ETSI TS 133 501 V15.2.0 (2018-10)

TECHNICAL SPECIFICATION

5G;
Security architecture and procedures for 5G System
(3GPP TS 33.501 version 15.2.0 Release 15)

Reference

RTS/TSGS-0333501vf20

Keywords

5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification 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.

1 Scope

The present document specifies the security architecture, i.e., the security features and the security mechanisms for the 5G System and the 5G Core, and the security procedures performed within the 5G System including the 5G Core and the 5G New Radio.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

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

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method ^{f}or 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

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

[26] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)"

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available http://www.secg.org/sec1-v2.pdf

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at http://www.secg.org/sec2-v2.pdf

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

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

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] IETF RFC 4282: "The Network Access Identifier".

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] IETF RFC 4279 "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

[60] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[61] RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

3 Definitions and abbreviations

3.1 Definitions

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

5G security context: The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.

NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.

NOTE 2: A 5G security context has type "mapped", "full native" or "partial native". Its state can either be "current" or "non-current". A context can be of one type only and be in one state at a time. The state of a particular context type can change over time. A partial native context can be transformed into a full native. No other type transformations are possible.

5G AS security context for 3GPP access: The cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UP Security Policy at the network side, and the counters used for replay protection.

NOTE 3: NH and NCC need to be stored also at the AMF during connected mode.

5G AS security context for non-3GPP access: The key K_{N3IWF}, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec SA.

5G Home Environment Authentication Vector: authentication data consisting of RAND, AUTN, XRES*, and K_{AUSF} for the purpose of authenticating the UE using 5G AKA.

NOTE 3a: This vector is received by the AUSF from the UDM/ARPF in the Nudm_Authentication_Get Response.

5G Authentication Vector: authentication data consisting of RAND, AUTN, HXRES*, and K_{SEAF}.

NOTE 3b: This vector is received by the SEAF from the AUSF in the Nausf_Authentication_Authenticate Response.

5G NAS security context: The key K_{AMF} with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values.

NOTE 4: The distinction between native 5G security context and mapped 5G security context also applies to 5G NAS security contexts. The 5G NAS security context is called "full" if it additionally contains the integrity and encryption keys and the associated identifiers of the selected NAS integrity and encryption algorithms.

5G Serving Environment Authentication Vector: a vector consisting of RAND, AUTN and HXRES*.

activation of security context: The process of taking a security context into use.

applicaton Layer Security: mechanism by which HTTP messages, exchanged between a Network Function in one PLMN and a Network Function in another PLMN, are protected on the N32-f interface between the two SEPPs in the two PLMNs.

anchor key: The security key K_{SEAF} provided during authentication and used for derivation of subsequent security keys.

authentication data: An authentication vector or transformed authentication vector.

authentication vector: A vector consisting of CK, IK, RAND, AUTN, and XRES.

backward security: The property that for an entity with knowledge of K_n, it is computationally infeasible to compute any previous K_{n-m} (m>0) from which K_n is derived.

NOTE 5: In the context of K_{gNB} key derivation, backward security refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to compute any previous K_{gNB} that has been used between the same UE and a previous gNB.

CM-CONNECTED state: This is as defined in TS 23.501 [2].

NOTE5a: The term CM-CONNECTED state corresponds to the term 5GMM-CONNECTED mode used in TS 24.501 [35].

CM-IDLE state: As defined in TS 23.501 [2].

NOTE5b: The term CM-IDLE state corresponds to the term 5GMM-IDLE mode used in TS 24.501 [35].

consumer's IPX (cIPX): IPX provider entity with a business relationship with the cSEPP operator.

consumer's SEPP (cSEPP): The SEPP residing in the PLMN where the service consumer NF is located.

current 5G security context: The security context which has been activated most recently.

NOTE5c: A current 5G security context originating from either a mapped or native 5G security context can exist simultaneously with a native non-current 5G security context.

forward security: The fulfilment of the property that for an entity with knowledge of K_m that is used between that entity and a second entity, it is computationally infeasible to predict any future K_{m+n} (n>0) used between a third entity and the second entity.

NOTE 6: In the context of K_{gNB} key derivation, forward security refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to predict any future K_{gNB} that will be used between the same UE and another gNB. More specifically, n hop forward security refers to the property that a gNB is unable to compute keys that will be used between a UE and another gNB to which the UE is connected after n or more handovers (n=1 or more).

full native 5G security context: A native 5G security context for which the 5G NAS security context is full according to the above definition.

NOTE6a: A full native 5G security context is either in state "current" or state "non-current".

Home Network Identifier: An identifier identifying the home network of the subscriber.

NOTE6b: Described in detail in TS 23.003 [19].

Home Network Public Key Identifier: An identifier used to indicate which public/private key pair is used for SUPI protection and de-concealment of the SUCI.

NOTE6c: Described in this document and detailed in TS 23.003 [19].

mapped 5G security context: An 5G security context, whose K_{AMF} was derived from EPS keys during interworking and which is identified by mapped ngKSI.

N32-c connection: A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN.

NOTE 6d: This is a long-lived connection that's used between the SEPPs for cipher suite and protection policy exchange, and error notifications.

N32-f connection: Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages.

NOTE 6e: When IPX providers are present in the path between the two SEPPs, an N32-f HTTP connection is setup on each hop towards the other SEPP.

native 5G security context: An 5G security context, whose K_{AMF} was created by a run of primary authentication and which is identified by native ngKSI.

non-current 5G security context: A native 5G security context that is not the current one.

NOTE 7: A non-current 5G security context may be stored along with a current 5G security context in the UE and the AMF. A non-current 5G security context does not contain 5G AS security context. A non-current 5G security context is either of type "full native" or of type "partial native".

partial native 5G security context: A partial native 5G security context consists of K_{AMF} with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values, which are initially set to zero before the first NAS SMC procedure for this security context.

NOTE 8: A partial native 5G security context is created by primary authentication, for which no corresponding successful NAS SMC has been run. A partial native context is always in state "non-current".

producer's IPX (pIPX): IPX provider entity with a business relationship with the pSEPP operator.

producer's SEPP (pSEPP): The SEPP residing in the PLMN where the service producer NF is located.

Routing Indicator: An indicator defined in TS 23.003 [19] that can be used for AUSF or UDM selection.

RM-DEREGISTERED state: This is as defined in TS 23.501 [2].

NOTE8a: The term RM-DEREGISTERED state corresponds to the term 5GMM-DEREGISTERED mode used in TS 24.501 [35].

RM-REGISTERED state: As defined in TS 23.501 [2].

NOTE8b: The term RM-REGISTERED state corresponds to the term 5GMM-REGISTERED mode used in TS 24.501 [35].

Scheme Output: the output of a public key protection scheme used for SUPI protection.

security anchor function: The function that serves in the serving network as the anchor for security in 5G.

subscription identifier: The SUbscription Permanent Identifier (SUPI).

NOTE8c: As defined in TS 23.501 [2] and detailed in 23.003 [19].

subscription identifier de-concealing function: The Subscription Identifier De-concealing Function (SIDF) service offered by the network function UDM in the home network of the subscriber responsible for de-concealing the SUPI from the SUCI.

subscription concealed identifier: A one-time use subscription identifier, called the SUbscription Concealed Identifier (SUCI), which contains the scheme-output, and additional non-concealed information needed for home network routing and protection scheme usage.

NOTE8d: Defined in the present document; detailed in TS 23.003 [19].

subscription credential(s): The set of values in the USIM and the ARPF, consisting of at least the long-term key(s) and the subscription identifier SUPI, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.

transformed authentication vector: an authentication vector where CK and IK have been replaced with CK' and IK'.

UE security capabilities: The set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE.

NOTE 9: This includes capabilities for NG-RAN and 5G NAS, and includes capabilities for EPS, UTRAN and GERAN if these access types are supported by the UE.

UE 5G security capability: The UE security capabilities for 5G AS and 5G NAS.

Master node: As defined in TS 37.340 [51].

ng-eNB: As defined in TS 38.300 [52].

Secondary node: As defined in TS 37.340 [51].

5G AS Secondary Cell security context: This context consists of the cryptographic keys at AS level for secondary cell with their identifiers , the identifier of the selected AS level cryptographic algorithms for secondary cell, the UP Security Policy at the network side, and counters used for replay protection.

ABBA parameter: Anti-Bidding down Between Architectures (ABBA) parameter provides antibidding down protection of security features against security features introduced in higher release to a lower release and indicates the security features that are enabled in the current network.

3.2 Abbreviations

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

5GC	5G Core Network
5G-AN	5G Access Network
5G-RAN	5G Radio Access Network
5G AV	5G Authentication Vector
AEAD	Authenticated Encryption with Associated Data
5G AV	5G Authentication Vector
5G HE AV	5G Home Environment Authentication Vector
5G SE AV	5G Serving Environment Authentication Vector
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
ALS	Application Layer Security
AMF	Access and Mobility Management Function
AMF	Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
AUTN	AUthentication TokeN
AV	Authentication Vector
AV'	transformed Authentication Vector
Cell-ID	Cell Identity as used in TS 38.331 [22]

cIPX	consumer's IPX
CP	Control Plane
cSEPP	consumer's SEPP
CTR	Counter (mode)
CU	Central Unit
DN	Data Network
DNN	Data Network Name
DU	Distributed Unit
EAP	Extensible Authentication Protocol
EMSK	Extended Master Session Key
EPS	Evolved Packet System
gNB	NR Node B
GUTI	Globally Unique Temporary UE Identity
HRES	Hash RESponse
HXRES	Hash eXpected RESponse
IKE	Internet Key Exchange
IPX	IP exchange service
KSI	Key Set Identifier
LI	Lawful Intercept
MN	Master Node
MR-DC	Multi-RAT Dual Connectivity
MSK	Master Session Key
N3IWF	Non-3GPP access InterWorking Function
NAI	Network Access Identifier
NAS	Non Access Stratum
NDS	Network Domain Security
NEA	Encryption Algorithm for 5G
NF	Network Function
NG	Next Generation
ng-eNB	Next Generation Evolved Node-B
ngKSI	Key Set Identifier in 5G
NIA	Integrity Algorithm for 5G
NR	New Radio
NSSAI	Network Slice Selection Assistance Information
PDN	Packet Data Network
PEI	Permanent Equipment Identifier
pIPX	producer's IPX
pSEPP	producer's SEPP
QoS	Quality of Service
RES	RESponse
SCG	Secondary Cell Group
SEAF	SEcurity Anchor Function
SEG	Security Gateway
SEPP	Security Edge Protection Proxy
SIDF	Subscription Identifier De-concealing Function
SMC	Security Mode Command
SMF	Session Management Function
SN	Secondary Node
SN Id	Serving Network Identifier
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UE	User Equipment
UEA	UMTS Encryption Algorithm
UDM	Unified Data Management
UIA	UMTS Integrity Algorithm
ULR	Update Location Request
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
XRES	eXpected RESponse

4 Overview of security architecture

4.1 Security domains

Figure 4-1 gives an overview of security architecture.

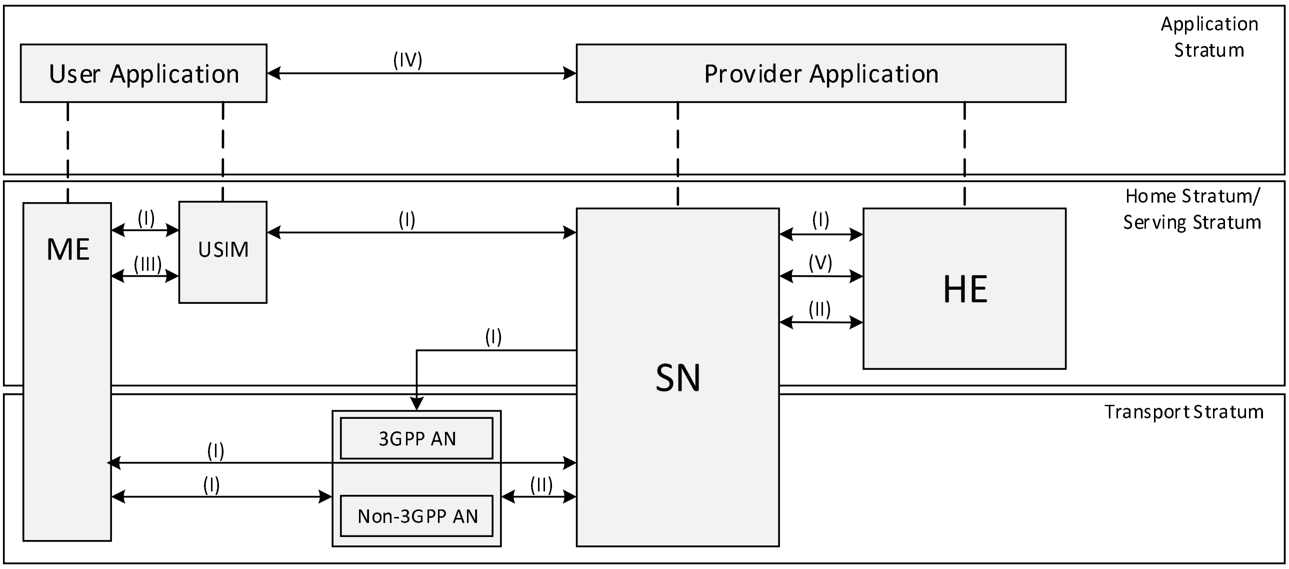

Figure 4-1: Overview of the security architecture

The figure illustrates the following security domains:

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.

- Network domain security (II): the set of security features that enable network nodes to securely exchange signalling data and user plane data.

- User domain security (III): the set of security features that secure the user access to mobile equipment.

- Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely. Application domain security is out of scope of the present document.

- SBA domain security (V): the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains . Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401 [10].

- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

Note: The visibility and configurability of security is not shown in the figure.

4.2 Security entity at the perimeter of the 5G Core network

To protect messages that are sent over the N32 interface, 5G System architecture introduces Security Edge Protection Proxy (SEPP) as the entity sitting at the perimeter of the PLMN network that:

- receives all service layer messages from the Network Function and protects them before sending them out of the network on the N32 interface and

- receives all messages on the N32 interface and forwards them to the appropriate Network Function after verifying security, where present.

The SEPP implements application layer security for all the service layer information exchanged between two NFs across two different PLMNs.

4.3 Security entities in the 5G Core network

The 5G System architecture introduces the following security entities in the 5G Core network:

AUSF:	AUthentication Server Function;
ARPF:	Authentication credential Repository and Processing Function;
SIDF:	Subscription Identifier De-concealing Function;
SEAF:	SEcurity Anchor Function.

5 Security requirements and features

5.1 General security requirements

5.1.1 Mitigation of bidding down attacks

An attacker could attempt a bidding down attack by making the UE and the network entities respectively believe that the other side does not support a security feature, even when both sides in fact support that security feature. It shall be ensured that a bidding down attack, in the above sense, can be prevented.

5.1.2 Authentication and Authorization

The 5G system shall satisfy the following requirements.

Subscription authentication: The serving network shall authenticate the Subscription Permanent Identifier (SUPI) in the process of authentication and key agreement between UE and network.

Serving network authentication: The UE shall authenticate the serving network identifier through implicit key authentication.

NOTE 1: The meaning of 'implicit key authentication' here is that authentication is provided through the successful use of keys resulting from authentication and key agreement in subsequent procedures.

NOTE 2: The preceding requirement does not imply that the UE authenticates a particular entity, e.g. an AMF, within a serving network.

UE authorization: The serving network shall authorize the UE through the subscription profile obtained from the home network. UE authorization is based on the authenticated SUPI.

Serving network authorization by the home network: Assurance shall be provided to the UE that it is connected to a serving network that is authorized by the home network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful authentication and key agreement run.

Access network authorization: Assurance shall be provided to the UE that it is connected to an access network that is authorized by the serving network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful establishment of access network security. This access network authorization applies to all types of access networks.

Unauthenticated Emergency Services: In order to meet regulatory requirements in some regions, the 5G system shall support unauthenticated access for emergency services. This requirement applies to all MEs and only to those serving networks where regulatory requirements for unauthenticated emergency services exist. Serving networks located in regions where unauthenticated emergency services are forbidden shall not support this feature.

5.1.3 Requirements on 5GC and 5G-RAN related to keys

The 5GC and 5G-RAN shall allow for use of encryption and integrity protection algorithms for AS and NAS protection having keys of length 128 bits. The network interfaces shall support the transport of 256 bit keys.

The keys used for UP, NAS and AS protection shall be dependent on the algorithm with which they are used.

5.2 Requirements on the UE

5.2.1 General

The support and usage of ciphering and integrity protection between the UE and the ng-eNB is identical to the support and usage of ciphering and integrity protection between the UE and the eNB as specified in TS 33.401 [10].

The PEI shall be securely stored in the UE to ensure the integrity of the PEI.

5.2.2 User data and signalling data confidentiality

The UE shall support ciphering of user data between the UE and the gNB.

The UE shall activate ciphering of user data based on the indication sent by the gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 as defined in Annex D of the present document.

The UE shall implement the ciphering algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Confidentiality protection of the user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [21] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

5.2.4 Secure storage and processing of subscription credentials

The following requirements apply for the storage and processing of the subscription credentials used to access the 5G network:

The subscription credential(s) shall be integrity protected within the UE using a tamper resistant secure hardware component.

The long-term key(s) of the subscription credential(s) (i.e. K) shall be confidentiality protected within the UE using a tamper resistant secure hardware component.

The long-term key(s) of the subscription credential(s) shall never be available in the clear outside of the tamper resistant secure hardware component.

The authentication algorithm(s) that make use of the subscription credentials shall always be executed within the tamper resistant secure hardware component.

It shall be possible to perform a security evaluation / assessment according to the respective security requirements of the tamper resistant secure hardware component.

NOTE: The security assessement scheme used for the security evaluation of the tamper resistant secure hardware component is outside the scope of 3GPP specifications.

5.2.5 Subscriber privacy

The UE shall support 5G-GUTI.

The SUPI should not be transferred in clear text over 5G-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC).

The Home Network Public Key shall be stored in the USIM.

The protection scheme identifier shall be stored in the USIM.

The ME shall support the null-scheme.

If the home network has not provisioned the Home Network Public Key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME.

Based on home operator's decision, indicated by the USIM, the calculation of the SUCI shall be performed either by the USIM or by the ME.

NOTE 1: If the indication is not present, the calculation is in the ME.

In case of an unauthenticated emergency call, privacy protection for SUPI is not required.

Provisioning, and updating the Home Network Public Key in the USIM shall be in the control of the home network operator.

NOTE 2: The provisioning and updating of the Home Network Public Key is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism.

Subscriber privacy enablement shall be under the control of the home network of the subscriber.

The UE shall only send the PEI in the NAS protocol after NAS security context is established, unless during emergency registration when no NAS security context can be established.

The Routing Indicator shall be stored in the USIM. If the Routing Indicator is not present in the USIM, the ME shall set it to a default value as defined in TS 23.003 [19].

5.3 Requirements on the gNB

5.3.1 General

The security requirements given in this section apply to all types of gNBs. More stringent requirements for specific types of gNBs may be defined in other 3GPP specifications.

5.3.2 User data and signalling data confidentiality

The gNB shall support ciphering of user data between the UE and the gNB.

The gNB shall activate ciphering of user data based on the security policy sent by the SMF.

The gNB shall support ciphering of RRC-signalling.

The gNB shall implement the following ciphering algorithms:

- NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The gNB may implement the following ciphering algorithm:

- 128-NEA3 as defined in Annex D of the present document.

Confidentiality protection of user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.3.3 User data and signalling data integrity

The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.

The gNB shall activate integrity protection of user data based on the security policy sent by the SMF.

The gNB shall support integrity protection and replay protection of RRC-signalling.

The gNB shall support the following integrity protection algorithms:

- NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The gNB may support the following integrity protection algorithm:

- 128-NIA3 as defined in Annex D of the present document.

Integrity protection of the user data between the UE and the gNB is optional to use, and shall not use NIA0.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB. NIA0 will add an unnecessary overhead of 32-bits MAC with no security benefits.

All RRC signalling messages except those explicitly listed in TS 38.331 [21] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

NIA0 shall be disabled in gNB in the deployments where support of unauthenticated emergency session is not a regulatory requirement.

5.3.4 Requirements for the gNB setup and configuration

Setting up and configuring gNBs by O&M systems shall be authenticated and authorized by gNB so that attackers shall not be able to modify the gNB settings and software configurations via local or remote access.

The certificate enrolment mechanism specified in TS 33.310 [6] for base station should be supported for gNBs. The decision on whether to use the enrolment mechanism is left to operators.

Communication between the O&M systems and the gNB shall be confidentiality, integrity and replay protected from unauthorized parties. The security associations between the gNB and an entity in the 5G Core or in an O&M domain trusted by the operator shall be supported. These security association establishments shall be mutually authenticated. The security associations shall be realized according to TS 33.210 [3] and TS 33.310 [5].

The gNB shall be able to ensure that software/data change attempts are authorized.

The gNB shall use authorized data/software.

Sensitive parts of the boot-up process shall be executed with the help of the secure environment.

Confidentiality of software transfer towards the gNB shall be ensured.

Integrity protection of software transfer towards the gNB shall be ensured.

The gNB software update shall be verified before its installation (cf. sub-clause 4.2.3.3.5 of TS 33.117 [24]).

5.3.5 Requirements for key management inside the gNB

The 5GC provides subscription specific session keying material for the gNBs, which also hold long term keys used for authentication and security association setup purposes. Protecting all these keys is important. The following requirements apply:

Any part of a gNB deployment that stores or processes keys in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then keys in cleartext shall be stored and processed in a secure environment. Keys stored inside a secure environment in any part of the gNB shall never leave the secure environment except when done in accordance with this or other 3GPP specifications.

5.3.6 Requirements for handling user plane data for the gNB

Any part of a gNB deployment that stores or processes user plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then user plane data in cleartext shall be stored and processed in a secure environment.

5.3.7 Requirements for handling control plane data for the gNB

Any part of a gNB deployment that stores or processes control plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then control plane data in cleartext shall be stored and processed in a secure environment.

5.3.8 Requirements for secure environment of the gNB

The secure environment is logically defined within the gNB. It ensures protection and secrecy of all sensitive information and operations from any unauthorized access or exposure. The following list defines the requirements of the secure environment:

The secure environment shall support secure storage of sensitive data, e.g. long-term cryptographic secrets and vital configuration data.

The secure environment shall support the execution of sensitive functions, e.g. en-/decryption of user data and the basic steps within protocols which use longterm secrets (e.g. in authentication protocols).

The secure environment shall support the execution of sensitive parts of the boot process.

The secure environment's integrity shall be assured.

Only authorised access shall be granted to the secure environment, i.e. to data stored and used within it, and to functions executed within it.

5.3.9 Requirements for the gNB F1 interfaces

Requirements given below apply to gNBs with split DU-CU implementations using F1 interface defined in TS 38.470 [31]. Signalling traffic (i.e. both F1-C interface management traffic defined in TS 38.470 [31] and F1-C signalling bearer defined in TS 38.472 [32] and user plane data can be sent on the F1 interface between a given DU and its CU.

F1-C interface shall support confidentiality, integrity and replay protection.

All management traffic carried over the CU-DU link shall be integrity, confidentiality and replay protected.

The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane.

F1-C and management traffic carried over the CU-DU link shall be protected independently from F1-U traffic.

NOTE: The above requirements allow to have F1-U protected differently (including turning integrity and/or encryption off or on for F1-U) from all other traffic on the CU-DU (e.g. the traffic over F1-C).

5.3.10 Requirements for the gNB E1 interfaces

Requirements given below apply to gNBs with split DU-CU implementions, particularly with an open interface between CU-CP and CU-UP using the E1 interface defined in TS 38.460[41].

The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected

5.4 Requirements on the ng-eNB

The security requirements for ng-eNB are as specified for eNB in TS 33.401 [10].

5.5 Requirements on the AMF

5.5.1 Signalling data confidentiality

The AMF shall support ciphering of NAS-signalling.

The AMF shall support the following ciphering algorithms:

- NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The AMF may support the following ciphering algorithm:

- 128-NEA3 as defined in Annex D of the present document.

Confidentiality protection NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.5.2 Signalling data integrity

The AMF shall support integrity protection and replay protection of NAS-signalling.

The AMF shall support the following integrity protection algorithms:

- NIA-0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The AMF may support the following integrity protection algorithm:

- 128-NIA3 as defined in Annex D of the present document.

NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement.

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected with an algorithm different to NIA-0 except for emergency calls.

5.5.3 Subscriber privacy

The AMF shall support to trigger primary authentication using the SUCI.

The AMF shall support assigning 5G-GUTI to the UE.

The AMF shall support reallocating 5G-GUTI to UE.

The AMF shall be able to confirm SUPI from UE and from home network. The AMF shall deny service to the UE if this confirmation fails.

5.6 Requirements on the SEAF

The security anchor function (SEAF) provides the authentication functionality via the AMF in the serving network. The SEAF shall fulfil the following requirements:

The SEAF shall support primary authentication using SUCI.

5.7 Void

5.8 Requirements on the UDM

5.8.1 Generic requirements

The long-term keys used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM.

5.8.2 Subscriber privacy related requirements to UDM and SIDF

The SIDF is responsible for de-concealment of the SUCI and shall fulfil the following requirements:

- The SIDF shall be a service offered by UDM.
- The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

The home network key used for subscriber privacy shall be protected from physical attacks in the UDM.

When private/public key pair(s) used for subscriber privacy, the UDM shall hold the key identifier(s).

The algorithm used for subscriber privacy shall be executed in the secure environment of the UDM.

5.8a Requirements on AUSF

The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access.

The AUSF shall provide SUPI to the VPLMN only after authentication confirmation if authentication request with SUCI was sent by VPLMN.

The AUSF shall inform the UDM that a successful or unsuccessful authentication of a subscriber has occurred.

5.9 Core network security

5.9.1 Trust boundaries

It is assumed for the set of requirements in this sub-clause that mobile network operators subdivide their networks into trust zones. Subnetworks of different operators are assumed to lie in different trust zones. Messages that traverse trust boundaries shall follow the requirements in sub-clause 5.9.2 of the present document, if not protected end to end by NDS/IP as specified in TS 33.210 [3].

5.9.2 Requirements on service-based architecture

Editor's note: Security Requirements for service-based interfaces are ffs

5.9.2.1 Security Requirements for service registration, discovery and authorization

NF Service Based discovery and registration shall support confidentiality, integrity, and replay protection.

NRF shall be able to ensure that NF Discovery and registration requests are authorized.

NF service based discovery and registration shall be able to hide the topology of the available / supported NF's in one administrative/trust domain from entities in different trust/administrative domains (e.g. between NFs in visited and the home networks.)

NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer.

Each NF shall validate all incoming messages. Messages that are not valid according to the protocol specification and network state shall be either rejected or discarded by the NF.

5.9.2.2 NRF security requirements

The Network Repository Function (NRF) receives NF Discovery Request from an NF instance, provides the information of the discovered NF instances to the NF instance, and maintains NF profiles.

The following NRF service-based architecture security requirements shall apply:

NRF and NFs that are requesting service shall be mutually authenticated.

NRF may provide authentication and authorization to NFs for establishing secure communication between each other

5.9.2.3 NEF security requirements

The Network Exposure Function (NEF) supports external exposure of capabilities of Network Functions to Application Functions, which interact with the relevant Network Functions via the NEF.

The interface between the NEF and the Application Function shall fulfil the following requirements:

- Integrity protection, replay protection and confidentiality protection for communication between the NEF and Application Function shall be supported.
- Mutual authentication between the NEF and Application Function shall be supported.
- Internal 5G Core information such as DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain.
- SUPI shall not be sent outside the 3GPP operator domain by NEF.

The NEF shall be able to determine whether the Application Function is authorized to interact with the relevant Network Functions..

5.9.3 Requirements for e2e core network interconnection security

5.9.3.1 General

The present sub-clause contains requirements common to sub-clauses 5.9.2 and 5.9.3.

A solution for e2e core network interconnection security shall satisfy the following requirements.

The solution shall support application layer mechanisms for addition, deletion and modification of message elements by intermediate nodes except for specific message elements described in the present document.

NOTE: Typical example for such a case is IPX providers modifying messages for routing purposes.

The solution shall provide confidentiality and/or integrity end-to-end between source and destination network for specific message elements identified in the present document. For this requirement to be fulfilled, the SEPP – cf

[2], clause 6.2.17 shall be present at the edge of the source and destination networks dedicated to handling e2e Core Network Interconnection Security. The confidentiality and/or integrity for the message elements is provided between two SEPPs of the source and destination PLMN–.

The destination network shall be able to determine the authenticity of the source network that sent the specific message elements protected according to the preceding bullet. For this requirement to be fulfilled, it shall suffice that a SEPP in the destination network that is dedicated to handling e2e Core Network Interconnection Security can determine the authenticity of the source network.

The solution should have minimal impact and additions to 3GPP-defined network elements.

The solution should be using standard security protocols.

The solution shall cover interfaces used for roaming purposes.

The solution should take into account considerations on performance and overhead.

The solution shall cover prevention of replay attacks.

The solution shall cover algorithm negotiation and prevention of bidding down attacks.

The solution should take into account operational aspects of key management.

5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)

The SEPP shall act as a non-transparent proxy node.

The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs that use the N32 interface to communicate with each other.

The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network.

The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.

The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties.

As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs.

The receiving SEPP shall be able to verify whether the sending SEPP is authorized to use the PLMN ID in the received N32 message.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications.

NOTE 1: Such a differentiation could be done e.g. by implementing separate certificate storages.

The SEPP shall discard malformed N32 signaling messages.

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling. This includes SEPP-to-SEPP signaling messages.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).

NOTE 2: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP's own PLMN, the message is discarded.

5.9.3.3 Protection of attributes

Integrity protection shall be applied to all attributes transferred over the N32 interface.

Confidentiality protection shall be applied to all attributes specified in SEPP's Data-type Encryption Policy (clause 13.2.3.2). The following attributes shall be confidentiality protected when being sent over the N32 interface, irrespective of the Data-type Encryption Policy:

- Authentication Vectors
- Cryptographic material
- Location data, e.g. Cell ID and Physical Cell ID

The following attributes should additionally be confidentiality protected when being sent over the N32 interface:

- SUPI

5.10 Visibility and configurability

5.10.1 Security visibility

Although in general the security features should be transparent to the user or application, for certain events and according to the user's or application's concern, greater visibility of the operation of following security feature shall be provided:

- AS confidentiality: (AS confidentiality, Confidentiality algorithm, bearer information)
- AS integrity: (AS integrity, Integrity algorithm, bearer information)
- NAS confidentiality: (NAS confidentiality, Confidentiality algorithm)
- NAS integrity: (NAS integrity, Integrity algorithm)

The UE shall provide above security information to the applications in the UE (e.g. via APIs), on a per PDU session granularity.

The serving network identifier shall be available for applications in the UE.

5.10.2 Security configurability

Security configurability lets a user to configure certain security feature settings on a UE that allows the user to manage additional capability or use certain advanced security features.

The following configurability feature should be provided:

- Granting or denying access to USIM without authentication as described in TS 33.401 [10].

5.11 Requirements for algorithms, and algorithm selection

5.11.1 Algorithm identifier values

5.11.1.1 Ciphering algorithm identifier values

All identifiers and names specified in this sub-clause are for 5G NAS and New Radio. In relation to AS capabilities, the identifiers and names for E-UTRAN connected to 5GC are specified in TS 33.401 [10].

Each encryption algorithm will be assigned a 4-bit identifier. The following values for ciphering algorithms are defined:

"0000_2"	NEA0	Null ciphering algorithm;
"0001_2"	128-NEA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NEA2	128-bit AES based algorithm; and
"0011_2"	128-NEA3	128-bit ZUC based algorithm.

128-NEA1 is based on SNOW 3G (see TS 35.215 [14]).

128-NEA2 is based on 128-bit AES [15] in CTR mode [16].

128-NEA3 is based on 128-bit ZUC (see TS 35.221 [18]).

Full details of the algorithms are specified in Annex D.

5.11.1.2 Integrity algorithm identifier values

All identifiers and names specified in the present sub-clause are for 5G NAS and New Radio. In relation to AS capabilities, the identifiers and names for E-UTRAN connected to 5GC are specified in TS 33.401 [10].

Each integrity algorithm used for 5G will be assigned a 4-bit identifier. The following values for integrity algorithms are defined:

"0000_2"	NIA0	Null Integrity Protection algorithm;
"0001_2"	128-NIA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NIA2	128-bit AES based algorithm; and
"0011_2"	128-NIA3	128-bit ZUC based algorithm.

128-NIA1 is based on SNOW 3G (see TS 35.215 [14]).

128-NIA2 is based on 128-bit AES [15] in CMAC mode [17].

128-NIA3 is based on 128-bit ZUC (see TS 35.221 [18]).

Full details of the algorithms are specified in Annex D.

5.11.2 Requirements for algorithm selection

a) UE in RRC_Connected and a serving network shall have agreed upon algorithms for

  - Ciphering and integrity protection of RRC signalling and user plane (to be used between UE and gNB)

  - Ciphering and integrity protection of RRC signalling and ciphering of user plane (to be used between UE ng-eNB)

  - NAS ciphering and NAS integrity protection (to be used between UE and AMF)

b) The serving network shall select the algorithms to use dependent on

  - the UE security capabilities of the UE,

  - the configured allowed list of security capabilities of the currently serving network entity

c) The UE security capabilities shall include NR NAS algorithms for NAS level, NR AS algorithms for AS layer and LTE algorithms for AS level if the UE supports E-UTRAN connected to 5GC.

NOTE: If the UE supports both E-UTRAN and NR connected to 5GC, the UE 5G security capabilities include both the LTE and NR algorithms.

d) Each selected algorithm shall be indicated to a UE in a protected manner such that a UE is ensured that the integrity of algorithm selection is protected against manipulation.

e) The UE security capabilities shall be protected against "bidding down attacks".

f) It shall be possible that the selected AS and NAS algorithms are different at a given point of time.

6 Security procedures between UE and 5G network functions

6.1 Primary authentication and key agreement

6.1.1 Authentication framework

6.1.1.1 General

The purpose of the primary authentication and key agreement procedures is to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the K_{SEAF} provided by the AUSF of the home network to the SEAF of the serving network.

Keys for more than one security context can be derived from the K_{SEAF} without the need of a new authentication run. A concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

The anchor key K_{SEAF} is derived from an intermediate key called the K_{AUSF}. The K_{AUSF} may be securely stored in the AUSF based on the home operator's policy on using such key.

NOTE 1: This feature is an optimization that might be useful, for example, when a UE registers to different serving networks for 3GPP-defined access and untrusted non-3GPP access (this is possible according to TS 23.501 [2]). The details of this feature are operator-specific and not in scope of this document.

NOTE 2: A subsequent authentication based on the K_{AUSF} stored in the AUSF gives somewhat weaker guarantees than an authentication directly involving the ARPF and the USIM. It is rather comparable to fast re-authentication in EAP-AKA'.

NOTE 2a: Void.

UE and serving network shall support EAP-AKA' and 5G AKA authentication methods.

The USIM shall reside on a UICC. The UICC may be removable or non removable.

NOTE 3: For non-3GPP access networks USIM applies in case of terminal with 3GPP access capabilities.

If the terminal supports 3GPP access capabilities, the credentials used with EAP-AKA' and 5G AKA for non-3GPP access networks shall reside on the UICC.

NOTE 4: EAP-AKA' and 5G AKA are the only authentication methods that are supported in UE and serving network, hence only they are described in sub-clause 6.1.3 of the present document. For a private network using the 5G system as specified in [7] an example of how additional authentication methods can be used with the EAP framework is given in the informative Annex B.

6.1.1.2 EAP framework

The EAP framework is specified in RFC 3748 [27]. It defines the following roles: peer, pass-through authenticator and back-end authentication server. The back-end authentication server acts as the EAP server, which terminates the EAP authentication method with the peer. In the 5G system, when EAP-AKA' is used, the EAP framework is supported in the following way:

- The UE takes the role of the peer.
- The SEAF takes the role of pass-through authenticator.
- The AUSF takes the role of the backend authentication server.

6.1.1.3 Granularity of anchor key binding to serving network

The primary authentication and key agreement procedures shall bind the K_{SEAF} to the serving network. The binding to the serving network prevents one serving network from claiming to be a different serving network, and thus provides implicit serving network authentication to the UE.

This implicit serving network authentication shall be provided to the UE irrespective of the access network technology, so it applies to both 3GPP and non-3GPP access networks.

Furthermore, the anchor key provided to the serving network shall also be specific to the authentication having taken place between the UE and a 5G core network, i.e. the K_{SEAF} shall be cryptographically separate from the key K_{ASME} delivered from the home network to the serving network in earlier mobile network generations.

The anchor key binding shall be achieved by including a parameter called "serving network name" into the chain of key derivations that leads from the long-term subscriber key to the anchor key.

The value of serving network name is defined in sub-clause 6.1.1.4 of the present document.

The chain of key derivations that leads from the long-term subscriber key to the anchor key is specified in sub-clause 6.1.3 of the present document for each (class) of authentication methods. The key derivation rules are specified in Annex A.

NOTE: No parameter like 'access network type' is used for anchor key binding as 5G core procedures are supposed to be access network agnostic.

6.1.1.4 Construction of the serving network name

6.1.1.4.1 Serving network name

The serving network name is used in the derivation of the anchor key. It serves a dual purpose, namely:

- It binds the anchor key to the serving network by including the SN Id.
- It makes sure that the anchor key is specific for authentication between a 5G core network and a UE by including a service code set to "5G".

In 5G AKA, the serving network name has a similar purpose of binding the RES* and XRES* to the serving network.

The serving network name is the concatenation of a service code and the SN Id such that the service code prepends the SN Id with a separation character ":".

NOTE: No parameter like 'access network type' is used for serving network name as it relates to a 5G core procedure that is access network agnostic.

