|  |  |
| --- | --- |
| 3GPP TR 33.702 V0.3.0 (2024-05) | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Security Assumptions 8

4.1 Task 1: UE connecting to the new TNAP within the same TNGF 8

4.2 Task 2: AUN3 device connecting to a new 5G-RG under the same W-AGF 8

4.3 Task 3: N5CW device connecting to a new TWAP under the same TWIF 9

4.4 Task 4: UE connecting to a new WLAN AP connected via the same NSWOF 10

5 Key issues 10

5.1 Key issue #1: Security aspect of UE connecting to a new TNAP within the same TNGF. 11

5.1.1 Key issue details 11

5.1.2 Threats 11

5.1.3 Potential security requirements 11

5.2 Key issue #2: Security aspect of AUN3 device connecting to a new 5G-RG within the same W-AGF. 11

5.2.1 Key issue details 11

5.2.2 Threats 11

5.2.3 Potential security requirements 11

5.3 Key issue #3: Security aspect of N5CW device connecting to a new TWAP within the same TWIF. 12

5.3.1 Key issue details 12

5.3.2 Threats 12

5.3.3 Potential security requirements 12

5.4 Key issue #4: Security aspect of UE connecting to a new WLAN AP connected via the same NSWOF. 12

5.4.1 Key issue details 12

5.4.2 Threats 12

5.4.3 Potential security requirements 12

5.X Key Issue #X: <Key Issue Name> 13

5.X.1 Key issue details 13

5.X.2 Security threats 13

5.X.3 Potential security requirements 13

6 Solutions 13

6.0 Mapping of solutions to key issues 13

6.1 Solution #1: TNAP mobility solution with rand 13

6.1.1 Introduction 13

6.1.2 Solution details 14

6.1.3 Evaluation 15

6.2 Solution #2: TNAP mobility solution with count 16

6.2.1 Introduction 16

6.2.2 Solution details 16

6.2.3 Evaluation 18

6.3 Solution #3: Using Fast BSS Transition for TNAP mobility 18

6.3.1 Introduction 18

6.3.2 Solution details 18

6.3.2.1 Solution overview 18

6.3.2.2 Details of FT 19

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

6.8 Solution #8: N5CW device reconnecting 30

6.8.1 Introduction 30

6.8.2 Solution details 31

6.8.3 Evaluation 32

6.9 Solution #9: N5CW device mobility solution with Nonce 32

6.9.1 Introduction 32

6.9.2 Solution details 33

6.9.3 Evaluation 35

6.10 Solution #10: FBSS over 5G architecture 35

6.10.1 Introduction 35

6.10.2 Solution details 35

6.10.3 Evaluation 35

6.11 Solution #11: Mobility of N5CW devices 35

6.11.1 Introduction 35

6.11.2 Solution details 36

6.11.3 Evaluation 37

6.12 Solution #12: AUN3 device mobility solution with Nonce 37

6.12.1 Introduction 37

6.12.2 Solution details 37

6.12.3 Evaluation 41

6.13 Solution #13: ERP based re-authentication for NSWO 41

6.13.1 Introduction 41

6.13.2.1 Solution overview 42

6.13.2.2 UE Re-Authentication Procedure for NSWO 43

6.13.3 Evaluation 43

6.14 Solution #14: solution for UE connecting to a new WLAN AP connected via the same NSWOF. 44

6.14.1 Introduction 44

6.14.2 Solution details 44

6.14.2.1 MSK refresh 46

6.14.3 Evaluation 46

6.15 Solution #15: Using FT for NSWO 46

6.15.1 Introduction 46

6.15.2 Solution details 47

6.15.3 Evaluation 47

6.Y Solution #Y: <Solution Name> 47

6.Y.1 Introduction 47

6.Y.2 Solution details 47

6.Y.3 Evaluation 47

7 Conclusions 47

Annex <X> (informative): Change history 48

# 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 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"

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

[6] RFC 5448: "Improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA')"

[7] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS) "

# 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.

A black background with white text

Description automatically generated

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 5G-RG. 5G-RG creates NAS Registration on behalf of AUN3 device. Authentication and key hierarchy are defined in TS 33.501[3], clause 7B-7 and Annex Z. The FN-RG is not in the scope of this study.



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.

A black background with white text

Description automatically generated

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.

A black background with white text

Description automatically generated

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 as defined in Annex S of TS 33.501[3].

A diagram of a plan

Description automatically generated with medium confidence

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

# 5 Key issues

## 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 to 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 33.501 [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.

# 6 Solutions

## 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: TNAP mobility solution with rand | X |  |  |  |
| Solution #2: TNAP mobility solution with count | X |  |  |  |
| Solution #3: Using Fast BSS Transition for TNAP mobility | X |  |  |  |
| Solution #4: Security Establishment for TNAP Mobility | X |  |  |  |
| Solution #5: TNAP mobility solution without full authentication | X |  |  |  |
| Solution #6: TNAP mobility using modified ERP | X |  |  |  |
| Solution #7: Using Fast BSS Transition for N5CW mobility |  |  | X |  |
| Solution #8: N5CW device reconnecting |  |  | X |  |
| Solution #9: N5CW device mobility solution with Nonce |  |  | X |  |
| Solution #10: FBSS over 5G architecture | X |  | X |  |
| Solution #11: Mobility of N5CW devices |  |  | X |  |
| Solution #12: AUN3 device mobility solution with Nonce |  | X |  |  |
| Solution #13: ERP based re-authentication for NSWO |  |  |  | X |
| Solution #14: solution for UE connecting to a new WLAN AP connected via the same NSWOF. |  |  |  | X |
| Solution #15: Using FT for NSWO |  |  |  | X |
|  |  |  |  |  |

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

### 6.1.1 Introduction

This solution addresses the security solution of TNAP mobility as 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. Temporary number can also be generated at UE and the network independently.

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. The UE response shall contain reauth Id if available from the previous connection, otherwise, UE response shall contain SUCI or 5G-GUTI.

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 in EAP-5G notification. 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). If the TNGF is not able to identify the context based on the reauth Id, then TNGF rejects the request and then UE provides the SUCI or 5G-GUTI.

9, 10,11. The TNAP#2 sends an EAP-5G 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



Figure 6.1.2.2-1 TNAP Mobility 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.

### 6.1.3 Evaluation

The solution addresses KI#1.

UE and TNGF perform 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 |

## 6.2 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 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



Figure 6.2.2.2-1 TNAP mobility 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 as described in 802.11[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 802.11[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 hierarchy as 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 802.11 [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 and #3.

### 6.4.2 Solution details

The solution describes to provide UE with TNGF ID and exchange freshness parameter (such as nonce to facilitate 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 is described below.

During EAP-5G procedure (i.e., executed in steps 4-10), at step 10b: The TNGF sends TNGF address and TNGF Nonce (TNonce) to UE. 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.



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 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 a suitable usage type distinguisher.

6a. The TNGF sends the EAP-5G notification to UE with Tnonce along with MAC (derived using the TNGF key for integrity protection) and the new TNAP key to TNAP2 in AAA message.

7. The UE following a successful MAC verification, derives a new Reauth-ID (using inputs same as described in step 5), the UE derives also a new TNAP key similarly to the TNGF (as in step 5).

8a-b. 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).

9. The UE resumes communication with TNGF via TNAP2.

Solution Adaptations for KI#3:

The solution#4 can be reused by replacing the following aspects: a) replace UE with N5CW; b) replace TNGF with TWIF; c) replace KTNGF with KTWIF; and d) replace TNAP with TWAP. Step 6a-b, EAP-5G notification can be skipped and the Tnonce can be sent over AAA to TWAP and further over L2 to N5CW.

### 6.4.3 Evaluation

The solution addresses KI#1 and it enables the following aspects.

