|  |
| --- |
| 3GPP TR 33.858 V18.1.0 (2023-09) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of enhanced support of Non-Public Networks (NPN) phase 2(Release 18) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 9

3.3 Abbreviations 9

4 Assumptions 9

5 Key issues 9

5.1 Key issue #1: Security of non-3GPP access for SNPN 9

5.1.1 Key issue details 9

5.1.2 Threats 9

5.1.3 Potential security requirements 9

5.2 Key issue #2: Authentication for UE access to hosting network 10

5.2.1 Key issue details 10

5.2.2 Threats 10

5.2.3 Potential security requirements 10

6 Proposed solutions 11

6.0 Mapping of solutions to key issues 11

6.1 Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios 11

6.1.1 Introduction 11

6.1.2 Solution details 12

6.1.3 System impact 12

6.1.4 Evaluation 12

6.2 Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios 12

6.2.1 Introduction 12

6.2.2 Solution details 13

6.2.3 System impact 13

6.2.4 Evaluation 13

6.3 Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN 13

6.3.1 Introduction 13

6.3.2 Solution details 14

6.3.3 System impact 14

6.3.4 Evaluation 14

6.4 Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios 14

6.4.1 Introduction 14

6.4.2 Solution details 14

6.4.3 System impact 15

6.4.4 Evaluation 15

6.5 Solution #5: Anonymous authentication during connection establishment in trusted non-3GPP network access. 15

6.5.1 Introduction 15

6.5.2 Solution details 15

6.5.3 System impact 16

6.5.4 Evaluation 16

6.6 Solution #6: Trusted non-3GPP Access for SNPN 16

6.6.1 Introduction 16

6.6.2 Solution details 16

6.6.3 System impact 16

6.6.4 Evaluation 16

6.7 Solution #7: Untrusted non-3GPP Access for SNPN 16

6.7.1 Introduction 16

6.7.2 Solution details 17

6.7.3 System impact 17

6.7.4 Evaluation 17

6.8 Solution #8: Reusing Existing N3GPP Security for SNPN 17

6.8.1 Introduction 17

6.8.2 Solution details 17

6.8.3 Evaluation 17

6.9 Solution #9: NSWO support in SNPN using any key-generating EAP-method 18

6.9.1 Introduction 18

6.9.2 Solution details 18

6.9.3 System impact 19

6.9.4 Evaluation 19

6.10 Solution #10: Access to localized services using existing mechanisms 19

6.10.1 Introduction 19

6.10.2 Solution details 20

6.10.2.1 Solution for access to localized services based on Home Network Credentials 20

6.10.2.2 Solution for access to localized services based on Onboarding Mechanism 20

6.10.3 System Impact 22

6.10.4 Evaluation 22

6.11 Solution #11: High-level solution on authentication for UE access to hosting network 22

6.11.1 Introduction 22

6.11.2 Solution details 23

6.11.3 System impact 23

6.11.4 Evaluation 23

6.12 Solution #12: Localised service authentication through onboarding procedure and registration afterwards. 23

6.12.1 Introduction 23

6.12.2 Solution details 24

6.12.3 System impact 24

6.12.4 Evaluation 24

6.13 Solution #13: Home network primary authentication – secondary authentication towards localised service 25

6.13.1 Introduction 25

6.13.2 Solution details 25

6.13.3 System impact 25

6.13.4 Evaluation 26

6.14 Solution #14: NSWO support in SNPN using any key-generating EAP-method for SNPN using CH AUSF/UDM 26

6.14.1 Introduction 26

6.14.2 Solution details 26

6.14.3 System impact 26

6.14.4 Evaluation 27

6.15 Solution #15: NSWO using SNPN credentials from CH AAA 27

6.15.1 Introduction 27

6.15.2 Solution details 27

6.15.3 System impact 27

6.15.4 Evaluation 27

6.16 Solution #16: Localized Service related authentication and network access 27

6.16.1 Introduction 27

6.16.2 Solution details 28

6.16.3 System impact 29

6.16.4 Evaluation 29

6.17 Solution #17: Authentication for UE to access hosting network and receive localized services using existing mechanisms. 29

6.17.1 Introduction 29

6.17.2 Solution details 29

6.17.3 System impact 30

6.17.4 Evaluation 30

6.18 Solution #18: UE creates the identifier in trusted non-3GPP access 30

6.18.1 Introduction 30

6.18.2 Solution details 30

6.18.3 System impact 31

6.18.4 Evaluation 31

6.19 Solution #19: Supporting CH using AAA for N3GPP Security in SNPN 31

6.19.1 Introduction 31

6.19.2 Solution details 31

6.19.3 Evaluation 31

6.20 Solution #20: NSWO using SNPN credentials from CH AAA via 5GC 31

6.20.1 Introduction 31

6.20.2 Solution details 32

6.20.3 System impact 32

6.20.4 Evaluation 32

7 Conclusions 32

7.1 Conclusions for KI#1 Security of non-3GPP access for SNPN 32

7.1.1 Scope 32

7.1.2 Conclusion for Untrusted N3GPP access to SNPN 33

7.1.3 Conclusion for Trusted N3GPP access to SNPN 33

7.1.4 Conclusion for N5CW device access to SNPN 33

7.1.5 Conclusion for NSWO support in SNPN 34

7.2 Conclusions for KI#2 Authentication for UE access to hosting network 34

7.3 Other conclusions 34

Annex A: Change history 35

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# 1 Scope

The aim of the present document is to study the security aspects for any potential enhancements to be developed based on the outcome of the study in TR 23.700-08 [2]. For each of the objectives in the scope of the study in TR 23.700-08 [2], potential security aspects that are to be covered in this study are as follows:

- Support for enhanced mobility by enabling support for idle and connected mode mobility between SNPNs without new network selection.

- Study if existing security mechanisms for mobility between PLMNs can be reused for SNPNs or if new security mechanisms are needed.

- Support for non-3GPP access for SNPN

- Study if existing security mechanisms for enabling non-3GPP access in a PLMN can be reused for enabling non-3GPP access in an SNPN or if new security mechanisms are needed.

- Address new requirements (e.g., TS 22.261 [3] requirements for Providing Access to Local Services) related to NPN

- Study the trust model for the resulting architecture for enabling Localized Services via a local hosting NPN.

- Study if existing mechanisms for a UE to access an NPN can be reused for enabling a UE to authenticate with and access the local hosting NPN and the localized services via the hosting NPN with proper authorization, or if new security mechanisms are needed.

# 2 References

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

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

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

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

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

[2] 3GPP TR 23.700-08: "Study on enhanced support of Non-Public Networks; Phase 2".

[3] 3GPP TS 22.261: "Service requirements for the 5G system".

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

[5] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[6] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[7] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[8] NIST Special Publication 800-90A (2015): "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

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

[10] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[11] 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].

**Local service, Localized service:** Service, which is localized (i.e. provided at specific/limited area) and/or can be bounded in time. The service can be realized via applications (e.g. live or on-demand audio/video stream, electric game, IMS, etc), or connectivity (e.g. UE to UE, UE to Data Network, etc.) as defined in TR 23.700-08 [2].

**Hosting network:** A network providing access to Local/Localized services as defined in TR 23.700-08 [2].

## 3.2 Symbols

void

## 3.3 Abbreviations

void

# 4 Assumptions

void

# 5 Key issues

## 5.1 Key issue #1: Security of non-3GPP access for SNPN

### 5.1.1 Key issue details

TR 23.700-08 [2] studies "Key Issue #2: Support of Non-3GPP access for SNPN". Clause 5.2.1 of TR 23.700-08 [2] states: *"Currently the 3GPP specifications do not support direct connection to SNPN via non-3GPP access networks"* and *"One objective of this key issue is to enable the 5GS to support direct connection of non-3GPP access networks to the SNPN's 5GC."*

The intention of this key issue is to study if existing security mechanisms for enabling non-3GPP access in a PLMN can be reused for enabling non-3GPP access in an SNPN, or if new security mechanisms are needed.

