3GPP TR 33.819 V16.1.0 (2020-07)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on security enhancements of 5G System (5GS) for vertical and Local Area Network (LAN) services;

(Release 16)

** 

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 Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [6](#__RefHeading___Toc45100288)

Introduction [7](#__RefHeading___Toc45100289)

1 Scope [8](#__RefHeading___Toc45100290)

2 References [8](#__RefHeading___Toc45100291)

3 Definitions of terms, symbols and abbreviations [8](#__RefHeading___Toc45100292)

3.1 Terms [8](#__RefHeading___Toc45100293)

3.2 Symbols [9](#__RefHeading___Toc45100294)

3.3 Abbreviations [9](#__RefHeading___Toc45100295)

4 Security aspects in the 5G System to enable enhanced support of Vertical and LAN Services [9](#__RefHeading___Toc45100296)

5 Key issues [10](#__RefHeading___Toc45100297)

5.1 Key Issues related to security for SNPNs [10](#__RefHeading___Toc45100298)

5.1.1 Key Issue #1.1: Completing AKA based authentication and calculating KSEAF for SNPNs [10](#__RefHeading___Toc45100299)

5.1.1.1 Key issue details [10](#__RefHeading___Toc45100300)

5.1.1.2 Security threats [10](#__RefHeading___Toc45100301)

5.1.1.3 Potential security requirements [10](#__RefHeading___Toc45100302)

5.1.1.4 Potential architectural requirements [10](#__RefHeading___Toc45100303)

5.2 Key Issues related to Security aspects on interworking between NPN and PLMN [10](#__RefHeading___Toc45100304)

5.2.1 Key Issue #2.1: Authentication and Authorization for Interworking, Roaming between NPN and PLMN [10](#__RefHeading___Toc45100305)

5.2.1.1 Key issue details [10](#__RefHeading___Toc45100306)

5.2.1.2 Security threats [11](#__RefHeading___Toc45100307)

5.2.1.3 Potential security requirements [11](#__RefHeading___Toc45100308)

5.2.2 Key Issue #2.2: Security and privacy aspects of service continuity and session continuity [11](#__RefHeading___Toc45100309)

5.2.2.1 Key issue details [11](#__RefHeading___Toc45100310)

5.2.2.2 Security threats [12](#__RefHeading___Toc45100311)

5.2.2.3 Potential security requirements [12](#__RefHeading___Toc45100312)

5.2.3 Key Issue #2.3: Independent credentials for authentication and authorization with NPN and PLMN [13](#__RefHeading___Toc45100313)

5.2.3.1 Key issue details [13](#__RefHeading___Toc45100314)

5.2.3.2 Security threats [13](#__RefHeading___Toc45100315)

5.2.3.3 Potential security requirements [13](#__RefHeading___Toc45100316)

5.3 Key Issues related to Security for 5G LAN services [13](#__RefHeading___Toc45100317)

5.3.1 Key Issue #3.1: Authentication and Authorization of UE in 5GLAN communication [13](#__RefHeading___Toc45100318)

5.3.1.1 Key issue details [13](#__RefHeading___Toc45100319)

5.3.1.2 Security threats [13](#__RefHeading___Toc45100320)

5.3.1.3 Potential security requirements [14](#__RefHeading___Toc45100321)

5.3.2 Key Issue #3.2: UP security policy for the 5GLAN Group [14](#__RefHeading___Toc45100322)

5.3.2.1 Key issue details [14](#__RefHeading___Toc45100323)

5.3.2.2 Security threats [14](#__RefHeading___Toc45100324)

5.3.2.3 Potential security requirements [14](#__RefHeading___Toc45100325)

5.4 Key Issues related to Security for TSC and 5GS interaction [14](#__RefHeading___Toc45100326)

5.4.1 Key Issue #4.1: Protection of interfaces that 5GS interacts with a TSN network [14](#__RefHeading___Toc45100327)

5.4.1.1 Key issue details [14](#__RefHeading___Toc45100328)

5.4.1.2 Security threats [15](#__RefHeading___Toc45100329)

5.4.1.3 Potential security requirements [15](#__RefHeading___Toc45100330)

5.4.2 Key Issue #4.2: TSC time synchronisation [15](#__RefHeading___Toc45100331)

5.4.2.1 Key issue details [15](#__RefHeading___Toc45100332)

5.4.2.2 Security threats [15](#__RefHeading___Toc45100333)

5.4.2.3 Potential security requirements [15](#__RefHeading___Toc45100334)

5.5 Key Issues related to authentication on NPNs [15](#__RefHeading___Toc45100335)

5.5.1 Key Issue #5.1: Key hierarchy for NPNs [15](#__RefHeading___Toc45100336)

5.5.1.1 Key issue details [15](#__RefHeading___Toc45100337)

5.5.1.2 Security threats [16](#__RefHeading___Toc45100338)

5.5.1.3 Potential security requirements [16](#__RefHeading___Toc45100339)

5.5.2 Key Issue #5.2: Authentication and authorization of NPN subscribers by an AAA [16](#__RefHeading___Toc45100340)

5.5.2.1 Key issue details [16](#__RefHeading___Toc45100341)

5.5.2.2 Security threats [16](#__RefHeading___Toc45100342)

5.5.2.3 Potential security requirements [16](#__RefHeading___Toc45100343)

5.6 Key Issues related to security for PNiNPNs [17](#__RefHeading___Toc45100344)

5.6.1 Key Issue #6.1: (D)DoS attack by large number of registration requests to CAG Cell [17](#__RefHeading___Toc45100345)

5.6.1.1 Key issue details [17](#__RefHeading___Toc45100346)

5.6.1.2 Security threats [17](#__RefHeading___Toc45100347)

5.6.1.3 Potential security requirements [17](#__RefHeading___Toc45100348)

5.6.2 Key Issue #6.2: CAG ID Privacy [17](#__RefHeading___Toc45100349)

5.6.2.1 Key issue details [17](#__RefHeading___Toc45100350)

5.6.2.2 Security threats [18](#__RefHeading___Toc45100351)

5.6.2.3 Potential security requirements [18](#__RefHeading___Toc45100352)

5.6.3 Key Issue #6.3: DoS attack by unauthorized removal of entries from the UE's Allowed CAG ID list [18](#__RefHeading___Toc45100353)

5.6.3.1 Key issue details [18](#__RefHeading___Toc45100354)

5.6.3.2 Security threats [18](#__RefHeading___Toc45100355)

5.6.3.3 Potential security requirements [19](#__RefHeading___Toc45100356)

6. Solutions [19](#__RefHeading___Toc45100357)

6.1 Solution #1: Solution for NPN network access via PLMN [19](#__RefHeading___Toc45100358)

6.1.1 Introduction [19](#__RefHeading___Toc45100359)

6.1.2 Solution details [20](#__RefHeading___Toc45100360)

6.1.2.1 Registration to NPN via PLMN [20](#__RefHeading___Toc45100361)

6.1.2.2 Registration to PLMN via NPN [21](#__RefHeading___Toc45100362)

6.1.3 Evaluation [21](#__RefHeading___Toc45100363)

6.2 Solution #2: Security solution for handling UP security policy for a 5GLAN Group [21](#__RefHeading___Toc45100364)

6.2.1 Introduction [21](#__RefHeading___Toc45100365)

6.2.2 Potential solution details [21](#__RefHeading___Toc45100366)

6.2.3 Evaluation [22](#__RefHeading___Toc45100367)

6.3 Solution #3: Security solution for mitigation of (D)DoS attack in PNiNPNs [22](#__RefHeading___Toc45100368)

6.3.1 Introduction [22](#__RefHeading___Toc45100369)

6.3.2 Potential solution details [22](#__RefHeading___Toc45100370)

6.3.3 Evaluation [24](#__RefHeading___Toc45100371)

6.4 Solution #4: Security solution for key derivation in SNPNs [24](#__RefHeading___Toc45100372)

6.4.1 Introduction [24](#__RefHeading___Toc45100373)

6.4.2 Solution details [24](#__RefHeading___Toc45100374)

6.4.3 Evaluation [24](#__RefHeading___Toc45100375)

6.5 Solution #5: Key hierarchy for authentication using non-AKA EAP methods in NPN [25](#__RefHeading___Toc45100376)

6.5.1 Introduction [25](#__RefHeading___Toc45100377)

6.5.2 Solution details [25](#__RefHeading___Toc45100378)

6.5.3 Evaluation [25](#__RefHeading___Toc45100379)

6.6 Solution #6: 5GLAN authentication [25](#__RefHeading___Toc45100380)

6.6.1 Introduction [25](#__RefHeading___Toc45100381)

6.6.2 Solution details [26](#__RefHeading___Toc45100382)

6.6.3 Evaluation [26](#__RefHeading___Toc45100383)

6.7 Solution #7: SMF handling the UP security policy for a 5GLAN Group based on information from DN AAA [26](#__RefHeading___Toc45100384)

6.7.1 Introduction [26](#__RefHeading___Toc45100385)

6.7.2 Potential solution details [27](#__RefHeading___Toc45100386)

6.7.3 Evaluation [27](#__RefHeading___Toc45100387)

6.8 Solution #8: TSC security [27](#__RefHeading___Toc45100388)

6.8.1 Introduction [27](#__RefHeading___Toc45100389)

6.8.2 Solution details [27](#__RefHeading___Toc45100390)

6.9 Solution #9: (D)DoS attack mitigation in PNiNPNs [27](#__RefHeading___Toc45100391)

6.9.1 Introduction [27](#__RefHeading___Toc45100392)

6.9.2 Solution details [27](#__RefHeading___Toc45100393)

6.9.3 Evaluation [28](#__RefHeading___Toc45100394)

6.10 Solution #10: Using NAS security for messages that modify the CAG list [28](#__RefHeading___Toc45100395)

6.10.1 Introduction [28](#__RefHeading___Toc45100396)

6.10.2 Solution details [28](#__RefHeading___Toc45100397)

6.10.3 Evaluation [29](#__RefHeading___Toc45100398)

6.11 Solution #11: DH based solution for CAG ID privacy [29](#__RefHeading___Toc45100399)

6.11.1 Introduction [29](#__RefHeading___Toc45100400)

6.11.2 Solution details [29](#__RefHeading___Toc45100401)

6.11.3 Evaluation [31](#__RefHeading___Toc45100402)

6.12 Solution #12: Hash based solution for CAG ID privacy [31](#__RefHeading___Toc45100403)

6.12.1 Introduction [31](#__RefHeading___Toc45100404)

6.12.2 Solution details [32](#__RefHeading___Toc45100405)

6.12.3 Evaluation [34](#__RefHeading___Toc45100406)

6.13 Solution #13: CAG ID Privacy in PNiNPNs by embedding CAG ID in the SUCI [34](#__RefHeading___Toc45100407)

6.13.1 Introduction [34](#__RefHeading___Toc45100408)

6.13.2 Solution details [35](#__RefHeading___Toc45100409)

6.13.3 Evaluation [36](#__RefHeading___Toc45100410)

6.14 Solution #14: CAG ID privacy by re-use of SUPI protection mechanism [36](#__RefHeading___Toc45100411)

6.14.1 Introduction [36](#__RefHeading___Toc45100412)

6.14.2 Solution details [36](#__RefHeading___Toc45100413)

6.14.3 Evaluation [37](#__RefHeading___Toc45100414)

6.15 Solution #15: CAG ID privacy by indication in RRC layer and providing CAG ID only after NAS security establishment [38](#__RefHeading___Toc45100415)

6.15.1 Introduction [38](#__RefHeading___Toc45100416)

6.15.2 Solution details [38](#__RefHeading___Toc45100417)

6.15.3 Evaluation [39](#__RefHeading___Toc45100418)

6.16 Solution #16: CAG ID privacy by sending CAG ID only in protected NAS signalling [39](#__RefHeading___Toc45100419)

6.16.1 Introduction [39](#__RefHeading___Toc45100420)

6.16.2 Solution details [39](#__RefHeading___Toc45100421)

6.16.3 Evaluation [40](#__RefHeading___Toc45100422)

6.17 Solution #17: Protection on TSC time synchronisation within UP security policy [40](#__RefHeading___Toc45100423)

6.17.1 Introduction [40](#__RefHeading___Toc45100424)

6.17.2 Solution details [40](#__RefHeading___Toc45100425)

6.17.3 Evaluation [40](#__RefHeading___Toc45100426)

6.18 Solution #18: CAG ID privacy considering RAN optimization [40](#__RefHeading___Toc45100427)

6.18.1 Introduction [40](#__RefHeading___Toc45100428)

6.18.2 Potential solution details [40](#__RefHeading___Toc45100429)

6.18.3 Evaluation [41](#__RefHeading___Toc45100430)

6.19 Solution #19: Privacy protected CAG ID Privacy in PNiNPNs [41](#__RefHeading___Toc45100431)

6.19.1 Introduction [41](#__RefHeading___Toc45100432)

6.19.2 Solution details [41](#__RefHeading___Toc45100433)

6.19.3 Evaluation [42](#__RefHeading___Toc45100434)

7 Conclusions [43](#__RefHeading___Toc45100435)

7.1 Security for 5G LAN services [43](#__RefHeading___Toc45100436)

7.2 Security for TSC [43](#__RefHeading___Toc45100437)

7.3 PLMN service access via SNPN and vice versa [43](#__RefHeading___Toc45100438)

7.4 Key hierarchy for NPNs [43](#__RefHeading___Toc45100439)

7.5 AKA based authentication and calculating KSEAF for SNPNs [43](#__RefHeading___Toc45100440)

7.6 Modification of CAG ID list in the UE [43](#__RefHeading___Toc45100441)

7.7 CAG ID Privacy [43](#__RefHeading___Toc45100442)

Annex A: Deployment options for authentication in SNPNs considering different types of NPN credentials [44](#__RefHeading___Toc45100443)

Annex B: Change history [46](#__RefHeading___Toc45100444)

# 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 present document covers 3 topics: 5GS support for Non-Public Network (NPN), 5G LAN-type services and Time Sensitive Communication.

