|  |  |
| --- | --- |
| 3GPP TR 33.857 V17.1.0 (2022-03) | |
| 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.  © 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 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 7

Introduction 8

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 10

3.1 Terms 10

3.2 Abbreviations 10

4 Architectural and security assumptions 11

4.1 Architectural requirements 11

4.2 Security assumptions 11

5 Key issues 11

5.1 Key Issue #1: Credentials owned by an external entity 11

5.1.1 Key issue details 11

5.1.2 Security threats 12

5.1.3 Potential security requirements 12

5.2 Key Issue #2: Provisioning of Credentials 12

5.2.1 Key issue details 12

5.2.2 Security threats 13

5.2.3 Potential security requirements 13

5.3 Key Issue #3: Security impacts from supporting IMS voice and IMS services in SNPNs 13

5.3.1 Key issue details 13

5.3.2 Security threats 13

5.3.3 Potential security requirements 13

5.4 Key Issue #4: Securing initial access for UE onboarding between UE and SNPN 14

5.4.1 Introduction 14

5.4.2 Security threats 14

5.4.3 Potential security requirements 14

5.5 Key Issue #5: Roaming-related security mechanisms for SNPNs 14

5.5.1 Key issue details 14

5.5.2 Security threats 14

5.5.3 Potential security requirements 14

6 Solutions 15

6.0 Mapping of Solutions to Key Issues 15

6.1 Solution #1: Primary authentication between an SNPN and third-party AAA server using EAP 15

6.1.1 Introduction 15

6.1.2 Solution Details 16

6.1.2.0 General 16

6.1.2.1 Procedure 17

6.1.3 System impact 18

6.1.4 Evaluation 19

6.2 Solution #2: EAP authentication between UE and external AAA via AUSF 19

6.2.1 Introduction 19

6.2.2 Solution details 19

6.2.3 System impact 20

6.2.4 Evaluation 21

6.3 Solution #3: Primary authentication between an SNPN and third-party AAA server using EAP-TTLS 21

6.3.1 Introduction 21

6.3.2 Solution Details 21

6.3.2.0 General 21

6.3.2.1 Procedure 22

6.3.3 System impact 24

6.3.4 Evaluation 24

6.4 Solution #4: Authentication Framework Enhancements to support SNPN access 24

6.4.1 Introduction 24

6.4.2 Solution details 24

6.4.2.1 SNPN access using PLMN owned subscription credentials 24

6.4.2.2 SNPN access using third-party owned subscription credentials 25

6.4.3 System impact 26

6.4.4 Evaluation 26

6.5 Solution #5: Network Access Authentication with Credentials owned by an AAA external to the SNPN 27

6.5.1 Introduction 27

6.5.2 Solution details 28

6.5.3 System impact 29

6.5.4 Evaluation 29

6.6 Solution #6: Network access authentication with credentials owned by an entity separate from the SNPN 29

6.6.1 Introduction 29

6.6.2 Solution details 30

6.6.3 System impact 31

6.6.4 Evaluation 31

6.7 Solution #7: EAP authentication between UE and external AAA with enhanced security of KAUSF 31

6.7.1 Introduction 31

6.7.2 Solution details 32

6.7.3 System impact 34

6.7.4 Evaluation 34

6.8 Solution #8: UE onboarding for SNPN with AAA-S as DCS 34

6.8.1 Introduction 34

6.8.2 Solution details 36

6.8.3 System impact 37

6.8.4 Evaluation 37

6.9 Solution #9: UE onboarding for SNPN with UDM as DCS 37

6.9.1 Introduction 37

6.9.2 Solution details 38

6.9.2.0 General 38

6.9.2.1 Procedure 38

6.9.3 System impact 39

6.9.4 Evaluation 39

6.10 Solution #10: Secure initial access to an SNPN onboarding network 39

6.10.1 Introduction 39

6.10.2 Solution details 40

6.10.3 System impact 41

6.10.4 Evaluation 41

6.11 Solution #11: Securing initial access by using primary authentication 41

6.11.1 Introduction 41

6.11.2 Solution details 42

6.11.3 System impact 43

6.11.4 Evaluation 43

6.12 Solution #12: Authentication for UE Onboarding for SNPN 43

6.12.1 Introduction 43

6.12.2 Solution details 45

6.12.2.1 Authentication for onboarding with default credentials is provisioned in UDM 45

6.12.2.2 Authentication for onboarding with default credentials is provisioned in DCS 46

6.12.3 System impact 47

6.12.4 Evaluation 47

6.13 Solution #13: UE Onboarding for an SNPN from Onboarding SNPN with Secondary Authentication using EAP method with UE identity privacy 47

6.13.1 Introduction 47

6.13.2 Solution details 48

6.13.3 System impact 50

6.13.4 Evaluation 51

6.14 Solution #14: Initial access for UE Onboarding for an SNPN from Onboarding SNPN using primary and secondary authentication 51

6.14.1 Introduction 51

6.14.2 Solution details 52

6.14.2.0 General 52

6.14.2.1 Using EAP-TLS Authentication Procedures over 5G Networks for initial one-way authentication 54

6.14.3 System impact 56

6.14.4 Evaluation 57

6.15 Solution #15: Privacy protection of UE onboarding identifier 57

6.15.1 Introduction 57

6.15.2 Solution details 57

6.15.3 System impact 58

6.15.4 Evaluation 58

6.16 Solution #16: UE onboarding for SNPN with the interaction between PS and DCS 58

6.16.1 Introduction 58

6.16.2 Solution details 59

6.16.2.1 Procedure 59

6.16.2.2 Procedure 60

6.16.3 System impact 61

6.16.4 Evaluation 61

6.17 Solution #17: Solution to Provisioning of PNI-NPN Credentials 61

6.17.1 Introduction 61

6.17.2 Solution details 61

6.17.3 System Impact 62

6.17.4 Evaluation 62

6.18 Solution #18 Solution on service authorization for SNPNs 63

6.18.1 Introduction 63

6.18.2 Solution Details 63

6.18.3 System impact 64

6.18.4 Evaluation 64

6.19 Solution #19: Secure onboarding without client authentication 65

6.19.1 Introduction 65

6.19.2 Solution details 65

6.19.3 System impact 68

6.19.4 Evaluation 68

6.20 Solution #20: Control plane based provisioning: PS to AUSF 68

6.20.1 Introduction 68

6.20.2 Solution details 69

6.20.3 System impact 70

6.20.4 Evaluation 70

6.21 Solution #21: Control plane based provisioning: PS to UDM 71

6.21.1 Introduction 71

6.21.2 Solution details 72

6.21.3 System impact 73

6.21.4 Evaluation 73

6.22 Solution #22: Solution for onboarding and provisioning 73

6.22.1 Introduction 73

6.22.2 Solution details 73

6.22.3 System impact 75

6.22.4 Evaluation 75

6.23 Solution #23: Solution to enable onboarding and secured UE access based on credentials owned by an external entity 76

6.23.1 Introduction 76

6.23.2 Solution details 76

6.23.3 System impact 78

6.23.4 Evaluation 78

6.24 Solution #24: Secure mutually authenticated onboarding without DCS 78

6.24.1 Introduction 78

6.24.2 Solution details 79

6.24.3 System impact 81

6.24.4 Evaluation 81

6.25 Solution #25: UE Onboarding for an SNPN with EAP-TLS 81

6.25.1 Introduction 81

6.25.2 Solution details 81

6.25.2.1 General 81

6.25.2.2 Procedure 82

6.25.3 System impact 83

6.25.4 Evaluation 83

7 Conclusions 84

7.1 Conclusions on KI #1: Credentials owned by an external entity 84

7.2 Conclusions on KI #2: Provisioning of Credentials 84

7.3 Conclusions on KI #3: Security impacts from supporting IMS voice and IMS services in SNPNs 84

7.4 Conclusions on KI #4: Securing initial access for UE onboarding between UE and SNPN 85

7.5 Conclusions on KI #5: Roaming-related security mechanisms for SNPNs 85

Annex A (informative): Change history 86

# 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 aim of the present document is to study the security aspects for any potential enhancements based on the outcome of the study in TR 23.700-07 [3]. For each of the objectives in the scope of the study in TR 23.700-07 [3], the security aspects that are to be covered in the present document are as follows:

- Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN

- Study potential solutions for authentication using credentials owned by an entity separate from the SNPN

- UE Onboarding and remote provisioning of non-USIM credentials

- Identify security Key Issues relating to UE Onboarding and remote provisioning with non-USIM credentials

- Identify methods by which the UE can be verified as "uniquely identifiable and verifiably secure"

- Critically review the security aspects of the proposed solutions in TR 23.700-07 [3] and make recommendations for security improvements where required.

- Study potential solutions for the secure provisioning of non-USIM credentials taking into account different deployment scenarios.

NOTE 1: The term USIM in this context denotes the IMSI accompanied by AKA credentials (i.e. for primary authentication with the PLMN).

- Support of IMS voice and emergency services for SNPN:

- Analyse 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.

NOTE 2: Key issue 2 in TR 23.700-07 [3] is assumed to not require any study from a security perspective.

# 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)"

[6] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[7] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[8] IETF RFC 7542: "The Network Access Identifier"

[9] 3GPP TS 23.003: "Numbering, addressing and identification"

[10] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)"

[11] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"

[12] IETF RFC 2903: "Generic AAA Architecture"

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 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 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 the present document unless otherwise stated.

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

**Onboarding SUCI:** A SUCI created from the Onboarding SUPI and used for onboarding purposes.

**Onboarding SUPI:** A SUPI that is based on the Unique UE Identifier and/or the Default UE Credentials and is used for onboarding purposes.

**Subscription Owner (SO):** The entity that stores and as result of the UE Onboarding procedures provide the subscription data and optionally other configuration information via the PS to the UE.

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

NOTE: The unique UE identifier is assumed to be unique within the DCS. It takes the form of a Network Access Identifier (NAI) using the NAI RFC 7542 [8].

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

DCS Default Credential Server

EIR Equipment Identity Register

ON Onboarding network

PEI Permanent Equipment Identifier

PS Provisioning Server

SO Subscription Owner

# 4 Architectural and security assumptions

## 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.

## 4.2 Security assumptions

- It is assumed for the case where non-USIM credentials are provisioned for SNPN, the non-USIM credentials are of a key generating EAP method type.

- It is assumed for the case where non-USIM credentials are provisioned for PNI-NPN, the non-USIM credentials are of an EAP method type.

# 5 Key issues

## 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.



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 and PNI-NPN. This Key Issue aims at studying the corresponding security implications related to the provisioning. For PNI-NPNs, only credentials for secondary and slice-specific authentication need to be considered.

The UE can perform the onboarding procedure with an onboarding network, and then the UE may be remotely provisioned with the credentials by a Provisioning Server (PS). Trust relationship between the PS and the credential owners (e.g., if they are different, does the credentials need to be protected from PS owner?) should be considered.

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

### 5.2.2 Security threats

An unauthorized UE may be able to access PS for maliciously requiring remote provisioning service.

An unauthorized PS may be able to provide wrong remote provisioning service to the UE.

Unprotected provisioning of credentials may cause the SNPN credentials to be obtained or manipulated.

### 5.2.3 Potential security requirements

The UE and the PS should be authorized for remote provisioning.

NOTE 1: The entity granting the authorization is not addressed in the present document.

Credentials shall be confidentiality protected, integrity protected, and replay protected during remote provisioning.

NOTE 2: Whether the protection in the above requirement requires to specify a solution in normative phase or whether it is left for implementation is not addressed in the present document.

NOTE 3: Whether the solution covers all type of devices (e.g. MEs with limited resources not able to run certain types of security protocols) is not addressed in the present document.

NOTE 4: The end points for the protection in the above requirement is not addressed in the present document.

NOTE 5: User intent to authorize the provisioning is not addressed in the present document.

NOTE 6: Further requirements are not addressed in the present document.

## 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. Legacy SNPNs do not support IMS emergency services but it is 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.

## 5.5 Key Issue #5: Roaming-related security mechanisms for SNPNs

### 5.5.1 Key issue details

TR 23.700-07 [3] defines a roaming architecture to support SNPN along with credentials owned by an entity separate from the SNPN. It needs to be studied whether and how security mechanisms related to roaming between PLMN are applicable for the roaming scenario between SNPN and SNPN/PLMN.

In current roaming architecture for PLMN, access token is a requirement for a NF in PLMN1 to access the services provided by a NF in PLMN2. This key issue proposes to study how current access token mechanism can be applied for SNPN when a NF consumer in a SNPN access the NF producer belonging to another SNPN/PLMN.

NOTE: Existing service authorization mechanism for PLMN roaming architecture are re-used as much as possible.

### 5.5.2 Security threats

Without authorization in place for the roaming scenario, an unauthorized NF consumer in a SNPN can access an NF producer in another SNPN/PLMN.

### 5.5.3 Potential security requirements

Service authorization shall be supported for the roaming architecture between SNPN and SNPN/PLMN.

# 6 Solutions

## 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 | 5 |
| Solution #1: Primary authentication between an SNPN and third-party AAA server using EAP | X |  |  |  |  |
| Solution #2: EAP authentication between UE and external AAA via AUSF | X |  |  |  |  |
| Solution #3: Primary authentication between an SNPN and third-party AAA server using EAP-TTLS | X |  |  |  |  |
| Solution #4: Authentication Framework Enhancements to support SNPN access | X |  |  |  |  |
| Solution #5: Network Access Authentication with Credentials owned by an AAA external to the SNPN | X |  |  |  |  |
| Solution #6: Network access authentication with credentials owned by an entity separate from the SNPN | X |  |  |  |  |
| Solution #7: EAP authentication between UE and external AAA with enhanced security of KAUSF | X |  |  |  |  |
| Solution #8: UE onboarding for SNPN with AAA-S as DCS |  |  |  | X |  |
| Solution #9: UE onboarding for SNPN with UDM as DCS |  |  |  | X |  |
| Solution #10: Secure initial access to an SNPN onboarding network |  |  |  | X |  |
| Solution #11: Securing initial access by using primary authentication |  |  |  | X |  |
| Solution #12: Authentication for UE Onboarding for SNPN |  |  |  | X |  |
| Solution #13: UE Onboarding for an SNPN from Onboarding SNPN with Secondary Authentication using EAP method with UE identity privacy |  |  |  | X |  |
| Solution #14: Initial access for UE Onboarding for an SNPN from Onboarding SNPN using primary and secondary authentication |  |  |  | X |  |
| Solution #15: Privacy protection of UE onboarding identifier |  |  |  | X |  |
| Solution #16: UE onboarding for SNPN with the interaction between PS and DCS |  | X |  | X |  |
| Solution #17: Solution to Provisioning of PNI-NPN Credentials |  | X |  |  |  |
| Solution #18: Solution on service authorization for SNPNs |  |  |  |  | X |
| Solution #19: Secure onboarding without client authentication |  |  |  | X |  |
| Solution #20: Control plane based provisioning: PS to AUSF |  | X |  |  |  |
| Solution #21: Control plane based provisioning: PS to UDM |  | X |  |  |  |
| Solution #22: Solution for onboarding and provisioning |  | X |  | X |  |
| Solution #23: Solution to enable onboarding and secured UE access based on credentials owned by an external entity |  |  |  | X |  |
| Solution #24: Secure mutually authenticated onboarding without DCS |  |  |  | X |  |
| Solution #25: UE Onboarding for an SNPN with EAP-TLS |  |  |  | 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

#### 6.1.2.0 General

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 SUCI based on the 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 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 SUCI from CdP-UE ID, it is assumed that the CdP-UE ID 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].

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 as the KAUSF. The AUSF also derives KSEAF from the KAUSF as defined in Annex A.6 of 33.501 [2].