Further impacts related to the solution includes:

For UE TNAP mobility scenario, the UE and TNGF derives new TNAP key following a successful MAC verification 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. The solution impacts EAP-5G procedure

TNGF: Need to provide Nonce during initial registration procedure and the existing TNGF address can be used as TNGF ID.

For KI#3, the evaluation is same as KI#1.

## 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

A screenshot of a computer

Description automatically generated

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 receiving 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 equivalent 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 #1 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 needs 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 #3

### 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.

## 6.8 Solution #8: N5CW device reconnecting

### 6.8.1 Introduction

This solution addresses the security solution of KI#3.

### 6.8.2 Solution details

T

Figure 6.8.2-1 N5CW mobility procedure

0: N5CW device is connected and authenticated via TWAP1 and TWIF as defined in clause 7A.2.4 of TS 33.501[3]. Once authenticated, TWIF sends the reauth Id to UE.

Format of the reauth id follows:

username/temp number>@nai-reauthent.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.

NOTE: Currently the NAI is defined as NAI = "<any\_username>@nai.5gc. mnc<MNC>.mcc<MCC>.3gppnetwork.org". For TWIF to identify the NAI or reauth Id, both should have a different format.

Alternatively, temporary number of reauth Id can be generated by UE as well.

Steps 1 is similar to step 1 defined in clause 7A.2.4 of TS 33.501[3].

2. The N5CW device shall send back an EAP response/Identity with reauth id if available. Otherwise, N5CW device respond with SUCI or 5G-GUTI as defined in step 2b of clause 7A.2.4 of TS 33.501[3]. Reauth Id shall contain home realm and temporary unique number to identify the UE.

3. The TWIF is able to retrieve the context based on reauth id. If the TWIF is not able to identify the context based on the reauth Id, then TWIF rejects the request and then N5CW device provides the SUCI or 5G-GUTI.

4. If TWIF is able to retrieve the context, the TWIF may skip the authentication and further derive the KTNAP from the KTWIF and generate reauth Id .

5. The TWIF shall send the TNAP key, RAND value, MAC value of the RAND and the Success indication in a message to the TNAP2.

6. TNAP2 forwards the with RAND to the N5CW device.

7. When N5CW device receives a RAND value along with EAP-SUCCESS, then N5CW device drives the KTNAP. If MAC is provided, the MAC verification is also performed.

8. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication, similar to step 12 in clause 7A.2.4 of TS 33.501[3]. TNAP2 forwards the Reauth Id to N5CW device via EAP-Req/Notification. Alternatively, Reauth Id can be provided in step 6 as well.

**Key Derivation**

When deriving KTNAP keys from the KTWIF for N5CW device during the mobility, the following parameters shall be used to form the string S.

- FC = 0xx

- P0 = RAND value

- L0 = length of RAND value

KTWIF is used as root key.

### 6.8.3 Evaluation

Impact on the nodes/device:

|  |  |
| --- | --- |
| Node/UE/NF | solution |
| N5CW device | - Derive new KTNAP keys  - receive reauth Id from TWIF and provide the same as NAI to next TNAP |
| TWIF | - Derive new KTNAP keys  - provide RAND and reauth Id to N5CW device. |
|  |  |

## 6.9 Solution #9: N5CW device mobility solution with Nonce

### 6.9.1 Introduction

This solution addresses key issue #3: Security aspect of N5CW device connecting to a new TWAP within the same TWIF.

In this solution, full authentication may be skipped if N5CW device is authenticated using security context which is obtained from a previous full authentication.

### 6.9.2 Solution details

6.9.2.1 Procedure



Figure 6.9.2.1-1 TWAP change procedure for N5CW device

1. N5CW device is connected to TWAP#1 as specified in clause 7A.2.4 in TS 33.501 [3] with the following changes:
   1. N5CW device generates NonceN5CW and sends it in EAP-Res/Identity. It indicates that N5CW device can perform horizontal key derivation on KAMF as specified in clause 6.9.2.2 of this document.
   2. AMF, which knows the N5CW device's capability, generates NonceAMF and 5G-GUTI after the primary authentication and AMF sends NonceAMF and 5G-GUTI to N5CW device.
   3. After the primary authentication, AMF and N5CW device store KAMF, 5G-GUTI and NonceAMF in the security context.
2. N5CW device decides to move from TWAP#1 to TWAP#2
3. TWAP#2 sends an EAP request/Identity to the N5CW device.
4. The N5CW generates a NonceN5CW and MACN5CW, before sending back an EAP response/Identity including 5G-GUTI, NonceN5CW, and MACN5CW. MACN5CW is generated using KAMF and NonceAMF received in step 1. MACN5CW may be the part of the output (e.g., most significant 128-bits of the output).
5. TWAP#2 sends AAA request to TWIF and the request includes 5G-GUTI, NonceN5CW, and MACN5CW.
6. TWIF creates a 5GC Registration Request message on behalf of the N5CW device. The Registration Request message contains 5G-GUTI, NonceN5CW, and MACN5CW.
7. TWIF sends the Registration Request message to AMF.
8. If the AMF is different from the old AMF which allocated the 5G-GUTI in step 1, the new AMF retrieves SUPI and security context from the old AMF. AMF verifies the MACN5CW using KAMF and NonceAMF stored in the security context. If the verification successful and AMF decides to skip a full authentication based on an operator's policy, the full authentication is skipped. AMF generates a new NonceAMF and 5G-GUTI. AMF also computes MACAMF using KAMF and NonceN5CW received in step 5. MACAMF may be the part of the output (e.g., most significant 128-bits of the output).
9. AMF performs horizontal key derivation on KAMF as specified in clause 6.9.2.2 using existing KAMF, NonceN5CW received in step 7, NonceAMF generated in step 8. AMF stores newly derived KAMF, 5G-GUTI, and newly generated NonceAMF in its security context. AMF derives KTWIF from the newly derived KAMF as specified in Annex A.9 in TS 33.501 [3].
10. NAS SMC procedure is performed as specified in clause 7A.2.4 in TS 33.501 [3].
11. AMF sends an N2 Initial Context Setup Request and provides the KTWIF key, NonceAMF, and MACAMF to TWIF.
12. TWIF derive a TNAP key, KTNAP, from KTWIF as specified in Annex A.22 in TS 33.501 [3]
13. TWIF sends the TNAP key, EAP Success message, NonceAMF, and MACAMF to the TWAP#2, which forwards EAP Success, NonceAMF, and MACAMF to the N5CW device.
14. The N5CW device verifies the MACAMF using NonceN5CW generated in step 4 and existing KAMF. If the verification is successful, the N5CW performs horizontal key derivation on KAMF as specified in clause 6.9.2.2 of this document using existing KAMF, NonceN5CW generated in step 4, and NonceAMF received in step 13. The N5CW device stores 5G-GUTI, the newly received NonceAMF, and newly derived KAMF in its security context. The N5CW device derives KTWIF and KTNAP from the newly derived KAMF as specified in Annex A.9 and Annex A.22 in TS 33.501 [3], respectively.
15. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication. A layer-2 or layer-3 connection is established between the TWAP#2 and TWIF for transporting all user-plane traffic of the N5CW device to TWIF.
16. The TWIF sends N2 Initial Context Setup Response message to the AMF.

6.9.2.2 Horizontal key derivation on KAMF

Horizontal key derivation on KAMF is performed similar to Annex A.13 in TS 33.501 [3] with some changes:

Derivation of KAMF' from KAMF during mobility in N5CW device uses the following input parameter:

* FC = 0xXX
* P0 = NonceN5CW
* L0 = length of NonceN5CW
* P1 = NonceAMF
* L1 = length of NonceAMF

The input key KEY is KAMF.