An NPN is a 5GS deployed for non-public use, for details consult TS 22.261 [1]. As described in TS 23.501 [7], an NPN may be deployed as a Stand-alone Non-Public Network (SNPN), i.e. a network operated by an NPN operator and not relying on network functions provided by a PLMN, or a Public Network Integrated NPN, i.e. a non-public network deployed with the support of a PLMN.

5G LAN-type services are services that allow a set of UEs (5G LAN Group) to use private communication, i.e. providing services with similar functionalities to Local Area Networks (LANs) and VPN’s but improved with 5G capabilities.

Time Sensitive Communication (TSC) is a communication service that allows deterministic communication and/or isochronous communication with high reliability and availability by integrating transparently the 5G System as a bridge in an IEEE TSN network.

# 1 Scope

The present document studies security enhancements to 5GS that are required to fulfil Stage-1 service requirements in vertical domains defined in TS 22.261 [1] and TS 22.104 [2] and addresses the solutions described by TR 23.734 [3] and TR 23.725 [4] studies.

Potential security requirements are provided and possible security architecture enhancements to 5GS in vertical domains are proposed that support these security requirements.

# 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*.

[0] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[1] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[2] 3GPP TS 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[3] 3GPP TR 23.734: "Study on enhancement of 5GS for Vertical and LAN Services".

[4] 3GPP TR 23.725: "Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC)".

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

[6] 3GPP TS 23.502: "Procedures for the 5G System".

[7] 3GPP TS 23.501: "System architecture for the 5G System (5GS) ".

[8] 3GPP TR 23.740: "Study on Enhancement of Network Slicing".

[9] IEEE 802.1AS™: "IEEE Standard for Local and metropolitan area networks -Timing and Synchronization for Time-Sensitive Applications".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [0] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [0].

**Service Continuity**: Uninterrupted user experience of a service, including the cases where the IP address and/or anchoring point change (as defined in 3GPP TS 23.501 [7]).

**Session Continuity**: Continuity of a PDU Session (as defined in 3GPP TS 23.501 [7]).

NOTE: For PDU Session of IPv4 or IPv6 or IPv4v6 type "session continuity" implies that the IP address is preserved for the lifetime of the PDU Session.

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [0] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [0].

CAG Closed Access Group

gPTP generalized Precision Time Protocol

NPN Non-Public Network

SNPN Standalone NPN

PNiNPN Public Network integrated NPN

TSC Time Sensitive Communication

TCN Time Sensitive Network

# 4 Security aspects in the 5G System to enable enhanced support of Vertical and LAN Services

A Non-Public Network (NPN) is a 5GS deployed for non-public use, see TS 22.261 [1]. An NPN may be deployed as described in TS 23.501 [7] in more detail:

- a Stand-alone Non-Public Network (SNPN), i.e. operated by an NPN operator and not relying on network functions provided by a PLMN, or

- a Public Network integrated NPN (PNiNPN), i.e. a NPN deployed with the support of a PLMN.

SNPN 5GS deployments are based on the architecture depicted in TS 23.501 [7], clause 4.2.3, and the additional functionality covered in clause TS 23.501 [7], clause 5.30.2.

PNiNPN can be enabled using network slicing (see Annex D of 23.501 [7]). To prevent unauthorized UEs from trying to access a PNiNPN, the Closed Access Group (CAG) functionality described in clause 5.30.3 of 23.501 [7] can be used in addition.

Vertical and LAN Services features include:

- Time Sensitive Communication (TSC) service as described in clause 4.4.8 and 5.27 of TS 23.501 [7], and

- 5GLAN-type service as described in clause 4.4.6 and 5.25 of TS 23.501 [7] and further defined in clause 4.13.8 of TS 23.502 [6].

In the following clauses, key issues and potential solutions of security aspects of SNPN and PiNPN as well as the Vertical and LAN Services features are addressed.

Many aspects of TS 33.501 [5] also apply to NPNs and it was decided to not copy those into the present document, but directly provide the specification text for the related NPN clauses as will be mentioned in the conclusion section.

# 5 Key issues

## 5.1 Key Issues related to security for SNPNs

### 5.1.1 Key Issue #1.1: Completing AKA based authentication and calculating KSEAF for SNPNs

#### 5.1.1.1 Key issue details

Binding the key to the serving network identity is a requirement for 5G security [1]. For SNPNs, the network identity used (see solution #1 in TR 23.734 [3]) is changed and may not even contain a complete PLMN ID. Hence the standard needs to clearly define the input parameters used to calculate KSEAF as well as KAUSF, RES\* and XRES\* for 5G AKA and IK' and CK' for EAP-AKA' in both the network and UE. Without such a clear definition the security set-up will fail.

When introducing SNPNs, it should also be ensured that the SNPN cannot masquerade as a public network, i.e., the keys derived for a public network and SNPN are different.

#### 5.1.1.2 Security threats

If using the same credentials for more than one network, the UE may be connected to a different standalone public network than the one it tried to connect to.

The UE may be connected to a SNPN when it tried to connect to a public network.

#### 5.1.1.3 Potential security requirements

The UE shall authenticate the serving SNPN identifier.

#### 5.1.1.4 Potential architectural requirements

The system shall support well-defined key derivations to enable the establishment of security for SNPNs.

## 5.2 Key Issues related to Security aspects on interworking between NPN and PLMN

### 5.2.1 Key Issue #2.1: Authentication and Authorization for Interworking, Roaming between NPN and PLMN

#### 5.2.1.1 Key issue details

There is a need for 5GS to support non-public operations for an enterprise using Non Public Networks (NPN) deployed in plants or factories. The envisioned deployment options for NPN are: standalone, hosted by a PLMN or a slice from a PLMN.

The purpose of this key issue is to identify specific issues for authentication and authorization when a UE needs to access and obtain services offered from a PLMN via a NPN and vice versa. Where a roaming agreement between a PLMN operator and an NPN operator allow, it need to be studied what security model could be adopted with authentication in both networks or authentication in only one of the networks, e.g. if a PLMN need to authenticate a UE for network access and to grant service over PLMN network.

In this key issue, a UE authentication with a PLMN (using credentials needed for PLMN) is called "PLMN Authentication" and with NPN (using credentials needed for NPN) is called "NPN Authentication".

This key issue assumes that:

- Authentication methods, identities, credentials for PLMN access are 3GPP only.

- NPN may or may not be considered trusted by PLMN.

- PLMN is considered trusted by NPN.

- PLMN Authentication is mandatory to access PLMN offered services via NPN.

The security aspects of authentication and authorization for PLMN and NPN interworking and roaming (including simultaneous access) are as follows:

- The UE identifier used for NPN Authentication.

- The NPN Authentication may use 3GPP or non 3GPP based credentials (e.g. using the EAP framework).

- When a UE is already authenticated/registered with the PLMN, an additional NPN authentication may or may not be performed to access and obtain NPN services via the PLMN.

#### 5.2.1.2 Security threats

Access of UEs to NPN offered services via PLMN unauthorized by NPN and/or PLMN.

Access of UEs to PLMN offered services via NPN unauthorized by NPN and/or PLMN.

#### 5.2.1.3 Potential security requirements

It is concluded that no normative work for this key issue is required since it is already addressed by the existing specification. Thus, potential security requirements for this key issue are not addressed in the present document.

### 5.2.2 Key Issue #2.2: Security and privacy aspects of service continuity and session continuity

#### 5.2.2.1 Key issue details

**Background**

Clause 3.1 of the present document contains definition of service continuity and session continuity, as specified in 3GPP TS 23.501 [7].

Service continuity and session continuity do not mean transfer of service and session from PLMN to NPN and vice-versa. The continuity is in the sense of transfer from native connective to tunnelled connection, and vice-versa. In other words, there is no "roaming" (in the same sense that it is used across PLMNs) between PLMN and NPN.

3GPP TS 23.734 uses the term service continuity in its key issues and solutions. That is fine because support for service continuity would cater session continuity as well. Regarding the key issue #6, i.e., access to PLMN services via NPN and vice-versa, 3GPP TS 23.734 [3] has concluded that solution #20 is chosen as baseline for normative work. Further, it has also concluded (according to solution #21) that seamless service continuity between PLMN and NPN is achieved by dual radio support and there no protocol changes.

In short, the chosen solution #20 works in the following way - one network (PLMN or NPN) treats another network (NPN or PLMN) as a non-3GPP access and tunnels communication using another network's N3IWF. See Figure 5.2.2.1-1.

|  |  |
| --- | --- |
|  |  |
| Figure 5.2.2.1-1: Baseline architecture for accessing PLMN via NPN (left) and NPN via PLMN (right) | |

**Description**

This key issue is about investigating security aspects of service and session continuity when accessing PLMN services via NPN and vice-versa. In other words, this key issue is for analysing IF and WHAT "new" security mechanisms would be required for the solution #20 in 3GPP TS 23.734 [3].

There are several aspects that are worth investigating for security and privacy impacts, e.g., because of:

- Nwu interfaces (NwuPLMN and NwuNPN) between UEs and PLMN/NPN N3IWFs;

- both the PLMN and the NPN having own security contexts for UEs even though a single radio is used;

- UEs discovering one network's N3IWF via another network's radio;

- UEs performing PDU Session(s) handover from NPN N3IWF to NPN 3GPP RAN, and PLMN 3GPP RAN to PLMN N3IWF;

- UEs performing PDU Session(s) handover from PLMN N3IWF to PLMN 3GPP RAN, and NPN 3GPP RAN to NPN N3IWF;

- etc.

#### 5.2.2.2 Security threats

It is concluded that no normative work for this key issue is required, since it is addressed by the existing specification. Thus, security threats for this key issue are not addressed in the present document.

#### 5.2.2.3 Potential security requirements

It is concluded that no normative work for this key issue is required, since it is addressed by the existing specification. Thus, potential security requirements for this key issue are not addressed in the present document.

### 5.2.3 Key Issue #2.3: Independent credentials for authentication and authorization with NPN and PLMN

#### 5.2.3.1 Key issue details

As per TR 23.734 [3], the possible deployment options for NPNs are: standalone, hosted by a PLMN or a slice from a PLMN. For standalone deployment option, study concludes solution #20 ("Supporting service continuity between Public PLMN a NPN via an N3IWF-like gateway") for key issue #6 related to service continuity ("Accessing PLMN service via NPNs and vice versa").

This key issue is related to support of credentials, for authentication and authorization when a UE needs to access and obtain services offered from a PLMN via a NPN and vice versa.

As per the concluded solution in TR 23.734 [3], to access PLMN services via NPN, UE obtains IP connectivity via the NPN, discovers a N3IWF provided by PLMN, and establishes connectivity to the PLMN via the N3IWF. Similar procedure to be followed by UE vice versa, to access NPN services via PLMN. PLMN and NPNs are different networks that UE will be connected to simultaneously.

For PLMN networks, 5G AKA and EAP-AKA' are supported authentication methods. For NPNs (Private networks) using 5G system, supported authentication methods are 5G AKA, EAP-AKA' and additional methods within EAP framework TS 33.501. UE and NPN need to be in possession of the security credentials corresponding to the authentication method (over EAP framework) used for primary authentication, based on the NPN operator policy.

#### 5.2.3.2 Security threats

The PLMN and NPNs should provide mutual authentication mechanism to ensure that the network services are provided only to the UEs with valid subscription. If same credential is shared for the PLMN network access and also for the NPN network(s) access, then compromise of the security credential at the UE or at any network entity, can lead to compromise of all other network, which shares the same credential.

#### 5.2.3.3 Potential security requirements

The 5G system should support subscription credentials for the NPN network access authentication and authorization that are independent of the credentials used to access the PLMN.