### 5.1.2 Threats

If non-3GPP access in an SNPN does not provide mutual authentication between UE and SNPN, it is possible to impersonate the UE or SNPN.

If communication between UE and SNPN via non-3GPP access is not confidentiality, integrity or replay-protected, it is possible to disclose, tamper or replay the communication.

### 5.1.3 Potential security requirements

The 5G system shall provide the means for UE and SNPN to mutually authenticate if non-3GPP access is used.

The 5G system shall provide the means to confidentiality, integrity and replay protect communication between UE and SNPN, if non-3GPP access is used.

NOTE: Threats and requirements for devices that are not UEs (e.g. FN-RG or N5GC device behind RG) are not addressed in this document.

## 5.2 Key issue #2: Authentication for UE access to hosting network

### 5.2.1 Key issue details

The terms "localized service" and "hosting network" are explained in clause 3.1 of the present document.

TR 23.700-08 [2] studies "Key Issue #3: Enabling NPN as hosting network for providing access to localized services" and "Key Issue #4: Enabling UE to discover, select and access NPN as hosting network and receive localized services".

The intention of this key issue is to study authentication of UE access to a hosting network, if existing security mechanisms can be reused or new security mechanisms are needed.

### 5.2.2 Threats

If the UE is not authenticated towards the network, it is possible to impersonate the UE.

If the network is not authenticated towards the UE, it is possible to impersonate the network.

### 5.2.3 Potential security requirements

The UE and the hosting network shall support mutual authentication between the UE and the network.

# 6 Proposed solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |
| --- | --- | --- |
| Solutions | KI#1: Security of non-3GPP access for SNPN | KI#2: Authentication for UE access to hosting network |
| Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios | X |  |
| Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios | X |  |
| Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN | X |  |
| Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios | X |  |
| Solution #5: Anonymous authentication during connection establishment in trusted non-3GPP network access | X |  |
| Solution #6: Trusted non-3GPP Access for SNPN | X |  |
| Solution #7: Untrusted non-3GPP Access for SNPN | X |  |
| Solution #8: Reusing Existing N3GPP Security for SNPN | X |  |
| Solution #9: NSWO support in SNPN using any key-generating EAP-method | X |  |
| Solution #10: Access to localized services using existing mechanisms |  | X |
| Solution #11: High-level solution on authentication for UE access to hosting network |  | X |
| Solution #12: Localised service authentication through onboarding procedure and registration afterwards. |  | X |
| Solution #13: Home network primary authentication – secondary authentication towards localised service |  | X |
| Solution #14: NSWO support in SNPN using any key-generating EAP-method for SNPN using CH AUSF/UDM | X |  |
| Solution #15: NSWO using SNPN credentials from CH AAA | X |  |
| Solution #16: Localized Service related authentication and network access |  | X |
| Solution #17: Authentication for UE to access hosting network and receive localized services using existing mechanisms. |  | X |
| Solution #18: UE creates the identifier in trusted non-3GPP access | X |  |
| Solution #19: Supporting CH using AAA for N3GPP Security in SNPN | X |  |
| Solution #20: NSWO using SNPN credentials from CH AAA via 5GC | X |  |

## 6.1 Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios

### 6.1.1 Introduction

This solution addresses key issue #1.

TR 23.700-08 [2] studies "Key Issue #2: Support of Non-3GPP access for SNPN". Clause 5.2.1 of TR 23.700-08 [2] states: "*Currently the 3GPP specifications do not support direct connection to SNPN via non-3GPP access networks" and "One objective of this key issue is to enable the 5GS to support direct connection of non-3GPP access networks to the SNPN's 5GC.*"

To access to SNPN via no-3GPP access, on the one hand, the UE may need to handle the new identity (e.g., onboarding SUCI/onboarding SUPI) and the new Registration Type (i.e. SNPN Onboarding) to N3IWF. On the other hand, the UE may use anonymous value SUCI during the registration procedure, which will result in N3IWF failing to locate KN3IWF to authenticate the identity of UE.

This solution is proposed to address the aforementioned problem and enables the UE to access SNPN via an untrusted non-3GPP access network.

### 6.1.2 Solution details

This solution reuses the untrusted non-3GPP access authentication procedure in PLMN scenarios in clause 7.2.1 of TS 33.501 [4] with the following modifications:

- In SNPN scenarios, if the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports SUPI privacy, then the UE can send an anonymous value SUCI to N3IWF based on configuration. And SNPN identifier, which consists of PLMN ID and NID, should also be included in AN parameters, which are sent to the N3IWF. Moreover, to fulfil the onboarding requirements, the UE may also send onboarding SUCI to the N3IWF.

- The AMF can choose 5G AKA, EAP-AKA', or any other key-generating EAP authentication method to authenticate UE as described in clause 6.1.3 or clause I.2.2 of TS 33.501 [4].

- If EAP-AKA' or key-generating EAP authentication method is used for authentication as described in clause 6.1.3.1 and clause I.2.2 of TS 33.501 [4], the AUSF includes the EAP-Success in step 7.

NOTE: The need for including SUPI privacy is not addressed in the present document.

### 6.1.3 System impact

This solution has impact on N3IWF.

### 6.1.4 Evaluation

UE can send an anonymous value SUCI/onboarding SUCI to N3IWF based on configuration.

SNPN identifier is sent to the N3IWF.

The AMF can choose 5G AKA, EAP-AKA', or any other key-generating EAP authentication method to authenticate UE.

If EAP-AKA' or key-generating EAP authentication method is used for authentication, the AUSF needs to be able to send an EAP-Success message to AMF.

## 6.2 Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios

### 6.2.1 Introduction

This solution addresses key issue #1.

Specifically, in SNPN scenarios, the UE may register for onboarding, therefore the UE needs to send new registration type to TNAN. Moreover, TNGF may need to leverage IDi to identify KTNGF, which can authenticate the identity of the UE. And IDi can be set as the SUCI/onboarding SUCI. However, in some cases, the UE may send anonymous value SUCI to TNGF in the registration request, making TNGF not able to locally link the identity of the UE with the corresponding KTNGF. Without the mapping between UE identity and KTNGF, TNGF cannot authenticate the identity of the UE.

To access to SNPN, on the one hand, the UE may provide the new identity (e.g. onboarding SUCI/onboarding SUPI) and the new Registration Type (i.e. SNPN Onboarding) to TNAN. On the other hand, the UE may use anonymous value SUCI during the registration procedure, which results in the consequence that TNGF cannot locate KTNGF to authenticate the identity of UE.

This solution enables the UE to access SNPN via trusted non-3GPP access network.

### 6.2.2 Solution details

This solution reuses the authentication mechanism in clause 7A.2.1 of TS 33.501 [4] with the following modifications.

- The UE may send SUCI/onboarding SUCI to the TNAP/TNGF. If the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports SUPI privacy, then the UE can send an anonymous value SUCI to TNAP/TNGF. If the UE indents to access SNPN, AN parameters should also include SNPN identifier, which consists of PLMN ID and NID. The authentication mechanisms could be 5G AKA, EAP-AKA', and any other key-generating EAP authentication method as described in clause I.2 of TS 33.501 [4].

- For the IKE\_AUTH exchange part in step 13a of clause 7.2.1 of TS 33.501 [4], names in the ID payloads should correspond to the keys used to generate the AUTH payload. In case the UE utilizes the anonymous value SUCI in step 5, the UE initiates an IKE\_AUTH exchange and includes the hash of its SUPI in ID payloads rather than anonymous value SUCI. To help TNGF identify KTNGF, the AMF should send the newly generated KTNGF and the corresponding hash of the SUPI to the TNGF. The AMF may obtain the SUPI from the AUSF.

NOTE: The UE can only provide SUCI/Onboarding SUCI in case it is configured with SUPI privacy parameters.

### 6.2.3 System impact

This solution has impact on TNAP/TNGF.

### 6.2.4 Evaluation

UE can send an anonymous value SUCI /onboarding SUCI to TNAP/TNGF.

AN parameters including SNPN identifier should be sent to TNAP/TNGF.