NOTE 2: If other input, not known to the external AAA is to be used for input when deriving the KAUSF from MSK is not addressed in the present document.

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.

NOTE 3: Whether the UE instead of the above can be pre-configured with the information which key derivation to use is not addressed in the present document.

### 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

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 needs to 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



Figure 6.2.2-1

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 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 "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.

NOTE 1: Whether such a SUCI calculation using non null scheme is needed at the UE is not addressed in the present document. The details on SUCI calculations, if needed, are not addressed in the present document.

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 over which 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 derives 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 TS 33.501.

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

NOTE 2: The architectural relationship between AUSF and \*-AAA including the derivation of keys is not addressed in the present document. 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 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

NOTE: The evaluation of the solution is not addressed in the present document.

## 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

#### 6.3.2.0 General

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: 6.3.2.1-1: 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].

NOTE 2: User privacy for key generating EAP methods not covered by current procedures in TS 33.501 [2] is not addressed in the present document.

2. The AMF/SEAF 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]. The AUSF starts EAP-TTLS by sending to the AMF/SEAF a Nausf\_UEAuthentication\_Authenticate Response message containing an EAP-Request message of EAP-type=EAP-TTLS with the Start (S) bit set, denoted as EAP-Request [EAP-TTLS, Start=1].

7. The AMF/SEAF forwards to the UE the EAP-Request [EAP-TTLS, Start=1] in the Authentication Request message, including the ngKSI and the ABBA parameters.

8. The UE replies to the AMF/SEAF an Authentication Response message containing an EAP-Response [EAP-TTLS] message whose data field encapsulates a TLS ClientHello message, denoted as EAP-Response [EAP-TTLS, ClientHello].

9. The AMF/SEAF forwards to the AUSF the EAP-Response [EAP-TTLS, ClientHello] message in a Nausf\_UEAuthentication\_Authenticate Request message.

10. The AUSF replies to the AMF/SEAF with EAP-Request [EAP-TTLS] message whose data field encapsulates a TLS ServerHello message, a TLS ServerCertificate message, a TLS ServerKeyExchange message, an optional CertificateRequest message, and a TLS ServerHelloDone message. Such EAP-Request message, denoted as EAP-Request [EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, CertificateReuest\*, ServerHelloDone], is encapsulated in a Nausf\_UEAuthentication\_Authenticate Response message.

11. The AMF/SEAF forwards to the UE the EAP-Request [EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, CertificateReuest\*, ServerHelloDone] message in an Authentication Request message, including the ngKSI and the ABBA parameters.

12. The UE authenticates the AUSF by validating the server certificate included in the EAP-Request message received in step 11. The UE needs to be provisioned with certificates of a trust anchor to validate the AUSF server certificate.

13. If the TLS server authentication is successful, then the UE replies to the AMF/SEAF with EAP-Response [EAP-TTLS] in an Authentication Response message. The data field of the EAP-Response [EAP-TTLS] message contains a ClientCertificate message if a CertifiateRequest messages was received in step 11, a TLS ClientKeyExchange message, an optional CertificateVerify message, a TLS ChangeCipherSpec message, and a TLS Finished message. This EAP-Response message is denoted as EAP-Response [EAP-TTLS, ClientCertificate\*, ClientKeyExchange, CertifiateVerify\*, ChangeCipherSpec, Finished].

14. The AMF/SEAF forwards to the AUSF the EAP-Response [EAP-TTLS, ClientKeyExchange, ChangeCipherSpec, Finished] message in a Nausf\_UEAuthentication\_Authenticate Request message.

15a. The AUSF verifies the client certificate if received in step 14.

15b. The AUSF sends to the AMF/SEAF an EAP-Request [EAP-TTLS] message with its data field encapsulating a TLS ChangeCipherSpec message and a TLS Finished message. This EAP-Request message, denoted as EAP-Request [EAP-TLS, ChangeCipherSpec Finished], is encapsulated in a Nausf\_UEAuthentication\_Authenticate Response message.

16. The AMF/SEAF forwards to the UE EAP-Request [EAP-TLS, ChangeCipherSpec Finished] message in an Authentication Request message, including the ngKSI and the ABBA parameters. By this point, the UE and the AUSF have successfully established a TLS tunnel to protect EAP-TTLS phase 2, as well as keying materials to be used to derive the MSK and EMSK.17. The UE runs EAP-TTLS phase 2 towards the AAA-H as specified in RFC 5281 [5].

18. After successful authentication, an EMSK is established from the keying materials obtained in step 16. 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 TS 33.501 [2].

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

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

21. Upon receiving the EAP-Success message, the UE derives an EMSK from the keying materials obtained in step 16. The UE further derives the KAUSF and the KSEAF according to 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 needs to be run.

**AUSF**

AUSF needs to support EAP-TTLS

**AAA-S**

None

### 6.3.4 Evaluation

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.

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 KAUSF/MSK instead of KAUSF/EMSK. This is achieved based on UE configuration (e.g., as part of provisioning the UE with the credentials necessary for performing the EAP authentication with the legacy AAA server), i.e. the EAP layer of the UE is configured to derive the KAUSF from the MSK instead of deriving it from the EMSK. The UE then derives KSEAF from the KAUSF as already defined in TS 33.501.

This solution assumes that the EAP layer of the UE has access to the credentials used for EAP authentication as well as the configuration information indicating the use of MSK for KAUSF derivation when legacy AAA server is used.

If the credentials owned by an external entity are stored in the USIM, this solution impacts the USIM.

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

The evaluation of the solution is not addressed in the present document.

## 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. The UE ID can be SUCI. For construction of the SUCI, existing methods in TS 33.501 [2] can be used.

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. The EAP messages are exchanged within multiple Authentication Request/Response messages. The Authentication Request message includes ABBA. The ABBA parameter is set to '1' if the SEAF receives the indicator that MSK is used to derive KAUSF from the AUSF. The AUSF sends an indicator if the AUSF finds PAF to do authentication. Upon receiving the ABBA which is set to '1', the NAS layer in the UE sends a notification to the EAP layer so that the EAP layer will return MSK to the NAS layer later, not EMSK.

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 EAP layer in the UE derives MSK and EMSK and returns MSK to the NAS layer if the EAP layer receives the notification in step 5. Besides, the NAS layer 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.

### 6.5.3 System impact

The UE, AMF, AUSF and UDM are impacted.

If it is agreed to have an unique network entity, PAF may be introduced.

The AAA-S has no impact.

### 6.5.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 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 subscription credentials are owned by the AAA-Server and not by the SNPN, the SNPN might have a default subscription profile specifying NSSAIs, QoS etc., but it is lacking the authentication information. The AUSF is taking the role of a AAA proxy towards the AAA server of the service provider holding the credentials. The AAA-Server is holding the subscription of the UE and keeps the credentials as any AAA-Server as well as it is taking the role of the EAP Server for authenticating the UE. 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 NAI of the UE at the service provider with username@realm is then used in the SNPN as SUPI, the SNPN does not have a private key of the service provider to perform any SUCI deconcealment.

### 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.

NOTE 1: In this solution the SBI-DIAMETER interworking functionality is collocated with the AUSF.

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. After successful authentication, the AAA-Server derives MSK.

The UE derives the same keys accordingly.

The AAA-Server may select the stored Routing ID (preconfigured) 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.

5. The AAA-Server sends the result of the authentication back in an authentication response to the AUSF and may include the MSK, validity time, Routing ID, result of the authentication 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.

6. 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.

NOTE 2: If there are multiple subscription profiles per realm, the UDM needs to be preconfigured with the NAIs of the UEs and the mapping to the corresponding subscription profiles.

The AUSF derives KAUSF from MSK and the KSEAF from the KAUSF according to TS 33.501.

7. 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.

8. 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.

9. The rest of the Registration procedure is performed.

### 6.6.3 System impact

If there are multiple subscription profiles per realm, the UDM needs to be preconfigured with the NAIs of the UEs and the mapping to the corresponding subscription profiles.

The SBI-DIAMETER interworking functionality is collocated with the AUSF. The AUSF receives the MSK from the AAA-Server.

### 6.6.4 Evaluation

Subscription is owned by the AAA-Server, i.e. SUPI and authentication credentials.

The AAA-Server does not need to provide a private key to the UDM for SUCI deconcealment.

## 6.7 Solution #7: EAP authentication between UE and external AAA with enhanced security of KAUSF

### 6.7.1 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).

It proposes a number of options to enhance the security of KAUSF, which may otherwise be derived solely from MSK received from an external AAA over interfaces outside the control of SNPN.

### 6.7.2 Solution details



Figure 6.7.2-1: Derive KAUSF from MSK and RAND



Figure 6.7.2-2: Derive KAUSF from a new key exchange



Figure 6.7.2-3: Derive KAUSF from a new EAP authentication

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" is 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 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 "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.

NOTE 1: Whether such a SUCI calculation using non null scheme is needed at the UE is not addressed in the present document. The details on SUCI calculation, if needed, are not addressed in the present document.

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 over which 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 sends an Access Accept messages to the AAA-P, including EAP Success, SUPI, and MSK.

Note that SUPI is needed since the SUPI received by AUSF in step 5 may be anonymous.

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

11-12. The AUSF performs additional steps to generate new keying materials to derive KAUSF.

In option 1 (see Figure 6.7.2-2), the AUSF generates some random data (namely RAND) and derive the KAUSF from both the RAND and the MSK.

In option 2 (see Figure 6.Y.2.2), a new key exchange (e.g., Diffie-Hellman) is executed between the AUSF and the UE to derive new key materials to be used for deriving KAUSF. The MSK received from the AAA-E can be used to authenticate the key exchange.

In option 3 (see Figure 6.7.2.2), a new EAP authentication is executed between the UE and the AUSF based on the MSK. For example, an EAP-TLS with PSK (preshared key) can be executed to derive a new MSK and a new EMSK. KAUSF is derived from the new EMSK.

13. The AUSF sends to the SEAF an EAP-Success message along with the SUPI and the KSEAF in a Nausf\_UEAuthentication\_Authenticate Response message. In option 1, the RAND is also included.

14. The SEAF forwards to the UE the EAP-Success message in an Authentication Result message or a Security Mode Command message, including ngKSI and ABBA. In option 1, the RAND is also included.

15. Upon receiving the EAP-Success message, the UE derives the KAUSF accordingly based on one of the three options in use.

### 6.7.3 System impact

This solution has impact on UE, AUSF, and UDM.

When UDM receives Nudm\_UEAuthentication\_Get\_Request and obtains a SUPI that needs to be authenticated by an external entity, the UDM may not be configured with the authentication method thus may not return an authentication method to the AUSF. 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. In addition, the AUSF needs to perform additional steps to enhance the security of KAUSF.

UE need to support the EAP method chosen by AAA-E for authentication. In addition, UE needs to know how to derive KAUSF and perform additional steps to enhance the security of KAUSF.

### 6.7.4 Evaluation

NOTE: The security benefits from the proposed methods are not addressed in the present document.

The evaluation of the solution is not addressed in the present document.

## 6.8 Solution #8: UE onboarding for SNPN with AAA-S as DCS

### 6.8.1 Introduction

This solution addresses Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN".

The assumption of this solution is that:

1. The UE has been provisioned with default UE credentials;

2. The AAA-S external the onboarding SNPN acts as the DCS.

The architecture of this solution is illustrated as Figure 6.8.1-1.



Figure 6.8.1-1: Architecture of UE onboarding for SNPN with AAA-S acting as DCS

NOTE 1: How to protect provisioning via Control Plane considering trust relationship between Onboarding SNPN and PS owner's domain is not addressed in the present document.

NOTE 2: Function and procedure of interface between AMF and PS, and whether the interface is needed, is not addressed in the present document.

### 6.8.2 Solution details



Figure 6.8.2-1: UE onboarding for SNPN with AAA-S acting as DCS

1. The UE sends a Registration Request message to the AMF, including the SUCI which is the concealment of the SUPI.

2. The AMF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the AMF wishes to initiate an authentication, including the SUCI and the SN-name (serving network name).

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

4. The UDM invokes the SIDF to de-conceal SUCI to gain SUPI.

Based on SUPI, the UDM chooses the authentication method.

5. As the UDM chooses an EAP authentication method, it sends a Nudm\_UEAuthentication\_Get Response message to the AUSF, including the SUPI and the address of the AAA-S.

6. The AUSF sends EAP Request to the AAA-S based on the address received from the UDM, including the SUPI of the UE to be authenticated.

7. The AAA-S and the UE execute the EAP authentication.

8. After the success of the EAP authentication, the AAA-S sends an EAP Response to the AUSF, including the MSK and the SUPI

9. The AUSF derives KAUSF from the MSK, and derives the KSEAF from the KAUSF.

10. The AUSF sends an Nausf\_UEAuthentication\_Authenticate Response message to the AMF, including the EAP success, the KSEAF and the SUPI.

11. The AMF returns the Registration Response to the UE, including EAP success, ngKSI and ABBA. The UE derives KAUSF from the MSK, and derives the KSEAF from the KAUSF in the same way as the AUSF does in step 9.

NOTE: Security implications of UE information pre configuration (e.g., for UE identity, SUCI de-concealment, authentication method selection) in O-SNPN considering trust relationship between Onboarding SNPN, DCS owner's domain and PS owner's domain is not addressed in the present document.

### 6.8.3 System impact

This solution has impact on UE, AUSF and UDM.

The UE derives KAUSF from MSK instead of EMSK.

The AUSF sends EAP Request to the AAA-S based on the address received from the UDM. The AUSF derives KAUSF from MSK instead of EMSK.

The UDM sends the address of the AAA-S to AUSF.

NOTE: Further system impacts are not addressed in the present document.

### 6.8.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 6.9 Solution #9: UE onboarding for SNPN with UDM as DCS

### 6.9.1 Introduction

This solution addresses Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN".

The assumption of this solution is that

1. The UE has been provisioned with default UE credentials;

2. The UDM in the onboarding SNPN acts as the DCS. This does not prevent the UE onboarding from other Onboarding SNPNs, in which case the Onboarding SNPN interacts with UDM to authenticate the UE.

The architecture of this solution is illustrated as Figure 6.9.1-1.



Figure 6.9.1-1: Architecture of UE onboarding for SNPN with UDM acting as DCS

NOTE 1: How to protect provisioning via Control Plane considering trust relationship between Onboarding SNPN and PS owner's domain is not addressed in the present document.

NOTE 2: Function and procedure of interface between AMF and PS, and whether the interface is needed, is not addressed in the present document.

### 6.9.2 Solution details

#### 6.9.2.0 General

In general, in order to gain access to the Provisioning Server (PS), the UE sends a registration request to the onboarding SNPN. The onboarding SNPN retrieves an authentication vector from the DCS, and then authenticate the UE with the authentication vector. After successful authentication, the onboarding SNPN can provide access of the PS to the UE.

#### 6.9.2.1 Procedure



Figure: 6.9.2.1-1: UE onboarding for SNPN with UDM acting as DCS

1. The UE sends a Registration Request message to the AMF, including the SUCI which is the concealment of the SUPI.

2. The AMF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the AMF wishes to initiate an authentication, including the SUCI and the SN-name (serving network name).

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

4. The UDM invokes the SIDF to de-conceal SUCI to gain SUPI.

Based on SUPI, the UDM chooses the authentication method.

5. If the authentication method chosen is 5G AKA, the authentication procedure specified in clause 6.1.3.2 of TS 33.501 [2] is used.

If the authentication method chosen is EAP-AKA', the authentication procedure specified in clause 6.1.3.1 of TS 33.501 [2] is used.

