW device. It is concluded that solution #9 is used as a basis for the normative specification.

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

SA2 TR 23700-17 was fully concluded for the KI2, where SA2 preferred UE-centric solutions. However, the information is delivered to the UE via PCF policies (ANDSP/WLANSP), which is protected by NAS security.

KI#2 was proposed on the basis of solution 13 and solution 14 in TR 23.700-17 where unprotected slice information is shared between UE and the network. However, Solution 13 and Solution 14 have not been chosen for normative work in TR23.700-17, hence this key issue does not need any normative work.

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

For both TNGF and N3IWF, solution #11 is the basis for normative work.

## 7.4 Key issue #5: Authentication of UE connecting to RG using NSWO

It is concluded that solution #12 is used as the basis for 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: S3-221341, 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 |
| 2022-10 | SA3#108Adhoc-e | S3-223127 |  |  |  | Inclusion of the documents approved at SA3#108Adhoc-e: S3-222935, S3-222936, S3-222937, S3-222939, S3-222940, S3-223007, S3-223008, S3-223009 | 0.3.0 |
| 2022-11 | SA3#109 | S3-224056 |  |  |  | Inclusion of the documents approved at SA3#109: S3-224048, S3-224049, S3-224050, S3-224051, S3-224052, S3-224053, S3-224054, S3-224055, S3‑223512, S3‑223881 | 0.4.0 |
| 2023-01 | SA3#109Adhoc-e | S3-230425 |  |  |  | Inclusion of the documents approved at SA3#109Adhoc-e: S3-230049,S3-230050, S3-230051,S3-230052,S3-230426, S3-230427, S3-230446, S3-230480, S3-230194, S3-230195, S3-230481, [S3-230439](https://apc01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_109AdHoc-e%2FDocs%2FS3-230285.zip&data=05%7C01%7Csmary%40LENOVO.COM%7Ca99fc658e27e4bf9479c08dafa2e3abe%7C5c7d0b28bdf8410caa934df372b16203%7C0%7C0%7C638097374104339869%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=H1zk4bOKw9Q6CFoAxV0nv3w%2B6HsF4pT9pldJhNc%2BdCE%3D&reserved=0), S3-230526, S3-230418, | 0.5.0 |
| 2023-02 | SA3#110 | S3-231511 |  |  |  | Inclusion of the documents approved at SA3#110: S3-231328, S3-230699, S3-230988, S3-231512, S3‑231513, S3‑231514, S3-230987 | 0.6.0 |