|  |
| --- |
| 3GPP TR 33.702 V0.1.0 (2024-02) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security for mobility over non-3GPP access to avoid full primary authentication (Release 19) |
|   |
|  |  |
| 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.© 2024, 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 6

Introduction 7

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 9

3.3 Abbreviations 9

4 Security Assumptions 9

4.1 Task 1: UE connecting to the new TNAP within the same TNGF 9

4.2 Task 2: AUN3 device connecting to a new 5G-RG under the same W-AGF 9

4.3 Task 3: N5CW device connecting to a new TWAP under the same TWIF 10

4.4 Task 4: UE connecting to a new WLAN AP connected via the same NSWOF 11

5 Key issues 11

5.1 Key issue #1: Security aspect of UE connecting to a new TNAP within the same TNGF. 12

5.1.1 Key issue details 12

5.1.2 Threats 12

5.1.3 Potential security requirements 12

5.2 Key issue #2: Security aspect of AUN3 device connecting to a new 5G-RG within the same W-AGF. 12

5.2.1 Key issue details 12

5.2.2 Threats 12

5.2.3 Potential security requirements 12

5.3 Key issue #3: Security aspect of N5CW device connecting to a new TWAP within the same TWIF. 13

5.3.1 Key issue details 13

5.3.2 Threats 13

5.3.3 Potential security requirements 13

5.4 Key issue #4: Security aspect of UE connecting to a new WLAN AP connected via the same NSWOF. 13

5.4.1 Key issue details 13

5.4.2 Threats 13

5.4.3 Potential security requirements 13

5.X Key Issue #X: <Key Issue Name> 14

5.X.1 Key issue details 14

5.X.2 Security threats 14

5.X.3 Potential security requirements 14

6 Solutions 14

6.0 Mapping of solutions to key issues 14

6.1 Solution #1: TNAP mobility solution with rand 14

6.1.1 Introduction 14

6.1.2 Solution details 15

6.2 Solution #2: TNAP mobility solution with count 16

6.2.1 Introduction 16

6.2.2 Solution details 17

6.2.3 Evaluation 18

6.3 Solution #3: Using Fast BSS Transition for TNAP mobility 19

6.3.1 Introduction 19

6.3.2 Solution details 19

6.3.2.1 Solution overview 19

6.3.2.2 Details of FT 20

6.3.3 Evaluation 21

6.4 Solution #4: Security Establishment for TNAP Mobility 22

6.4.1 Introduction 22

6.4.2 Solution details 22

6.4.3 Evaluation 24

6.5 Solution #5: TNAP mobility solution without full authentication 24

6.5.1 Introduction 24

6.5.2 Solution details 25

6.5.3 Evaluation 26

6.6 Solution #6: TNAP mobility using modified ERP 26

6.6.1 Introduction 26

6.6.2 Solution details 27

6.6.3 Evaluation 29

6.7 Solution #7: Using Fast BSS Transition for N5CW mobility 29

6.7.1 Introduction 29

6.7.2 Solution details 30

6.7.2.1 Solution overview 30

6.7.3 Evaluation 30

6.Y Solution #Y: <Solution Name> 30

6.Y.1 Introduction 30

6.Y.2 Solution details 30

6.Y.3 Evaluation 30

7 Conclusions 30

Annex <X> (informative): Change history 31

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

Editor’s Note: This clause contains some background information for the study.

# 1 Scope

The following objectives will be studied in this document:

* Study the security aspects and procedure enhancements needed to support UE connecting to a new target TNAP within the same TNGF without performing full primary authentication.
* Study the security aspects and procedure enhancements needed to support AUN3 connecting to a new target RG under the same WAGF without performing full primary authentication.
* Study the security aspects and procedure enhancements needed to support N5CW devices connecting to a new target Trusted WLAN AP within the same TWIF without performing full primary authentication.
* Study the security aspects and procedure enhancements needed to support UE connecting to a new WLAN AP that shares the same NSWOF without performing full authentication.

The present document does not cover actual mobility, where call/session continuity is maintained. I.e., when UE/device is moving from one AP/TNAP/TWAP to another, connectivity can break, and then UE will reconnect.