NOTE: Security implications of UE information pre-configuration (e.g., for UE identity, SUCI de-concealment, authentication method selection) in O-SNPN considering trust relationship between Onboarding SNPN, DCS owner's domain and PS owner's domain is not addressed in the present document.

### 6.9.3 System impact

The UDM acts as the DCS to provide default credentials.

NOTE: Further system impacts are not addressed in the present document.

### 6.9.4 Evaluation

The solution assumes that the UE has been provisioned with credentials for mutual authentication with the onboarding SNPN, i.e. it does not satisfy the assumption that the UE has not been provisioned with SNPN credentials for the onboarding SNPN.

NOTE: Further evaluation is not addressed in the present document.

## 6.10 Solution #10: Secure initial access to an SNPN onboarding network

### 6.10.1 Introduction

This solution addresses key issue#4 Securing initial access for UE onboarding between UE and SNPN. The proposed solution relies on the deployment scenario described in Key issue #1 Credentials owned by an external entity where the deployment utilizes an external AAA-S. Therefore, the solution assumes the UE has been preprovisioned with default credentials to be used for primary authentication, the solution uses EAP-TLS as an example.

Note that any solution candidate to Key issue #1 fits the concept of this solution. Using a key generating EAP method allows for derivation of keys to use protecting the air interface and the DCS provides a temporary SUPI to the onboarding network, this solution proposes to use the identifier from the default credentials. This way the UE becomes uniquely identifiable and verifiably secure. Since EAP-TLS credentials does not have storage requirements on USIM, the UE cannot be assumed to have a USIM therefore it might not be possible to have a Home network public key available at the UE, therefore an anonymous SUCI is adopted.

The onboarding network trusts the DCS to perform authentication on its behalf. The solution does not take a stand on how the PS relates to DCS and onboarding network.

### 6.10.2 Solution details



Figure 6.10.2-1: Initial access with key derivation

0. In this solution, the DCS is assumed to be pre-configured with the PS address for each onboarding SUPI. E.g., the owner of the DCS can configure the PS address in the DCS when the UE is sold to or being deployed by the SO.

1. The UE sends a registration request to the onboarding SNPN acting as onboarding network. The UE includes an onboarding indication and an anonymous SUCI as described in clause B 2.1.2.2 of TS 33.501 [2].

NOTE 1: How the UE selects an onboarding network is out of scope of the present document.

2. AMF forwards the registration request to AUSF.

3. The AUSF decides based on the onboarding indication that an external authentication is to be performed and uses the realm part of the SUCI to route the request to the right DCS.

4. The AUSF interacts with the DCS in order to have the DCS perform primary authentication. The AUSF uses a AAA-P/IWF to interact with the DCS.

5. UE and DCS performs primary authentication based on EAP-TLS. Since the SUCI was anonymous in line with clause B 2.1.2.2 of TS 33.501 [2] the tunnel is setup first before certificates are exchanged.

6. The DCS sends an EAP response to the AUSF. Including keying material and a SUPI. In this case the UE ID from the certificate would act as SUPI. The response also includes the PS Address.

7. The AUSF sends a success message to the AMF including keying material, the SUPI and the PS address.

8. The AMF includes an indicator on how the UE derives its keys to the UE in the NAS message carrying the EAP Success.

NOTE 2: This solution proposes an indicator to communicate how the UE derive keys. Whether or not sending the indicator is necessary is in the scope of Key Issue #1 "Credentials owned by an external entity".

9. The UE derives its keys and the registration is complete.

10. The AMF sends the PS address to the UE over the established secure NAS connection. The AMF may also store the PS address for future use, e.g. to send it to the SMF for enabling user plane access limitation towards the PS.

This solution describes initial access of the UE to the onboarding network using authentication with the DCS, and how the ON or UE obtain the PS address. The actual connection between UE and PS is not in scope of this solution.

The DCS and the onboarding network have a business agreement that the DCS provides mutual authentication with UEs for the purpose of initial access to the onboarding network. This implies that there is mutual trust between AUSF and DCS. Security mechanisms for the interface between DCS and onboarding network are out of scope of this solution.

### 6.10.3 System impact

**UE**

Potentially key hierarchy depending on the outcome of KI#1.

**AMF**

Relay of potentially needed indicator for how the UE should derive keys. Relay of onboarding indicator.

**AUSF**

AAA-P functionality in order to communicate with external party.

**AAA-S**

Depends on if KI#1 decides the AAA-S should be 5G aware or not.

### 6.10.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 6.11 Solution #11: Securing initial access by using primary authentication

### 6.11.1 Introduction

This solution addresses key issue #4 (Securing initial access for UE onboarding between UE and SNPN).

This solution describes a high-level framework for securing the initial access over the onboarding network (ON) by using primary authentication. Once the initial access is established, the UE uses this access to communicate with the provisioning server to receive the necessary SNPN credentials. The actual provisioning mechanisms are outside the scope of this solution.

### 6.11.2 Solution details

In this solution, it is assumed that the UE is provisioned with the necessary credentials (including Unique UE Identifier, Default UE credentials) by the Default Credential Server (DCS) so that the primary authentication can be performed between the UE and onboarding network/DCS. The DCS also maintains these credentials so that primary authentication can be performed between the UE and the DCS. The actual method/processes used to configure this information in the UE and the DCS is outside the scope of this solution.

In this solution, the following trust/security relationships are assumed:

- ON trusts the DCS to perform primary authentication of the UE for the initial access.

- DCS has a roaming relationship with the ON for the purposes of initial access and trusts the ON to perform the functions of 5G serving network.

- UE and the PS have a trust relationship that is used to provide end-to-end confidentiality, integrity and reply protection of the SNPN credentials between the UE and the PS. Therefore, no specific trust is assumed between the PS and the ON/DCS for the secure provisioning of the SNPN credentials.

The following call-flow shows the entities and the high-level steps involved in the UE onboarding.



Figure 6.11.2.-1: Securing initial access for UE onboarding by re-using 5GS primary authentication

0) The UE is pre-configured by the DCS with the necessary information (e.g., Unique UE Identifier, Default UE credentials) for the UE to register with an onboarding network (ON). In case AKA based credentials are used, they are stored on the UICC. In case of non-AKA credentials, the storage and handling of these non-AKA credentials within the UE are not in the scope of this solution. The UE is not configured with any SNPN credentials. The DCS also stores the UE's credentials information required for the authentication of the UE.

1) UE discovers and performs onboarding network selection.

2) UE sends the Registration Request to the onboarding network. The request includes the UE identifier. In case of AKA based credentials, UE identifier is set to the SUCI as specified in TS 33.501 [2]. In case of non-AKA based credentials, the UE identifier is in NAI format, in which case UE identifier privacy, if required, is provided by the selected EAP authentication method.

3) Based on the received UE identifier, the ON selects DCS and forwards the authentication request to the DCS.

4) The ON interacts with the DCS in order to perform primary authentication. Based on the UE identifier received from the ON, the DCS selects the authentication method. The authentication method, which can be either AKA-based (5G AKA or EAP-AKA') or non-AKA-based (e.g., EAP-TLS or EAP-TTLS). In case of non-AKA based methods, the selected EAP method is a key-generating EAP method that provides mutual authentication. Once the primary authentication is successful, KAUSF is established as follows: if the DCS is 5GS aware (i.e., the DCS supports 5G key hierarchy), the UE and the DCS end up establishing KAUSF; otherwise (i.e., DCS is a legacy AAA server), the DCS sends the MSK to the ON, which is used to derive the KAUSF between the UE and the ON. The rest of the keys in the 5GS key hierarchy are derived as specified in TS 33.501 [2]. At the end of this step, in case UE subscriber privacy is in force, the DCS also provides the UE's SUPI (i.e., UE permanent identifier) to the ON.

NOTE 1: The DCS and the ON have a business agreement that the DCS provides mutual authentication with UEs for the purpose of initial access to the ON. This implies that there is mutual trust between ON and DCS. Security mechanisms for the interface between DCS and ON are out of scope of this solution.

5) NAS SMC is performed between the UE and the ON, establishing NAS security.

6) After the successful NAS SMC, ON sends Registration Accept to the UE.

7) The UE is now ready to securely access the Provisioning Server. The Provisioning Server discovery is performed as per the conclusions in clause 8.4.1 of TR 23.700-07 [3]. The ON uses the discovered PS address to find the right Provisioning Server. The Provisioning Server securely provisions the SNPN credentials. The provisioning of SNPN credentials may be Control Plane based or User Plane based. The provisioning messages are end-to-end protected between the UE and the PS. In case of control plane based provisioning, the provisioning messages are routed either via the DCS (when the DCS is 5GS aware, e.g., DCS hosts UDM/AUSF) or directly via the ON (when the DCS is non-5GS aware). The actual provisioning method or protocol is outside the scope of this solution.

NOTE 2: Whether the provisioning message is transferred directly via ON or DCS may depend on SLA among different parties (e.g. DCS, ON, PS).

8) Once the provisioning of SNPN credentials is completed, the UE de-registers from the ON.

9) Using the provisioned SNPN credentials, the UE is now ready to register to the SNPN.

### 6.11.3 System impact

Though this solution reuses the existing 5GS security mechanisms specified in TS 33.501 [2], enhancements to 5GS are needed so that the 5GC (as an onboarding network) can interface with the DCS in order to perform primary authentication. The conclusion(s) from Key Issue #1 can be reused for these enhancements such that the DCS is the external entity that hosts the credentials used for primary authentication necessary for the initial access.

### 6.11.4 Evaluation

This solution assumes that there is end-to-end security between the UE and the PS. If there is no end-to-end security between the UE and the PS, the ON may compromise the credentials (e.g. modify, eavesdrop) provisioned by the PS.

## 6.12 Solution #12: Authentication for UE Onboarding for SNPN

### 6.12.1 Introduction

This solution addresses key issue #4.

The authentication architecture is shown in figure 6.12.1-1.

UE

(R)AN

UPF

N2

N4

PS

N1

N3

N6

N12

N13

AMF

SMF

AUSF

UDM

N11

N8

O-SNPN

SO-SNPN

DCS

Nxx

Trusted 3rd party

PAF

TBD

Nxy

**Figure 6.12.1-1: Architecture for authentication for UE onboarding for SNPN**

The authentication related functions in the architecture are:

- Default Credential Server (DCS), stores UE's default credential. The solution assumes that the owner of DCS belongs to 3rd party, who is different from SO. If the SO decides to use DCS to authenticate the UE, there is an agreement between 3rd party and SO, and the SO trusts 3rd party.

- 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.

### 6.12.2 Solution details

#### 6.12.2.1 Authentication for onboarding with default credentials is provisioned in UDM

**UE**

**RAN**

**AMF**

**AUSF**

**UDM**

2. Construct SUCI

8. Primary Authentication

a.Provisioning unique ID and default credential

10. AS SMC

9. NAS SMC

b.Provisioning unique ID, authentication method and default credential

1. Broadcast

(on-boarding information)

3. Registration Request

(SUCI)

4. Nausf\_UEAuthentication\_

Authenticate Request (SUCI)

5. Nudm\_UEAuthentication

\_Get Request (SUCI)

6. Retrieve default credential

7. Nudm\_UEAuthentication\_

Get Response (SUPI, AV,

authentication method)

**O-SNPN**

**SO-SNPN**

Figure 6.12.2-1: Authentication for onboarding with default credentials is provisioned in UDM

Preconditions:

- UE has been provisioned with unique ID, and default credential. In case that the UE is in automatic selection model, the UE may be provisioned with a priority list of O-SNPNs.

- UDM has been provisioned with unique ID, default credential and authentication method at onboarding phase.

Procedures:

1. RAN broadcasts onboarding information. The onboarding information includes indication for onboarding support, and SNPN identity of the O-SNPN and SNPN identity of the connected SO-SNPN.

2. The UE may manually get an SNPN ID of SO-SNPN. The UE may output list of SO-SNPN in the onboarding information in the scream, and the user can select one of an expected SO-SNPN.

The UE may automatically get an SNPN ID of SO-SNPN. The UE may be provisioned with a priority list of O-SNPNs. The UE can select O-SNPN using priority list and O-SNPN in the onboarding information, and get the related SNPN ID of SO-SNPN in the onboarding information.

The UE constructs SUCI using the schemes described in TS 33.501 [2] according to SNPN ID of SO-SNPN and UE's unique ID, in the following manner. The Home Network Identifier is set as SNPN identity of SO-SNPN so that the AMF can select the right AUSF. The Scheme Output is set as unique ID.

3. The UE sends the Registration Request message to the SEAF, containing SUCI.

4. The SEAF sends Nausf\_UEAuthentication\_Authenticate Request message to AUSF. The message includes SUCI.

5. The AUSF sends the Nudm\_UEAuthentication\_Get Request message to UDM. The message includes SUCI.

6. The UDM de-conceals the SUCI to SUPI, and gets the unique ID. The UDM checks whether the unique ID is provisioned, if not, the UDM rejects the registration. If the UDM has been provisioned with the related default credential, the UDM retrieves default credential and authentication method according to unique ID. The UDM may generate AV according to the default credential and authentication method.

7. The UDM sends the SUPI, authentication method and AV to the AUSF in the Nudm\_UEAuthentication\_Get Response.

8. The UE and AUSF perform the authentication procedure. After successful authentication, the UE and SEAF derive KSEAF and KAMF. If the authentication is failed, the UE may re-select the O-SNPN or SO-SNPN as depicted in step 2.

9. The UE and the AMF perform NAS SMC procedure to activate NAS security.

10. The UE and the RAN perform AS SMC procedure to activate AS security.

NOTE: If the SO does not want to continue the use of the default credential in the UDM except for the initial access for onboarding (e.g., default credential received from an external entity), the procedure depicted above can be used to replace the default credential with a different credential.

#### 6.12.2.2 Authentication for onboarding with default credentials is provisioned in DCS

**PAF**

**UE**

**RAN**

**SEAF**

**AUSF**

**UDM**

2. Construct SUCI

a.Provisioning unique ID and default credential

16. AS SMC

15. NAS SMC

b.Provisioning unique ID

1. Broadcast

(on-boarding information)

3. Registration Request

(SUCI)

4. Nausf\_UEAuthentication\_

Authenticate Request (SUCI)

5. Nudm\_UEAuthentication

\_Get Request (SUCI)

6. Cannot retrieve default credential

7. Nudm\_UEAuthentication

\_Get Response (SUPI)

**O-SNPN**

**SO-SNPN**

**DCS**

b.Provisioning unique ID, authentication method and default credential

8. SBI (EAP trigger,

AAA address)

9. AAA (EAP trigger)

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

11. AAA(EAP success, MSK)

12. SBI (MSK,

EAP success)

13. Nausf\_UEAuthentication\_

Authenticate Response (EAP success, Kseaf)

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

**Trusted 3rd party**

Figure 6.12.2-2: Authentication for onboarding with default credentials is provisioned in DCS

Preconditions:

- UE has been provisioned with unique ID, and default credential. In case that the UE is in automatic selection model, the UE may be provisioned with a priority list of O-SNPNs.

- UDM has been provisioned with unique ID at onboarding phase

- DCS has been provisioned with unique ID, authentication method and default credential.

Procedures:

1 - 5. The same steps with step 1-5 in clause 6.12.2.1.

6. The UDM de-conceals the SUCI to SUPI, and gets the unique ID. The UDM checks whether the unique ID is provisioned, if not, the UDM rejects the registration. If the UDM has been provisioned with the unique ID, but has not been provisioned the related default credential, the UDM sends the SUPI, and DCS address derived from SUPI to the AUSF directly.

7. The UDM sends the SUPI and DCS address to AUSF in the Nudm\_UEAuthentication\_Get Response.

8. The AUSF invokes external primary authentication service provided by PAF. The AUSF sends SBI message containing the DCS address and EAP trigger (e.g. EAP-TLS start) message to the PAF.

