|  |
| --- |
| 3GPP TR 33.887 V0.3.0 (2022-10) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security aspects for 5WWC Phase 2(Release 18) |
|   |
|  | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

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

Contents

Foreword 5

Introduction 6

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 Assumptions 8

5 Key issues 8

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

5.1.1 Key issue details 8

5.1.2 Threats 8

5.1.3 Potential security requirements 8

5.2 Key issue #2: Security aspect of slice information exposure of N3IWF/TNGF to UE 9

5.2.1 Key issue details 9

5.2.2 Threats 9

5.2.3 Potential security requirements 9

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

5.3.1 Key issue details 9

5.3.2 Threats 9

5.3.3 Potential security requirements 9

5.4 Key issue #4: Security aspect of TNAP mobility 10

5.4.1 Key issue details 10

5.4.2 Threats 10

5.4.3 Potential security requirements 10

6 Proposed solutions 10

6.0 Mapping of solutions to key issues 10

6.1 Solution #1: EAP\_AKA prime based authentication for AUN3 devices 10

6.1.1 Introduction 10

6.1.2 Solution details 11

6.1.3 Evaluation 12

6.2 Solution #2: EAP base authentication for AUN3 devices behind RG in PLMN 13

6.2.1 Introduction 13

6.2.2 Solution details 13

6.2.3 Evaluation 14

6.3 Solution #3: EAP base authentication for AUN3 devices behind RG in SNPN 14

6.3.1 Introduction 14

6.3.2 Solution details 15

6.3.3 Evaluation 16

6.4 Solution #4: EAP base authentication for AUN3 devices behind RG in SNPN by AAA server 16

6.4.1 Introduction 16

6.4.2 Solution details 16

6.Y.3 Evaluation 17

6.Y Solution #Y: <Title> 18

6.Y.1 Introduction 18

6.Y.2 Solution details 18

6.Y.3 Evaluation 18

7 Conclusions 18

7.1 Key issue #1: Authentication of AUN3 device behind RG and supporting EAP 18

7.2 Key issue #2: Security aspect of slice information exposure of N3IWF/TNGF to UE 18

Annex X: Change history 19

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

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

# 1 Scope

The objectives of this study are to identify key issues, potential security and privacy requirements and solutions with respect to:

* Whether and how to identify, authenticate and authorize the Authenticable Non-3GPP devices behind the Residential Gateway (RG) connecting to the network.
* Whether and how to identify, authenticate and authorize the 3GPP devices (UE or N5CW devices) behind the Residential Gateway (RG) connecting to the network.
* Security aspects of supporting slice in 5WWC.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23700-17 "Study on the support for 5WWC, Phase 2"

[3] 3GPP TR 33.316 "Wireless and wireline convergence access support for the 5G System (5GS)"

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

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

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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].

Definition format (Normal)

**<defined term>:** <definition>.

**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 format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

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

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 Assumptions

This clause contains assumptions for the study. If there are no assumptions at the end of the study, the clause will be removed before sending for approval.

# 5 Key issues

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

### 5.1.1 Key issue details

The AUN3 device is a non-3GPP device that does not support NAS over non-3GPP access, but it can be identified and/or authenticated by 5GC. For example, an AUN3 device may support EAP-AKA’, or does not support EAP based authentication but has a subscription with the 5GC.

This key issue considers AUN3 devices supporting EAP based authentication.

AUN3 devices supporting EAP can be connected to RG via WLAN or wireline. RG is connected to 5GC via 3GPP access or W-AGF as defined in TS 23.316[3] clause 4.10. Currently, authentication of these AUN3 devices is not sufficiently defined in 3GPP. I.e., how AUN3 devices connected with RG over wifi are authenticated and how the interface between AUN3 devices and RG is protected.

### 5.1.2 Threats

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

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

### 5.1.3 Potential security requirements

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

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

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

### 5.2.1 Key issue details

The solutions to KI #2 enable the selection of TNGF/N3IWF that support the S-NSSAI(s) required by the UE, as defined in 3GPP TR 23700-17[2]. Many solutions are presented, and one of the categories is:

* UE is able to discover the slice of TNGF/N3IWF and select TNGF/N3IWF accordingly.

Exposing the S-NSSAI information from the network nodes (TNGF/N3IWF) to any UE will cause privacy issues and should be studied.

### 5.2.2 Threats

If UE and network node exchanges interested slice information without any protection, then the MitM will be able to intercept what slices/services UE is interested in. Therefore, it will leak the privacy information of the UE..

.

### 5.2.3 Potential security requirements

The 5G system shall provide means to protect the slice information associated with the initial UE communication with the N3IWF/TNGF node.

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

### 5.3.1 Key issue details

The solutions to KI #2 enable the selection of TNGF/N3IWF that support the S-NSSAI(s) required by the UE, as defined in 3GPP TR 23700-17[2]. Many solutions are presented, and one of the categories is.

* The UE chooses the default TNGF/N3IWF, and the network selects the appropriate TNGF/N3IWF based on UE slice requirements and relocates the TNGF.

The TR 23700-17 [2] few solutions, for example, solutions 10 and 11, include the IKE v2 procedure enhancement to relocate the TNGF. Security aspects of the solutions in this category should be studied.

### 5.3.2 Threats

TBD.

### 5.3.3 Potential security requirements

TBD.