The system shall support (but not mandate) the use of independent subscription credentials for access to different NPN networks.

## 5.3 Key Issues related to Security for 5G LAN services

### 5.3.1 Key Issue #3.1: Authentication and Authorization of UE in 5GLAN communication

#### 5.3.1.1 Key issue details

TR 23.734, Clause 5.4.1 [3] describes a key issue #5: 5GLAN Group Management, which raises an issue on "how to authorize a UE for 5GLAN communication". Also Figure 6.14.2-2 [3] depicts the procedure for 5GLAN group discovery and configuration through registration.

Therefore, this new key issue is proposed to provide necessary detailed security procedures in order to support authentication and authorization for 5GLAN group communication. If this issue is not addressed, it may lead any illegitimate UE to gain access to the 5GLAN type services without any authentication and authorization.

#### 5.3.1.2 Security threats

The 5GLAN services are different from the public network services, the system should provide a mutual authentication and authorization mechanism to ensure that these 5GLAN services will be provided to only the UE's subscribed to the 5GLAN group. If the 5GLAN UE is not authenticated and authorized, then any illegitimate UE may get the 5GLAN-type services provided by 5GLAN group which were not subscribed to these services. It can also lead to risk of theft of service and Denial of Service against the 5GLAN group communication.

#### 5.3.1.3 Potential security requirements

Mutual authentication mechanism between 5GLAN UE and 5GLAN group shall be supported.

Authorization of 5GLAN UE's for 5GLAN-type services in 5GLAN group shall be supported.

### 5.3.2 Key Issue #3.2: UP security policy for the 5GLAN Group

#### 5.3.2.1 Key issue details

This key issue addresses the security aspects of key issue #4.1: 5GLAN Group Management in TR 23.734 [3].

TR 23.734 [3] has recommended solution #29 "Unified architecture for 5G LAN-type service" for the normative work for 5GLAN group communication.

PDU sessions established by different UE's belonging to one and the same 5GLAN group will be handled by the same SMF. The SMF is responsible for managing the PDU sessions belonging to the 5GLAN group, for example it includes the management of the total number of established and activated PDU Sessions.

During the PDU session establishment, the 5G Core Network determines and provide the UP security policy for a PDU session to the gNB connected to 5GC according to TS 23.501 [7] and TS 23.502 [6]. This key issue investigates whether there is a problem if the 5G Core Network enforce different configurations of UP security (encryption and integrity protection) in the UP security policy for multiple PDU sessions established with different UE's belonging to one and the same 5GLAN Group.

#### 5.3.2.2 Security threats

If the user plane traffic sent between the UE and the gNB for one PDU session is using lower security then the other PDU sessions for the other UE's belonging to the same 5GLAN group, then this would imply that the security for the weakest link applies to the whole 5GLAN group. In summary, the security properties of the group communication are determined by the security properties of the weakest communication path.

For example: if encryption is switched off between the UE and the gNB for one PDU session over one path, while all other communication paths between all other UE's and RAN nodes within the same 5GLAN group are encrypted, then the effect is that all the information exchanged within the 5GLAN group will be eavesdropped. Or if the attacker knows that integrity protection is enabled on one path between the UE and the gNB but not on a second path between a second UE and a gNB, then the attacker could insert or modify user plane data for group communication within the 5GLAN group sent over the second path.

#### 5.3.2.3 Potential security requirements

The system shall support a single security user plane policy for a 5GLAN group.

## 5.4 Key Issues related to Security for TSC and 5GS interaction

### 5.4.1 Key Issue #4.1: Protection of interfaces that 5GS interacts with a TSN network

#### 5.4.1.1 Key issue details

5GS may integrate with Time Sensitive Networking (TSN) as defined by IEEE 802.1Q, a technology that provides deterministic messaging on standard Ethernet. Time Sensitive Communication (TSC) as defined in TS 23.501 [7] allows the 5G System to be integrated transparently as a bridge in an external IEEE TSN network. 5G System specific procedures in 5GC and RAN, wireless communication links, etc. remain hidden from the TSN network. To achieve such transparency to the TSN network and the 5GS to appear as any other TSN Bridge.

This "logical" TSN bridge includes TSN Translator functionality for interoperation between TSN System and 5G System both for user plane and control plane. 5GS TSN translator functionality consists of Device-side TSN translator (DS-TT) and Network-side TSN translator (NW-TT). The 5GS provides multiple interfaces to external services/networks that can be used for integration of 5GS as a TSN bridge, such as N5, N6, N33. The interfaces interact with the TSN network need to be properly protected.

#### 5.4.1.2 Security threats

In case the interfaces interact with a TSN network lack confidentiality, integrity and replay protection, it will be possible for an attacker to eavesdrop, modify data and replay packets.

#### 5.4.1.3 Potential security requirements

The interfaces interacting with a TSN network shall support confidentiality, integrity and replay protection.

### 5.4.2 Key Issue #4.2: TSC time synchronisation

#### 5.4.2.1 Key issue details

Time synchronisation is essential for the 5GS providing the TSC service. The time synchronisation mechanisms for the 5GS as IEEE bridge in TSN are shown in the figure of clause 5.27 in 23.501 [7].

gPTP (Generalized Precision Time Protocol) messages [9] are needed for the time synchronisation over the 5GS as IEEE bridge in the TSN. They are transmitted in the user plane between the ingress and egress boundaries involving then the DS-TT, the UE, the gNB, the UPF and the NW-TT.

The transfer of gPTP messages need to be protected.

#### 5.4.2.2 Security threats

The intrinsic timing aspects that a 5GS Bridge as a TSN Bridge need to support may provide ground for vulnerabilities like:

- Blocking the deterministic transmission with strict latencies boundaries.

- Manipulation of the clock synchronization between NW elements (Master/Slave) and with global time reference (Grand Master).

- Manipulation of Time aware Scheduling and traffic shaping.

- Manipulation to the selection of communication paths and reservation of bandwidth and time slots.

#### 5.4.2.3 Potential security requirements

The transfer of gPTP messages should support integrity, confidentiality protection and anti-replay protection.

## 5.5 Key Issues related to authentication on NPNs

### 5.5.1 Key Issue #5.1: Key hierarchy for NPNs

#### 5.5.1.1 Key issue details

The current key hierarchy in TS 33.501 [5] assumes that an AKA method is used to authenticate the UE. This will not necessarily be true for NPNs. In particular, non-AKA methods do not require the long-term key K to be stored in UE and network and derivation of KAUSF from an EAP-based authentication other than EAP-AKA' is not described.

#### 5.5.1.2 Security threats

With a lack of clarity on how general EAP based authentication methods (i.e. ones other than EAP-AKA') result in the creation of the 5G key hierarchy, it is possible that incompatible UE and network implementation may occur.

#### 5.5.1.3 Potential security requirements

From the above security threats, the following requirements can be drawn:

- The key hierarchy shall support EAP-based authentication methods other than EAP-AKA'.

NOTE 1: This requirement takes no stance on whether this support is described normatively or informatively.

NOTE 2: This requirement will not change the key hierarchy for primary authentication in public networks.

### 5.5.2 Key Issue #5.2: Authentication and authorization of NPN subscribers by an AAA

#### 5.5.2.1 Key issue details

In the 5G System, the authentication credentials are stored and processed in the UDM/ARP as described in TS 33.501 [5]. For standalone NPNs, it is understood that it is recommended not to have any restriction on the credentials and the authentication methods. This is since the NPN operators might already have their own identity and credential management systems, typically legacy AAA infrastructures for authentication and authorization of the devices or the users.

Now in order to allow the use of any authentication credentials and methods, the common practise was to support an interaction with a AAA entity. This is for example what has been done for the Secondary Authentication where the SMF interacts with an external AAA entity in the DN. This is also what was adopted in the slicing enhancement study captured in TR 23.740 [8] and where it is assumed that the AUSF interacts with AAA entity for the slice specific authentication procedure.

Introducing such a feature in the 5G System for the Primary Authentication would have considerable impact on the UE. In fact, if the AUSF is to interact with AAA entity, and endorse an authenticator role instead of the server role in the EAP framework, then the key hierarchy needs to be revised for this use case so that the KAUSF is derived from the MSK instead of the EMSK key.

For that, the focus of this key issue is to whether it is possible and if yes how to allow such an interaction with AAA while preserving the current role of the AUSF and the UDM in the Primary Authentication framework as described in TS 33.501 [5].

#### 5.5.2.2 Security threats

Security threats for this key issue are not addressed in the present document.

#### 5.5.2.3 Potential security requirements

Potential security requirements for this key issue are not addressed in the present document.

## 5.6 Key Issues related to security for PNiNPNs

### 5.6.1 Key Issue #6.1: (D)DoS attack by large number of registration requests to CAG Cell

#### 5.6.1.1 Key issue details

To enable NPNs deployed as part of a PLMN, TR 23.734 [3]) concludes Solution #2 (Closed Access Group) as the basis for normative work, to address the Key Issues (key Issue #1: Network discovery, selection and access control for NPNs and Key Issue #2: Network Identification for NPNs in TR 23.734 [3]).

PNiNPNs are NPNs (NPNs) which are deployed with the support of public PLMNs using Closed Access Group (CAG) and/or network slicing. When an NPN is made available via a PLMN, then the UE has a subscription for the PLMN to access the network and obtain the services provided by the network. A CAG identifies a group of subscribers who are permitted to access one or more CAG cells. When an UE accesses a CAG cell, the network need to verify whether the UE is allowed to access the CAG cell. For state transition and during mobility, it is endorsed that *"The AMF shall verify whether the CAG identifier received from NG-RAN is part of the UE's Allowed CAG list as received from the UDM".*

However, for the network to verify a UE's access to CAG cell, network needs to know the UE's SUPI. As per TS 33.501 [5], during initial NAS procedure (Registration Procedure), UE sends the Subscription concealed identifier (SUCI) to the network. The serving network receives the UE's SUPI from the AUSF, only after successful primary authentication. Therefore, if the serving network needs to perform the access control on the UE during initial Registration procedure, then AMF will have to wait until completion of successful primary authentication procedure.

It is likely that, large number of malicious UEs, with or without valid subscription, performing Registration procedures, to access the network via CAG cells. In this scenario, if these malicious UEs are not allowed to access the CAG cell, then there is an overhead (signalling and also computational) on the network and especially in the UDM, AMF and gNB, as the network needs to de-conceal the SUCI and performs authentication procedure and then checks whether the UEs are allowed to access the CAG cell. If such attempts are done on a particular CAG cell or distributed at different CAG cells, then it leads to (Distributed) Denial of Service ((D)DoS) attack on the 5G system.

This key issue needs to be investigated, to minimize the (D)Dos attack on the PNiNPN.

#### 5.6.1.2 Security threats

The PNiNPNs should provide a mechanism for verification of UE's access to CAG cell. When a large number of malicious UEs, which are not allowed to access a CAG cell, perform Registration procedures with the network, then there is an overhead on the network, to perform primary authentication and then do CAG cell access check. Such attempts, when done on a particular cell or distributed at different cells, leads to (Distributed) Denial of Service ((D)DoS) attack on the 5G system. Signalling attack on the core network (like UDM, to generate AVs) has a bigger effect than the access network and will impact larger number of UEs.

This threat is also mentioned in the TS 22.261 [1], clause 6.25.1.

#### 5.6.1.3 Potential security requirements

The 5G system should mitigate the (D)DoS attack on PNiNPNs, resulting from large number of Registrations requests from UEs which are not allowed to access a CAG cell.

### 5.6.2 Key Issue #6.2: CAG ID Privacy

#### 5.6.2.1 Key issue details

TS 23.501 [7] and TS 23.502 [6] support NPNs (NPNs) deployed with the assistance of PLMN using Closed Access Groups (CAG) and/or network slicing. These type of NPNs are called Public network integrated NPNs (PNiNPNs). CAG is proposed as a mechanism to enable the network to prevent UE from trying to access a Network Slice dedicated to an NPN in an area where the UE is not allowed to use the slice ([6] clause 5.30.3).

The procedure for network and cell selection and access control is illustrated in [6] clause 5.30.3 and [3] clause 4.2.2.2.2) and summarized below.

Before trying to access a CAG cell, the UE compares its locally configured Allowed CAG list against the CAG IDs broadcasted as plaintext (i.e., without confidentiality protection) by a CAG cell.

If the UE finds at least one matching CAG ID, the UE proceeds with a Registration procedure using its SUCI. The UE includes a CAG ID in the Access Stratum parameters when establishing an AS connection. The UE transmits the CAG ID as plaintext (i.e., neither confidentiality nor integrity nor replay protected)

The UE goes through a full primary authentication so that the AMF can obtain the CAG related subscription information from the UDM. AMF verifies that one CAG ID from the UE subscription corresponds to the UE selected CAG ID as forwarded by NG\_RAN in the N2 message.