6.1.1.4.2 Construction of the serving network name by the UE

The UE shall construct the serving network name as follows:

1. It shall set the service code to "5G".
2. It shall set the network identifier to the SN Id of the network that it is authenticating to.
3. Concatenate the service code and the SN Id with the separation character ":".

6.1.1.4.3 Construction of the serving network name by the SEAF

The SEAF shall construct the serving network name as follows:

1. It shall set the service code to "5G".
2. It shall set the network identifier to the SN Id of the serving network to which the authentication data is sent by the AUSF.
3. Concatenate service code and the SN Id with the separation character ":".

NOTE: AUSF gets the serving network name from the SEAF. Before using the serving network name, AUSF checks that the SEAF is authorized to use it, as specified in clause 6.1.2.

6.1.2 Initiation of authentication and selection of authentication method

The initiation of the primary authentication is shown in Figure 6.1.2-1.

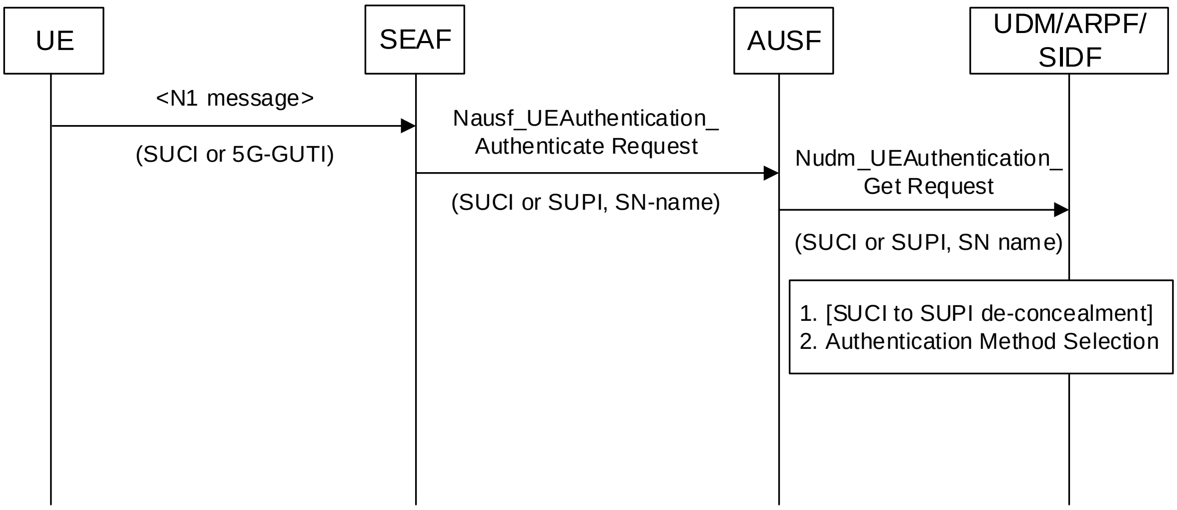
UE
SEAF
AUSF
UDM/ARPF/ SIDF
<N1 message>
(SUCI or 5G-GUTI)
Nausf_UEAuthentication_ Authenticate Request
(SUCI or SUPI, SN-name)
Nudm_UEAuthentication_ Get Request
(SUCI or SUPI, SN name)
1. [SUCI to SUPI de-concealment]
2. Authentication Method Selection

Figure 6.1.2-1: Initiation of authentication procedure and selection of authentication method

The SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

The SEAF shall invoke the Nausf_UEAuthentication service by sending a Nausf_UEAuthentication_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

The Nausf_UEAuthentication_Authenticate Request message shall contain either:

- SUCI, as defined in the current specification, or
- SUPI, as defined in TS 23.501 [2].

The SEAF shall include the SUPI in the Nausf_UEAuthentication_Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI is included in Nausf_UEAuthentication_Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.

The Nausf_UEAuthentication_Authenticate Request shall furthermore contain:

- the serving network name, as defined in sub-clause 6.1.1.4 of the present document.

NOTE 2: The local policy for the selection of the authentication method does not need to be on a per-UE basis, but can be the same for all UEs.

Upon receiving the Nausf_UEAuthentication_Authenticate Request message, the AUSF shall check that the requesting SEAF in the serving network is entitled to use the serving network name in the Nausf_UEAuthentication_Authenticate Request by comparing the serving network name with the expected serving network name. The AUSF shall store the received serving network name temporarily. If the serving network is not authorized to use the serving network name, the AUSF shall respond with "serving network not authorized" in the Nausf_UEAuthentication_Authenticate Response.

The Nudm_UEAuthentication_Get Request sent from AUSF to UDM includes the following information:

- SUCI or SUPI;
- the serving network name;

Upon reception of the Nudm_UEAuthentication_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request.

Based on SUPI, the UDM/ARPF shall choose the authentication method, based on the subscription data.

NOTE 3: The Nudm_UEAuthentication_Get Response in reply to the Nudm_UEAuthentication_Get Request and the Nausf_UEAuthentication_Authenticate Response message in reply to the Nausf_UEAuthentication_Authenticate Request message are described as part of the authentication procedures in clause 6.1.3.

6.1.3 Authentication procedures

6.1.3.1 Authentication procedure for EAP-AKA'

EAP-AKA' is specified in RFC 5448 [12]. The 3GPP 5G profile for EAP-AKA' is specified in the normative Annex F.

The selection of using EAP-AKA' is described in sub-clause 6.1.2 of the present document.

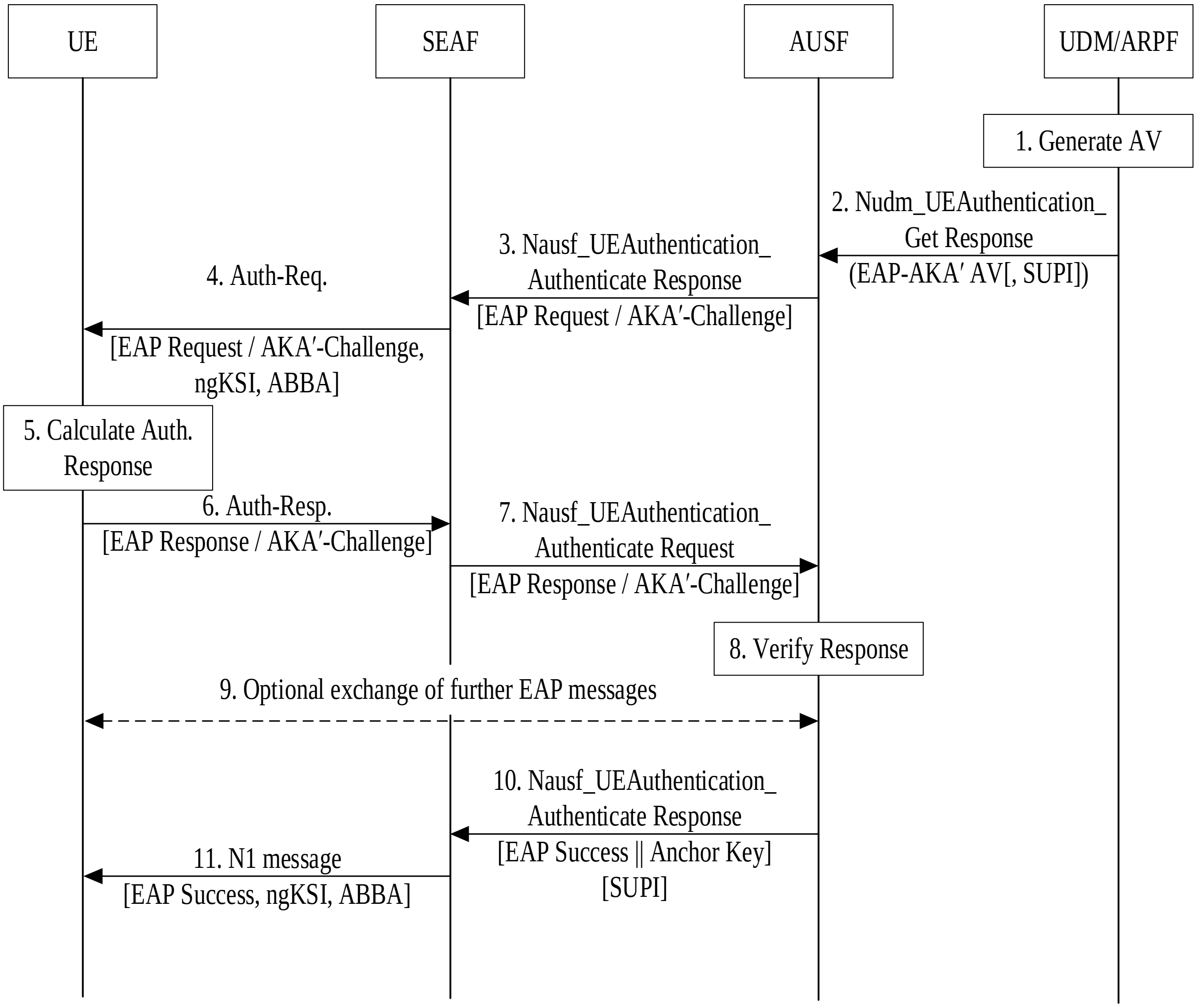
UE
SEAF
AUSF
UDM/ARPF
1. Generate AV
2. Nudm_UEAuthentication_ Get Response
(EAP-AKA′ AV[, SUPI])
3. Nausf_UEAuthentication_ Authenticate Response
[EAP Request / AKA′-Challenge]
4. Auth-Req.
[EAP Request / AKA′-Challenge, ngKSI, ABBA]
5. Calculate Auth. Response
6. Auth-Resp.
[EAP Response / AKA′-Challenge]
7. Nausf_UEAuthentication_ Authenticate Request
[EAP Response / AKA′-Challenge]
8. Verify Response
9. Optional exchange of further EAP messages
10. Nausf_UEAuthentication_ Authenticate Response
[EAP Success || Anchor Key]
[SUPI]
11. N1 message
[EAP Success, ngKSI, ABBA]

Figure 6.1.3.1-1: Authentication procedure for EAP-AKA'

The authentication procedure for EAP-AKA' works as follows, cf. also Figure 6.1.3.1-1:

1. The UDM/ARPF shall first generate an authentication vector with Authentication Management Field (AMF) separation bit = 1 as defined in TS 33.102 [9]. The UDM/ARPF shall then compute CK' and IK' as per the normative Annex A and replace CK and IK by CK' and IK'.

2. The UDM shall subsequently send this transformed authentication vector AV' (RAND, AUTN, XRES, CK', IK') to the AUSF from which it received the Nudm_UEAuthentication_Get Request together with an indication that the AV' is to be used for EAP-AKA' using a Nudm_UEAuthentication_Get Response message.

NOTE: The exchange of a Nudm_UEAuthentication_Get Request message and an Nudm_UEAuthentication_Get Response message between the AUSF and the UDM/ARPF described in the preceding paragraph is the same as for trusted access using EAP-AKA' described in TS 33.402 [11], sub-clause 6.2, step 10, except for the input parameter to the key derivation, which is the value of <network name>. The "network name" is a concept from RFC 5448 [12]; it is carried in the AT_KDF_INPUT attribute in EAP-AKA'. The value of <network name> parameter is not defined in RFC 5448 [12], but rather in 3GPP specifications. For EPS, it is defined as " access network identity " in TS 24.302 [13], and for 5G, it is defined as "serving network name" in sub-clause 6.1.1.4 of the present document.

In case SUCI was included in the Nudm_UEAuthentication_Get Request, UDM will include the SUPI in the Nudm_UEAuthentication_Get Response.

The AUSF and the UE shall then proceed as described in RFC 5448 [12] until the AUSF is ready to send the EAP-Success.

3. The AUSF shall send the EAP-Request/AKA'-Challenge message to the SEAF in a Nausf_UEAuthentication_Authenticate Response message. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1.

4. The SEAF shall transparently forward the EAP-Request/AKA'-Challenge message to the UE in a NAS message Authentication Request message. The ME shall forward the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM. This message shall include the ngKSI and ABBA parameter. In fact, SEAF shall include the ngKSI and ABBA parameter in all EAP-Authentication request message. ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful.

NOTE 1: The SEAF needs to understand that the authentication method used is an EAP method by evaluating the type of authentication method based on the Nausf_UEAuthentication_Authenticate Response message.

5. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [4]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [4], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME shall derive CK' and IK' according to Annex A.3.

   If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3. 3.

6. The UE shall send the EAP-Response/AKA'-Challenge message to the SEAF in a NAS message Auth-Resp message.

7. The SEAF shall transparently forwards the EAP-Response/AKA'-Challenge message to the AUSF in Nausf_UEAuthentication_Authenticate Request message.

8. The AUSF shall verify the message, and if the AUSF has successfully verified this message it shall continue as follows, otherwise it shall return an error.

9. The AUSF and the UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the SEAF. The SEAF shall transparently forward these messages.

NOTE 2: EAP Notifications as described in RFC 3748 [27] and EAP-AKA Notifications as described in RFC 4187 [21] can be used at any time in the EAP-AKA exchange. These notifications can be used e.g. for protected result indications or when the EAP server detects an error in the received EAP-AKA response.

10. The AUSF derives EMSK from CK’ and IK’ as described in RFC 5448[12] and Annex F. The AUSF uses the first 256 bits of EMSK as the K_{AUSF} and then calculates K_{SEAF} from K_{AUSF} as described in clause A.6. The AUSF shall send an EAP Success message to the SEAF inside Nausf_UEAuthentication_Authenticate Response, which shall forward it transparently to the UE. Nausf_UEAuthentication_Authenticate Response message contains the K_{SEAF}. If the AUSF received a SUCI from the SEAF when the authentication was initiated (see sub-clause 6.1.2

of the present document), then the AUSF shall also include the SUPI in the Nausf_UEAuthentication_Authenticate Response message.

NOTE 3: For lawful interception, the AUSF sending SUPI to SEAF is necessary but not sufficient. By including the SUPI as input parameter to the key derivation of K_{AMF} from K_{SEAF}, additional assurance on the correctness of SUPI is achieved by the serving network from both, home network and UE side. See also step 11.

11. The SEAF shall send the EAP Success message to the UE in the N1 message. This message shall also include the ngKSI and the ABBA parameter. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1.

NOTE 4: Step 11 could be NAS Security Mode Command.

NOTE 5: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

The key received in the Nausf_UEAuthentication_Authenticate Response message shall become the anchor key, K_{SEAF} in the sense of the key hierarchy in sub-clause 6.2 of the present document. The SEAF shall then derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7 and send it to the AMF. On receiving the EAP-Success message, the UE derives EMSK from CK' and IK' as described in RFC 5448 and Annex F. The ME uses the first 256 bits of the EMSK as the K_{AUSF} and then calculates K_{SEAF} in the same way as the AUSF. The UE shall derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7.

The further steps taken by the AUSF upon receiving a successfully verified EAP-Response/AKA'-Challenge message are described in sub-clause 6.1.4 of the present document.

If the EAP-Response/AKA'-Challenge message is not successfully verified, the subsequent AUSF behaviour is determined according to the home network's policy.

If the AUSF and SEAF determines that the authentication was successful, then the SEAF provides the ngKSI and the K_{AMF} to the AMF.

6.1.3.2 Authentication procedure for 5G AKA

6.1.3.2.0 5G AKA

5G AKA enhances EPS AKA [10] by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message.

The selection of using 5G AKA is described in sub-clause 6.1.2 of the present document.

NOTE 1: 5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.

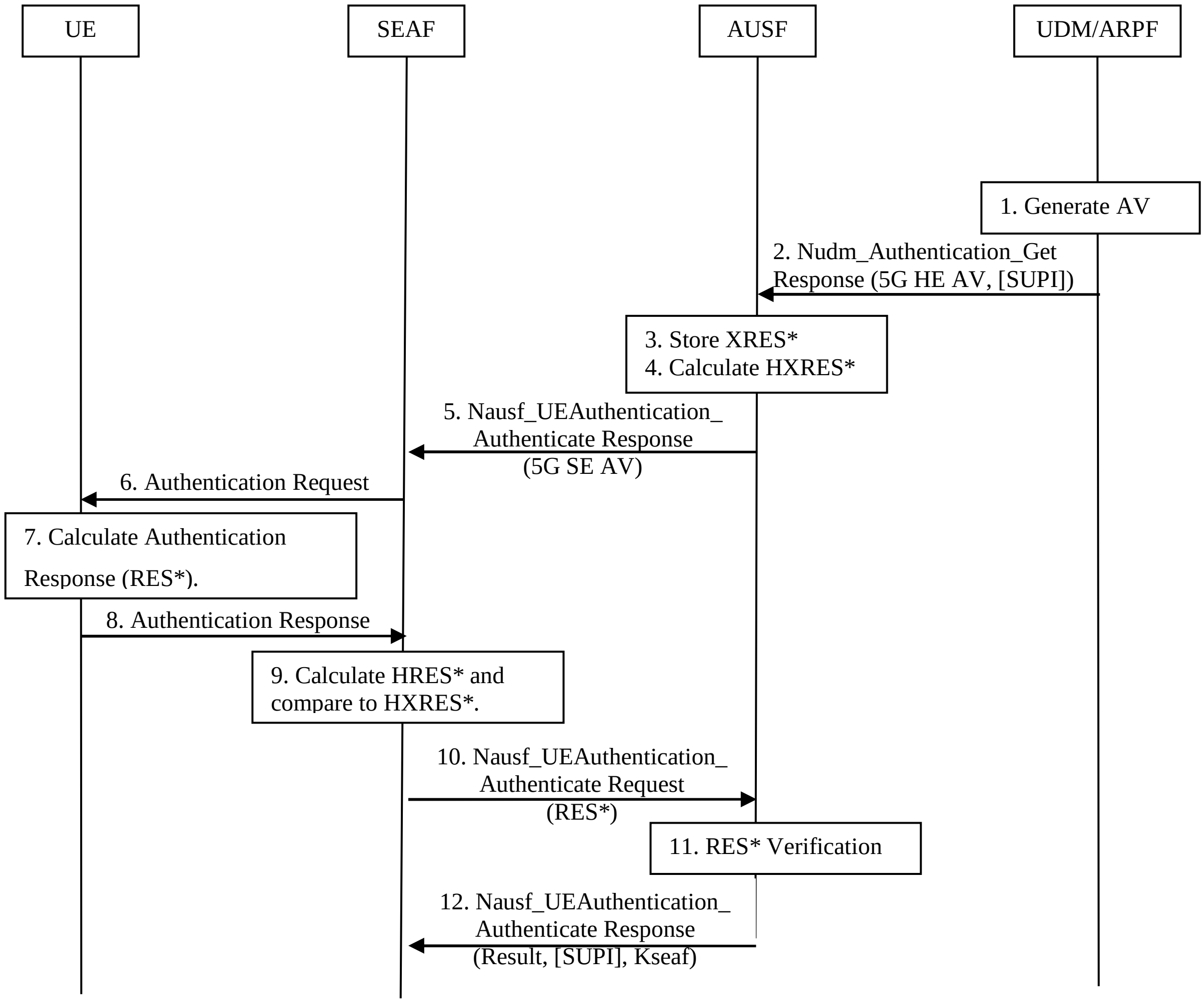
UE
SEAF
AUSF
UDM/ARPF
1. Generate AV
2. Nudm_Authentication_Get Response (5G HE AV, [SUPI])
3. Store XRES*
4. Calculate HXRES*
5. Nausf_UEAuthentication_ Authenticate Response (5G SE AV)
6. Authentication Request
7. Calculate Authentication Response (RES*).
8. Authentication Response
9. Calculate HRES* and compare to HXRES*.
10. Nausf_UEAuthentication_ Authenticate Request (RES*)
11. RES* Verification
12. Nausf_UEAuthentication_ Authenticate Response (Result, [SUPI], Kseaf)

Figure 6.1.3.2-1: Authentication procedure for 5G AKA

The authentication procedure for 5G AKA works as follows, cf. also Figure 6.1.3.2-1:

1. For each Nudm_Authenticate_Get Request, the UDM/ARPF shall create a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1"as defined in TS 33.102 [9] . The UDM/ARPF shall then derive K_{AUSF} as per Annex A.2, and calculate XRES* as per Annex A.4. Finally, the UDM/ARPF shall create a 5G HE AV from RAND, AUTN, XRES*, and K_{AUSF}.

2. The UDM shall then return the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G-AKA in a Nudm_UEAuthentication_Get Response. In case SUCI was included in the Nudm_UEAuthentication_Get Request, UDM will include the SUPI in the Nudm_UEAuthentication_Get Response.

3. The AUSF shall store the XRES* temporarily together with the received SUCI or SUPI. The AUSF may store the K_{AUSF}.

4. The AUSF shall then generate the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES* from XRES* according to Normative Annex A.5 and K_{SEAF} from K_{AUSF} according to Annex A.6, and replacing the XRES* with the HXRES* and K_{AUSF} with K_{SEAF} in the 5G HE AV.

5. The AUSF shall then remove the K_{SEAF} return the 5G SE AV (RAND, AUTN, HXRES*) to the SEAF in a Nausf_UEAuthentication_Authenticate Response.

6. The SEAF shall send RAND, AUTN to the UE in a NAS message Authentication -Request. This message shall also include the ngKSI that will be used by the UE and AMF to identify the K_{AMF} and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1. The ME shall forward the RAND and AUTN received in NAS message Authentication Request to the USIM.

NOTE 2: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the 5G AV by checking whether AUTN can be accepted as described in TS 33.102[4]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [4], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME then shall compute RES* from RES according to Annex A.4. The ME shall calculate K_{AUSF} from CK||IK according to clause A.2. The ME shall calculate K_{SEAF} from K_{AUSF} according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN.

NOTE: This separation bit in the AMF field of AUTN can not be used anymore for operator specific purposes as described by TS 33.102 [9], Annex F.

8. The UE shall return RES* to the SEAF in a NAS message Authentication Response.

9. The SEAF shall then compute HRES* from RES* according to Annex A.5, and the SEAF shall compare HRES* and HXRES*. If they coincide, the SEAF shall consider the authentication successful from the serving network point of view. If not, the SEAF proceed as described in sub-clause 6.1.3.2.1. If the UE is not reached, and the RES* is never received by the SEAF, the SEAF shall consider authentication as failed, and indicate a failure to the AUSF.

10. The SEAF shall send RES* together with the corresponding SUCI or SUPI, as received from the UE, in a Nausf_UEAuthentication_Authenticate Request message to the AUSF.

11. When the AUSF receives the Nausf_UEAuthentication_Authenticate Request message including a RES* it may verify whether the AV has expired. If the AV has expired the AUSF may consider the authentication as unsuccessful from the home network point of view. AUSF shall compare the received RES* with the stored XRES*. If the RES* and XRES* are equal, the AUSF shall consider the authentication as successful from the home network point of view. .

12. The AUSF shall indicate to the SEAF in the Nausf_UEAuthentication_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the K_{SAEF} shall be sent to the SEAF in the Nausf_UEAuthentication_Authenticate Response. In case the AUSF received a SUCI from the SEAF when the authentication was initiated (see sub-clause 6.1.2 of the present document), and if the authentication was successful, then the AUSF shall also include the SUPI in Nausf_UEAuthentication_ Authenticate Response .

If the authentication was successful, the key K_{SEAF} received in the Nausf_UEAuthentication_Authenticate Response message shall become the anchor key in the sense of the key hierarchy in sub-clause 6.2 of the present document. Then the SEAF shall derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7, and shall provide the ngKSI and the K_{AMF} to the AMF.

If a SUCI was used for this authentication, then the SEAF shall only provide ngKSI and K_{AMF} to the AMF after it receives the Nausf_UEAuthentication_ Authenticate Response message containing SUPI; no communication services will be provided to the UE until the SUPI is known to the serving network.

The further steps taken by the AUSF after the authentication procedure are described in sub-clause 6.1.4 of the present document.

6.1.3.2.1 Void

6.1.3.2.2 RES* verification failure in SEAF or AUSF or both

This clause describes how RES* verification failure in the SEAF or in the AUSF shall be handled.

In step 9 in Figure 6.1.3.2-1, the SEAF shall compute HRES* from RES* according to Annex A.5, and the SEAF shall compare HRES* and HXRES*. If they don't coincide, then the SEAF shall consider the authentication as unsuccessful.

The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf_UEAuthentication_Authenticate Response message from the AUSF in step 12in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf_UEAuthentication_Authenticate Response message to the SEAF that the verification of the RES* was not successful in the AUSF, or

- if the verification of the RES* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated.

Also, if the SEAF does not receive any Nausf_UEAuthentication_Authenticate Request message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE.

6.1.3.3 Synchronization failure or MAC failure

6.1.3.3.1 Synchronization failure or MAC failure in USIM

This clause describes synchronisation failure or MAC failure in USIM.

In step 7 in Figure 6.1.3.2-1 when 5G AKA is used; or in step 5 in Figure 6.1.3.1-1 when EAP-AKA’ is used, at the receipt of the RAND and AUTN, if the verification of the AUTN fails, then the USIM indicates to the ME the reason for failure and in the case of a synchronisation failure passes the AUTS parameter (see TS 33.102 [9]) to the ME.

If 5G AKA is used: The ME shall respond with NAS message Authentication Failure with a CAUSE value indicating the reason for failure. In case of a synchronisation failure of AUTN (as described in TS 33.102 [9]), the UE also includes AUTS that was provided by the USIM. Upon receipt of an authentication failure message, the AMF/SEAF may initiate new authentication towards the UE. (see TS 24.501 [35]).

If EAP-AKA’ is used: The ME shall proceed as described in RFC 4187 [21] and RFC 5448 [12] for EAP-AKA’.

6.1.3.3.2 Synchronization failure recovery in Home Network

Upon receiving an authentication failure message *with synchronisation failure* (AUTS) from the UE, the SEAF sends an Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF and the AUSF sends an Nudm_UEAuthentication_Get Request message to the UDM/ARPF, together with the following parameters:

- *RAND* sent to the UE in the preceding Authentication Request, and

- *AUTS* received by the SEAF in the response from the UE to that request, as described in subsection 6.1.3.2.0 and 6.1.3.3.1.

An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE.

The SEAF does not send new authentication requests to the UE before having received the response to its Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" from the AUSF (or before it is timed out).

When the UDM/ARPF receives an Nudm_UEAuthentication_Get Request message with a "*synchronisation failure indication*" it acts as described in TS 33.102 [9], clause 6.3.5 where ARPF is mapped to HE/AuC. The UDM/ARPF sends an Nudm_UEAuthentication_Get Response message with a new authentication vector for either EAP-AKA’ or 5G-AKA depending on the authentication method applicable for the user to the AUSF. The AUSF runs a new authentication procedure with the UE according to clauses 6.1.3.1 or 6.1.3.2 depending on the authentication method applicable for the user.

6.1.4 Linking increased home control to subsequent procedures

6.1.4.1 Introduction

The 5G authentication and key agreement protocols provide increased home control. Compared to EPS AKA in EPS, this provides better security useful in preventing certain types of fraud as explained in more detail below.

This increased home control comes in the following forms in 5GS:

- In the case of EAP-AKA', the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the EAP-Response/AKA'-Challenge received by the AUSF has been successfully verified, cf. sub-clause 6.1.3.1 of the present document.

- In the case of 5G AKA, the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the Authentication Confirmation message received in Nausf_UEAuthentication_Authenticate Request by the AUSF has been successfully verified, cf. sub-clause 6.1.3.2 of the present document.

When 3GPP credentials are used in above cases, the result is reported to the UDM. Details are described in clause 6.1.4.1a.

The feature of increased home control is useful in preventing certain types of fraud, e.g. fraudulent Nudm_UECM_Registration Request for registering the subscriber's serving AMF in UDM that are not actually present in the visited network. But an authentication protocol by itself cannot provide protection against such fraud. The authentication result needs to be linked to subsequent procedures, e.g. the Nudm_UECM_Registration procedure from the AMF in some way to achieve the desired protection.

The actions taken by the home network to link authentication confirmation (or the lack thereof) to subsequent procedures are subject to operator policy and are not standardized.

But informative guidance is given in sub-clause 6.1.4.2 as to what measures an operator could usefully take. Such guidance may help avoiding a proliferation of different solutions.

6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF

The information sent from the AUSF to the UDM that a successful or unsuccessful authentication of a subscriber has occurred, shall be used to link authentication confirmation to subsequent procedures. The AUSF shall send the Nudm_UEAuthentication_ResultConfirmation service operation for this purpose as shown in figure6.1.4.1a-1.

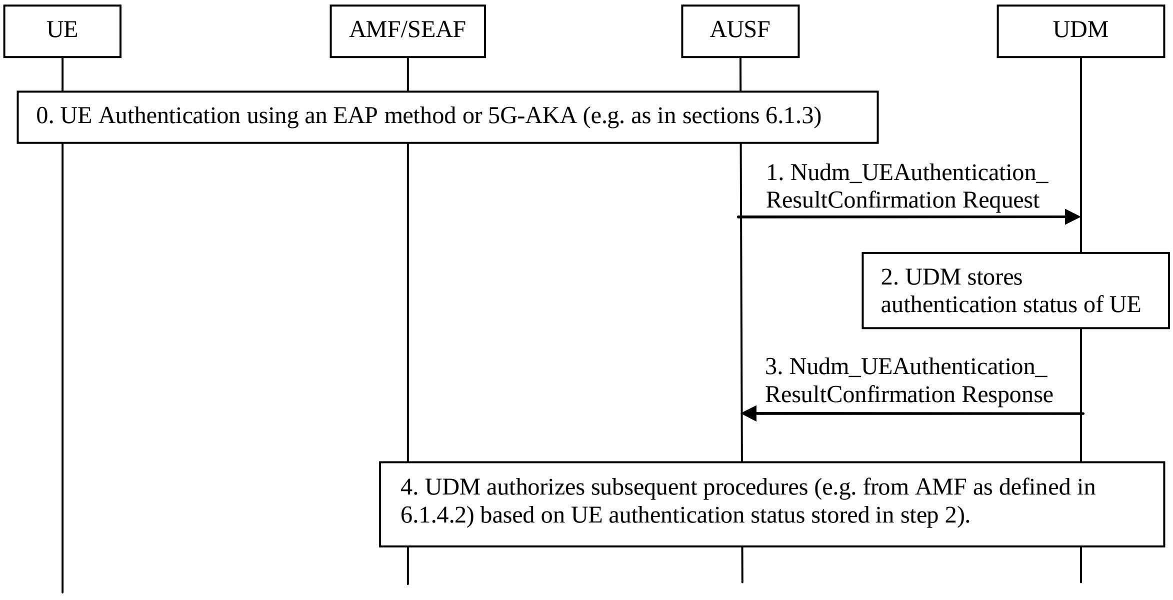
UE
AMF/SEAF
AUSF
UDM
0. UE Authentication using an EAP method or 5G-AKA (e.g. as in sections 6.1.3)
1. Nudm_UEAuthentication_ ResultConfirmation Request
2. UDM stores authentication status of UE
3. Nudm_UEAuthentication_ ResultConfirmation Response
4. UDM authorizes subsequent procedures (e.g. from AMF as defined in 6.1.4.2) based on UE authentication status stored in step 2).

Figure 6.1.4.1a-1: Linking increased Home control to subsequent procedures

1. The AUSF shall inform UDM about the result and time of an authentication procedure with a UE using a Nudm_UEAuthentication_ResultConfirmation Request. This may include the SUPI, a timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

NOTE: It may be sufficient for the purposes of fraud prevention to send only information about successful authentications, but this is up to operator policy.

2. The UDM shall store the authentication status of the UE (SUPI, authentication result, timestamp, and the serving network name).

3. UDM shall reply to AUSF with a Nudm_UEAuthentication_ResultConfirmation Response.

4. Upon reception of subsequent UE related procedures (e.g. Nudm_UECM_Registration_Request from AMF) UDM may apply actions according to home operator's policy to detect and achieve protection against certain types of fraud (e.g. as proposed in section 6.1.4.2).

6.1.4.2 Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF

This sub-clause gives informative guidance on how a home operator could link authentication confirmation (or the lack thereof) to subsequent Nudm_UECM_Registration procedures from AMF to achieve protection against certain types of fraud, as mentioned in the preceding sub-clause.

Approach 1:

The home network records the time of the most recent successfully verified authentication confirmation of the subscriber together with the identity of the 5G visited network that was involved in the authentication. When a new Nudm_UECM_Registration Request arrives from a visited network, the home network checks whether there is a sufficiently recent authentication of the subscriber by this visited network. If not, the Nudm_UECM_Registration Request is rejected. The rejection message may include, according to the home networks policy, an indication that the visited network should send a new Nausf_UEAuthentication_Authenticate Request (cf. sub-clause 6.1.2 of the present document) for fetching a new authentication vector before repeating the Nudm_UECM_Registration Request.

NOTE 1: With this approach, the authentication procedure and the Nudm_UECM_Registration procedure are performed independently. They are coupled only through linking information in the home network.

NOTE 2: It is up to the home network to set the time threshold to define what 'sufficiently recent' is.

Approach 2:

As a variant of the above Approach 1, Approach 2 is based on a more fine-grained policy applied by the home network; the home network could classify roaming partners into different categories, depending on the trust - e.g. derived from previous experience placed in them, for example as follows:

- For a visited network in the first category, the home network would require a successful authentication 'immediately preceding' the Nudm_UECM_Registration Request from an AMF.

- For a visited network in the second category, the home network would only check that an authentication in a network visited by the subscriber was sufficiently recent (taking into account that there may have been a security context transfer between the visited networks).

- For a visited network in the third category, the home network would perform no checks regarding Nudm_UECM_Registration Requests and authentication at all.

Further approaches are possible, depending on the home operator's policy.

6.2 Key hierarchy, key derivation, and distribution scheme

6.2.1 Key hierarchy

Requirements on 5GC and NG-RAN related to keys are described in clause 5.1.3. The following describes the keys of the key hierarchy generation in a 5GS in detail.:

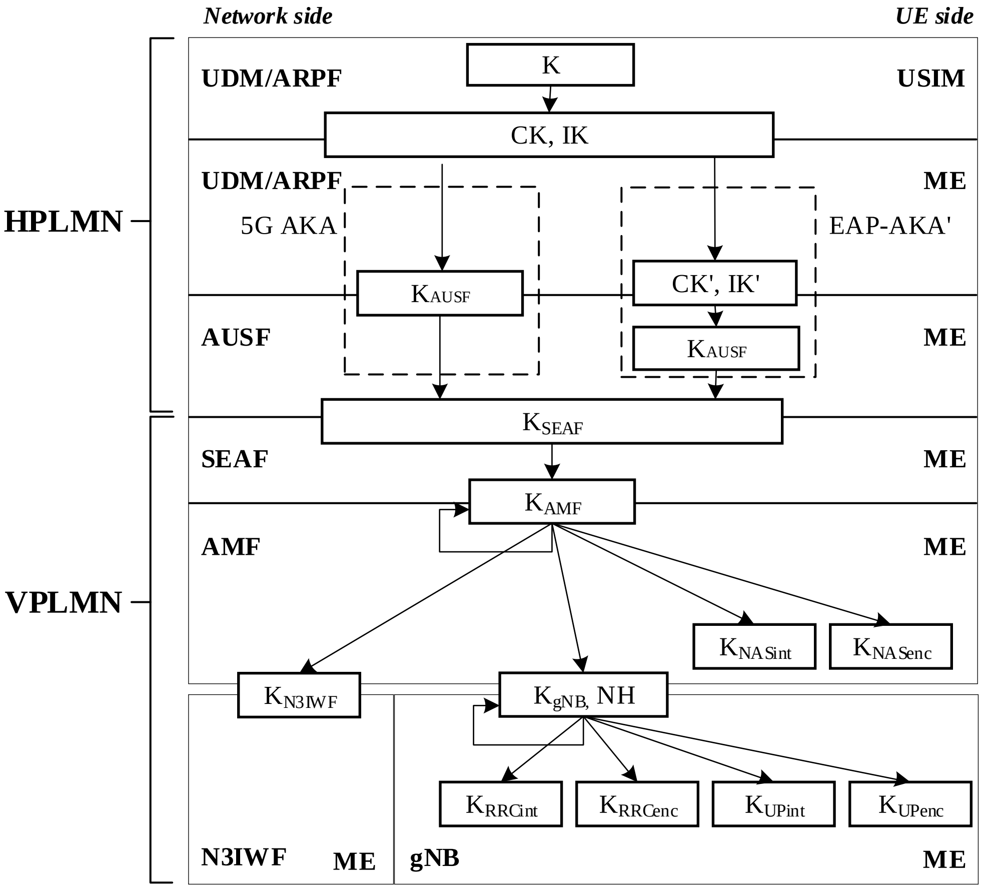

Figure 6.2.1-1: Key hierarchy generation in 5GS

The keys related to authentication (see Figure 6.2.1-1) include the following keys: K, CK/IK. In case of EAP-AKA', the keys CK', IK' are derived from CK, IK as specified in clause 6.1.3.1.

The key hierarchy (see Figure 6.2.1-1) includes the following keys: K_{AUSF}, K_{SEAF}, K_{AMF}, K_{NASint}, K_{NASenc}, K_{N3IWF}, K_{gNB}, K_{RRCint}, K_{RRCenc}, K_{UPint} and K_{UPenc}.

Keys for AUSF in home network:

- K_{AUSF} is a key derived
  - by ME and AUSF from CK', IK' in case of EAP-AKA', CK' and IK' is received by AUSF as a part of transformed AV from ARPF; or,
  - by ME and ARPF from CK, IK in case of 5G AKA, K_{AUSF} is received by AUSF as a part of the 5G HE AV from ARPF.
- K_{SEAF} is an anchor key derived by ME and AUSF from K_{AUSF}. K_{SEAF} is provided by AUSF to the SEAF in the serving network.

Key for AMF in serving network:

- K_{AMF} is a key derived by ME and SEAF from K_{SEAF}. K_{AMF} is further derived by ME and source AMF when performing horizontal key derivation.

Keys for NAS signalling:

- K_{NASint} is a key derived by ME and AMF from K_{AMF}, which shall only be used for the protection of NAS signalling with a particular integrity algorithm.