NOTE: FC value to be determined during normative phase.

### 6.9.3 Evaluation

This solution has impact on AMF.

Impact on the entities:

|  |  |
| --- | --- |
| Entity | solution |
| N5CW device | - generates and provides NonceN5CW to AMF.  - calculates MACN5CW using NonceAMF and KAMF.  - derives new PMK using newly derived KAMF.  - verifies MACAMF and stores NonceAMF with KAMF in its security context. |
| AMF | - verifies MACN5CW and computes MACAMF using NonceN5CW and KAMF.  - derives new PMK using newly derived KAMF.  - generates and provides NonceAMF to N5CW.  - stores NonceAMF with KAMF in its security context. |

Editor’s Note: Further evaluation is FFS.

## 6.10 Solution #10: FBSS over 5G architecture

### 6.10.1 Introduction

The solution address KI#1 and KI#3.

### 6.10.2 Solution details

If FBSS is determined to use for UE TNAP mobility by the network (i.e., TNGF), then Solution #3 aspects can be used as baseline with the following adaptations:

The Root Key holder (R0KH) functionality is co-located/offered by the TNGF.

The TNGF determines to use FT and initiate FT key hierarchy if both the UE and TNAP supports FT protocol (if the TNAP supports 802.11). The TNAP’s FT capability can be sent to the TNGF in any AAA message during the primary authentication.

NOTE 1: Following FT key derivation, further steps 10d to step 22 are same as in TS 33.501 [3] Clause 7A.2.1, figure 7A.2.1-1.

Solution Adaptations for KI#3:

The solution can be reused by replacing the following aspects: a) replace UE with N5CW; b) replace TNGF with TWIF; c) replace KTNGF with KTWIF; and d) replace TNAP with TWAP.

### 6.10.3 Evaluation

Evaluation in solution#3 can be reused with the following additional aspects.

The solution reuses existing trusted non-3GPP access architecture.

The TNGF need to know UE and TNAP’s FT support to initiate FT key hierarchy. TNAP indicates it’s FT support to TNGF over AAA message. TNGF need to support FT. Further details if any are upto normative work.

For KI#3, the evaluation is same as KI#1.

The solution reuses existing 5G architecture.

## 6.11 Solution #11: Mobility of N5CW devices

### 6.11.1 Introduction

This solution addresses “Key issue #3: Security aspect of N5CW device connecting to a new TWAP within the same TWIF”.

The proposed solution relies on a previous successful authentication to a TWAP under the control of the same TWIF. It is assumed here that the primary authentication was performed successfully at the TWIF for the particular N5CW device and that the derived key KTWIF ( = KTNGF key) is stored in the N5CW device and in the TWIF together with the device identity SUCI or 5G-GUTI. The re-authentication is performed by an encrypted authentication token, which contains information for the derivation of the new access point key KTNAP = Pairwise Master Key (PMK).

### 6.11.2 Solution details



Figure6.11.2-1: N5CW Reauthentication call flow

1. The N5CW device associates with the trusted WLAN network and the EAP-AKA’ authentication procedure is initiated.

2. The N5CW device shall provide its Network Access Identity (NAI) The Trusted WLAN Access Point (TWAP) selects a Trusted WLAN Interworking Function (TWIF), e.g. based on the received realm, and sends an AAA request to the selected TWIF.

If the N5CW device registers to 5GC over 3GPP access for the first time when the above procedure is initiated, then the NAI shall include the SUCI. If the N5CW device has registered to 5GC over 3GPP access when the above procedure is initiated, then the NAI includes the 5G-GUTI assigned to the N5CW device over 3GPP access.

The N5CW device constructs an authentication token based on the device identity (SUCI or 5G-GUTI) and a generated nonce, protected with the previously derived KTWIF . The token may be integrity protected with the corresponding key. The N5CW includes the authentication token in the EAP-Response message towards the TWIF.

The N5CW device derives a new KTNAP using the KTWIF and the Nonce.

3. The TWIF recognizes based on the presence of the authentication token that the N5CW device was already authenticated and registered before and selects the corresponding key (KTWIF or PMK) based on the include device identity (SUCI or 5G-GUTI).

4. The TWIF decrypts the token and verifies the included identity matches the one in the EAP response and then derives a new KTNAP using the KTWIF and the Nonce. In case the message was integrity protected, the TWIF verifies the MAC-I.

5. The TWIF sends the TNAP key and the EAP-Success message to the Trusted WLAN Access Point, which forwards the EAP-Success to the N5CW device. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication according to IEEE 802.11.

6. A layer-2 or layer-3 connection is established between the Trusted WLAN Access Point and the TWIF for transporting all user-plane traffic of the N5CW device to TWIF.

Editor’s Note: it is FFS how the TWIF is be able to correlate the session if the UE uses SUCI

Editor’s Note: it is FFS how the TWIF is be able to correlate the session if the UE gets asigend a new 5G-GUTI

### 6.11.3 Evaluation

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

*TBD*

## 6.12 Solution #12: AUN3 device mobility solution with Nonce

### 6.12.1 Introduction

This solution addresses key issue #2: Security aspect of AUN3 device connecting to a new 5G-RG within the same W-AGF.

In this solution, full authentication may be skipped if AUN3 device is authenticated by a security context which is obtained from a previous full authentication.

### 6.12.2 Solution details

6.12.2.1 AUN3 device not supporting 5G key hierarchy

6.12.2.1.1 Procedure



Figure 6.12.2.1.1-1 5G-RG change procedure for AUN3 device not supporting 5G key hierarchy

1. AUN3 device is connected to 5G-RG#1 as specified in clause 7B.7.2 in TS 33.501 [3] with the following changes:
   1. AUN3 device generates a NonceAUN3 and sends it in EAP-ID-Response. It indicates that AUN3 device can derive PMK as specified in clause 6.12.2.1.2 of this document.
   2. AMF, which knows the AUN3 device's capability, generates NonceAMF and 5G-GUTI after the primary authentication and AMF sends NonceAMF and 5G-GUTI to AUN3 device.
   3. After the primary authentication, AMF and AUN3 device store MSK, 5G-GUTI and NonceAMF in the security context.
2. AUN3 device decides to move from 5G-RG#1 to 5G-RG#2, so 802.11 connection is established between AUN3 device and 5G-RG#2.
3. 5G-RG#2 initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer 2 frame.
4. The AUN3 generates a new NonceAUN3 and MACAUN3, before sending back an EAP response/Identity including 5G-GUTI, NonceAUN3, and MACAUN3. MACAUN3 is generated using MSK and NonceAMF received in step 1. MACAUN3 may be the part of the output (e.g., most significant 128-bits of the output).
5. 5G-RG#2 sends a NAS Registration Request message to the AMF, including 5G-GUTI, AUN3 device indicator, NonceAUN3, and MACAUN3.
6. If the AMF is different from the old AMF which allocated the 5G-GUTI in step 1, the new AMF retrieves SUPI and security context from the old AMF. AMF verifies the MACAUN3 using MSK and NonceAMF stored in the security context. If the verification is successful and AMF decides to skip a full authentication based on an operator's policy, the full authentication is skipped. AMF generates a new NonceAMF and 5G-GUTI. AMF also computes MACAMF using existing MSK and NonceAUN3 received in step 5. MACAMF may be the part of the output (e.g., most significant 128-bits of the output). AMF stores MSK, 5G-GUTI, and newly generated NonceAMF in its security context.
7. AMF derives PMK as specified in clause 6.12.2.1.2 using existing MSK, NonceAUN3 received in step 5, NonceAMF generated in step 6.
8. AMF sends EAP-Success and PMK to the 5G-RG#2 in N1 message.
9. The 5G-RG#2 sends to the AUN3 device the EAP-Success message including 5G-GUTI, NonceAMF, and MACAMF.
10. The AUN3 device verifies the MACAMF using NonceAUN3 generated in step 4 and existing MSK. If the verification is successful, AUN3 derives PMK as specified in clause 6.12.2.1.2 using existing MSK, NonceAUN3 generated in step 4, and NonceAMF received in step 9. The AUN3 device stores 5G-GUTI, the newly received NonceAMF, and MSK in its security context.
11. If the layer 2 connection is over WLAN, the AUN3 device and the 5G-RG#2 use the first 256-bit of the PMK for WLAN keys derivation.
12. The AUN3 device and the 5G-RG#2 performs four-way handshaking to establish WLAN secure connection.