For trusted non-3GPP Access in SNPN scenarios, the authentication mechanisms could be 5G AKA, EAP-AKA', and any other key-generating EAP authentication method as described in clause I.2 of TS 33.501 [4] should be supported

UE and TNGF leverages the hash of the SUPI to identify KTNGF when anonymous SUCI is employed in the EAP procedure.

The KTNGF identification mechanism has impacts on UE, AMF, and the TNGF.

In specific, the UE should be able to generate the hash of the SUPI.

The AMF should be able to generate and deliver the hash of the SUPI for the TNGF.

The TNGF should be able to locate the KTNGF via the hash of the SUPI.

This solution allows the UE to be tracked as the same hash value is sent each time

This solution allows TNGF to track the UE as the hash of the SUPI remains the same across connections

## 6.3 Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN

### 6.3.1 Introduction

This solution solves Key issue #1 in the case of using anonymous SUCI in trusted non-3GPP access.

When introducing non-3GPP access in SNPN it is assumed that most security procedures can be reused. However, the use of anonymous SUCI is only applicable to SNPNs so there are not yet any procedures specified for this case in relation to non-3GPP access.

In the current procedures for trusted non-3GPP access in clause 7A.2.1 of TS 33.501 [4], it is specified to use the SUCI/GUTI to map the user to the correct KTNGF in step 13. When using anonymous SUCI, this is not a good solution since an anonymous SUCI is not unique. Instead, another identifier is needed. This solution proposes to use a hash of the key KTNGF as identifier in case anonymous SUCI is used during the authentication towards the SNPN.

This solution defines adaptations of existing procedures needed to support the use of anonymous SUCI in trusted access for SNPN.

### 6.3.2 Solution details

Procedures in clause 7A.2.1 of TS 33.501 [4] are reused with the following exception:

- In step 13, if the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used, then a new type of identifier is used. The new identifier is proposed to be a hash of the key KTNGF. (potentially using some additional input). It is proposed to send the new identifier using the IDi payload.

It is already specified in section 3.5 of RFC 7296 [5] that the ID payload used for transport of IDi can be used to transfer a key identifier by setting the ID Type to ID\_KEY\_ID. Support of this ID Type is mandatory. The RFC does not specify how such a key identifier is generated. The proposal here is thus to use a hash of the key KTNGF potentially using some additional input to create a key identifier.

### 6.3.3 System impact

This solution has impact on UE and TNGF.

### 6.3.4 Evaluation

This solution solves Key issue #1 in the case of using anonymous SUCI in trusted non-3GPP access. If anonymous SUCI is not supported in trusted non-3GPP access, methods like EAP-TLS can only be used if the UE is also configured with a public key for SUCI concealment.

The solution requires that the TNGF decides that it is an anonymous SUCI and not a legacy SUCI or 5G-GUTI and generates a new KEY ID based on this decision

## 6.4 Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios

### 6.4.1 Introduction

This solution addresses key issue #1.

TR 23.700-08 [2] studies "Key Issue #2: Support of Non-3GPP access for SNPN". Clause 5.2.1 of TR 23.700-08 [2] states: "*Currently the 3GPP specifications do not support direct connection to SNPN via non-3GPP access networks" and "One objective of this key issue is to enable the 5GS to support direct connection of non-3GPP access networks to the SNPN's 5GC*."

Devices that do not support 5GC NAS signalling over WLAN access (referred to as "Non-5G-Capable over WLAN" devices, or N5CW devices for short) may access 5GC in a SNPN via a trusted WLAN Access Network that supports a Trusted WLAN Interworking Function (TWIF).

This solution enables N5CW to access SNPN via trusted non-3GPP WLAN Access Network.

### 6.4.2 Potential solution details

For N5CW device in a PLMN, the authentication procedure only include EAP-AKA', which is defined in clause 6.1.3.1 of TS 33.501 [4]. However, in SNPN scenarios, N5CW supports key-generating EAP authentication methods.

This solution reuses the authentication procedure in clause 7A.2.4 of TS 33.501 [4] with the following modifications.

- As described in clause I.2 of TS 33.501 [4], the authentication mechanisms utilized in step 8 of clause 7A.2.4 of TS 33.501 [4] should include key-generating EAP authentication methods.

- In step 2, NAI includes identifier of SNPN (i.e. PLMN ID and the NID of the SNPN).

- N5CW sends UE identity (e.g. SUCI/on boarding SUCI) and AN parameters to the TWAP/TWIF. And SNPN identifier, which consists of PLMN ID and NID, should be included in AN parameters. Moreover, in SNPN scenarios, if the construction of SUCI as described in clause 6.12 of TS 33.501[4] cannot be used and if the employed EAP method supports SUPI privacy, the UE can send an anonymous value SUCI based on configuration.

- If the UE is accessing 5GS for Onboarding, the AN parameters sent from UE to TWAP /TWIF needs to include Onboarding indication. And the Registration Type needs to be set as "SNPN Onboarding".

- The TWIF shall create a 5GC Registration Request message on behalf of the N5CW device. The TWIF needs to use UE identity, AN parameters, Registration Type that are received from N5CW.

NOTE 1: Whether onboarding for N5CW devices is in scope is not addressed in the present document.

NOTE 2: The need for including SUPI privacy is not addressed in the present document.

### 6.4.3 System impact

This solution has impact on TWAP/TWIF.

### 6.4.4 Evaluation

UE identity (e.g. SUCI/on boarding SUCI)/ anonymous value SUCI should be sent to the TWAP/TWIF.

SNPN identifier should be sent to TWAP/TWIF.

NAI sent to TWAP/TWIF should include the identifier of SNPN (i.e. PLMN ID and the NID of the SNPN).

## 6.5 Solution #5: Anonymous authentication during connection establishment in trusted non-3GPP network access.

### 6.5.1 Introduction

This is a solution to KI#1.

When a UE access a trusted non-3gpp access network, it used either SUCI or 5G-GUTI for identification. In case of an NPN deployment, the UE might use an anonymous SUCI when the EAP method supports its, as specified in TS 33.501 [4] clause I.5. The anonymous SUCI will protect the identity of the UE and makes it impossible to differentiate between a group of UE's using the same realm. As the authentication and key derivation steps are independent of the IPsec establishment, the TNGF cannot link the authentication and derived key to an IKE\_AUTH request – As the same identifier is used for multiple UE's.

This solution provides a method to fill the gap caused by introducing the anonymous SUCI which is already standardised in TS 33.501 [4] clause I.5. The solution proposes, that the TNGF creates a unique temporary identifier, shares it after authentication alongside other information necessary to establish the IPsec connection (e.g., TNGF address), to the UE. When the UE initiates the establishment of the IPSec channel, the UE uses the temporary identifier as identifier and thereby enables the TNGF to identify the correct key material (KTNGF) for the session.

The temporary identifier is only applicable when the anonymous identifier is used, therefore it is proposed as an optional parameter.

### 6.5.2 Solution details

Procedures in clause 7A.2.1 of TS 33.501 [4] are reused with the following exception:

- In step 9b, when an anonymous SUCI has been used in step 5, transfer a unique temporary identifier, allocated by the TNGF, to the UE alongside the TNGF address.

 - In step 13b, use the unique temporary identifier provided in step 9b as IDi, in case an anonymous identifier was used in step 5.

The allocation of a temporary identifier by the TNGF, distributed to the UE, enables the TNGF to identify the KTNGF which is used in the IKE\_AUTH procedure in step 13b and c.

### 6.5.3 System impact

This solution impacts TNGF and UE.

### 6.5.4 Evaluation

The solution fulfils the requirements for key issue #1 by extending the procedure in TS 33.501 [4] clause 7A.2.1 to encounter for the use of an anonymised SUCI/SUPI when concealment is not applicable. This gives a UE and SNPN the means to mutually authenticate and hereby confidentiality, integrity and replay protect the communication as stated in the requirements.

## 6.6 Solution #6: Trusted non-3GPP Access for SNPN

### 6.6.1 Introduction

This solution addresses key issue #1.