If AMF finds a matching CAG ID then the UE is allowed to access the CAG cell, i.e., Registration is accepted.

If AMF does not find a matching CAG ID then UE is not allowed to access the CAG, i.e., Registration is rejected. The UE removes the CAG ID from its Allowed CAG list.

#### 5.6.2.2 Security threats

NG-RAN broadcasting its list of CAG IDs allows an eavesdropper to positively identify NG-RAN cell as a specific cell (e.g., serving a particular, sometimes small, set of Critical Infrastructure UEs).

In the current CAG access control mechanism, the UE sends the selected matching CAG ID in plain text over the air in its Registration Request message. This introduces security threat to the privacy of CAG ID. An adversary is able to eavesdrop on the UE Registration Procedure and learn the transmitted in the clear matched CAG ID. If the adversary is aware of sensitive CAGs (e.g., dedicated to Law Enforcement Agency (LEA)) they can infer the presence of members of such CAG (e.g., LEA).

#### 5.6.2.3 Potential security requirements

The 5G System shall support privacy protection of the CAG ID in the CAG access control mechanism.

### 5.6.3 Key Issue #6.3: DoS attack by unauthorized removal of entries from the UE's Allowed CAG ID list

#### 5.6.3.1 Key issue details

TS 23.501 [7] and 23.502 [6] support NPNs (NPNs) deployed with the assistance of PLMN using Closed Access Groups (CAG) and/or network slicing. These types of NPNs are called "Public network integrated NPNs" (PNiNPNs). CAG is proposed as a mechanism to enable the network to prevent UE from trying to access a Network Slice dedicated to an NPN in an area where the UE is not allowed to use the slice (TS 22.261 [1] clause 5.30.3).

More specifically, according to [1] clause 5.30.3.4, "If the CAG Identifier received from the NG-RAN is not part of the UE's Allowed CAG list, then the AMF rejects the NAS request with an appropriate cause code, whereas the UE removes that CAG Identifier, if it exists, from its Allowed CAG list".

#### 5.6.3.2 Security threats

The UE updates its Allowed CAG list (i.e., removes a CAD ID entry from the list) in response to a Registration Reject with the appropriate cause code. When such Registration Reject is not protected, an active attacker may attempt to send a Registration Reject message to the UE with the appropriate code causing the UE to remove the CAG ID from its Allowed CAG list. In such scenario, the attacker is able to cause the UE to "permanently forget" a given CAG ID and impede UE service with that CAG ID. In this scenario, the adversary will produce a persistent DoS attack on the UE, preventing it from accessing the network via that particular CAG ID. In the worse-case scenario, an adversary may cause the exhaustion of the UE's Allowed CAG list (e.g., by sending one or multiple Registration Reject messages to the UE) potentially resulting in its permanent (i.e., until re-provisioned with a new CAG list) inability to register with the network (i.e., if UE is only allowed to access 5GS via CAG cells).

#### 5.6.3.3 Potential security requirements

The 5G System shall be able to provide protection against persistent DOS attack caused by unauthorized removal of entries from the UE's Allowed CAG ID list.

# 6. Solutions

## 6.1 Solution #1: Solution for NPN network access via PLMN

### 6.1.1 Introduction

This solution addresses the security requirement for the Authentication and Authorization for Interworking between NPN and PLMN in key issue #2.1.

From the security point of view, three security requirements are specified for the access of UE to NPN via PLMN (and vice versa), i.e.:

- Requirement 1: Authentication between UE and PLMN network while UE access to the PLMN network.

- Requirement 2: Authorization for the PLMN PDU session establishment to ensure that UE is authorized to access to NPN services.

- Requirement 3: Authentication between UE and NPN network via PLMN network.

If the Requirement 2 is specified by the secondary authentication in the PLMN network, two authentication procedures between UE and NPN will be introduced, i.e. one is used for PDU session establishment authorization, the other one is used for UE registration to NPN. Therefore, duplicate authentications between UE and NPN will consume the computation and communication resource between them.

This solution proposes a new procedure for the above security requirements and reuses the secondary authentication for the Authorization of the PLMN PDU session establishment. Meanwhile, protection between UE and NPN can be based on the output of secondary authentication.

### 6.1.2 Solution details

#### 6.1.2.1 Registration to NPN via PLMN



Figure 6.1.2.1-1: Registration to NPN via PLMN

The procedure assumes that the UE has separate credentials for the PLMN and the NPN.

1. The UE firstly registers into the PLMN network based on the PLMN credential.

2. The UE sends the PDU session establishment request to the AMF, to setup the PDU session for the services provided by the NPN.

The UE initiates the PDU session establishment procedure as in step 4 of Figure 11.1.2-1 in TS 33.501 [5].

The following steps 3a, 3b, 4 are the same as steps 5a-13 in clause 11.1.2 of TS 33.501 [5].

5. After the successful completion of the authentication procedure, NPN-AUSF sends EAP Success message to the NPN-AMF, including the NPN SEAF key.

6. After receiving the EAP-success and NPN SEAF key from the NPN-AUSF, NPN-AMF generates the NPN AMF key, and NPN-GUTI for the UE, and sends EAP success, NPN-GUTI, NPN-ngKSI, and NPN-ABBA to the PLMN SMF via NPN-N3IWF and PLMN-UPF, where the NPN-ngKSI and NPN-ABBA are determined during the secondary authentication procedure.

7. The PLMN SMF sends a Namf\_Communication\_N1N2MessageTransfer to the AMF as in step 11 of Figure 4.3.2.2.1-1 in TS 23.502 [6]. This message includes EAP success, NPN-GUTI, NPN-ngKSI, and NPN-ABBA to be sent to the UE within the NAS SM PDU Session Establishment Accept message.

If the authorization is successful, PDU Session Establishment proceeds further starting at step 9a of Figure 4.3.2.2.1-1 in TS 23.502 [6]. The SMF initiates a N4 Session Modification procedure with the selected UPF as in steps 9.a and 9.b of Figure 4.3.2.2.1-1 in TS 23.502 [6].

8. PLMN AMF forwards NAS SM PDU Session Establishment Accept message along with EAP Success, NPN-GUTI, NPN-ngKSI, and NPN-ABBA to the UE as described in steps 12 and step 13 of Figure 4.3.2.2.1-1 in TS 23.502 [6].

The UE-requested PDU Session Establishment proceeds further as described in sub-clause 4.3.2.3 in TS 23.502 [6].

9. The UE sends the registration request message to the NPN-AMF, including the NPN-GUTI, NPN-ngKSI, NPN-UE security capability.

10. Based on the received NPN-GUTI, NPN-ngKSI, and NPN-UE capability, NPN-AMF firstly determines the NPN-AMF key, then proceeds the NPN-NAS SMC procedure with UE.

The UE-requested registration procedure proceeds further as described in clause 4.2.2.2.2 in TS 23.502 [6].

#### 6.1.2.2 Registration to PLMN via NPN

This procedure can refer to the clause 6.1.2.1.

### 6.1.3 Evaluation

The use of the secondary authentication in this solution requires more justification.

## 6.2 Solution #2: Security solution for handling UP security policy for a 5GLAN Group

### 6.2.1 Introduction

This solution addresses key issue #3.2: UP security policy for the 5GLAN group.

TR 23.734 [2] has recommended solution #29 "Unified architecture for 5G LAN-type service" for the normative work for 5GLAN group communication.In this solution a single SMF and a single PSA UPF is responsible for all the PDU Sessions for 5GLAN group communication within a single 5GLAN group. The same SMF is responsible for managing the PDU sessions belonging to the same 5GLAN group.

According to TS 23.501 [7] and TS 23.502 [6], the SMF determines and provide the UP security policy for a PDU session to the gNB connected to 5GC during the PDU session establishment procedure.

The UP security policy indicates whether UP confidentiality and/or UP integrity protection are activated or not for all DRBs belonging to that PDU session. The gNB uses UP security policy to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

According to TS 23.501 [7], the User Plane Security Policy provides the same level of information as the User Plane Security Enforcement information. Once the User Plane Security Enforcement information is determined at the establishment of the PDU Session, it is provided to the NG-RAN and applies for the life time of the PDU Session. The User Plane Security Enforcement information provides the NG-RAN with User Plane security policies for a PDU session. It indicates:

- whether UP integrity protection is:

- Required: for all the traffic on the PDU Session UP integrity protection shall apply.

- Preferred: for all the traffic on the PDU Session UP integrity protection should apply.

- Not Needed: UP integrity protection shall not apply on the PDU Session.

- whether UP confidentiality protection is:

- Required: for all the traffic on the PDU Session UP confidentiality protection shall apply.

- Preferred: for all the traffic on the PDU Session UP confidentiality protection should apply.

- Not Needed: UP confidentiality shall not apply on the PDU Session.

### 6.2.2 Potential solution details

This solution requires the same security activation status in the UP security policy for all UE's belonging to the same 5GLAN group. If gNB decides the security activation on its own, the user plane traffic sent between the UE and the gNB for one PDU session could use different security compared to the other PDU sessions for the other UE's belonging to the same 5GLAN group. In such case, the security for the whole 5GLAN group is indeterministic. In summary, the security properties of the group communication will inadvertently be determined by the security properties of the weakest communication path.

This solution requires that the ciphering and integrity protection activation status of DRBs of all UEs belonging to the same 5GLAN Group shall be the same. For that reason, the SMF shall send the same security activation status in the User Plane Security Policy to the gNBs for establishing PDU sessions with UEs belonging to the same 5GLAN Group.

This solution further requires that the gNBs shall not override the UP Security Policy received from the SMF. For that reason, the SMF shall not send the "Preferred" option in User Plane Security Policy to the gNBs for establishing PDU sessions with UEs belonging to the same 5GLAN Group. In other words, the setting defined in clause 5.10.3 TS 23.501 [7] shall apply with the following modifications:

Encryption:

- "Required" or "Not Needed" may be used;

- "Preferred" shall not be used.

Integrity protection:

- "Required" or "Not Needed" may be used;

- "Preferred" shall not be used.

NOTE: If 5GLAN group communication is taking place over E-UTRA (connected to 5GC), then the setting of "Required" for Integrity protection is not supported.

### 6.2.3 Evaluation

The proposed solution meets all the requirements of key issue #3.2.

## 6.3 Solution #3: Security solution for mitigation of (D)DoS attack in PNiNPNs

### 6.3.1 Introduction

This solution addresses key issue #6.1 (D)DoS attack in PNiNPNs.

As mentioned in the security threat of the key issue #6.1 during initial NAS Attach procedures (Registration procedures) from NPN UEs, that are accessing via CAG cell, network has to wait until completion of primary authentication to verify whether the UEs are allowed to access a CAG cell, which is an overhead on the network, if the requesting UE's are not allowed to access the CAG cell.

This solution details on, checking an UE's access to a CAG cell during initial NAS procedure (Registration procedure) and reject initial NAS (Registration) request from the UE, if the network identified UE is not allowed to access the CAG cell. Doing this avoids overhead on network (gNB, AMF, AUSF, UDM) and mitigates (D)DoS attack on PNiNPNs.

### 6.3.2 Potential solution details

During initial NAS (Registration) procedure, the network to verify whether a NPN UE is allowed to access the CAG cell, as early as possible, in order to avoid unnecessary signalling overhead. The steps below detail on how this verification can be done:

1) NPN UE sends initial NAS (Registration) request to the network. In this request procedure, NG-RAN verifies if CAG identifier (Identifier of the CAG cell which the UE accesses) is within ngRAN's allowed CAG ID list and sends the CAG identifier to the serving network's AMF.

2) As per TS 33.501 [5] AMF/SEAF initiates primary authentication by sending in Nausf\_UEAuthentication\_Authenticate request message to the AUSF and includes in this request the CAG identifier received from NG-RAN.

3) If there is CAG identifier in the Nausf\_UEAuthentication\_Authenticate request received from SEAF, AUSF includes the CAG identifier in Nudm\_UEAuthentication\_Get Request message to the UDM.

4) UDM de-conceals SUCI, and if the CAG Identifier is included in the Nudm\_UEAuthentication\_Get Request message, then it verifies whether the UE (SUPI) is allowed to access the CAG cell. If the UE is allowed to access the CAG cell, then the UDM proceeds further with the procedures as specified in TS 33.501 [5]. Additionally, the UDM includes the "Allowed CAG list" of the UE to the AMF, to perform the check for the subsequent procedure when needed.

5) If the UE is not allowed to access the CAG cell, then, based on stored authentication status of the UE and/or update to the UE’s Allowed CAG List, the UDM may decide to proceed further with primary authentication procedure or includes "CAG cell Reject" in Nudm\_UEAuthentication\_Get Response message to AUSF, and does not proceed further in authentication procedure, for example, selection of authentication method and generation of authentication vector, like so.