6.12.2.1.2 PMK key derivation



Figure 6.12.2.1.2-1 Key hierarchy for AUN3 device not supporting 5G key hierarchy

PMK can be derived in AMF/AUN3 device as follows:

PMK = PRF'(most significant 256 bits of MSK, NonceAUN3|NonceAMF)[640..1151], as specified in RFC 5448 [6].

6.12.2.2 AUN3 device supporting 5G key hierarchy

6.12.2.2.1 Procedure



Figure 6.12.2.2.1-1 5G-RG change procedure for AUN3 device supporting 5G key hierarchy

1. AUN3 device is connected to 5G-RG#1 as specified in clause 7B.7.3 in TS 33.501 [3] with the following changes:
   1. AUN3 device generates NonceAUN3 and sends it in EAP-Res/Identity. It indicates that AUN3 device can perform horizontal key derivation on KAMF as specified in clause 6.12.2.2.2 of this document.
   2. AMF, which knows the AUN3 device's capability, generates NonceAMF and 5G-GUTI after the primary authentication and AMF sends NonceAMF and 5G-GUTI to AUN3 device.
   3. After the primary authentication, AMF and AUN3 device store KAMF, 5G-GUTI and NonceAMF in the security context.
2. AUN3 device decides to move from 5G-RG#1 to 5G-RG#2, so 802.11 connection is established between AUN3 device and 5G-RG#2.
3. 5G-RG#2 initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer 2 frame.
4. The AUN3 generates a NonceAUN3 and MACAUN3, before sending back an EAP response/Identity including 5G-GUTI, NonceAUN3, and MACAUN3. MACAUN3 is generated using KAMF and NonceAMF received in step 1. MACAUN3 may be the part of the output (e.g., most significant 128-bits of the output).
5. 5G-RG#2 sends a NAS Registration Request message to the AMF, including 5G-GUTI, AUN3 device indicator, NonceAUN3, and MACAUN3.
6. If the AMF is different from the old AMF which allocated the 5G-GUTI in step 1, the new AMF retrieves SUPI and security context from the old AMF. AMF verifies the MACAUN3 using KAMF and NonceAMF stored in the security context. If the verification is successful and AMF decides to skip a full authentication based on an operator's policy, the full authentication is skipped. AMF generates a new NonceAMF and 5G-GUTI. AMF also computes MACAMF using KAMF and NonceAUN3 received in step 5. MACAMF may be the part of the output (e.g., most significant 128-bits of the output).
7. AMF performs horizontal key derivation on KAMF as specified in clause 6.12.2.2.2 using existing KAMF, NonceAUN3 received in step 5, NonceAMF generated in step 6. AMF stores newly derived KAMF, 5G-GUTI, and newly generated NonceAMF in its security context. AMF derives KWAGF from the newly derived KAMF as specified in Annex A.9 in TS 33.501 [3].
8. AMF sends EAP-Success and PMK to the 5G-RG#2 in N1 message.
9. The 5G-RG#2 sends to the AUN3 device the EAP-Success message including 5G-GUTI, NonceAMF, and MACAMF.
10. The AUN3 device verifies the MACAMF using NonceAUN3 generated in step 4 and existing KAMF. If the verification is successful, AUN3 performs horizontal key derivation on KAMF as specified in clause 6.12.2.2.2 using existing KAMF, NonceAUN3 generated in step 4, and NonceAMF received in step 9. The AUN3 device stores 5G-GUTI, the newly received NonceAMF, and newly derived KAMF in its security context. AUN3 device derives KWAGF from the newly derived KAMF as specified in Annex A.9 in TS 33.501 [3].
11. If the layer 2 connection is over WLAN, the AUN3 device and the 5G-RG#2 use KWAGF as the PMK, from which the WLAN keys are derived.
12. The AUN3 device and the 5G-RG#2 performs four-way handshaking to establish WLAN secure connection.

6.12.2.2.2 Horizontal key derivation on KAMF

Horizontal key derivation on KAMF is performed similar to Annex A.13 in TS 33.501 [3] with some changes:

Derivation of KAMF' from KAMF during mobility in AUN3 device supporting 5G key hierarchy uses the following input parameter:

* FC = 0xXX
* P0 = NonceAUN3
* L0 = length of NonceAUN3
* P1 = NonceAMF
* L1 = length of NonceAMF

The input key KEY is KAMF.

NOTE: FC value to be determined during normative phase.

### 6.12.3 Evaluation

|  |  |
| --- | --- |
| Node/UE/NF | solution |
| AUN3 device | - generates and provides NonceAUN3 to AMF.  - computes MACAUN3 using NonceAMF and MSK/KAMF.  - derives new PMK from MSK/newly derived KAMF.  - verifies MACAMF and stores NonceAMF with MSK/KAMF in its security context. |
| AMF | - verifies MACN5CW and computes MACAMF using NonceAUN3 and MSK/KAMF.  - derives new PMK from MSK/newly derived KAMF.  - generates and provides NonceAMF to AUN3.  - stores NonceAMF with MSK/KAMF in its security context. |

Editor’s Note: Further evaluation is FFS.

## 6.13 Solution #13: ERP based re-authentication for NSWO

### 6.13.1 Introduction

This solution addresses key issue #4: Security aspect of UE connecting to a new WLAN AP connected via the same NSWOF

6.13.2 Solution details

### 6.13.2.1 Solution overview

In TS 33.501, annex S.3.2 5G NSWO procedures describe the UE authentication for connectivity through a NSWOF. Here it is adapted with minor revisions to store the context information during initial full authentication, and subsequently use this information to optimize the UE authentication when the UE connects to a different WLAN AP.EAP Re-authentication Protocol (ERP) [4] is an EAP method-independent protocol for efficient re-authentication between the peer and an EAP re-authentication server. ERP allows a peer and server to mutually verify proof of possession of key material from an earlier EAP method run and to establish a security association between the peer and the authenticator. The APs in WLAN AN shall act as ER authenticators and NSWOF shall act as ERP server. AUSF remains to be an EAP authentication server.

A diagram of a system

Description automatically generated

**Fig. 6.13.2.1-1 Revised UE authentication procedure with NSWOF**

* Steps 1 through 4 are fully compliant with annex S.3.2 in TS 33.501
* In step #5 the NSWOF indicates its EAP re-authentication capability by including the ER-Indicator
* AUSF in step #8 acting as EAP authentication server by responds with ER-Ack/ER-Nak.
* No changes are needed for steps #9 through 15.
* In step 16 the AUSF shall send to NSWOF the DSRK and EMSKname, DSRKLifetime (RFC 6696 [3], pg.11, sec 3.2, Fig 4) in addition to the MSK and EAP Success.
* In step17 the NSWOF retains the DSRK and EMSKname and sends the MSK and EAP success indicator to the Authenticator
* No changes in steps 18(a), 18(b), 18(c) and 18(d)

### 6.13.2.2 UE Re-Authentication Procedure for NSWO

The following is a new and optimized procedure for UE re-authentication, that avoids full authentication during UE mobility from a AP to another in the WLAN AN connected to the same NSWOF. It uses the context information saved in NSWOF during the initial UE full authentication. During re-authentication there are no messages exchanged with AUSF and UDM.