The normal trusted access procedures are used, only if the UE sends an anonymous SUCI, then the TNGF and the UE use the assigned IP address, which is unique within the TNGF, as identifier in the IDi according to RFC 7296.

### 6.6.2 Solution details

This solution reuses the trusted non-3GPP access authentication procedure in PLMN scenarios in clause 7A.2.1 of TS 33.501 [4] with the following modifications:

If the UE sends an anonymous SUCI in step 5 of the procedure, then the TNGF will use the IP address, which the TNGF assigns to the UE as unique identifier to bind the security key. In step 13, the UE includes the ID\_IPV4\_ADDR or ID\_IPV6\_ADDR with the assigned IP address in the IDi. The TNGF uses the received IP address to locate the KTIPSe for the connection.

### 6.6.3 System impact

This solution impacts TNGF.

This solution may impact the protocol between TNGF and TNAP.

### 6.6.4 Evaluation

The assigned IP address is unique within an TNGF and can be used as identifier to locate the security key.

The TNGF has to identify an anonymous SUCI and uses in that case the IP address of the UE to locate the key. Another issue is, the TNGF may not be always involved to assign the IP address according to the TS 23.502[7], thus the solution may need the TNAP to send the IP address of the UE to the TNGF when the TNAP is used to assign the IP address. Thus, it may impact to protocol used between TNAP and TNGF.

## 6.7 Solution #7: Untrusted non-3GPP Access for SNPN

### 6.7.1 Introduction

This solution addresses key issue #1.

The normal untrusted access procedures are used, only if the UE sends an anonymous SUCI, then the N3IWF assigns a unique identifier and the UE uses the unique identifier in the IDi when sending the IKE\_AUTH with AUTH.

### 6.7.2 Solution details

This solution reuses the untrusted non-3GPP access authentication procedure in PLMN scenarios in clause 7.2.1 of TS 33.501 [4] with the following modifications:

If the UE sends an anonymous SUCI in step 5 of the procedure, then the N3IWF assigns a unique identifier, which is unique within the N3IWF and used to bind the communication and the security key received in step 12. The N3IWF provides the assigned unique identifier to the UE in an IKE\_AUTH\_Response and the UE includes the unique identifier in the IDi when sending the IKE\_AUTH with AUTH in step 14. The N3IWF uses the received unique identifier to locate the KN3IWF for the connection.

### 6.7.3 System impact

The N3IWF assigns a unique identifier to the UE when sending an anonymous SUCI, the UE sends the unique identifier with the IKE\_AUTH with AUTH.

### 6.7.4 Evaluation

The identifier is unique within the N3IWF and used to bind the communication and the security key to the UE.

The IDi is the random number added by the UE to locate the KN3IWF in step3 of 7.2.1 of TS 33.501[2], thus, the existing procedure defined in clause 7.2.1 of TS 33.501 [2] can be reused.

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

## 6.8 Solution #8: Reusing Existing N3GPP Security for SNPN

### 6.8.1 Introduction

This solution addresses key issue #1 on Security of non-3GPP access for SNPN.

### 6.8.2 Solution details

For support of untrusted non-3GPP access for SNPN, it is proposed to reuse the security mechanisms defined in clause 7 in TS 33.501 [4].

For support of trusted non-3GPP access for SNPN, it is proposed to reuse the security mechanisms defined in clause 7A in TS 33.501 [4].

For support of wireline access for SNPN, it is proposed to reuse the security mechanisms defined in clause 7B in TS 33.501 [4].

For support of NSWO for SNPN, it is proposed to reuse the security mechanisms defined in Annex S in TS 33.501 [4].

NOTE: The solution does not address the case of anonymous SUCI.

### 6.8.3 Evaluation

This solution addresses the requirement of key issue #1.The solution is based on existing N3GPP Security mechanisms and procedures and hence has no additional standard impact.

This solution proposes to reuse trusted non-3GPP access defined in clause 7A in TS 33.501 [4] for SNPN. However, the existing solution defined in clause 7A in TS 33.501 [4] can only be used when SUPI or 5G-GUTI is used.

## 6.9 Solution #9: NSWO support in SNPN using any key-generating EAP-method

### 6.9.1 Introduction

This solution solves Key issue #1 in the case of NSWO using any key-generating EAP-method.

Current procedures for NSWO are only defined to use EAP-AKA'. This solution extends the NSWO procedures to be able to use any key-generating EAP-method in SNPN.

The proposed procedure is based on the current procedures in Annex S.2.3 of TS 33.501 [4]. The procedures assume access to subscribed SNPN.

### 6.9.2 Solution details



Figure 6.9.2-1: Authentication procedure for NSWO in SNPN

Steps 1-2 are performed as described in Annex S.3.2 of TS 33.501 [4].

Step 3 is performed as described in Annex S.3.2 of TS 33.501 [4] with the following addition: If the EAP method supports privacy and the UE is configured to use anonymous SUCI, the UE may send an anonymous value SUCI based on configuration.

Steps 4-6 are performed as described in Annex S.3.2 of TS 33.501 [4].

7. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF to de-conceal SUCI to gain SUPI.

Based on the subscription the UDM selects the appropriate EAP method to be used. The UDM includes an indicator of the selected EAP method and the SUPI to AUSF in a Nudm\_UEAuthentication\_Get Response message.

8. Authentication is performed between the AUSF and UE using the selected EAP method. After a successful authentication the AUSF derives the MSK key. The decision to use MSK instead of EMSK is based on the NSWO indicator received in step 5.

Steps 9-11 are performed as described in steps 16-18 of Annex S.3.2 of TS 33.501 [4].

### 6.9.3 System impact

The solution has impact on UE and AUSF. No impact on WLAN AP, NSWOF or UDM.

### 6.9.4 Evaluation

This solution solves Key issue #1 in aspect of supporting NSWO in SNPN that has AUSF/UDM. It reuses the procedures of Annex S of TS 33.501 [4] as much as possible adding the possibility of using any key-generating EAP-method. This addition affects the following steps of the procedure:

- Step 3: added possibility to use anonymous SUCI as described in clause 6.9.2

- Step 7: UDM selects EAP method based on configuration as described in clause 6.9.2

- Step 8: Authentication may be performed using any key generating EAP-method as described in clause 6.9.2

## 6.10 Solution #10: Access to localized services using existing mechanisms

### 6.10.1 Introduction

This solution addresses Key Issue #2 (Authentication for UE access to hosting network). The proposed solutions use existing mechanisms in 33.501 [4].

As per the conclusion in 23.700-08 [2], clause 8.4, when UE accesses the Hosting network using the subscription/credentials of its Home network, only two cases are considered:

- If the Home network is PLMN, the Hosting network can be PNI-NPN or SNPN.

- If the Home network is SNPN, the Hosting network can be only SNPN.

In both cases, solutions to these scenarios can be considered in the following categories

- UE uses home network credentials to access the hosting network.

- UE uses credentials obtained using the onboarding procedure as defined in 33.501[4] Annex I.9("Security of UE onboarding in SNPNs" to access the hosting network.

Note: Onboarding procedures only provide connectivity to obtain credentials. The credentials provisioning protocol is out of scope.

Following clause details how UE can use existing mechanisms and methodologies to access localized services.

### 6.10.2 Solution details

#### 6.10.2.1 Solution for access to localized services based on Home Network Credentials

To access the hosting network, the UE determines whether it can reuse home network credentials. As per 23.700-08 [2], the UE concludes that a home network credential can be utilized if the SNPN ID of the hosting network is contained in the SNPN priority lists connected with the home network subscription and the hosting network shows support for CH credentials. Existing 33.501 [4] primary authentication can be reused in this case. No normative work is needed from the SA3 WG perspective.

#### 6.10.2.2 Solution for access to localized services based on Onboarding Mechanism

Figure 6.10.2.2-1 shows a general overview of the access to localized services based on the onboarding mechanism. If UE uses credentials other home network credentials, then credentials obtained using the onboarding procedure as defined in 33.501 [4] Annex I.9 ("Security of UE onboarding in SNPNs" can be used to access the hosting network.