- K_{NASenc} is a key derived by ME and AMF from K_{AMF}, which shall only be used for the protection of NAS signalling with a particular encryption algorithm.

Key for NG-RAN:

- K_{gNB} is a key derived by ME and AMF from K_{AMF}. K_{gNB} is further derived by ME and source gNB when performing horizontal or vertical key derivation. The K_{gNB} is used as K_{eNB} between ME and ng-eNB.

Keys for UP traffic:

- K_{UPenc} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of UP traffic with a particular encryption algorithm.

- K_{UPint} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of UP traffic between ME and gNB with a particular integrity algorithm.

Keys for RRC signalling:

- K_{RRCint} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of RRC signalling with a particular integrity algorithm.

- K_{RRCenc} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of RRC signalling with a particular encryption algorithm.

Intermediate keys:

- NH is a key derived by ME and AMF to provide forward security as described in Clause A.10.

- K_{NG-RAN} * is a key derived by ME and NG-RAN (i.e., gNB or ng-eNB) when performing a horizontal or vertical key derivation as specified in Clause 6.9. 2.1.1 using a KDF as specified in Clause A.11/A.12.

- K'_{AMF} is a key that can be derived by ME and AMF when the UE moves from one AMF to another during inter-AMF mobility as specified in Clause 6.9.3 using a KDF as specified in Annex A.13.

Key for the non-3GPP access:

- K_{N3IWF} is a key derived by ME and AMF from K_{AMF} for the non-3GPP access. K_{N3IWF} is not forwarded between N3IWFs.

6.2.2 Key derivation and distribution scheme

6.2.2.1 Keys in network entities

Keys in the ARPF

The ARPF shall store the long-term key K. The key K shall be 128 bits or 256 bits long.

During an authentication and key agreement procedure, the ARPF shall derive CK' and IK' from K in case EAP-AKA' is used and derive K_{AUSF} from K in case 5G AKA is used. The ARPF shall forward the derived keys to the AUSF.

The ARPF holds the home network private key that is used by the SIDF to deconceal the SUCI and reconstruct the SUPI. The generation and storage of this key material is out of scope of the present document.

Keys in the AUSF

In case EAP-AKA' is used as authentication method, the AUSF shall derive a key K_{AUSF} from from CK'and IK' for EAP-AKA' as specified in clause 6.1.3.1. The K_{AUSF} may be stored in the AUSF between two subsequent authentication and key agreement procedures.

The AUSF shall generate the anchor key, also called K_{SEAF}, from the authentication key material received from the ARPF during an authentication and key agreement procedure.

Keys in the SEAF

The SEAF receives the anchor key, K_{SEAF}, from the AUSF upon a successful primary authentication procedure in each serving network.

The SEAF shall never transfer K_{SEAF} to an entity outside the SEAF. Once K_{AMF} is derived K_{SEAF} shall be deleted.

The SEAF shall generate K_{AMF} from K_{SEAF} immediately following the authentication and key agreement procedure and hands it to the AMF.

NOTE 1: This implies that a new K_{AMF}, along with a new K_{SEAF}, is generated for each run of the authentication and key agreement procedure.

NOTE 2: The SEAF is co-located with the AMF.

Keys in the AMF

The AMF receives K_{AMF} from the SEAF or from another AMF.

The AMF shall, based on policy, derive a key K'_{AMF} from K_{AMF} for transfer to another AMF in inter-AMF mobility. The receiving AMF shall use K'_{AMF} as its key K_{AMF}.

NOTE: The precise rules for key handling in inter-AMF mobility can be found in clause 6.9.3.

The AMF shall generate keys K_{NASint} and K_{NASenc} dedicated to protecting the NAS layer.

The AMF shall generate access network specific keys from K_{AMF}. In particular,

- the AMF shall generate K_{gNB} and transfer it to the gNB.
- the AMF shall generate NH and transfer it to the gNB, together with the corresponding NCC value.
  The AMF may also transfer an NH key, together with the corresponding NCC value, to another AMF, cf. clause 6.9.
- the AMF shall generate K_{N3IWF} and transfer it to the N3IWF when K_{AMF} is received from SEAF, or when K'_{AMF} is received from another AMF.

Keys in the NG-RAN

The NG-RAN (i.e., gNB or ng-eNB) receives K_{gNB} and NH from the AMF. The ng-eNB uses K_{gNB} as K_{eNB}.

The NG-RAN (i.e., gNB or ng-eNB) shall generate all further access stratum (AS) keys from K_{gNB} and /or NH.

Keys in the N3IWF

The N3IWF receives K_{N3IWF} from the AMF.

The N3IWF shall use K_{N3IWF} as the key MSK for IKEv2 between UE and N3IWF in the procedures for untrusted non-3GPP access, cf. clause 11.

Figure 6.2.2-1 shows the dependencies between the different keys, and how they are derived from the network nodes point of view.

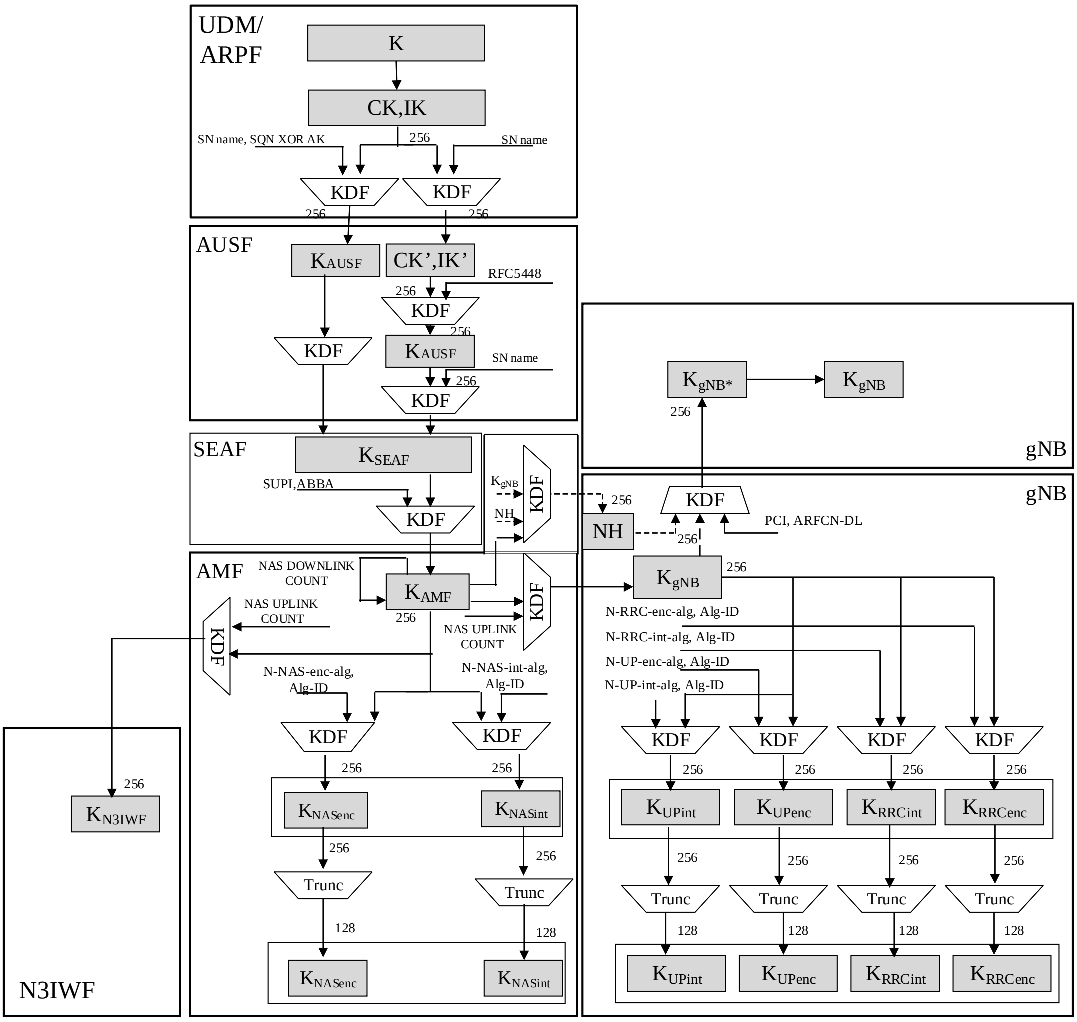

Figure 6.2.2-1: Key distribution and key derivation scheme for 5G for network nodes

6.2.2.2 Keys in the UE

For every key in a network entity, there is a corresponding key in the UE.

Figure 6.2.2-2 shows the corresponding relations and derivations as performed in the UE.

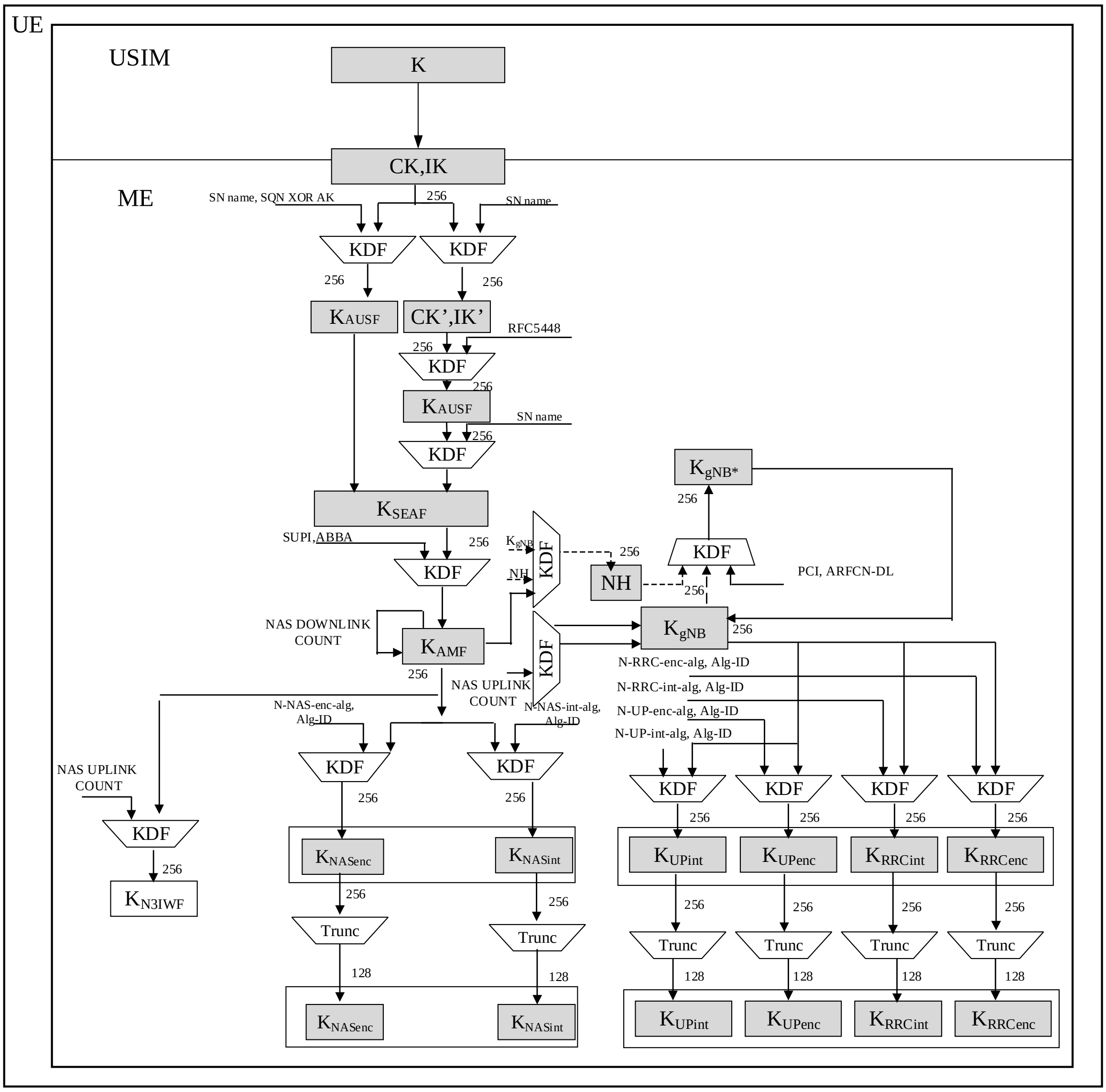

Figure 6.2.2-2: Key distribution and key derivation scheme for 5G for the UE

Keys in the USIM

The USIM shall store the same long-term key K that is stored in the ARPF.

During an authentication and key agreement procedure, the USIM shall generate key material from K that it forwards to the ME.

If provisioned by the home operator, the USIM shall store the home network public key used for concealing the SUPI.

Keys in the ME

The ME shall generate the K_{AUSF} from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in clause 6.1.3.

When 5G AKA is used, the generation of RES* from RES shall be performed by the ME.

Storage of the K_{AUSF} at the UE is optional. If the USIM supports 5G parameters storage, K_{AUSF} shall be stored in the USIM. Otherwise, K_{AUSF} shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of K_{SEAF} from the K_{AUSF}. If the USIM supports 5G parameters storage, KSEAF shall be stored in the USIM. Otherwise, KSEAF shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of K_{AMF}. If the USIM supports 5G parameters storage, K_{AMF} shall be stored in the USIM. Otherwise, KAMF shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of all other subsequent keys that are derived from the K_{AMF}.

Any 5G security context, K_{AUSF} and K_{SEAF} that are stored at the ME shall be deleted from the ME if:

a) the USIM is removed from the ME when the ME is in power on state;

b) the ME is powered up and the ME discovers that the USIM is different from the one which was used to create the 5G security context;

c) the ME is powered up and the ME discovers that there is no USIM is present at the ME.

6.2.3 Handling of user-related keys

6.2.3.1 Key setting

Key setting happens at the end of successful authentication procedure. Authentication and key setting may be initiated by the network as often as the network operator wishes when an active NAS connection exists. Key setting can occur as soon as the identity of the mobile subscriber (i.e. 5G-GUTI or SUPI) is known by the AMF. A successful run of 5G AKA or EAP AKA' results in a new K_{AMF} that is stored in the UE and the AMF with a new partial, non-current security context.

NAS keys (i.e. K_{NASint} and K_{NASenc}) and AS keys (i.e. K_{gNB}, K_{RRCenc}, K_{RRCint}, K_{UPenc}, K_{UPint}) are derived from K_{AMF} using the KDFs specified in Annex A. The NAS keys derived from the new K_{AMF} are taken in use in the AMF and the UE by means of the NAS security mode command procedure (see sub-clause 6.7.2). The AS keys are taken into use with the AS security mode command procedure (see sub-clause 6.7.4) or with the key change on the fly procedure (see sub-clause 6.9.6).

For the non-3GPP access, the key K_{N3IWF} is derived from the K_{AMF}. K_{N3IWF} is stored in the UE and the N3IWF as specified in subclause 7.2.1. This key K_{N3IWF} and the IPsec SA cryptographic keys are taken into use with the establishment of IPsec Security Association (SA) between the UE and the N3IWF.

NOTE: For mapped security contexts, the K_{AMF} is derived from EPS keys during interworking with EPS (see clause 8).

6.2.3.2 Key identification

The key K_{AMF} shall be identified by the key set identifier ngKSI. ngKSI may be either of type native or of type mapped. An ngKSI shall be stored in the UE and the AMF together with K_{AMF} and the temporary identifier 5G-GUTI, if available.

NOTE 1: The 5G-GUTI points to the AMF where the K_{AMF} is stored.

A native ngKSI is associated with the K_{SEAF} and K_{AMF} derived during primary authentication. It is allocated by the SEAF and sent with the authentication request message to the UE where it is stored together with the K_{AMF}. The purpose of the ngKSI is to make it possible for the UE and the AMF to identify a native security context without invoking the authentication procedure. This is used to allow re-use of the native security context during subsequent connection set-ups.

A mapped ngKSI is associated with the K_{AMF} derived from EPS keys during interworking, cf. clause 8 of the present document. It is generated in both the UE and the AMF respectively when deriving the mapped K_{AMF} when moving from EPS to 5GS. The mapped ngKSI is stored together with the mapped K_{AMF}.

The purpose of the mapped ngKSI is to make it possible for the UE and the AMF to indicate the use of the mapped K_{AMF} in interworking procedures (for details cf. clause 8).

The format of ngKSI shall allow a recipient of such a parameter to distinguish whether the parameter is of type native or of type mapped. The format shall contain a type field and a value field. The type field indicates the type of the key set. The value field consists of three bits where seven values, excluding the value '111', are used to identify the key set. The value '111' is reserved to be used by the UE to indicate that a valid K_{AMF} is not available for use. The format of ngKSI is described in [35]

K_{NASenc} and K_{NASint} in the key hierarchy specified in clause 6.2.1, which are derived from K_{AMF}, can be uniquely identified by ngKSI together with those parameters from the set {algorithm distinguisher, algorithm identifier}, which are used to derive these keys from K_{AMF}.

The K_{N3IWF} can be uniquely determined by ngKSI together with the uplink NAS COUNT are used to derive it according to clause A.9.

The initial K_{gNB} can be uniquely determined by ngKSI, together with the uplink NAS COUNT are used to derive it according to clause A.9.

The intermediate key NH as defined in clause 6.9.2.1.1 can be uniquely determined by ngKSI, together with the initial K_{gNB} derived from the current 5G NAS security context for use during the ongoing CM-CONNECTED state and a counter counting how many NH-derivations have already been performed from this initial K_{gNB} according to clause A.10. The next hop chaining count, NCC, represents the 3 least significant bits of this counter.

Intermediate key K_{NG-RAN}*, as well as non-initial K_{gNB}, defined in clause 6.9.2.1.1 can be uniquely identified by ngKSI together with those parameters from the set {K_{gNB} or NH, sequence of PCIs and ARFCN-DLs}, which are used to derive these keys from K_{gNB} or NH.

K_{RRCint}, K_{RRCenc}, K_{UPint}, and K_{UPenc} in the key hierarchy specified in clause 6.2.1 can be uniquely identified by ngKSI together with those parameters from the set {algorithm distinguisher, algorithm identifier}, which are used to derive these keys from K_{gNB}.

NOTE 2: In addition to 5G security contexts, the UE may also cache EPS security contexts. These EPS security contexts are identified by the eKSI, as defined in TS 33.401 [10].

6.2.3.3 Key lifetimes

K_{AUSF}, and K_{SEAF} shall be created when running a successful primary authentication as described in clause 6.1.3.

K_{AMF} shall be created in the following cases:

1. Primary authentication
2. NAS key re-keying as described in clause 6.9.4.2
3. NAS key refresh as described in clause 6.9.4.3
4. Interworking procedures with EPS (cf. clauses 8 and 10)

In case the UE does not have a valid K_{AMF}, an ngKSI with value "111" shall be sent by the UE to the network, which can initiate (re)authentication procedure to get a new K_{AMF} based on a successful primary authentication.

K_{NASint} and K_{NASenc} are derived based on a K_{AMF} when running a successful NAS SMC procedure as described in clause 6.7.2.

K_{N3IWF} is derived from K_{AMF} and remains valid as long as the UE is connected to the 5GC over non- 3gpp access or until the UE is reauthenticated.

K_{gNB} and NH are derived based on K_{AMF} or K_{gNB} or NH in the following cases:

1. Inter-gNB-CU-handover as described in clause 6.9.2.3.1
2. State transitions as described in clause 6.8
3. AS key re-keying as described in clause 6.9.4.4
4. AS key refresh as described in clause 6.9.4.5

The K_{RRCint}, K_{RRCenc}, K_{UPint} and K_{UPenc} are derived based on K_{gNB} after a new K_{gNB} is derived.

6.3 Security contexts

6.3.1 Distribution of security contexts

6.3.1.1 General

The present clause focuses on the security contexts themselves; the handling of security contexts in mobility procedures is described in clause 6.9.

6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain

The transmission of the following subscriber identities and security data is permitted between 5G core network entities of the same serving network domain:

- SUPI in the clear
- 5G security contexts, as described in clause 6.9

A 5G authentication vector shall not be transmitted between SEAFs.

Once the subscriber identities and security data have been transmitted from an old to a new network entity the old network entity shall delete the data.

6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains

The transmission of the following subscriber identities and security data is permitted between 5G core network entities of different serving network domains:

- SUPI in the clear
- 5G security contexts, as described in clause 6.9, if the security policy of the transmitting 5G serving network domain allows this.

A 5G authentication vector or non-current 5G security contexts shall not be transmitted to a different 5G serving network domain.

6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains

NOTE 1: No direct interworking between 5G networks and network of generations prior to EPS are foreseen. Therefore, only the interaction between 5G and EPS serving network domains is addressed here.

The transmission of the SUPI in the clear is permitted between 5G and EPS core network entities if it has the form of an IMSI.

The transmission of any unmodified 5G security contexts to a EPS core network entity is not permitted. Details of security context transfer between EPS and 5G core network entities can be found in clause 8.

The transmission of a 5G authentication vector to an EPS core network entity is not permitted. The transmission of any unused EPS authentication vectors to a 5G core network entity is not permitted. If SEAF receives any unused authentication vectors (e.g. in mobility scenarios from legacy MME) they shall be dropped without any processing.

NOTE 2: The rules above differ from the corresponding rules in 3GPP TS 33.401, clause 6.1.6: The latter allows forwarding of UMTS authentication vectors from an SGSN to an MME and back to the same SGSN under certain conditions. But this feature goes against a strict security separation of EPS and 5G domains. As its performance advantage is questionable it was not copied into 5G.

NOTE 3: Security context mapping between EPS and 5G serving networks is allowed, according to clause 8.

6.3.2 Multiple registrations in same or different serving networks

6.3.2.0 General

There are two cases where the UE can be multiple registered in different PLMN's serving networks or in the same PLMN's serving networks. The first case is when the UE is registered in one PLMN serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN serving network over the other type of access (e.g. non-3GPP). The second case is where the UE is registered in the same AMF in the same PLMN serving network over both 3GPP and non-3GPP accesses. The UE will establish two NAS connections with the network in both cases.

NOTE: The UE uses the same subscription credential(s) for multiple registrations in the same or different serving networks.

6.3.2.1 Multiple registrations in different PLMNs

The UE shall independently maintain and use two different 5G security contexts, one per PLMN's serving network. . Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN.

The ME shall store the two different 5G security contexts on the USIM if the USIM supports the 5G parameters storage. If the USIM does not support the 5G parameters storage, then the ME shall store the two different 5G security contexts in the ME non-volatile memory. Both of the two different 5G security contexts are current 5G security context.

Editor's Note: It is FFS to define the event(s) that triggers the storage of the key in the ME or in the USIM. Also, the appropriate clause needs to be considered.

6.3.2.2 Multiple registrations in the same PLMN

When the UE is registered in the same AMF in the same PLMN serving network over both 3GPP and non-3GPP accesses, the UE shall establish two NAS connections with the network. Upon receiving the registration request message, the AMF should check whether the UE is authenticated by the network. The AMF may decide to skip a new authentication run in case there is an available 5G security context for this UE by means of 5G-GUTI, e.g. when the UE successfully registered to 3GPP access, if the UE registers to the same AMF via non-3GPP access, the AMF can decide not to run a new authentication if it has an available security context to use. In this case, the UE shall directly take into use the available common 5G NAS security context and use it to protect the registration over the non-3GPP access. The AMF and the UE shall establish a common NAS security context consisting of a single set of NAS keys and algorithm at the time of first registration over any access. The AMF and the UE shall also include parameters specific to each NAS connection in the common NAS security context. The connection specific parameters are specified in clause 6.4.2.2 of the present document.

6.4 NAS security mechanisms

6.4.1 General

This sub-clause describes the security mechanisms for the protection of NAS signalling and data between the UE and the AMF over the N1 reference point. This protection involves both integrity and confidentiality protection. The security parameters for NAS protection are part of the 5G security context described in sub-clause 6.3 of the present document.

6.4.2 Security for multiple NAS connections

6.4.2.1 Multiple active NAS connections with different PLMNs

TS 23.501 [2] has a scenario when the UE is registered to a VPLMN's serving network via 3GPP access and to another VPLMN's or HPLMN's serving network via non-3GPP access at the same time. When the UE is registered in one PLMN's serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN's serving network over another type of access (e.g. non-3GPP), then the UE has two active NAS connections with different AMF's in different PLMNs. As described in clause 6.3.2.1, the UE shall independently maintain and use two different 5G security contexts, one per PLMN serving network. Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN. All the NAS and AS security mechanisms defined for single registration mode are applicable independently on each access using the corresponding 5G security context.

NOTE: The UE belongs to a single HPLMN.

6.4.2.2 Multiple active NAS connections in the same PLMN's serving network

When the UE is registered in a serving network over two types of access (e.g. 3GPP and non-3GPP), then the UE has two active NAS connections with the same AMF. A common 5G NAS security context is created during the registration procedure over the first access type.

In order to realize cryptographic separation and replay protection, the common NAS security-context shall have parameters specific to each NAS connection. The connection specific parameters include a pair of NAS COUNTs for uplink and downlink and unique NAS connection identifier. The value of the unique NAS connection identifier shall be set to "0x01" for 3GPP access and set to "0x02" for non-3GPP access.

In mobility and interworking scenarios, a newly created partial NAS security context is activated only on the NAS connection reporting the mobility, NAS context is enabled one by one for multiple connections.

When the UE is simulanteously registered over both types of accesses, and if an authentication procedure followed by a NAS SMC run takes place over one of the accesses (say access A), then the new NAS security context shall only be activated over that access (access A). The UE and the AMF shall retain and continue to use the old NAS security context over the other access (say access B). In order to activate the new NAS security context over the other access (access B), the AMF shall trigger a NAS SMC run over that access. During the second NAS SMC run (on access B), the AMF shall include the same ngKSI associated with the new NAS security context. After a successful second NAS SMC procedure over the other access (access B), both the UE and the AMF shall delete the old NAS security context.

6.4.3 NAS integrity mechanisms

6.4.3.0 General

Integrity protection for NAS signalling messages shall be provided as part of the NAS protocol.

6.4.3.1 NAS input parameters to integrity algorithm

The input parameters to the NAS 128-bit integrity algorithms as described in Annex D shall be set as follows.

The KEY input shall be equal to the K_{NASint} key.

The BEARER input shall be equal to the NAS connection identifier.

The DIRECTION bit shall be set to 0 for uplink and 1 for downlink.

The COUNT input shall be constructed as follows:

COUNT := 0x00 || NAS COUNT

Where NAS COUNT is the 24-bit NAS UL COUNT or the 24-bit NAS DL COUNT value, depending on the direction, that is associated to the current NAS connection identified by the value used to form the BEARER input.

A NAS COUNT shall be constructed as follows:

NAS COUNT := NAS OVERFLOW || NAS SQN

Where

- NAS OVERFLOW is a 16-bit value which is incremented each time the NAS SQN is incremented from the maximum value.
- NAS SQN is the 8-bit sequence number carried within each NAS message.

The use and mode of operation of the 128-bit integrity algorithms are specified in Annex D.

6.4.3.2 NAS integrity activation

NAS integrity shall be activated using the NAS SMC procedure or after an inter-system handover from EPC.

Replay protection shall be activated when integrity protection is activated, except when the NULL integrity protection algorithm is selected. Replay protection shall ensure that the receiver only accepts each incoming NAS COUNT value once using the same NAS security context.

Once NAS integrity has been activated, NAS messages without integrity protection shall not be accepted by the UE or the AMF. Before NAS integrity has been activated, NAS messages without integrity protection shall only be accepted by the UE or the AMF in certain cases where it is not possible to apply integrity protection.

NAS integrity shall stay activated until the 5G security context is deleted in either the UE or the AMF. It shall not be possible to change from non-NULL integrity protection algorithm to NULL integrity protection.

6.4.3.3 NAS integrity failure handling

The supervision of failed NAS integrity checks shall be performed both in the ME and the AMF. In case of failed integrity check (i.e. faulty or missing NAS-MAC) is detected after the start of NAS integrity protection, the concerned message shall be discarded except for some NAS messages specified in TS 24.501 [35]. For those exceptions the AMF shall take the actions specified in TS 24.501 [35] when receiving a NAS message with faulty or missing NAS-MAC. Discarding NAS messages can happen on the AMF side or on the ME side.

6.4.4 NAS confidentiality mechanisms

6.4.4.0 General

Confidentiality protection for NAS signalling messages shall be provided as part of the NAS protocol.

6.4.4.1 NAS input parameters to confidentiality algorithm

The input parameters for the NAS 128-bit ciphering algorithms shall be the same as the ones used for NAS integrity protection as described in clause 6.4.3, with the exception that a different key, K_{NASenc}, is used as KEY, and there is an additional input parameter, namely the length of the key stream to be generated by the encryption algorithms.

The use and mode of operation of the 128-bit ciphering algorithms are specified in Annex D.

NOTE: In the context of the present subclause 6.4.4, a message is considered ciphered also when the NULL encryption algorithm NEA0 is applied.

6.4.4.2 NAS confidentiality activation

NAS confidentiality shall be activated using the NAS SMC procedure or after an inter-system handover from EPC.

Once NAS confidentiality has been activated, NAS messages without confidentiality protection shall not be accepted by the UE or the AMF. Before NAS confidentiality has been activated, NAS messages without confidentiality protection shall only be accepted by the UE or the AMF in certain cases where it is not possible to apply confidentiality protection.

NAS confidentiality shall stay activated until the 5G security context is deleted in either the UE or the AMF.

6.4.5 Handling of NAS COUNTs

The NAS security context created at the registration time of the first access type contains the NAS integrity and encryption keys, selected algorithm common for all NAS connections. In addition, each NAS connection shall have a unique NAS connection identifier, a distinct pair of NAS COUNTs, one NAS COUNT for uplink and one NAS COUNT for downlink, associated with it. In the NAS security context, the NAS connection identifier shall be the differentiator for the connection-specific parameters.

It is essential that the NAS COUNTs for a particular K_{AMF} are not reset to the start values (that is the NAS COUNTs only have their start value when a new K_{AMF} is generated). This prevents the security issue of using the same NAS COUNTs with the same NAS keys, e.g. key stream re-use, in the case a UE moves back and forth between two AMFs and the same NAS keys are re-derived.

In the AMF, all the distinct pairs of NAS COUNTs part of the same 5G NAS security context, shall only be set to the start value in the following cases:

- for a partial native 5GC NAS security context created by a successful primary authentication run on one of the NAS connections established between the same AMF and the UE, or,
- for a mapped 5G security context generated when a UE moves from an MME to the AMF during both idle and connected mode mobility, or,
- for a new K_{AMF} taken into use in a target AMF during mobility registration update or handover.

The start value of NAS COUNT shall be zero (0).

6.4.6 Protection of initial NAS message

The initial NAS message is the first NAS message that is sent after the UE transitions from the idle state. The UE shall send a limited set of IEs (called the cleartext IEs) including those needed to establish security and/or enable the selection of the AMF in the initial message when it has no NAS security context. In this case, the UE shall include the additional IEs in the NAS Security Mode Complete message to provide ciphering protection of these IEs. When the UE has a security context, the UE shall send the complete initial message integrity protected with the cleartext IEs unciphered. The cleartext IEs include those required to allow the AMF to verify the message, establish security and/or enable the selection of the AMF. The UE shall send all other IEs ciphered. The AMF uses a hash value to protect the integrity of the unciphered IEs (see 6.7.2 for more details) in case there was no security context in the UE or the check of the integrity protection at the AMF fails.

The protection of the initial NAS message proceeds as shown in Figure 6.4.6-1.

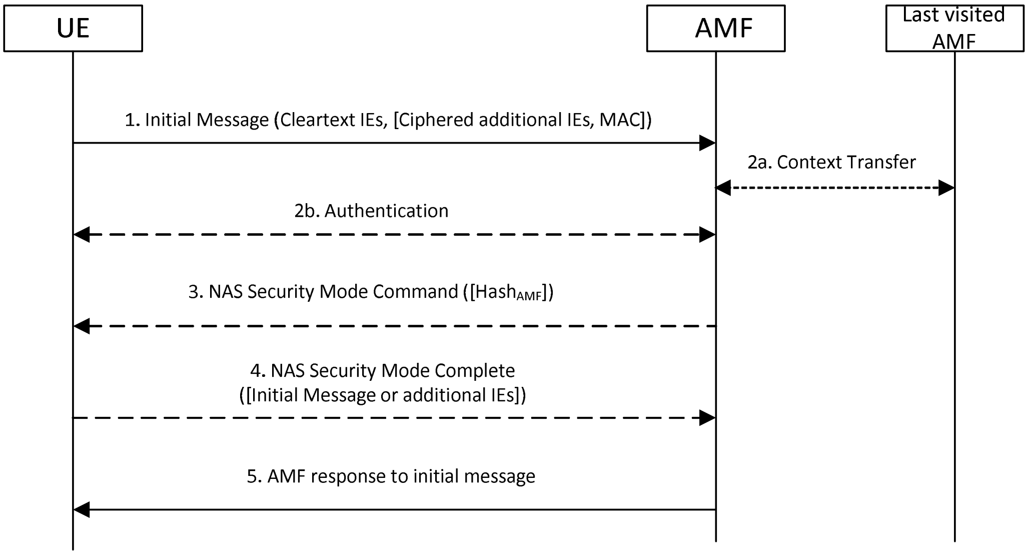
UE
AMF
Last visited AMF
1. Initial Message (Cleartext IEs, [Ciphered additional IEs, MAC])
2a. Context Transfer
2b. Authentication
3. NAS Security Mode Command ([Hash$_{AMF}$])
4. NAS Security Mode Complete ([Initial Message or additional IEs])
5. AMF response to initial message

Figure 6.4.6-1: Protecting the initial NAS message

Step 1: The UE shall send the Initial message to the AMF. If the UE has no NAS security context, the Initial NAS message shall only contain the cleartext IEs, i.e. subscription identifiers (e.g. SUCI or GUTIs), UE security capabilities, S-NSSAIs, ngKSI, the last visited TAIs, indication that the UE is moving from EPC and IE containing the TAU Request in the case idle mobility from 4G.

Editor's Note: The proposed cleartext IEs necessary to establish security and slected the AMF has to be verified in liaison with other Working Groups and is therefore FFS.

If the UE has a NAS security context, the initial message shall contain the complete message, where the information given above shall be sent in cleartext but the rest of the message is ciphered. With a NAS security context, the initial message shall also be integrity protected. In the case that the initial message was protected, the AMF has the same security context and successfully checks the integrity, then steps 2 to 4 may be omitted.

Step 2: If the AMF does not have the security context or if the integrity check fails, then the AMF shall initiate an authentication procedure with the UE.

Step 3: After a successful authentication of the UE, the AMF shall send the NAS Security Mode Command message. If the Initial message was sent without integrity protection or the integrity protection did not pass (due either to a MAC failure or the AMF not being able to find the used security context), the AMF shall include the hash of the Initial NAS message in the NAS Security Mode Complete message. If the AMF did not get the additional IEs from step 1, either due to them not being included or because the AMF could not decrypt the IE, then the AMF shall include the hash of the Initial NAS message in the NAS Security Mode Command message.

Step 4: The UE shall send the NAS Security Mode Complete message to the network in response to a NAS Security Mode Command message. The NAS Security Mode Complete message shall be ciphered and integrity protected. Furthermore the NAS Security Mode Complete message shall include the complete Initial NAS message if the check of the hash failed (see 6.7.2). In this case, the AMF shall treat this as the initial NAS message to respond to. Otherwise, the NAS Security Mode Complete message shall contain the additional IEs in the NAS Security Mode Command message if the checking of the hash succeeds. In this case, the AMF uses the cleartext IEs from step 1 and the additional IEs from this step as the initial NAS message to respond to.

Step 5: The AMF shall send its response to the Initial NAS message. This message shall be ciphered and integrity protected.

6.4.7 Security aspects of SMS over NAS

Specific services of SMS over NAS are defined in TS 23.501 [2], and procedures for SMS over NAS are specified in TS 23.502 [8].

For registration and de-registration procedures for SMS over NAS, the details are specified in subclause 4.13.3.1 and 4.13.3.2 in TS 23.502 [8]. The NAS message can be protected by NAS security mechanisms.

For MO/MT SMS over NAS via 3GPP/non-3GPP when the UE has already activated NAS security with the AMF before sending/receiving SMS, the NAS Transport message shall be ciphered and integrity protected using the NAS security context by the UE/AMF as described in sub-clause 6.4 in the present document.

6.5 RRC security mechanisms

6.5.1 RRC integrity mechanisms

RRC integrity protection shall be provided by the PDCP layer between UE and gNB and no layers below PDCP shall be integrity protected. Replay protection shall be activated when integrity protection is activated (except for when the selected integrity protection algorithm is NIA0, see Annex D). Replay protection shall ensure that the receiver accepts each particular incoming PDCP COUNT value only once using the same AS security context.

The use and mode of operation of the 128-NIA algorithms are specified in Annex D.

The input parameters to the 128-bit NIA algorithms as described in Annex D are the RRC message as MESSAGE, an 128-bit integrity key K_{RRCint} as KEY, a 5-bit bearer identity BEARER which value is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION and a bearer specific direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side. UE may trigger a recovery procedure as specified in TS 38.331 [22].

NOTE: Failed integrity check does not always imply that the concerned message is silently discarded.

6.5.2 RRC confidentiality mechanisms

RRC confidentiality protection is provided by the PDCP layer between UE and gNB.

The use and mode of operation of the 128-NEA algorithms are specified in Annex D.

The input parameters to the 128-bit NEA algorithms as described in Annex D are a 128-bit cipher Key K_{RRCenc} as KEY, a 5-bit bearer identity BEARER which corresponds to the radio bearer identity, the 1-bit direction of transmission DIRECTION, the length of the keystream required LENGTH and a bearer specific direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

6.6 UP security mechanisms

6.6.1 UP security policy

The SMF shall provide UP security policy for a PDU session to the gNB during the PDU session establishment procedure as specified in TS 23.502 [8].