9. The PAF finds DCS according to the DCS address, translates SBI message to AAA protocol, and sends the EAP trigger message to the DCS.

10. - 14. Since DCS can be regarded as an external AAA, those steps can reuse authentication procedure steps similar with authentication solutions with credentials owned by an external AAA in key issue #1, e.g. solution 1, 3, 4, 5, etc. After successful authentication, the UE and AMF derives the KAMF. If the authentication is failed, the UE may re-select the O-SNPN or SO-SNPN as depicted in step 2.

15. The UE and the AMF perform NAS SMC procedure to activate NAS security.

16. The UE and the RAN perform AS SMC procedure to activate AS security.

### 6.12.3 System impact

In case that authentication for onboarding with default credentials is provisioned in UDM, UE, RAN, UDM may be impacted.

In case that authentication for onboarding with default credentials is provisioned in DCS, UE, RAN, AUSF, PAF (which may be collocated with AUSF), and UDM may be impacted. DCS can be legacy AAA.

### 6.12.4 Evaluation

The solution can address key issue #4.

The solution assumes that there is an N12 interface between O-SNPN and SO-SNPN, so that the SO-SNPN knows that authentication result.

In addition, the UE is mutually authenticated by O-SNPN. The UE has activated both NAS and AS security with O-SNPN, the UE can establish a secure 3GPP connection (e.g. PDU session) via UP. The drawback is that the UE needs to be provisioned with information about the subscription owner before or at onboarding. Either a list of possible O-SNPNs is known before onboarding, or the UE has a screen and the user selects the SO-SNPN. These conditions will not be always be met in deployments where devices without screen are to be onboarded zero-touch at any vertical network, including those deployed after the manufacturing of the device.

## 6.13 Solution #13: UE Onboarding for an SNPN from Onboarding SNPN with Secondary Authentication using EAP method with UE identity privacy

### 6.13.1 Introduction

This solution addresses key issue 4," Securing initial access for UE onboarding between UE and SNPN," for UEs without UICC and figure 6.13.2-1 shows a general use-case for this key issue. The actual provisioning mechanisms are outside the scope of this solution. In this solution, UE performs primary authentication using null algorithms, while an EAP method guarantying user identity privacy (e.g. EAP-TTLS, EAP-TLS v.1.3 or EAP-TLS v 1.2 with privacy option) is mandated for mutual authentication with DCS as part of secondary authentication.

When the UEs are deployed without a provisioned subscription, it provides a solution on how UE subscription/credentials are afterward provisioned to the UEs. The solution enables UEs to get network connectivity to an O-SNPN ("onboarding SNPN") so that it can be provisioned with necessary subscription credentials and configuration for the SO-SNPN that will own the UE's subscription ("SNPN owning the subscription"). The solution removes the complexity of O-SNPN by avoiding the need for any new Control plane interfaces, the connectivity between the O-SNPN and DCS relying on the existing interface for secondary authentication..

### 6.13.2 Solution details

Following pre-conditions are assumed:

- The UE is provisioned with some default UE credentials and a unique UE identifier at the manufacturing time. The unique UE identifier is assumed to be unique within the DCS. It takes the form of a Network Access Identifier (NAI), which is composed of the user part and the realm part, which may identify the domain name of the DCS.

- The UE is not provisioned with *subscription credentials* that grant access to a SO-SNPN.

- The Onboarding SNPN (O-SNPN) that is used by the UE in the onboarding process is not necessarily the same as the SO-SNPN (Subscription Owner SNPN) for which subscription credentials will be provisioned in the UE.

- The O-SNPN operator has access to a Default Credential Server (DCS), which is used to verify that UE is subject to onboarding based on the UE identifier and the associated default UE credentials. The DCS is used for UE authentication/authorization in the O-SNPN during the establishment of a PDU Session for onboarding purposes. The DCS owner is out of the present document's scope and can be inside or outside of the O-SNPN, e.g., DCS can be owned by the device manufacturer, by an SNPN other than the O-SNPN, or by a 3rd party.

The solution recommends using an EAP method guaranteeing user identity privacy (e.g. EAP-TTLS, EAP-TLS v.1.3 or EAP-TLS v 1.2 with privacy option) as an authentication mechanism for secondary authentication to O-SNPN.

NOTE 1: Provisioning is out of scope of this solution.

In some deployments, the DCS and the Provisioning Server can be the same entity. In deployments where the DCS and the Provisioning Server are different entities, it is expected that they communicate with each other for the purpose of UE authentication based on the default UE credentials via an interface that is outside of this solution's scope. The SO-SNPN owning the subscription (SO-SNPN) interacts with the Provisioning Server during the UE onboarding procedure and provides the corresponding UE's subscription credentials and UE's configuration data to be provisioned to the UE. The actual provisioning mechanisms are outside the scope of this solution.



Figure 6.13.2-1: UE Onboarding for Remote Provisioning Procedure

0. UE pre-configuration: The UE is provisioned with default UE credentials that allow for successful UE authentication with DCS and a unique UE identifier. A configuration may also include information for selecting SNPN needed to access the provisioning server.

1. Initial access to the Onboarding SNPN:

a. Selection of SNPN: UE selects the O-SNPN based on the indication in SIB broadcasted by O-SNPN (e.g., "Support for onboarding" indicator). In this step, if the UE wants to initiate the UE onboarding, the UE either automatically discovers and selects the O-SNPN network based on the broadcasted information or presents a list of available ONs to the user for manual selection. The UE registers to O-SNPN for onboarding by including an indication in the Registration Request, indicating that the registration is for UE onboarding.

b. Registration Procedure: During the registration procedure, the UE provides the UE-specific information, e.g. corresponding identity (encoded in SUPI format) to the network. The user may also provide the UE with additional information, such as an application identifier and/or Service Provider Identifier. NAS SMC is performed using NULL algorithms.

NOTE 2: Primary Authentication is not performed in this solution.

NOTE 3: Clarification of whether and how SUPI concealment can be used during the registration procedure is not addressed in the present document.

2. Configuration PDU session: UE obtains limited connectivity to the Provisioning Server. In the Configuration PDU Session Establishment Request, the UE includes DCS identity and optionally includes PS identity, SO-SNPN identity, or both. When the UE provides SO-SNPN identity, the SMF in the O-SNPN may decide to override the PS identity provided by the UE and send the new PS identity to the UE in the PDU Session Establishment Accept as PCO parameter. The PS identity received in the PDU Session Establishment Accept overrides any configured PS identity in the UE.

NOTE 4: How to address the following attack is not addressed in the present document: if it lacks NAS security protection, PS identity can be modified of some attack, e.g. MITM attack, which could cause the DoS attack.

NOTE 5: Call flow in figure needs correction to map steps described in solution.

3. The PDU session establishment authentication/authorization is performed as described in TS 23.502 [6] clause 4.3.2.3 and in TS 33.501[2] clause 11.1.2. Secondary authentication with DCS is triggered by the SMF during PDU Session establishment.

4. The SMF selects the DCS either based on the DCS identity sent from the UE to the SMF or based on the realm part of the UE identity.. As secondary authentication is EAP-based, any EAP method can be used for secondary authentication to DCS. In this case any EAP method guaranteeing user identity privacy (e.g. EAP-TTLS, EAP-TLS v.1.3 or EAP-TLS v 1.2 with privacy option) can be used to provide privacy of the UE identity. Specifically when EAP-TTLS is used, to provide privacy of the UE identity, as per the RFC 5281, "anonymous@realm", is sent during the phase 1 of TTLS. In the second phase of EAP-TTLS, UE is authenticated by DCS using unique UE identity and default UE credentials as per RFC 5281[5].

5. The UE discovers the Provisioning Server using the stored PS identity. At this point, the stored PS identity is either the PS identity pre-configured in the UE, or the PS identity entered manually by the user, or the PS identity received by the O-SNPN. If the UE still does not have a stored PS identity, then the UE uses a well-known FQDN to perform PS discovery. The UE provides the provisioning server with the unique UE identifier, and optionally with the identity of the selected SO-SNPN. The provisioning server discovers the DCS identity sent from the UE to PS or based on using the realm part of the unique UE identity and authenticates the UE based on the default UE credentials. The interface between DCS and PS is out of the scope of this solution.

NOTE 6: This solution assumes there is trust relationship between DCS and PS. Specifics of the interface between DCS and PS including the aspects of mutual authentication, encryption and integrity protection are out of the scope of this solution.

NOTE 7: When the Onboarding network is the same as SNPN owning the subscription of the UE, the Provisioning Server is owned by the Onboarding Network

6. The Provisioning Server interacts with UE over secure connection.

7. Upon successful provisioning in the previous step, the UE releases the Configuration PDU Session and deregisters from the O-SNPN.

8. Upon a successful de-registration, the UE initiates a regular procedure, including a selection of a SO-SNPN, Registration using the provisioned credentials with the SO-SNPN owning the subscription, and PDU Session establishment(s). Depending on the provisioned subscription credentials, the UE may select an SNPN that is the same or different from the SNPN owning the credentials.

### 6.13.3 System impact

UE:

- During the registration procedure, UE provides information to the SNPN, indicating that the registration is for restricted onboarding service only.

- Support for an EAP method guaranteeing user identity privacy (e.g. EAP-TTLS, EAP-TLS v.1.3 or EAP-TLS v 1.2 with privacy option)

- the UE might have been provisioned with some initial default configuration, including PLMN ID and NID of the SNPN, S-NSSAI, DNN needed to access the provisioning server.

NG-RAN:

- A new indication in SIB to indicate that the SNPN provides access to onboarding service.

5GC:

- SMF to provide Limited connectivity to the provisioning server.

### 6.13.4 Evaluation

NOTE: Evaluation for the security and architectural implications of using EAP-TTLS is not addressed in the present document.

The evaluation of the solution is not addressed in the present document.

## 6.14 Solution #14: Initial access for UE Onboarding for an SNPN from Onboarding SNPN using primary and secondary authentication

### 6.14.1 Introduction

This solution addresses key issue 4," Securing initial access for UE onboarding between UE and SNPN," for devices without UICC and figure 6.Y.1-1 shows a general use-case for this key issue. The actual provisioning mechanisms are outside the scope of this solution. In this solution, UE authenticates network using one-way authentication as part of authentication procedure and performs mutual authentication with DCS using any EAP method as part of secondary authentication.

When the UEs are deployed without a provisioned subscription, it provides a solution on how UE subscription/credentials are afterward provisioned to the UEs. The solution enables UEs to get network connectivity to an O-SNPN ("onboarding SNPN") so that it can be provisioned with necessary subscription credentials and configuration for the SO-SNPN that will own the UE's subscription ("SNPN owning the subscription"). The solution removes the complexity of O-SNPN by avoiding the need for any new Control plane interfaces, the connectivity between the O-SNPN and DCS relying on the existing interface for secondary authentication.



Figure 6.14.1-1: UE onboarding in non-public network

### 6.14.2 Solution details

#### 6.14.2.0 General

Following pre-conditions are assumed:

- The UE is provisioned with some default UE credentials and a unique UE identifier at the manufacturing time. The unique UE identifier is assumed to be unique within the DCS. It takes the form of a Network Access Identifier (NAI), which is composed of the user part and the realm part, which may identify the domain name of the DCS. UE is provisioned with set of roots of trust certificate information that UE will use to authenticate O-SNPN during the authentication.

- The UE is not provisioned with *subscription credentials* that grant access to a SO-SNPN.

- The Onboarding SNPN (O-SNPN) that is used by the UE in the onboarding process is not necessarily the same as the SO-SNPN (Subscription Owner SNPN) for which subscription credentials will be provisioned in the UE.

- The O-SNPN operator has access to a Default Credential Server (DCS), which is used to verify that UE is subject to onboarding based on the UE identifier and the associated default UE credentials. The DCS is used for UE authentication/authorization in the O-SNPN during the establishment of a PDU Session for onboarding purposes. The DCS owner is out of the present document's scope and can be inside or outside of the O-SNPN, e.g., DCS can be owned by the device manufacturer, by an SNPN other than the O-SNPN, or by a 3rd party.

In some deployments, the DCS and the Provisioning Server can be the same entity. In deployments where the DCS and the Provisioning Server are different entities, it is expected that they communicate with each other for the purpose of UE authentication based on the default UE credentials via an interface that is outside of this solution's scope.

NOTE 1: Provisioning is out of scope of this solution.

The SO-SNPN owning the subscription (SO-SNPN) interacts with the Provisioning Server during the UE onboarding procedure and provides the corresponding UE's subscription credentials and UE's configuration data to be provisioned to the UE. The actual provisioning mechanisms are outside the scope of this solution.



Figure 6.14.2.0-1: UE Onboarding for Remote Provisioning Procedure

0. UE pre-configuration: The UE is provisioned with default UE credentials that allow for successful UE authentication and a unique UE identifier. A configuration may also include information for selecting SNPN needed to access the provisioning server.

1. Initial access to the Onboarding SNPN:

a. Selection of SNPN: UE selects the O-SNPN based on the indication in SIB broadcasted by O-SNPN (e.g., "Support for onboarding" indicator). In this step, if the UE wants to initiate the UE onboarding, the UE either automatically discovers and selects the O-SNPN network based on the broadcasted information or presents a list of available ONs to the user for manual selection. The UE registers to O-SNPN for onboarding by including an indication in the Registration Request, indicating that the registration is for UE onboarding.

b. Registration Procedure: During the registration procedure, the UE provides the UE-specific information, e.g. corresponding identity (encoded in SUPI format) to the network. The user may also provide the UE with additional information, such as an application identifier and/or Service Provider Identifier. An authentication using non-AKA (e.g. EAP-TLS) based method is performed. The SUPI is of the type of NAI in the form of username@realm. The "username" is either "anonymous" or UE identity can be omitted if the subscriber identifier privacy is required by SNPN. The UE performs the one-way authentication of O-SNPN based on O-SNPN's certificate.

2. Configuration PDU session: UE obtains limited connectivity to the Provisioning Server. In the Configuration PDU Session Establishment Request, the UE includes DCS identity and optionally includes PS identity, SO-SNPN identity, or both. When the UE provides SO-SNPN identity, the SMF in the O-SNPN may decide to override the PS identity provided by the UE and send the new PS identity to the UE in the PDU Session Establishment Accept as PCO parameter. The PS identity received in the PDU Session Establishment Accept overrides any configured PS identity in the device. It is assumed that one and only one Configuration PDU session can be established, and connectivity of this PDU session is limited (cf. RLOS), so that the UE can only access a Provisioning Server.

3. The PDU session establishment authentication/authorization is performed as described in TS 23.502 [6] clause 4.3.2.3 and in TS 33.501 [2] clause 11.1.2. Secondary authentication is triggered with the DCS by the SMF during PDU Session establishment. The SMF selects the DCS either based on the DCS identity sent from the UE to the SMF or based on the realm part of the UE identity. It is required that the secondary authentication performed between the UE and the DCS is an EAP authentication that supports mutual authentication

NOTE 2: Clarification of, if the O-SNPN can perform mutual EAP authentication with DCS as part of secondary authentication, why such a EAP authentication cannot be performed as part of primary authentication in step 1 is not addressed in the present document.

4. The UE discovers the Provisioning Server using the stored PS identity. At this point, the stored PS identity is either the PS identity pre-configured in the UE, or the PS identity entered manually by the user, or the PS identity received by the O-SNPN. If the UE still does not have a stored PS identity, then the UE uses a well-known FQDN to perform PS discovery. The UE provides the provisioning server with the unique UE identifier, optionally the identity of the selected SO-SNPN. The provisioning server discovers the DCS using DCS identity sent from the UE to PS or based on the realm part of the unique UE identity and authenticates the UE and make a secure connection for provisioning with the UE, based on the default UE credentials. Interface between DCS and PS is out of the scope of this solution.