Figure 6.10.2.2-1: Overview of Access to localized services based on Onboarding Mechanism per Annex I.9.2 of TS 33.501 [4]

Figure 6.10.2.2-2 shows the procedures for access to localized services.



Figure 6.10.2.2-2: Procedures to Access localized services based on Onboarding

1. The Localized Service Provider (LSP) establishes a service agreement with the operator of a Hosting Network. The LSP also establishes a service agreement with the UE to enable the UE to receive the information needed to discover/access Hosting Network and the localized service. The hosting network is configured based on the service agreement, e.g., DNN/S-NSSAI configuration for access to localized service, QoS, number of end-users, time, location, whether home network services can be accessed via the hosting network, etc. The configuration of the Hosting Network is performed by means that are outside of the 3GPP scope. The UE performs the procedures defined in TS 23.502 to get the 5GC network access.

NOTE 1: In figure 6.10.2.2-2, the same network takes the role of the Onboarding network and then of the hosting network. Also, DCS can be involved in step 1c for primary authentication or as a part of step 2 (secondary authentication).

2. Localized service advertisements prompt UE's user using default credentials where UE authenticates with the DCS (e.g., per TS 33.501 [4] Annex I.9.2). The procedures are similar to the existing 23.501 [6] clause 5.30.2.10.2. e.g., After a successful onboarding procedure, the LSP sends a Security Profile corresponding to the UE and LSP certificate to the LSP access. The Security Profile associated with the LSP contains all the necessary data to establish a TLS tunnel between the LSP and UE.

NOTE 2: Aspects related to information configuration, such as PVS IP address and PVS FQDN, depend on WG SA2's conclusions.

3. After step 2, the UE needs to disconnect from the network (so far in the role of onboarding network) and reconnect again (now in the role of Hosting network). The user performs a selection of the Hosting Network. UE connects to the Hosting Network and is authenticated by the LSP in the role of Credential Holder (e.g., using a AAA server) using credentials downloaded in 2. UE requests a PDU Session and accesses the localized service of the LSP via the Hosting Network. Upon expiry of the time-restricted credentials, the LSP in the role of Credential Holder requests a release of the UE. When the localized service agreement is terminated, the Hosting Network removes the configured information by means that are outside of the 3GPP scope.

### 6.10.3 System Impact

For clause 6.10.2.1, there is not any system impact on existing security architecture per 33.501 [4].

For clause 6.10.2.2, the existing UE onboarding procedure cannot be used as is for access to localized services. As per 23.501 [6] clause 5.30.2.10.4.2 (Onboarding configuration for the UE), The PVS information, such as PVS IP address and PVS FQDN(s) provided by the onboarding network takes precedence over any such information stored in the UE. In contrast, the PVS information provided by the DCS takes precedence over the information stored in the onboarding network.

### 6.10.4 Evaluation

For clause 6.10.2.1, With the proposed solutions above, there is not any system impact on the existing security architecture per 33.501 [4]. The solution addresses key issue 2 and fulfils the requirements of mutual authentication between UE and the Hosting Network.

The solution considers two scenarios for UE access to the hosting network using the subscription/credentials of the home network:

- If the home network is a PLMN, the hosting network can be a PNI-NPN or a stand-alone network providing non-3GPP access (SNPN).

- If the home network is an SNPN, the hosting network can only be an SNPN.

In both cases, the UE has two options for accessing the hosting network:

- The UE can use home network credentials to access the hosting network, in which case existing primary authentication methods in TS 33.501 [4] can be reused.

- The UE can use credentials obtained through an onboarding procedure defined in Annex I.9 of TS 33.501 [4], which provides connectivity to obtain credentials. The credentials provisioning protocol is outside the scope of this solution. The solution addresses both cases where if UE is preconfigured with PVS address information and the UE receives PVS address information from the SMF during the PDU Session Establishment Accept message; the UE can determine based on local configuration whether to apply or ignore the PVS address information provided by the SMF.

## 6.11 Solution #11: High-level solution on authentication for UE access to hosting network

### 6.11.1 Introduction

This solution addresses Key Issue #2 "Authentication for UE access to hosting network". It provides a high-level exploration of the solution space, based on the analysis of the different possible use and business cases.

### 6.11.2 Solution details

The study in TR 23.700-08 [2] has considered different scenarios for UE access to hosting network. From an authentication point of view, the scenarios can be broadly classified into the following two cases:

1) There is a business relationship between hosting network and home network.

2) There is no business relationship between hosting network and home network.

For case 1), the business relationship between hosting network and home network can have different implications on the authentication architecture. At least the following cases are possible:

1a) Home network (PLMN or SNPN) is Credentials Holder using AUSF/UDM, hosting network is SNPN.

1b) Hosting network is PNI-NPN and home network is the underlying PLMN.

1c) Hosting network is PNI-NPN and the underlying PLMN has a roaming relationship with the home network.

For case 1a), the authentication to the hosting network is already specified in Annex I.2.4 of TS 33.501 [4]. For case 1b), the authentication to the hosting network can be based on the PLMN-credentials of the home network. Additional secondary or slice-specific authentication to access the hosting network is also possible. For case 1c), the authentication to the hosting network can also be based on the PLMN-credentials of the home network. In addition to primary authentication, secondary authentication to access the hosting network (PNI-NPN deployed by the VPLMN) is possible with local breakout.

For case 2), the following cases need to be considered:

2a) Hosting network is SNPN and does not have a business relationship with the home network.

2b) Hosting network is PNI-NPN and the underlying PLMN does not have a roaming relationship (or other business relationship) with the home network: This case does not seem to be possible, since PLMNs usually have a roaming relationship.

In case 2a), the UE needs new credentials to authenticate to the hosting network. Hosting network credentials can be provisioned to UE using existing user plane mechanisms, over visited or home network connectivity or using onboarding as specified in TS 23.501 [6] clause 5.30.2.10, TS 23.502 [7] clause 4.2.2.2.4 and TS 33.501 [4] Annex I.9. Onboarding requires default UE credentials to be pre-configured on the UE.

This solution structures the possible scenarios in a different way than in the conclusions in TR 23.700-08, clause 8.4.1.

### 6.11.3 System impact

The high-level solutions described in the solution details do not have normative specification impact.

### 6.11.4 Evaluation

This solution addresses the security requirements of Key Issue #2 "Authentication for UE access to hosting network". It does not require new normative work.

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

## 6.12 Solution #12: Localised service authentication through onboarding procedure and registration afterwards.

### 6.12.1 Introduction

This is a solution to KI#2.

The solution proposes to use the onboarding procedures defined in TS 33.501 [4] clause I.9 and TS 23.501 [6] clause 5.30.2.10 to provision the credentials, which afterwards are used to authenticate to the hosting network and hereby get access to the localised service.

The solutions assumes that the service provider and user have a service agreement and as part of that agreement the UE also have the default credentials provisioned. The license agreement and provisioning of default credentials is out of scope.

The onboarding of the UE is done towards the hosting network, which might host the DCS or the DCS can be located at the service provider. The hosting network enables the UE to get onboarded through the onboarding service provided, implying credentials to the hosting network/service is installed. In this solution the hosting network is not an PNI-NPN, as default credentials-based onboarding is not applicable because the UE already have a subscription for the HPLNM.

To access the localised service, the UE registers to the hosting network using the installed credentials.

### 6.12.2 Solution details

Procedures in this solution is based the procedures defined in TS 33.501 [4] clause I and TS 23.501 [6] clause 5.30.2.10 concerning UE onboarding.



1) The service provider and user contractual agrees to enable the service. This implies that the service provider, provides the UE with the default UE credentials. The provisioning of default UE credentials is out of scope.

2) The UE initiates an onboarding procedure towards the hosting network which in this case act like an onboarding network. The DCS may be hosted in the hosting network or by the service provider. The onboarding procedures follow the already standardised solution in TS 23 23.501 [6] clause 5.30.2.10 and TS 33.501 [4] clause I.9.