The UP security policy shall indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all DRBs belonging to that PDU session. The UP security policy shall be used to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

The gNB shall activate UP confidentiality and/or UP integrity protection per each DRB, according to the received UP security policy, using RRC signalling as defined in clause 6.6.2. If the user plane security policy indicates "Required" or "Not needed", the gNB shall not overrule the UP security policy provided by the SMF. If the gNB cannot activate UP confidentiality and/or UP integrity protection when the received UP security policy is "Required", the gNB shall reject establishment of UP resources for the PDU Session and indicate reject-cause to the SMF.

NOTE 1: Local SMF can override the confidentiality option in the UP security policy received from the home SMF based on its local policy, roaming agreement and/or regulatory requirements.

At an Xn-handover from the source gNB to the target gNB, the source gNB shall include in the HANDOVER REQUEST message, the UE's UP security policy. If the UP security policy is ‘Required’, the target gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF. For the accepted PDU sessions, the target gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy and shall indicate that to the UE in the HANDOVER COMMAND by the source gNB.

If the UE receives an indication in the HANDOVER COMMAND that UP integrity protection and/or UP encryption for a PDU session is enabled at the target gNB, the UE shall generate or update the UP encryption key and/or UP integrity protection key and shall activate UP encryption and/or UP integrity protection for the respective PDU session.

NOTE 2: If the security policy is ‘Preferred’, it is possible to have a change in activation or deactivation of UP integrity after the handover.

Further, in the Path-Switch message, the target gNB shall send the UE's UP security policy and corresponding PDU session ID received from the source gNB to the SMF. The SMF shall verify that the UE's UP security policy received from the target gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target gNB. This UP security policy information, if included by the SMF, is delivered to the target gNB in the Path-Switch Acknowledge message. Additionally, the SMF may log the event and may take additional measures, such as raising an alarm.

If the target gNB receives UE's UP security policy from the SMF in the Path-Switch Acknowledge message, the target gNB shall update the UE's UP security policy with the received UE's UP security policy. If UE's current UP confidentiality and/or UP integrity protection activation is different from the received UE's UP security policy, then the target gNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure to reconfigure the DRBs to activate or de-activate the UP integrity/confidentiality as per the received policy from SMF.

In case of the target gNB receives both UE security capability and UP security policy, then gNB initiates the intra-cell handover procedure which contains selected algorithm and an NCC to the UE. New UP keys shall be derived and used at both the UE and the target gNB.

At an N2-handover the SMF shall send the UE's UP security policy to the target gNB via the target AMF. The target gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF via the target AMF. For all other PDU sessions, the target gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy.

6.6.2 UP security activation mechanism

AS UP integrity protection and ciphering activation shall be done as part of the DRB addition procedure using RRC Connection Reconfiguration procedure as described in this clause, see Figure 6.6.2-1.

The SMF shall send the UP security policy to the gNB as defined in Clause 6.6.1.

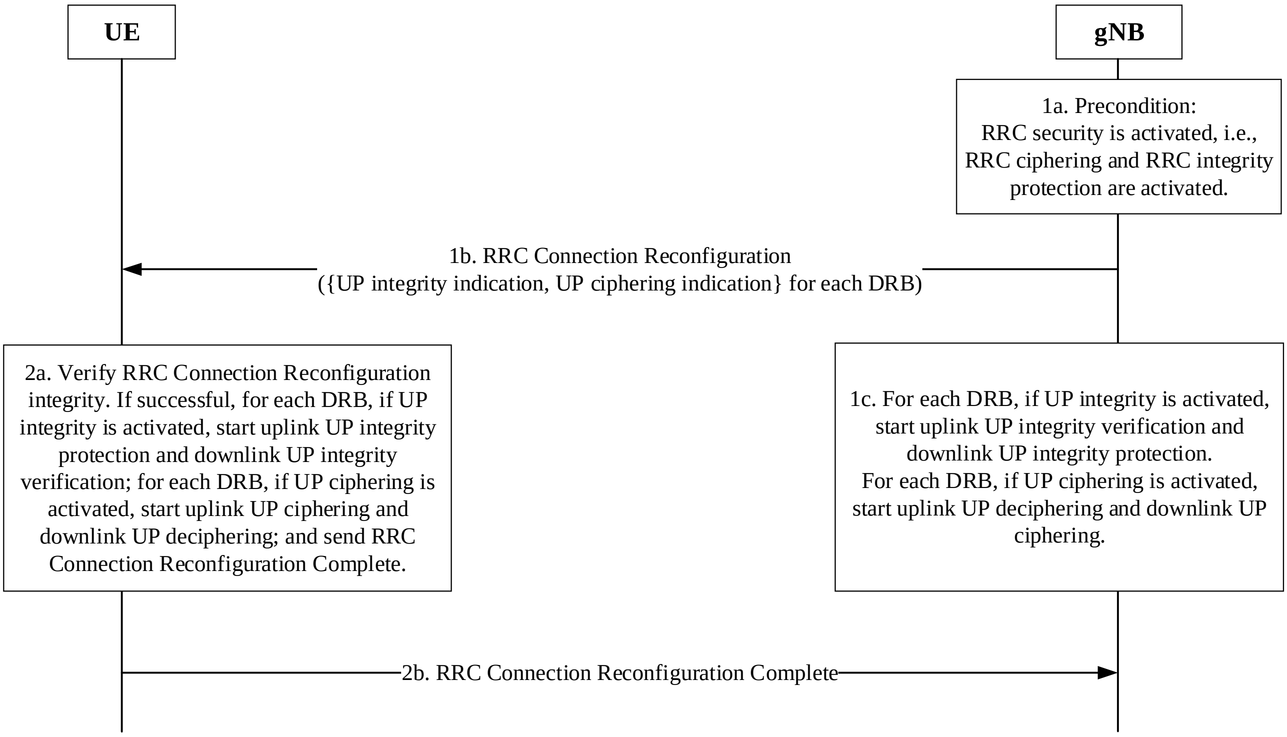
UE
gNB
1a. Precondition:
RRC security is activated, i.e., RRC ciphering and RRC integrity protection are activated.
1b. RRC Connection Reconfiguration
({UP integrity indication, UP ciphering indication} for each DRB)
2a. Verify RRC Connection Reconfiguration integrity. If successful, for each DRB, if UP integrity is activated, start uplink UP integrity protection and downlink UP integrity verification; for each DRB, if UP ciphering is activated, start uplink UP ciphering and downlink UP deciphering; and send RRC Connection Reconfiguration Complete.
1c. For each DRB, if UP integrity is activated, start uplink UP integrity verification and downlink UP integrity protection.
For each DRB, if UP ciphering is activated, start uplink UP deciphering and downlink UP ciphering.
2b. RRC Connection Reconfiguration Complete

Figure 6.6.2-1: User plane (UP) security activation mechanism

1a. This RRC Connection Reconfiguration procedure which is used to add DRBs shall be performed only after RRC security has been activated as part of the AS security mode command procedure defined in Clause 6.7.4.

1b. The gNB shall send the RRC Connection Reconfiguration message to the UE for UP security activation containing indications for the activation of UP integrity protection and ciphering for each DRB according to the security policy.

1c. If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB does not have K_{UPint}, the gNB shall generate K_{UPint} and UP integrity protection for such DRBs shall start at the gNB. Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB does not have K_{UPenc}, the gNB shall generate K_{UPenc} and UP ciphering for such DRBs shall start at the gNB.

2a. UE shall verify the RRC Connection Reconfiguration message. If successful:

2a.1 If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have K_{UPint}, the UE shall generate K_{UPint} and UP integrity protection for such DRBs shall start at the UE.

2a.2 Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have K_{UPenc}, the UE shall generate K_{UPenc} and UP ciphering for such DRBs shall start at the UE

2b. If the UE successfully verifies integrity of the RRC Connection Reconfiguration message, the UE shall send the RRC Connection Reconfiguration Complete message to the gNB.

If UP integrity protection is not activated for DRBs, the gNB and the UE shall not integrity protect the traffic of such DRB and shall not put MAC-I into PDCP packet.

If UP ciphering is not activated for DRBs, the gNB and the UE shall not cipher the traffic of such DRBs.

6.6.3 UP confidentiality mechanisms

The PDCP protocol, as specified in TS 38.323 [23] between the UE and the 5G-RAN, shall be responsible for user plane data confidentiality protection.

The use and mode of operation of the 128-bit NEA algorithms are specified in Annex D.

The input parameters to the 128-bit NEA algorithms as described in Annex D are the message packet, an 128-bit cipher key K_{UPenc} as KEY, a 5-bit bearer identity BEARER which value is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, the length of the keystream required LENGTH and a bearer specific, and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

6.6.4 UP integrity mechanisms

The PDCP protocol, as specified in TS 38.323 [23] between the UE and the 5G-RAN, shall be responsible for user plane data integrity protection.

The use and mode of operation of the 128-bit NIA algorithms are specified in Annex D.

The input parameters to the 128-bit NIA algorithms as described in Annex D are, the message packet, a 128-bit integrity key K_{UPenc} as KEY, a 5-bit bearer identity BEARER value of which is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, and a bearer specific, and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

6.7 Security algorithm selection, key establishment and security mode command procedure

6.7.1 Procedures for NAS algorithm selection

6.7.1.1 Initial NAS security context establishment

Each AMF shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for NAS integrity algorithms, and one for NAS ciphering algorithms. These lists shall be ordered according to a priority decided by the operator.

To establish the NAS security context, the AMF shall choose one NAS ciphering algorithm and one NAS integrity protection algorithm. The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists.

6.7.1.2 AMF change

If the change of the AMF at N2-Handover or mobility registration update results in the change of algorithm to be used for establishing NAS security, the target AMF shall indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC). The AMF shall select the NAS algorithm which has the highest priority according to the ordered lists (see sub-clause 6.7.1.1 of the present document).

6.7.2 NAS security mode command procedure

The NAS SMC shown in Figure 6.7.2-1 shall be used to establish NAS Security context between the UE and the AMF. This procedure consists of a roundtrip of messages between the AMF and the UE. The AMF sends the NAS Security Mode Command message to the UE and the UE replies with the NAS Security Mode Complete message.

NOTE 1: The NAS SMC procedure is designed such that it protects the Registration Request against a man-in-the-middle attack where the attacker modifies the IEs containing the UE security capabilities provided by the UE in the Registration Request. It works as follows: if the method completes successfully, the UE is attached to the network knowing that no bidding down attack has happened. In case a bidding down attack was attempted, the verification of the NAS SMC will fail and the UE replies with a reject message meaning that the UE will not attach to the network.

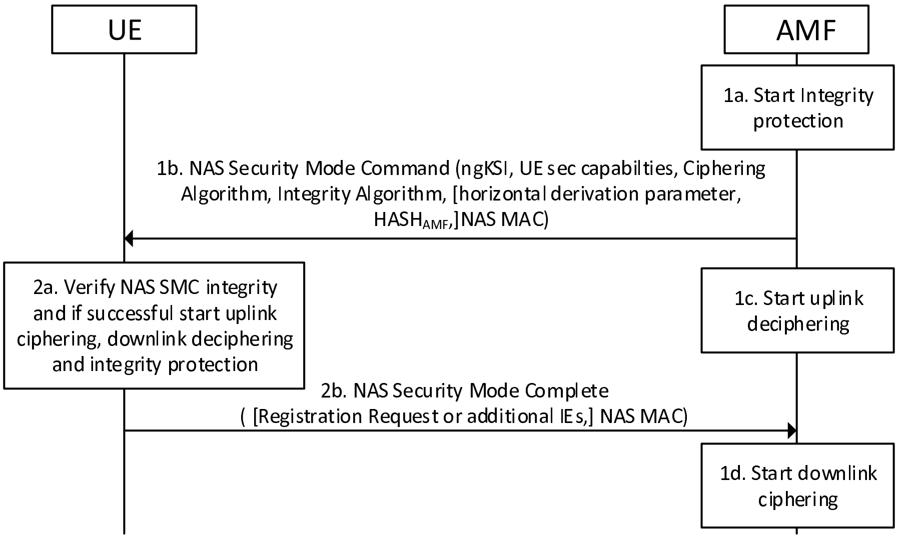
UE
AMF
1a. Start Integrity protection
1b. NAS Security Mode Command (ngKSI, UE sec capabilties, Ciphering Algorithm, Integrity Algorithm, [horizontal derivation parameter, HASH$_{AMF}$,]NAS MAC)
2a. Verify NAS SMC integrity and if successful start uplink ciphering, downlink deciphering and integrity protection
1c. Start uplink deciphering
2b. NAS Security Mode Complete ([Registration Request or additional IEs,] NAS MAC)
1d. Start downlink ciphering

Figure 6.7.2-1: NAS Security Mode Command procedure

1a. The AMF activates the NAS integrity protection before sending the NAS Security Mode Command message.

1b. The AMF sends the NAS Security Mode Command message to the UE. The NAS Security Mode Command message shall contain: the replayed UE security capabilities, the selected NAS algorithms, and the ngKSI for identifying the K_{AMF}. The NAS Security Mode Command message may contain: K_AMF_change_flag (carried in the additional 5G security parameters IE specified in TS 24.501 [35]) to indicate a new K_{AMF} is calculated $HASH_{AMF}$, Anti-Bidding down Between Architectures (ABBA) parameter. In the case of horizontal derivation of K_{AMF} during mobility registration update or during multiple registration in same PLMN, horizontal derivation parameter shall be included in the NAS Security Mode Command message as described in clause 6.9.3.

The inclusion of $HASH_{AMF}$ is described in clause 6.4.6. The AMF shall calculate a $HASH_{AMF}$ as described in Annex H.2. This message shall be integrity protected (but not ciphered) with NAS integrity key based on the K_{AMF} indicated by the ngKSI in the NAS Security Mode Command message (see Figure 6.7.2-1). NAS uplink deciphering at the AMF with this context starts after sending the NAS Security Mode Command message.

NOTE 2: Void.

In case the network supports interworking using the N26 interface between MME and AMF, the AMF shall also include the selected EPS NAS algorithms (defined in Annex B of TS 33.401 [10]) to be used after mobility to EPS in the NAS Security Mode Command message (see clause 8.5.2). The UE shall store the algorithms for use after mobility to EPS using the N26 interface between MME and AMF. The AMF shall store the selected EPS algorithms in the UE security context.

This message shall be integrity protected (but not ciphered) with NAS integrity key derived from the K_{AMF} indicated by the ngKSI in the NAS Security Mode Command message.

1c. The AMF activates NAS uplink deciphering after sending the NAS Security Mode Command message.

2a. The UE shall verify the NAS Security Mode Command message. This includes checking that the UE security capabilities sent by the AMF match the ones stored in the UE to ensure that these were not modified by an attacker and verifying the integrity protection using the indicated NAS integrity algorithm and the NAS integrity key based on the K_{AMF} indicated by the ngKSI.

In case the NAS Security Mode Command message includes a $HASH_{AMF}$, the UE shall calculate $HASH_{UE}$ from the entire initial NAS message that it has sent and compare it against $HASH_{AMF}$. The UE shall calculate $HASH_{UE}$ as described in Annex H.2.

The UE may calculate the $HASH_{UE}$ after it sends the Registration Request and before it receives the NAS Security Mode Command message. Alternatively, the UE may calculate the $HASH_{UE}$ after successfully verifying a NAS Security Mode Command message that includes a $HASH_{AMF}$.

In case the NAS Security Mode Command message includes a horizontal derivation parameter, the UE shall derive a new K_{AMF} as described in Annex A.13 and set the NAS COUNTs to zero.

If the verification of the integrity of the NAS Security Mode Command message is successful, the UE shall start NAS integrity protection and ciphering/deciphering with the security context indicated by the ngKSI.

2b. The UE sends the NAS Security Mode Complete message to the AMF ciphered and integrity protected. The NAS Security Mode Complete message shall include PEI in case AMF requested it in the NAS Security Mode Command message. The handling of $HASH_{AMF}$ is described in clause 6.4. The AMF shall set the NAS COUNTs to zero if horizontal derivation of K_{AMF} is performed.

If the verification of the NAS Security Mode Command message is not successful in the UE, it shall reply with a NAS Security Mode Reject message (see TS 24.501 [35]). The NAS Security Mode Reject message and all subsequent NAS messages shall be protected with the previous, if any, 5G NAS security context, i.e., the 5G NAS security context used prior to the failed NAS Security Mode Command message. If no 5G NAS security context existed prior to the NAS Security Mode Command message, the NAS Security Mode Reject message shall remain unprotected.

NOTE 2: A failed hash comparison does not affect the security establishment as the UE has still checked the UE security capabilities the AMF sent in the NAS Security Mode Command message.

The AMF shall de-cipher and check the integrity protection on the NAS Security Mode Complete message using the key and algorithm indicated in the NAS Security Mode Command message. NAS downlink ciphering at the AMF with this security context shall start after receiving the NAS Security Mode Complete message. If the AMF has sent $HASH_{AMF}$ in 1b, the AMF shall perform as described in clause 6.4.6.

1d. The AMF activates NAS downlink de-ciphering.

NOTE 3: If the uplink NAS COUNT will wrap around by sending the NAS Security Mode Reject message, the UE releases the NAS connection instead of sending the NAS Security Mode Reject message.

6.7.3 Procedures for AS algorithm selection

6.7.3.0 Initial AS security context establishment

This clause provides the details for AS security algorithms negotiation and consideration during the UE initial AS security context establishment.

Each gNB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator. When AS security context is to be established in the gNB, the AMF shall send the UE 5G security capabilities to the gNB. The gNB shall choose the ciphering algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities.

The gNB shall choose the integrity algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities. The chosen algorithms shall be indicated to the UE in the AS SMC. The chosen ciphering algorithm is used for ciphering (when activated) of the user plane and RRC traffic. The chosen integrity algorithm is used for integrity protection (when activated) of the user plane and RRC traffic. Activation of ciphering and integrity protection for the RRC traffic shall be done as defined by clause 6.7.4. Activation of ciphering and integrity protection for the user plane traffic shall be done based on the UP security policy received from the SMF as defined by clause 6.6.2.

6.7.3.1 Xn-handover

At handover from a source gNB over Xn to a target gNB, the source gNB shall include the UE's 5G security capabilities and ciphering and integrity algorithms used in the source cell in the handover request message. The target gNB shall select the algorithm with highest priority from the received 5G security capabilities of the UE according to the prioritized locally configured list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the target gNB selects different algorithms compared to the source gNB. If the UE does not receive any selection of integrity and ciphering algorithms, it continues to use the same algorithms as before the handover (see TS 38.331 [22]). In the Path-Switch message, the target gNB shall send the UE's 5G security capabilities received from the source gNB to the AMF. The AMF shall verify that the UE's 5G security capabilities received from the target gNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB in the Path-Switch Acknowledge message. Additionally, the AMF may log the event and may take additional measures, such as raising an alarm.

If the target gNB receives UE's 5G security capabilities from the AMF in the Path-Switch Acknowledge message, the target gNB shall update the AS security context of the UE with these 5G security capabilities of the UE. The target gNB shall select the algorithm with highest priority from these 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). If the algorithms selected by the target gNB are different from the algorithms used at the source gNB, then the target gNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure indicating the selected algorithms and a NCC to the UE.

NOTE: Transferring the ciphering and integrity algorithms used in the source cell to the target gNB in the handover request message allows for the target gNB to decipher and verify the integrity of the RRC Reestablishment Complete message on SRB1 in the potential RRC Connection Re-establishment procedure. The information is also used by the target gNB to decide if it is necessary to include a new selection of security algorithms in the Handover Command message.

6.7.3.2 N2-handover

At handover from a source gNB to a target gNB over N2 (possibly including an AMF change and hence a transfer of the UE's 5G security capabilities from the source AMF to the target AMF), the target AMF shall send the UE's 5G security capabilities to the target gNB in the NGAP HANDOVER REQUEST message (see TS 33.413 [34]). The target gNB shall select the algorithm with highest priority from the UE's 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the target gNB selects different algorithms compared to the source gNB. If the UE does not receive any selection of integrity and ciphering algorithms, it continues to use the same algorithms as before the handover (see TS 38.331 [22]).

For N2-handover, the source gNB shall include AS algorithms used in the source cell (ciphering and integrity algorithms) in the source to target transparent container that shall be sent to the target gNB. The AS algorithms used by in the source cell are provided to the target gNB so that it can decipher and integrity verify the RRC Connection Reestablishment Complete message on SRB1 in the potential RRC Connection Re-establishment procedure.

6.7.3.3 Intra-gNB-CU handover

It is not required to change the AS security algorithms during intra-gNB-CU handover. If the UE does not receive an indication of new AS security algorithms during an intra-gNB-CU handover, the UE shall continue to use the same algorithms as before the handover (see TS 38.331 [22]).

6.7.3.4 Transitions from RRC-INACTIVE to RRC-CONNECTED states

At state transition from RRC-INACTIVE to RRC-CONNECTED, the source gNB shall include the UE 5G security capabilities and the ciphering and integrity algorithms the UE was using with the source cell in the <Xn-AP Retrieve UE Context Response> message.

The target gNB shall check if it supports the received algorithms, if the target gNB supports the received ciphering and integrity algorithms, the target gNB shall check the received algorithms to its locally configured list of algorithms (this applies for both integrity and ciphering algorithms). If the target gNB selects the same security algorithms, the target gNB shall use the selected algorithms to derive RRC integrity and RRC encryption keys to protect the <RRC Connection Resume> message and send to the UE on SRB1.

If the target gNB does not support the received algorithms or if the target gNB prefers to use different algorithms, the target gNB shall send an <RRC Connection Setup> message on SRB0 in order to proceed with RRC connection establishment as if the UE was in RRC-IDLE (fallback procedure) to the UE. Then the UE performs NAS based RRC recovery and negotiates a suitable algorithm with target gNB via AS SMC procedure.

6.7.3.5 RNA Update procedure

If the source gNB decides to relocate UE context to the target gNB during an RNA Update procedure, the source gNB shall include the UE 5G security capabilities and the ciphering and integrity algorithms the UE was using with the source cell in the <Xn-AP Retrieve UE Context Response> message. AS security algorithm selection is as described in clause 6.7.3.4.

6.7.3.6 Algorithm negotiation for unauthenticated UEs in LSM

UEs that are in limited service mode (LSM) and that cannot be authenticated by the AMF/SEAF (for whatever reason) may still be allowed to establish emergency session by sending the emergency registration request message. It shall be possible to configure whether the AMF allows unauthenticated UEs in LSM to establish bearers for emergency session or not. If an AMF allows unauthenticated UEs in LSM to establish bearers for an emergency session, then for the NAS protocol, the AMF shall use NIA0 and NEA0 as the integrity and ciphering algorithm respectively.

If the AMF allows an unauthenticated UE in LSM to establish bearers for emergency session after it has received the emergency registration request message from the UE, the AMF shall:

- Select NIA0 and NEA0, regardless of the supported algorithms announced previously by the UE as the NAS algorithms and signal this to the UE via the NAS security mode command procedure when activating the 5G NAS security context.
- Set the UE 5G security capabilities to only contain EIA0, EEA0, NIA0 and NEA0 when sending these to the 5G RAN in the following messages:
    - NGAP UE INITIAL CONTEXT SETUP
    - NGAP UE CONTEXT MODIFICATION REQUEST
    - NGAP HANDOVER REQUEST

NOTE: As a result of that the AMF only sending a UE 5G security capability containing EIA0, EEA0, NIA0 and NEA0 to the 5G RAN, the 5G RAN is only able of selecting a null integrity protection for AS integrity protection and a null ciphering algorithm for AS confidentiality protection. That is, if NIA0 is used for NAS integrity protection, then NIA0 or EIA0 will always be used for AS integrity protection.

If NIA0 is disabled at the gNB for regulatory requirements and the gNB receives the UE 5G security capabilities to only contain NIA0 for integrity protection algorithms from the AMF in one of the above messages, the gNB shall reject the session.

The rules for when the AMF shall select NIA0 for NAS integrity protection, and when the UE shall accept a NAS security mode command selecting NIA0 for NAS integrity protection depends on whether the UE and AMF can be certain that no 5G NAS security context can be established. The rules for determining this is defined in clause 10 of this specification. If the AMF has selected NIA0 as the NAS integrity protection algorithm, the UE shall accept selection of NIA0 or EIA0 as the AS integrity protection algorithm. Selection of AS integrity protection algorithm happens via the AS security mode command procedure or via a handover command. The UE shall under no other circumstances accept selection of null integrity algorithm as the AS integrity protection algorithm.

6.7.4 AS security mode command procedure

The AS SMC procedure is for RRC and UP security algorithms negotiation and RRC security activation. AS SMC procedure can be triggered to establish a secure RRC signalling-only connection during UE registration or PDU session establishment as specified in TS 38.413 [34] and TS 23.502 [8]. The activation of UP security is as described in clause 6.6.2. AS SMC procedure consists of a roundtrip of messages between gNB and UE. The gNB sends the AS security mode command to the UE and the UE replies with the AS security mode complete message. See Figure 6.7.4-1.

The AS security mode command message sent from gNB to UE shall contain the selected RRC and UP encryption and integrity algorithms. This AS security mode command message shall be integrity protected with RRC integrity key based on the current K_{gNB}.

The AS security mode complete message from UE to gNB shall be integrity protected with the selected RRC algorithm indicated in the AS security mode command message and RRC integrity key based on the current K_{gNB}.

RRC downlink ciphering (encryption) at the gNB shall start after sending the AS security mode command message. RRC uplink deciphering (decryption) at the gNB shall start after receiving and successful verification of the AS security mode complete message.

RRC uplink ciphering (encryption) at the UE shall start after sending the AS security mode complete message. RRC downlink deciphering (decryption) at the UE shall start after receiving and successful verification of the AS security mode command message.

If any control of the AS security mode command is not successful in the UE, the UE shall reply with an unprotected security mode failure message (see TS 38.331[22]).

Ciphering and integrity protection of UP downlink and uplink, at the UE and the gNB, shall start as defined by clause 6.6.2.

AS SMC shall be used only during an initial context setup between the UE and the gNB (i.e., to activate an initial K_{gNB} at RRC-IDLE to RRC-CONNECTED state transition).

NOTE: Derivation of a K_{gNB} at RRC-IDLE to RRC-CONNECTED state ensures that AS SMC establishes a fresh K_{gNB}. Consequently, the PDCP COUNTs can be reset.

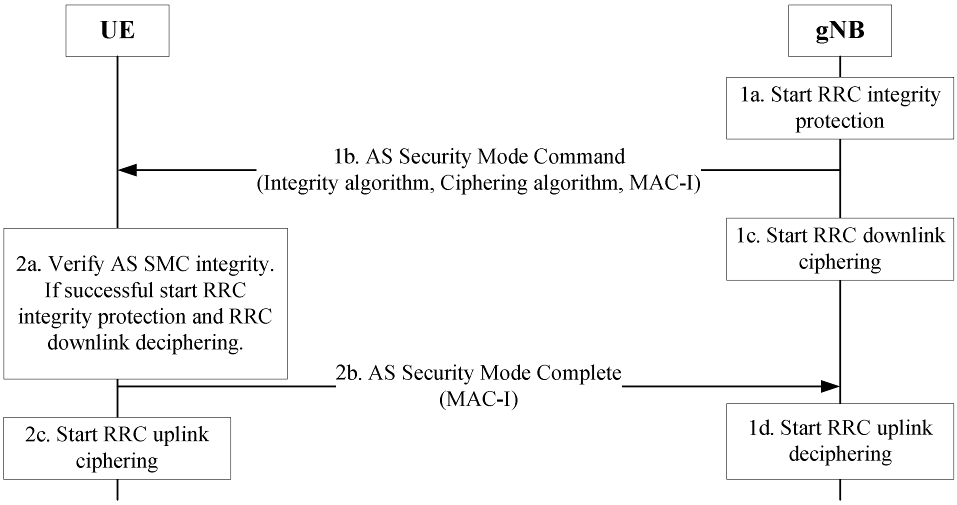
UE
gNB
1a. Start RRC integrity protection
1b. AS Security Mode Command (Integrity algorithm, Ciphering algorithm, MAC-I)
1c. Start RRC downlink ciphering
2a. Verify AS SMC integrity. If successful start RRC integrity protection and RRC downlink deciphering.
2b. AS Security Mode Complete (MAC-I)
2c. Start RRC uplink ciphering
1d. Start RRC uplink deciphering

Figure 6.7.4-1: AS Security Mode Command Procedure

6.8 Security handling in state transitions

6.8.1 Key handling at connection and registration state transitions

6.8.1.1 Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states

6.8.1.1.0 General

One state machine in the UE and AMF is handling the registration states over 3GPP access and a second state machine is handling the registration states over non-3GPP access. This clause and its sub-clauses applies to both 3GPP access and non-3GPP access. UDM manages separate/independent UE Registration procedure for each access. The AMF shall associate Registration state per access type with the UE.

6.8.1.1.1 Transition from RM-REGISTERED to RM-DEREGISTERED

There are different reasons for transition to the RM-DEREGISTERED state. If a NAS messages leads to state transition to RM-DEREGISTERED, it shall be security protected by the current 5G NAS security context (mapped or native), if such exists in the UE or the AMF.

NOTE: The present document only considers the states RM-DEREGISTERED and RM REGISTERED and transitions between these two states. Other documents define additional RM states (see, e.g. 5GMM states in TS 24.501 [35]).

On transitioning to RM-DEREGISTERED, the UE and AMF shall do the following:

1. If they have a full non-current native 5G NAS security context and a current mapped 5G NAS security context, then they shall make the non-current native 5G NAS security context the current one.

2. They shall delete any mapped or partial 5G NAS security contexts they hold.

Handling of the remaining security parameters for each of these cases are given below:

1. Registration reject: All remaining security parameters shall be removed from the UE and AMF

2. Deregistration:

    a. UE-initiated

        i. If the reason is switch off then all the remaining security parameters shall be removed from the UE and AMF with the exception of the current native 5G NAS security context (as in clause 6.1.1), which should remain stored in the AMF and UE.

        ii. If the reason is not switch off then AMF and UE shall keep all the remaining security parameters.

    b. AMF-initiated

        i. Explicit: all the remaining security parameters shall be kept in the UE and AMF if the detach type is re-registration.

        ii. Implicit: all the remaining security parameters shall be kept in the UE and AMF.

    c. UDM/ARPF-initiated: If the message is "subscription withdrawn" then all the remaining security parameters shall be removed from the UE and AMF.

3. Registration reject: There are various reasons for Registration reject. The action to be taken shall be as given in TS 24.501 [35].

Storage of the full native 5G NAS security context including the pair(s) of distinct NAS COUNT values associated with each access together with respective NAS connection identifier, excluding the UE security capabilities and the keys K_{NASint} and K_{NASenc}, in the UE when the UE transitions to RM-DEREGISTERED state is done as follows:

a) If the ME does not have a full native 5G NAS security context in volatile memory, any existing native 5G NAS security context stored on the USIM or in non-volatile memory of the ME shall be marked as invalid.

b) If the USIM supports RM parameters storage, then the ME shall store the full native 5G NAS security context parameters on the USIM (except for K_{NASint} and K_{NASenc}), mark the native 5G NAS security context on the USIM as valid, and not keep any native 5G NAS security context in non-volatile ME memory.

c) If the USIM does not support RM parameters storage, then the ME shall store the full native 5G NAS security context (except for K_{NASint} and K_{NASenc}) in a non-volatile part of its memory and mark the native 5G NAS security context in its non-volatile memory as valid.

d) For the case that the AMF or the UE enter RM-DEREGISTERED state without using any of the above procedures, the handling of the remaining security parameters shall be as specified in TS 24.501 [35].

6.8.1.1.2 Transition from RM-DEREGISTERED to RM-REGISTERED

6.8.1.1.2.1 General

When starting the transition away from RM DEREGISTERED state with the intent to eventually transitioning to RM-REGISTERED state, if no current 5G NAS security context is available in the ME, the ME shall retrieve native 5G NAS security context stored on the USIM if the USIM supports RM parameters storage and if the stored native 5G NAS security context on the USIM is marked as valid. If the USIM does not support RM parameters storage the ME shall retrieve stored native 5G NAS security context from its non-volatile memory if the native 5G NAS security context is marked as valid. The ME shall derive the K_{NASint} and K_{NASenc} from the K_{AMF} after retrieving the stored 5G NAS security context; see Annex A on NAS key derivation. The retrieved native 5G NAS security context with the derived K_{NASint} and K_{NASenc} shall then become the current 5G NAS security context.

When the ME is transitioning away from RM DEREGISTERED state with the intent to eventually transitioning to RM-REGISTERED state, if the USIM supports RM parameters storage, the ME shall mark the stored 5G NAS security context on the USIM as invalid. If the USIM does not support RM parameters storage, the ME shall mark the stored 5G NAS security context in its non-volatile memory as invalid.

If the ME uses a 5G NAS security context to protect NAS messages, the distinct NAS COUNT values together with the NAS connection identifier associated with this access, are updated in the volatile memory of the ME. If the attempt to transition away from RM DEREGISTERED state with the intent to eventually transitioning to RM-REGISTERED state fails, the ME shall store the (possibly updated) 5G NAS security context including the distinct NAS COUNT values together with the NAS connection identifier associated with this access, on the USIM or non-volatile ME memory and mark it as valid.

NOTE: The present document only considers the states RM-DEREGISTERED and RM REGISTERED and transitions between these two states. Other documents define additional RM states (see, e.g. 5GMM states in TS 24.501 [35]).

When the UE transits from RM-DEREGISTERED to RM-REGISTERED/CM-CONNECTED, there are two cases to consider, either a full native 5G NAS security context exists, or it does not.

6.8.1.1.2.2 Full native 5G NAS security context available

The UE shall transmit a NAS Registration Request message. This message is integrity protected using the distinct NAS COUNT values and the NAS connection identifier associated with this access, and for the case that the 5G NAS security context used by the UE is non-current in the AMF, the rules in clause 6.3.2 apply. Furthermore, provided that the NAS Registration Request was with "PDU session(s) to be re-activated" and there is no NAS SMC procedure before the AS SMC the NAS COUNT of the Registration Request message shall be used to derive the K_{gNB} with the KDF as specified in Annex A.

As a result of the NAS Registration Request with "PDU session(s) to be re-activated", the gNB shall send an AS SMC to the UE to activate AS security. The K_{gNB} used, is derived in the current 5G NAS security context.

When the UE receives the AS SMC without having received a NAS Security Mode Command after the Registration Request with "PDU session(s) to be re-activated", it shall use the uplink NAS COUNT of the Registration Request message that triggered the AS SMC to be sent as freshness parameter in the derivation of theK_{gNB}. From this K_{gNB} the RRC protection keys and the UP protection keys shall be derived as described in sub-clause 6.2.3.1.

The same procedure for refreshing K_{gNB} can be used regardless of the fact if the UE is connecting to the same AMF to which it was connected previously or to a different AMF. In case UE connects to a different AMF and this AMF selects different NAS algorithms, the NAS keys have to be re-derived in the AMF with the new algorithm IDs as input using the KDF as specified in Annex A.

In addition, there is a need for the AMF to send a NAS SMC to the UE to indicate the change of NAS algorithms and to take the re-derived NAS keys into use. The UE shall assure that the NAS keys used to verify the integrity of the NAS SMC are derived using the algorithm ID specified in the NAS SMC. The NAS SMC Command and NAS SMC Complete messages are protected with the new NAS keys.

If there is a NAS Security Mode Command after the Registration Request with "PDU session(s) to be re-activated" but before the AS SMC, the UE and AMF use the uplink NAS COUNT of the most recent NAS Security Mode Complete and the related KAMF as the parameter in the derivation of the K_{gNB}. From this K_{gNB} the RRC protection keys and the UP protection keys are derived as described in sub-clause 6.2.3.1.

6.8.1.1.2.3 Full native 5G NAS security context not available

If in the process described in clause 6.8.1.1.2.2, there is no full native 5G NAS security context available in the AMF (i.e. either the UE has sent an unprotected Registration Request message or the UE has protected the Registration Request message with a current native 5G security context which no longer is stored in the AMF) a primary authentication run is required. If there is a full native 5G NAS security context available in the AMF, then the AMF may (according to AMF policy) decide to run a new primary authentication and a NAS SMC procedure (which activates the new 5G NAS security context based on the K_{AMF} derived during the primary authentication run) after the Registration Request.

If the Registration Request was with "PDU session(s) to be re-activated", the NAS SMC procedure is executed before the corresponding AS SMC. The NAS (uplink and downlink) COUNTs are set to start values, and the start value of the uplink NAS COUNT shall be used as freshness parameter in the K_{gNB} derivation from the fresh K_{AMF} (after primary authentication) when UE receives AS SMC the K_{gNB} is derived from the current 5G NAS security context, i.e., the fresh K_{AMF} is used to derive the K_{gNB}. The KDF as specified in clause Annex A shall be used to derive the K_{gNB}.

NOTE: Using the start value for the uplink NAS COUNT in this case cannot lead to the same combination of K_{AMF} and NAS COUNT being used twice. This is guaranteed by the fact that the first integrity protected NAS message the UE sends to the AMF after primary authentication is the NAS SMC complete message.

The NAS SMC complete message shall include the start value of the uplink NAS COUNT that is used as freshness parameter in the K_{gNB} derivation and the K_{AMF} is fresh. After a primary authentication, a NAS SMC needs to be sent from the AMF to the UE in order to take the new NAS keys into use. Both NAS SMC and NAS SMC Complete messages are protected with the new NAS keys.

6.8.1.1.2.4 UE registration over a second access type to the same AMF

It is assumed in this clause that the UE is already registered over a first access type (say access A). Clauses 6.8.1.1.2.1 and 6.8.1.1.2.2 applies as well when the UE attempts to register over a new access type (access B) to the same AMF with the following addition/exception:

Whenever the UE registers over a second access type (access B) to the same AMF, with the intention to transitioning from RM-DEREGISTERED to RM-REGISTERED state, then a full native 5G NAS security context is already available in the UE and the AMF. In this case, the UE shall directly take into use the available full 5G NAS security context and use it to protect the Registration Request over the second access using the distinct pair of NAS COUNTs for this second access type (access B).

