|  |  |
| --- | --- |
| 3GPP TR 33.857 V0.2.0 (2020-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on enhanced security support for Non-Public Networks;  (NPN);  (Release 17) | |
|  | |
|  |  |
|  | |
| 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.  © 2020, 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

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 Architectural and security assumptions 8

4.1 Architectural requirements 8

5 Key issues 8

5.1 Key Issue #1 Credentials owned by an external entity 8

5.1.1 Key issue details 8

5.1.2 Security threats 9

5.1.3 Potential security requirements 9

5.2 Key Issue #2 Provisioning of Credentials 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 10

5.3 Key Issue #3 Security impacts from supporting IMS voice and IMS services in SNPNs 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key Issue #4: Securing initial access for UE onboarding between UE and SNPN 10

5.4.1 Introduction 10

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

5.X Key Issue #X: <Key Issue Name> 11

5.X.1 Key issue details 11

5.X.2 Security threats 11

5.X.3 Potential security requirements 11

6 Solutions 11

6.0 Mapping of Solutions to Key Issues 11

6.1 Solution #1: Primary authentication between an SNPN and third-party AAA server using EAP 12

6.1.1 Introduction 12

6.1.2 Solution Details 12

6.1.2.1 Procedure 13

6.1.3 System impact 15

6.1.4 Evaluation 15

6.2 Solution #2: EAP authentication between UE and external AAA via AUSF 15

6.2.1 Introduction 15

6.2.2 Solution details 16

6.2.3 System impact 17

6.2.4 Evaluation 17

6.3 Solution #3: Primary authentication between an SNPN and third-party AAA server using EAP-TTLS 17

6.3.1 Introduction 17

6.3.2 Solution Details 17

6.3.2.1 Procedure 18

6.3.3 System impact 19

6.3.4 Evaluation 20

6.4 Solution #4: Authentication Framework Enhancements to support SNPN access 20

6.4.1 Introduction 20

6.4.2 Solution details 20

6.4.2.1 SNPN access using PLMN owned subscription credentials 20

6.4.2.2 SNPN access using third-party owned subscription credentials 20

6.4.3 System impact 22

6.4.4 Evaluation 22

6.5 Solution #5: Network Access Authentication with Credentials owned by an AAA external to the SNPN 22

6.5.1 Introduction 22

6.5.2 Solution details 24

6.5.3 System impact 25

6.5.4 Evaluation 25

6.6 Solution #6: Network access authentication with credentials owned by an entity separate from the SNPN 25

6.6.1 Introduction 25

6.6.2 Solution details 25

6.6.3 System impact 27

6.6.4 Evaluation 27

6.Y Solution #Y: <Solution Name> 27

6.Y.1 Introduction 27

6.Y.2 Solution details 27

6.Y.3 System impact 27

6.Y.4 Evaluation 27

7 Conclusions 28

Annex A (informative): Change history 28

# 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

The 5GS already supports certain specific features for Non-Public Networks, these are evolved in the architectural study documented in 3GPP TR 23.700-07[3], considering new functionality for Non-Public Networks. One of the main architectural changes in need of security enhancements are the allowance of credentials owned by a separate entity than a Standalone Non-Public Network. The other is onboarding and remote provisioning of non-USIM credentials to allow for a seamless setup of Non-Public Networks.

# 1 Scope

The present document …

# 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 TS 33.501: "Security architecture and procedures for 5G System"

[3] 3GPP TR 23.700-07: "Study on enhanced support of non-public networks (Release 17)"

[4] 3GPP TS 23.501: "System Architecture for the 5G System"

[5] IETF RFC 5281: " Extensible Authentication Protocol Tunneled Transport Layer Security

Authenticated Protocol Version 0 (EAP-TTLSv0) "

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 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].

**Provisioning Server:** The server that provisions the authenticated/authorized UE with the NPN credentials.

**SNPN credentials:** Information that the UE uses for authentication to access a SNPN.

For the purposes of the present document, the following terms and definitions given in 3GPP TR 23.700-07 [3] apply:

**Default UE credentials**: Information that the UE have before the actual onboarding procedure to make it uniquely identifiable and verifiably secure.

**Default Credential Server (DCS)**: The server that can authenticate a UE with default UE credentials or provide means to another entity to do it.

**NPN:** Non-Public Network as defined in TS 23.501 [4]. The terminology NPN refers to both SNPN and PNI-NPN in this TR unless otherwise stated.

**Onboarding Network (ON)**: The network providing initial registration and/or access to the UE for UE Onboarding.

**Unique UE identifier**: Identifying the UE in the network and the DCS and is assigned and configured by the DCS.

## 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].

DCS Default Credential ServerON Onboarding network

PS Provisioning Server

# 4 Architectural and security assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

## 4.1 Architectural requirements

- Solutions are built on the 5G System security architectural principles as in TS 33.501 [2] and conclusions drawn in TR 23.700-07 [3], including flexibility and modularity for newly introduced functionalities.