NOTE: Provisioning of credentials is out of scope.

3) The UE registers to the hosting network and authenticates using credentials provisioned in step 2. After registration the UE has access to the localised service.

### 6.12.3 System impact

No system impacts.

### 6.12.4 Evaluation

This solution fulfils the requirement in key issue #2 by utilising the onboarding procedure to provision credentials which then is used to mutual authenticate to the hosting network during registration to the hosting network.

## 6.13 Solution #13: Home network primary authentication – secondary authentication towards localised service

### 6.13.1 Introduction

This is a solution to KI#2.

This solution proposes to use home routed primary authentication towards the home network to establish the connection and secondary authentication towards the localised service provider to authenticate and get access to the service. The solution reuses already existing methods to authenticate the UE, namely home routed authentication, and local break out (break out from hosting network) secondary authentication towards the localised service provider.

### 6.13.2 Solution details

Procedures in this solution is based the procedures defined in TS 33.501 [4] clause 11 concerning secondary authentication.



Figure 6.13.2-1

1) The hosting network, home network and service provider agree on a service agreement.

2) The UE registers to the hosting network which “home routes” the authentication request to the home network which performs the primary authentication of the subscriber and establishes the key hierarchy as defined in TS 33.501 clause 6. The hosting network will act as a visited network and the home network as the home network.

3) The SMF in the hosting network will initiate the secondary authentication as described in TS 33.501 [4] clause 11, as defined for the local breakout configuration. The AAA can either be managed by the service provider or the hosting network.

### 6.13.3 System impact

No system impacts.

### 6.13.4 Evaluation

This solution fulfils the requirement in key issue #2 by primary authenticate with the home network to mutual authenticate the UE and establishing the root of the key hierarchy for the hosting network and afterwards provide the hosting network the capability secondary authenticate according to TS 33.501 clause 11 configured as local break out.

## 6.14 Solution #14: NSWO support in SNPN using any key-generating EAP-method for SNPN using CH AUSF/UDM

### 6.14.1 Introduction

This solution solves Key issue #1 in the case of NSWO using any key-generating EAP-method in SNPN with CH AUSF/UDM.

The proposed procedure is based on the current procedures for roaming in Annex S.4 of TS 33.501 [4].

### 6.14.2 Solution details

The description of NSWO for roaming defined in Annex S.4 of TS 33.501 [4] can be applied with the following adjustments:

- The procedures of Annex S.4 point to the roaming architecture options described in clause 4.2.15 in TS 23.501 [6].

- This roaming architecture is applicable by letting the Credential Holder taking the part of HPLMN. Figure 6.14.2-1 shows a modified version of Figure 4.2.15-3 of TS 23.501 [6], where HPLMN is replaced with CH and VPLMN is replaced by SNPN.

- The only impact on the SNPN is that it needs to deploy a AAA Proxy.

- The CH needs to deploy a NSWOF

- To be able to support all key-generating EAP-mechanisms, the procedures of Solution #9 of the present document can be applied on the proposed architecture.



Figure 6.14.2-1: Proposed roaming reference architectures to support authentication for Non-seamless WLAN offload in SNPN with CH AUSF/UDM

### 6.14.3 System impact

The solution has impact on UE (needs to support NSWO).SNPN needs to deploy AAA proxy and CH needs to deploy NSWOF.

### 6.14.4 Evaluation

This solution solves Key issue #1 in aspect of supporting NSWO in SNPN that deploys CH AUSF/UDM. It reuses the procedures of Annex S of TS 33.501 [4] as much as possible adding the possibility of using any key-generating EAP-method.

## 6.15 Solution #15: NSWO using SNPN credentials from CH AAA

### 6.15.1 Introduction

This solution addresses Key issue #1 in the case of NSWO using SNPN credentials from Credentials Holder AAA.

The proposed procedure is based on the current procedures for NSWO in Annex S.4 of TS 33.501 [4].

### 6.15.2 Solution details

In this solution, NSWO using SNPN credentials from CH AAA is achieved by reusing procedures defined in Solution 9 of the present document with following modifications:

- The WLAN AN can route the SWa messages directly to the CH AAA via AAA proxy instead of NSWOF/AUSF/UDM.

- The same key generating EAP method (including the SUPI/identifier privacy aspects) used by the SNPN over NG-RAN is reused over WLAN AN.



Figure 6.15.2-1: Reference architecture to support authentication for Non-seamless WLAN offload using SNPN credentials from CH AAA Server

NOTE: The ability to differentiate the authentication of the UE between NSWO case and primary authentication case has not been addressed in the present document.

### 6.15.3 System impact

The solution has impact on UE (needs to support NSWO over WLAN). SNPN/CH needs to deploy AAA proxy.

### 6.15.4 Evaluation

This solution solves Key issue #1 in case of the SNPN wants to reuse the credentials from CH AAA for NSWO. To support this architecture, Rel-17 NSWO can be reused and there is no specification impact on the entities involved in the 3GPP network side. Therefore, no normative work is expected.

## 6.16 Solution #16: Localized Service related authentication and network access

### 6.16.1 Introduction

The solution address KI#2.

### 6.16.2 Solution details

The solution covers the following different scenarios of authentication related to Providing Access to Localized Services (PALS) based on TR 23.700-08 [2].

Considering security aspects related to network access, the authentication scenarios can be broadly classified as two Cases based on the type of credentials used for the hosting network access authentication:

Case 1. The UE hosting network access relies on home network credentials.

1a: The hosting network can be PNI-NPN or SNPN and the home network is PLMN.

1b: The hosting network can be SNPN and the home network is SNPN

For both scenarios listed above, the UE can determine to use home network credentials basedonTR 23.700-08 [2] clause 8.4.5. The primary authentication for case 1 can be similar to TS 33.501 [4] Clause I.6 i.e., based on home network credentials. The primary authentication for case 1b can be based on TS 33.501[4] Clause I.2, the home network acts as credentials holder using AUSF/UDM. For the above two cases, as the UE uses home network credentials, the SUPI protection with SUCI can be achieved similar to TS 33.501 [4].

Case 2. The UE hosting network access relies on other credentials (e.g., preconfigured/provisioned using application layer outside the scope of 3GPP similar to localized service information preconfiguration described in TR 23.700-08 [2] Clause 8.4.3). For the following cases, it can be possible that the credential holder can hold the provisioned UE credentials to support hosting network access, further it can be possible that in case 2a, the SUPI protection using SIDF functions cannot be achieved due to lack of SIDF support at the localized server provider side, but the localized service provider offers other means to ensure SUPI privacy (i.e., for the NAI). Similarly in case 2b, it can be possible that the provisioned credentials do not include hosting network public key and related information to support non-null scheme SUCI generation even if the hosting network supports UDM with SID functionality.

2a: The hosting network can be the Onboarding network and the external credential holder can belong to the localized service provider.

2b: The hosting network can be the Onboarding network and the credential holder can belong to the hosting network itself.

For cases 2a and 2b, it is very essential to consider two main security aspects listed below:

1. The procedure defined in TS 33.501 [4] Clause I.2.2.2, uses anonymous SUCI whereas per TS 23.003 [9] Clause 2.2B, the username set to either the "anonymous" string or to an empty string. Where the first option is a static string and the later one is skipping the username part. In both cases, the main threat is that an end user can launch DDoS over the network, and the network will be able to identify the UE only after executing multiple round-trips of authentication related message exchanges leading to DDoS with flooding over the network.

2. According to TR 33.926 [10], Denial of service (DoS) attacks deny service to valid users, and it insists that, 'need to protect against certain types of DoS threats simply to improve system availability and reliability'. Further it states, 'A large number of compromised or misbehaving user equipments (UE) can cause a fault on the GNP with a consequent denial of service.'.

So, any security procedure including authentication procedure should take into account these finding to improve the security from the previous releases. Therefore, following aspects are proposed for cases 2a and 2b, if non-null schemes cannot be used for SUPI protection.