NOTE 3: This solution assumes there is trust relationship between DCS and PS. Specifics of the interface between DCS and PS including the aspects of mutual authentication, encryption and integrity protection are out of the scope of this solution.

NOTE 4: When the Onboarding network is the same as SNPN owning the subscription of the UE, the Provisioning Server is owned by the Onboarding Network.

5. Upon successful provisioning, the UE releases the Configuration PDU Session and deregisters from the O-SNPN.

6. Upon a successful de-registration, the UE initiates a regular procedure, including a selection of a SO-SNPN, Registration using the provisioned credentials with the SO-SNPN owning the subscription, and PDU Session establishment(s). Depending on the provisioned subscription credentials, the UE may select an SNPN that is the same or different from the SNPN owning the credentials.

#### 6.14.2.1 Using EAP-TLS Authentication Procedures over 5G Networks for initial one-way authentication

Figure 6.14.2.1-1 below shows the EAP-TLS Authentication Procedures over 5G Networks as described in TS 33.501 Annex B.2.1; the difference with respect to the EAP-TLS authentication procedure for one-way authentication is highlighted and described below.



Figure 6.14.2.1-1: Using EAP-TLS Authentication Procedures over 5G Networks for initial one-way authentication

Step 1: When the UE sends a registration request with Registration Type as Onboarding, the UE sends an anonymous SUCI described in clause B 2.1.2.2 of TS 33.501 [2].

Step 2: The AMF (SEAF) selects an AUSF and sends the Nausf\_UEAuthentication\_Authenticate Request message to the AUSF, including information to assist the AUSF in selecting the EAP-TLS authentication method for one-way authentication.

NOTE 1: The information to assist the AUSF in selecting EAP-TLS for one-way authentication can be sent as an explicit parameter or can be encoded inside the realm part of the SUCI. Alternatively, the AMF (SEAF) can use a dedicated AUSF for onboarding.

Steps 3, 4, 5: are not required as the AUSF determines the authentication method.

It is required that the secondary authentication performed between the UE and the DCS is an EAP authentication that supports mutual authentication

Steps 6, 7, 8, 9: Same procedure as described in TS 33.501[2] Annex B.2.1.

Steps 10-11: The AUSF replies to the SEAF with EAP-Request/EAP-TLS in the Nausf\_UEAuthentication\_Authenticate Response, which may include a chain of TLS certificates leading to root of trust certificate authority.

Step 12: The UE authenticates the server with the received message from step 8.

NOTE 2: The underlying assumption is that the device is configured with a set of root-of-trust certificates at manufacturing time.

NOTE 3: If the AUSF has a certificate issued by a root-of-trust authority, it includes a single certificate in step 10. Otherwise, the AUSF includes a chain of certificates that leads to the root-of-trust authority.

NOTE 4: O-SNPN prepares a Certificate Signing Request (CSR) and submits it to the CA of their choice (trusted by business agreement) [7]. A CSR carries the list of hosts that should appear in the certificate, along with a public key and proof of possession of the corresponding private key (via a digital signature). CA then validates subscriber's identity (O-SNPN) using different procedures as per business agreement.

Extended Validation (EV) certificates [7] can be used to provide certificates to ON by subordinate CA's or CA's. EV Certificates cannot be obtained by individuals or rogue entities, or non-incorporated entities. When fraudulent certificate requests are submitted, CAs tend to maintain a list of domain names and refuse to issue certificates for them without manual confirmation. EV certificates can be used to provide certificates to ON by subordinate CA's or CA's.

To further ascertain the security of one-way authentication, O-SNPN with a business relationship with Intermediate CA and Registration Authority can use the following certificate extensions as per [7]. Signed Certificate Timestamps (SCT), Extended Key usage, and named constraint can also be used together for intermediate certificates to avoid arbitrary public certificates for fraudulent O-SNPN and provide a reliable authentication/verification mechanism of server certificates' one-way authentication.

To verify the TLS handshake integrity, the server sends cryptographic signatures of the exchanged data. The handshake proceeds only if the signatures can be verified. Any other result would imply a modification of the network traffic by a third party.

Steps 13-14: If the TLS server authentication is successful, the UE replies with EAP-Response/EAP-TLS in the Authentication Response message. The response message does not include the TLS Certificate, and TLS\_certificate\_verify message as the network authentication of the UE is not required.

With one-way authentication where only the UE authenticates the onboarding network, the key material for AS and NAS security is generated following the same procedure as described in TS 33.501[2] Annex B.2.1.

### 6.14.3 System impact

UE:

- During the registration procedure, UE provides information to the SNPN, indicating that the registration is for restricted onboarding service only.

- the UE might have been provisioned with some initial default configuration, including PLMN ID and NID of the SNPN, S-NSSAI, DNN needed to access the provisioning server.

NG-RAN:

- A new indication in SIB to indicate that the SNPN provides access to onboarding service.

5GC:

- SMF to provide Limited connectivity to the provisioning server

- AMF to handle Registration procedure for onboarding

- AUSF to handle one-way authentication

### 6.14.4 Evaluation

A rogue network pretending to be an O-SNPN will need to assert a valid identity via a digital certificate as part of the one-way authentication.

In the absence of client authentication, it may be possible that a malicious entity can perform a MITM attack by relaying secondary authentication to a legitimate UE and thus register to the O-SNPN. This could cause issues both for security and for charging of the O-SNPN

During the Registration procedure, UE authenticates the network with one-way primary authentication of O-SNPN using an appropriate EAP method, e.g., EAP-TLS. The mutual authentication required between DCS and UE is provided as part of the secondary authentication.

All key hierarchy and derivation remain the same as defined in 33.501 [2].

Mutual authentication between DCS and UE is provided via secondary authentication. UE is allowed to set up a PDU session but with only limited connectivity. To mitigate any security issues, the AUSF, SMF, and UPF can be isolated on a distinct network slice dedicated to UE onboarding.

This solution does not provide mutual authentication between the UE and the O-SNPN.

NOTE: Further evaluation is not addressed in the present document.

## 6.15 Solution #15: Privacy protection of UE onboarding identifier

### 6.15.1 Introduction

This solution addresses key issue#4 Securing initial access for UE onboarding between UE and SNPN. The solution aims to address the potential privacy issue introduced by sharing the onboarding SUPI in plaintext. Privacy concerns are strongly related to the trustworthiness of the networks and therefore also the thrust model – who trusts who.

It assumed that the UE and DCS can trust the Onboarding network. This implies that the onboarding network has performed mutual authentication between the entity connected to the DCS and the DCS. Therefore, it implies by the transitive property that the UE can trust the onboarding network. The trust relation is a fundamental property and therefore cases where this is not achieved is out of scope for this solution.

In the next clause, the details of the solution are explained.

### 6.15.2 Solution details

Figure 6.15.2-1 shows a generalisation of the solution. The solution assumes, the AUSF and DCS has proven the mutual trust. The prove of mutual trust can be achieved by, but not limited to, authentication mechanism, authorisations schemes, token schemes, certification etc. The trust between DCS and AUSF can also be achieved by business agreements and other out of band solutions. This is not part of the figure.

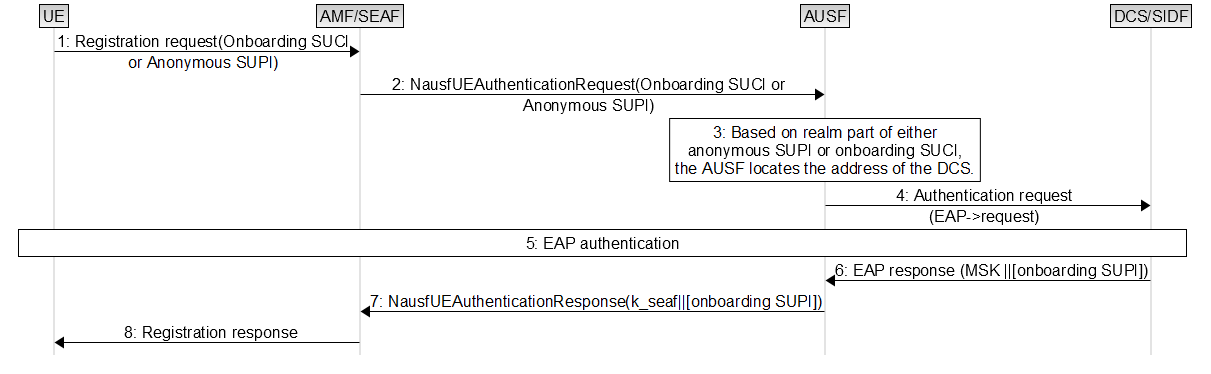


Figure 6.15.2-1: initial access and sharing of identity.

1. The UE sends a registration request to the onboarding network. The request contains either the onboarding SUCI or anonymous SUPI. At this point, the UE are not aware whether the onboarding network can be trusted and therefore the onboarding SUPI can only be shared anonymous or concealed.

2. AMF/SEAF forwards the registration request to the AUSF.

3. Based on either the realm of the anonymous SUPI or onboarding SUCI the AUSF identifies the address path of the DCS.

4. The AUSF initiates the authentication by sending an EAP message to the DCS.

5. The authentication might cover multiple messages including requesting the identity. Different EAP protocols have different termination points of the security channel, like TLS and TTLS.

6. Depending on the authentication result, the DCS will return the MSK (assuming TLS) and onboarding SUPI.

7. If the EAP result contains the onboarding SUPI it will be forward in the response to the AMF/SEAF.

8. Registration response.

### 6.15.3 System impact

This solution is having impact on AUSF.

AUSF: Capability to forward the authentication request to the DCS.

### 6.15.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 6.16 Solution #16: UE onboarding for SNPN with the interaction between PS and DCS

### 6.16.1 Introduction

This solution addresses Key Issue #2 "Provisioning of Credentials" and Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN".

The assumption of this solution is that:

1. The UE has been provisioned with default UE credentials from DCS;

2. The UDM is configured with a mapping of the Universal UE ID with the PS address.

3. The Universal UE ID is the UE permanent ID which is unique for every single UE. The Universal UE ID can be SUCI or other kinds of UE ID that can uniquely differentiate a UE.

### 6.16.2 Solution details

#### 6.16.2.1 Procedure

A mechanism of UE onboarding and provisioning for SNPN with the interaction between PS and DCS is described in the Figure 6.16.2.1-1. The main idea of this mechanism is that the UE firstly registers with the O-SNPN with restricted access and then performs authentication with DCS via User Plane. After the success of authentication with DCS, the PS provisions the SNPN credential to the UDM and UE, respectively.

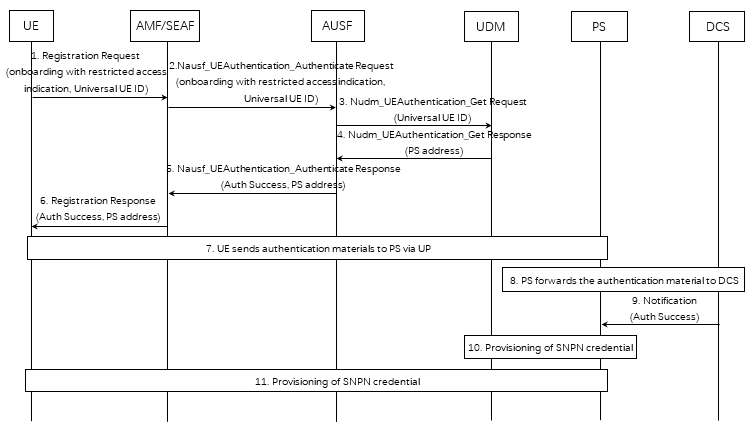


Figure: 6.16.2.1-1: UE onboarding and provisioning for SNPN with the interaction between PS and DCS(authentication via UP)

1. The UE sends Registration Request to AMF. The Registration Request includes a "Onboarding with restricted access" indication and a Universal UE ID.

2. The AMF sends Nudm\_UECM\_Get Request with the Universal UE ID to UDM.

NOTE: The format of the Universal UE ID can be either SUPI or PEI. The format of SUPI and PEI can refer to TS 23.003 [9] clause 2.2A and 6.4, respectively. The privacy protection of SUPI can refer to TS 33.501 [2] Annex I.5.

3. Upon the receipt of the Nudm\_UECM\_Get Request, the UDM sends Nudm\_UECM\_Get response with the PS address to AMF.

4. Upon the receipt of the Nudm\_UECM\_Get Response from the UDM, the AMF sends Registration accept, containing PS address, to UE.

5. The UE sends authentication materials (i.e. signing material and default credential ID) to PS via UP once it obtains the restricted access.

6. The PS identifies the DCS address via UE Universal ID and forwards the authentication material to the DCS.

7. The DCS authenticate the UE through verifying the authentication material. If the verification succeeds, the DCS sends a notification including the Authentication Success to PS.

8. The PS provisions the UDM with SNPN credential. The detailed provisioning method is out of the scope of the present document.

9. The PS provisions the UE with SNPN credential. The detailed provisioning method is out of the scope of the present document.

#### 6.16.2.2 Procedure

A mechanism of UE onboarding and provisioning for SNPN with the interaction between PS and DCS is described in the Figure 6.16.2.2-1. The main idea of this mechanism is that the UE performs primary authentication. After the success of primary authentication, the PS provisions the SNPN credential to the UDM and UE, respectively.

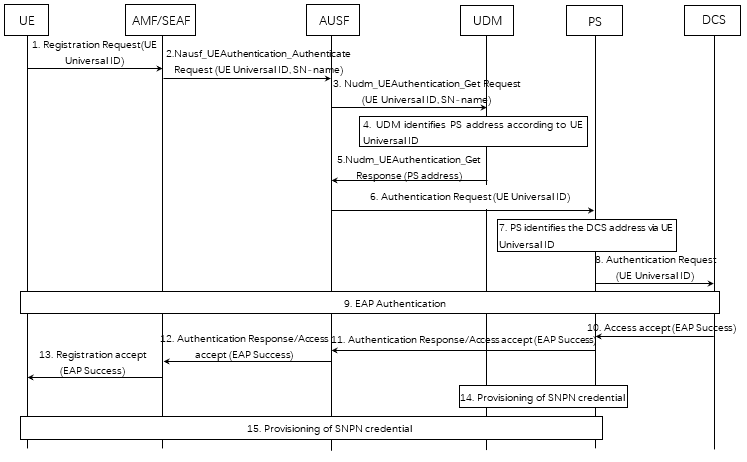


Figure: 6.16.2.2-1: UE onboarding and provisioning for SNPN with the interaction between PS and DCS (primary authentication)

1. The UE sends a Registration Request to the AMF. The registration Request includes the UE Universal ID.

NOTE: The format of the Universal UE ID can be either SUPI or PEI. The format of SUPI and PEI can refer to TS 23.003 [x] clause 2.2A and 6.4, respectively. The privacy protection of SUPI can refer to TS 33.501 [2] Annex I.5.

2. The AMF sends Nausf\_UEAuthentication\_Authentication Request, containing UE Universal ID and SN-Name, to the AUSF.

3. The AUSF sends Nudm\_UEAuthentication\_Get Request, containing UE Universal ID and SN-Name, to the UDM.

4. The UDM identifies PS address according to UE Univeral ID.

5. The UDM sends Nudm\_UEAuthentication\_Get Response, containing PS address, to the AUSF.

6. The AUSF executes the Primary Authentication by sending EAP request, containing UE Universal ID, to the PS.

7. The PS identifies the DCS address via UE identity ID.

8. The PS forwards the Authentication Request, containing UE Universal ID, to the DCS.

9. The UE and DCS conducts EAP authentication.

10. If the authentication successes, the DCS sends an Access accept containing EAP success to the PS.

11. The PS sends an Authentication Response/Access accept to the AUSF.

12. The AUSF sends Authentication Response/Access accept to the AMF.

13. The AMF sends Registration accept to the UE.

14. The PS provisions the UDM with SNPN credential. The detailed provisioning method is out of the scope of SA3.

15. The PS provisions the UE with SNPN credential. The detailed provisioning method is out of the scope of SA3.

### 6.16.3 System impact

System impact of the solution is not addressed in the present document.