# 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 33.887: " Study on security aspects for support for 5G Wireless and Wireline Convergence (5WWC) phase 2”

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

[4] 3GPP TS 23.502: "Procedures for the 5G System"

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Security Assumptions

## 4.1 Task 1: UE connecting to the new TNAP within the same TNGF

Solutions for KI4 in TR 33.887 [2] are reproduced in the present document.

Here is the architecture diagram for UE moving from TNAP1 to TNAP2, connected via the same TNGF.



Figure 4.1-1: UE moves from TNAP1 to TNAP2

## 4.2 Task 2: AUN3 device connecting to a new 5G-RG under the same W-AGF

The AUN3 device does not support NAS over non 3GPP Access and connect to 5GC via RG. 5G-RG creates NAS Registration on behalf of AUN3 device. Authentication is defined in TS 33.501[3], clause 7B-7 and Annex Z.

Figure 4.2-1 AUN3 device connection to 5G

Here is the architecture diagram for AUN3 moving from 5G-RG1 to 5G-RG2, connected via the same W-AGF.



Figure 4.2-2: AUN3 device moves from 5G-RG to another 5G-RG

## 4.3 Task 3: N5CW device connecting to a new TWAP under the same TWIF

The N5CW device does not support NAS over non 3GPP Access and connect to 5GC via TWIF. TWIF creates NAS Registration on behalf of N5CW device. Authentication of N5CW device via trusted WLAN is defined in TS 33.501[3], clause 7A.2.4.

Here is the architecture diagram for N5CW moving from TWAP1 to TWAP2, connected via the same TWIF.



Figure 4.3-1: N5CW device moves from TWAP1 to TWAP2

## 4.4 Task 4: UE connecting to a new WLAN AP connected via the same NSWOF

Here is the architecture diagram for UE moving from one WLAN to another WLAN, connected via the same NSWOF.



Figure 4.4-1: UE moves from WLAN AP to another WLAN AP connected via the same NSWOF

# 5 Key issues

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

## 5.1 Key issue #1: Security aspect of UE connecting to a new TNAP within the same TNGF.

### 5.1.1 Key issue details

When UE moves from TNAP1 to TNAP2, where both TNAPs are nearby or overlapping, the UE connectivity can break while connecting to the new TNAP2. Additionally, UE also goes through another full primary authentication procedure, even though the second non-3GPP access connects to the same TNGF.

A new full primary authentication may lead to additional signalling and may cause latency in the UE connection. If we skip the full primary authentication, it provides connection time optimisation, but then the security aspect of UE to target TNAP/TNGF should be studied.

### 5.1.2 Threats

Not applicable.

### 5.1.3 Potential security requirements

The 5GS should support a mechanism to establish secure connection for the UE switching from one TNAP to another TNAP within the same TNGF without performing full primary authentication.

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.

## 5.2 Key issue #2: Security aspect of AUN3 device connecting to a new 5G-RG within the same W-AGF.

### 5.2.1 Key issue details

When AUN3 device moves from 5G-RG1 and 5G-RG2, where both 5G-RG are nearby or overlapping, the AUN3 device connectivity can break while connecting to the new 5G-RG2. Additionally, AUN3 also goes through another full primary authentication procedure, even though both 5G-RGs connects to the same W-AGF.

A new full primary authentication may lead to additional signalling and may cause latency in the AUN3 device connection. If we skip the full primary authentication, it provides connection time optimisation, but then the security aspect of the AUN3 device to target 5G-RG should be studied.

### 5.2.2 Threats

Not applicable.

### 5.2.3 Potential security requirements

The 5GS should support a mechanism to establish secure connection for the AUN3 device switching from one 5G-RG to another 5G-RG within the same W-AGF without performing full primary authentication.

While switching from one 5G-RG to another 5G-RG within the same W-AGF, the interface between AUN3 device and the new 5G-RG shall be confidentiality, integrity, and replay protected.