The AMF may decide to run a new primary authentication as part of the Registration procedure on this second access (access B). If a new primary authentication is run, then the new derived partial 5G NAS security context needs to be taken into use on this second access (access B) with a NAS SMC using the distinct pair of NAS COUNTs for this second access. As the UE is already registered on the first access (access A), then the AMF needs to run a NAS SMC procedure on the first access in order to take the partial 5G NAS security context into use as described in clause 6.4.2.2.

If there is a need for the AMF to take a new partial 5G NAS security context into use, derived from primary authentication executed on the first access (access A), then the AMF needs to send a NAS SMC to the UE on the second access (access B) in order to take the new partial 5G NAS security context into use as described in clause 6.4.2.2.

6.8.1.2 Key handling at transitions between CM-IDLE and CM-CONNECTED states

6.8.1.2.0 General

One state machine in the UE and AMF is handling the connection states over 3GPP access and a second state machine is handling the connection states over non-3GPP access. This clause and its sub-clauses applies to both 3GPP access and non-3GPP access when not explicitly stated.

Editor's Note: the impact on the connection states transitions when NAS signalling takes place over non-3GPP access is FFS.

Editor's Note: the impact on the connection states transitions when UE has two established NAS connections with the same AMF is FFS.

6.8.1.2.1 Transition from CM-IDLE to CM-CONNECTED

The UE sends an initial NAS message to initiate transition from CM-IDLE to CM-CONNECTED state (see TS 24.501 [35].

If a full native 5G NAS security context is already available in the UE and the AMF, then the UE shall directly take into use the available full 5G NAS security context and use it to protect the initial NAS message using the distinct pair of NAS COUNTs together with the NAS connection identifier for this access.

If the UE is simultaneously registered over both 3GPP access and non-3GPP access in the same AMF, then if there is a need for the AMF to take a new partial 5G NAS security context into use on this access (access A), derived from primary authentication executed on a different access, then the AMF needs to send a NAS SMC to the UE on this access (access A) in order to take the new partial 5G NAS security context also into use on this access as described in clause 6.4.2.2.

On transitions to CM-CONNECTED, the AMF should be able to check whether a new authentication is required, e.g. because of prior inter-provider handover.

If the UE is simultaneously registered over both 3GPP access and non-3GPP access in the same AMF, then if a new primary authentication is run, then the new derived partial 5G NAS security context needs to be taken into use on this access (access A) with a NAS SMC using the distinct pair of NAS COUNTs for this access. But the new derived partial 5G NAS security context also needs to be taken into use on the other accesses (access B) with a NAS SMC using the distinct pair of NAS COUNTs for the respective access as part of the NAS procedure as described in clause 6.4.2.2.

When cryptographic protection for radio bearers is established RRC protection keys and UP protection keys shall be generated as described in sub-clause 6.2.3.1 while K_{AMF} is assumed to be already available in the AMF.

The initial NAS message shall be integrity protected by the current 5G NAS security context if such exists using the distinct pair of NAS COUNTs together with the NAS connection identifier for this access. If no current 5G NAS security context exists the ME shall signal "no key available" in the initial NAS message.

K_{AMF} may have been established in the AMF as a result of a primary authentication run on this access or on a different access, or as a result of a 5G security context transfer from another AMF during N2 handover or idle mode mobility.

When the gNB releases the RRC connection, the UE and the gNB shall delete the keys they store such that state in the network for CM-IDLE state UEs will only be maintained in the AMF.

6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access

This sub-clause applies to establishment of keys for cryptographically protected radio bearers in 3GPP access only.

The procedure the UE uses to establish cryptographic protection for radio bearers is initiated by an NAS Service Request message or Registration Request message with "PDU session(s) to be re-activated" included from the UE to the AMF. The AMF may initiate the procedure to establish cryptographic protection for radio bearers when "PDU session(s) to be re-activated" is not included in the Registration request and but there is pending downlink UP data or pending downlink signalling.

Editor's Note: The procedures the UE uses to establish cryptographic protection for radio bearers are FFS.

Upon receipt of the NAS message, if the AMF does not require a NAS SMC procedure before initiating the NGAP procedure INITIAL CONTEXT SETUP, the AMF shall derive key K_{gNB} as specified in Annex A using the uplink NAS COUNT (see TS 24.501 [35]) corresponding to the NAS message and the K_{AMF} of the current 5G NAS security context.

The AMF shall communicate the K_{gNB} to the serving gNB in the NGAP procedure INITIAL CONTEXT SETUP. The UE shall derive the K_{gNB} from the K_{AMF} of the current 5G NAS security context.

As a result of the NAS Service Request or Registration procedure, with "PDU session(s) to be re-activated" radio bearers are established, and the gNB sends an AS SMC to the UE. When the UE receives the AS SMC without having received a NAS Security Mode Command, it shall use the NAS uplink COUNT of the NAS message that triggered the AS SMC as freshness parameter in the derivation of the K_{gNB}. The KDF as specified in Annex A shall be used for the K_{gNB} derivation using the K_{AMF} of the current 5G NAS security context. From the K_{gNB} the RRC protection keys and the UP protection keys are derived by the UE and the gNB as described in sub-clause 6.2.

If the NAS procedure establishing radio bearers contains a primary authentication run (which is optional), the NAS uplink and downlink COUNT for the new K_{AMF} shall be set to the start values (i.e. zero). If the NAS procedure establishing radio bearers contains a NAS SMC (which is optional), the value of the uplink NAS COUNT from the most recent NAS Security Mode Complete shall be used as freshness parameter in the K_{gNB} derivation from fresh K_{AMF} of the current 5G NAS security context when executing an AS SMC. The KDF as specified in Annex A shall be used for the K_{gNB} derivation also in this case.

6.8.1.2.3 Establishment of keys for cryptographically protected traffic in non-3GPP access

In the case of non-3GPP access, there are no individual radio bearers set up between the UE and N3IWF. For non-3GPP access, an IPsec tunnel is established between the UE and the interworking function N3IWF. The main SA is used solely for the transport of NAS messages between the UE and the AMF/SMF.

Corresponding to the PDU session of the UE, based on the policies and configuration, N3IWF determines the number of IPsec child SAs to be established and the QoS profiles associated with each IPsec child SA. For example, the N3IWF may decide to establish one IPsec child SA and associate all QoS profiles with this IPsec child SA. In this case, all QoS Flows of the PDU Session would be transferred over one IPsec child SA. N3IWF may also decide to establish different child SAs corresponding to the different QoS flows.

Corresponding to radio bearers in 3GPP access which are mapped to QoS values, for non-3GPPaccess there are only child SAs mapped to QoS values. Cryptographically each child SA is different with distinct key materials exchanged as per RFC 7296 [25].

6.8.1.2.4 Transition from CM-CONNECTED to CM-IDLE

On CM-CONNECTED to CM-IDLE transitions the gNB does no longer need to store state information about the corresponding UE.

In particular, on CM-CONNECTED to CM-IDLE transitions:

- The gNB and the UE shall release all radio bearers and delete the AS security context.
- AMF and the UE shall keep the 5G NAS security context stored.

Editor's Note: The exceptions from when the AMF and the UE shall keep the 5G NAS security context stored is FFS.

6.8.1.3 Key handling for the Registration procedure when registered in 5G-RAN

NOTE: This clause applies to both 3GPP access and non-3GPP access.

Before the UE can initiate the Registration procedure, the UE needs to transition to CM-CONNECTED state. The UE shall use the current 5G security context to protect the Registration Request and include the corresponding 5G-GUTI and ngKSI value. The Registration Request shall be integrity-protected, but not confidentiality-protected. UE shall use the current 5G security context algorithms to protect the Registration Request message. For the case that this security context is non-current in the AMF, the rules in clause 6.3.2 apply.

If "PDU session(s) to be re-activated" is included in the Registration request message or if the AMF chooses to establish radio bearers when there is pending downlink UP data or pending downlink signalling, radio bearers will be established as part of the Registration procedure and a K_{gNB} will be derived. If there was no subsequent NAS SMC, the value of the uplink NAS COUNT, associated withthe 3GPP access over which the Registration request message was sent from the UE to the AMF, is used as freshness parameter in the K_{gNB} derivation using the KDF as specified in clause Annex A.9.

In the case a primary authentication is run successfully, the uplink and downlink NAS COUNT shall be set to the start values (i.e. zero).

In the case source and target AMF use different NAS algorithms, the target AMF re-derives the NAS keys from K_{AMF} with the new algorithm identities as input and provides the new algorithm identifiers within a NAS SMC. The UE shall assure that the NAS keys used to verify the integrity of the NAS SMC are derived using the algorithm identity specified in the NAS SMC.

If there is a NAS Security Mode Command after the Registration Request over 3GPP access, the UE and AMF shall use the value of the uplink NAS COUNT associated with the 3GPP access of the most recent NAS Security Mode Complete and the related K_{AMF} as the parameter in the derivation of the K_{gNB}. From this K_{gNB} the RRC protection keys and the UP protection keys are derived as described in sub-clause 6.2.3.1.

In the case of Registration over non-3GPP access, the UE and AMF shall use the uplink NAS COUNT associated with the non-3GPP access of the most recent NAS Security Mode Complete and the related K_{AMF} as the parameter in the derivation of the K_{N3IWF}. IPsec SA is established between the UE and N3IWF using the K_{N3IWF} as described in sub-clause 7.2.1 of this document.

6.8.2 Security handling at RRC state transitions

6.8.2.1 Security handling at transitions between RRC_INACTIVE and RRC-CONNECTED states

6.8.2.1.1 General

In 5G, the RRC-INACTIVE state allows gNB to suspend the UE's RRC connection while the gNB and the UE continue to maintain the UE 5G AS security context. The UE RRC connection can be resumed at a later time by allowing the UE to transition into RRCCONNECTED state. The UE may transition from RRCINACTIVE state to RRCCONNECTED state to the same last serving gNB which sent the UE into RRCINACTIVE state or to a different gNB. While the UE is in RRCINACTIVE state, the UE and last serving gNB store the UE 5G AS security context which can be reactivated when the UE transitions from RRCINACTIVE to RRCCONNECTED. The gNB and the UE shall behave as defined in following sub-clauses.

6.8.2.1.2 State transition from RRCCONNECTED to RRCINACTIVE

The gNB shall send to the UE an <RRC Connection Inactive> message that is ciphered and integrity protected in PDCP layer using a current AS security context. The gNB shall include a fresh I-RNTI, and an NCC in that <RRC Connection Inactive> message. The I-RNTI is used for context identification, and the UE ID part of the I-RNTI assigned by the gNB shall be different in consecutive suspends of the same UE. This is to avoid tracking of UEs based on the I-RNTI. If the gNB has a fresh and unused pair of {NCC, NH}, the gNB shall include the NCC in the <RRC Connection Inactive> message. Otherwise, the gNB shall include the same NCC associated with the current K_{gNB} in the <RRC Connection Inactive> message. The NCC is used for AS security.

The gNB shall delete the current AS keys K_{RRCenc}, K_{UPenc} (if available), and K_{UPint} (if available) after sending the <RRC Connection Inactive> message to the UE, but shall keep the current AS key K_{RRCint}. If the sent NCC value is fresh and belongs to an unused pair of {NCC, NH}, the gNB shall save the pair of {NCC, NH} in the current UE AS security context and shall delete the current AS key K_{gNB}. If the sent NCC value is equal to the NCC value associated with the current K_{gNB}, the gNB shall keep the current AS key K_{gNB} and NCC. The gNB shall store the sent I-RNTI together with the current UE context including the remainder of the AS security context.

Upon receiving the <RRC Connection Inactive> message from the gNB, the UE shall verify that the integrity of the received <RRC Connection Inactive> message is correct by checking the PDCP MAC-I. If this verification is successful, then the UE shall take the received NCC value and save it as stored NCC with the current UE context. The UE shall delete the current AS keys K_{RRCenc}, K_{UPenc} (if available), and K_{UPint} (if available) , but keep the current AS key K_{RRCint} key. If the stored NCC value is different from the NCC value associated with the current K_{gNB}, the UE shall delete the current AS key K_{gNB}. If the stored NCC is equal to the NCC value associated with the current K_{gNB}, the UE shall keep the current AS key K_{gNB}. The UE shall store the received I-RNTI together with the current UE context including the remainder of the AS security context, for the next state transition.

6.8.2.1.3 State transition from RRCINACTIVE to RRCCONNECTED to a new gNB

When the UE decides to resume the RRC connection to transit from RRC_INACTIVE to RRC_CONNECTED, the UE sends <RRC Connection Resume Request> message on SRB0 and hence it is not integrity protected. However, the <RRC Connection Resume Request> message shall include the I-RNTI and an <InactiveMAC-I>. The I-RNTI (short or full I-RNTI) is used for context identification and its value shall be the same as the I-RNTI that the UE had received from the source gNB in the <RRC Connection Inactive> message. The <InactiveMAC-I> is a 16-bit message authentication token, the UE shall calculate it using the integrity algorithm (NIA) in the stored AS security context, which was negotiated between the UE and the source gNB and the current K_{RRCint} with the following inputs:

- KEY : it shall be set tocurrent K_{RRCint};
- BEARER : all its bits shall be set to 1.
- DIRECTION : its bit shall be set to 1;
- COUNT : all its bits shall be set to 1;
- MESSAGE : it shall be set to <VarInactiveMAC-Input> as defined in TS 38.331 [22] with following inputs:

  source C-RNTI, source PCI, target Cell-ID.

For protection of all RRC messages except <RRC Connection Reject> message following the sent <RRC Connection Resume Request> message, the UE shall derive a K_{gNB}* using the target PCI, target ARFCN-DL and the K_{gNB}/NH based on either a horizontal key derivation or a vertical key derivation as defined in clause 6.9.2.1.1 and Annex A.11. The UE shall further derive K_{RRCint}, K_{RRCenc}, K_{UPenc} (optionally), and K_{UPint} (optionally) from the newly derived K_{gNB}*.

When the target gNB receives the <RRC Connection Resume Request> message from the UE, the target gNB extracts the I-RNTI from the <RRC Connection Resume Request> message. The target gNB contacts the source gNB based on the information in the I-RNTI by sending an <Xn-AP Retrieve UE Context Request> message with the following included: I-RNTI, the <InactiveMAC-I> and target Cell-ID, in order to allow the source gNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context.

The source gNB retrieves the stored UE context including the UE 5G AS security context from its database using the I-RNTI. The source gNB verifies the <InactiveMAC-I> using the current K_{RRCint} key stored in the retrieved UE 5G AS security context (calculating the <InactiveMAC-I> in the same way as described above). If the verification of the

<InactiveMAC-I> is successful, then the source gNB calculates K_{gNB}* using the target cell PCI, target ARFCN-DL and the K_{gNB}/NH in the current UE 5G AS security context based on either a horizontal key derivation or a vertical key derivation according to whether the source gNB has an unused pair of {NCC, NH} as described in Annex A.11. The source gNB can obtain the target PCI and target ARFCN-DL from a cell configuration database by means of the target Cell-ID which was received from the target gNB. Then the source gNB shall respond with an <Xn-AP Retrieve UE Context Response> message to the target gNB including the UE context that contains the UE 5G AS security context. The UE 5G AS security context sent to the target gNB shall include the newly derived K_{gNB}*, the NCC associated to the K_{gNB}*, the UE 5G security capabilities, and the ciphering and integrity algorithms used by the UE with the source cell.

The target gNB shall check if it supports the ciphering and integrity algorithms the UE used with the last source cell. If the target gNB does not support the ciphering and integrity algorithms used in the last source cell or if the target gNB prefers to use different algorithms than the source gNB, then the target gNB shall send an <RRC Connection Setup> message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC_IDLE (i.e., a fallback procedure).

If the target gNB supports the ciphering and integrity algorithms used with the last source cell and these algorithms are the chosen algorithms by the target gNB, the target gNB shall derive new AS keys (RRC integrity key, RRC encryption key and UP keys) using the algorithms the UE used with the source cell and the received K_{gNB}*. The target gNB shall reset all PDCP COUNTs to 0 and activate the new keys in PDCP layer. The target gNB shall respond to the UE with an <RRC Connection Resume> message on SRB1 which is integrity protected and ciphered in PDCP layer using the new RRC keys.

When the UE receives the <RRC Connection Resume> message, the UE shall decrypt the message using the K_{RRCenc} that was derived based on the newly derived K_{gNB}*. The UE shall also verify the <RRC Connection Resume> message by verifying the PDCP MAC-I using the K_{RRCint} that was derived from the newly derived K_{gNB}* If verification of the <RRC Connection Resume> message is successful, the UE shall delete the current K_{RRCint} key and the UE shall save the K_{RRCint}, K_{RRCenc}, K_{UPenc} (optionally), and K_{UPint} (optionally) from the newly derived K_{gNB}* as part of the UE current AS security context. In this case,. the UE shall send the <RRC Connection Resume Complete> message both integrity protected and ciphered to the target gNB on SRB1 using the current K_{RRCint} and K_{RRCenc}.

If the UE receives <RRC Connection Reject> message from the target gNB in response to the UE <RRC Resume Request> message, the UE shall delete newly derived AS keys used for connection resumption attempt, including newly derived K_{gNB}*, newly derivedRRC integrity key, RRC encryption key and UP keys, and keep the current K_{RRCint} and the K_{gNB}/NH in its current AS context.

Security is fully resumed on UE side after reception and processing of RRC connection resume message. The UE can receive data on DRB(s) after having received and processed RRC connection resume message. UL data on DRB(s) can be sent after <RRC Connection Resume Complete> message has been successfully sent.

After a successful transition from RRC_INACTIVE to RRC_CONNECTED the target gNB shall perform Path Switch procedure with the AMF.

6.8.2.1.4 State transition from RRCINACTIVE to RRCCONNECTED to the same gNB

The target gNB may be the same as the source gNB in the description in the previous subclause. If so, the single gNB performs the roles of both the source and target gNB.

6.8.2.2 Key handling during mobility in RRC-INACTIVE state

6.8.2.2.1 General

The purpose of this procedure is to allow the UE to notify the network if it moves out of the configured RNA (RAN-based Notification Area) or if UE initiates a periodic RAN-based notification area update procedure. The UE and gNB store the AS security context in RRC_INACTIVE state and reactivate the AS security context when the UE initiates the RAN-based Notification Area Update (RNAU) procedure.

6.8.2.2.2 RAN-based notification area update to a new gNB

When the UE decides to initiate the RANU procedure the UE may initiate the procedure with a new gNB. In this case, the UE, the target gNB and the source gNB follow the detailed procedure as described in clause 6.8.2.1.3 with the following deviations:

The target gNB shall check if it supports the ciphering and integrity algorithms the UE used with the last source cell. If the target gNB does not support the ciphering and integrity algorithms used in the last source cell or if the target gNB prefers to use different algorithms than the source gNB, then the target gNB shall send an < RRC Connection Setup > message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC_IDLE (fallback procedure).

If the target gNB selects the ciphering and integrity protection algorithms which the UE used with the last source cell and the target gNB decides to send the UE directly back to RRC_INACTIVE state without bringing the UE to RRC_CONNECTED state, the target gNB shall perform a Path Switch procedure with the AMF to get a fresh {NCC, NH} pair before sending the <RRC Connection Inactive> message to the UE. After the target gNB receives a fresh {NCC, NH} pair in the Path Switch Acknowledgement message from the AMF, the target gNB shall set the value of NCC in the <RRC Connection Inactive> message to the NCC value of the received fresh {NCC, NH} pair.

6.8.2.2.3 RAN-based notification area update to the same gNB

When the UE decides to initiate a periodic RANU procedure, the target gNB may be same as the source gNB. If so the single gNB performs the roles of both the source gNB and the target gNB.

6.9 Security handling in mobility

6.9.1 General

Editor's Note: The use of K_{SEAF} in 4G-5G interworking is ffs and may impact this clause.

6.9.2 Key handling in handover

6.9.2.1 General

6.9.2.1.1 Access stratum

The general principle of key handling for K_{NG-RAN}*/NH at handovers is depicted in Figure 6.9.2.1.1-1.

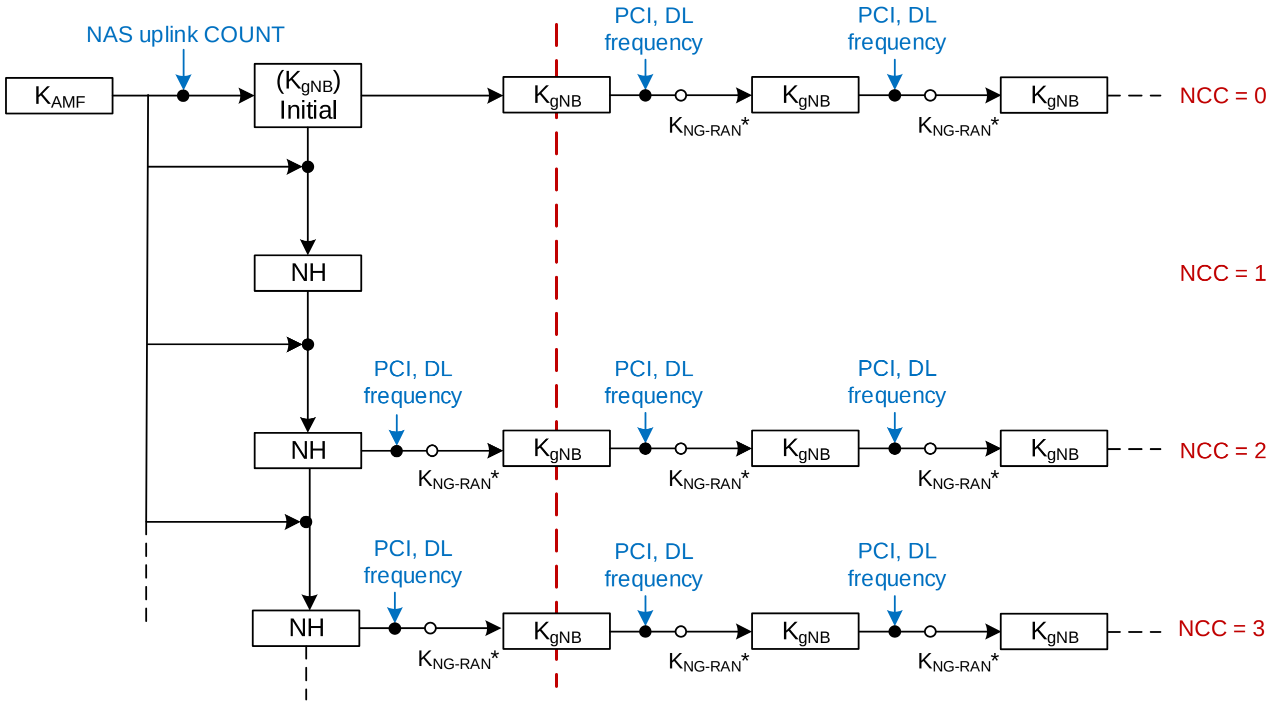

Figure 6.9.2.1.1-1: Model for the handover key chaining

The following is an outline of the key handling model to clarify the intended structure of the key derivations. The detailed specification is provided in sub-clauses 6.9.2.2 and 6.9.2.3.

Whenever an initial AS security context needs to be established between UE and gNB, AMF and the UE shall derive a K_{gNB} and a Next Hop parameter (NH). The K_{gNB} and the NH are derived from the K_{AMF}. A NH Chaining Counter (NCC) is associated with each K_{gNB} and NH parameter. Every K_{gNB} is associated with the NCC corresponding to the NH value from which it was derived. At initial setup, the K_{gNB} is derived directly from K_{AMF}, and is then considered to be associated with a virtual NH parameter with NCC value equal to zero. At initial setup, the derived NH value is associated with the NCC value one.

NOTE 1: At the UE, the NH derivation associated with NCC=1 could be delayed until the first handover performing vertical key derivation.

Whether the AMF sends the K_{gNB} key or the {NH, NCC} pair to the serving gNB is described in detail in sub-clauses 6.9.2.2 and 6.9.2.3. The AMF shall not send the NH value to gNB at the initial connection setup. The gNB shall initialize the NCC value to zero after receiving NGAP Initial Context Setup Request message.

NOTE 2: Since the AMF does not send the NH value to gNB at the initial connection setup, the NH value associated with the NCC value one cannot be used in the next Xn handover or the next intra-gNB handover, for the next Xn handover or the next intra-gNB handover the horizontal key derivation (see Figure 6.9.2.1.1-1) will apply.

NOTE 3: One of the rules specified for the AMF in sub-clause 6.9.2.3.3 of the present document states that the AMF always computes a fresh {NH, NCC} pair that is given to the target gNB. An implication of this is that the first {NH, NCC} pair will never be used to derive a K_{gNB}. It only serves as an initial value for the NH chain.

The UE and the gNB use the K_{gNB} to secure the communication between each other. On handovers, the basis for the K_{gNB} that will be used between the UE and the target gNB, called $K_{NG\text{-}RAN}$*, is derived from either the currently active K_{gNB} or from the NH parameter. If $K_{NG\text{-}RAN}$* is derived from the currently active K_{gNB} this is referred to as a horizontal key derivation (see Figure 6.9.2.1.1-1) and if the $K_{NG\text{-}RAN}$* is derived from the NH parameter the derivation is referred to as a vertical key derivation (see Figure 6.9.2.1.1-1).

As NH parameters are only computable by the UE and the AMF, it is arranged so that NH parameters are provided to gNBs from the AMF in such a way that forward security can be achieved.

On handovers with vertical key derivation the NH is further bound to the target PCI and its frequency ARFCN-DL before it is taken into use as the K_{gNB} in the target gNB. On handovers with horizontal key derivation the currently active K_{gNB} is further bound to the target PCI and its frequency ARFCN-DL before it is taken into use as the K_{gNB} in the target gNB.

6.9.2.1.2 Non access stratum

During mobility, NAS aspects that need to be considered are the possible K_{AMF} change, the possible NAS algorithm change at AMF change, and the possible presence of a parallel NAS connection. There is the possibility that the source AMF and the target AMF do not support the same set of NAS algorithms or have different priorities regarding the use of NAS algorithms. In this case, the target AMF re-derives the NAS keys from the existing K_{AMF} (if unchanged) or derives the NAS keys from the new K_{AMF} (if changed) using the NAS algorithm identities and NAS algorithm types as input to the NAS key derivation functions (see Annex A.8). When the K_{AMF} has not changed, all inputs, in particular the K_{AMF}, will be the same in the re-derivation except for the NAS algorithm identity. When the K_{AMF} has changed, new NAS keys are derived irrespective of change in NAS algorithms.

In case the K_{AMF} has changed or the target AMF decides to use NAS algorithms different from the ones used by the source AMF, the target AMF shall provide needed parameters to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC).

NOTE 1: It is per operator's policy how to configure selection of handover types. Depending on an operator's security requirements, the operator can decide whether to have Xn or N2 handovers for a particular gNB according to the security characteristics of a particular gNB.

NOTE 2: Following key change indicators are involved with N2 handovers. 1) Source AMF indicates AS key re-keying required meaning that the K_{AMF} sent by source AMF to the target AMF is not in sync with current gNB with keyAmfChangeInd (K_{AMF} Change Indicator). 2) Source AMF indicates that the K_{AMF} sent by source AMF to target AMF has been calculated using horizontal K_{AMF} derivation with keyAmfHDerivationInd (K_{AMF} Horizontal Derivation Indicator). 3) The target AMF indicates a horizontal K_{AMF} derivation to the UE with K_AMF_change_flag in the NAS Container to tell the NAS layer of the UE to change $K_{AMF.}$ 4). The target AMF indicates anAS key re-keying to the NG-RAN with NSCI (New Security Context Indicator). 5) The NG-RAN indicates a AS re-keying to the UE with keyChangeIndicator so that the AS layer of the UE knows that new K_{gNB} needs to be derived from new K_{AMF} instead of NH, and NCC needs to be reset to zero.

6.9.2.2 Key derivations for context modification procedure

As outlined in clause 6.9.2.1, whenever a fresh K_{gNB} is calculated from the K_{AMF}, the AMF shall transfer the K_{gNB} to the serving gNB in a message modifying the security context in the gNB. The AMF and the UE shall compute the fresh K_{gNB} as defined in Annex A.9 according to the rules in clause 6.9.6.4. An NCC value 0 is associated with the fresh K_{gNB}. From the fresh K_{gNB}, the gNB and the UE shall compute the K_{gNB}* and then use the computed K_{gNB}* as the K_{gNB} as described in clause 6.9.4.4.

NOTE 1: Unlike EPS, in 5GS the NAS and the AS security contexts are synchronized as a part of handover procedure, if a handover is occurring. See sub-clauses under the clause 6.9.2.3 (key derivations during handover) of the present document.

6.9.2.3 Key derivations during handover

6.9.2.3.1 Intra-gNB-CU handover

The gNB shall have a policy deciding at which intra-gNB -CU handovers the K_{gNB} can be retained and at which a new K_{gNB} needs to be derived. At an intra-gNB-CU handover, the gNB shall indicate to the UE whether to change or retain the current K_{gNB} in the HO Command message. Retaining the current K_{gNB} shall only be done during intra-gNB-CU handover.

If the current K_{gNB} is to be changed, the gNB and the UE shall derive a K_{gNB}* as in Annex A.11 using target PCI, its frequency ARFCN-DL, and either NH or the current K_{gNB} depending on the following criteria: the gNB shall use the NH for deriving K_{gNB}* if an unused {NH, NCC} pair is available in the gNB (this is referred to as a vertical key derivation), otherwise if no unused {NH, NCC} pair is available in the gNB, the gNB shall derive K_{gNB}* from the current K_{gNB} (this is referred to as a horizontal key derivation). The gNB shall send the NCC used for the K_{gNB}* derivation to UE in HO Command message. The gNB and the UE shall use the K_{gNB}* as the K_{gNB}, after handover.

If the current K_{gNB} is to be retained, the gNB and the UE shall continue using the current K_{gNB}, after handover.

NOTE: This clause is also applicable when gNB is implemented as a single unit, i.e., when the gNB is not split into CU and DU.

6.9.2.3.2 Xn-handover

As in intra-gNB handovers, for Xn handovers the source gNB shall perform a vertical key derivation in case it has an unused {NH, NCC} pair. The source gNB shall first compute K_{gNB}* from target PCI, its frequency ARFCN-DL, and either from currently active K_{gNB} in case of horizontal key derivation or from the NH in case of vertical key derivation as described in Annex A.11.

Next, the source gNB shall forward the {K_{gNB}*, NCC} pair to the target gNB. The target gNB shall use the received K_{gNB}* directly as K_{gNB} to be used with the UE. The target gNB shall associate the NCC value received from source gNB with the K_{gNB}. The target gNB shall include the received NCC into the prepared HO Command message, which is sent back to the source gNB in a transparent container and forwarded to the UE by source gNB.

When the target gNB has completed the handover signalling with the UE, it shall send a NGAP PATH SWITCH REQUEST message to the AMF. Upon reception of the NGAP PATH SWITCH REQUEST, the AMF shall increase its locally kept NCC value by one and compute a new fresh NH from its stored data using the function defined in Annex A.10. The AMF shall use the K_{AMF} from the currently active 5G NAS security context for the computation of the new fresh NH. The AMF shall then send the newly computed {NH, NCC} pair to the target gNB in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The target gNB shall store the received {NH, NCC} pair for further handovers and remove other existing unused stored {NH, NCC} pairs if any.

If the AMF had activated a new 5G NAS security context with a new K_{AMF}, different from the 5G NAS security context on which the currently active 5G AS security context is based, but has not yet successfully performed a UE Context Modification procedure, the sent NGAP PATH SWITCH REQUEST ACKNOWLEDGE message shall in addition contain a NSCI (New Security Context Indicator). The AMF shall in this case derive a new initial K_{gNB} from the new K_{AMF} and the uplink NAS COUNT in the most recent NAS Security Mode Complete message as specified in Annex A.9. The AMF shall associate the derived new initial K_{gNB} with a new NCC value equal to zero. Then, the AMF shall use {the derived new initial K_{gNB}, the new NCC value initialized to zero} pair as the newly computed {NH, NCC} pair to be sent in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The gNB shall in this case set the value of keyChangeIndicator field to true in further handovers. The gNB should in this case perform an intra-gNB handover immediately and send appropriate response to the AMF.

NOTE: Because the NGAP PATH SWITCH REQUEST message is transmitted after the radio link handover, it can only be used to provide keying material for the next handover procedure. Thus, for Xn-handovers key separation happens only after two hops because the source gNB knows the target gNB keys. The target gNB can immediately initiate an intra-gNB handover to take the new NH into use once the new NH has arrived in the PATH SWITCH REQUEST ACKNOWLEDGE message.

6.9.2.3.3 N2-Handover

Upon reception of the NGAP HANDOVER REQUIRED message, if the source AMF does not change the active K_{AMF} (meaning no horizontal K_{AMF} derivation) and if AS key re-keying is not required, the source AMF shall increment its locally kept NCC value by one and compute a fresh NH from its stored data using the function defined in Annex A.10. The source AMF shall use the K_{AMF} from the currently active 5GS NAS security context for the computation of the fresh NH. The source AMF shall send the fresh {NH, NCC} pair to the target AMF in the Namf_Communication_CreateUEContext Request message. The Namf_Communication_CreateUEContext Request message shall in addition contain the K_{AMF} that was used to compute the fresh {NH, NCC} pair and its corresponding ngKSI and corresponding uplink and downlink NAS COUNTs.

If the source AMF had activated a new 5G NAS security context with a new K_{AMF}, different from the 5G NAS security context on which the currently active 5G AS security context is based, but has not yet successfully performed a UE Context Modification procedure, the Namf_Communication_CreateUEContext Request message shall in addition contain an indication that the K_{AMF} sent by source AMF to target AMF is not in sync with current K_{gNB} (i.e., keyAmfChangeInd) which means that AS key re-keying is required.

The source AMF uses its local policy to determine whether to perform horizontal K_{AMF} derivation on currently active K_{AMF}. If horizontal K_{AMF} derivation is performed, the Namf_Communication_CreateUEContext Request shall contain an indication (i.e., keyAmfHDerivatoinInd) that the new K_{AMF} has been calculated, an indication (i.e., keyAmfChangeInd) that AS key re-keying is required, and the downlink NAS COUNT used in the horizontal derivation of the sent K_{AMF}. The ngKSI for the newly derived K_{AMF} key has the same value and the same type as the ngKSI of the current K_{AMF}. The source AMF shall include the ngKSI for the newly derived K_{AMF} key in the Namf_Communication_CreateUEContext Request as well.

The source AMF shall always increment the downlink NAS COUNT by one.

Unlike the S10 FORWARD RELOCATION REQUEST message in EPS, the Namf_Communication_CreateUEContext Request message in 5G shall not contain data and meta-data related to old 5G security context.

NOTE 1: Void.

If the target AMF receives the indication of horizontal K_{AMF} derivation (i.e., keyAmfHDerivationInd), it shall derive the NAS keys from the received K_{AMF} as specified in clause A.8 and set the NAS COUNTs to zero. The target AMF shall create a NASC (NAS Container) containing the K_AMF_change_flag, the received downlink NAS COUNT, ngKSI, selected NAS security algorithms, and NAS MAC. The K_AMF_change_flag is set to one when the target AMF receives keyAmfHDerivationInd_. Otherwise, the K_AMF_change_flag is set to zero. If the target AMF does not receive keyAmfHDerivationInd but wants to change the NAS algorithms, it shall create a NASC using the selected NAS security algorithms in the same manner as the case for the horizontal K_{AMF} derivation . However, the target AMF shall not set the NAS COUNTs to zero.

The target AMF shall calculate a 32-bit NAS MAC over the parameters included in the NASC using the K_{NASint} key. The input parameters to the NAS 128-bit integrity algorithms as described in Annex D.3 shall be set as follows when calculating NAS MAC.

The calculation of NAS MAC shall be the 32-bit output of the selected NIA and shall use the following inputs:

- KEY : it shall be set to the corresponding K_{NASint};
- COUNT : it shall be set to 2^{32}-1;
- MESSAGE : it shall be set to the content of NAS Container as defined in TS 24.501 [35];
- DIRECTION : its bit shall be set to 1; and
- BEARER : it shall be set to 0 (i.e., the value of the NAS connection identifier for 3GPP access).

The use of the 2^{32}-1 as the value of the COUNT for the purpose of NAS MAC calculation/verification does not actually set the NAS COUNT to 2^{32}-1. The reason for choosing such a value not in the normal NAS COUNT range, i.e., [0, 2^{24}-1] is to avoid any possibility that the value may be reused for normal NAS messages.

Replay protection is achieved by the UE checking if the downlink NAS COUNT included in the NAS Container is replayed or not. The UE shall not accept the same downlink NAS COUNT value twice before a newly derived K_{AMF} is taken into use and the corresponding downlink NAS COUNT is set to zero. The target AMF shall increment the downlink NAS COUNT by one after creating a NASC.

The NASC is included in the NGAP HANDOVER REQUEST message to the target gNB. The purpose of this NASC could be compared to a NAS SMC message. If the target AMF receives the keyAmfChangeInd, it shall set the NCC to zero and shall further compute a temporary K_{gNB} as defined in Annex A.9. It shall further send the {NCC=0, NH=temporary K_{gNB} } pair and the New Security Context Indicator (NSCI) to the target gNB within the NGAP HANDOVER REQUEST message. The target AMF shall further set the NCC to one and shall further compute a NH as specified in Annex A.10. The target AMF shall further store the {NCC=1, NH} pair.

NOTE 2: The NAS Container (NASC) is defined as Intra N1 mode NAS transparent container in TS 24.501 [35].

NOTE 3: The downlink NAS COUNT is always included in the Namf_Communication_CreateUEContext Request and used by the target AMF for NAS MAC computation. This provides replay protection for NASC.