### 6.16.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 6.17 Solution #17: Solution to Provisioning of PNI-NPN Credentials

### 6.17.1 Introduction

This solution aims at addressing Key Issue #2 about provisioning of PNI-NPN credentials.

### 6.17.2 Solution details

The architectural assumption of this solution is as below. The PNI-NPN provisioning server is connected to NEF if the PNI-NPN provisioning server is outside the operator domain, in order to acquire derived keys using AKMA to protect the communication between the UE and the PNI-NPN provisioning server. Once the secure tunnel is established between the UE and the PNI-NPN provisioning server, the PNI-NPN credentials could be provisioned to the UE from the PNI-NPN provisioning server via the protected tunnel.



The procedures are as follows:



The pre-requisite is as what defined in TS 33.535 [10], the UE has completes a successful primary authentication and thus results in KAKMA and A-KID generated and stored at AAnF.

UE sends the Access Request to the PNI-NPN provisioning server, carrying the generated A-KID.

While receiving the Access Request from the UE, the PNI-NPN provisioning server requests the derived keys used for protection the communication between the UE and the provisioning server from AAnF, carrying A-KID and PNI-NPN provisioning server ID.

AAnF generates KPNINPN from KAKMA.

AAnF sends the generated KPNINPN and its lifetime to PNI-NPN provisioning server.

While receiving the KPNINPN, the PNI-NPN provisioning server sends the access response to the UE and indicates the UE to generate KPNINPN accordingly.

UE and the PNI-NPN provisioning server establishes a secure tunnel between them based on KPNINPN, in order to allow PNI-NPN provisioning server sends the PNI-NPn credentials in a secure manner.

### 6.17.3 System Impact

System impact of the solution is not addressed in the present document.

### 6.17.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 6.18 Solution #18 Solution on service authorization for SNPNs

### 6.18.1 Introduction

This solution address Key Issue #5 Roaming-related security mechanisms for SNPNs. Considering the entity separate from the SNPN can be a PLMN or some other Service provider and the SNPN follows similar architecture as 5GC, legacy roaming architecture can be used as the reference in this case, e.g., the AMF in V-SNPN interacts with the AUSF in Home SP (PLMN or SNPN) to get the UE authentication services. SEPPs are also assumed to be located between Home SP and V-SNPN for control plane messages protection.

### 6.18.2 Solution Details

In case of roaming architecture, service authorization procedure is similar to the one indicated in TS 33.501 [1] clause 13.4.1.2.

**Step 1: obtaining access token from Home SP for service access**



Figure 6.18.2-1: NF Service Consumer in V-SNPN obtaining access token before NF Service access

1. The NF Service Consumer in V-SNPN invokes Nnrf\_AccessToken\_Get Request (V-SNPN ID, PLMN ID/H-SNPN ID and other parameters defined in TS 33.501 [1] clause 13.4.1.2) from NRF in the same SNPN.

2. The NRF in SNPN forwards the parameters it obtained from the NF Service Consumer to the NRF in PLMN/H-SNPN.

3. The NRF in PLMN/H-SNPN checks whether the NF Service Consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the NRF in PLMN/H-SNPN generates an access token as defined in TS 33.501 [1] clause 13.4.1.1 with SNPN IDs as additional claims.

4. If the authorization is successful, the access token is included in Nnrf\_AccessToken\_Get Response message to the NRF in V-SNPN.

5. The NRF in V-SNPN forwards the Nnrf\_AccessToken\_Get Response to the NF Service Consumer.

**Step 2: service authorization based on token verification**

The following figure and procedure describe how authorization is performed during service request of the NF Service Consumer in V-SNPN.



Figure 6.18.2-2: NF Service Consumer in V-SNPN requesting service access with an access token in roaming case

1. The NF Service Consumer in V-SNPN requests the service from a NF Service Producer of Home SP. The NF Service Consumer includes the access token obtained from the NRF in step 1 in the Service Request.

- During the transmission of the request, the pSEPP checks that the V-SNPN ID in the subject claim of the access token matches the remote SNPN ID corresponding to the N32-f context Id in the N32 message.

2. The NF Service Producer of Home SP verify the token as follows:

- The NF Service Producer ensures the integrity of the token by verifying the signature using the public key of the NRF of Home SP or checking the MAC value using the shared secret.

- If integrity check is successful, the NF Service Producer verifies the claims in the token as defined in TS 33.501 [1] clause 13.4.1.1.2. In addition, the NF Service Producer erifies that the V-SNPN ID contained in the API request is identical to the one contained in the subject claim of the access token. The NF Service Producer also checks that the PLMN ID/H-SNPN ID in the audience claim of the access token matches its own PLMN/H-SNPN identity.

### 6.18.3 System impact

The NF consumer in V-SNPN includes SNPN ID in access token request.

The NRF in home PLMN or H-SNPN generates the access token per SNPN ID.

The NF producer in home PLMN or H-SNPN is able to verify the access token containing SNPN ID (PLMN ID+NID) from the NF consumer in V-SNPN.

The SEPP maintains N32-f context as per SNPN and perform the verification based on SNPN ID (PLMN ID+NID).

### 6.18.4 Evaluation

This solution meets the requirements of KI#5.

## 6.19 Solution #19: Secure onboarding without client authentication

### 6.19.1 Introduction

This solution addresses key issue#4 Securing initial access for UE onboarding between UE and SNPN. The scope of the solution is limited to cases, in which the subsequent onboarding can be executed using a restricted PDU session.

In this solution one-way authentication including 5G key hierarchy is executed. The main difference to other solutions is that the network does not authenticate the UE, e.g., no peer authentication is applied during EAP-TLS authentication, The main difference of the modified variant with respect to EAP-TLS is that it does include server authentication only, but no client authentication.

That is, no default credentials or default credential server needs to be involved. Default credentials will be used only during the actual provisioning step, which is outside the scope of this solution.

A O-SNPN can get a certificate from well know certificate authorities, which are trusted by the ecosystem. This could be GSMA or another industry association capable of operation a certification program. The CI role can be delegated to companies which can handle this like for the case of eSIM. In this case the device manufacturer just needs to install the set of relevant root CA certificates on the UE. Selection and operation of the CAs is out of scope of this solution.

In case the onboarding UE has been configured with the identities of one or several allowed O-SNPNs (for instance by the user using the UE's user interface), the onboarding UE can fully authenticate and authorize the O-SNPN using the installed root CA certificates.

If the UE has not been configured with identities of allowed O-SNPNs, the UE can still authenticate the O-SNPN, i.e., verify the validity of the O-SNPN certificate. For the actual provisioning the onboarding UE will establish a secure channel to the provisioning server and execute mutual authentication and authorization with the provisioning server independent of the O-SNPN. Thus, security does not rely on the UE authorizing the O-SNPN as part of primary authentication.

Since no client authentication is required, a potentially large number of UEs can blindly request onboarding from the O-SNPN. This problem can be mitigated by executing an Equipment Identity Check using the PEI of the onboarding UE. This implies that the UE provider needs to provide the PEI to the onboarding network owner prior to onboarding the UE.

### 6.19.2 Solution details

Figure 6.19.2-1 shows a generalisation of the solution.



Figure 6.19.2-1: initial access and sharing of identity

1. The UE sends a Registration Request including a SUCI to the network.  
As an example the SUCI can be constructed in such way that the SUCI's Home Network Identifier HNI is set to a fixed predefined string, like "onboarding", which can be used by the 5GS to determine that the UE is requesting access without client authentication for onboarding purposes. The scheme output of the SUCI can be set to an empty string Alternatively also new registration type specified by SA2 could be utilized for the purpose of finding out that the UE is requesting unauthenticated access for onboarding purposes. In this case HNI and scheme output can be set to empty strings.

NOTE 1: Details can be defined during normative phase.

2. AMF / SEAF forwards request to AUSF.

3. Based on the received SUCI the AUSF concludes that the UE wants to execute unauthenticated access and selects a corresponding EAP-TLS method configured without client authentication. The selection of the EAP method might be carried out by the AUSF, or the AUSF might invoke the UDM for this (not shown in Figure 6.19.2-1)

NOTE 2: Decision of whether UDM needs to be involved can be taken during normative work.

4. UE and AUSF execute EAP based authentication using the selected EAP-TLS method. This is following the procedure in TS 33.501 [2] described for EAP-TLS except that the selected EAP-TLS method without client authentication.

5. Before the last step of the EAP procedure the AUSF calculates KAUSF and KSEAF as defined in TS 33.501 [2], i.e., The EMSK resulting from the executed EAP session is used as input for the derivation of KAUSF.

6. The AUSF returns response message including EAP Success message, KSEAF and SUPI. The SUPI is set to a predefined constant value, which indicates to the SEAF that the UE has not been authenticated.

7. AMF / SEAF finalizes the EAP session towards the UE.

8. SEAF calculates the KAMF as specified in TS 33.501 [2] with the difference that not a real SUPI, but a reserved string is used as input to the key derivation function. The calculation of the remaining 5G keys is according to TS 33.501 [2].

9. UE calculates all 5G keys according to the definitions in TS 33.501 [2], with the difference that not a real SUPI but the same reserved string also used by the SEAF is used as input to the key derivation function.

10. UE and AMF establish security context as defined in TS 33.501 [2].

11. AMF and UE exchange Identity Request/Response messages to obtain UE's (PEI) (as defined in TS 23.502 [6]), e.g., based on local configuration in AMF.

12. AMF sends Equipment Identity Check Request to the EIR using PEI as input parameter.

13. EIR checks, if PEI is on an Allowed-List of UEs, which are entitled for onboarding.

NOTE 3: The PEI based identity check might be optional for the O-SNPN. Therefore, it is up to the O-SNPN, if it wants to make use of this additional security mechanism. However, a UE, which wants to use unauthenticated access for onboarding needs to support Identity Request/Response message.

NOTE 4: The PEI of the onboarding UE has been added to the O-SNPNs Allowed-List prior to the onboarding. That is, the device owner, which is an entity or person trusted by the O-SNPN, has provided the PEI of the UE to the O-SNPN.

NOTE 5: The PEI sent from the UE to the AMF is not cryptographically protected. That is a malicious UE might simply send the PEI of another UE. However, since the authorization is done by the EIR using a positive list, an attacker might need to know or guess a valid PEI. Furthermore, the authorization using the PEI, is just used to avoid overload situations of the O-SNPN and is not used to derive any security association. The actual mutual authentication and authorization between UE and PVS will take place during the subsequent provisioning step, which is outside the scope of this solution.

14. If UE's PEI was on the Allowed list, the AMF will reply with a positive response.

15. AMF confirms Registration

After the one-way authentication and optionally PEI based authorization has been executed, the UE can request a restricted PDU Session as studied in TR 23.007-7 [3] and currently standardized in TS 23.501 [4]. The actual provisioning of the Subscriber profile is executed subsequently and outside the scope of this solution.

### 6.19.3 System impact

The solution has impact on the following system components:

UE: Support of EAP-TLS without client authentication

AUSF: Support of EAP-TLS without client authentication

EIR: The EIR needs to hold a list with PEIs of onboarding UEs, which are entitled for onboarding, and authorize onboarding UEs based on this list.

### 6.19.4 Evaluation

This solution provides an approach for how an onboarding UE can attach to an onboarding network without usage of a default credentials server. It relies on one-way authentication, i.e. the UE authenticates the network, but the network does not authenticate the UE.

Unauthenticated UE could connect to the onboarding network for purposes other than provisioning but can be prevented by restricting onboarding connectivity to trusted provisioning servers as one solution among others. In this solution, UE is not authenticated. This means an adversary can register any number of UEs and exhaust the resources in the onboarding network. Furthermore, such registered malicious UEs can be used to send any amount of control plane messages to the NFs in the onboarding network, the implications of which has not been fully studied. To mitigate the overload risk, the O-SNPN can utilize Equipment Identity Check and authorize onboarding UEs based on its PEI. This also implies that the UE provider needs to provide the PEI's to the OSNPN prior to onboarding. An attacker might be able to probe the OSNPN and hereby guess a valid PEI which then circumvent the overload mechanism.

The solution could be used for initial access for provisioning protocols like the consumer variant of GSMA RSP [3]. GSMA RSP is self-contained and does not have any security requirements for the transport layer.

## 6.20 Solution #20: Control plane based provisioning: PS to AUSF

### 6.20.1 Introduction

This solution addresses Key issue #2 "Provisioning of Credentials".

The architecture of this solution is illustrated as Figure 6.20.1-1. It is assumed that the domain of the PS has trust relationship with the O-SNPN.



Figure 6.20.1-1: Architecture of control plane based provisioning: PS to AUSF

### 6.20.2 Solution details



Figure 6.20.2-1: Control plane based provisioning: PS to AUSF

1. A successful authentication has been performed among the UE, the Onboarding Network and the DCS. The UE and the AUSF store the KAUSF.

2. The AMF sends an Authentication\_Notification to the PS of the UE, including the AUSF ID of the AUSF which stores the KAUSF.

3-4. The PS invokes Nausf\_UPUProtection service operation message by including the UPU Data to the AUSF indicated by the AUSF ID received in the last message to get UPU-MAC-IAUSF and CounterUPU as specified in clause 14.1.4 of TS 33.501[2]. If the PS decided that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the PS sets the corresponding indication in the UE Parameters Update Data (see TS 24.501 [11]) and include the ACK Indication in the Nausf\_UPUProtection service operation message to signal that it also needs the expected UPU-XMAC-IUE, as specified in clause 14.1.4 of TS 33.501 [2].

The details of the CounterUPU is specified in clause 6.15.2.2 of TS 33.501 [2]. The inclusion of UE Parameters Update Data in the calculation of UPU-MAC-IAUSF allows the UE to verify that it has not been tampered by any intermediary. The expected UPU-XMAC-IUE allows the PS to verify that the UE received the UE Parameters Update Data correctly.

5. The PS invokes Nudm\_SDM\_Notification service operation, which contains UE Parameters Update Data, UPU-MAC-IAUSF, CounterUPU within the Access and Mobility Subscription data. If the PS requests an acknowledgement, it temporarily stores the expected UPU-XMAC-IUE.

6. Upon receiving the Nudm\_SDM\_Notification message, the AMF sends a DL NAS Transport message to the served UE. The AMF includes in the DL NAS Transport message the transparent container received from the PS.

7. On receiving the DL NAS Transport message, the UE calculates the UPU-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.19 of TS 33.501 [2]) on the received UE Parameters Update Data and the CounterUPU and verify whether it matches the UPU-MAC-IAUSF value received in the DL NAS Transport message. If the verification of UPU-MAC-IAUSF is successful, the UE updates its stored parameters with the received parameters in PS Update Data.

8. If the PS has requested an acknowledgement from the UE and the UE has successfully verified and updated the UE Parameters Update Data provided by the PS, then the UE sends the UL NAS Transport message to the serving AMF. The UE generates the UPU-MAC-IUE as specified in Annex A.20 of TS 33.501 [2] and include the generated UPU-MAC-IUE in a transparent container in the UL NAS Transport message.