# 5 Key issues

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

## 5.1 Key Issue #1 Credentials owned by an external entity

### 5.1.1 Key issue details

This Key Issue aims at addressing security implications introduced in solutions related to Key Issue #1 Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN in TR 23.700-07 [3].

TR 23.700-07 [3] contains numerous solutions addressing Key Issue #1, where some solutions rely on a AAA-S external to the SNPN, depicted in 5.1.1-2, and others on an AUSF separated from the SNPN the UE is attempting to access, depicted in 5.1.1-1. These architectural changes may have an impact on security architecture, for instance, primary authentication.

Editor’s note: The solutions depicted are preliminary and might expand or reduce based on SA2 conclusion.

Figure 5.1.1-1: SNPN + PLMN

Figure 5.1.1-2: SNPN + non-PLMN

The solution are to describe how authentication is done with credentials owned by an entity separate from the SNPN and how keys may be shared between an entity separate from the SNPN and the SNPN, considering trust relationship between the SNPN and the separate entity owing the credentials.

### 5.1.2 Security threats

Weak authentication procedures may allow attackers to impersonate the UE towards the SNPN or vice versa.

Sharing of keying material between the SNPN and an entity separate from the SNPN during the key establishment procedure where authentication and key agreement is the same, may imply that a third party can derive keys on its own.

### 5.1.3 Potential security requirements

- The UE and SNPN shall support network access authentication procedure with credentials owned by an entity separate from the SNPN.

## 5.2 Key Issue #2 Provisioning of Credentials

### 5.2.1 Key issue details

This Key Issue aims at addressing security implications introduced in solutions related to Key Issue #4 in TR 23.700-07 [3].

The objective of Key Issue #4 in TR 23.700-07 [3] is twofold, UE onboarding and then remote provisioning of non USIM credentials for SNPN. This Key Issue aims at treating the security implications related to the provisioning part.

Designing completely new protocols is not in scope of this key issue.

Editor’s note: other details are FFS.

### 5.2.2 Security threats

Unprotected provisioning of SNPN credentials may cause the SNPN credentials to be obtained or manipulated by on-boarding network.

### 5.2.3 Potential security requirements

FFS

## 5.3 Key Issue #3 Security impacts from supporting IMS voice and IMS services in SNPNs

### 5.3.1 Key issue details

This key issue aims to analyse the potential security impacts from supporting IMS voice and IMS services in SNPNs. In Rel-16 SNPNs do not support IMS emergency services but for Rel-17 its expected that the enabling of IMS and IMS services for SNPNs is to be studied.

UEs that are to be used in SNPN are currently not required to have IMS credentials. It needs to be studied especially how these UEs can authenticate with the network. This means that solutions that address UEs without IMS credentials are in scope of this key issue.

Architectural requirement: Solutions to this key issue need to describe how the security, especially authentication, of supporting IMS voice and IMS services in SNPN is to be addressed.

### 5.3.2 Security threats

If the UE and the network do not mutually authenticate, an attacker could either impersonate the network towards the UE or the UE towards the network.

### 5.3.3 Potential security requirements

The UE and the network shall mutually authenticate before granting access to IMS and IMS services.

## 5.4 Key Issue #4: Securing initial access for UE onboarding between UE and SNPN

### 5.4.1 Introduction

The key issue addresses the authentication and authorization aspects of UE onboarding for SNPN in key issue #4 in TR 23.700-07 [3].

TR 23.700-07 [3] is studying UE identification, support of exposure API, network selection, authentication, and authorization procedure for UE and SNPN, and architecture enhancement to enable provisioning of SNPN credentials for primary authentication and SNPN configurations into the UE to enable SNPN access.

Especially, the procedure for securing initial access for UE onboarding between UE and an SNPN via an Onboarding SNPN before the UE's SNPN credentials are provisioned is considered in this key issue. The assumption is that the UE has not been provisioned with SNPN credentials for the SNPN the UE wants to access, nor for the onboarding SNPN. The UE may be provisioned with default credentials (e.g. Default UE Credentials). As part of this key issue, it should be considered if a Default Credential Server is deployed or not.

### 5.4.2 Security threats

- Unauthorized access by UEs to the onboarding SNPN may cause the resources of the onboarding SNPN to be misused or overloaded.

- Unauthorized onboarding SNPN serving the UE may mislead the UE, e.g., deliver wrong information to the UE.

### 5.4.3 Potential security requirements

The 5GS shall support a procedure allowing a UE to securely access an onboarding SNPN in order to gain access to SNPN credentials provisioning server.