If the target AMF does not receive the keyAmfChangeInd, it shall store locally the K_{AMF} and {NH, NCC} pair received from the source AMF and then send the received {NH, NCC} pair to the target gNB within the NGAP HANDOVER REQUEST message.

Upon receipt of the NGAP HANDOVER REQUEST message from the target AMF, the target gNB shall compute the K_{gNB} to be used with the UE by performing the key derivation defined in Annex A.11 with the {NH, NCC} pair received in the NGAP HANDOVER REQUEST message and the target PCI and its frequency ARFCN-DL. The target gNB shall associate the NCC value received from AMF with the K_{gNB}. The target gNB shall include the NCC value from the received {NH, NCC} pair, and the NASC if such was also received, into the HO Command message to the UE and remove any existing unused stored {NH, NCC} pairs. If the target gNB had received the NSCI, it shall set the keyChangeIndicator field in the HO Command message to true.

NOTE 4: The source AMF may be the same as the target AMF in the description in this sub-clause. If so the single AMF performs the roles of both the source and target AMF. In this case, actions related to N14 messages are handled internally in the single AMF.

6.9.2.3.4 UE handling

The UE behaviour is the same regardless if the handover is intra-gNB, Xn, or N2.

If the UE also receives a NASC (NAS Container) in the HO Command message, the UE shall update its NAS security context as follows:

NOTE 1: The purpose of this NASC could be compared to a NAS SMC message.

- The UE shall verify the freshness of the downlink NAS COUNT in the NASC.
- If the NASC indicates a new K_{AMF} has been calculated (i.e., K_AMF_change_flag is one),
    - The UE shall compute the horizontally derived K_{AMF} using the K_{AMF} from the current 5G NAS security context identified by the ngKSI included in the NASC and the downlink NAS COUNT in the NASC, as specified in Annex A.13.

  - The UE shall assign the ngKSI included in the NASC to the ngKSI of the new derived K_{AMF}. The UE shall further configure NAS security based on the horizontally derived K_{AMF} and the selected NAS security algorithms in the NASC.
  - The UE shall further verify the NAS MAC in the NASC as described in Clause 6.9.2.3.3 and if the verification is successful, the UE shall further set the NAS COUNTs to zero.
- If K_{AMF} change is not indicated,
  - If the verification is successful, the UE shall configure the NAS security based on the parameters included in the NASC but shall not set the NAS COUNTs to zero.
  - The UE shall verify the NAS MAC in the NASC.
  - The UE shall further set the downlink NAS COUNT value of the currently active NAS security context to the received downlink NAS COUNT value in the NASC.

If keyChangeIndicator in the HO command is true

- If the HO Command message contained a NASC parameter with the K_AMF_change_flag set to one:
  - The UE shall use the horizontally derived K_{AMF} and the zero NAS COUNT in the derivation of the temporary K_{gNB}. The UE shall further processe this temporary key as described in subclause 6.9.4.4.

Else:

- The UE handling related to key derivation shall be done as defined in clause 6.9.4.4.

Else

- If the NCC value the UE received in the HO Command message from target eNB via source gNB is equal to the NCC value associated with the currently active K_{gNB}, the UE shall derive the K_{gNB}* from the currently active K_{gNB} and the target PCI and its frequency ARFCN-DL using the function defined in Annex A.11.
- If the UE received an NCC value that was different from the NCC associated with the currently active K_{gNB}, the UE shall first synchronize the locally kept NH parameter by computing the function defined in Annex A.10 iteratively (and increasing the NCC value until it matches the NCC value received from the source gNB via the HO command message. When the NCC values match, the UE shall compute the K_{gNB}* from the synchronized NH parameter and the target PCI and its frequency ARFCN-DL using the function defined in Annex A.11.

The UE shall use the K_{gNB}* as the K_{gNB} when communicating with the target gNB.

6.9.3 Key handling in mobility registration update

The procedure shall be invoked by the target AMF after the receiving of a Registration Request message of type mobility registration update from the UE wherein the UE and the source AMF are identified by means of a temporary identifier 5G-GUTI.

The protocol steps for the source AMF and target AMF performing context transfer are as follows:

a) The target AMF sends a message to the source AMF, this message contains 5G-GUTI and the received Registration Request message.

b) The source AMF searches the data of the UE in the database and checks the integrity protection on the Registration Request message.

   i) If the UE is found and the integrity check succeeds, when the source AMF does not change K_{AMF} according to its local policy, the source AMF shall send a response back that:

      - shall include the SUPI, and
      - may include any current 5G security context it holds.

ii) If the UE is found and the integrity check succeeds, when the source AMF changes K_{AMF} according to its local policy, the source AMF shall send a response back that:

- shall include the SUPI,
- keyAmfHDerivationInd, and
- may include a new 5G security context it derives from the current one it holds.

The source AMF subsequently deletes the 5G security context which it holds.

If the UE cannot be identified or the integrity check fails, then the source AMF shall send a response indicating that the temporary identifier 5G-GUTI cannot be retrieved.

c) If the target AMF receives a response with a SUPI, it creates an entry and stores the 5G security context that may have beenreceived .

If the target AMF receives a response indicating that the UE could not be identified, it shall initiate the subscription identification procedure described in clause 6.12.4 of the present document.

NOTE: Void.

K_{SEAF} shall not be forwarded to another AMF set.

At mobility registration update, the source AMF shall use local policy to determine whether to perform horizontal K_{AMF} derivation. If the source AMF determines not to perform horizontal K_{AMF} derivation, the source AMF shall transfer current security context to the target AMF. If the source AMF determines to perform horizontal K_{AMF} derivation, the source AMF shall derive a new key K_{AMF} from the currently active K_{AMF} and the uplink NAS COUNT value in the received Registration Request message. The ngKSI for the newly derived K_{AMF} key is defined such as the value field and the type field are taken from the ngKSI of the current K_{AMF}. The source AMF shall transfer the new K_{AMF}, the new ngKSI, the UE security capability, the keyAmfHDerivationInd to the target AMF. The key derivation of the new K_{AMF} is specified in Annex A.13. If the source AMF has derived a new key K_{AMF}, the source AMF shall not transfer the old K_{AMF} to the target AMF and the source AMF shall in this case also delete any stored non-current 5G security context, and not transfer any non-current 5G security context to the target AMF.

When the target AMF receives the new K_{AMF} together with the keyAmfHDerivationInd, then the target AMF shall decide whether to use the K_{AMF} directly according to its local policy after receiving the response from the source AMF.

If the target AMF, according to its local policy, decides to not use the K_{AMF} received from the source AMF, it can perform a re-authentication procedure to the UE to establish a new NAS security context.

If the target AMF decides to use the key K_{AMF} received from source AMF (i.e., no re-authentication), it shall send the K_AMF_change_flag set to 1 to the UE in the NAS SMC including replayed UE security capabilities, the selected NAS algorithms and the ngKSI for identifying the new K_{AMF} from which the UE shall derive a new K_{AMF} to establish a new NAS security context between the UE and target AMF.

The target AMF shall reset the NAS COUNTs to zero and derive new NAS keys (K_{NASint} and K_{NASenc}) from the new K_{AMF} using the selected NAS algorithm identifiers as input. The target AMF shall integrity protect the NAS Security Mode Command message with the new K_{NASint} key.

If the UE receives the K_AMF_change_flag set to 1 in the NAS Security Mode Command message, then the UE shall derive a new key K_{AMF} from the current active K_{AMF} identified by the received ngKSI in the NAS Security Mode Command message using the uplink NAS COUNT valuethat was sent in the Registration Request message. The UE shall assign the received ngKSI in the NAS Security Mode Command message to the ngKSI of the new derived K_{AMF}. The UE shall derive new NAS keys (K_{NASint} and K_{NASenc}) from the new K_{AMF} and integrity check the NAS Security Mode Command message using the new K_{NASint} key.

The UE shall then derive a new initial K_{gNB} from the new K_{AMF} as specified in Annex A.9.

The UE shall associate the derived new initial K_{gNB} with a new NCC value equal to zero and reset the NAS COUNTs to zero.

After the ongoing mobility registration procedure is successfully completed, the ME shall replace the currently stored K_{AMF} and ngKSI values on both USIM and ME with the new K_{AMF} and the associated ngKSI.

6.9.4 Key-change-on-the-fly

6.9.4.1 General

Key change on-the-fly consists of key refresh or key re-keying.

Key refresh shall be possible for K_{gNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-enc}, and K_{UP-int} and shall be initiated by the gNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same K_{gNB}. The procedure is described in clause 6.9.4.5.

Key re-keying shall be possible for the K_{gNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-enc}, and K_{UP-int}. This re-keying shall be initiated by the AMF when a 5G AS security context different from the currently active one shall be activated. The procedures for doing this are described in clause 6.9.4.4.

AS Key change on-the-fly is accomplished using a procedure based on intra-cell handover. The following AS key changes on-the-fly shall be possible: local K_{gNB} refresh (performed when PDCP COUNTs are about to wrap around), K_{gNB} re-keying performed after an AKA run, activation of a native context after handover from E-UTRAN.

Editor's note: Following NAS key related text are adapted from TS 33.401 and kept here for completeness and to not miss them out. It is FFS whether they need updating according to the agreements in SA3 and whether to move them to Clause 6.5.

Key re-keying shall be possible for $K_{NAS-enc}$ and $K_{NAS-int}$. Re-keying of $K_{NAS-enc}$ and $K_{NAS-int}$ shall be initiated by the AMF when a 5G NAS security context different from the currently active one shall be activated. The procedures for doing this are described in clause 6.9.4.2.

Re-keying of the entire 5G key hierarchy including K_{AMF} shall be achieved by first re-keying K_{AMF}, then $K_{NAS-enc}$ and $K_{NAS-int}$, followed by re-keying of the K_{gNB} and derived keys. For NAS key change on-the-fly, activation of NAS keys is accomplished by a NAS SMC procedure.

6.9.4.2 NAS key re-keying

Editor's note: It is FFS whether this clause need updating according to the agreements in SA3 related to NAS keys (e.g. number of NAS keys, number of NAS SMCs, horizontal derivation of K_{AMF}, etc.).

After a primary authentication has taken place, new NAS keys from a new K_{AMF} shall be derived, according to Annex A.8.

To re-activate a non-current full native 5G security context after handover from E-UTRAN the UE and the AMF take the NAS keys into use by running a NAS SMC procedure according to clause 6.7.2.

AMF shall activate fresh NAS keys from a primary authentication run or activate native security context, which has a sufficiently low NAS COUNT values, before the NAS uplink or downlink COUNT wraps around with the current security context.

6.9.4.3 NAS key refresh

Editor's Note: This clause is meant to contain content about K_{AMF} refresh. Scenarios for K_{AMF} refresh are FFS.

6.9.4.4 AS key re-keying

The K_{gNB} re-keying procedure is initiated by the AMF. It may be used under the following conditions:

- after a successful AKA run with the UE as part of activating a partial native 5G security context; or
- as part of synchronizing the NAS and the AS security contexts as a part of handover procedure, if a handover is occuring; or
- as part of re-activating a non-current full native 5G security context after handover from E-UTRAN according to clause 8.4; or
- to create a new K_{gNB} from the current K_{AMF}.

NOTE 1: To perform a key change on-the-fly of the entire key hierarchy, the AMF has to change the 5G NAS security context before changing the 5G AS security context.

In order to be able to re-key the K_{gNB}, the AMF requires a fresh uplink NAS COUNT from a successful NAS SMC procedure with the UE. In the case of creating a new K_{gNB} from the current K_{AMF} a NAS SMC procedure shall be run first to provide this fresh uplink NAS COUNT. This NAS SMC procedure does not have to change other parameters in the current EPS NAS security context. The AMF derives the new K_{gNB} using the key derivation function as specified in Annex A.9 using the K_{AMF} and the uplink NAS COUNT used in the most recent NAS Security Mode Complete message. The derived new K_{gNB} is sent to the gNB in an NGAP UE CONTEXT MODIFICATION REQUEST message triggering the gNB to perform the AS key re-keying. The gNB runs the key change on-the-fly procedure with the UE. During this procedure the gNB shall indicate to the UE that a key change on-the-fly is taking place. The procedure used is based on an intra-cell handover, and hence the same K_{gNB} derivation steps shall be taken as in a normal handover procedure. The gNB shall indicate to the UE to change the current K_{gNB} in intra-cell handover during this procedure. Network-side handling of AS key re-keying that occur as a part of Xn and N2 handovers are described is defined in clauses 6.9.2.3.2 and 6.9.2.3.3 of the present document.

When the UE receives an indication that the procedure is a key change on-the-fly procedure, the UE shall derive a temporary K_{gNB} by applying the key derivation function as specified in Annex A.9 using the K_{AMF} from the current 5G NAS security context and the uplink NAS COUNT in the most recent NAS Security Mode Complete message. UE-side handling of AS key re-keying that occur as a part of Xn and N2 handovers is described in clause 6.9.2.3.4 of the present document.

From this temporary K_{gNB} the UE shall derive the $K_{NG\text{-}RAN}$* as normal (see Annex A.11/A.12). The gNB shall take the K_{gNB} it received from the AMF, which is equal to the temporary K_{gNB}, as basis for its $K_{NG\text{-}RAN}$* derivations. From this step onwards, the key derivations continue as in a normal handover.

If the AS level re-keying fails, then the AMF shall complete another NAS security mode procedure before initiating a new AS level re-keying. This ensures that a fresh K_{gNB} is used.

The NH parameter shall be handled according to the following rules:

- The UE, AMF, and gNB shall delete any old NH upon completion of the context modification.
- The UE and AMF shall use the K_{AMF} from the currently active 5G NAS security context for the computation of the fresh NH. The computation of NH parameter value sent in the Namf_Communication_CreateUEContext Request, NGAP HANDOVER REQUEST, and NGAP PATH SWITCH REQUEST ACKNOWLEDGE messages shall be done according to clauses 6.9.2.3.2 and 6.9.2.3.3.

6.9.4.5 AS key refresh

This procedure is based on an intra-cell handover. The K_{gNB} chaining that is performed during a handover ensures that the K_{gNB} is re-freshed with respect to the RRC and UP COUNT after the procedure. The gNB shall indicate to the UE to change the current K_{gNB} in intra-cell handover during this procedure.

6.9.5 Rules on Concurrent Running of Security Procedures

6.9.5.1 Rules related to AS and NAS security context synchronization

Concurrent runs of security procedures may, in certain situations, lead to mismatches between security contexts in the network and the UE. In order to avoid such mismatches, the following rules shall be adhered to:

1. AMF shall not initiate any of the N2 procedures including a new key towards a UE if a NAS Security Mode Command procedure is ongoing with the UE.
2. The AMF shall not initiate a NAS Security Mode Command towards a UE if one of the N2 procedures including a new key is ongoing with the UE.
3. When the AMF has sent a NAS Security Mode Command to a UE in order to take a new K_{AMF} into use and receives a request for an inter-AMF handover or an inter-RAT handover from the serving gNB, the AMF shall wait for the completion of the NAS SMC procedure (i.e. receiving NAS Security Mode Complete) before initiating an inter-AMF handover or initiating an inter-RAT handover.
4. When the AMF has initiated a NGAP UE Context Modification procedure in order to take a new K_{gNB} into use, and receives a request for an inter-AMF handover from the serving gNB, and decides not to change the K_{AMF} for the inter-AMF handover, the AMF shall wait for the (successful or unsuccessful) completion of the UE Context Modification procedure before initiating an inter-AMF handover.

5. Once the source AMF has initiated inter-AMF handover to the target AMF, or inter-system handover to the target MME, the source AMF shall not send any downlink NAS messages to the UE until it is aware that the handover has either failed or has been cancelled.

6.9.5.2 Rules related to parallel NAS connections

Concurrent runs of security procedures in parallel over two different NAS connections when terminated in the same AMF can lead to race conditions and mismatches between the security contexts in the network and the UE. In order to avoid such mismatches, the following rules shall be followed:

1. The SEAF/AMF shall not initiate a primary authentication or NAS SMC procedure in case a primary authentication or a NAS SMC procedure is ongoing on a parallel NAS connection. Authentication procedures followed by a NAS SMC procedures taking the new 5G security context into use, shall be performed on one NAS signalling connection at a time.

2. When the AMF has sent a NAS Security Mode Command to a UE in order to take a new K_{AMF} into use and receives a context transfer request message for the UE from another AMF, the AMF shall wait for the completion of the NAS SMC procedure (e.g. receiving NAS Security Mode Complete) before transferring the context.

3. The UE shall not initiate a NAS registration over a second NAS connection to an AMF of the same network before primary authentication on the first NAS connection is complete.

6.10 Dual connectivity

6.10.1 Introduction

6.10.1.1 General

This clause describes the security functions necessary to support a UE that is simultaneously connected to more than one NG-RAN node, i.e., Multi-RAT dual connectivity (MR-DC) with 5GC as described in TS 37.340 [51]. The security functions are described in the context of the functions controlling the dual connectivity.

6.10.1.2 Dual Connectivity protocol architecture for MR-DC with 5GC

The dual connectivity protocol architecture for MR-DC with 5GC is shown in figure 6.10.1.2-1. The TS 37.340 [51] is to be referred for further details of the architecture illustrating MCG, SCG, and Split bearers for both SRBs and DRBs. The architecture has the following variants:

- NG-RAN E-UTRA-NR Dual Connectivity (NGEN-DC) is the variant when the UE is connected to one ng-eNB that acts as a Master Node (MN) and one gNB that acts as a Secondary Node (SN). The ng-eNB is connected to the 5GC and the gNB is connected to the ng-eNB via Xn interface.

- NR-E-UTRA Dual Connectivity (NE-DC) is the variant when the UE is connected to one gNB that acts as a MN and one ng-eNB that acts as a SN. The MN (i.e., gNB) is connected to 5GC and the ng-eNB (i.e., SN) is connected to the gNB via Xn interface.

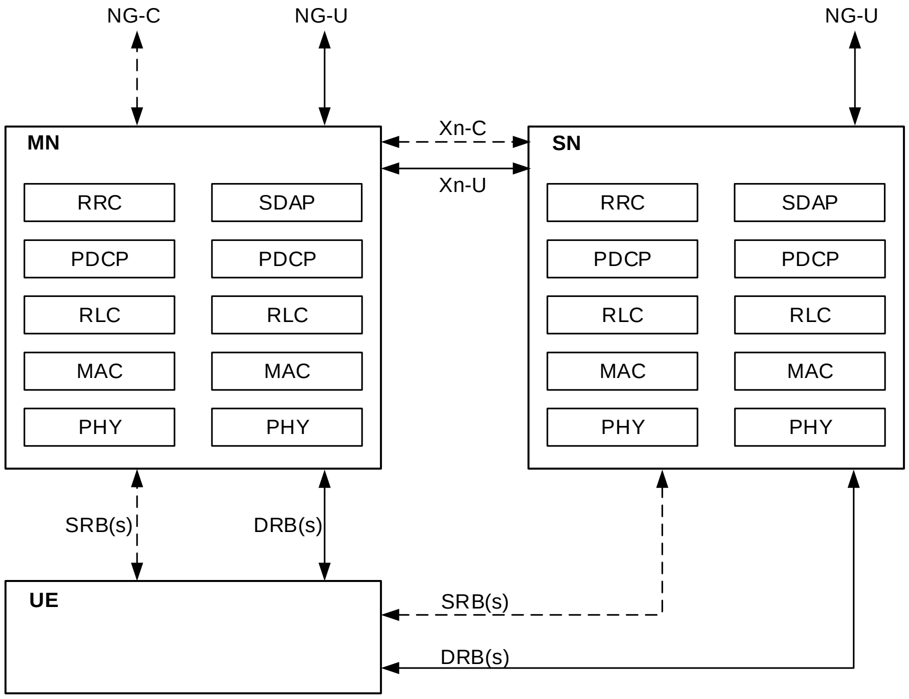

Figure 6.10.1.2-1 Multi-RAT dual connectivity (MR-DC) protocol architecture.

When the MN establishes security context between an SN and the UE for the first time for a given AS security context shared between the MN and the UE, the MN generates the K_{SN} for the SN and sends it to the SN over the Xn-C. To generate the K_{SN}, the MN associates a counter, called an SN Counter, with the current AS security context. The SN Counter is used as freshness input into K_{SN} derivations as described in the clause 6.10.3.2. The MN sends the value of the SN Counter to the UE over the RRC signalling path when it is required to generate a new K_{SN}. The K_{SN} is used to derive further RRC and UP keys that are used between the UE and SN.

6.10.2 Security mechanisms and procedures for DC

6.10.2.1. SN Addition or modification

When the MN is executing the Secondary Node Addition procedure (i.e. initial offload of one or more radio bearers to the SN), or the Secondary Node Modification procedure (as in clauses 10.2.2 and 10.3.2 in TS 37.340 [51]) which requires an update of the K_{SN}, the MN shall derive an K_{SN} as defined in clause 6.10.3.2 The MN shall maintain the SN Counter as defined in Clause6.10.3.1

When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last K_{SN} change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh K_{SN}, and then shall perform a SN Modification procedure to update the K_{SN}.

The dual connectivity procedure with activation of encryption/decryption and integrity protection follows the steps outlined on the Figure 6.10.2.1-1.

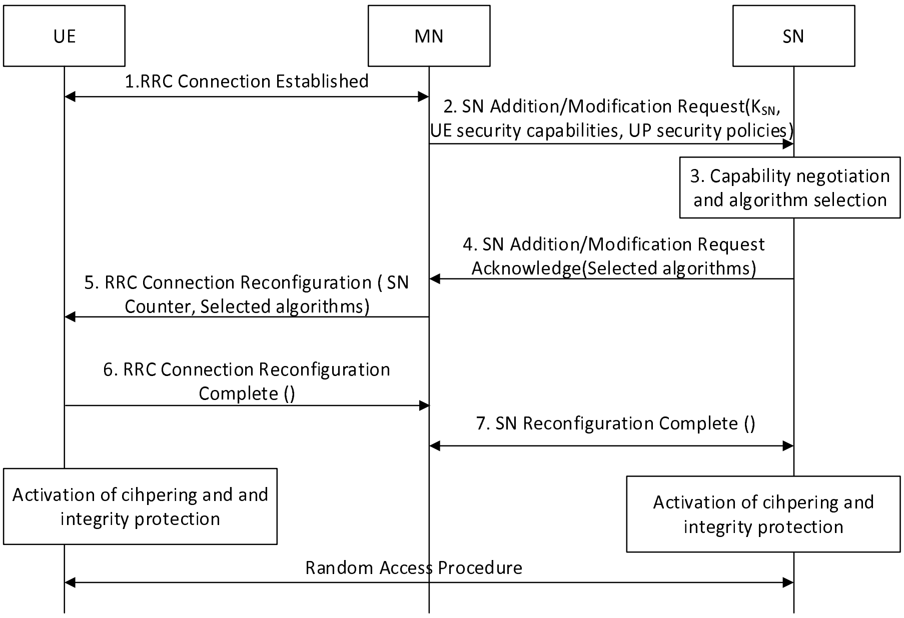
UE
MN
SN
1.RRC Connection Established
2. SN Addition/Modification Request(K_SN, UE security capabilities, UP security policies)
3. Capability negotiation and algorithm selection
4. SN Addition/Modification Request Acknowledge(Selected algorithms)
5. RRC Connection Reconfiguration (SN Counter, Selected algorithms)
6. RRC Connection Reconfiguration Complete ()
7. SN Reconfiguration Complete ()
Activation of cihpering and and integrity protection
Activation of cihpering and integrity protection
Random Access Procedure

Figure 6.10.2.1-1. Security aspects in SN Addition/Modification procedures (MN initiated)

1. The UE and the MN establish the RRC connection.

2. The MN sends SN Addition/Modification Request to the SN over the Xn-C to negotiate the available resources, configuration, and algorithms at the SN. The MN computes and delivers the K_{SN} to the SN if a new key is needed. The UE security capabilities (see subclause 6.10.4) shall also be sent to SN.

3. The SN allocates the necessary resources and chooses the ciphering algorithm and integrity algorithm which has the highest priority from its configured list and is also present in the UE security capability. If a new K_{SN} was delivered to the SN then the SN calculates the needed RRC and UP keys.

4. The SN sends SN Addition/Modification Acknowledge to the MN indicating availability of requested resources and the identifiers for the selected algorithm(s) for the requested DRBs and/or SRB for the UE.

5. The MN sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SN. The MN shall include the SN Counter parameter to indicate a new K_{SN} is needed and the UE shall compute the K_{SN} for the SN. The MN forwards the UE configuration parameters (which contains the algorithm identifier(s) received from the SN in step 4) to the UE (see subclause 6.10.3.3 for further details).

NOTE 3: Since the message is sent over the RRC connection between the MN and the UE, it is integrity protected using the K_{RRCint} of the MN. Hence the SN Counter cannot be tampered with.

6. The UE accepts the RRC Connection Reconfiguration Request after validating its integrity. The UE shall compute the K_{SN} for the SN if an SN Counter parameter was included. The UE shall also compute the needed RRC and UP keys for the associated DRBs and/or SRB. The UE sends the RRC Reconfiguration Complete to the MN. The UE activates the chosen encryption/decryption and integrity protection keys with the SN at this point.

7. MN sends SN Reconfiguration Complete to the SN over the Xn-C to inform the SN of the configuration result. On receipt of this message, SN may activate the chosen encryption/decryption and integrity protection with UE. If SN does not activate encryption/decryption and integrity protection with the UE at this stage, SN shall activate encryption/decryption and integrity protection upon receiving the Random Access request from the UE.

6.10.2.2 Secondary Node key update

6.10.2.2.1 General

The SN shall request the Master Node to update the K_{SN} over the Xn-C, when uplink and/or downlink PDCP COUNTs are about to wrap around for any of the SCG DRBs or SCG SRB.

If the Master Node re-keys its currently active AS key in an 5G AS security context the Master Node shall update any K_{SN} associated with that 5G AS security context.

Whenever the UE or SN start using a fresh K_{SN}, they shall re-calculate the RRC and UP keys from the fresh K_{SN}.

6.10.2.2.2 MN initiated

The Master Node may update the K_{SN} for any reason. If the MN decides to update the K_{SN}, the MN shall perform a SN modification procedure to deliver the fresh K_{SN} to the SN as defined in clause 6.10.2.1. The MN shall provide the value of the SN Counter used in the derivation of the K_{SN} to the UE in an integrity protected RRC Connection Reconfiguration procedure. The UE shall derive the K_{SN} as described in clause A.16.

6.10.2.2.3 SN initiated

When uplink and/or downlink PDCP COUNTs are about to wrap around for any of the SCG DRBs or SCG SRB, the SN shall request the MN to update the K_{SN} over the Xn-C using the SN Modification procedure with MN involvement. The SN shall send the SN Modification Required message including K_{SN} key update an indication to the MN as shown in Figure 6.10.2.2.3-1. When the MN receives K_{SN} Key update indication, the MN shall derive a fresh K_{SN} and send the derived K_{SN} to the SN in the SN Modification Request message as in clause 6.10.2.1. Rest of the flows are like the call flow in Clause 6.10.2.1.

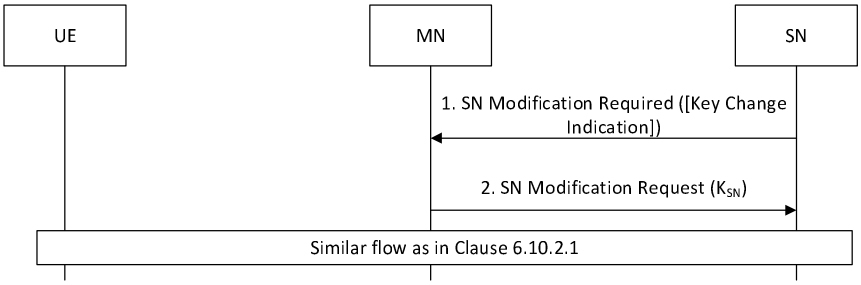
UE
MN
SN
1. SN Modification Required ([Key Change Indication])
2. SN Modification Request (K_{SN})
Similar flow as in Clause 6.10.2.1

Figure 6.10.2.2.3-1. SN Key update procedure using SN Modification procedure (SN initiated with MN involvement)

6.10.2.3 SN release and change

When the SN releases the last UE radio bearer on the SN or when the SN is changed, i.e., the UE radio bearer(s) is moved from the SN, the SN and the UE shall delete the SN RRC and UP keys. The SN and UE shall also delete the K_{SN}, if it was not deleted earlier.

6.10.3 Establishing the security context between the UE and SN

6.10.3.1 SN Counter maintenance

The MN shall maintain a 16-bit counter, SN Counter, in its AS security context. The SN Counter is used when computing the K_{SN}.

The MN maintains the value of the counter SN Counter for a duration of the current 5G AS security context between UE and MN. The UE does not need to maintain the SN Counter after it has computed the K_{SN} since the MN provides the UE with the current SN Counter value when the UE needs to compute a new K_{SN}.

The SN Counter is a fresh input to K_{SN} derivation. That is, the UE assumes that the MN provides a fresh SN Counter each time and does not need to verify the freshness of the SN Counter.

NOTE: An attacker cannot, over the air modify the SN Counter and force re-use of the same SN Counter. The reason for this is that the SN Counter is delivered over the RRC connection between the MN and the UE, and this connection is both integrity protected and protected from replay.

The MN shall set the SN Counter to ‘0’ when a new AS root key, K_{NG-RAN}, in the associated 5G AS security context is established. The MN shall set the SN Counter to ‘1’ after the first calculated K_{SN}, and monotonically increment it for each additional calculated K_{SN}. The SN Counter value '0' is used to calculate the first K_{SN}.

If the MN decides to release the offloaded connections to the SN and later decides to re-start the offloading to the same SN, the SN Counter value shall keep increasing, thus keeping the computed K_{SN} fresh.

The MN shall refresh the root key of the 5G AS security context associated with the SN Counter before the SN Counter wraps around. Refreshing the root key is done using intra cell handover as described in subclause 6.7.3.3 of the present document. When the root key is refreshed, the SN Counter is reset to '0' as defined above.

6.10.3.2 Derivation of keys

The UE and MN shall derive the security key K_{SN} of the SN as defined in Annex A.16 of the present document.

The SN RRC and UP keys shall be derived from the K_{SN} both at the SN and the UE using the function given in Annex A.7 of TS 33.401 [10] if the SN is a ng-eNB or using the function given in Annex A.8 of the present specification if the SN is a gNB.

Once all the SN RRC and UP keys have been derived from the K_{SN}, the SN and UE may delete the K_{SN}.

6.10.3.3 Negotiation of security algorithms

The MN shall receive the UE security capabilities from the AMF or the previous NG-RAN node. These security capabilities include both LTE and NR security capabilities.

When establishing one or more DRBs and/or SRBs for a UE at the SN, as shown on Figure 6.10.2.1-1, the MN shall provide the UE security capabilities of the UE to the SN in the SN Addition/Modification Request message.

Upon receipt of this message, the SN shall select the algorithms with highest priority in its locally configured list of algorithms that are also present in the received UE security capabilities and include the selected algorithms in SN Addition/Modification Request Acknowledge.

The MN shall provide the selected algorithms to the UE during the RRCConnectionReconfiguration procedure that configures the DRBs and/or SRB with the SN for the UE. The UE shall use the indicated algorithms for the DRBs and/or SRB whose PDCP terminates on the SN.

NOTE: The algorithms that the UE uses with the MN can be the same or different to the algorithms used with the SN.

6.10.4 Protection of traffic between UE and SN

This subclause provides the details of the needed SN RRC and UP keys and the algorithms used to protect the traffic whose PDCP terminates on the SN. The UE and SN may either calculate all the SN RRC and UP keys at once or as there are required to be used. The RRC and UP keys are K_{RRCenc} and K_{RRCint} for the SRB whose PDCP terminates on the SN and K_{UPenc} for the DRBs whose PDCP terminate on the SN.

When the SN is a gNB, the RRC and UP traffic is protected using the mechanism described in subclauses 6.5 and 6.6 respectively of the current document with the algorithms specified in Annex D of the present document.

When the SN is a ng-eNB, the RRC and UP traffic is protected using the mechanism described in subclauses 7.4 and 7.3 respectively of TS 33.401 [10] with the algorithms specified in Annex C of TS 33.401 [10].

NOTE: Integrity protection of the user plane whose PDCP terminates on the SN is not supported.

6.10.5 Handover Procedure

During N2 and Xn handover, the DRB and/or SRB connections between the UE and the SN shall be released, and the SN and the UE shall delete the SN RRC and UP keys since they shall be refreshed by the new K_{SN} derived by the target-MN.

6.10.6 Signalling procedure for PDCP COUNT check

SN may request the MN to execute a counter check procedure specified in Clause 6.13 of this specification to verify the value of the PDCP COUNT(s) associated with DRB(s) offloaded to the SN. To accomplish this, the SN shall communicate this request, including the expected values of PDCP COUNT(s) and associated radio bearer identities to the MN over the Xn-C.

If the MN receives a RRC counter check response from the UE that contains one or several PDCP COUNT values (possibly associated with both MN and SN), the MN may release the connection or report the difference of the PDCP COUNT values to the serving AMF or O&M server for further traffic analysis, e.g., detecting the attacker.

6.10.7 Radio link failure recovery

Since the MN holds the control plane functions in MR-DC as in clause 6.10.1.2, the UE runs the RRC re-establishment procedure with the MN as specified in Clause 6.11 of the present document. During the RRC re-establishment procedure, the radio bearers between the UE and the SN shall be released.

6.11 Security handling for RRC Connection Re-establishment Procedure

The K_{NG-RAN}* and token calculation at handover preparation are cell specific instead of gNB specific. During the handover procedure, at potential RRC Connection re-establishment (e.g., in handover failure case), the UE may select a cell different from the target cell to initiate the re-establishment procedure. To ensure that the UE RRCConnectionRe-establishment attempt is successful when the UE selects another cell under the control of the target gNB at handover preparation, the serving gNB may prepare multiple K_{NG-RAN}*s and tokens for multiple cells which are under the control of the target gNB. The serving gNB may prepare for multiple cells belonging to the serving gNB itself.

The preparation of these cells includes sending security context containing K_{NG-RAN}*s and tokens for each cell to be prepared, as well as the corresponding NCC, the UE 5G security capabilities, and the security algorithms used in the source cell for computing the token, to the target gNB. The source gNB shall derive the K_{NG-RAN}*s as described in Annex A.11/A.12 based on the corresponding target cell's physical cell ID and frequency ARFCN-DL.

In order to calculate the token, the source gNB shall use the negotiated NIA-algorithm from the 5G AS Security context from the source gNB with the following inputs: source C-RNTI, source PCI and target Cell-ID, where source PCI and source C-RNTI are associated with the cell the UE last had an active RRC connection with and target Cell-ID is the identity of the target cell where the RRCConnectionReestablishmentRequest is sent to.

- KEY shall be set to K_{RRCint} of the source cell;
- all BEARER bits shall be set to 1;
- DIRECTION bit shall be set to 1;
- all COUNT bits shall be set to 1.

The token shall be the 16 least significant bits of the output of the used integrity algorithm.

In order to avoid UE's inability to perform the RRC re-establishment procedure due to a failure during a handover or a connection re-establishment, the UE shall keep the K_{gNB} used in the source cell until the handover or a connection re-establishment has been completed successfully or until the UE has deleted the K_{gNB} for other reasons (e.g., due to transitioning to CM-IDLE).

For Xn handover, the target gNB shall use the received multiple K_{NG-RAN}*s. But for N2 handover, the target gNB discards the multiple K_{NG-RAN}*s received from the source gNB, and derives the K_{NG-RAN}*s as described in Annex A.11/A.12 based on the received fresh {NH, NCC} pair from AMF for forward security purpose.

When an RRCConnectionReestablishmentRequest is initiated by the UE, the RRCConnectionReestablishmentRequest shall contain the token corresponding to the cell the UE tries to reconnect to. This message is transmitted over SRB0 and hence not integrity protected.

If the target gNB has a prepared K_{NG-RAN}* for the specific cell, the target gNB receiving the RRCConnectionReestablishmentRequest shall respond with an RRCConnectionReestablishment message containing the NCC received during the preparation phase if the token is valid, otherwise the target gNB shall reply with an RRCConnectionReestablishmentReject message. The RRCConnectionReestablishment and RRCConnectionReestablishmentReject messages are also sent on SRB0 and hence not integrity protected. Next the target gNB and UE shall do the following: The UE shall firstly synchronize the locally kept NH parameter as defined in Annex A.10 if the received NCC value is different from the current NCC value in the UE itself. Then the UE shall derive K_{NG-RAN}* as described in Annex A.11/A.12 based on the selected cell's physical cell ID and its frequency ARFCN-DL. The UE shall use this K_{NG-RAN}* as K_{gNB}. The gNB uses the K_{NG-RAN}* corresponding to the selected cell as K_{gNB}. Then, UE and gNB shall derive and activate keys for integrity protection and verification from this K_{gNB} and the AS algorithms (ciphering and integrity algorithms) obtained during handover preparation procedures which were used in source gNB. Even if the AS algorithms used by the source gNB do not match with the target gNB local algorithm priority list the source gNB selected AS algorithms shall take precedence when running the RRCConnectionRe-establishment procedure. The target gNB and UE should refresh the selected AS algorithms and the AS keys based on local prioritized algorithms after the RRCConnectionReestablishment procedure.

NOTE: When the AS algorithms transferred by source gNB are not supported by the target gNB, the target gNB will fail to decipher or integrity verify the RRCReestablishmentComplete message on SRB1. As a result, the RRCConnectionReestablishment procedure will fail.

The UE shall respond with an RRCReestablishmentComplete on SRB1, integrity protected and ciphered using these new keys. The RRCConnectionReconfiguration procedure used to re-establish the remaining radio bearers shall only include integrity protected and ciphered messages.

6.12 Subscription identifier privacy

6.12.1 Subscription permanent identifier

In the 5G system, the globally unique 5G subscription permanent identifier is called SUPI as defined in 3GPP TS 23.501 [2]. The SUCI is a privacy preserving identifier containing the concealed SUPI.