A diagram of a computer system

Description automatically generated

**Fig. 6.13.2-2 UE Re-authentication procedure with NSWOF ( Change diagram )**

* In steps #1 and #2 the UE get associated with the new AP, the AP indicates its EAP Re-auth capability by sending
  + - (1) EAP-Initiate/ Re-auth-Start
    - (2) EAP-Request/Identity

This indicates to the UE that the AP being associated with is EAP re-auth capable.

* In steps #3 through #6 the UE then initiates the EAP re-auth process by exchanging the following messages in the format as specified in RFC 6696 [3] sections 5.3.2 and 5.3.3.
  + - EAP-Initiate Re-Auth
    - EAP-Finish Re-Auth
  + In step #7 the UE gets associated new AP in the WLAN AN after successful authentication

In this manner during its mobility in WLAN access network the device may get associated with different parts of access network and get re-authenticated. Each time the device re-authenticates with the network, the key derivation process shall follow procedures in (RFC 6696[3] Sec 4 and RFC 5295[4])

### 6.13.3 Evaluation

This solution addresses key issue #4 and meets the security requirements to re-authenticate UE without performing full primary authentication. The network function changes needed to support this solution are listed below

**NSWOF**

* During initial authentication, the NSWOF shall include the ERindicator as an additional attribute to the AUSF in the Nausf\_UEAuthentication\_Authenticate\_Request message ( in step 5 TS 33.501, annex S.3.2 )
* During initial authentication the Nausf\_UEAuthentication\_Authenticate\_Response message ( in step 8 TS 33.501, annex S.3.2 ) the NSWOF shall receive an additional attributes ER-Ack or ER-Nak from AUSF
* During initial authentication the Nausf\_UEAuthentication\_Authenticate\_Response message ( in step 16 TS 33.501, annex S.3.2 ) the NSWOF shall receive additional attributes DSRK, EMSKname, DRSKLifetime from AUSF. NSWOF shall retain these additional attributes with itself.

**AUSF**

* During initial authentication, the NSWOF shall include the ERindicator as an additional attribute to the AUSF in the Nausf\_UEAuthentication\_Authenticate\_Request message ( in step 5 TS 33.501, annex S.3.2 ). AUSF shall process these additional attributes
* During initial authentication the Nausf\_UEAuthentication\_Authenticate\_Response message ( in step 8 TS 33.501, annex S.3.2 ) the AUSF shall send an additional attributes ER-Ack or ER-Nak fto the NSWOF. If reauth is supported by AUSF, it shall include ER-Ack other shall send ER-Nak
* During initial authentication the Nausf\_UEAuthentication\_Authenticate\_Response message ( in step 16 TS 33.501, annex S.3.2 ) the AUSF shall send additional attributes DSRK, EMSKname, DRSKLifetime to NSWOF.

**WLAN**

* TBD

**UE**

* UE needs to support ERP

Editor’s Note: It is FFS how the solution fulfills the requirement that mobility shall be for WLAN APs connected to the same NSWOF. Further evaluation is FFS.

## 6.14 Solution #14: solution for UE connecting to a new WLAN AP connected via the same NSWOF.

### 6.14.1 Introduction

This solution targets KI #4. In this solution, AUSF maintains the MSK after the authentication so that further MSK can be derived or refreshed without performing full authentication. The concept of the solution is:

* After successful NSWO authentication, the NSWO UE context is maintained in the AUSF with the newly created NSWO UE Reauth ID and MSK key for future use. The AUSF also shares the NSWO UE Reauth ID with NSWOF along with MSK.
* NSWOF provides the MSK and NSWO UE Reauth ID to the WLAN AP, and the WLAN AP provides the same to UE.
* When UE moves or tries to reconnect to WLAN2 for NSWO, the UE provides the NSWO UE Reauth ID in the EAP-ID response. NSWOF/AUSF identifies the UE based on this NSWO UE Reauth ID and refreshes the MSK and NSWO UE temporary ID.
* A newly generated NSWO UE Reauth ID and RAND are sent to UE via WLAN AN. The UE shall refresh the MSK based on the RAND and secure the connection via the MSK.

Note: Instead of AUSF, NSWOF can also maintains the context and derive the further keys.

### 6.14.2 Solution details

Detailed procedure of the solution is:

 Figure 6.14.2-1 UE connecting to new WLAN AP for NSWO

1: UE connects to NSWO and performed the authentication as defined in figure S.3-1, TS 33.501[3], step 1 to 15.

2: AUSF generates NSWO UE Reauth ID along with MSK and stores the same in the AUSF context.

The AUSF shall send Nausf\_UEAuthentication\_Authenticate Response message with EAP-Success, NSWO UE Reauth ID and MSK key to NSWOF. The AUSF may optionally provide the SUPI to NSWOF.

NSWO UE Reauth ID may contain AUSFID, TEMPORARY\_NUMBER and Homerealm, where

Temporary number can also be generated at UE and network independently using the shared constant value.

NOTE: This AUSF ID in the reauth ID will help NSWOF to reach to the right AUSF.

3. The NSWOF shall send the EAP-success, NSWO UE Reauth ID and MSK to WLAN AN over the SWa interface.

4: This step is similar to figure S.3-1, TS 33.501[3], Step 17b to 18d. And UE and WLAN secure the connection.

5: The WLAN AP provides NSWO UE Reauth ID to UE via EAP-Req/Notification.

NOTE: EAP-Req/Notification is already used by different flow to provide the data to UE, please refer to figure 7A.2.1-1, step 10b of 33.501[3]. Alternatively, NSWO UE Reauth ID can be provided to UE via EAP-SUCCESS.

6: UE moves or connect to WLAN AP2 for NSWO and connect to WLAN AP2 and perform step 1 of figure S.3-1, TS 33.501[3].

7: The UE sends an EAP Response/Identity message. If the UE determines to use the NSWO service, the UE shall use the NSWO UE Reauth ID if available otherwise use the SUCI as defined Annex X of 33501.

8: The EAP Response/Identity message shall be routed over the SWa interface towards the NSWOF based on the realm part of the NSWO UE Reauth ID.

9. The NSWOF shall determine the AUSF address based on the NSWO UE Reauth ID and send the message Nausf\_UEAuthentication\_Authenticate Request with NSWO UE Reauth ID, Access Network Identity and NSWO indicator towards the AUSF.

10: Based on NSWO UE Reauth ID, the AUSF shall retrieve the context and refresh the MSK and generate new NSWO UE Reauth ID.

11: The AUSF shall send Nausf\_UEAuthentication\_Authenticate Response message with EAP-Success, NSWO UE Reauth ID, RAND and MSK key to NSWOF. The AUSF may optionally provide the SUPI to NSWOF.

12: The NSWOF shall send the EAP-success, NSWO UE Reauth ID, RAND and MSK to WLAN AN over the SWa interface.

13: The WLAN AP2 provides EAP-SUCCESS and RAND to the UE.

14: UE refreshes the MSK based on the RAND. If MAC is provided, the UE validate the MAC before using the RAND.

15: Step 18b to 18d of figure S.3-1, TS 33.501[3], are performed and the WLAN AP2 and UE interface is secured

16: The WLAN AP provides NSWO UE Reauth ID to UE via EAP-Req/Notification.

#### 6.14.2.1 MSK refresh

When refreshing the MSK during the mobility, the following parameters shall be used to form the string S.

- FC = 0xx

- P0 = RAND value

- L0 = length of RAND value

MSK is used as root key.

### 6.14.3 Evaluation

UE and AUSF: UE and AUSF need to refresh the MSK based on the RAND and handle NSWO UE Reauth-ID.