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Key Issues | | | |
| Solutions | 1 | 2 | 3 | 4 |
| 1 | X |  |  |  |
| 2 | X |  |  |  |
| 3 | X |  |  |  |
| 4 | X |  |  |  |
| 5 | X |  |  |  |
| 6 | X |  |  |  |

## 6.1 Solution #1: Primary authentication between an SNPN and third-party AAA server using EAP

### 6.1.1 Introduction

This solution address Key Issue #1 Credentials owned by an external entity, in particular the case where the separate entity is deployed as a AAA server. It is assumed that the AAA server is some existing solution. Hence, no updates to the AAA server can be made.

The assumed architecture is described in TR 23.700-7 [3], clause 6.8.2.2. An illustration is provided here for convenience in Figure 6.1.1-1. The SNPN includes a complete 5GS SNPN network and the CdP is the Credential provider (AAA server in this case).



Figure 6.1.1-1: Access to SNPN services using credentials from Credential Provider (CdP) for authentication in the SNPN

### 6.1.2 Solution Details

This solution enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN. The credential provider will typically correspond with an already existing credential management system owned by the vertical owner of the SNPN 5GS.

The UE is provisioned with credentials (for any key-generating EAP method) managed by the CdP, which include an identifier and related security information and the CdP Identifier. The UE initiates registration in the SNPN using a SUPI containing a network-specific identifier, provided by the CdP and provisioned in the UE.

For the primary authentication procedure, the UDM allows the UE to run primary authentication with credentials owned by a certain CdP. The UDM indicates to the AUSF to proceed with primary authentication involving the corresponding CdP.

In this scenario the authentication server role is taken by the AAA. The AUSF acts as EAP authenticator and interacts with the AAA to execute the primary authentication procedure.

The shift of the AAA being the AAA server will result in an impact on the key hierarchy. The KAUSF is in this scenario derived from MSK instead of EMSK. This leads to impact on the UE and AUSF and also in the primary authentication procedure in the sense that an indication could be sent to the UE that the alternative key hierarchy is to be applied.

#### 6.1.2.1 Procedure



Figure: 6.1.2-1: Primary authentication with external domain

0. The UE is configured with credentials from the CdP e.g. SUPI containing a network-specific identifier and credentials for any key-generating EAP-method.

It is further assumed that there exists a trust relation between the AUSF (AAA-IWF) and the AAA. These entities need to be mutually authenticated, and the information transferred on the interface need to be confidentiality, integrity and replay protected.

1. The UE selects the SNPN and initiates UE registration in the SNPN. In case no SUPI is provisioned in the UE, the UE creates a SUCI/SUPI based on the CdP-UE ID provided by the CdP and provisioned in the UE.

NOTE 1: In the case of the UE constructing the SUPI, it is assumed that the SUPI is on NAI format and includes also the CdP ID in the domain part of the NAI, e.g. UEID@CdPID.

For construction of the SUCI, existing methods in TS 33.501 [2] can be used. If the public key of the SNPN is not provisioned in the UE, null scheme can be used with anonymised SUPI as described in Annex B of TS 33.501 [2].

Editor's note: User privacy for key-generating EAP-methods not covered by current procedures in TS 33.501 [2] is FFS.”

2. The AMF within the SNPN initiates primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF as currently specified in TS 33.501 [2]. The AMF selects an AUSF based on the SUCI presented by the UE as specified in TS 23.501 [4].

3. The AUSF checks with UDM within the SNPN for the authentication method to be executed for the UE using a Nudm\_UEAuthentication\_Get service operation as currently specified in TS 33.501 [2]. The AUSF selects a UDM also using the SUCI provided by the AMF as specified in TS 23.501 [4].

4. The UDM resolves the SUCI to the SUPI before checking the authentication method applicable for the UE. The UDM can obtain the common subscription data or individual subscription data based on the SUPI.   
  
The UDM determines that primary authentication is to be performed, with an external entity based on subscription data or by looking at the realm part of the SUPI in NAI format.

5. The UDM provides the AUSF with the UE SUPI and the applicable authentication method for the UE. In this case, the UDM indicates to the AUSF to run primary authentication with credentials owned by a certain CdP. The UDM provides the AUSF also with the address of the CdP if required. CdP UE ID is also provided if available in the subscription data.

6. Based on the indication from the UDM, the AUSF interacts with the CdP to execute the primary authentication procedure. The AUSF derives the CdP-UE ID from the SUPI unless received from UDM. The AUSF uses a AAA-P/IWF to interact with the CdP.