## 5.3 Key issue #3: Security aspect of N5CW device connecting to a new TWAP within the same TWIF.

### 5.3.1 Key issue details

When the N5CW device moves from TWAP1 to TWAP2, where both TWAPs are nearby or overlapping, the N5CW device connectivity can break while connecting to the new TWAP. Additionally, the N5CW device also goes through another full primary authentication procedure, even though both TWAPs connect to the same TWIF.

A new full primary authentication may lead to additional signalling and may cause latency in the N5CW device connection. If we skip the full primary authentication, it provides connection time optimisation, but then the security aspect of the N5CW device to target TWAP should be studied.

### 5.3.2 Threats

Not applicable.

### 5.3.3 Potential security requirements

The 5GS should support a mechanism to establish secure connection for the N5CW device switching from one TWAP to another TWAP within the same TWIF without performing full primary authentication.

While switching from one TWAP to another TWAP within the same TWIF, the interface between the N5CW device and the new TWAP shall be confidentiality, integrity, and replay protected.

## 5.4 Key issue #4: Security aspect of UE connecting to a new WLAN AP connected via the same NSWOF.

### 5.4.1 Key issue details

When UE moves from WLAN AP1 to WLAN AP2, where both WLAN APs are nearby or overlapping, the UE connectivity can break while connecting to the new WLAN AP. Additionally, UE also goes through another full authentication procedure at the NSWOF as defined in annex S of TS 33501[3], even though both WLAN APs connect to the same NSWOF.

A new full authentication may lead to additional signalling and may cause latency in the UE connection. This is inefficient and disrupts the user experience. If we skip the full authentication, it provides connection time optimisation, but then the security aspect of the UE to target WLAN should be studied.

### 5.4.2 Threats

Not applicable.

### 5.4.3 Potential security requirements

The 5GS should support a mechanism to authenticate the UE switching from one WLAN AP to another WLAN AP connected to the same NSWOF without performing full authentication.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Editor’s Note: Each solution should be mapped here.

## 6.1 Solution #1: TNAP mobility solution with rand

### 6.1.1 Introduction

This solution addresses the security solution of TNAP mobility defined in KI#1.

### 6.1.2 Solution details

6.1.2.1 Procedure



Figure 6.1.2-1 TNAP mobility procedure

UE is connected to TNAP#1 via the procedure defined in TS 33.501[3] 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 6.1.2.2 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.

6.1.2.2 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.

## 6.2 Solution #2: TNAP mobility solution with count

### 6.2.1 Introduction

This solution addresses the security issue due to TNAP mobility defined in KI#1.

### 6.2.2 Solution details

6.2.2.1 Procedure



Figure 6.2.2-1 TNAP mobility procedure

1) UE is connected to TNAP#1 via the procedure defined in TS 33.501[3] 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 6.2.2.2 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.

6.2.2.2 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.

### 6.2.3 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

NOTE: Count desynchronization issue is not addressed in this solution.

## 6.3 Solution #3: Using Fast BSS Transition for TNAP mobility

### 6.3.1 Introduction

This solution addresses key issue #1: Security aspect of TNAP mobility

### 6.3.2 Solution details

#### 6.3.2.1 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 [3] 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 6.3.2-1 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 6.3.2-1 shows how the 5G and FT key hierarchies link together in this solution.



Figure 6.3.2-1: 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.

#### 6.3.2.2 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 6.3.2.2-1 show a UE attaching to the first AP that results in establishing the FT key hierarchy.



Figure 6.3.2.2-1: 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 6.3.2.2-2 shows AP mobility using the over the air procedure.



Figure 6.3.2.2-2: AP mobility

Steps 0: The UE has connected to an AP and established the FT key hierarchy as shown in Figure 6.3.2.2-1.

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.

### 6.3.3 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.

## 6.4 Solution #4: Security Establishment for TNAP Mobility

### 6.4.1 Introduction

The solutions address Key Issue #1.

### 6.4.2 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 6.4.2-1. 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 6.4.2-2 as described below.



Figure 6.4.2-1: 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[4], clause 4.12a.2.2 and the related authentication steps are shown in TS 33.501[3] 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 6.4.2-2: Security Establishment procedure for TNAP Mobility

The steps shown in Figure 6.4.2-2 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 6.4.2-1 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[3] Clause 7A.2.1.