6) If there is "CAG Cell Reject" in Nudm\_UEAuthentication\_Get Response message from UDM, then the AUSF forwards the same to the AMF/SEAF in Nausf\_UEAuthentication\_Authenticate response message.

7) If there is "CAG Cell Reject" in the Nausf\_UEAuthentication\_Authenticate response message from the AUSF, then the AMF rejects the UE's registration request by sending the Registration Reject message with an appropriate cause value, to the UE.

This method avoids overhead on UDM of generating Authentication Vector and the network to perform authentication, for the UEs that access via unauthorized CAG cell.

NOTE: Privacy aspects of sending CAG Identifier from UE to the network is not part of this solution.



Figure 6.3.2-1: Access control during Registration Procedure

### 6.3.3 Evaluation

Key Issue #6.1 in the present document is about (D)DoS attack on PNiNPNs, resulting from large number of Registration requests from UEs which are not allowed to access a CAG cell. The solution addresses the key issue by minimizing the overhead on the network during the Registration procedure, avoiding the (D)DoS attack proposed in Key Issue.

During Registration procedure, the network verifies whether an UE is allowed to access a CAG cell and reject the UE's request, if the UE is not allowed to access the CAG cell. This verification is done prior to primary authentication and avoids signalling and computational overhead on the network, when an UE is not allowed to access a CAG cell.

This solution provides flexibility for the network, to avoid the signalling and computational overhead, by allowing the UDM to determine to check the UE’s access to a CAG cell prior to authentication.

In case of change of allowed CAG ID, provisioning the updated CAG ID to the UE is out of scope of this solution. Update to Allowed CAG list by the UE will be based on successfully protected message from the network. In case of change of Allowed CAG List, provisioning of the updated Allowed CAG list to the UE will be specified by CT1.

The proposed solution meets the requirement of key issue #6.1.

## 6.4 Solution #4: Security solution for key derivation in SNPNs

### 6.4.1 Introduction

This solution addresses key issue #1.1 on the derivation of keys in SNPNs.

### 6.4.2 Solution details

For SNPNs, the serving network name that is used as an input to the calculation of KAUSF, RES\* and XRES\* for 5G AKA, CK' and IK' for EAP\_AKA' and KSEAF for all authentication methods should be defined differently from that of the public networks as:

a) the input should not be the same as a public network as this would allow a SNPN to masquerade as a public network;

b) the input should prevent one standalone public network masquerading as another.

Hence, it is proposed that for SNPNs, the serving network name used in the input to the above key derivation is as follows:

serving network name = 5G:PLMN\*:NPN ID

with PLMN\* equal to either a PLMN ID or a shortened one based on the conclusion on what to broadcast for SNPNs and NPN ID as defined in TR 23.734 [3].

The final decision on PLMN\* and the exact coding format will need to be taken as the definition of these is completed.

### 6.4.3 Evaluation

The proposed solution meets all the requirements of key issue #1.1.

This solution makes small change to the key derivation for public network to enable the same key derivation function to be used for SNPNs. The change is defining the serving network name for SNPNs to include the NPN ID in the derivation of KSEAF for all authentication methods, KAUSF, RES\* and XRES\* for 5G AKA, and CK' and IK' for EAP-AKA'.

## 6.5 Solution #5: Key hierarchy for authentication using non-AKA EAP methods in NPN

### 6.5.1 Introduction

This solution addresses key issue #5.1: Key hierarchy for NPNs.

### 6.5.2 Solution details

NOTE: The key hierarchy (subclause 6.2.1 of TS 33.501 [5]) and the key derivation and distribution (clause 6.2.2 of TS 33.501 [5]) clauses cannot apply to generic non-AKA EAP methods of authentication as they are written on the assumption that an AKA method is used for authentication.

For the purposes of this solution to describe the key hierarchy modifications, it is assumed that the EAP authentication terminates in the AUSF in the network.

The major change needed is on the derivation of KAUSF. It is proposed that this derivation is as follows:

- KAUSF is derived from the EMSK created by the EAP authentication as for EAP-AKA'.

The following figure captures a visual representation of that change:



Figure 6.5.2-1: KAUSF derivation for generic non-AKA EAP methods

Other text from clauses 6.2.1 and 6.2.2 of TS 33.501 [5] cannot be directly used for generic non-AKA EAP methods (e.g. where the text is specific to the key hierarchy and derivation and distribution for the AKA authentication methods).

### 6.5.3 Evaluation

The proposed solution meets all the requirements of key issue #5.1.

This solution seems to make the smallest amount of change possible to the key hierarchy for AKA methods to make it applicable to non-AKA EAP based authentication methods as compared to EAP-AKA'. It only varies in the way the EAP based method derives the EMSK from an EAP authentication. This change is necessary as the EAP-AKA' way of deriving EMSK does not apply to general EAP methods.

## 6.6 Solution #6: 5GLAN authentication

### 6.6.1 Introduction

This solution addresses key issue #3.1 on Authentication and Authorization of UE in 5GLAN communication.

In TS 23.501 5.28.3 [7] the following is stated:

*During establishment of the PDU Session, secondary authentication as described in clause 5.6.6 and in TS 23.502 [3], clause 4.3.2.3, may be performed in order to authenticate and authorize the UE for accessing the DNN associated with the 5G-LAN group.*

*Authentication and authorization for a DNN using secondary authentication implies authentication and authorization for the associated 5G-LAN group. There is no 5G-LAN group specific authentication or authorization defined.*

Thus, key issue #3.1 can be concluded by referencing the security solution of TS 33.501 for secondary authentication.

### 6.6.2 Solution details

TS 23.501 clause 5.28 [7] describes the feature in support for 5G LAN-type service 5G LAN.

There is no 5G-LAN group specific authentication or authorization defined for 5GLAN group communication. Authentication and authorization for a DNN using secondary authentication implies authentication and authorization for the associated 5G-LAN group.

The secondary authorization/authentication by an DN-AAA server during the PDU Session establishment is described in TS 23.502 clause 4.3.2.3 [6].

Thus, the security solution of TS 33.501 [5] for secondary authentication applies and a clause summarising the topic by giving references to above mentioned specifications is sufficient.

### 6.6.3 Evaluation

The proposed solution meets all the requirements of key issue #3.1. The solution reuses the existing mechanisms as described in TS 23.501 [7], TS 23.502 [6] and TS 33.501 [5].

## 6.7 Solution #7: SMF handling the UP security policy for a 5GLAN Group based on information from DN AAA

### 6.7.1 Introduction

This solution provides an enhancement to Solution #2 and addresses key issue #3.2: UP security policy for the 5GLAN group. A single SMF and a single PSA UPF is responsible for all the PDU Sessions for 5GLAN group communication within a single 5GLAN group. The same SMF is responsible for managing the PDU sessions belonging to the same 5GLAN group.

When application layer end-to-end security is applied between a UE and DN that is reached via a 5GS, there is no significant security gain in doing PDCP layer user plane traffic encryption and/or integrity protection between the UE and the gNB.

Solution #2 suggests that SMF only uses "required" or "not needed" for indicating the protection required. This decision is done by the network (not by the UE), based on a policy that needs to be available in the network at the time of the decision.

According to TS 23.501 [7] and TS 23.502 [6], the SMF determines and provides the UP security policy for a PDU session to the gNB connected to 5GC during the PDU session establishment procedure. In this solution it is suggested to provide SMF with information from the DN AAA Server, i.e. whether end-to-end security is already applied at the data radio bearer and thus, would not be needed anymore by the NPN. Depending on this information the SMF will indicate "required" or "not needed" to gNB for the protection required.

Then, in line with solution #2, after SMF has evaluated the information received from the DN AAA, it generates a UP security policy for all DRBs belonging to that PDU session, i.e. it indicates whether UP confidentiality and/or UP integrity protection are activated or not for all DRBs belonging to that PDU session. The gNB uses UP security policy to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

### 6.7.2 Potential solution details

This solution requires the same security activation status in the UP security policy for all UE's belonging to the same 5GLAN group.

The SMF may have received indication of a DN AAA server whether user plane encryption and/or integrity protection is applied end-to end and thus, the SMF can make a decision on whether additional protection to the data radio bearers of the respective PDU session is needed. Based on this input the SMF makes a decision on the protection level that the gNB shall apply and shall send the same security activation status in the User Plane Security Policy to the gNBs for establishing PDU sessions with UEs belonging to the same 5GLAN Group.

Thus, the ciphering and integrity protection activation status of DRBs of all UEs belonging to the same 5GLAN Group shall be the same.

### 6.7.3 Evaluation

The proposed solution meets all the requirements of key issue #3.2.

## 6.8 Solution #8: TSC security

### 6.8.1 Introduction

This solution addresses key issue #4.1 on time sensitive communication (TSC).

TSC allows the 5G System to be integrated transparently as a bridge in an IEEE TSN network, where the 5GS system acts as one or more TSN Bridges of a TSN network as defined by IEEE 802.1Q. This "logical" TSN bridge includes TSN Translator functionality for interoperation between TSN System and 5G System both for user plane and control plane. 5GS TSN translator functionality consists of Device-side TSN translator (DS-TT) and Network-side TSN translator (NW-TT). The so-called 5GS Bridge is composed of the ports on a single UPF (i.e. PSA) side, the user plane tunnel between the UE and UPF, and the ports on the DS-TT side.

For each 5GS Bridge of a TSN network, the ports on NW-TT side support the connectivity to the TSN network, the ports on the DS-TT side are associated to the PDU Session providing connectivity to the TSN network.

### 6.8.2 Solution details

The 5G System is integrated transparently as one or several TSN Bridges in an IEEE TSN network. No changes to the security as specified in TS 33.501 [5] are needed for a TSN Bridge connecting via a 5GS TSN Bridge with another TSN Bridge.

## 6.9 Solution #9: (D)DoS attack mitigation in PNiNPNs

### 6.9.1 Introduction

This solution addresses key issue #6.3: DoS attack by unauthorized removal of entries from the UE's Allowed CAG ID list.

This solution mitigates DoS attack on PNiNPNs by the UE rejecting a NAS Registration Reject message that is not integrity protected. The solution also addresses the case when the UE receives a protected Registration Reject with the appropriate cause for CAG ID rejection when the UE has only a single CAG ID left in its Allowed CAG list.

### 6.9.2 Solution details

If the UE receives a CAG ID rejection cause in Registration Reject message that is not protected or that fails a security protection check then the UE ignores the message and does not update its Allowed CAG list (i.e., remove the rejected CAG ID from its Allowed CAG list).

If the UE receives a CAG access rejection cause in Registration Reject message that is protected, then the UE removes the rejected CAG ID from its Allowed CAG list.

In case the UE Allowed CAG list is exhausted following such a protected Registration Reject message the UE cannot access the network anymore (if the UE is limited to access via CAG cells). To prevent this situation, the UE indicates in the NAS Registration Request message that it has a single CAG ID in its Allowed CAG list and optionally that it is limited to CAG only access. Following authentication, if the AMF determines that the subscription data is out of sync with UE configuration, then AMF updates UE configuration with current Allowed CAG list from the subscription data. If the UE is not Registered while its subscription is updated with currently configured CAG ID being removed/replaced may lead to such an out of sync situation between the UE configuration and subscription data. The UE updates it Allowed CAG list accordingly and perform and new CAG cell selection and access using the updated CAG ID(s).

The UE may initially have more than one CAG ID in its configuration before trying to connect to the network. The UE may end up removing all CAG IDs following multiple Registration reject if those CAG ID were removed from the subscription. 3GPP TS 23.501 [7], clause 5.30.3.4 prescribes that when UE transitions from CM-IDLE to CM-CONNECTED the AMF rejects the NAS request if the provided CAG ID is not part of the Allowed CAG list without any consideration if this may lead to an exhaustion of the UE Allowed CAG list and cause the DoS situation described above. Therefore, the case where the UE has only one CAG ID is no different from a generic use case when the UE transitions from CM-IDLE to CM-CONNECTED and the AMF rejects the NAS request if the provided CAG ID is not part of the Allowed CAG list.

### 6.9.3 Evaluation

Key Issue #6.3 describes a DoS attack in PNiNPNs, caused by exhaustion of the UE Allowed CAG list and therefore inability to perform any CAG based cell selection and access when the UE is only allowed to access the network via CAG cell.

This solution mitigates DoS attack in a PNiNPN by the UE ignoring Registration Reject messages with a CAG ID rejection cause, that are not protected or that fail security checks. Furthermore, the solution also prevents the situation where the UE Allowed CAG list exhaustion is caused by a protected Registration Reject message with a CAG ID rejection cause.