The SUPI is privacy protected over-the-air by using the SUCI which is described in clause 6.12.2. Handling of SUPI and privacy provisioning related to concealing the SUPI shall be done according to the requirements specified in clause 5 and details provided in clause 6.12.2.

6.12.2 Subscription concealed identifier

The SUbscription Concealed Identifier, called SUCI, is a privacy preserving identifier containing the concealed SUPI.

The UE shall generate a SUCI using a protection scheme with the raw public key, i.e. the Home Network Public Key, that was securely provisioned in control of the home network. The protection schemes shall be the ones specified in Annex C of this document or the ones specified by the HPLMN.

The UE shall construct a scheme-input from the subscription identifier part of the SUPI as follows:.

- For SUPIs containing IMSI, the subscription identifier part of the SUPI includes the MSIN of the IMSI as defined in TS 23.003 [19]. This also applies to SUPIs taking the form of a IMSI based NAI as defined in TS 23.003 [19].

- For SUPIs taking the form of a non-IMSI based NAI, the subscription identifier part of the SUPI includes the "username" portion of the NAI as defined in NAI RFC 7542 [57].

The UE shall execute the protection scheme with the constructed scheme-input as input and take the output as the scheme-output.

The UE shall not conceal the Home Network Identifier and the Routing Indicator.

The UE shall construct the SUCI with the following data fields:

- The Home Network Identifier of the SUPI as specified in 23.003 [19]. It is constructed as follows:

    - For SUPIs containing IMSI, the Home Network Identifier includes the MNC/MCC of the IMSI as defined in TS 23.003 [19]. This also applies to SUPIs taking the form of a IMSI based NAI as defined in TS 23.003 [19].

    - For SUPIs taking the form of a non-IMSI based NAI, the Home Network Identifier includes the "realm" portion of the NAI as defined in NAI RFC 7542 [57].

- The Routing Indicator as specified in TS 23.003 [19].

    - The Protection Scheme Identifier that represents a protection scheme as specified in Annex C of this specification, or a protection scheme specified by the HPLMN.

    - The Home Network Public Key Identifier as specified in this document and detailed in TS 23.003 [19].

- The scheme-output as specified in this document and detailed in TS 23.003 [19].

NOTE 1: The format of the SUPI protection scheme identifiers is defined in Annex C.

NOTE 2: The identifier and the format of the scheme output are defined by the protection schemes in Annex C. In case of non-null schemes, the freshness and randomness of the SUCI will be taken care of by the corresponding SUPI protection schemes.

In case of null-scheme being used, the Home Network Public Key Identifier shall be set to a default value as described in TS 23.003 [19].

The UE shall include a SUCI only in the following 5G NAS messages:

- if the UE is sending a Registration Request message of type "initial registration" to a PLMN for which the UE does not already have a 5G-GUTI, the UE shall include a SUCI to the Registration Request message, or
- if the UE includes a 5G-GUTI when sending a Registration Request message of type "re-registration" to a PLMN and, in response, receives an Identity Request message, then the UE shall include a fresh SUCI in the Identity Response message (see clause 6.12.4).

NOTE 3: In response to the Identifier Request message, the UE never sends the SUPI.

The UE shall generate a SUCI using "null-scheme" only in the following cases:

- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen PLMN, or
- if the home network has configured "null-scheme" to be used, or
- if the home network has not provisioned the public key needed to generate a SUCI.

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give the ME any parameter for the calculation of the SUCI including the home network public key, the Home Network Public Key Identifier and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the Home Network Public Key , the Home Network Public Key Identifier and the Protection Scheme Identifier. The operator should use proprietary identifier for protection schemes if the operator chooses that the calculation of the SUCI shall be done in USIM.

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision in the USIM an ordered priority list of the protection scheme identifiers that the operator allows. The priority list of protection scheme identifiers in the USIM shall only contain protection scheme identifiers specified in Annex C, and the list may contain one or more protection schemes identifiers. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Routing Indicator, the Home Network Public Key, the Home Network Public Key Identifier and the list of protection scheme identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list are obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if the home network public key or the priority list are not provisioned in the USIM.

NOTE 4: The above feature is introduced since additional protection schemes could be specified in the future for a release newer than the ME release. In this case, the protection scheme selected by older MEs may not be the protection scheme with the highest priority in the list of the USIM.

6.12.3 Subscription temporary identifier

A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003 [19].

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE in Registration Accept message.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE in Registration Accept message.

Upon receiving network triggered Service Request message from the UE (i.e., Service Request message sent by the UE in response to a Paging message), the AMF shall use a UE Configuration Update procedure to send a new 5G-GUTI to the UE. This UE Configuration Update procedure shall be used before the current NAS signalling connection is released, i.e., it need not be a part of the Service Request procedure because doing so delays the Service Request procedure.

NOTE 1: It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above.

NOTE 2: It is left to implementation to generate 5G-GUTI containing 5G-TMSI that uniquely identifies the UE within the AMF.

5G-TMSI generation should be following the best practices of unpredictable identifier generation.

6.12.4 Subscription identification procedure

The subscriber identification mechanism may be invoked by the serving network when the UE cannot be identified by means of a temporary identity (5G-GUTI). In particular, it should be used when the serving network cannot retrieve the SUPI based on the 5G-GUTI by which the subscriber identifies itself on the radio path.

The mechanism described in figure 6.12.4-1 allows the identification of a UE on the radio path by means of the SUCI.

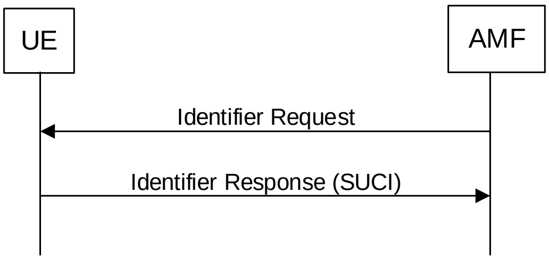

Figure 6.12.4-1: Subscription identifier query

The mechanism is initiated by the AMF that requests the UE to send its SUCI.

The UE shall calculate a fresh SUCI from SUPI using the home network public key, and respond with Identifier Response carrying the SUCI. The UE shall implement a mechanism to limit the frequency at which the UE responds with a fresh SUCI to an Identifier Request for a given 5G-GUTI.

NOTE 1: If the UE is using any other scheme than the null-scheme, the SUCI does not reveal the SUPI.

AMF may initiate authentication with AUSF to receive SUPI as specified in clause 6.1.3.

In case the UE registers for Emergency Services and receives an Identifier Request, the UE shall use the null-scheme for generating the SUCI in the Identifier Response.

NOTE 2: Registration for Emergency does not provide subscription identifier confidentiality.

6.12.5 Subscription identifier de-concealing function (SIDF)

SIDF is responsible for de-concealing the SUPI from the SUCI. When the home network public key is used for encryption of SUPI, the SIDF shall use the private key that is securely stored in the home operator's network to decrypt the SUCI. The de-concealment shall take place at the UDM. Access rights to the SIDF shall be defined, such that only a network element of the home network is allowed to request SIDF.

NOTE: One UDM can comprise several UDM instances. The Routing Indicator in the SUCI can be used to identify the right UDM instance that is capable of serving a subscriber.

6.13 Signalling procedure for PDCP COUNT check

The following procedure is used optionally by the gNB to periodically perform a local authentication. At the same time, the amount of data sent during the AS connection is periodically checked by the gNB and the UE for both up and down streams. If UE receives the Counter Check request, it shall respond with Counter Check Response message. Whenever user plane integrity protection is activated and used on a DRB, the procedure defined in this clause shall not be used for that particular DRB.

The gNB is monitoring the PDCP COUNT values associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.

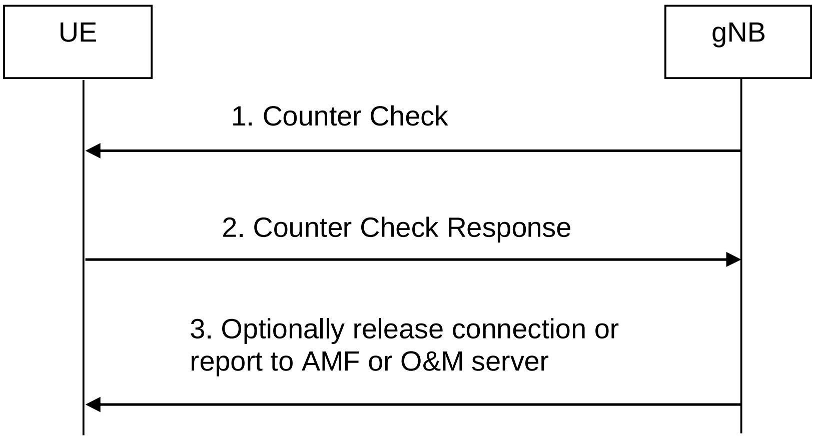
UE
gNB
1. Counter Check
2. Counter Check Response
3. Optionally release connection or report to AMF or O&M server

Figure 6.13-1: gNB periodic local authentication procedure

1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the gNB. The Counter Check message contains the most significant parts of the PDCP COUNT values (which reflect amount of data sent and received) from each active radio bearer.

2. The UE compares the PDCP COUNT values received in the Counter Check message with the values of its radio bearers. Different UE PDCP COUNT values are included within the Counter Check Response message.

3. If the gNB receives a counter check response message that does not contain any PDCP COUNT values, the procedure ends. If the gNB receives a counter check response that contains one or several PDCP COUNT values, the gNB may release the connection or report the difference of the PDCP COUNT values for the serving AMF or O&M server for further traffic analysis for e.g. detecting the attacker.

6.14 Steering of roaming security mechanism

6.14.1 General

This clause describes the security functions necessary to support steering of the UE in the VPLMN during registration procedure and also after registration as described in TS 23.122 [53] Annex C. The security functions are described in the context of the functions supporting the control plane solution for steering of roaming in 5GS.

If the control plane solution for Steering of Roaming is supported by the HPLMN, the AUSF shall store the K_{AUSF} after the completion of the primary authentication.

The content of Steering Information List as well as the conditions for sending it to the UE are described in TS 23.122 [53] Annex C and are not repeated below. For example, the Steering Information List may include a list of preferred PLMN/access technology combinations or HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'.

6.14.2 Security mechanisms

6.14.2.1 Procedure for steering of UE in VPLMN during registration

The security procedure for the case when the UE registers with VPLMN AMF is described below in figure 6.14.2.1-1:

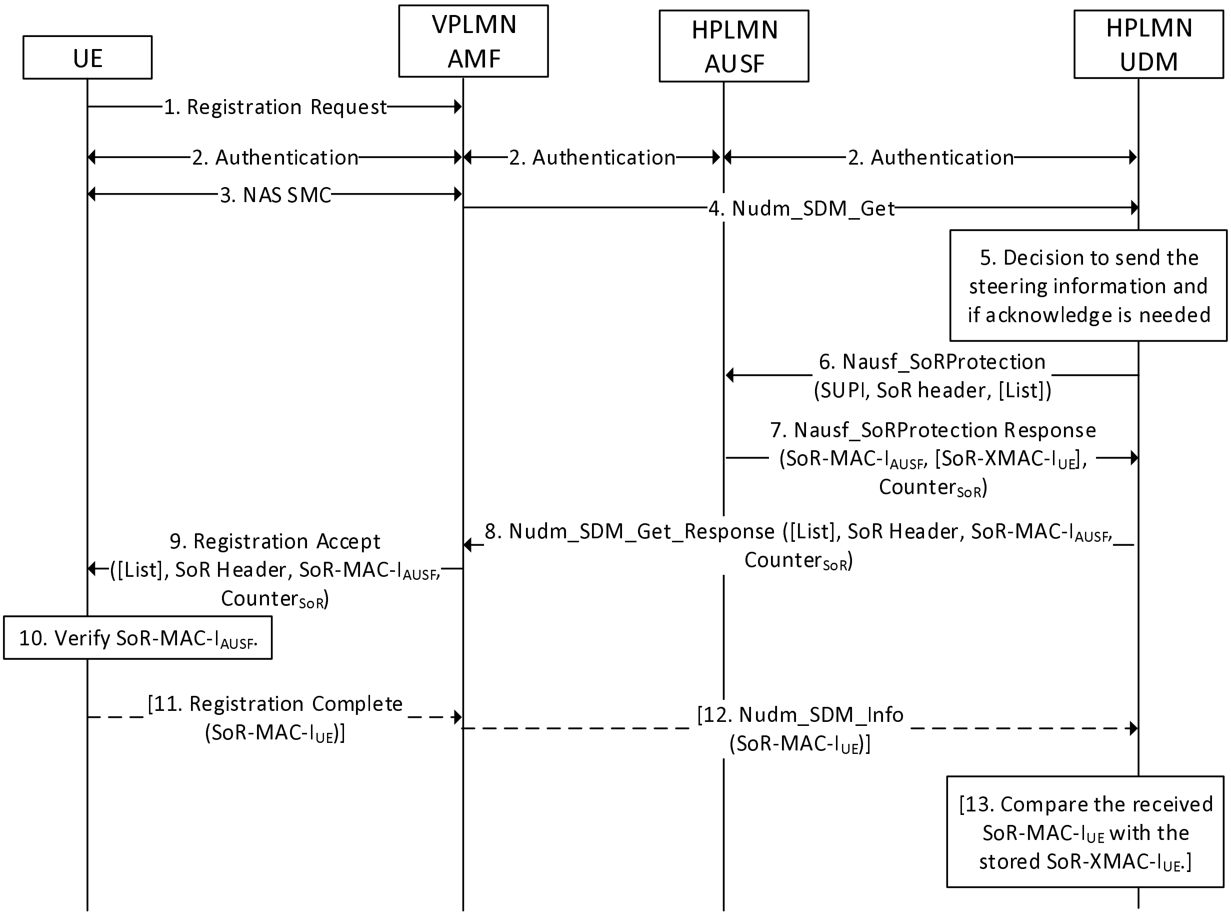
UE
VPLMN AMF
HPLMN AUSF
HPLMN UDM
1. Registration Request
2. Authentication
2. Authentication
2. Authentication
3. NAS SMC
4. Nudm_SDM_Get
5. Decision to send the steering information and if acknowledge is needed
6. Nausf_SoRProtection (SUPI, SoR header, [List])
7. Nausf_SoRProtection Response (SoR-MAC-I_AUSF, [SoR-XMAC-I_UE], Counter_SoR)
8. Nudm_SDM_Get_Response ([List], SoR Header, SoR-MAC-I_AUSF, Counter_SoR)
9. Registration Accept ([List], SoR Header, SoR-MAC-I_AUSF, Counter_SoR)
10. Verify SoR-MAC-I_AUSF.
[11. Registration Complete (SoR-MAC-I_UE)]
[12. Nudm_SDM_Info (SoR-MAC-I_UE)]
[13. Compare the received SoR-MAC-I_UE with the stored SoR-XMAC-I_UE.]

Figure 6.14.2.1-1: Procedure for providing list of preferred PLMN/access technology combinations

1) The UE initiates registration by sending Registration Request message to the VPLMN AMF.

2-3) The VPLMN AMF executes the registration procedure as defined in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]. As part of the registration procedure, the VPLMN AMF executes primary authentication of the UE and then initiates the NAS SMC procedure, after the authentication is successful.

4) The VPLMN AMF invokes Nudm_SDM_Get service operation message to the UDM to get amongst other information the Access and Mobility Subscription data for the UE (see step 14b in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]).

5) The UDM decides to send the Steering Information, and obtains the list as descirbed in TS 23.122 [53].

6-7) The UDM shall invoke Nausf_SoRProtection service operation message to the AUSF to get SoR-MAC-I$_{AUSF}$ and Counter$_{SoR}$ as specified in sub-clause 14.1.3 of this document. If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering Information List, then the UDM shall indicate in the SoR header (see TS 24.501 [35]) that it also needs the expected SoR-XMAC-I$_{UE}$, as specified in sub-clause 14.1.3 of this document.

The details of the Counter$_{SoR}$ is specified in sub-clause 6.14.2.3 of this document. In case, the Steering Information List is not available or HPLMN determines that no steering of the UE is required, then the List indication valuein the SoR header shall be set to null and list shall not be included. The inclusion of list of preferred PLMN/access technology combinations (if provided) and the SoR header in the calculation of SoR-MAC-I$_{AUSF}$ allows the UE to verify that the Steering Information List received is not tampered with or removed by the VPLMN and if the UDM requested an acknowledgement. The expected SoR-XMAC-I$_{UE}$ allows the UDM to verify that the UE received the Steering Information List.

8) The UDM responds to the Nudm_SDM_Get service operation to the VPLMN AMF, which shall include the SoR header, Steering Information List, SoR-MAC-I_{AUSF} and $Counter_{SoR}$ within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-I_{UE}.

9) The VPLMN AMF shall include the Steering Information List, the SoR-MAC-I_{AUSF}, $Counter_{SoR}$ and the SoR header to the UE in the Registration Accept message;

10) On receiving the Registration Accept message, if the USIM is configured with the indication that the UE shall receive the Steering Information List, then the UE shall calculate the SoR-MAC-I_{AUSF} in the same way as the AUSF (as specified in Annex A.17) on the received Steering information, the $Counter_{SoR}$ and the SoR header and verifies whether it matches the SoR-MAC-I_{AUSF} value received in the Registration Accept message. Based on the SoR-MAC-I_{AUSF} verification outcome, the behaviour of the UE is specified in TS 23.122 [53].

11) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering Information List has been provided by the HPLMN in step 9, then the UE shall send the Registration Complete message to the serving AMF. The UE shall generate the SoR-MAC-I_{UE} as specified in Annex A.18 and includes the generated SoR-MAC-I_{UE} in a transparent container in the Registration Complete message.

12) The AMF sends a Nudm_SDM_Info request message to the UDM. If a transparent container with the SoR-MAC-I_{UE} was received in the Registration Complete message, the AMF shall include the transparent container in the Nudm_SDM_Info request message.

13) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering Information List in step 8, then the UDM shall compare the received SoR-MAC-I_{UE} with the expected SoR-XMAC-I_{UE} that the UDM stored temporarily in step 8.

6.14.2.2 Procedure for steering of UE in VPLMN after registration

The security procedure for the steering of UE in VPLMN after registration is described below in figure 6.14.2.2-1:

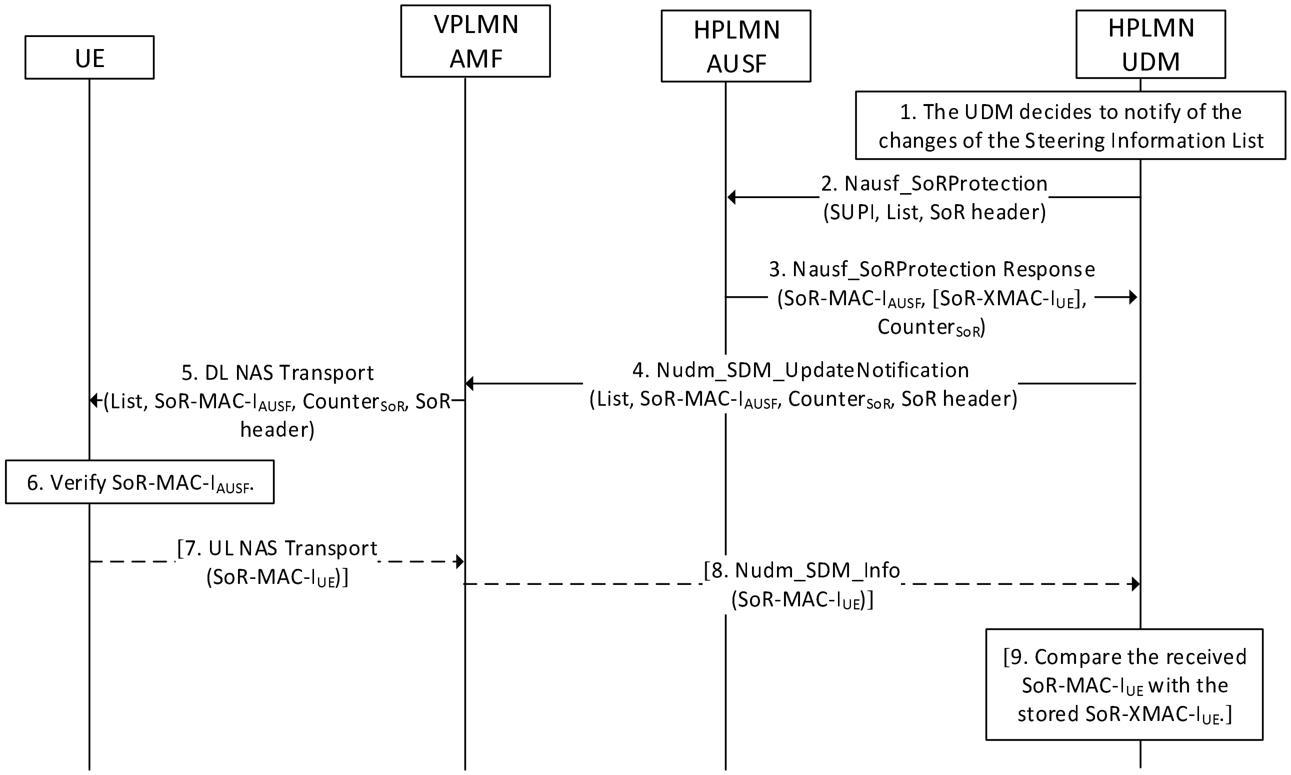
UE
VPLMN AMF
HPLMN AUSF
HPLMN UDM
1. The UDM decides to notify of the changes of the Steering Information List
2. Nausf_SoRProtection (SUPI, List, SoR header)
3. Nausf_SoRProtection Response (SoR-MAC-IAUSF, [SoR-XMAC-IUE], CounterSoR)
4. Nudm_SDM_UpdateNotification (List, SoR-MAC-IAUSF, CounterSoR, SoR header)
5. DL NAS Transport (List, SoR-MAC-IAUSF, CounterSoR, SoR header)
6. Verify SoR-MAC-IAUSF.
[7. UL NAS Transport (SoR-MAC-IUE)]
[8. Nudm_SDM_Info (SoR-MAC-IUE)]
[9. Compare the received SoR-MAC-IUE with the stored SoR-XMAC-IUE.]

Figure 6.14.2.2-1: Procedure for providing list of preferred PLMN/access technology combinations

1) The UDM decides to notify the UE of the changes to the Steering Information List by the means of invoking Nudm_SDM_UpdateNotification service operation.

2-3) The UDM shall invoke Nausf_SoRProtection service operation message by including the SoR header and Steering Information List to the AUSF to get SoR-MAC-I_{AUSF} and $Counter_{SoR}$ as specified in sub-clause 14.1.3 of this document. If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering Information List, then the UDM shall indicate in the SoR header (see TS 24.501 [35]) that it also needs the expected SoR-XMAC-I_{UE}, as specified in sub-clause 14.1.3 of this document.

The details of the $Counter_{SoR}$ is specified in sub-clause 6.14.2.3 of this document. The inclusion of Steering Information List and the acknowledge indication in the calculation of SoR-MAC-I_{AUSF} allows the UE to verify that the Steering Information List received is not tampered with or removed by the VPLMN and if the UDM requested an acknowledgement. The inclusion of these information in the calculation of the expected SoR-XMAC-I_{UE} allows the UDM to verify that the UE received the Steering Information.

4) The UDM shall invoke Nudm_SDM_UpdateNotification service operation, which contains the list of preferred PLMN/access technology combinations, SoR-MAC-I_{AUSF}, $Counter_{SoR}$ within the Access and Mobility Subscription data and the SoR header. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-I_{UE}.

5) Upon receiving the Nudm_SDM_UpdateNotification message, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the transparent container received from the UDM.

6) On receiving the DL NAS Transport message, the UE shall calculate the SoR-MAC-I_{AUSF} in the same way as the AUSF (as specified in Annex A.17) on the received Steering information, the $Counter_{SoR}$ and the SoR header and verifies whether it matches the SoR-MAC-I_{AUSF} value received in the DL NAS Transport message.

7) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering Information List has been provided by the HPLMN, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the SoR-MAC-I_{UE} as specified in Annex A.18 and includes the generated SoR-MAC-I_{UE} in a transparent container in the UL NAS Transport message.

8) The AMF shall send a Nudm_SDM_Info request message to the UDM. If a transparent container with the SoR-MAC-I_{UE} was received in the UL NAS Transport message, the AMF shall include the transparent container in the Nudm_SDM_Info request message.

9) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering Information List, then the UDM shall compare the received SoR-MAC-I_{UE} with the expected SoR-XMAC-I_{UE} that the UDM stored temporarily in step 4.

6.14.2.3 SoR Counter

The AUSF and the UE shall associate a 16-bit counter, $Counter_{SoR}$, with the key K_{AUSF}.

The UE shall initialize the $Counter_{SoR}$ to 0x00 0x00 when the K_{AUSF} is derived.

To generate the SoR-MAC-I_{AUSF}, the AUSF shall use a counter, called a $Counter_{SoR}$. The $Counter_{SoR}$ shall be incremented by the AUSF for every new computation of the SoR-MAC-I_{AUSF}. The $Counter_{SoR}$ is used as freshness input into SoR-MAC-I_{AUSF} and SoR-MAC-I_{UE} derivations as described in the Annex A.17 and Annex A.18 respectively, to mitigate the replay attack. The AUSF shall send the value of the $Counter_{SoR}$ (used to generate the SoR-MAC-I_{AUSF}) along with the SoR-MAC-I_{AUSF} to the UE. The UE shall only accept $Counter_{SoR}$ value that is greater than stored $Counter_{SoR}$ value. The UE shall store the received $Counter_{SoR,}$ only if the verification of the received SoR-MAC-I_{AUSF} is successful. The UE shall use the stored $Counter_{SoR}$ received from the HPLMN, when deriving the SoR-MAC-I_{UE} for the SoR acknowledgement.

The AUSF and the UE shall maintain the $Counter_{SoR}$ for lifetime of the K_{AUSF}.

The AUSF that supports the control plane solution for steering of roaming shall initialize the $Counter_{SoR}$ to 0x00 0x01 when the K_{AUSF} is derived. The AUSF shall set the $Counter_{SoR}$ to 0x00 0x02 after the first calculated SoR-MAC-I_{AUSF}, and monotonically increment it for each additional calculated SoR-MAC-I_{AUSF}. The SoR Counter value of 0x00 0x00 shall not be used to calculate the SoR-MAC-I_{AUSF} and SoR-MAC-I_{UE}.

The AUSF shall suspend the SoR protection service for the UE, if the $Counter_{SoR}$ associated with the K_{AUSF} of the UE, is about to wrap around. When a fresh K_{AUSF} is generated for the UE, the $Counter_{SoR}$ at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume the SoR protection service for the UE.

7 Security for non-3GPP access to the 5G core network

7.1 General

Security for non-3GPP access to the 5G Core network is achieved by a procedure using IKEv2 as defined in RFC 7296 [25] to set up one or more IPsec ESP [26] security associations. The role of IKE initiator (or client) is taken by the UE, and the role of IKE responder (or server) is taken by the N3IWF.

During this procedure, the AMF delivers a key K_{N3IWF} to the N3IWF. The AMF derives the key K_{N3IWF} from the key K_{AMF}. The key K_{N3IWF} is then used by UE and N3IWF to complete authentication within IKEv2.

7.2 Security procedures

7.2.1 Authentication for Untrusted non-3GPP Access

This clause specifies how a UE is authenticated to 5G network via an untrusted non-3GPP access network. It uses a vendor-specific EAP method called "EAP-5G", utilizing the "Expanded" EAP type and the existing 3GPP Vendor-Id, registered with IANA under the SMI Private Enterprise Code registry. The "EAP-5G" method is used between the UE and the N3IWF and is utilized for encapsulating NAS messages. If the UE needs to be authenticated by the 3GPP home network, any of the authentication methods as described in clause 6.1.3 can be used. The method is executed between the UE and AUSF as shown below.

When possible, the UE shall be authenticated by reusing the existing UE NAS security context in AMF.

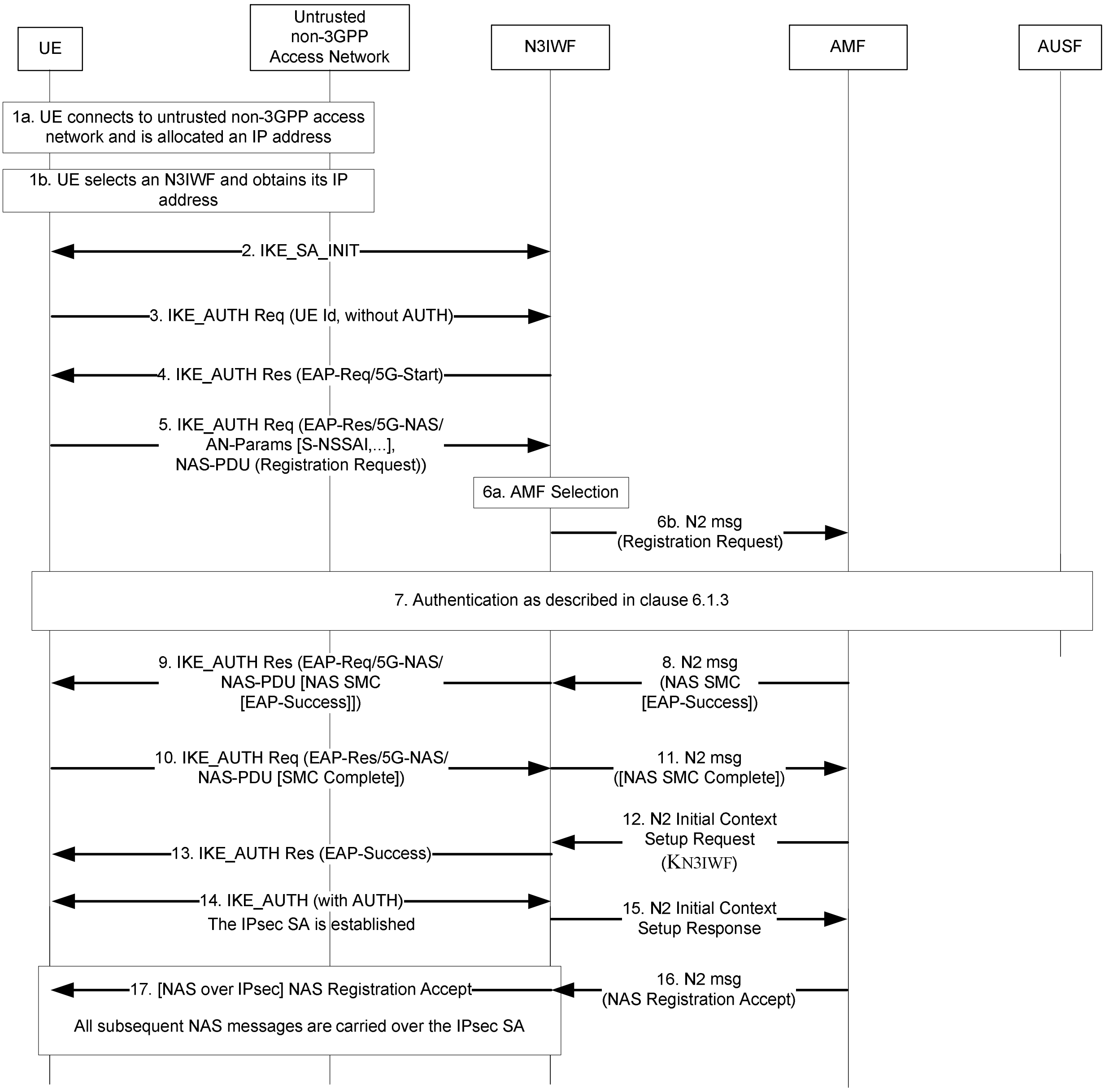
UE
Untrusted non-3GPP Access Network
N3IWF
AMF
AUSF
1a. UE connects to untrusted non-3GPP access network and is allocated an IP address
1b. UE selects an N3IWF and obtains its IP address
2. IKE_SA_INIT
3. IKE_AUTH Req (UE Id, without AUTH)
4. IKE_AUTH Res (EAP-Req/5G-Start)
5. IKE_AUTH Req (EAP-Res/5G-NAS/ AN-Params [S-NSSAI,...], NAS-PDU (Registration Request))
6a. AMF Selection
6b. N2 msg (Registration Request)
7. Authentication as described in clause 6.1.3
9. IKE_AUTH Res (EAP-Req/5G-NAS/ NAS-PDU [NAS SMC [EAP-Success]])
8. N2 msg (NAS SMC [EAP-Success])
10. IKE_AUTH Req (EAP-Res/5G-NAS/ NAS-PDU [SMC Complete])
11. N2 msg ([NAS SMC Complete])
12. N2 Initial Context Setup Request (KN3IWF)
13. IKE_AUTH Res (EAP-Success)
14. IKE_AUTH (with AUTH)
The IPsec SA is established
15. N2 Initial Context Setup Response
17. [NAS over IPsec] NAS Registration Accept
All subsequent NAS messages are carried over the IPsec SA
16. N2 msg (NAS Registration Accept)

Figure 7.2.1-1: Authentication for untrusted non-3GPP access

1. The UE connects to an untrusted non-3GPP access network with procedures outside the scope of 3GPP. When the UE decides to attach to 5GC network, the UE selects an N3IWF in a 5G PLMN, as described in TS 23.501 [2] clause 6.3.6.

2. The UE proceeds with the establishment of an IPsec Security Association (SA) with the selected N3IWF by initiating an IKE initial exchange according to RFC 7296 [25]. After step 2 all subsequent IKE messages are encrypted and integrity protected by using the IKE SA established in this step.

3. The UE shall initiate an IKE_AUTH exchange by sending an IKE_AUTH request message. The AUTH payload is not included in the IKE_AUTH request message, which indicates that the IKE_AUTH exchange shall use EAP signalling (in this case EAP-5G signalling). As per the RFC 7296 [25], in the IDi the UE shall set the ID type as ID_KEY-ID in this message and set its value equal to any random number. The UE shall not use its GUTI/SUCI/SUPI as the Id in this step. If the UE is provisioned with the N3IWF root certificate, it shall include the CERTREQ payload within the IKE_AUTH request message to request N3IWF's certificate.

4. The N3IWF responds with an IKE_AUTH response message which includes the N3IWF identity, the AUTH payload to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange) and an EAP-Request/5G-Start packet. The EAP-Request/5G-Start packet informs the UE to initiate an EAP-5G session, i.e. to start sending NAS messages encapsulated within EAP-5G packets. If the UE has sent a CERTREQ payload in step 3, the N3IWF shall also include the CERT payload including N3IWF certificate.

5. The UE shall validate the N3IWF certificate and shall confirm that the N3IWF identity matches the N3IWF selected by the UE. An absence of the certificate from the N3IWF if the UE had requested the certificate or unsuccessful identity confirmation shall result in a connection failure. The UE shall send an IKE_AUTH request which includes an EAP-Response/5G-NAS packet that contains a Registration Request message containing UE security capabilities and the SUCI. If UE is already with the 5GC over 3GPP access and there is an available security context, the UE shall integrity protect the Registration Request message and shall send the 5G-GUTI instead of SUCI. The N3IWF shall refrain from sending an EAP-Identity request. The UE may ignore an EAP Identity request or respond with the SUCI it sent in the Registration Request.

NOTE: The N3IWF does not send an EAP-Identity request because the UE includes its identity in the IKE_AUTH request in message 5. This is in line with RFC 7296 [25], clause 3.16.

6. The N3IWF shall select an AMF as specified in TS 23.501 [2], clause 6.5.3. The N3IWF forwards the Registration Request received from the UE to the AMF.

7. If the AMF receives a 5G-GUTI and the Registration is integrity protected, it may use the security context to verify the integrity protection as describe in clause 6.4.6. If integrity is verified successfully and no newer security context has been activated over the 3GPP access, then step 8 to step 11 may be skipped. If integrity is verified successfully and a newer security context has been activated over the 3GPP access then authentication may be skipped but the AMF shall activate the newer context with a NAS SMC procedure as described in step 8 and onwards.Otherwise, the AMF shall authenticate the UE.

   If the AMF decides to authenticate the UE, it shall use one of the methods from clause 6.1.3. In this case, the AMF shall send a key request to the AUSF. The AUSF may initiate an authentication procedure as specified in clause 6.1.3. Between AMF and UE, the authentication packets are encapsulated within NAS authentication messages and the NAS authentication messages are carried in N2 signalling between the AMF and N3IWF, and then are encapsulated within EAP-5G/5G-NAS packets between the N3IWF and the UE.

   In the final authentication message from the home network, the AUSF shall send the anchor key K_{SEAF} derived from K_{AUSF} to the SEAF. The SEAF shall derive the K_{AMF} from K_{SEAF} and send it to the AMF which is used by the AMF to derive NAS security keys. If EAP-AKA' is used for authentication as described in clause 6.1.3.1, then the AUSF shall include the EAP-Success. The UE also derives the anchor key K_{SEAF} and from that key it derives the K_{AMF} followed by NAS security keys. The NAS COUNTs associated with NAS connection identifier "1" are set at the UE and AMF.

8. The AMF shall send a Security Mode Command (SMC) to the UE in order to activate NAS security associated with NAS connection identifier "1". This message is first sent to N3IWF (within an N2 message). If EAP-AKA' is used for authentication, the AMF shall encapsulate the EAP-Success received from AUSF within the SMC message.

9. The N3IWF shall forward the NAS SMC to UE within an EAP-Request/5G-NAS packet.

10. The UE completes the authentication (if initiated in step 7) and creates a NAS security context or activates another one based on the received ngKSI in the NAS SMC. UE shall respond to the NAS SMC it received from the AMF based on the selected algorithms and parameters as described in clause 6.7.2. The UE shall encapsulate the NAS SMC Complete in the EAP-5G Response.