7. The UE executes the applicable authentication method with the CdP.

8. After successful authentication, the AUSF is provided by the MSK from the AAA.

9. The AUSF uses the most significant 256 bits of MSK (instead of EMSK) as the KAUSF. The AUSF also derives KSEAF from the KAUSF as defined in Annex A.6 of 33.501 [2].   
  
Editor's note: It is FFS whether the security implications of using MSK as the KAUSF is acceptable or if other input, not known to the external AAA is to be used for input when deriving the KAUSF from MSK.

10. The AUSF sends to the AMF the successful indication together with the SUPI of the UE and the resulting KSEAF, and optionally an indicator that MSK has been used.

11. The AMF sends the MSK indicator to the UE in a NAS message

12. The UE decides to derive the KAUSF from MSK instead of EMSK, either based on the indicator received from AMF or by interpretation of the realm part of the NAI that might indicate the use of external CdP.   
  
Editor's note: It is FFS whether the UE instead of the above can be pre-configured with the information which key derivation method to use.

### 6.1.3 System impact

**UE**

KAUSF is derived from MSK instead of EMSK. The decision to do this can be based on an indicator received from the AMF or by interpretation of the realm part of the UE ID in NAI format.

**AMF**

Relay of new MSK indicator

**UDM**

Decision if external authentication is to be triggered, e.g. by interpreting the realm part of NAI or by UE subscription data.

**AUSF**

KAUSF is derived from MSK instead of EMSK.

Send new indicator towards AMF indicating MSK usage.

**AAA-S**

None

### 6.1.4 Evaluation

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

The solution fulfils the potential security requirements of KI#1 and shows how a key-generating EAP method can be used as primary authentication with a separate entity.

UE and AUSF are impacted by the use of a new key hierarchy option.

As a result of the proposed solution, the CdP will be able to derive the KAUSF from the MSK. As a consequence of this, the CdP could use this to compromise security mechanisms based on KAUSF. Because of this, a the CdP must be trusted by the SNPN.

To protect the transfer of the MSK, the interface between AAA-IWF and the AAA needs security measures to prevent the MSK (and thereby KAUSF) from being compromised by any external parties.

## 6.2 Solution #2: EAP authentication between UE and external AAA via AUSF

### 6.2.1 Introduction

This solution addresses the key issue #1 - Credentials owned by an external entity. It supports the use of any key generating EAP method to authenticate UE by an external entity consisting of a AAA server (AAA-E).

Particular considerations are given to maintain the same key hierarchy as other primary authentication (e.g., EAP-AKA’) when the credentials are owned by an internal entity (i.e., UDM). Such consideration allows to eliminate impact on UE side and minimize impact on core network components.

To maintain the key hierarchy on the UE side, this proposal requires AAA server to be able to derive KSEAF from EMSK according to TS 33.501.

### 6.2.2 Solution details



1. The UE sends to the SEAF a Registration Request message, including the SUCI which is constructed from the UE SUPI. The SUPI is of the type of NAI in the form of username@realm. The “username” shall be either “anonymous” or omitted if the subscriber identifier privacy is required by SNPN and the public key of the SNPN is not provisioned in the UE.

2. The SEAF sends to the AUSF Nausf\_UEAuthentication\_Authenticate Request message, including the SUCI and the SN-name (the serving network name).

3. The AUSF sends to the UDM the the Nudm\_UEAuthentication\_Get Request, including the SUCI and the SN-name.

4. The UDM de-conceals the SUCI to obtain the SUPI. If the SUCI is not constructed using the null-scheme, the UDM invokes the SIDF located within the UDM to de-conceal the SUCI.

The the “username” portion of the SUPI could be a real username, “anonymous”, or null (i.e., omitted). In any case, the UDM uses the SUPI to determine that the credentials of this UE is owned by an external entity and return the information that is needed by the AUSF to use the AAA-E to authenticate the UE.

Editor Note. Since the EAP method itself may provide subscriber privacy, it is FFS whether such a SUCI calculation using non-null scheme is needed at the UE. If it is needed, the details on SUCI calculation is FFS

5. The UDM sends to the AUSF the Nudm\_UEAuthentication\_Get Response, which also includes the SUPI and any additional information that may assist AUSF to reach AAA-E.

6. The AUSF uses SUPI, any assistant information from the UDM, and/or local information to determine that an AAA server needs to be invoked to authenticate the UE.

The AUSF sends an authentication request to the AAA server. The exact message format of this authentication request depends on the interface overwhich the request is sent. It could be a service based interface if there is an interworking function to external AAA-E, or an AAA interface (e.g., RADIUS or DIAMETER) which may go through an AAA proxy (AAA-P).

Note that SUPI is needed to route the request to the ultimate destination AAA-E since there may be additional AAA proxies in front of the AAA-E. SN-Name is needed to derive KSEAF.