NSWOF impact: relay the NSWO UE Reauth ID as received.

WLAN: provide NSWO UE Reauth ID and RAND to UE.

## 6.15 Solution #15: Using FT for NSWO

### 6.15.1 Introduction

This solution addresses key issue #4: Security aspect of UE connecting to a new WLAN AP connected via the same NSWOF.

### 6.15.2 Solution details

This solution is similar to solution #3 (see 6.3 of the present document) except that there is no need to derive a new key (KFT in solution #3) as MSK provided to the WLAN Access Network (AN) (see Annex S of TS 33.501 [3]). MPMK is derived directly from MSK as described in 802.11 [6]. Hence no standards changes are needed in this case to deploy FT as there is no need for 5GC to derive the MPMK.

To realise this solution, the WLAN AN that the UE is connecting needs to support FT and hence contains a R0HK. The R0KH receives the MSK and takes the MPMK from the MSK to generate the FT root key. The R0KH passes the PMK-R1 to R1KH (i.e., AP) so the R1KH can complete the 4-way handshake with the UE.

### 6.15.3 Evaluation

Solution #15 requires no changes to the standards to enable a solution to key issue #4 as FT can be deployed in the WLAN AN.

## 6.16 Solution #16: N5CW device mobility using security context in AMF

### 6.16.1 Introduction

This solution resolves key issue #3 Security aspect of N5CW device connecting to a new TWAP within the same TWIF. Whenever reconnection of the device, security context (e.g. previously stored key) in the AMF can be utilized to avoid repeative primary authentication. If the N5CW device is already registered in 5GC, the AMF has security context for the N5CW device.

To derive new KTWIF for the N5CW device reconnecting, part of KTWIF can be stored and the stored KTWIF will be utilized in the next derivation during reconnection. By using previously stored part of KTWIF in the KDF, new KTWIF can be derived during reconnection. To do this, previously stored part of KTWIF can replace UL NAS COUNT in the KDF of KTWIF.

### 6.16.2 Solution details



Figure 6.16.2-1: TWAP mobility procedure

The steps shown in Figure 6.16.2-1 is described as below:

1-4. Follows TS 33.501[3] Clause 7A.2.4

5. The AMF checks whether the N5CW device is first time registration or not. If the N5CW device is already registered, step 6 can be skipped. Otherwise, continue to step 6 for mutual authentication procedures.

6. The EAP-AKA’ procedure will be triggered to perform mutual authentication between the N5CW device and the home network as specified in TS 33.501[3] clause 6.1.3.1.

7. The AMF shall derive an KTWIF key from the received KAMF key as specified in TS 33.501[3] Annex A.9.

If the N5CW device is first time registered or there is no stored part of KTWIF in the AMF, for key derivation of KTWIF, UL NAS COUNT as zero is used in KDF. After deriviation of KTWIF, the AMF stores part of KTWIF for next reconnection.

If there is stored KTWIF in the AMF and the N5CW device is previously registered as checked in step 5, for key derivation of new KTWIF, previously stored KTWIF is used for KDF instead of UL NAS COUNT. After deriviation of KTWIF, the AMF stores part of KTWIF for next reconnection.

NOTE: The AMF can be pre-configured by operator which part of KTWIF will be stored from the full key stream. (e.g., LSB or MSB, or specific middle of key stream)

8-13. Follows TS 33.501[3] Clause 7A.2.4 Step 10-14.

### 6.16.3 Evaluation

Editor’s Note: The security of using the current key as input to the key derivation is FFS.

Editor's Note: Further evaluation is FFS.

## 6.17 Solution #17: N5CW device mobility solution without AMF impact

### 6.17.1 Introduction

This solution addresses key issue #3: Security aspect of N5CW device connecting to a new TWAP within the same TWIF.

In this solution, full authentication may be skipped if N5CW device is authenticated using security context which is obtained from a previous full authentication.

### 6.17.2 Solution details

6.17.2.1 Procedure



Figure 6.17.2.1-1 TWAP change procedure for N5CW device

1. N5CW device is conntected to TWAP#1 as specified in clause 7A.2.4 in TS 33.501 [3] with the following changes:

- N5CW device generates NonceN5CW and sends it in EAP-Res/Identity. It indicates that N5CW device can derive the new key from KTWIF as specified in clause 6.17.2.2 of this document.

- TWIF, which knows the N5CW device's capability, generates NonceTWIF and Temporary UE ID after the primary authentication and TWIF sends NonceTWIF and Temporary UE ID to N5CW device.

- After the primary authentication, TWIF and N5CW device store Temporary UE ID, KTWIF, and NonceTWIF in the security context.

1. N5CW device decides to move from TWAP#1 to TWAP#2
2. TWAP#2 sends an EAP request/Identity to the N5CW device.
3. The N5CW generates a NonceN5CW and MACN5CW, before sending back an EAP response/Identity. The EAP response/Identity includes 5G-GUTI, Temporary UE ID, NonceN5CW, and MACN5CW. MACN5CW is generated using KTWIF and NonceTWIF received in step 1. MACN5CW may be the part of the output (e.g., most significant 128-bits of the output).
4. TWAP#2 sends AAA request to TWIF and the request includes 5G-GUTI, Temporary UE ID, NonceN5CW, and MACN5CW.
5. TWIF retrieves the security context based on Temporary UE ID. If TWIF cannot retrieve the security context, TWIF creates registration request message and sends it to AMF as specified in clause 7A.2.4 in TS 33.501 [3]. Otherwise, TWIF verifies the MACN5CW using KTWIF and NonceTWIF stored in its security context. If the verification is successful and TWIF decides to skip a full authentication based on an operator's policy, the full authentication is skipped. TWIF generates a new NonceTWIF. TWIF also computes MACTWIF using KTWIF and NonceN5CW received in step 5. MACTWIF may be the part of the output (e.g., most significant 128-bits of the output).
6. TWIF derives KTNAP using existing KTWIF, NonceN5CW received in step 5, and NonceTWIF gerenated in step 6, as specified in clause 6.17.2.2. TWIF stores KTWIF, Temporary UE ID, and newly generated NonceTWIF in its security context.
7. TWIF sends the TNAP key, EAP Success message, NonceTWIF, and MACTWIF to the TWAP#2, which forwards EAP Success, NonceTWIF, and MACTWIF to the N5CW device.
8. The N5CW device verifies the MACTWIF using NonceN5CW generated in step 4 and existing KTWIF. If the verification is successful, the N5CW derives KTNAP using existing KTWIF, NonceN5CW generated in step 4, and NonceTWIF received in step 9, as specified in clause 6.17.2.2. The N5CW device stores 5G-GUTI, the newly received NonceTWIF, and KTWIF in its security context.
9. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication. A layer-2 or layer-3 connection is established between the TWAP#2 and TWIF for transporting all user-plane traffic of the N5CW device to TWIF.

6.17.2.2 New KTNAP derivation from KTWIF

When deriving a KTNAP from KTWIF in N5CW mobility case, the following parameters are used to form the input S to the KDF.

* FC = 0xXX
* P0 = NonceN5CW
* L0 = length of NonceN5CW
* P1 = NonceTWIF
* L1 = length of NonceTWIF

The input key KEY is KTWIF.

NOTE: FC value to be determined during normative phase.