For Cases 2a and 2b if the SUPI privacy with non-null SUCI generation is not feasible, then it is proposed that, the credentials provisioned to the UE and the credential holder will contain an identifier (ID) which is associated to the actual SUPI related to the localized service subscription information. This ID do not leak any information about the UE/User (i.e., it can be anonymous or pseudonymous and it assignment is completely up to the localized service provider outside the scope of 3GPP). This ID is termed as digital identifier in general here in this solution. The UE while generating the null SUCI from the SUPI, the UE uses only the digital identifier as username part of the NAI to ensure SUPI privacy during primary authentication.

For NAI based SUPI, if the UE is provisioned with a digital identifier, then the UE can use the digital identifier as the username part of NAI for SUCI generation. The SUCI construction related to scheme Output can be same as described in TS 33.501 [4], but the SUPI type should be set as digital identifier based NAI type.

For case 2a, the AUSF/UDM can forward the SUPI, which is digital identifier username based NAI, further the external CH (e.g., AAA) can fetch associated subscription information and executes primary authentication as defined in TS 33.501 [4] Clause I.2.2.2.2.

For case 2b, the UDM on receiving the SUCI with SUPI type indicating 'digital identifier based NAI type', deconceals the SUCI as in TS 33.501 [4], fetches the SUPI (i.e., NAI SUPI) related to the digital identifier and continues with the existing authentication procedure defined in TS 33.501 [4].

*"As clearly stated in RFC 7542, the purpose of the NAI is to allow a user to be associated with an account name, as well as to assist in the routing of the authentication request across multiple domains. In alignment the proposal in this solution allows the NAI to use a digital identifier (i.e., available as part of the default credentials related to PALS service) in the username part which allows the external CH to find the default credentials related to the UE and initiate a suitable authentication. Further the realm part of the NAI facilitates to route to the right external CH."*

NOTE: As an option if required based on the configurations available in the default credentials, the NAI can be signed by the UE and the external CH can verify the sign., e.g., legacy AAA is already capable of doing this as covered in generic AAA architecture RFC 2903 [11].

### 6.16.3 System impact

For case 1, no impact as existing mechanism from TS 33.501 [4] is reused.

For case 2, the UE need to support an identifier which do not reveal any information about the UE to be used in username part of the NAI to access the network and to assist in identifying the credentials associated to the UE. The credential holder needs to fetch the actual subscription information/identifiers associated to the digital identifier to perform the authentication. As, this identifier needs to be routed via AMF and AUSF up to the external CH the related impact applies.

### 6.16.4 Evaluation

The solution proposes the usage of a pseudonymous SUCI for the case of onboarding. However, identifiers used during onboarding are generally only used once, since onboarding only happens once. Therefore, a pseudonymous SUCI is not needed in the case of onboarding.

## 6.17 Solution #17: Authentication for UE to access hosting network and receive localized services using existing mechanisms.

### 6.17.1 Introduction

This solution addresses KI #2: Authentication for UE access to hosting network.

### 6.17.2 Solution details

As per the conclusions of the study in TR 23.700-08 [2], it is up to UE to discover, select the hosting network, and decided what credentials are used to access hosting network.

From an authentication point of view, there are two types of cases for UE access to hosting network:

1) The UE accesses the Hosting network using the subscription/credentials of its Home network.

2) The UE accesses the Hosting network using the other credentials rather than the subscription/credentials from the UE Home network.

For case 1), The authentication method specified in in Annex I.2 of TS 33.501 [4] can be reused for UE access to SNPN as hosting network. Existing primary authentication can be reused for UE access to PNI-NPN as hosting network. In the case of PNI-NPN as hosting network using S-NSSAI, slice-specific authentication can also be used.

NOTE 1: Only UEs equipped with a USIM configured with PLMN credentials can access a hosting network which is a PNI-NPN. When the UE requests to access the hosting network, the home PLMN credential(s) are used during authentication procedure.

For case 2), The provisioning of Default credentials is out of scope, for example, it can be pre-configured on the UE. If the UE has Default credentials and the UE determines that new credentials for accessing hosting network are needed, the UE uses the Default credentials for the onboarding mechanism with the ON-SNPN acting as hosting network. The onboarding procedures are already specified in TS 23.501 [6] clause 5.30.2.10, TS 23.502 [7] clause 4.2.2.2.4 and TS 33.501 [4] Annex I.9 to provision the credentials.

NOTE 2: In case that the UE is preconfigured with PVS address information and the UE receives PVS address information from the SMF during the PDU Session Establishment Accept message, the UE may determine based on local configuration whether to apply or ignore the PVS address information provided by the SMF.

After having the access to the hosting network, the UE can receive localized services based on the services agreements between the hosting network and localized service provider.

### 6.17.3 System impact

This solution does not have system impacts.

### 6.17.4 Evaluation

This solution addresses the security requirements of KI #2: Authentication for UE access to hosting network.

It uses existing mechanisms, and does not require normative work.

## 6.18 Solution #18: UE creates the identifier in trusted non-3GPP access

### 6.18.1 Introduction

This solution addresses key issue #1.

When anonymous SUCI is used as IDi sent in the IKEv2 message, the TNGF cannot get the right Key KTGNF, because different UE may use the same anonymous SUCI. This solution proposes the UE creates a random number that is included in both AN parameter and IDi payload, and the N3IWF can use the existing logic to find the Key KTGNF.

### 6.18.2 Solution details

This solution reuses the trusted non-3GPP access authentication procedure in clause 7.2A.1 of TS 33.501 [4] with the following modifications:

- In step 5, when anonymous SUCI is used, the UE sets any random number into the UE ID of the AN parameters part.

NOTE 1: How to include the random number is not addressed in this solution, because it is in the scope of CT1. For example, CT1 may agree with a solution either put the UE ID together with the anonymous SUCI, or define a new IE.

- In step 13b, the UE sets the ID type as ID\_KEY-ID in this message and set its value equal to the random number as used in step 5.

NOTE 2: The random numbers assigned by different UEs may be the same, and the TNGF can mitigate this issue by implementation, for example by using a 64bit or 128bit random number which reduces the probability of collision.

### 6.18.3 System impact

The solution impacts on UE.

The solution may impact on TNGF due to the different potential designs of sending the UE ID.

### 6.18.4 Evaluation

This solution addresses KI#1 when the anonymous SUCI is used in trusted non-3GPP access by UE sets a random number in the AN parameter and IDi payload.

How to include the random number and whether it impacts on TNGF is stage3 work, thus this solution may or may not impact on the TNGF.

The random numbers assigned by different UEs may be the same, and the TNGF can mitigate this issue by implementation, for example, by using a 64bit or 128bit random number which reduces the probability of collision.

## 6.19 Solution #19: Supporting CH using AAA for N3GPP Security in SNPN

### 6.19.1 Introduction

This solution addresses key issue #1 on Security of non-3GPP access for SNPN.

### 6.19.2 Solution details

For untrusted non-3GPP access in SNPN, support for credential holder using AAA server for primary authentication between the UE and the AAA server**,** as specified in clause I.2.2.2 of TS 33.501 [4].

For trusted non-3GPP access in SNPN, support for credential holder using AAA server for primary authentication between the UE and the AAA server**,** as specified in clause I.2.2.2 of TS 33.501 [4].

For trusted WLAN access for N5CW devices in SNPN, support for credential holder using AAA server for primary authentication between the N5CW device and the AAA server**,** as specified in clause I.2.2.2 of TS 33.501 [4].

For NSWO in SNPN, support for credential holder using AAA server for primary authentication between the UE and the AAA server**,** can use the solution specified in clause 6.15 of the present document.

### 6.19.3 Evaluation

This solution addresses the requirement of key issue #1 by applying clause I.2.2.2 of TS 33.501 [4] for primary authentication to procedures in SNPN, including untrusted N3GPP procedure, trusted N3GPP procedure and trusted WLAN access procedure (N5CW devices).

This solution requires minimal normative work since it reuses existing specifications in TS 33.501 [4].

## 6.20 Solution #20: NSWO using SNPN credentials from CH AAA via 5GC

### 6.20.1 Introduction

This solution addresses Key issue #1 in the case of NSWO using SNPN credentials from Credentials Holder AAA.