9. If a transparent container with the UPU-MAC-IUE was received in the UL NAS Transport message, the AMF sends a Nudm\_SDM\_Info request message with the transparent container to the PS.

10. If the PS indicated that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the PS compares the received UPU-MAC-IUE with the expected UPU-XMAC-IUE that the PS stored temporarily in step 5.

NOTE 1: Whether hop by hop confidentiality protection of credentials is enough is not addressed in the present document.

NOTE 2: How UDM in SO-SNPN gets provisioning data is not addressed in the present document.

NOTE 3: The need for standardization of the reference point between PS and AUSF is not addressed in the present document. Whether the AUSF is exposed directly or through NEF is not addressed in the present document.

NOTE 4: If PNI-NPN credential is certificate, what is included in UPU data is not addressed in the present document.

### 6.20.3 System impact

A new reference point between PS and AUSF has to be defined.

NOTE: Further system impact is not addressed in the present document.

### 6.20.4 Evaluation

The credentials provisioned by the PS are known to the O-SNPN.

NOTE: Further evaluation is not addressed in the present document.

## 6.21 Solution #21: Control plane based provisioning: PS to UDM

### 6.21.1 Introduction

This solution addresses Key issue #2 "Provisioning of Credentials".

The architecture of this solution is illustrated as Figure 6.21.1-1. It is assumed that the domain of the PS has trust relationship with the O-SNPN.



Figure 6.21.1-1: Architecture of control plane based provisioning: PS to UDM

### 6.21.2 Solution details



Figure 6.21.2.1-1: Control plane based provisioning: PS to UDM

1. A successful authentication has been performed among the UE, the Onboarding Network and the DCS. The UE and the AUSF store the KAUSF.

2. The AMF sends an Authentication\_Notification to the PS of the UE.

3. The PS sends a Provisioning\_Request message to the UDM, including SUPI and Provisioning Data.

4-5. The UDM invokes Nausf\_UPUProtection service operation message by including the UPU Data to the AUSF to get UPU-MAC-IAUSF and CounterUPU as specified in clause 14.1.4 of TS 33.501 [2]. If the UDM decided that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM sets the corresponding indication in the UE Parameters Update Data (see TS 24.501 [11]) and include the ACK Indication in the Nausf\_UPUProtection service operation message to signal that it also needs the expected UPU-XMAC-IUE, as specified in clause 14.1.4 of TS 33.501 [2].

The details of the CounterUPU is specified in clause 6.15.2.2 of TS 33.501 [2]. The inclusion of UE Parameters Update Data in the calculation of UPU-MAC-IAUSF allows the UE to verify that it has not been tampered by any intermediary. The expected UPU-XMAC-IUE allows the UDM to verify that the UE received the UE Parameters Update Data correctly.

6. The UDM invokes Nudm\_SDM\_Notification service operation, which contains UE Parameters Update Data, UPU-MAC-IAUSF, CounterUPU within the Access and Mobility Subscription data. If the PS requests an acknowledgement, it temporarily stores the expected UPU-XMAC-IUE.

7. Upon receiving the Nudm\_SDM\_Notification message, the AMF sends a DL NAS Transport message to the served UE. The AMF includes in the DL NAS Transport message the transparent container received from the UDM.

8. On receiving the DL NAS Transport message, the UE calculates the UPU-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.19) on the received UE Parameters Update Data and the CounterUPU and verify whether it matches the UPU-MAC-IAUSF value received in the DL NAS Transport message. If the verification of UPU-MAC-IAUSF is successful, the UE updates its stored parameters with the received parameters in PS Update Data.

9. If the UDM has requested an acknowledgement from the UE and the UE has successfully verified and updated the UE Parameters Update Data provided by the PS, then the UE sends the UL NAS Transport message to the serving AMF. The UE generates the UPU-MAC-IUE as specified in Annex A.20 and include the generated UPU-MAC-IUE in a transparent container in the UL NAS Transport message.

10. If a transparent container with the UPU-MAC-IUE was received in the UL NAS Transport message, the AMF sends a Nudm\_SDM\_Info request message with the transparent container to the UDM.

11. If the UDM indicated that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM compares the received UPU-MAC-IUE with the expected UPU-XMAC-IUE that the PS stored temporarily in step 806.

12. The UDM sends a Provisioning\_Response message to the PS, including result code of the provisioning operation.

NOTE 1: Whether hop by hop confidentiality protection of credentials is enough is not addressed in the present document.

NOTE 2: How UDM in SO-SNPN gets provisioning data is not addressed in the present document.

NOTE 3: The need for standardization of the reference point between PS and UDM is not addressed in the present document. Whether the UDM is exposed directly or through NEF is not addressed in the present document.

NOTE 4: If PNI-NPN credential is certificate, what is included in UPU data is not addressed in the present document.

### 6.21.3 System impact

System impact of the solution is not addressed in the present document.

### 6.21.4 Evaluation

The credentials provisioned by the PS are known to the O-SNPN.

NOTE: Further evaluation is not addressed in the present document.

## 6.22 Solution #22: Solution for onboarding and provisioning

### 6.22.1 Introduction

This solution addresses Key Issue #2 "Provisioning of Credentials" and Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN".

### 6.22.2 Solution details

The UE is identified by the DCS based on the onboarding SUCI, the DCS can deconceal the SUCI to a onboarding SUPI. The DCS can authenticate the UE based on the onboarding credentials and provision the MSK to the AUSF for setting up the security over the radio interface for AS and NAS per normal procedures. The DCS and UE derive a provisioning key which is used to protect the profile from the Provisioning Server.



Figure 6.22.2-1: Network access authentication with credentials owned by an entity separate from the SNPN

1. The UE sends a Registration Request with the Onboarding SUCI of the DCS as UE identity to the AMF.

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

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 DCS. The AUSF identifies the DCS and takes the role of an AAA-Proxy, sending a related AAA message to the corresponding AAA-Server. The AUSF sends an Authentication Request with the onboarding SUCI to the DCS.

NOTE 1: In this solution the SBI-DIAMETER interworking functionality is collocated with the AUSF.

4. The DCS deconceals the SUCI to a SUPI and verifies the authentication request based on the username. The DCS selects the subscriber profile based on the SUPI and performs an EAP based authentication with the UE, using the pre-shared onboarding credentials in the UE and in the DCS.

5. After successful authentication, the DCS sends the result of the authentication, the onboarding SUPI, MSK, validity time and address of the Provisioning Server back in an authentication response to the AUSF.

6. The AUSF verifies the response and derives the KAUSF from the MSK and the KSEAF according to TS 33.501. the UE is performing the same key derivation accordingly.

7. The AUSF sends an authentication response to the AMF/SEAF including the authentication result from the DCS and the KSEAF, the onboarding SUPI, the validity time, i.e. time until the onboarding expires and the address of the Provisioning Server.

8. The AMF performs NAS SMC with the UE.

9. After a successful NAS SMC procedure, the AMF sends the Registration Accept including the address of the Provisioning Server.

10. The UE performs a normal PDU Session Establishment procedure to gain IP connectivity.

11. The UE and the DCS derive a Provisioning Key KPro from the MSK in the same way.

12. The DCS provides the provisioning information Onboarding SUPI and Provisioning Key KPro to the Provisioning Server. The selection for the Provisioning Server may be performed based on the stored address in the DCS per onboarding SUPI.

NOTE 2: The solution introduces a new interface between the DCS and the PS.

13. The Provisioning Server selects the Profile based on the onboarding SUPI.

14. The UE establishes and IPSec SA with the Provisioning Server by using the KPro. All messages are now confidentiality and integrity protected by the IPsec tunnel.

15. The Provisioning Server provisions the new profile to the UE via the IPSec tunnel.

16. The Provisioning Server acknowledges the successful provisioning to the DCS.

17. The DCS deletes or deactivates the onboarding profile that relates to the onboarding SUPI. This prevents that if onboarding credentials are compromised, succeeding impersonation attacks from malicious UEs are prevented from being provisioned with the valid profile.

18. The UE deregisters from the Onboarding network and may also delete or deactivate the onboarding profile.

19: The UE select the NPN according to the provisioned profile and registers to the NPN according to the normal procedures in TS 23.501/TS 33.501.

### 6.22.3 System impact

The solution introduces a new interface between the DCS and the PS.

### 6.22.4 Evaluation

The evaluation of the solution is not addressed in the present document.

## 6.23 Solution #23: Solution to enable onboarding and secured UE access based on credentials owned by an external entity

### 6.23.1 Introduction

The solution address 'Key issue #4: Securing initial access for UE onboarding between UE and SNPN'. In addition, the solution also takes into account the requirements from TS 22.261 [x] clause 6.14.2 which is on enabling 5GS to support a secure mechanism to remotely provision 3GPP/non 3GPP identities and credentials of a uniquely identifiable and verifiably secure device. The proposed solution considers that a UE is configured with the default credentials including a default UE ID which allows to verify and securely identify the device to enable onboarding to an onboarding SNPN to provision SNPN credentials. It is assumed that the default identity is a secure identity by itself, it does not leak any information by itself about the UE (i.e., privacy friendly by design) and it can be used to refer to a set of information about the UE stored in the DCS, but it is more important to prevent impersonation due to replay attack as part of the solution.

### 6.23.2 Solution details

The solution described in this clause is to deal with onboarding of UEs to SNPN based on default credentials, where DCS (i.e., AAA server) is involved.



Figure 6.23.2-1: Secured Initial access for onboarding based on credentials owned by external entity

The steps shown in Figure 6.23.2-1 is described as follows.

0. In this solution, the UE and the DCS is assumed to be pre-configured with the default UE ID (i.e., onboarding ID associated with the default credentials) and the default credentials. The DCS in addition is pre-configured with the corresponding PS address for each onboarding default UE ID. The default UE ID can be a set of strings/digits (e.g.,123456789abcdefghi) which together with the DCS domain name can act as URI for the DCS to identify the right default credentials corresponding to the UE during the onboarding procedure. The default UE ID together with DCS domain name can take NAI format (e.g., 123456789abcdefghi@DCSdomain).

NOTE 1: The method of assigning the default UE ID can be up to the DCS. The default credentials associated with the default UE ID can be any cryptographic material, such as public-private key pairs, DCS information (i.e., address), and cryptographic algorithms etc., and it is up to the DCS.

The default UE ID and the DCS domain information in NAI format can be used as SUPI for the onboarding phase by the UE and the network. The default UE ID and DCS domain name conveys no privacy sensitive information about the User or UE/device. The UE constructs the onboarding SUPI in the NAI format using the Default UE ID and DCS address. Further the UE set the time stamp and generates a digital signature for the onboarding SUPI and Timestamp using it is private key available as part of the default credentials. As, the external entity DCS cannot be expected to support SIDF functionality specified in TS 33.501 [2], the UE and DCS offer the authenticity of the default UE ID based on digital signature as described in this solution. Further the existing 5G systems depends on routing ID and HN ID to select the right AUSF instance in the network, whereas the UE that attempts onboarding registration, cannot provide any routing ID as well as HN ID to select the right AUSF instance in the O-SNPN. Therefore, this solution also takes care of selecting the right AUSF instance based on the onboarding SUPI.

NOTE 2: If an ongoing onboarding procedure fails due to any network issues, the UE still can use the same default UE ID for the onboarding with replay protection by adding a timestamp and digital signature to ensure the authenticity of the default UE ID. Digital signature prevents tampering and malicious replay of default UE ID. The UE can generate the digital signature of onboarding SUPI and the timestamp (i.e., by generating hash and encrypting that data) using its private key and send it along with the actual data such as onboarding SUPI and timestamp to the DCS via the 3GPP network during the onboarding registration procedure. The DCS on receiving the onboarding SUPI, fetches the default credentials corresponding to the default UE ID and uses the public key of the UE to verify the digital signature. If the DCS finds the verification as successful (i.e., if the message digest of the received data is identical to the decrypted digital signature then the digital signature verification is considered successful), then the DCS considers that the received default UE ID and timestamp are provided by the UE which has the actual default credentials related to it. AAA functions can support digital signature according to the security considerations discussed in RFC 2903 [12] and so the DCS being the AAA server can support the default UE ID protection based on digital signature.

NOTE 3: The primary aspect is that, if the attacker replays a UE ID with malicious intensions, the digital signature verification will help the DCS to identify the malicious behaviour right at the first step of identifier verification and this enables the DCS to skip any further unnecessary message exchanges with the malicious device and this also prevents unnecessary resource exhaustion.

1. The UE sends a registration request to the onboarding SNPN acting as onboarding network. The UE includes a Subscription unique onboarding identifier (SUOI) which consists of Onboarding SUPI, Timestamp and the digital signature.

NOTE 4: The UE selects an O-SNPN based on TS 23.501.

2. AMF/SEAF forwards the registration request to the right onboarding AUSF (which can interact with DCS either directly or via a NSSAAF) based on the SUOI.

3-4. The onboarding AUSF sends the authentication request with SUOI to the NSSAAF and the NSSAAF uses the realm part of the SUOI to route the request to the right DCS.

5. The DCS based on the default UE ID in the SUOI, fetches the related default credentials data along with cryptographic information and verifies the digital signature as described in NOTE 1.

6. If the verification is successful, based on the default configuration locally stored, the DCS selects an authentication method and performs authentication method specific message exchanges with the UE. If the authentication is successful, the DCS determines to provide the onboard root key along with authentication result to the onboarding AUSF.

7-8. The DCS sends an authentication response to the AUSF via NSSAAF. It includes authentication result as 'success', onboarding root key (e.g., MSK) and a minimum data set (verified default UE ID, provisioning server address etc.,). The default UE ID will act as the onboarding SUPI/default SUPI in the onboarding SNPN.

9. The onboarding AUSF stores the authentication result and minimum data set in the UDM/UDR, and the provisioning server address information can be later used by the network (i.e., SMF) for restricted user plane connection to the provisioning server to provision the SNPN credentials which is out of the scope of this solution. The onboarding AUSF considers the key received from the DCS as AUSF key and derives an anchor key similar to the method specified in 33.501, but with an additional input of nonce to establish cryptographic separation and network binding specific to the SNPN. Further the onboarding AUSF sends a EAP success message to the AMF/SEAF including Kseaf, nonce and the SUPI. The nonce is sent in NAS SMC without being encrypted but with integrity protection.

NOTE 5: The need for the nonce and how the secrecy specific to SNPN is achieved is not addressed in the present document. The reason is that 'even without nonce, cryptographic separation is achieves in 5G as further keys are derived – also not clear how secrecy would be achieved with unprotected nonce'.

NOTE 6: The minimum data set refers to the information such as UE and onboarding support information (example., UE information (verified default UE ID, PS address (if any), default credentials validity (if any)) which is expected to be provided by the DCS to the 3GPP network following a successful authentication of the UE.

10. The EAP success and other information received from step 8 can be provided to the UE in a NAS SMC similar to the 33.501. The AMF initiates NAS SMC with the UE as in 33.501.

11-12. The UE derives its keys based on the configurations in the default credentials and the registration is complete.

NOTE 7: For the case that the default UE ID and credentials are preconfigured by a PLMN, the existing concealment mechanisms can be applied for the SUPI and the authentication method and key generation can be followed similar to the mechanisms specified in 33.501 (i.e., as in EAP-AKA' and 5G AKA).

This solution describes initial access of the UE to the onboarding network based on the mutual authentication between the UE and the DCS. The onboarding network which does not have direct trust relationship with the UE allows the initial access based on the UE and DCS mutual authentication (i.e., based on any key generating EAP method, e.g., EAP-TLS) and their trust relationship and based on the onboarding network's trust/business relationship with the DCS. Further the solution details the issue of the Provisioning Server address to the onboarding SNPN, but the connection between UE and PS is not in scope of this solution.