7. An intermediate entity (e.g., AAA-P) forwards the authentication request to the AAA-E.

8. The AAA-E and the UE performs an EAP authentication that is selected by the AAA-E.

9. Upon the successful completion of EAP authentication, the AAA-E dervises KSEAF from EMSK according to 33.501, sends an Access Accept messages to the AAA-P, including EAP Success, SUPI, and KSEAF.

Note that SUPI is needed since the SUPI received by AUSF in step 5 may be anonymous. KSEAF is derived by the AAA-E to maintain the same key hierarchy as the other primary authentication method (e.g., EAP-AKA’). Further, having AAA-E deriving KSEAF and send it the AUSF fully complies with RFC 5295.

10. The AAA-P forwards the Access Accept (or translates it to a service authentication response) to the AUSF, including EAP Success, SUPI, and KSEAF.

11. The AUSF sends to the SEAF an EAP-Success message along with the SUPI and the KSEAF in a Nausf\_UEAuthentication\_Authenticate Response message.

12. The SEAF forwards to the UE the EAP-Success message in an Authentication Result message or a Security Mode Command message.

Upon receiving the EAP-Success message, the UE derives the KAUSF and the KSEAF in the same way as the AUSF according to 3GPP TS 33.501.

By this point, the EAP authentication between the AAA-E and the UE has been successfully completed.

Editor’s Note: The architectural relationship between AUSF and \*-AAA including the derivation of keys is FFS. This includes the transfer of keys/messages in steps 6,7, 9 and 10.

### 6.2.3 System impact

This solution has impact on UDM, AUSF, and AAA-E.

When UDM receives Nudm\_UEAuthentication\_Get\_Request and obtains a SUPI that is owned by an external entity, it may not be able to and need not to select an authentication method. In addition, the UDM may need to return information back to allow AUSF to use an AAA-E to authenticate the UE.

When AUSF receives Nudm\_UEAuthentication\_Get\_Response, it needs to be able to make decision to use an AAA-E to authenticate the UE.

AAA-E needs to derive KSEAF according to 3GPP TS 33.501.

There is no impact on UE side other than that the UE need to support the EAP method chosen by AAA-E for authentication.

### 6.2.4 Evaluation

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

## 6.3 Solution #3: Primary authentication between an SNPN and third-party AAA server using EAP-TTLS

### 6.3.1 Introduction

This solution address Key Issue #1 Credentials owned by an external entity, in particular, the case where the separate entity is deployed as a AAA server. It is assumed that the AAA server is some existing solution. Hence, no updates to the AAA server can be made.

### 6.3.2 Solution Details

This solution relies on the decision in Annex I of TS 33.501[2] that any key generating EAP-method can be used for primary authentication to SNPN. In this case EAP-TTLS is used.

In this setting, a TLS tunnel is established between the UE and AUSF, based on the AUSF server certificate only. Through the established tunnel, any legacy authentication protocol can be run towards the AAA, for example other EAP methods. In this case, the KAUSF is derived by the AUSF from the EMSK established in the first (outer) authentication. This would not impact the key hierarchy. However, this would mean that the KAUSF is based solely on the AUSF credentials, not on the UE credentials or the output keys from the UE authentication.

Also, for this to work, the UE would need to be provisioned with the root of trust to enable verification of the AUSF certificate. The root of trust for the SNPN could potentially be provided during the onboarding procedure (studied in KI#4 of TR 23.700-7 [3]) or installed during manufacturing.

#### 6.3.2.1 Procedure



Figure: 6.3.2-1: Primary authentication with external domain

0. The UE is configured with credentials from the CdP e.g. SUPI containing a network-specific identifier, and credentials for any key-generating EAP-method.

The UE and TTLS server (AUSF) may have a one-way security relationship based on the TTLS server's (AUSF) possession of a private key guaranteed by a CA certificate which the user trusts or may have a mutual security relationship based on certificates for both parties.

1. The UE selects the SNPN and initiates UE registration in the SNPN. The UE creates a SUCI/SUPI based on the CdP-UE ID provided by the CdP and provisioned in the UE.

NOTE 1: It is assumed that the SUPI is on NAI format and includes also the CdP ID in the domain part of the NAI, e.g. UEID@CdPID.

For construction of the SUCI, existing methods in TS 33.501 [2] can be used. If the public key of the SNPN is not provisioned in the UE, null scheme can be used with anonymised SUPI as described in Annex B of TS 33.501 [2].

Editor's note: User privacy for key-generating EAP-methods not covered by current procedures in TS 33.501 [2] is FFS.”

2. The AMF within the SNPN initiates primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF as currently specified in TS 33.501 [2]. The AMF selects an AUSF based on the SUCI presented by the UE as specified in TS 23.501 [4].