Per TS 23.501 [7], the use case when the UE has only one CAG ID is no different from a generic use case when the UE transitions from CM-IDLE to CM-CONNECTED and the AMF rejects the NAS request if the provided CAG ID is not part of the Allowed CAG list. This solution is also addressing the use case with the UE having only one CAG ID as no different from the generic use case described in TS 23.501 [7].

This solution meets the potential requirement of key issue #6.3.

## 6.10 Solution #10: Using NAS security for messages that modify the CAG list

### 6.10.1 Introduction

This solution addresses key issue #6.3: DoS attack in PNiNPNs which is performed by modifying CAG lists in the UE using unprotected NAS messages.

The proposed solution is simple that the UE should only modify the CAG list based on a successfully integrity protected message.

### 6.10.2 Solution details

The solution is to simply protect the messages that are used to modify the CAG list in the UE using the existing NAS security. Namely:

- When the AMF wants to modify the CAG list in the UE, the AMF applies the NAS security to such messages; and

- The UE only modifies its CAG list based on receiving a successfully integrity protected NAS message requesting the UE to modify its CAG list.

### 6.10.3 Evaluation

The solution fulfils the requirement in key issue #6.3.

The impact of the solution is to require the AMF to protect NAS messages that modify the CAG list in the UE and the UE to only modify the CAG list based on a successfully integrity protected NAS message.

## 6.11 Solution #11: DH based solution for CAG ID privacy

### 6.11.1 Introduction

This solution addresses PNiNPN related key issue #6.2: CAG ID privacy.

This solution aims to provide a method to protect the CAG ID(s) transmitted during the CAG access control mechanism (i.e., over unicast or broadcast messages).

The UE selects a CAG cell after finding a hash value of one of its Allowed CAG ID(s) matching one of the hash values of CAG ID(s) broadcasted by the CAG cell. The UE establishes a shared secret with the gNB using a Diffie-Hellman based key agreement protocol (e.g. ECDH) and derives a secret key to protect its matching CAG ID in the AS layer during AS connection establishment. The UE is allowed to access the CAG cell if the provided protected CAG ID matches one of the cell supported CAG ID(s) or according to policy exceptions (e.g., emergency services access only). The UE is denied access otherwise.

### 6.11.2 Solution details

The solution shown in Figure 6.11.2-1 details a procedure for CAG Cell selection and access with a CAG ID protected using a ECDH key agreement protocol.

This solution aims to protect against passive attacks (e.g., eavesdropping) against CAG ID confidentiality and privacy. In cases of False Base Station (FBS) (i.e., active) attacks against CAG ID confidentiality and privacy, the presented solution may provide an adequate protection when other means of protection against FBS attacks are implemented.



Figure 6.11.2-1: UE transmitted CAG ID protection using an ECDH based key agreement protocol

0. The UE is configured with an Allowed CAG list from the HPLMN. The RAN, e.g., gNB is configured with supported CAG ID(s). The UE and gNB are configured with EC domain parameters (e.g., curve25519).

Note that CAG ID update in the UE following a subscription change is performed using existing protected NAS UE Configuration Update procedure as per current CAG ID solution in TS 23.501 [7].

1. The gNB performs the following operations:

a. generates an ephemeral private key x (e.g., a random 32 bytes number)

b. generates an ephemeral public key K\_A using x (e.g., K\_A = X25519(x, 9), where 9 is the curve base point)

c. generates a pseudo-random number (e.g., RAND\_CELL = least significant n bits of K\_A)

d. computes the hash value for each of its configured CAG ID(s) using RAND\_CELL

By computing RAND\_CELL as a function (e.g., truncation) of K\_A, the CAG IDs hash values are bound to ephemeral public key K\_A. This enables the protection of the DH key agreement against a MiTM attack where the attacker tries to replace the gNB K\_A by its own to establish a shared secret with the UE (e.g., in order to obtain the cleartext CAG IDs).

The gNB may generate a new K\_A periodically in order to mitigate UE CAG ID replay attacks. The gNB may also include a nonce (e.g., pseudo-random number) in the broadcast message that may change independently of K\_A. For example, new a and K\_A may be used for some given time period (e.g., every few hours), whereas a new nonce may be generated and used independently from the K\_A generation and for different for (e.g., shorter time periods, every few minutes). This process may provide additional freshness (e.g., based on policy) and may be used in order to save on K\_A processing cost while providing protection against UE connection requests replay attacks.

2. The UE acquires from the System Information (e.g., SIB1) the following parameters: K\_A, and the list of hashed CAG IDs. The UE also acquires a nonce if included in the broadcast System Information (SI).

3. The UE performs the following operations:

a. select one or more CAG ID from Allowed CAG IDs whose hash value using RAND\_CELL matches a CAG ID hash value from gNB (where RAND\_CELL is obtained from K\_A as in step 1).

b. generates an ephemeral private key y

c. generates an ephemeral public key K\_B using y (e.g., K\_B = X25519(y, 9))

d. generates a shared secret S using y and K\_A (e.g., S = X25519(y, K\_A))

e. derives a secret key K from S using a key derivation function, K\_A, K\_B and a UE identity (e.g., K = HMAC-SHA256(S, K\_A || K\_B || C-RTNI)). If a nonce is included in the broadcast SI, the UE may use the nonce in the computation of K (e.g., concatenation with the other parameters).

f. for the selected CAG ID, computes a protected CAG ID using K (e.g., protected CAG IDK = CAG ID encrypted/integrity protected using K and AES algorithm)

4. The UE sends a Registration Request and includes in the RRC part of the message the following parameters: K\_B, a protected CAG IDK. The UE may also include the nonce from the broadcast SI.

5. The gNB performs the following operations:

a. generates a shared secret S using K\_B and x (e.g., S = X25519(x, K\_B))

b. derives a secret key K from S using a key derivation function as done in UE, step 3.e

c. check integrity protection and decrypts CAG IDK using K (e.g., using an AES algorithm)

The gNB may verify the freshness of the UE request by validating that the included nonce corresponds to the current nonce in the broadcast SI. The gNB may also consider as valid a request using the previous nonce (e.g., based on policy). This may be used to avoid rejecting a UE that attempts to connect using a nonce that has just been replaced with a new one in the broadcast SI.

6. The NG-RAN (gNB) includes the decrypted CAD ID in the N2 message sent to the AMF so that AMF can further check if the provided CAG-ID is in the allowed list and complete the rest of the registration procedure as per conventional steps.

### 6.11.3 Evaluation

Solution #11 addresses PNiNPN related key issue #6.2: CAG ID privacy and associated potential security requirements protecting against passive attacks (e.g., eavesdropping) on CAG ID confidentiality and privacy over unicast or broadcast messages.

This solution provides a method for protection of the CAG ID(s) transmitted during broadcast/CAG cell selection and in UL AS signalling during access control procedure.

## 6.12 Solution #12: Hash based solution for CAG ID privacy

### 6.12.1 Introduction

This solution addresses PNiNPN related key issue #6.2: CAG ID privacy.

This solution aims to provide a method to protect against passive attacks (e.g., eavesdropping) against confidentiality and privacy of CAG ID(s) transmitted during the CAG access control procedure (i.e., over unicast or broadcast messages). In cases of False Base Station (FBS) (i.e., active) attacks against CAG ID confidentiality and privacy, the presented solution may provide an adequate protection when other means of protection against FBS attacks are implemented.

The UE selects a CAG cell after finding a hash value of one of its Allowed CAG ID(s) matching one of the hash values of CAG ID(s) broadcasted by the CAG cell. The UE connects with the network by providing a fresh hash value of its matching CAG ID in the AS layer during AS connection establishment. The UE is allowed by NG-RAN to access the CAG cell if the provided hashed CAG ID matches the hash value of one of the cell supported CAG ID(s) or according to policy (e.g., emergency services access only). The UE is denied access otherwise.

Note that CAG ID is assumed to be of sufficient length (e.g., 64 - 128 bits) to provide sufficient entropy for resisting dictionary attacks. The transmitted hash value can be truncated to accommodate broadcast channel constraints while remaining adequately resistant to collisions.

### 6.12.2 Solution details

The solution shown in Figure 6.12.2-1 details a procedure for CAG Cell selection and access using a hashed CAG ID based mechanism.



Figure 6.12.2-1: Hashed CAG ID based Access control AS connection establishment

0. The UE is configured with an Allowed CAG list from the HPLMN. The gNB is configured with Supported CAG ID(s).

Note that CAG ID update in the UE following a subscription change is performed using existing protected NAS UE Configuration Update procedure as per current adopted CAG ID solution in TS 23.501 [7].

1. The NG-RAN broadcast (e.g., in SB1) one or multiple supported CAG Identifiers (ID) individually hashed using a random number RAND\_CELL also included in the broadcast message. Each CAG cell may use a different RAND\_CELL such that two CAG cells supporting common CAG ID(s) (i.e., serving common NPN(s)) will still be broadcasting completely different hashed CAG ID(s). It is assumed that RAND\_CELL is refreshed periodically (e.g., every time the Cell Supported CAG ID(s) are updated a new RAND\_CELL is generated).

2. The UE performs CAG Cell selection based on matching of hashed CAG ID:

a. The UE computes a hash for each of its Allowed CAG ID using RAND\_CELL as a salt

b. The UE compares the hash values of its Allowed CAG ID with those of the Cell supported CAG ID from the broadcast message to find at least one matching hashed CAG ID.

c. The UE selects an Allowed CAG ID that has a matching hash.

3. The UE sends an initial NAS message to the network including a hash of the selected CAG IDs in the AS layer. The hash is computed using a combination of RAND\_UE and C-RNTI as salt. A UE specific identifier such as C-RNTI is used such as two UEs accessing the CAG cell using the same CAG ID will transmit different hashed CAG ID. It is assumed that RAND\_UE is refreshed periodically such as to reduce to possibility of a UE hashed CAG ID replay attack and long enough to allow legitimate AS connection to complete (e.g., as multiple of RRC connection timers, T300, T352).

4. The NG-RAN checks that the UE is allowed to access the CAG cell based on matching of hashed CAG ID:

a. The NG-RAN computes a hash for each of its Supported CAG ID using RAND\_UE and C-RNTI as a salt.

b. The NG-RAN checks that the UE provided hashed CAG ID matches one of the hashed supported CAG ID.

Note: NG-RAN may forward the decrypted CAG-ID to the AMF and request AMF to compare the decrypted CAG-ID received from NG-RAN with the list of allowed CAG IDs.

5a. [Conditional] If no match for the UE provided hashed CAG ID is found, the NG-RAN drops the RRC connection immediately. The NG-RAN may still proceed with subsequent steps if no matching CAG ID is found based on policy (e.g., if the RRC establishment cause is set to emergency).

5b. [Conditional] If a matching hashed CAG ID is found, NG-RAN sends a message over the N2 interface to the AMF, including the cleartext CAG ID for which a matching hash was found. The message may be sent in absence of matching CAG ID (e.g., emergency services access) in which case no CAG ID is included in the message.

6. The AMF determines whether to allow UE to access the CAG cell based on the message from NG-RAN and operator's policy.

7a. [Conditional] If no CAG ID is provided by NG\_RAN for the CAG cell, the AMF sends a NAS rejection message to the UE, followed by the release of AS/NAS connection. If no CAG ID is provided, the AMF may still allow access based on operator's policy (e.g., emergency services access) and perform next step instead.

7b. [Conditional] If a CAG ID is provided by NG\_RAN for the CAG cell, the AMF proceeds with regular Registration procedure as per TS 23.502. If no CAG ID is provided, the AMF may still allow access based on operator's policy (e.g., proceed with emergency registration procedure).

### 6.12.3 Evaluation

Solution #12 addresses PNiNPN related key issue #6.2: CAG ID privacy and associated potential security requirements protecting against passive attacks (e.g., eavesdropping) on CAG ID confidentiality and privacy over unicast or broadcast messages.

This solution provides a method for protection of the CAG ID(s) transmitted during broadcast/CAG cell selection and in UL AS signalling during access control procedure.

Solution #12 does not prevent passive attacks from the members of the same CAG ID group using their knowledge of CAG ID.

## 6.13 Solution #13: CAG ID Privacy in PNiNPNs by embedding CAG ID in the SUCI

### 6.13.1 Introduction

This solution addresses the key issue #6.2: CAG ID Privacy.

As mentioned in the security threat of the key issue #6.2, during initial NAS Attach procedures (Registration procedures) from the NPN UEs, that are accessing via CAG cell, the UE sends the selected matching CAG ID in clear over the air in the Registration Request message. An attacker can eavesdrop on the UE Registration request message and identify the CAG Cell (CAG ID) that the UE is attempting to access. If the CAG Cells are sensitive in nature, it is possible for an attacker to link the UE to these sensitive CAGs.

This solution details on protecting CAG ID from eavesdropping, during the initial NAS procedure (Registration procedure) where the UE is accessing NG-RAN using a CAG cell and the UE does not have valid security context.