 The UE context was created in the TNGF when the UE performed an initial registration (see Fig. 6.4.2-1) 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.

### 6.4.3 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.

## 6.5 Solution #5: TNAP mobility solution without full authentication

### 6.5.1 Introduction

This solution addresses key issue #1: Security aspect of TNAP mobility.

In this solution, the TNAP is the EAP authenticator and the TNGF is the authentication server. The full authentication means the UE runs an EAP-5G authentication with the TNGF and run a primary authentication with the AUSF that is encapsulated in the EAP-5G authentication. Compare to the full authentication, this procedure does not need to run the primary authentication with AUSF, thus it is referred to as the non-full(without full) authentication procedure.

### 6.5.2 Solution details



Figure 6.5.2-1: TNAP mobility procedure

1-3. UE connected to TNAP#1 by performing the procedure defined in TS33.501[3] 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[3] with the usage type distinguisher set to 0x03, with the input key KTNGF

Note: whether the additional key KTNGF is needed is not addressed in this solution.

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 forward 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[3] A.22.

10. TNGF sends EAP-Success message to TNAP#2, KTNAP’ generated in step 9 is carried in this message. TNAP#2 forward 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[3] 7A.2.1 step12- step19.

### 6.5.3 Evaluation

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

This solution impacts UE and TNGF without affecting other NFs.

This solution proposes to use the SUCI or 5G-GUTI used in the IDi of IPsec as the key identifier in the non-full authentication procedure to locate the key KTNGF. In case the UE used SUCI in the primary authentication it need to store the SUCI and use it when it wants to TNAP mobility.

## 6.6 Solution #6: TNAP mobility using modified ERP

### 6.6.1 Introduction

This solution targets key issue #1 Security aspect of TNAP mobility without full authentication.

In earlier versions of TS 23.502 [4] 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.

### 6.6.2 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 6.6.2-1. A proposal for how the key hierarchy can be made to reflect the needs is provided in Figure 6.6.2-2.

In this solution, the 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 lower layer keys (rIK, rMSK1, etc) are derived from rRK according to RFC 6696 [8].

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

Another difference compared to ERP is that in standard ERP, the AUSF would need to receive an indication to derive rRK during primary authentication. This is called the bootstrapping steps of ERP. With the proposed modification however, a similar bootstrapping is not needed since the rRK will be based on KTNGF that is anyway present in the TNGF. This means that the bootstrapping is implicit rather than explicit. The rRK can be derived by TNGF once a mobility request is received or at any time when it is convenient.



Figure 6.6.2-1 Current key hierarchy for trusted non-3GPP access



Figure 6.6.2-2 Proposal for updated key hierarchy for trusted non-3GPP access to support TNAP mobility

NOTE 1: Initial UE identifier between UE and target TNAP, and its protection is not addressed by this document.

NOTE 2: Session correlation at the TNGF when the target TNAP contacts the TNGF is not addressed by this document.

### 6.6.3 Evaluation

This solution modifies the key derivation in ERP.

The procedures are based on KTNGF instead of EMSK.

The solution impacts TNGF and UE.

NOTE 1: Initial UE identifier between UE and target TNAP, and its protection is not addressed by this document.

NOTE 2: Session correlation at the TNGF when the target TNAP contacts the TNGF is not addressed by this document.

## 6.7 Solution #7: Using Fast BSS Transition for N5CW mobility

### 6.7.1 Introduction

This solution addresses key issue #1

### 6.7.2 Solution details

#### 6.7.2.1 Solution overview

The solution#3 can be reused by replacing the following parameters:

1. replace UE with N5CW.

2. replace TNGF with TWIF

3. replace KTNGF with KTWIF

### 6.7.3 Evaluation

Evaluation in solution#3 can be reused.

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

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-240315 |  |  |  | TR Skeleton | 0.0.0 |
| 2024-02 | SA3#115 | S3‑240927 |  |  |  | Inclusion of the documents approved at SA3#115:S3‑240925, S3‑240920, S3‑240921, S3‑240922, S3‑240923, S3‑240924, S3‑240364, S3‑240926  | 0.1.0 |
|  |  |  |  |  |  |  |  |