3. The AUSF checks with UDM within the SNPN for the authentication method to be executed for the UE using a Nudm\_UEAuthentication\_Get service operation as currently specified in TS 33.501 [2]. The AUSF selects a UDM also using the SUCI provided by the AMF as specified in TS 23.501 [4].

4. The UDM resolves the SUCI to the SUPI before checking the authentication method applicable for the UE. The UDM can obtain the common subscription data or individual subscription data based on the SUPI.   
  
The UDM determines that primary authentication is to be performed using EAP-TTLS based on subscription data or by interpreting the realm part of the NAI.

5. The UDM provides the AUSF with the UE SUPI and the applicable authentication method for the UE. In this case, the UDM indicates to the AUSF to run primary authentication using EAP-TTLS. The UDM provides the AUSF also with the address of the CdP if required. CdP UE ID is also provided if available in the subscription data.

6. Based on the indication from the UDM, the AUSF runs EAP-TTLS phase 1 towards the UE as specified in RFC 5281 [5].

7. The UE runs EAP-TTLS phase 2 towards the CdP (AAA) as specified in RFC 5281 [5].

8. After successful authentication, an EMSK is established from the authentication in step 6. The AUSF derives the KAUSF from the EMSK as described in 33.501 [2] (using the 256 msb of the EMSK as KAUSF). The AUSF also derives KSEAF from the KAUSF as defined in Annex A.6 of 33.501 [2].

9-10. As described in steps 20, 21 of Annex B in TS 33.501, [2].

### 6.3.3 System impact

**UE**

UE needs to be provisioned with the CA certificate used for signing the AUSF certificate.

UE needs to support EAP-TTLS.

**AMF**

None

**UDM**

UDM needs to be able to determine that EAP-TTLS shall be run.

**AUSF**

AUSF needs to support EAP-TTLS

**AAA-S**

None

### 6.3.4 Evaluation

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

The solution fulfils the potential security requirements of KI#1 and shows how a key-generating EAP method can be used as primary authentication with a separate entity.

Key hierarchy is not impacted.

## 6.4 Solution #4: Authentication Framework Enhancements to support SNPN access

### 6.4.1 Introduction

This solution address key issue #1 (Credentials owned by an external entity).

### 6.4.2 Solution details

#### 6.4.2.1 SNPN access using PLMN owned subscription credentials

When PLMN credentials are used to access the SNPN, this solution proposes that the existing roaming architecture for 5GS is reused, where the SNPN takes the role of VPLMN and the entity owning the PLMN credentials takes the role of HPLMN.

#### 6.4.2.2 SNPN access using third-party owned subscription credentials

When the subscription credentials are owned by a third-party entity, it is assumed that the SNPN trusts the third-party to store and process the subscription credentials used for primary authentication. Two architecture variants are considered depending on the authentication method used, i.e., EAP-based authentication method (EAP-AKA’ or another EAP authentication method) or 5G AKA.

**Variant 1: EAP-based authentication framework:**

In this variant, in order to isolate SNPN from the third-party network, a proxy AUSF (denoted as AUSF\* here onwards) is introduced in the SNPN network. AUSF\* supports N12 interface towards the AMF. The AUSF\* also interfaces with the third-party using the N12\* interface.

The EAP based 5GS primary authentication is performed between the UE and the AAA server in the third-party network. The AAA server can be either 5GS aware AAA (i.e., a AAA server that implements the necessary functions (e.g., AUSF/UDM/ARPF/SIDF for successful 5GS authentication, including providing of KSEAF to the SNPN after successful authentication) or a non-5GS aware AAA (e.g., a legacy AAA that supports a key generating EAP authentication method but does not support 5GS specific functions).

The figure below illustrates the EAP-based authentication framework.



Figure 6.4.2.2-1: EAP based 5G authentication framework for SNPN access

In case the AAA server is 5GS aware, then the N12\* can be the same as the N12 interface with AUSF\* providing a AAA proxy functionality for security isolation between the SNPN and the third-party network.

In case the AAA server is non-5GS aware (i.e., legacy AAA server), after successful EAP authentication, the AAA can only provide the MSK to the AUSF\*. Furthermore, the AUSF\* derives the KSEAF from the received MSK (treating it as the KAUSF). The N12\* interface is a standard AAA/EAP interface.

Editor’s Note: It is FFS whether the security implications of using MSK as the KAUSF is acceptable in case legacy AAA server is used for SNPN access.

**Variant 2: 5G AKA based authentication framework:**

In this variant, the AUSF\* is located in the SNPN and the rest of the necessary 5GS authentication functions (i.e., AUSF/UDM/ARPF/SIDF) resides in the 3rd party network. AUSF\* is a N12 proxy and provides the necessary isolation between the SNPN and the third-party network. The figure below illustrates the 5G AKA based authentication framework.