### 6.17.3 Evaluation

Impact on the entities:

|  |  |
| --- | --- |
| Entitiy | solution |
| N5CW device | - generates MACN5CW and NonceN5CW.  - verifies MACTWIF and derives a new TNAP key.  - stores NonceTWIF and Temporary UE ID with KTWIF in its security context |
| TWIF | - generates MACTWIF, NonceTWIF, and Temporary UE ID.  - verifies MACN5CW and derives a new TNAP key.  - stores NonceTWIF and Temporary UE ID with KTWIF in its security context. |

## 6.18 Solution #18: AUN3 device reconnecting

### 6.x.1 Introduction

This solution addresses the security solution for KI#2. There are two kinds of AUN3 devices:

* AUN3 device not supporting 5G key hierarchy (authentication is defined in Section 7B.7.2 of TS 33.501 [3])
* AUN3 device supports 5G key hierarchy. (Authentication is defined in Section 7B.7.3 of TS 33.501 [3]).

Therefore, we need solutions for both kinds of devices.

6.18.2.1 Procedure for AUN3 device not supporting key hierarchy



Figure 6.18.2-1 AUN3 mobility procedure

0: AUN3 device is connected and authenticated via RG1 as defined in clause 7B.7.2 of TS 33.501 [3]. RG also provide 5G GUTI to the AUN3 device. AMF also stores MSK in the UE context after the successful authentication.

1. AUN3 device wants to connect to RG2 and it initiates a layer 2 connection with the 5G-RG either.

2. The 5G-RG shall initiate the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer 2 frame (e.g., EAPOL).

3. The AUN3 device shall send back an EAP response/Identity with 5G-GUTI if available. Otherwise, AUN3 device respond with Network Access Identifier (NAI) in the form of username@realm. If the AUN3 device supports SUPI privacy, the AUN3 device shall send SUCI in the EAP response/Identity.

4,5. The 5G-RG shall send a NAS Registration Request message to the AMF, including the 5G-GUTI of the AUN3 device and AUN3 device indicator. This message is sent via W-AGF where W-AGF just relay it via N2. Please refer to the W-AGF functionality defined in TS 23.316[7].

6. The AMF is able to retrieve the UE context based on 5G-GUTI. Based on the AUN3 device indicator and local policy and a valid GUTI, the AMF may skip the authentication and refresh the MSK using RAND.

7. The AMF shall send EAP-Success, RAND, MAC and MSK to the 5G-RG via W-AGF.

Step 7 could be NAS Security Mode Command with NULL encryption and NULL integrity protection or Authentication Result.

8. The 5G-RG sends to the AUN3 device the EAP-Success message, RAND and MAC in a layer 2 frame.

9. If MAC verification is successful, the AUN3 device generate/refresh the MSK.

10. If the layer 2 connection is over WLAN (IEEE 802.11), the AUN3 device and the 5G-RG use the first 256-bit of the MSK as the PMK, from which the WLAN keys are derived. The AUN3 and the 5G-RG performs four-way handshaking to establish WLAN secure connection.

**Key Derivation**

When deriving keys for AUN3 device during the mobility, the following parameters shall be used to form the string S.

- FC = 0xx

- P0 = RAND value

- L0 = length of RAND value

MSK is used as root key.

6.18.2.2 Procedure for AUN3 device supporting key hierarchy



Figure 6.18.2-2 AUN3 supporting 5G key hierarchy mobility procedure

0: AUN3 device supporting 5G key hierarchy is connected and authenticated via RG1 as defined in clause 7B.7.3 of TS 33.501 [3]. RG also provide 5G GUTI to the AUN3 device. AMF also stores the UE context with KAMF and SUPI after the successful authentication.

1. AUN3 device wants to connect to RG2 and it initiates a layer 2 connection with the 5G-RG either via Ethernet or WLAN. If the layer 2 connection is based on Ethernet, steps 12-14 are skipped.

2. The 5G-RG shall initiate the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer 2 frame (e.g., EAPOL).

3. The AUN3 device shall send back an EAP response/Identity with 5G-GUTI if available. Otherwise, AUN3 device respond with Network Access Identifier (NAI) in the form of username@realm.

4. The 5G-RG shall send a NAS Registration Request message to the AMF, including the 5G-GUTI of the AUN3 device, and AUN3 device indicator. This message is sent via W-AGF where W-AGF just relay it via N2. Please refer to the W-AGF functionality defined in TS 23.316[7].

5. The AMF is able to retrieve the UE context based on 5G-GUTI.

6. Based on the AUN3 device indicator, valid GUTI and local policy, the AMF may skip the authentication and refresh the KWAGF using RAND. The AMF determine AUN3 device support 5G key hierarchy based on subscription data.

7. The AMF shall send EAP-Success, RAND, optional MAC and KWAGF to the 5G-RG.

Step 7 could be NAS Security Mode Command with NULL encryption and NULL integrity protection or Authentication Result.

8. The 5G-RG sends to the AUN3 device the EAP-Success message, RAND and MAC in a layer 2 frame.

9. If MAC verification is successful, the AUN3 device generate/refresh the KWAGF.

10. If the layer 2 connection is over WLAN (IEEE 802.11), the AUN3 device and the 5G-RG use KWAGF as the PMK, from which the WLAN keys are derived. The AUN3 and the 5G-RG performs four-way handshaking to establish WLAN secure connection.

**Key Derivation**

When deriving KWAGF key for AUN3 device during the mobility, the following parameters shall be used to form the string S.

- FC = 0xx

- P0 = RAND value

- L0 = length of RAND value

KAMF is used as root key.

### 6.18.3 Evaluation

Impact on the nodes/UE:

Editor’s Note: Further evaluation is FFS.

## 6.19 Solution #19: AUN3 device mobility solution without AMF impact

### 6.19.1 Introduction

This solution addresses key issue #2: Security aspect of AUN3 device connecting to a new 5G-RG within the same W-AGF.

In this solution, full authentication may be skipped if AUN3 device is authenticated by a security context which is obtained from a previous full authentication.

### 6.19.2 Solution details

6.19.2.1 AUN3 device not supporting 5G key hierarchy

6.19.2.1.1 Procedure



Figure 6.19.2.1.1-1 5G-RG change procedure for AUN3 device not supporting 5G key hierarchy

1. AUN3 device is connected to 5G-RG#1 as specified in clause 7B.7.2 in TS 33.501 [3] with the following changes:

- AUN3 device generates a NonceAUN3 and sends it in EAP-ID-Response. It indicates that AUN3 device can derive the key as specified in clause 6.19.2.1.2 of this document.

- W-AGF, which knows the AUN3 device's capability, generates NonceWAGF and Temporary UE ID after the primary authentication and W-AGF sends NonceWAGF and Temporary UE ID to AUN3 device.

- After the primary authentication, W-AGF and AUN3 device store MSK, Temporary UE ID, and NonceWAGF in the security context.

1. AUN3 device initiates a layer 2 connection with the 5G-RG#2 either via Ethernet or WLAN.
2. 5G-RG#2 initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer 2 frame.
3. The AUN3 generates NonceAUN3 and MACAUN3, before sending back an EAP response/Identity. The EAP response/Identity includes SUCI, Temporary UE ID received in step 1, NonceAUN3, and MACAUN3. MACAUN3 is generated using MSK and NonceWAGF received in step 1. MACAUN3 may be the part of the output (e.g., most significant 128-bits of the output).
4. 5G-RG#2 sends a NAS Registration Request message to the W-AGF, including SUCI, Temporary UE ID, AUN3 device indicator, NonceAUN3, and MACAUN3.
5. W-AGF retrieves the security context based on Temporary UE ID. If W-AGF cannot retrieve the security context, W-AGF forwards Registration Request message to AMF as specified in clause 7B.7.2 in TS 33.501 [3], and the full authentication is performed. W-AGF verifies the MACAUN3 using MSK and NonceWAGF stored in the security context. If the verification is successful and W-AGF decides to skip a full authentication based on an operator's policy, the full authentication is skipped. W-AGF generates a new NonceWAGF and Temporary UE ID. W-AGF also computes MACWAGF using existing MSK and NonceAUN3 received in step 5. MACWAGF may be the part of the output (e.g., most significant 128-bits of the output). W-AGF stores MSK, Temporary UE ID, and newly generated NonceWAGF in its security context.
6. W-AGF derives the key as specified in clause 6.19.2.1.2 using existing MSK, NonceAUN3 received in step 5, NonceWAGF generated in step 6.
7. W-AGF sends EAP-Success and the key to the 5G-RG#2 in N1 message.
8. The 5G-RG#2 sends to the AUN3 device the EAP-Success message including Temporary UE ID, NonceWAGF, and MACWAGF.
9. The AUN3 device verifies the MACWAGF using NonceAUN3 generated in step 4 and existing MSK. If the verification is successful, AUN3 derives the key as specified in clause 6.19.2.1.2 using existing MSK, NonceAUN3 generated in step 4, and NonceWAGF received in step 9. The AUN3 device stores Temporary UE ID, the newly received NonceWAGF, and MSK in its security context.
10. If the layer 2 connection is over WLAN, the AUN3 device and the 5G-RG#2 use the first 256-bit of the key for WLAN keys derivation.
11. The AUN3 device and the 5G-RG#2 performs four-way handshaking to establish WLAN secure connection.