## 5.4 Key issue #4: Security aspect of TNAP mobility

### 5.4.1 Key issue details

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

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

### 5.4.2 Threats

TBD.

### 5.4.3 Potential security requirements

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

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

# 6 Proposed solutions

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

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

### 6.1.1 Introduction

This solution addresses the authentication of AUN3 devices based on the EAP\_AKA prime method.

### 6.1.2 Solution details

6.1.2.1 Procedure

 Figure 6.1.2.1-1: EAP-AKA prime based AUN3 authentication

1a. The AUN3 device establishes a WLAN connection with the WLAN Access Network (AN), using procedures specified in IEEE 802.11.

1b, 1c. L2 connection and EAP identity retrieval are performed. AUN3 device sends back EAP Response/Identity message. The AUN3 device uses SUCI in NAI format (i.e., username@realm format as specified in clause 28.7.3 of TS 23.003) or 5G-GUTI.

2a, 3a, 3b, 3c. If the RG is an FN-RG, the FN-RG sends the EAP response/Identity including the NAI to the W-AGF. The W-AGF creates a registration request on behalf of the AUN3 device with a new indication that the registration is on behalf of an AUN3 device where protection is required for the interface between the AUN3 device and RG. The W-AGF selects the AMF/SEAF.The W-AGF sends to the AMF/SEAF a registration request on behalf of the AUN3 device. The registration request includes the NAI SUCI, wireline network name if available, and the new indication. The same message content is forwarded from AMF to AUSF and then from AUSF to UDM.

2b, 3b, 3c. If the RG is a 5G-RG, the 5G-RG sends a NAS Registration Request message to the AMF, including the received SUCI and the new indicator for encryption required for AUN3 device.

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

5. Based on the indication in step 3, AMF derives the WAGF key.

6. The AMF sends NAS Security Mode Command mode and provides the WAGF key (KWAGF') to W-AGF.

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

Note: whether the PMK is derived by RG and W-AGF is out if 3GPP scope.

8. RG and AUN3 device will derive WLAN keys from PMK.

9. The AUN3 device performs a 4-way handshake to establish a secure connection with the WLAN AN.

6.1.2.2 Key derivation

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

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

- FC = 0x<to be defined>

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

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

- P1 = Access type distinguisher

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

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

6.1.2.2.2 KAUN3 key

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

- FC = 0x<to be defined>

- P0 = Usage type distinguisher

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

Usage type distinguisher value is set to 0x01.

### 6.1.3 Evaluation

TBD

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

### 6.2.1 Introduction

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

### 6.2.2 Solution details



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

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

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm.

Editor’s Note: subscription identifier privacy protection is FFS.

4a-4b. If the RG is an FN-RG, the FN-RG sends the EAP response/Identity including the NAI to the W-AGF. The W-AGF constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. If the RG is a 5G-RG, the 5G-RG constructs a SUCI from the NAI-based SUPI of the AUN3 device, and sends a NAS Registration Request message to the AMF, including the SUCI and an AUN3 device indicator.

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

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

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

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

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

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

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

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

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

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

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

### 6.2.3 Evaluation

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

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

### 6.3.1 Introduction

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

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

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

### 6.3.2 Solution details



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

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

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm.

Editor’s Note: subscription identifier privacy protection is FFS.

4a-4b. If the RG is an FN-RG, the FN-RG sends the EAP response/Identity including the NAI to the W-AGF. The W-AGF constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. If the RG is a 5G-RG, the 5G-RG constructs a SUCI from the NAI-based SUPI of the AUN3 device, and sends a NAS Registration Request message to the AMF, including the SUCI and an AUN3 device indicator.

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

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

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

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

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

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

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

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

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

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

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

### 6.3.3 Evaluation

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

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

### 6.4.1 Introduction

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

### 6.4.2 Solution details



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

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

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm.

Editor’s Note: subscription identifier privacy protection is FFS.

4a-4b. If the RG is an FN-RG, the FN-RG sends the EAP response/Identity including the NAI to the W-AGF. The W-AGF constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. If the RG is a 5G-RG, the 5G-RG constructs a SUCI from the NAI-based SUPI of the AUN3 device, and sends a NAS Registration Request message to the AMF, including the SUCI and an AUN3 device indicator.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 6.4.3 Evaluation

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

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

### 6.Y.1 Introduction

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

# 7 Conclusions

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

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

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities.

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

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

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

Annex X:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-07 | SA3#107e-AdHoc | S3-221341 |  |  |  | TR Skeleton (approved at SA3#107e-AdHoc) | 0.0.0 |
| 2022-07 | SA3#107e-AdHoc | S3-221703 |  |  |  | Inclusion of the documents approved at SA3#107e-AdHoc: S3-221636, S3-221637 S3-221638 | 0.1.0 |
| 2022-07 | SA3#107e-AdHoc |  |  |  |  | It removes the revision mark version from the zip file | 0.1.1 |
| 2022-08 | SA3#108-e | S3-222399 |  |  |  | Inclusion of the documents approved at SA3#108-e: S3-221767, S3-222395 | 0.2.0 |
| 2022-10 | SA3#108Adhoc-e | S3-223127 |  |  |  | Inclusion of the documents approved at SA3#108Adhoc-e: S3-222937, S3-222939, S3-222940, S3-223007, S3-223008, S3-223009, S3-222936, S3-222935 | 0.3.0 |