### 6.13.2 Solution details

The steps below details on how the CAG ID is protected during initial NAS (Registration) procedure, when the UE is accessing the NG-RAN using a CAG cell and the UE does not have valid security context (UE does not have a GUTI or the stored GUTI is not valid):

1. During initial NAS (Registration) procedure, when the UE does not have valid security, then the UE protects CAG Identifier (CAG ID of the CAG cell that the UE attempts to access) by embedding it in the UE's SUCI, which is sent over the air by the UE to the serving network as the UE identifier. UE constructs the CAG ID embedded SUCI, if configured by the home network in the Allowed CAG List. CAG ID is embedded into the SUCI as follows:

a. During the calculation of SUCI, the UE concatenates the CAG ID with MSIN/Username and generates the scheme output of the SUCI.

b. When the SUPI is of type IMSI, the subscription identifier part of the IMSI (i.e., MSIN) is concatenated with CAG ID to construct the scheme-input and generate scheme output of SUCI.

c. When the SUPI is of type network specific identifier, the subscription identifier part of the SUPI is concatenated with CAG ID and used to construct the scheme-input and generate scheme output of SUCI.

2. NPN UE sends an initial NAS (Registration) request to the serving network. In this registration request procedure, the serving network's AMF receives the SUCI embedded with CAG ID (Identifier of the CAG cell which the UE accesses) and "CAG ID in SUCI" indication message from the UE as UE identifier and CAG ID indication respectively.

3. As per TS 33.501 [5] AMF/SEAF initiates primary authentication by sending in Nausf\_UEAuthentication\_Authenticate request message to the AUSF and includes in this request the CAG identifier (CAG ID) embedded SUCI and "CAG ID in SUCI" indication message received from the UE.

4. If there is "CAG ID in SUCI" indication message in the Nausf\_UEAuthentication\_Authenticate request received from SEAF, AUSF includes the "CAG ID in SUCI" indication message in Nudm\_UEAuthentication\_Get Request message to the UDM.

5. If there is "CAG ID in SUCI" indication message Nudm\_UEAuthentication\_Get Request message then the UDM de-conceals the SUCI to SUPI and CAG ID. The de-concealment is done using same mechanisms used for concealing SUPI with CAG ID by the UE. If there is no "CAG ID in SUCI" indication message Nudm\_UEAuthentication\_Get Request message then the UDM de-conceals the SUCI to SUPI. If the UDM de-conceals SUPI and CAG ID (If there is "CAG ID in SUCI" indication message in Nudm\_UEAuthentication\_Get Request message) successfully, then the UDM shall proceed further with the procedures as specified in TS 33.501 [5] in authentication procedure, for example, selection of authentication method and generation of authentication vector, like so.

6. If the CAG ID is de-concealed successfully from the SUCI by the UDM, then the UDM includes the de-concealed "CAG ID" in Nudm\_UEAuthentication\_Get Response message to AUSF along with UE’s SUPI.

7. If there is "CAG ID" in Nudm\_UEAuthentication\_Get Response message from UDM, then the AUSF forwards the same to the AMF/SEAF in Nausf\_UEAuthentication\_Authenticate response message upon successful primary authentication of the UE.

8. If there is "CAG ID" in the Nausf\_UEAuthentication\_Authenticate response message from the AUSF, then the AMF uses this CAG ID as the selected CAG ID by the UE and proceed further with subsequent procedures. AMF may send this received CAG ID from the AUSF for the UE to the NG-RAN.

As home network public key and protection scheme used for SUCI (with CAG ID embedded) derivation are same, UDM that de-conceals SUCI will also be able to de-conceal CAG ID. Sending CAG ID concealed in SUCI over the air to the network prevents a man in the middle from identifying the NPN/CAG Cell that the UE is attempting to access.



Figure 6.13.2-1: CAG ID protection during Registration Procedure

### 6.13.3 Evaluation

Key Issue #6.2 is about privacy protection of CAG ID of the CAG cell that the UE selects and indicates to the network. The solution addresses the key issue by embedding the CAG ID in the UE’s SUCI along with the UE’s SUPI. This enables the UE (during Initial NAS attach procedures) to send protected CAG ID to the network when UE does not have a valid security context. The network (UDM) de-conceals the SUCI to SUPI and CAG ID. As home network public key and protection scheme used for SUCI (with CAG ID embedded) derivation are same, UDM that de-conceals SUCI will also be able to de-conceal CAG ID. This solution needs a mechanism to provide CAG ID to the UICC if the SUCI is calculated in the UICC.

The proposed solution meets the requirement of key issue #6.2.

## 6.14 Solution #14: CAG ID privacy by re-use of SUPI protection mechanism

### 6.14.1 Introduction

This solution addresses key issue #6.2: CAG ID Privacy.

The UE shall re-use mechanism for protection of SUPI to protect CAG ID privacy.

### 6.14.2 Solution details

The detailed procedure of the security solution for CAG is illustrated as below:



Figure 6.14.2-1: Security procedure or registration with CAG access control

The procedure is based on the TS 23.501 [7] and TS 23.502 [6], with the following changes:

Step 2:

When the UE generate an integrated SUCI, the scheme-input further include the CAG ID. Or

The UE generate a concealed CAG ID using the protection scheme with the Home Network Public Key and with the CAG ID as the scheme-input.

The concealment of CAG ID is performed by the UE whenever a SUCI is required, including UE sending a Registration Request message and UE responding to an Identity Response message.

Step 3 and 4:

The RR message further includes the integrated SUCI or the concealed CAG ID.

Step 5:

UDM/SIDF is responsible for de-concealing the CAG ID from the integrated SUCI if the UE generated the SUCI with adding CAG ID to the scheme-input. Or

UDM/SIDF is responsible for de-concealing the CAG ID from the concealed SUCI using the same mechanism of decealing SUPI from SUCI.

### 6.14.3 Evaluation

The solution fulfils the requirement in key issue #6.2.

## 6.15 Solution #15: CAG ID privacy by indication in RRC layer and providing CAG ID only after NAS security establishment

### 6.15.1 Introduction

This solution addresses key issue #6.2 and proposes a new mechanism to confidentially protect the CAG ID during the CAG access control using the NAS security protection.

### 6.15.2 Solution details

During the registration procedure, the AMF checks that whether the requested CAG ID protected by NAS security sending from UE is within both the NG-RAN's allowed CAG Lists, and subscribed CAG retrieved from the UDM. If the verification successes, the AMF sends the allowed CAG ID to the NG-RAN.

Details procedure during the initial registration is as follows.



Figure 6.15.2-1: CAG ID access control in initial registration scenario

0. UE is configured with Allowed CAG ID list.

1. NG-RAN broadcasts the system information including the CAG ID list supported by the NG-RAN.

2. UE checks there is as least one match between allowed CAG list and NG-RAN-s CAG ID(s).

3. UE to NG-RAN: AN message (AN parameters, Registration Request (Registration type, SUCI, etc.), where the AN parameter includes an indicator, indicating that the UE requires to access the CAG ID(s) broadcasted by the NG-RAN.

4. NG-RAN to AMF: N2 message (N2 parameters, Registration Request (as described in step 1) where the N2 parameter include NG-RAN’s CAG ID(s). If the indicator is received from the UE, the CAG ID(s) supported by the NG-RAN (i.e. NG-RAN’ CAG ID(s)) shall be forwarded to the AMF within the N2 parameters.

5-8. The AMF initiates the following UE authentication.

9. AMF initiates NAS SMC procedure, and sends the NAS security mode command to the UE.

10. UE sends the requested CAG ID to the AMF within the NAS security mode command complete message, which is confidentiality and integrity protected. Here the requested CAG ID belongs to the match CAG IDs in step 2.

11. The AMF retrieves the subscription data from the UDM, which includes the subscribed CAG lists of the UE.

12. The AMF checks whether the requested CAG ID sending from UE is within both the NG-RAN’s allowed CAG Lists, and subscribed CAG lists in the UDM. If the checking does not pass, the AMF sends the registration reject message to the UE. Otherwise, the AMF does the following steps. Here denoting the requested CAG ID as the allowed CAG ID, if the above checking passes.

13. The AMF sends the allowed CAG ID to the NG-RAN within the N2 message.

14. The AMF sends the registration accept to the UE.

For the other registration scenarios, initial NAS protection shall be used here for the requested CAG ID protection while transferred from UE to AMF.

### 6.15.3 Evaluation

The above solution addresses the requirements of key issue #6.2: CAG ID Privacy.

The solution reuses the NAS security context to confidentially protect the CAG ID during the CAG access control, without introducing new security mechanism in UDM or AUSF.

The impact of the solution is to require the UE to send the requested CAG ID after NAS security is established. And then the AMF could check whether the requested CAG ID sending from UE is within both the NG-RAN's allowed CAG lists, and subscribed CAG lists in the UDM.

The compatibility of this security solution with the existing architecture solution would need more evaluation.

## 6.16 Solution #16: CAG ID privacy by sending CAG ID only in protected NAS signalling

### 6.16.1 Introduction

This solution addresses key issue #6.2: CAG ID Privacy.

### 6.16.2 Solution details

This solution proposes to modify the handling of CAG ID at idle to connected transitions on a CAG cell as follows:

- UE sends the CAG ID in the initial NAS message as a non-cleartext IE.

- NG-RAN node passes its supported list of CAG IDs along with the NAS message to the AMF.

- The AMF checks whether the CAG-ID the UE is trying to access is on the list of CAG IDs supported by the NG-RAN Node and allowed to be accessed by the UE based on the subscription data.

Editor's Note: This revised functionality should be checked by SA2, SA3, RAN3 and CT1.

The solution has the advantage that the CAG-ID that the UE is accessing is sent in encrypted NAS signalling.

### 6.16.3 Evaluation

TBD

## 6.17 Solution #17: Protection on TSC time synchronisation within UP security policy

### 6.17.1 Introduction

This solution addresses key issue #4.2 on UP security policy and TSC time synchronisation.

UPF forwards the gPTP message to the UE via user plane (i.e. using the PDU session applicable for sending gPTP messages). Only one PDU session per UE per UPF is used for sending gPTP messages regardless of how many external TSN working domains have their clock information delivered through a given UPF serving that UE.

### 6.17.2 Solution details

The 5GS needs to map configuration information obtained from the TSN network for the 5GS Bridge into 5GS QoS within PDU Session and TSC Assistance Information [7]. Similarly, SMF needs to map security requirements for TSC to assist the secure transfer of any message over a 5GS bridge.

The gPTP messages needed for the time synchronisation (i.e. distribution of the 5G system clock, time stamping) are received from the TSN network and transferred in 5GS in the user plane. In the establishment of a PDU session to the TSN working domain, the SMF provides gNB with the UP security policy, which also applies for gPTP messages transferred to the UE DS-TT. The SMF sets the UP security policy for encryption and integrity protection to "required" in order to protect these messages.

### 6.17.3 Evaluation

This solution meets the potential requirement of Key Issue #4.2.

## 6.18 Solution #18: CAG ID privacy considering RAN optimization

### 6.18.1 Introduction

This solution addresses key issue #6.2: CAG ID Privacy.

TS 23.502 [6] 4.2.2.2 step 1 mandates "*The AN parameter shall include a CAG Identifier if the UE is accessing the NG-RAN using a CAG cell* (see TS 23.501 [2] clause 5.30.3)." This is for optimized RAN procedures. The impact of privacy compromise is arguable due to the fact that the UE is accessing RAN anonymous and several other parameters are also sent in RAN in the clear for the same reason, i.e. RAN optimization.

### 6.18.2 Potential solution details

It is operator decision if the subscribers of its network are allowed to request access to a CAG already early in RAN message. In this case, the CAG ID is sent in the clear in RAN.

CAG ID shall always be protected as non-clear IE in NAS signalling.

### 6.18.3 Evaluation

This solution does not allow an eavesdropper to link a CAG ID to a specific SUPI-identified UE. However, if sent over RAN, up to operator configuration, the anonymity set gets reduced, but no personal identifiable information can be inferred. The solution keeps the balance between advantage of early knowledge of CAG ID in in RAN and any impact of a heavy privacy solution for CAG ID. When UE is sending CAG ID in RRCSetupRequest, an adversary can only connect the clear-text IEs in the NAS with the information sent in RAN. Thus, CAG ID is only possible to connect to a SUCI, a one-time identifier, but not the real identity SUPI of the UE. If the operator does not want to provide the advantage of early notification in RAN, the CAG ID is protected with the already existing mechanism for initial NAS protection. Thus, minimal impact to Rel-15 solution.

## 6.19 Solution #19: Privacy protected CAG ID Privacy in PNiNPNs

### 6.19.1 Introduction

This solution addresses the key issue #6.2: CAG ID Privacy.