### 6.23.3 System impact

UE: Need to construct subscription unique onboarding identifier using onboarding SUPI (i.e., default UE ID), time stamp and digital signature. Anchor key generation includes nonce as additional input.

AMF/SEAF: Selects the right onboarding AUSF which can connect with NSSAAF for onboarding based on the onboarding SUPI.

AUSF: Need to support Anchor key generation using nonce as additional input: Need to store PS address in the UDM for the duration of the onboarding registration.

DCS: Need to verify the default UE ID received in the SUOI by verifying the digital signature where the AAA function can support digital signature handling. Further DCS need to a key along with the verified default UE ID to 3GPP network. In case if any additional data about UE and PS address need to be provided, then it need to provide them as a data set to the SNPN.

### 6.23.4 Evaluation

This solution enables the UE and DCS to perform mutual authentication with credentials owned by DCS an entity separate from the SNPN to allow SNPN access for onboarding.

NOTE: Further evaluation is not addressed in the present document.

## 6.24 Solution #24: Secure mutually authenticated onboarding without DCS

### 6.24.1 Introduction

This solution addresses key issue#4 Securing initial access for UE onboarding between UE and SNPN. The scope of the solution is limited to cases, in which the subsequent onboarding are executed using a restricted PDU session.

The aim of the solution is the reduce the complexity of deploying the 3GPP technology into already well-defined ecosystems which includes provisioning schemes. That could be OPC UA or another industry specific provisioning protocol or framework. The actual provisioning protocol is out of scope for this solution.

In this solution each UE is equipped with a private key and a UE default certificate issued by a CA run e.g. by the UE manufacturer. During UE onboarding the O-SNPN can execute primary authentication and verify the UE default certificate without involvement of a DCS. The CA certificate for the verification of UE default certificate as well as the identity of the onboarding UE is configured at the O-SNPN prior to onboarding.

The final provisioning of the SO-SNPN credentials including mutual authentication between UE and Provisioning Server (PS) is preformed over an industry defined protocol or framework.

### 6.24.2 Solution details

Figure 6.24.2-1 shows a generalisation of the solution.



Figure 6.24.2-1: Initial access and provisioning.

Prior to onboarding the UE is provisioned with default credentials, e.g. during manufacturing, and the UDM is provisioned with onboarding records containing information to verify the UE default credentials.

1. The UE sends a Registration Request including a SUCI to the network.

2. AMF / SEAF forwards request to AUSF.

3. Based on the received SUCI the AUSF concludes that the UE wants to execute authenticated access and selects a corresponding EAP-TLS method configured.

4. UE and AUSF execute EAP based authentication using the selected EAP-TLS method. This is following the procedure in TS 33.501 [2]. The PKI of the UE default and server certificates are out of scope.

5. Before the last step of the EAP procedure the AUSF calculates KAUSF and KSEAF as defined in TS 33.501 [2], i.e., The MSK resulting from the executed EAP session is used as input for the derivation of KAUSF.

6. The AUSF returns response message including EAP Success message, KSEAF and SUPI.

7. AMF / SEAF finalizes the EAP session towards the UE.

8. SEAF calculates the KAMF as specified in TS 33.501 [2].

9. UE calculates all 5G keys according to the definitions in TS 33.501 [2].

10. UE and AMF establish security context as defined in TS 33.501 [2].

11. The UE and PS establishes a secure connection utilising an industry specific protocol. The same protocol is utilised to provisioning the UE specific credentials to the UE.

The actual provisioning of the subscriber profile is executed subsequently and outside the scope of this solution.

### 6.24.3 System impact

No system impact identified.

### 6.24.4 Evaluation

This solution provides the options to authenticate a UE without interaction with a DCS by using already standardised methods in TS 33.501 [2] in the context of SNPN. It enables the UE and O-SNPN to mutually authenticate and hereby establish a security context, which might be further utilised for provisioning. This can be achieved without involvement of the DCS; i.e., without the need for integration between the O-SNPN and DCS. The default credentials needs to be provisioned to the UE prior to onboarding.

The solution enables an SNPN provider to utilise an industry specific protocol for provisioning of credentials but still enable mutual authentication to create the security context of the transport layer.

## 6.25 Solution #25: UE Onboarding for an SNPN with EAP-TLS

### 6.25.1 Introduction

This solution addresses key issue 4 "Securing initial access for UE onboarding between UE and SNPN". This solution describes how the UE performs the initial access to the O-SNPN (Onboarding SNPN) with the primary authentication between the UE and the O-SNPN using EAP-TLS to obtain the address of the PS (Provisioning Server) that is responsible for managing and distributing the credentials of the target SNPN. The actual provisioning mechanism from the PS to the UE is outside the scope of this solution. This solution aims at a deployment scenario in which a DCS only acts as a CA and as a function that de-conceals the SUCI so that the DCS can be lightweight.

### 6.25.2 Solution details

#### 6.25.2.1 General

In this solution as depicted in the figure 6.25.2.2-1, during the onboarding procedure the UE and the O-SNPN perform primary authentication using EAP TLS. To perform EAP-TLS between the UE and the O-SNPN the following fundamental approaches are applied in this solution.

The UE is pre-configured with:

- A UE certificate.

- An unique user identifier within the DCS domain in NAI (Network Access Identifier) format.

- All the necessary SUCI generation information including a list of public key(s) of the DCS and their corresponding identifier(s)

- The root or any intermediary CA certificates that can be used to authenticate the O-SNPN during the authentication procedure.

The O-SNPN:

- has a network certificate.

- obtains the root or any intermediary CA certificates that can used to authenticate the UE from the DCS during the authentication procedure.

It is assumed that the O-SNPN and the DCS have a business engagement so that the security sensitive information needed for the primary authentication can be transmitted between them securely. The actual interface between them is out of scope of this solution.

#### 6.25.2.2 Procedure



Figure 6.25.2.2-1: Remote UE onboarding procedure

0. The UE is pre-configured with an unique user identifier (SUPI) within the DCS domain in NAI format (e.g., user1@example.com), a UE certificate, the root or any intermediary CA certificates that can be used to authenticate the O-SNPN certificate during the primary authentication and the SUCI generation information including a list of public key(s) of the DCS and their corresponding identifier(s). The SUCI computation at UE and the SUCI de-concealment and validation at DCS are same as specified in TS 33.501 [2].

NOTE: The SUCI generation information is pre-configured together with UE certificate as described in clause 6.25.2.1. If no Routing Indicator is configured, this data field is set to the default value 0.

1. The UE selects O-SNPN for onboarding and sends Registration Request message to the AMF containing the SUCI. When computing a SUCI, the UE uses the provisioned public key of the DCS. Assuming the SUPI in NAI format provided by the DCS is user1@example.com, the routing indicator is 0 and the DCS's public key identifier is 15, the NAI format for the SUCI takes the form:

- For the Profile<A> protection scheme:

type1.rid0.schid1.hnkey15.ecckey<ECC ephemeral public key>.cip<encryption of user1>.mac<MAC tag value>@example.com

2. The AMF sends Authentication Request including the received SUCI to the AUSF and indicates that the UE is registering for onboarding.

3. The AUSF selects DCS based on the SUCI and requests information that is necessary to authenticate the UE. When requesting, the AUSF includes the UE's SUCI. It is assumed that there is a prior business relationship and a secure connection established between the AUSF and the DCS. The interface between AUSF and DCS can be defined via a NEF if the DCS is considered as AF, or via a NSSAAF if the DCS can support legacy protocols (e.g., Diameter).

4. The DCS finds the SUPI to identify the UE by de-concealing the received SUCI using its private key that is corresponding to the DCS's public key identifier. This implies that the DCS needs to mimic the role of SIDF/UDM with functionality related to SUCI de-concealment. Then the DCS retrieves the necessary information for the identified UE from its data base as follows and provides them along with the UE's SUPI to the AUSF of the O-SNPN:

1) The root or any intermediary CA certificates that can be used to authenticate the identified UE's certificate

2) The PS\_Address that can be used for the UE to ask credentials for the target SNPN later

5. With the received SUPI and the authentication information, the AUSF chooses EAP-TLS as the authentication method and performs the primary authentication with the UE as specified in TS 33.501 Annex B.2.1.1 (from step 6). The UE authenticates the O-SNPN with the certificates given in step 0, and the O-SNPN authenticates the UE with the certificates provided in step 5.

6. The AUSF sends the authentication result including the keying material, the SUPI and the PS\_Address to the AMF.

7. After performing the NAS SMC the AMF sends Registration Accept to the UE.

8. The AMF sends the PS address to the SMF during the PDU Session Establishment procedure.

### 6.25.3 System impact

UE:

- The UE needs to be provisioned by the DCS with some information that are required for primary authentication with O-SNPN

- When registering to O-SNPN for onboarding, the UE builds SUCI using the public key and other information provisioned by the DCS

- The UE needs to support authentication using EAP-TLS

AUSF:

- The AUSF needs to find DCS's address based on the SUCI

- The AUSF needs to retrieve the necessary information to authenticate the UE and the PS\_address for the UE from the DCS

- The AUSF needs to support authentication using EAP-TLS

AMF:

- The AMF sends the PS\_address to the SMF during the PDU Session Establishment procedure

### 6.25.4 Evaluation

This solution fulfils the potential security requirements of KI#4 and shows how the UE can be registered to the onboarding network with the DCS.

This solution provides mutual authentication between the UE and the O-SNPN.

The solution requires presence of the USIM to store public key(s) of the DCS and SUCI generation information.

The USIM aspects in this solution are neither fully developed nor evaluated

This solution provides the UE identifier privacy protection by encrypting the UE identifier to SUCI in NAI format using the pre-configured SUCI generation information. Applying the existing UE identifier privacy protection mechanism by omitting the username part from NAI as described in Annex B.2.1.2.2 in TS 33.501 [2] is not applicable in this solution as the DCS needs to identify the UE before it sends the root-of-trust certificates.

In this solution, the root-of-trust certificates need to be sent dynamically from the DCS to the AUSF for each UE authentication.

In this solution, the DCS only acts as a CA and as a function that supports de-concealment of the SUCI.

This solution requires the AUSF of the O-SNPN to be able to securely communicate with the DCS.

# 7 Conclusions

## 7.1 Conclusions on KI #1: Credentials owned by an external entity

For SUPI privacy, reuse existing mechanism in Annex I.5 in TS 33.501 [2].

In case that the external entity is 5GS aware (i.e., has the AUSF/UDM and is capable of deriving 5G key hierarchy after a successful primary authentication), it is concluded that the existing 5GS roaming architecture is reused.

In case that the external entity is non-5GS aware (legacy AAA server), the following is concluded:

- The SNPN access with a credential owned by an external entity is performed via an AUSF in the SNPN that selects a NSSAAF to interface with the external entity.

- When the legacy AAA server supports key deriving EAP method, the enhanced AUSF uses the MSK received from the AAA to derive the necessary 5G keys (e.g., KAUSF, KSEAF).

- If an SNPN uses an external entity that is a legacy AAA server supporting a key generating EAP method, it is strongly recommended that the same credentials that are used for authentication between UE and the 5G SNPN are not used for the authentication between the UE and a non-5G network, assuming that 5G SNPN and non-5G network are in different security domains, since MSKs obtained from the non-5G network could be used to impersonate the 5G SNPN towards the UE.

- The UE is provisioned with an indication that the key KAUSF needs to be derived from MSK instead of EMSK.

- For potential use of legacy AAA by an external entity (AAA-E) that does not support key generating EAP authentication method, EAP-TTLS as specified in RFC 5281 [5] can be described in an informative annex, with TLS tunnel terminating within the SNPN.

NOTE: Further conclusion(s) are not addressed in the present document.

## 7.2 Conclusions on KI #2: Provisioning of Credentials

It is concluded that user plane will be used for provisioning of SO-SNPN or PNI-NPN credentials in the present document. Definition in 3GPP of UP and CP provisioning protocols is out of scope of the present document.

## 7.3 Conclusions on KI #3: Security impacts from supporting IMS voice and IMS services in SNPNs

No normative work related to this key issue is concluded.

## 7.4 Conclusions on KI #4: Securing initial access for UE onboarding between UE and SNPN

For initial access for UE onboarding, the following authentication methods are concluded to be specified in normative work:

- Primary authentication between UE and AUSF in the O-SNPN as currently described in TS 33.501 [2], including Annex B. No interaction with DCS during primary authentication. Optionally, after primary authentication during the establishment of onboarding PDU session, O-SNPN can trigger secondary authentication with the DCS using default credentials as per clause 11.1 in 33.501 [2].

- Primary authentication with mutual authentication between UE and DCS. AUSF is involved. DCS can be AAA server, in that case NSSAAF is involved. DCS can also be external entity using AUSF/UDM.

- Primary authentication between the UE and DCS via AUSF using EAP-TTLS, as concluded in KI#1. AUSF is the EAP-TTLS server, and DCS is the AAA server.

NOTE 1: Further conclusion(s) are not addressed in the present document.

NOTE 2: Identity protection and/or privacy aspects during onboarding are not addressed in the present document.

## 7.5 Conclusions on KI #5: Roaming-related security mechanisms for SNPNs

Roaming-related security mechanisms for PLMNs are re-used whenever possible, and adapted to SNPNs with PLMN/SNPN as external entity when necessary. Solution #18 describes necessary changes to the token-based authorization procedure as currently specified in TS 33.501 [2].

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 |
| 2020-11 | SA3#101-e | S3-203400 |  |  |  | Version after incorporating changes from S3-202885, S3-203265, S3-203398, S3-203469, S3-203468, S3-203438, S3-203439, S3-203397 and S3-203401 | 0.3.0 |
| 2021-02 | SA3#102-e | S3-210780 |  |  |  | Version after incorporating changes from S3-210658, S3-210341, S3-210561, S3-210431, S3-210432, S3-210613, S3-210614, S3-210704, S3-210318, S3-210638, S3-210639, S3-210602, S3-210657, S3-210621, S3-210622, S3-210583, S3-210584, S3-210409, S3-210612, S3-210801, S3-210644, S3-210645 | 0.4.0 |
| 2021-03 | SA3#102bis-e | S3-211347 |  |  |  | Version after incorporating changes from S3-211301, S3-211233, S3-211259, S3-211244, S3-211187, S3-211302, S3-211283, S3-211005, S3-211206, S3-211077, S3-211260, S3-211314 | 0.5.0 |
| 2021-05 | SA3#103-e | S3-212220 |  |  |  | Version after incorporating changes from S3-212197, S3-212166, S3-212198, S3-211727, S3-211729, S3-211730, S3-211731, S3-211733, S3-212207, S3-212248, S3-212241 | 0.6.0 |
| 2021-09 | SA3#104-e | S3-213208 |  |  |  | Version after incorporating changes from S3-213066, S3-213082, S3-212558, S3-213070, S3-212689, S3-212733, S3-213147, S3-213042, S3-212969, S3-213065 | 0.7.0 |
| 2021-10 | SA3#104e ad-hoc | S3-213612 |  |  |  | Version after incorporating changes from S3-213608, S3-213625, S3-213611 | 0.8.0 |
| 2021-11 | SA3#105-e | S3-214362 |  |  |  | Version after incorporating changes from S3-214380, S3-214160, S3-214359, S3-214351, S3-213963, S3-214335, S3-214341, S3-214338, S3-214282, S3-214286 | 0.9.0 |
| 2021-12 | SA#94e | SP-211396 |  |  |  | Presented for information and approval | 1.0.0 |
| 2021-12 | SA#94e |  |  |  |  | EditHelp review and upgrade to change control version | 17.0.0 |
| 2022-03` | SA#95e | SP-220232 | 0001 | - | F | Editorials suggested by Edithelp | 17.1.0 |