Figure 6.4.2.2-2: 5G AKA based authentication framework for SNPN access

### 6.4.3 System impact

This solution has no UE impacts expect when an EAP authentication is used with a legacy AAA server, in which case, the UE needs to derive KSEAF from MSK instead of KAUSF. Therefore, when legacy AAA server is used, the UE needs to know that KSEAF is derived from MSK instead of KAUSF/EMSK, which can be implicit based on the EAP method implementation on the UE.

Editor’s Note: When a legacy AAA server is used, it needs to be further clarified how the UE knows that the KSEAF is derived from the MSK.

There are no impacts on the serving network entities (e.g., (R)AN, AMF/SEAF).

A new AAA proxy function, AUSF\*, is introduced in the SNPN network.

### 6.4.4 Evaluation

TBD

## 6.5 Solution #5: Network Access Authentication with Credentials owned by an AAA external to the SNPN

### 6.5.1 Introduction

This solution addresses key issue #1, especially for SNPN + non-PLMN scenario depicted in figure 5.1.1-2.

The specific architecture is shown in figure 6.5.1-1 from TR 23.700-07 [3].

UE

(R)AN

UPF

N2

N4

N1

N3

N12

N13

AMF

SMF

AUSF

UDM

N11

N8

SNPN

AAA

Nxx

3rd party

PAF

TBD

**Figure 6.5.1-1: Architecture for Network Access Authentication with Credentials owned by an AAA external to the SNPN**

The solution assumes that:

* The 3rd party provides AAA, and the UE credentials are stored in the AAA.
* Primary Authentication Function (PAF) is introduced in SNPN for translation of SBI protocol and AAA protocol. The function can be collocated with NSSAAF, or AUSF.

The UE provides SUCI to the SNPN, and the AUSF retrieves UE’s credentials from the AAA according to SUCI and trigger EAP based authentication. In this solution, AAA performs role of authentication server.

### 6.5.2 Solution details

**PAF**

**AAA**

**AUSF**

**UE**

**SEAF**

1. Registration Request

(UE ID)

2. Nausf\_UEAuthentication\_

Authenticate Request (UE ID)

3. SBI

(EAP trigger, AAA address)

4.AAA

(EAP trigger)

5. EAP (e.g. EAP-TLS)

6. AAA (EAP success, MSK)

10. Nausf\_UEAuthentication\_

Authenticate Response (EAP success, Kseaf)

7. SBI (EAP success, MSK)

9. Derive Kseaf according to Kausf

11. Auth-Req. (EAP success, ngKSI, ABBA)

12. Derive Kamf according to MSK

8. Derive Kausf according to MSK

**Figure 6.5.2-1: Network Access Authentication**

1. The UE sends the Registration Request message to the SEAF, containing UE ID.

2. The SEAF sends Nausf\_UEAuthentication\_Authenticate Request message to AUSF. The message includes the UE ID.

3. The AUSF invokes external primary authentication service provided by PAF. The AUSF sends SBI message containing AAA address and EAP trigger (e.g. EAP-TLS start) message. The AUSF derives AAA address according to UE ID.

4. The PAF finds AAA according to AAA address, translates SBI message to AAA protocol, and sends the EAP trigger message to the AAA. The EAP trigger message can be EAP-start message to trigger AAA for EAP authentication.

5. The AAA triggers EAP authentication based on EAP trigger message, and plays as authentication server role. PAF, AUSF, and SEAF transparent the EAP messages exchanged between UE and AAA.

6. If the authentication successes, the AAA derives MSK and EMSK, the AAA sends EAP success message and MSK with AAA protocol to the PAF.

7. The PAF sends EAP success message and MSK via SBI to the AUSF.

8. The AUSF derives KAUSF according to MSK.

9. The AUSF calculates KSEAF from KAUSF.

10. The AUSF sends the Nausf\_UEAuthentication\_Authenticate message to the SEAF, the message includes EAP success message together with the derived KSEAF.

11. The SEAF sends Authentication Request message to the UE, the authentication procedure is finished. The message includes EAP success message, ngKSI and ABBA parameter. The SEAF derives the KAMF according the KSEAF.

12. Upon receiving the EAP-Success message, the UE derives MSK and EMSK and uses the MSK to derive the KAUSF, and then derives KSEAF according to KAUSF. The UE derives the KAMF from the KSEAF. The KAMF will be used to enable NAS and AS security.

Editor’s Note: Security implications of deriving Kausf from MSK is ffs.

Editor’s Note: It needs to be clarified whether and how SUPI concealment can be used.