The proposed procedure is based on the current procedures for NSWO in Annex S.4 of TS 33.501 [4] and for Credential Holder using AAA server for primary authentication in clause I.2.2.2 of TS 33.501 [4].

### 6.20.2 Solution details

Figure 6.20.2-1: Procedure for NSWO using SNPN credentials from CH AAA Server via 5GC

Steps 1-5 are performed as described in Annex S.3.2 of TS 33.501 [4], with the following addition: If the EAP method supports privacy and the UE is configured to use anonymous SUCI, the UE may send an anonymous value SUCI based on configuration. If the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports SUPI privacy, then the UE can send an anonymous SUPI based on configuration.

Steps 6-16 are replaced by steps 3-10 of clause I.2.2.2 of TS 33.501 [4], except in step 6 that an NSWO\_indicator is also sent to the UDM by the AUSF.

Remaining steps are performed as described in steps 16-18d of Annex S.3.2 of TS 33.501 [4].

### 6.20.3 System impact

The solution has no new impact on UE, WLAN AN, or 5GC.

### 6.20.4 Evaluation

This solution solves Key issue #1 when the credentials from CH AAA are used for NSWO.

It reuses Annex S.3.2 and clause I.2.2.2 of TS 33.501 [4], thus require minimal normative specification.

# 7 Conclusions

## 7.1 Conclusions for KI#1 Security of non-3GPP access for SNPN

### 7.1.1 Scope

TR 23.700-08 [2] has concluded in clause 8.2 that N3GPP access to SNPN includes the following types of access:

- Untrusted/Trusted N3GPP access including support for onboarding

- NSWO access to SNPN using SNPN credentials

The case of N5CW devices has not been addressed by TR 23.700-08 [2], but there are solutions for this case proposed in this study.

### 7.1.2 Conclusion for Untrusted N3GPP access to SNPN

Solution #1 is selected as basis for normative work for untrusted access to SNPN.

This means that the procedure specified in TS 33.501 [4] clause 7.2.1 will be reused for normative work with the following modifications:

- **Support for all key generating EAP-methods:** Extend the applicable authentication mechanism in steps 7 and 8 to key-generating EAP authentication methods

- **Support for onboarding**: Add possibility to send onboarding SUCI in step 5

- **Support for usage of anonymous SUCI**: Add possibility to send anonymous SUCI in step 5 (also affecting steps 6 and 7) if the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports privacy.

- **Support for credential holder using AAA server for primary authentication,** as specified in clause I.2.2.2 of TS 33.501 [4].

- Support for Credentials Holder using AUSF and UDM for primary authentication, as specified in clause I.2.4 of TS 33.501 [4].

### 7.1.3 Conclusion for Trusted N3GPP access to SNPN

The following is agreed as basis for normative work with regards to the aspects:

- Support for all key generating EAP-methods

- Support for usage of anonymous SUCI

- Support for onboarding

This implies that the procedure specified in TS 33.501 [4] clause 7A.2.4 will be reused for normative work with the following modifications:

- **Support for usage of anonymous SUCI:**

- Add possibility to send anonymous SUCI in step 5 (affecting also following steps 5-8) if the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports privacy.

- If the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used to identify the UE, the UE sends a 64-bit random number in step 5 and use this random number as key identifier in step 13. The random number generation by the UE should follow the recommendations given in SP 800-90A [13] or equivalent.

- If the TNGF cannot locate the UE (e.g., due to collision), the TNGF will reject the UE. The UE may retry with a new random number.

**- Support for all key generating EAP-methods:** Extension of applicable authentication mechanism in step 8 to key-generating EAP authentication methods.

**- Support for onboarding:** Add possibility to send onboarding SUCI in step 5

- **Support for credential holder using AAA server for primary authentication,** as specified in clause I.2.2.2 of TS 33.501 [4].

- Support for Credentials Holder using AUSF and UDM for primary authentication, as specified in clause I.2.4 of TS 33.501 [4].

### 7.1.4 Conclusion for N5CW device access to SNPN

Solution #4 is selected as basis for normative work with regards to the aspects:

- Support for all key generating EAP-methods

- Support for usage of anonymous SUCI if the construction of SUCI as described in clause 6.12 of TS 33.501 [2] cannot be used and if the employed EAP method supports privacy.

- Support for SNPN Id (PLMN Id and NID) carried in NAI

- Support for credential holder using AAA server for primary authentication, as specified in clause I.2.2.2 of TS 33.501 [4].

- Support for Credentials Holder using AUSF and UDM for primary authentication, as specified in clause I.2.4 of TS 33.501 [4].

### 7.1.5 Conclusion for NSWO support in SNPN

The solutions support usage of anonymous SUCI if the construction of SUCI as described in clause 6.12 of TS 33.501 [4] cannot be used and if the employed EAP method supports privacy.

Solution #9 is selected as basis for normative work with respect to the aspects of supporting NSWO in SNPN that has AUSF/UDM.

How the UDM selects authentication method in case of anonymous SUCI is to be specified as part of normative work.

Solution #14 is selected as basis for normative work with respect to the aspects of supporting NSWO in SNPN using a CH with AUSF/UDM.

Solution #15 is selected as basis for normative work with respect to the aspects of supporting NSWO in SNPN using SNPN credentials from CH AAA.

## 7.2 Conclusions for KI#2 Authentication for UE access to hosting network

Existing authentication procedures can be used for authentication for UE access to hosting network in the possible scenarios as concluded in TR 23.700-08 [2].

## 7.3 Other conclusions

Security of UE Onboarding in SNPNs as described in Annex I.9 of TS 33.501 [4] does not require the usage of anonymous SUCI.

Annex A:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e | S3-220957 |  |  |  | Skeleton | 0.0.0 |
| 2022-07 | SA3#107e AdHoc | S3-221674 |  |  |  | Version after incorporating changes from S3-221492 and S3-221681 | 0.1.0 |
| 2022-10 | SA3#108Adhoc-e | S3-223120 |  |  |  | Version after incorporating changes from S3-222931, S3-222965, S3-222990, S3-222931, S3-223118 | 0.2.0 |
| 2022-11 | SA3#109 | S3-224036 |  |  |  | Version after incorporating changes from S3-224034, S3-224035, S3-223804, S3-224037, S3-223669, S3-223668, S3-224043, S3-224044, S3-224045, S3-224046 | 0.3.0 |
| 2023-01 | SA3#109Adhoc-e | S3-230483 |  |  |  | Version after incorporating changes from S3-230429, S3-230431, S3-230432, S3-230521, S3-230318, S3-230382, S3-230383, S3-230384, S3-230453, S3-230490, S3-230523, S3-230444, S3-230445, S3-230460, S3-230461 | 0.4.0 |
| 2023-03 | SA3#110 | S3-231503 |  |  |  | Version after incorporating changes from S3-231501, S3-231502, S3-231533, S3-231534, S3-231535, S3-231504, S3-230995, S3-230991 | 0.5.0 |
| 2023-03 | SA#99 | SP-230134 |  |  |  | Presented for information | 1.0.0 |
| 2023-04 | SA3#110Adhoc-e | S3-232133 |  |  |  | Version after incorporating changes from S3-232170, S3-232143, S3-232223, S3-231757, S3-232136, S3-232137, S3-232109 | 1.1.0 |
| 2023-06 | SA3#111 | S3-233237 |  |  |  | Version after incorporating changes from S3-233402, S3-233403, S3-232828, S3-233235, S3-232908, S3-233404, S3-233236 | 1.2.0 |
| 2023-06 | SA#100 | SP-230574 |  |  |  | Presented for approval | 2.0.0 |
| 2023-06 | SA#100 |  |  |  |  | Upgrade to change control version | 18.0.0 |
| 2023-06 | SA#100 |  |  |  |  | EditHelp review | 18.0.1 |
| 2023-09 | SA#101 | SP-230893 | 0001 | - | F | Addressing comments from EditHelp | 18.1.0 |