As mentioned in the security threat of the key issue #6.2, during initial NAS Attach procedures (Registration procedures) from the NPN UEs, that are accessing using a CAG cell, the UE sends the selected matching CAG ID in clear over the air to the serving network. An attacker can eavesdrop on this message and identify the CAG Cell (CAG ID) that the UE is attempting to access. If the CAG Cells are sensitive in nature, it is possible for an attacker to link the UE to these sensitive CAGs.

This solution details on protecting CAG ID from eavesdropping, during the initial NAS procedure (Registration procedure) where the UE is accessing NG-RAN using a CAG cell and the UE does not have valid security context. This solution aligns with the procedure of sending selected CAG ID by the UE to the serving network in AN parameters.

### 6.19.2 Solution details

The steps below details on how the CAG ID is protected during initial NAS (Registration) procedure, when the UE is accessing the NG-RAN using a CAG cell and the UE does not have valid security context (UE does not have a GUTI or the stored GUTI is not valid):

1. During initial NAS (Registration) procedure, when the UE does not have valid security, then the UE protects CAG Identifier (CAG ID of the CAG cell that the UE attempts to access) by concealing the selected CAG Identifier to generate privacy protected CAG Identifier. UE constructs the privacy protected CAG Identifier (CCAG ID), if configured by the home network in the Allowed CAG List. CCAG ID (privacy protected CAG ID) is constructed by UE using the home operator network’s public key, protection scheme and method used for concealing the UE identifier in SUCI.

2. During initial NAS (Registration) request procedure to the serving network, the NPN UE sends the CCAG ID to the NG-RAN in AN Parameters. In this registration request procedure, the serving network's AMF receives the CCAG ID (concealed identifier of the CAG cell which the UE accesses) from the NG-RAN in N2 parameters.

3. As per TS 33.501[5] AMF/SEAF initiates primary authentication by sending in Nausf\_UEAuthentication\_Authenticate request message to the AUSF and includes in this request the concealed CAG identifier (CCAG ID) received from the NG-RAN. When the AMF receives the CAG ID from the UE via NG-RAN (in N2 parameters), with UE’s identity as SUCI (Concealed Subscription Identifier SUPI), then AMF considers received CAG ID is concealed CAG ID (CCAG ID) and forwards CCAG ID along with SUCI to UDM of the home network for de-concealment of CCAG ID.

4. If there is CCAG ID in the Nausf\_UEAuthentication\_Authenticate request received from SEAF, AUSF includes the CCAG ID in Nudm\_UEAuthentication\_Get Request message to the UDM.

5. If there is CCAG ID in Nudm\_UEAuthentication\_Get Request message then the UDM de-conceals the CCAG ID to CAG ID. The de-concealment of CCAG ID is done using same parameters, public key, protection mechanism and method used for de-concealing UE identifier in SUCI. The UDM de-conceals the SUCI to SUPI. If the UDM de-conceals SUPI and CAG ID (If there is CCAG ID in Nudm\_UEAuthentication\_Get Request message) successfully, then the UDM proceeds further with the procedures as specified in TS 33.501 [5] in authentication procedure, for example, selection of authentication method and generation of authentication vector, like so.

6. If the CAG ID is de-concealed successfully by the UDM, then the UDM includes the de-concealed "CAG ID" in Nudm\_UEAuthentication\_Get Response message to AUSF along with UE’s SUPI.

7. If there is "CAG ID" in Nudm\_UEAuthentication\_Get Response message from UDM, then the AUSF forwards the same to the AMF/SEAF in Nausf\_UEAuthentication\_Authenticate response message upon successful primary authentication of the UE.

8. If there is "CAG ID" in the Nausf\_UEAuthentication\_Authenticate response message from the AUSF, then the AMF uses this CAG ID as the selected CAG ID by the UE and proceed further with subsequent procedures . AMF may send this received CAG ID from the AUSF for the UE to the NG-RAN.

As home network public key and protection scheme used for SUCI and CCAG ID derivation are same, UDM that de-conceals SUCI will also be able to de-conceal CCAG ID. Sending privacy protected CAG ID (CCAG ID) over the air to the network prevents a man in the middle from identifying the NPN/CAG Cell that the UE is attempting to access.



Figure 6.19.2-1: CAG ID protection during Registration Procedure

### 6.19.3 Evaluation

Key Issue #6.2 is about privacy protection of CAG ID of the CAG cell that the UE selects and indicates to the network. The solution addresses the key issue by concealing the CAG ID using the protection mechanisms of the UE’s SUPI and sending the concealed CAG ID over the air to the serving network. This enables the UE (during Initial NAS attach procedures) to send protected CAG ID to the serving network when UE does not have a valid security context. The network (UDM) deconceals the CAG ID and returns the de-concealed CAG ID to the serving network AMF via AUSF. As home network public key and protection scheme used for concealing CAG ID and SUPI are same, UDM that de-conceals SUCI will also be able to de-conceal the CAG ID. This solution needs a mechanism to provide CAG ID to the UICC if the SUCI is calculated in the UICC.

The proposed solution meets the requirement of key issue #6.2.

# 7 Conclusions

## 7.1 Security for 5G LAN services

For Key Issue #3.1 (Authentication and Authorization of UE in 5GLAN communication), solution #6 in clause 6.6 is selected for normative work for Authentication and Authorization of UE in 5GLAN communication. A clause referencing TS 23.501 [7], TS 23.502 [6] and TS 33.501 [5] for secondary authentication for 5GLAN group communication service will be added to TS 33.501 [5].

It is recommended that the normative work for key issue #3.2 is based on Solution #2: Security solution for handling UP security policy for a 5GLAN Group on providing the same UP security policy for all 5G LAN group members, and Solution#7, which adds the additional aspect of SMF using for policy enforcement information provided by DN-AAA about protection mechanisms already applied by the DN in order to avoid double protection.

NOTE: The enforcement of the same UP security policy to all group members has no security reason, but it reduces complexity.

## 7.2 Security for TSC

For Key Issue #4.1 (Protection of interfaces that 5GS interact with TSN), solution #8 in clause 6.8 is selected for normative work, i.e. for authentication, a UE that is enabled to use TSC services authenticates to the 5GS using the procedures as specified in TS 33.501, clause 6.1.

For Key Issue #4.2 (UP security policy and TSC time synchronisation), solution #17 is selected, i.e. after the UE is authenticated and data connection is set up, any data received from a TSC bridge or another 5GS TSC-enabled UE is transported between DS-TT in the UE and NW-TT in the UPF in a protected way using the mechanisms for UP security as described in TS 33.501, clause 6.6. The SMF provides the UP security enforcement information for a PDU session to the ng-eNB/gNB. It is set it to "required" for data transferred to a 5GS TSC-enabled UE. This is also applicable to the gPTP messages sent in the user plane.

## 7.3 PLMN service access via SNPN and vice versa

It is concluded that no normative work for Key Issue #5.2 (Authentication and authorization of NPN subscribers by an AAA) is required, as addressed by the existing specification.

## 7.4 Key hierarchy for NPNs

The normative work for Key Issue #5.1 (Key hierarchy for NPNs) should be based on solution #5 in clause 6.5.

## 7.5 AKA based authentication and calculating KSEAF for SNPNs

The normative work for Key Issue #1.1 (Completing AKA based authentication and calculating KSEAF for SNPNs) should be based on solution #4 in clause 6.4.

## 7.6 Modification of CAG ID list in the UE

The normative work for key issue #6.3 (DoS attack by unauthorized removal of entries from the UE's Allowed CAG ID list) should be based on solution #10 in clause 6.10.

## 7.7 CAG ID Privacy

It is concluded that no normative work for Key Issue #6.2 (CAG ID Privacy) is required.

Annex A:  
Deployment options for authentication in SNPNs considering different types of NPN credentials

These deployment options are given as example only to ease the understanding of NPN.

Depending on whether a standalone NPN (SNPN) involves a AAA server (or simply the AAA server thereafter) in UE authentication, two options of deploying authentication schemes for 5G Core (5GC) for NPN should be considered:

- SNPN fully uses 5GC with authentication by AUSF/UDM/ARPF (referred to as *NPN-without-AAA*)

- SNPN involves a AAA server in authentication, which interworks with 5GC NFs (referred to as *NPN-with-AAA*)

NOTE: The reason of considering for SNPN an AAA server is that most enterprises deploying NPNs may already have AAA servers for authenticating their users. Thus, it may be desirable to allow a NPN to interwork with the AAA server. Further, it allows to illustrate how 5G core can function as an EAP pass-through authenticator without the need of implementing any specific authentication method. The involvement of an AAA server in an SNPN has impact on the role assignment in EAP framework.

**SNPN-without-AAA**

The SNPN fully uses 5GC without involving any AAA server to authenticate UEs. This case is equivalent to PLMN in terms of EAP role assignment. More specifically, UE acts as EAP peer, SEAF acts as pass-through authenticator, and AUSF acts as the EAP server (see figure A.1). Thus, authentication methods supported by this option are implemented by UE and AUSF. Note that each supported authentication method needs to be selectable by UDM.



Figure A.1

**SNPN-with-AAA**

The SNPN uses the AAA server to authenticate UE. In this case, UE and SEAF continue to take the role of EAP peer and pass-through authenticator respectively. However, the role of AUSF is subject to discussion, depending on how it is designed to interwork with the AAA server. More specifically, AUSF may continue to take the role of EAP server, take the role of pass-through authenticator (see figure below), or may not take any role at all. In the case that AUSF does not take the role of EAP server, the AAA server can take such role (see figure A.2).



Figure A.2

Thus, authentication methods supported by this option are implemented by UE and either by AUSF or the AAA server. In the latter case, the 5G core becomes transparent. However, interfaces need to be defined between 5G Core and the AAA server to transport EAP messages, as well as keying materials (e.g., MSK) that might be transported back from the AAA server.

**Types of UE Credentials in SNPN**

The types of UE credentials also play important role in both UE authentication and key hierarchy. More specifically, different types of UE credentials often require different authentication methods, which in turn have impact on EAP peer (UE) and EAP server (AUSF or AAA server). Further, different authentication methods also have impact on the key hierarchy. More specifically, it is distinguished between the following 2 credential types.

- a public key-based credential (e.g., certificate-based) allows to establish a root key, and

- a shared secret-based credential often serves as the root key itself, i.e., allowing to derive all subsequent keys from a shared secret.

Both 3GPP credentials and non-3GPP credentials should be supported for NPNs. 3GPP credentials are clearly defined in TS 33.501 [5]. Non-3GPP credentials can be classified as *certificate-based* and *non-certificate-based* (see table A.1).

Table A.1: Classification of UE Credentials in SNPNs

|  |  |  |
| --- | --- | --- |
| Credential Types in NPNs | UE credentials in NPNs | |
| 3GPP UE Credentials | Shared Symmetric Keys | |
| Non-3GPP UE Credentials | Certificate-based | Non-certificate-based |

**Combination options of deployment and credential type**

The combinations of two deployment options and two credentials types result in four authentication options for SNPNs (see table A.2).

Table A.2: Authentication Options in SNPN

|  |  |  |
| --- | --- | --- |
|  | NPN-without-AAA | NPN-with-AAA |
| Certificate-based UE Credentials | Option A.1  (EAP-TLS) | Option B.1 |
| Non-certificate-based UE Credentials | Option A.2 | Option B.2 |

**Remarks to the authentication options in SNPNs**

Among them, only Option A.1 is covered by TS 33.501, Annex B, which provides EAP-TLS as an example authentication method. The root of the key hierarchy is the EMSK established by TLS.

Option B.1 is suggested to not follow up, since AUSF needs to implement EAP-TLS to support Option A.1 anyway. Thus, this option appears to have only drawbacks without clear benefit .

For non-certificate-based UE credentials (Option A.2. and B.2), there are a number of authentication methods that can be considered. Once the authentication methods supported by NPNs are decided, the key hierarchy can be defined accordingly.

Annex B:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-12 | SA#86 | SP-191143 |  |  |  | Presented for approval | 2.0.0 |
| 2019-12 | SA#86 |  |  |  |  | EditHelp review + Change control version | 16.0.0 |
| 2020-07 | SA#88E | SP-200374 | 0001 | 2 | D | Introduction to Vertical LAN study | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0002 | 2 | F | Resolution of ed note on serving network name | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0003 | 2 | F | KI on interworking NPN and PLMN - security requirements | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0004 | 2 | F | KI on service continuity - threats and reqs | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0005 | 1 | F | Resolution of editors note on AAA | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0006 | 2 | F | Threats and requirements on AAA | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0007 | 1 | F | Resolution of editor's note in solution 1 | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0008 | 1 | F | Resolution of editor's note in solution 15 | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0009 | 1 | F | Resolution of editor's note on UP security policy enforcement | 16.1.0 |
| 2020-07 | SA#88E | SP-200374 | 0010 | - | F | Adding conclusion on KI #6.2 | 16.1.0 |