Editor’s Note: It needs to be clarified how the UE knows that the K\_AUSF is derived from the MSK instead of the EMSK."

### 6.5.3 System impact

TBA.

### 6.5.4 Evaluation

TBA.

## 6.6 Solution #6: Network access authentication with credentials owned by an entity separate from the SNPN

### 6.6.1 Introduction

This solution addresses Key Issue #1 “Credentials owned by an external entity”.

The AUSF is taking the role of a AAA proxy towards the the AAA server of the service provider holding the credentials. It is assumed that the SNPN and the service provider have a SLA in place with respective security for the secure transport of messages between the two entities, e.g. TLS or IPSec. The AAA server is 5GS aware and can derive a KAUSF.

The assumption here is that the UDM grants a certain number of default profiles for the service provider and the service provider is on the other hand configured with the routing ID for the particular UDM holding those subscritpions.

The NAI of the UE at the service provider with username@realm is then used in the SNPN as SUPI.

### 6.6.2 Solution details



Figure 6.6.2: Network access authentication with credentials owned by an entity separate from the SNPN

1. The UE sends a Registration Request with the NAI (pseudonym@realm or username@realm) of the Service Provider as UE identity to the AMF. The username of the NAI maybe set to anonymous if the EAP method of the Service Provider supports privacy, or to a pre-configured pseudonym or the subscription identifier of the Service Provider.

2. The AMF detects based on the realm of the NAI that the Registration Request is not from a subscriber of the SNPN but from a Service Provider. The AMF authorizes the request by verifying the realm of the NAI and whether the SNPN has an active agreement with this Service Provider. The AMF forwards the request to the AUSF which may be preconfigured for handling requests towards external Service Providers.

3. The AUSF may perform authorization of the registration request by verifying the realm of the NAI and whether the SNPN has an active agreement with this Service Provider. The AUSF identifies the Service Provider and takes the role of an AAA-Proxy, sending a related AAA message to the corresponding AAA-Server.

4. The AAA-Server verifies the authentication request based on the username. If the AAA-Server supports privacy, then the related EAP message e.g. in tunnel mode, will receive the real identity protected in the first exchange with the UE during authentication. The AAA-Server selects the subscriber profile based on the username and performs an EAP based authentication with the UE, using the pre-shared credentials in the UE and the subscriber profile in the AAA-Server.

5. After successful authentication, the AAA-Server derives EMSK and further using the most significant 256 bits of EMSK as the KAUSF.

The UE derives the same keys accordingly.

The AAA-Server may select the stored Routing ID (preconfigured in step 0) for the SNPN as well as the validity time for one authentication period, i.e. after which the AMF should trigger a re-authentication request.

6. The AAA-Server sends the result of the authentication back in an authentication response to the AUSF and may include the KAUSF, validity time, Routing ID, result of the authenticaiton and the NAI of the UE with the real username of the subscription profile in the AAA-Server of the UE, which is used further as the SUPI in the SNPN.

7. The AUSF verifies the response and selects the UDM e.g. based on pre-configuration or based on the Routing ID. The AUSF sends to the UDM the NAI of the UE and the result of the authentication, similar to clause 6.1.4.1a of TS 33.501.

The AUSF derives the KSEAF from the KAUSF according to 3GPP TS 33.501.

8. The AUSF sends an authentication response to the AMF/SEAF including the authentication result from the Service Provider and the KSEAF, the NAI of the UE to be used as SUPI, the validity time, i.e. time until the next re-authentication.

9. The AMF/SEAF may perform from now on the normal procedures like for a normal 5G subscriber, e.g. NAS SMC, AS SMC etc. and sets up the security for the NAS protocol and the radio interface. For KAMF derivation the NAI of the UE is used as specified in TS 33.501.

Editor’s Note: The architectural relation between AUSF and AAA including the derivation of keys is FFS.

### 6.6.3 System impact

Editor’s Note: Each solution should clearly list which entities need new functionality and what functionality they need for the provided solution to work.

### 6.6.4 Evaluation

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

## 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 System impact

Editor’s Note: Each solution should clearly list which entities need new functionality and what functionality they need for the provided solution to work.

### 6.Y.4 Evaluation

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

# 7 Conclusions

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

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100-e | S3-201582 |  |  |  | TR Skeleton | 0.0.0 |
| 2020-08 | SA3#100-e | S3-202068 |  |  |  | Version after incorporating changes from S3-202089, S3-202091, S3-202092, S3-202093 and S3-201925 | 0.1.0 |
| 2020-10 | SA3#100bis-e | S3-202716 |  |  |  | Version after incorporating changes from S3-202732, S3-202715, S3-202515, S3-202681, S3-202721, S3-202682, S3-202724, S3-202750 and S3-202783 | 0.2.0 |