6.19.2.1.2 Key derivation from MSK in AUN3 mobility case



Figure 6.19.2.1.2-1 Key hierarchy for AUN3 device not supporting 5G key hierarchy

Key can be derived in W-AGF/AUN3 device as follows:

Key = PRF'(part or all of MSK, NonceAUN3|NonceWAGF)[640..1151], as specified in RFC 5448 [6].

6.19.2.2 AUN3 device supporting 5G key hierarchy

6.19.2.2.1 Procedure



Figure 6.19.2.2.1-1 5G-RG change procedure for AUN3 device supporting 5G key hierarchy

1. AUN3 device is connected to 5G-RG#1 as specified in clause 7B.7.3 in TS 33.501 [3] with the following changes:

- AUN3 device generates NonceAUN3 and sends it in EAP-Res/Identity. It indicates that AUN3 device can derive the key as specified in clause 6.19.2.2.2 of this document.

- W-AGF, which knows the AUN3 device's capability, generates NonceWAGF and Temporary UE ID after the primary authentication and W-AGF sends NonceWAGF and Temporary UE ID to AUN3 device.

- After the primary authentication, W-AGF and AUN3 device store KWAGF, Temporary UE ID, and NonceWAGF in the security context.

1. AUN3 device initiates a layer 2 connection with the 5G-RG#2 either via Ethernet or WLAN.
2. 5G-RG#2 initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer 2 frame.
3. The AUN3 generates NonceAUN3 and MACAUN3, before sending back an EAP response/Identity. The EAP response/Identity includes SUCI, Temporary UE ID, NonceAUN3, and MACAUN3. MACAUN3 is generated using KWAGF and NonceWAGF received in step 1.
4. 5G-RG#2 sends a NAS Registration Request message to the W-AGF, including SUCI, Temporary UE ID, AUN3 device indicator, NonceAUN3, and MACAUN3.
5. W-AGF retrieves the security context based on Temporary UE ID. If W-AGF cannot retrieve the security context, W-AGF forwards Registration Request message to AMF as specified in clause 7B.7.3 in TS 33.501 [3], and the full authentication is performed. Otherwise, W-AGF verifies the MACAUN3 using KWAGF and NonceWAGF stored in the security context. If the verification is successful and W-AGF decides to skip a full authentication based on an operator's policy, the full authentication is skipped. W-AGF generates a new NonceWAGF and Temporary UE ID. W-AGF also computes MACWAGF using KWAGF and NonceAUN3 received in step 5.
6. W-AGF derives a new key as specified in clause 6.19.2.2.2 using existing KWAGF, NonceAUN3 received in step 5, NonceWAGF generated in step 6. W-AGF stores KWAGF, Temporary UE ID, and newly generated NonceWAGF in its security context.
7. W-AGF sends EAP-Success, the key derived from KWAGF, MACWAGF, and NonceWAGF to the 5G-RG#2.
8. The 5G-RG#2 sends to the AUN3 device the EAP-Success message including Temporary UE ID, NonceWAGF, and MACWAGF.
9. The AUN3 device verifies the MACWAGF using NonceAUN3 generated in step 4 and existing KWAGF. If the verification is successful, AUN3 derives a new key as specified in clause 6.19.2.2.2 using existing KWAGF, NonceAUN3 generated in step 4, and NonceWAGF received in step 9. The AUN3 device stores Temporary UE ID, the newly received NonceWAGF, and KWAGF in its security context.
10. If the layer 2 connection is over WLAN, the AUN3 device and the 5G-RG#2 use the new key as PMK, from which the WLAN keys are derived.
11. The AUN3 device and the 5G-RG#2 perform four-way handshaking to establish WLAN secure connection.

6.19.2.2.2 Key derivation from KWAGF in AUN3 mobility case

When deriving the key from KWAGF in AUN3 mobility case, the following parameters are used to form the input S to the KDF:

* FC = 0xXX
* P0 = NonceAUN3
* L0 = length of NonceAUN3
* P1 = NonceWAGF
* L1 = length of NonceWAGF

The input key KEY is KWAGF.

NOTE: FC value to be determined during normative phase.

### 6.19.3 Evaluation

Impact on the entities:

|  |  |
| --- | --- |
| Entitiy | solution |
| AUN3 device | - generates MACAUN3 and NonceAUN3.  - verifies MACWAGF and derives a fresh key from MSK/KWAGF.  - stores NonceWAGF and Temporary UE ID with MSK/KWAGF in its security context. |
| W-AGF | - generates MACWAGF, NonceWAGF, and Temporary UE ID  - verifies MACAUN3 and derives a fresh key from MSK/KWAGF.  - stores NonceWAGF and Temporary UE ID with MSK/KWAGF in its security context. |

Editor’s Note: Further evaluation is FFS.

## 6.20 Solution #20: Using Fast BSS Transition for AUN3 mobility

### 6.20.1 Introduction

This solution addresses key issue #3

### 6.20.2 Solution details

#### 6.20.2.1 Solution overview

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

1. replace UE with AUN3.

2. replace TNGF with W-AGF

3. replace KTNGF with KTWIF

4. replace AP with 5G-RG.

### 6.20.3 Evaluation

Evaluation in solution#3 can be reused.

Editor’s Note: evaluation on key holder and based on what the FT key is initially provided to root key holder is FFS.

## 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.

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

It is concluded to use a fast BSS transition-based solution 3 as a base for the normative work. The R0KH holder may be collocated with TNGF or may be a separate entity.

Editor’s Note: Conclusion on other non-3GPP trusted access technologies is FFS.

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

It is concluded to use a fast BSS transition-based solution 7 as a base for the normative work. The R0KH holder may be collocated with TWIF or may be a separate entity.

Editor’s Note: Conclusion on other non-3GPP trusted access technologies is FFS.

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 |
| 2024-04 | SA3#115 AdHoc-e | S3-241507 |  |  |  | Inclusion of the documents approved at SA3#115AdHoc-e:  S3-241585, S3-241430, S3-241510, S3-241146, S3-241194, S3-241587, S3-241573, S3-241572, S3-241522, S3-241586, S3-241653, S3-241511, S3-241517, S3-241198, S3-241429, S3-241195, S3-241336, S3-241337 | 0.2.0 |
| 2024-05 | SA5#116 | S3‑242602 |  |  |  | Inclusion of the documents approved at SA3#116:  S3‑242598, S3‑242599, S3‑242559, S3‑241806, S3‑242281, S3-242560, S3‑242600, S3‑242561, S3‑242601, S3‑242563, S3‑242142, S3‑241807 | 0.3.0 |