11. The N3IWF shall forward the NAS packet containing NAS SMC Complete to the AMF over the N2 interface.

12. The AMF upon reception of the NAS SMC Complete from the UE or upon success of integrity protection verification, initiates the NGAP procedure to set up the AN context. AMF shall compute the N3IWF key, K_{N3IWF}, using the uplink NAS COUNT associated with NAS connection identifier "1" as defined in Annex A.9 for the establishment of the IPsec SA between the UE and the N3IWF and shall include it in the NGAP Initial Context Setup Request sent to the N3IWF.

13. N3IWF sends an EAP-Success/EAP-5G to the UE upon reception of the NGAP Initial Context Setup Request containing the N3IWF key, KN3IWF. This completes the EAP-5G session and no further EAP-5G packets are exchanged. If the N3IWF does not receive the K_{N3IWF} from AMF, the N3IWF shall respond with an EAP-Failure

14. The IPsec SA is established between the UE and N3IWF by using the N3IWF key K_{N3IWF} that was created in the UE using the uplink NAS COUNT associated with NAS connection identifier "1" as defined in Annex A.9 and was received by N3IWF from the AMF in step 12.

15. Upon successful establishment of the IPsec SA between the UE and the N3IWF, the N3IWF shall send the NGAP Initial Context Setup Response message to the AMF.

16. When NGAP Initial Context Setup Response for the UE is received by the AMF, AMF shall send the NAS Registration Accept message for the UE over the N2 towards the N3IWF.

17. Upon receiving the NAS Registration Accept message from the AMF, the N3IWF shall forward it to the UE over the established IPsec SA. All further NAS messages between the UE and the N3IWF shall be sent over the established IPsec SA.

8 Security of interworking

8.1 General

As described in TS 23.501 [2], in order to interwork with EPC, the UE can operate in Single Registration or Dual Registration mode.

When operating in Dual Registration mode, the UE shall independently maintain and use two different security contexts, an EPS security context to interact with the Evolved Packet System and a 5G security context to interact with the 5G System. Therefore, during inter-system mobility, when the target system is EPS, the UE shall take into use the EPS security context and hence all the security mechanisms described in TS 33.401 [10] are applicable. In the other direction, i.e. when the target system is the 5GC, the UE shall take into use the 5G security context and hence all the security mechanisms described in the present document are applicable.

When operating in Single Registration mode, there are two cases depending on the support of the N26 interface between the AMF and the MME. In both cases the security mechanisms described in all the subsequent sub-clauses are applicable.

8.2 Registration procedure for mobility from EPS to 5GS over N26

During mobility from EPS to 5GS, the security handling described below shall apply.

The UE shall include the UE 5G security capability alongside the mapped 5G GUTI in the Registration Request message. The UE shall also include the 5G GUTI and the ngKSI that identify a native 5G security context if available, e.g. established during an earlier visit to 5G, and integrity protect the Registration Request using the selected security algorithms in the native 5G NAS security context. The Registration Request shall contain the TAU request integrity protected using the EPS NAS security context shared with the source MME.

NOTE: The enclosed TAU request in the Registration Request contains a complete TAU Request.

Upon receipt of the Registration Request, the AMF shall interact with the MME identified by the mapped 5G GUTI to retrieve the UE context. The AMF shall include the enclosed TAU request in the Context Request message to the MME. The MME shall verify the TAU request using the stored UE security context and if the verification is successful, the MME shall send the UE context to the AMF.

The AMF shall verify the integrity of the Registration Request message if the AMF obtained the 5G security context identified by the 5G GUTI. In case the verification succeeds then the AMF shall then dispose of any EPS security parameters received from the source MME in the Context Response message. In case the verification fails or the 5G UE context is not available then the AMF shall treat the Registration Request message as if it was unprotected. In such case, the AMF may either derive a mapped 5G security context from the EPS context received from the source MME as described in clause 8.6.2 or initiate a primary authentication procedure to create a new native 5G security context. If the AMF derives a mapped 5G security context from the EPS security context, then the ngKSI associated with the newly derived mapped 5G security context and the uplink and downlink 5G NAS COUNTs are defined and set as described in clause 8.6.2. The AMF shall use and include the ngKSI to the UE in NAS SMC procedure, for the UE to identify the EPS security context used for the derivation of a mapped 5G security context. If a mapped 5G security context is created or the native 5G security context has been changed (e.g., due to a new K_{AMF}’ derivation or NAS algorithm change), the AMF shall activate the resulting 5G security context by a NAS SMC procedure. If the AMF wants to continue to use the native 5G security context used by the UE to protect the Registration Request, the AMF may skip the NAS SMC procedure and send the Registration Accept message protected using the native 5G security context identified by the 5G-GUTI and the ngKSI included in the Registration Request message.

In case the type value in the received ngKSI in NAS SMC indicates a mapped security context, then the UE shall use the value field in the received ngKSI to identify the EPS security context from which the UE derives the mapped 5G security context as described in clause 8.6.2.

The Registration Accept message shall be protected by the new mapped 5G security context (if a mapped 5G security context was activated by NAS SMC) or by the new native 5G security context (if a new native 5G security context was activated by NAS SMC). Otherwise, the current native 5G security context shall be used. If the AMF chooses to derive an initial K_{gNB} from a new K_{AMF} key (either the mapped K_{AMF}' key or the native K_{AMF} key), then the initial K_{gNB} is derived as specified in Annex A.9 using the start value of the uplink 5G NAS COUNT protecting the NAS Security Mode Command Complete message and an access type distinguisher set to "3GPP access". If the UE receives an AS SMC message, then the UE shall derive an initial K_{gNB} from a new K_{AMF} key in the same way as the AMF.

8.3 Handover procedure from 5GS to EPS over N26

8.3.1 General

This subclause covers the case of handover from 5GS to EPS, as defined in TS 23.502 [8].

8.3.2 Procedure

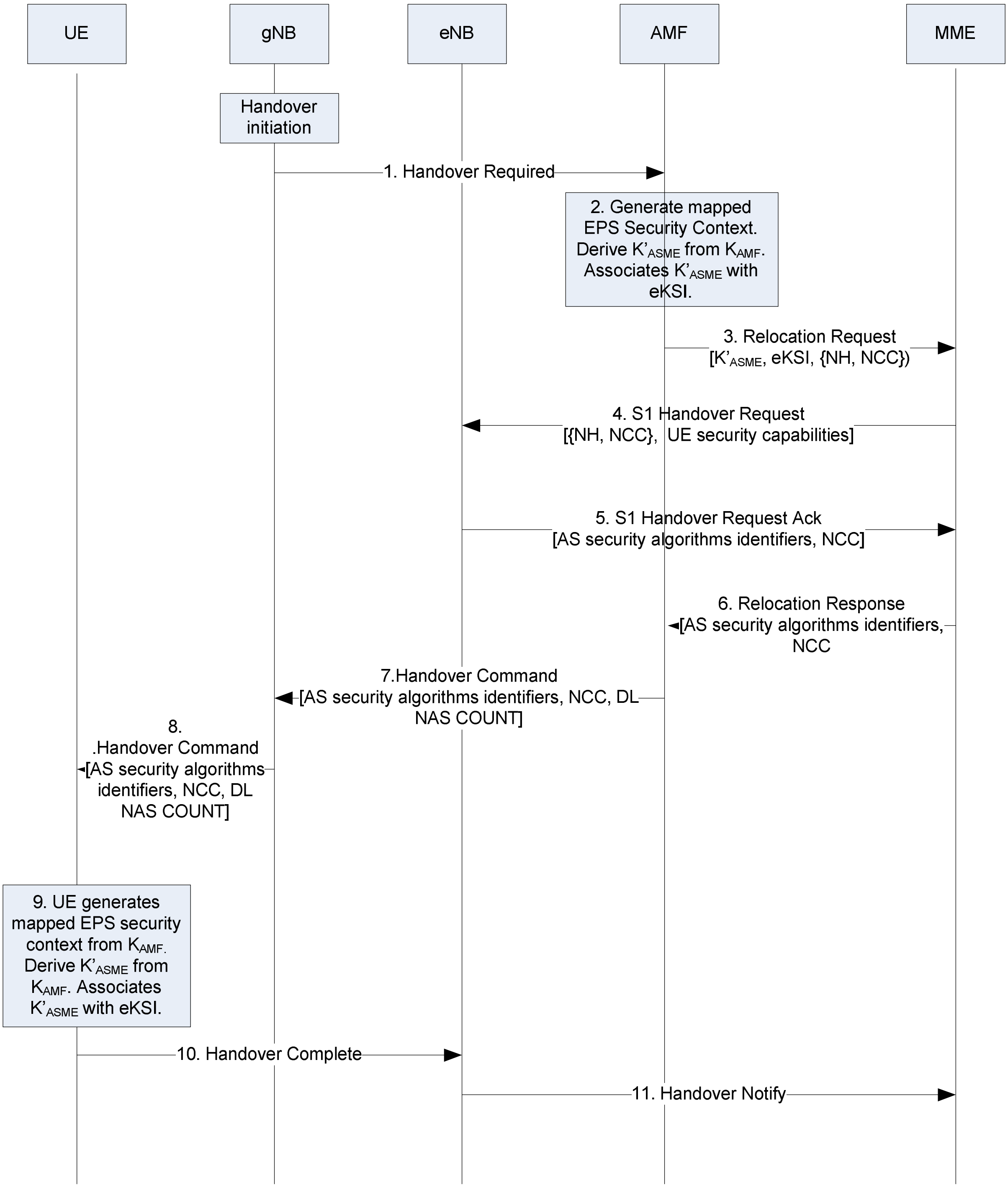
UE
gNB
eNB
AMF
MME
Handover initiation
1. Handover Required
2. Generate mapped EPS Security Context. Derive K'ASME from KAMF. Associates K'ASME with eKSI.
3. Relocation Request [K'ASME, eKSI, {NH, NCC})
4. S1 Handover Request [{NH, NCC}, UE security capabilities]
5. S1 Handover Request Ack [AS security algorithms identifiers, NCC]
6. Relocation Response [AS security algorithms identifiers, NCC
7.Handover Command [AS security algorithms identifiers, NCC, DL NAS COUNT]
8. .Handover Command [AS security algorithms identifiers, NCC, DL NAS COUNT]
9. UE generates mapped EPS security context from KAMF. Derive K'ASME from KAMF. Associates K'ASME with eKSI.
10. Handover Complete
11. Handover Notify

Figure 8.3.2-1 Handover from 5GS to EPC over N26

NOTE 1: This procedure is based on clause 4.11.1.2.1 in TS 23.502 and only includes steps and description that are relevant to security.

If the UE is initially registered and connected to the 5GC, the 5GC has a current security context for the UE. The current 5G security context may be a mapped 5G security context resulting from a previous mobility from EPC, or a native 5G security context resulting from a primary authentication with the 5GC.

1. The gNB sends a Handover Required message to the AMF, including UE’s identity and UE’s security capabilities.

2. When the source AMF performs a handover procedure to the EPC, after checking the UE's access rights and security capabilities, the source AMF shall prepare a UE context including a mapped EPS security context for the target MME. To construct the mapped EPS security context, the source AMF shall derive a K’$_{ASME}$ using the

K_{AMF} key and the current downlink 5G NAS COUNT of the current 5G security context as described in clause 8.6.1 and then increments its stored downlink 5G NAS COUNT value by one.

The source AMF shall select the EPS NAS algorithms identifiers (it has stored) to be used in the target MME at interworking handover to EPS, for encryption and integrity protection.

NOTE 2: A legacy target MME is expecting to receive the selected EPS NAS algorithms identifiers over N26 from the source AMF as the target MME believes the source AMF is another MME. The source AMF has therefore provisioned the EPS NAS security algorithms identifiers to be used at interworking handover to EPS to the UE in the 5G NAS SMC in 5G access as described in clause 6.7.2. The target MME could re-select different EPS NAS algorithms though to be used with the UE by running a NAS SMC in the following Tracking Area Update procedure.

The uplink and downlink EPS NAS COUNT associated with the newly derived K_{ASME}' key are set to the values as described in clause 8.6.1. The eKSI for the newly derived K_{ASME}' key is defined as described in clause 8.6.1.

The source AMF shall also derive the initial K_{eNB} key from the K_{ASME}' key and the uplink NAS COUNT as specified in Annex A.3 of TS 33.401 [10] using 2^{32}-1 as the value of the uplink NAS COUNT parameter.

NOTE 3: The source AMF and the UE only uses the 2^{32}-1 as the value of the uplink NAS COUNT for the purpose of deriving K_{eNB} and do not actually set the uplink NAS COUNT to 2^{32}-1. The reason for choosing such a value not in the normal NAS COUNT range, i.e., [0, 2^{24}-1] is to avoid any possibility that the value may be used to derive the same K_{eNB} again.

The source AMF subsequently derives NH two times as specified in clause A.4 of TS 33.401 [10]. The {NH, NCC=2} pair is provided to the target MME as a part of UE security context in the Relocation Request message.

3. The source AMF shall transfer the UE security context (including new K_{ASME}', eKSI, uplink and downlink EPS NAS COUNT's, UE EPS security capabilities, selected EPS NAS algorithms identifiers) to the target MME in the Relocation Request message. The UE NR security capabilities may be sent by the source AMF as well.

4. When the target MME receives Relocation Request message from source AMF, then the target MME shall derive EPS NAS keys (i.e., K_{NASenc} and K_{NASint}) from the received K_{ASME}' key with the received EPS NAS security algorithm identifiers as input, to be used in EPC as described in Annex A.7 in TS 33.401 [10]. The target MME needs to include the {NH, NCC=2} pair and the UE security capabilities in the S1 HANDOVER REQUEST message to the target LTE eNB. The UE security capabilities include the UE EPS security capabilities received from the source AMF.

5. Upon receipt of the S1 HANDOVER REQUEST from the target MME, the target LTE eNB shall compute the KeNB to be used with the UE and proceed as described in clause 7.2.8.4.3 in TS 33.401[10].

6. The target MME shall include the target to source transparent container received from the target LTE eNB in the Relocation Response message sent to the source AMF.

7. The source AMF shall include the target to source transparent container and the 4 LSB of the downlink NAS COUNT value used in K'_{ASME} derivation in step 2, in the Handover command sent to the source gNB.

8. The source gNB shall include the target to source transparent container and the 4 LSB of the downlink NAS COUNT value in the Handover command sent to the UE.

   Upon the reception of the Handover Command message, the UE shall estimate the downlink NAS COUNT value using the received 4 LSB of the downlink NAS COUNT value and its stored downlink NAS COUNT value. The UE shall ensure that the estimated downlink NAS COUNT value is greater than the stored downlink NAS COUNT value. Then, the UE shall derive the mapped EPS security context, i.e. derive K_{ASME}' from K_{AMF} as described in clause 8.6.1 using the estimated downlink 5G NAS COUNT value. After the derivation the UE shall set the downlink NAS COUNT value in the 5G NAS security context to the received downlink NAS COUNT value.

9. The eKSI for the newly derived K_{ASME}' key is defined as described in clause 8.6.1. The UE shall also derive the EPS NAS keys (i.e. K_{NASenc} and K_{NASint}) as the MME did in step 4 using the EPS NAS security algorithms identifiers stored in the ME and provisioned by the AMF to the UE in 5G NAS SMC in earlier 5G access. The UE shall also derive the initial K_{eNB} from the K_{ASME}' and the uplink NAS COUNT as specified in Annex A.3 of TS 33.401 [10] using 2^{32}-1 as the value of the uplink NAS COUNT parameter.

The UE shall also derive the {NH, NCC=2} pair as described in A.4 of TS 33.401 [10] and further derive the K_{eNB} to be used with the UE by performing the key derivation defined in Annex A.5 in TS 33.401[10]. The UE shall derive the AS RRC keys and the AS UP keys based on the K_{eNB} and the received AS EPS security algorithms identifiers selected by the target eNB as described in Annex A.7 in TS 33.401 [10]. The uplink and downlink EPS NAS COUNT associated with the derived EPS NAS keys are set to the values as described in clause 8.6.1. The UE shall immediately take into use the newly created mapped EPS security context, both for NAS and AS communication.

8.4 Handover from EPS to 5GS over N26

8.4.1 General

This clause covers the case of handoff from EPS to 5GS, as defined in TS 23.502 [8].

8.4.2 Procedure

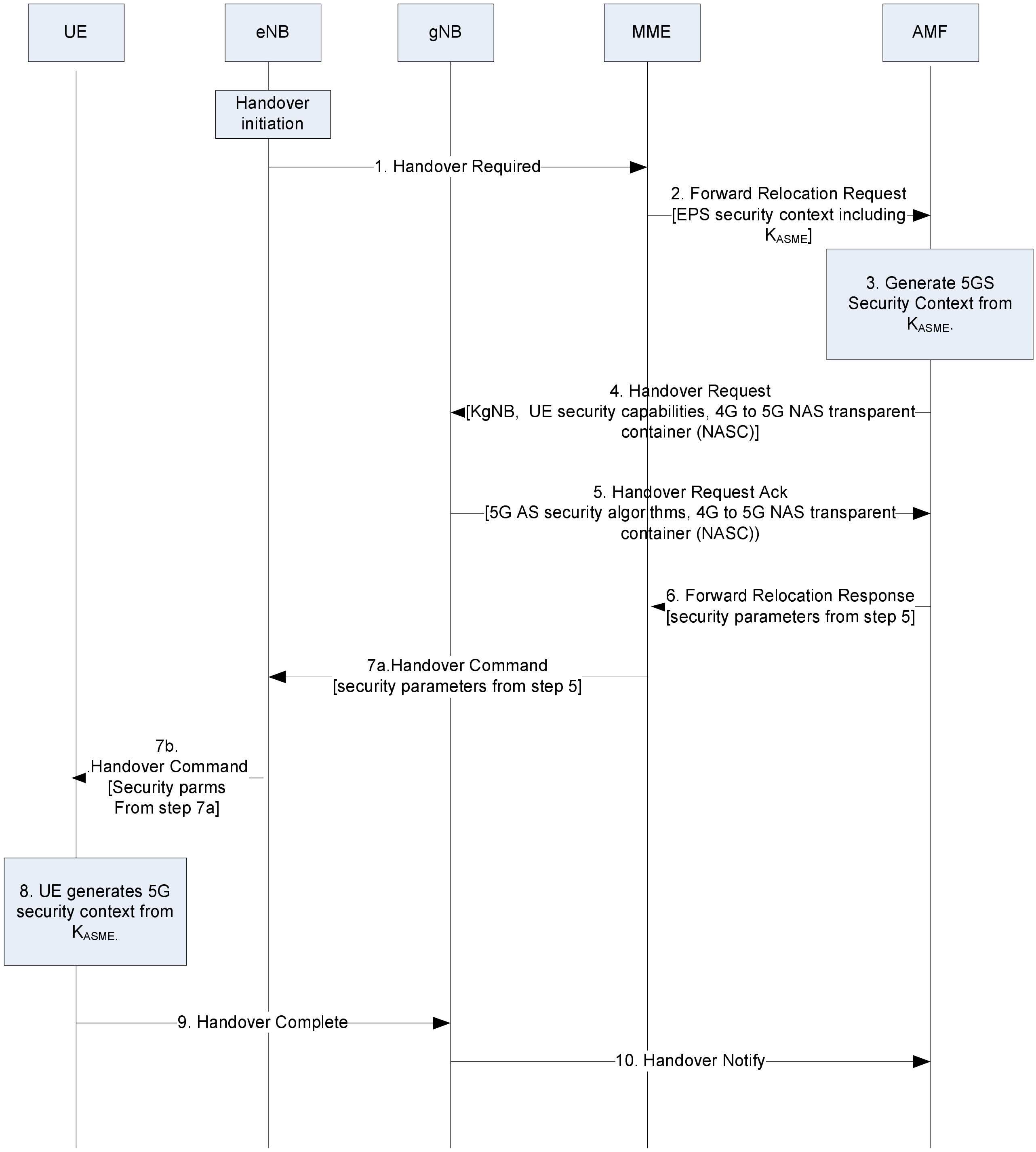
UE
eNB
gNB
MME
AMF
Handover initiation
1. Handover Required
2. Forward Relocation Request [EPS security context including K_{ASME}]
3. Generate 5GS Security Context from K_{ASME}.
4. Handover Request [KgNB, UE security capabilities, 4G to 5G NAS transparent container (NASC)]
5. Handover Request Ack [5G AS security algorithms, 4G to 5G NAS transparent container (NASC))
6. Forward Relocation Response [security parameters from step 5]
7a.Handover Command [security parameters from step 5]
7b. .Handover Command [Security parms From step 7a]
8. UE generates 5G security context from K_{ASME}.
9. Handover Complete
10. Handover Notify

Figure 8.4.2-1: Handover from EPS to 5GS over N26

NOTE 1: This procedure is based on clause 4.11.1.2.2 in TS 23.502 [8] and only includes steps and description that are relevant to security.

As the UE is connected to the EPS, the source MME has a current EPS security context for the UE. The current EPS security context may be a mapped EPS security context resulting from a previous mobility from 5GC, or a native EPS security context resulting from a primary authentication with the EPS.

1. The source eNB sends a Handover Required message to the source MME, including UE's identity and UE's security capabilities.

NOTE 2: The source MME checks whether the UE's security capabilities and access rights are valid in order to decide whether it can initiate handover to 5GS.

2. The source MME selects the target AMF and sends a Forward Relocation Request to the selected target AMF. The source MME includes UE's EPS security context including K_{ASME}, eKSI, UE EPS security capabilities, selected EPS NAS algorithm identifiers, uplink and downlink EPS NAS COUNTs, {NH, NCC} pair, in this message. If the source MME has the UE NR security capabilities stored, then it will forward the UE NR security capabilities as well to the target AMF.

3. The target AMF shall construct a mapped 5G security context from the EPS security context received from the source MME. The target AMF shall derive a mapped K_{AMF} key from the received K_{ASME} and the NH value in the EPS security context received from the source MME as described in clause 8.6.2.

   If the target AMF receives the UE 5G security capabilities, then the target AMF shall select the 5G NAS security algorithms (to be used in the target AMF for encryption and integrity protection) which have the highest priority from its configured list.

   If the target AMF does not receive the UE 5G security capabilities from the source MME, then the target AMF shall assume that the following default set of 5G security algorithms are supported by the UE (and shall set the UE 5G security capabilities in the mapped 5G NAS security context according to this default set):

   a. NEA0, 128-NEA1 and 128-NEA2 for NAS signalling ciphering, RRC signalling ciphering and UP ciphering;

   b. 128-NIA1 and 128-NIA2 for NAS signalling integrity protection, RRC signalling integrity protection and UP integrity protection.

   The target AMF then derives the complete mapped 5G security context. The target AMF shall derive the 5G NAS keys (i.e., K_{NASenc} and K_{NASint}) from the new K_{AMF}' with the selected 5G NAS security algorithm identifiers as input, to be used in AMF as described in clause A.8. The uplink and downlink 5G NAS COUNTs associated with the derived 5G NAS keys are set to the value as described in clause 8.6. 2. The ngKSI for the newly derived K_{AMF}' key is defined such as the value field is taken from the eKSI of the K_{ASME} key (i.e. included in the received EPS security context) and the type field is set to indicate a mapped security context. The target AMF shall also derive the initial K_{gNB} from the mapped K_{AMF}' key as specified in Annex A.9.

   The target AMF associates this mapped 5G Security context with ngKSI.

NOTE 3: The target AMF derives a K_{gNB} using the K_{AMF} instead of using the {NH, NCC} pair received from the MME.

   The target AMF shall create a NAS Container to signal the necessary security parameters to the UE. The NAS Container shall include a NAS MAC, the selected 5G NAS security algorithms, the ngKSI associated with the derived K_{AMF}' and the NCC value associated with the NH parameter used in the derivation of the K_{AMF}'. The target AMF shall calculate the NAS MAC as described in clause 6.9.2.3.3. with the COUNT parameter set to the maximal value of 2^{32}-1.

4. The target AMF requests the target gNB to establish the bearer(s) by sending the Handover Request message.

   The target AMF sends the NAS Container created in step 3 along with, the derived K_{gNB} and the UE security capabilities in the Handover Request message to the target gNB.

5. The target gNB shall selects the 5G AS security algorithms from the list in the UE security capabilities

   The target gNB shall derive the 5G AS security context, by deriving the 5G AS keys (K_{RRCint}, K_{RRCenc}, K_{UPint}, and K_{UPenc}) from the K_{gNB} and the selected 5G AS security algorithm identifiers as described in Annex A.8.

   The target gNB sends a Handover Request Ack message to the target AMF. It includes the selected 5G AS algorithms and the NAS Containerreceived from the target AMF (in step 4) in the Target to Source Container, and includes it in the Handover Request Ack message.

6. The target AMF sends the Forward Relocation Response message to the source MME. The required security parameters obtained from gNB in step 5 as the Target to Source Container are forwarded to the source MME.

7. The source MME sends the Handover Command to the source eNB. The source eNB commands the UE to handover to the target 5G network by sending the Handover Command. This message includes all the security related parameters in the NAS Containerobtained from the target AMF in step 6.

8. The UE derives a mapped K_{AMF}' key from the K_{ASME} in the same way the AMF did in step 3. It shall also derive the 5G NAS keys and K_{gNB} as the AMF did in step 3. It associates this mapped 5G security context with the ngKSI included in the NAS Container.

NOTE 4: Void.

The mapped 5G security context shall become the current 5G security context.

9. The UE sends the Handover Complete message to the target gNB. This shall be ciphered and integrity protected by the AS keys in the current 5G security context.

10. The target gNB notifies the target AMF with a Handover Notify message.

If the UE has a native 5G security context established during the previous visit to 5GS, then the UE shall provide the associated the 5G GUTI as an additional GUTI in the Registration Request following the handover procedure. The AMF shall retrieve the native security context using the 5G GUTI. The AMF may activate the native K_{AMF} by performing a NAS SMC procedure. If the handover is not completed successfully, the new mapped 5G security context cannot be used in the future. In this case, the AMF shall delete the new mapped 5G security context.

8.5 Idle mode mobility from 5GS to EPS over N26

8.5.1 General

This clause covers the case of idle mode mobility from 5GS to EPS, as defined in TS 23.502 [8].

8.5.2 Procedure

NOTE: This procedure is based on clause 4.11.1.3.2 in TS 23.502 [8] and only includes steps and descriptions that are relevant to security.

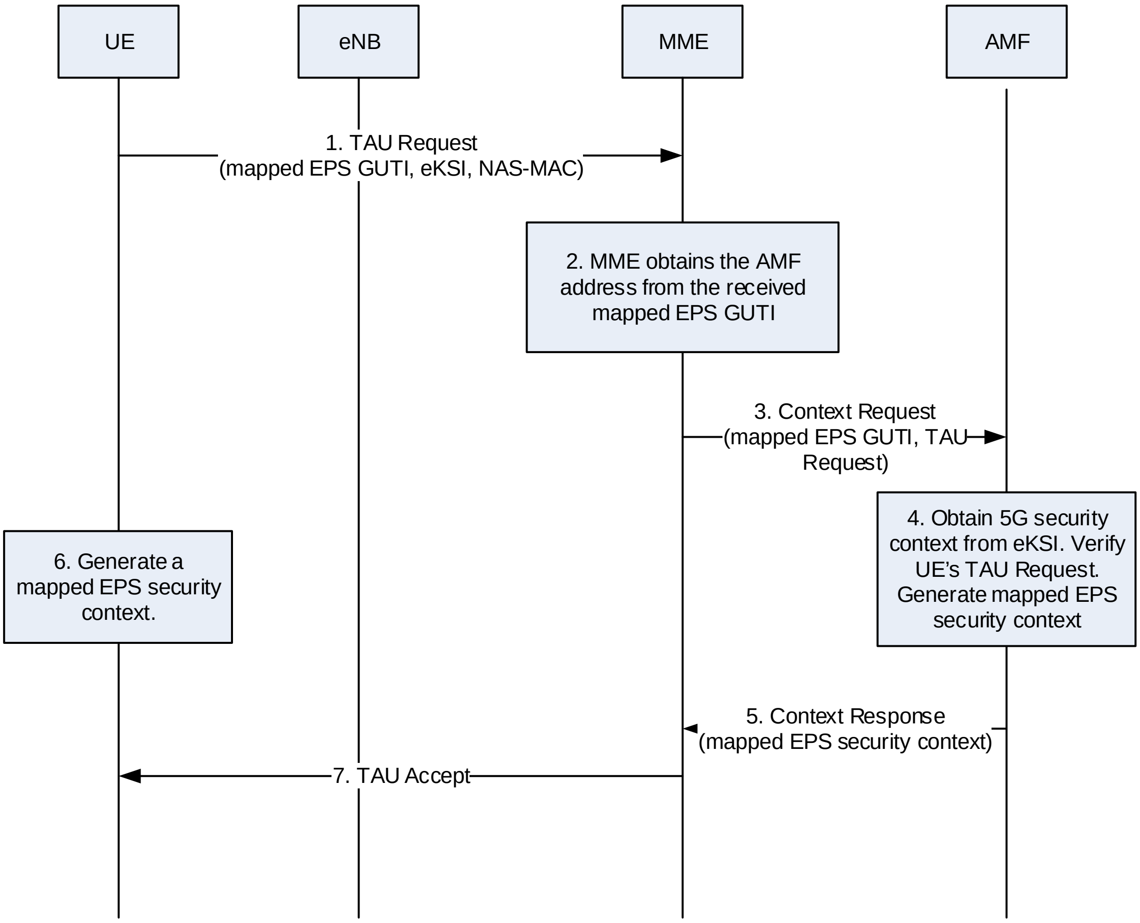
UE
eNB
MME
AMF
1. TAU Request
(mapped EPS GUTI, eKSI, NAS-MAC)
2. MME obtains the AMF address from the received mapped EPS GUTI
3. Context Request
(mapped EPS GUTI, TAU Request)
4. Obtain 5G security context from eKSI. Verify UE's TAU Request. Generate mapped EPS security context
6. Generate a mapped EPS security context.
5. Context Response
(mapped EPS security context)
7. TAU Accept

Figure 8.5.2-1: Idle mode mobility from 5G to 4G

1. The UE initiates the TAU procedure by sending a TAU Request to the MME with a mapped EPS GUTI derived from the 5G GUTI and its EPS security capabilities. The mapped EPS GUTI contains the information of the AMF that has the latest UE context in the 5G network.

   The UE integrity protects the TAU Request message using the current 5G NAS security context identified by the 5G GUTI used to derive the mapped EPS GUTI. More precisely, the UE shall compute the NAS MAC for the TAU request as it is done for a 5G NAS message over a 3GPP access. Consequently, this results in an increase of the stored NAS Uplink COUNT value in the NAS COUNT pair associated with the 3GPP access. The corresponding ngKSI value of the 5G Security context is included in the eKSI parameter of the TAU Request message.

2. Upon receipt of the TAU Request, the MME obtains the AMF address from the mapped EPS GUTI value.

3. The MME forwards the complete TAU Request message including the eKSI, NAS-MAC and mapped EPS GUTI in the Context Request message.

4. The AMF shall use the eKSI value field to identify the 5G NAS security context and use it to verify the TAU Request message as if it was a 5G NAS message received over 3GPP access.

5. If the verification is successful, the AMF shall derive a mapped EPS NAS security context as described in clause 8.6.1. The AMF shall set the EPS NAS algorithms to the ones indicated earlier to the UE in a NAS SMC as described in clause 6.7.2.

   The AMF shall include the mapped EPS NAS security context in the Context Response message it sends to the MME. The AMF shall never transfer 5G security parameters to an entity outside the 5G system.

6. The UE shall derive a mapped EPS NAS security context as described in clause 8.6.1. The UE shall select the EPS algorithms using the ones received in an earlier NAS SMC from the AMF as described in clause 6.7.2. The UE shall immediately activate the mapped EPS security context and be ready to use it for the processing of the TAU Accept message in step 7.

7. The MME completes the procedure with a TAU Accept message.

8.6 Mapping of security contexts

8.6.1 Mapping of a 5G security context to an EPS security context

The derivation of a mapped EPS security context from a 5G security context is done as described below:

- The K_{ASME}' key, taken as the K_{ASME}, shall be derived from the K_{AMF} using the current 5G NAS Uplink COUNT value in idle mode mobility or the 5G NAS Downlink COUNT value in handovers as described in Annex A.14.

- The eKSI for the newly derived K_{ASME} key shall be defined such as the value field is taken from the ngKSI and the type field is set to indicate a mapped security context.

- The EPS NAS COUNT values in the mapped context shall be set to 0.

- The selected EPS NAS algorithms shall be set to the EPS algorithms signalled to the UE by the AMF during an early authentication procedure followed by a NAS SMC as described in clause 6.7.2.

NOTE: Whenever an algorithm change is required, the target MME initiates an NAS SMC to select other algorithms as described in TS 33.401 [10].

8.6.2 Mapping of an EPS security context to a 5G security context

The derivation of a mapped 5G security context from an EPS security is done as described below.

- The K_{AMF}' key, taken as the K_{AMF}, shall be derived from the K_{ASME} using the current EPS NAS Uplink COUNT in idle mode mobility or the NH value in handovers as described in clause A.15.

- The ngKSI for the newly derived K_{AMF} key shall be defined such as the value field is taken from the eKSI and the type field is set to indicate a mapped security context.

- The 5G NAS COUNT values in the mapped 5G security context shall be set to 0.

NOTE: The selection of the 5G NAS algorithms is performed by the AMF and signalled to the UE either in the NAS Container during handovers as described in clause 8.4, or in a NAS SMC during idle mode mobility as described in clause 8.2.

8.7 Interworking without N26 interface in single-registration mode

When the UE supports single-registration mode and network supports interworking procedure without N26 interface:

- For mobility from 5GC to EPC, if the UE has a current EPS NAS security context, the UE shall start using the EPS security context as defined in TS 33.401 [10].

- For mobility from EPC to 5GC, if the UE has a current 5G NAS security context, the UE shall start using the 5G NAS security context as defined in the present document.

9 Security procedures for non-service based interfaces

9.1 General

9.1.1 Use of NDS/IP

The protection of IP based interfaces for 5GC and 5G-AN according to NDS/IP is specified in TS 33.210 [3]. Traffic on interfaces carrying control plane signalling can be both integrity and confidentiality protected according to NDS/IP.

NOTE 1: Void.

9.1.2 Implementation requirements

IPsec ESP implementation shall be done according to RFC 4303 [4] as profiled by TS 33.210 [3]. For IPsec implementation, tunnel mode is mandatory to support while transport mode is optional.

IKEv2 certificate-based authentication implementation shall be done according to TS 33.310 [5]. The certificates shall be supported according to the profile described by TS 33.310 [5]. IKEv2 shall be supported conforming to the IKEv2 profile described in TS 33.310 [5].

9.1.3 QoS considerations

If the sender of IPsec traffic uses DiffServ Code Points (DSCPs) to distinguish different QoS classes, either by copying DSCP from the inner IP header or directly setting the encapsulating IP header's DSCP, the resulting traffic may be reordered to the point where the receiving node's anti-replay check discards the packet. If different DSCPs are used on the encapsulating IP header, then to avoid packet discard under one IKE SA and with the same set of traffic selectors, distinct Child-SAs should be established for each of the traffic classes (using the DSCPs as classifiers) as specified in RFC 4301 [6].

9.2 Security mechanisms for the N2 interface

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in TS 33.310 [17], Annex E.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect N2 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

9.3 Security requirements and procedures on N3

N3 is the reference point between the 5G-AN and UPF. It is used to carry user plane data from the UE to the UPF.

The transport of user data over N3 shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the N3 reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec is mandatory to implement on the gNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

NOTE: The use of cryptographic solutions to protect N3 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

QoS related aspects are further described in sub-clause 9.1.2 of the present document.

9.4 Security mechanismsfor the Xn interface

Xn is the interface connecting 5G-RAN nodes. It consists of Xn-C and Xn-U. Xn-C is used to carry signalling and Xn-U user plane data.

The transport of control plane data and user data over Xn shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec shall be supported on the gN

In addition to IPsec, for the Xn-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in TS 33.310 [17], Annex E.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.B.

NOTE 2: The use of cryptographic solutions to protect Xn is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

9.5 Interfaces based on DIAMETER or GTP

This clause applies to all DIAMETER or GTP-based interfaces between the 5G Core and other network entities that are not part of the 5G System. These includes the Rx interface between the PCF and the IMS System and the N26 interface between the AMF and the MME.

The protection of these interfaces shall be supported according to NDS/IP as specified in TS 33.210 [3].

9.5.1 Void

9.6 Void

9.7 Void

9.8 Security mechanisms for protection of the gNB internal interfaces

9.8.1 General

The following clause applies to the gNB supporting the split architecture.

9.8.2 Security mechanisms for the F1 interface

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane.

In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in TS 33.310 [17], Annex E.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect F1 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

NOTE 3: The security considerations for DTLS over SCTP are documented in RFC 6083[58].

9.8.3 Security mechanisms for the E1 interface

The E1 interface connects the gNB-CU-CP to the gNB-CU-UP. It is only used for the transport of signalling data.

In order to protect the traffic on the E1 interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in TS 33.310 [17], Annex E.

IPsec is mandatory to support on the gNB-CU-UP and the gNB-CU-CP. Observe that on both the gNB-CU-CP and the gNB-CU-UP sides, a SEG may be used to terminate the IPsec tunnel.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect E1 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

9.9 Security mechanisms for non-SBA interfaces internal to the 5GC

Interfaces internal to the 5G Core can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, confidentiality and integrity protection is required.

For the protection of the non-SBA 5GC internal interfaces, such as N4 and N9, NDS/IP shall be used as specified in [3], unless security is provided by other means, e.g. physical security.

10 Security aspects of IMS emergency session handling

10.1 General

This clause addresses security procedures for IMS emergency session handling.

10.2 Security procedures and their applicability

10.2.1 Authenticated IMS Emergency Sessions

10.2.1.1 General

Authenticated emergency services are provided to UEs in the following scenarios:

a) A UE in RM-DEREGISTERED state requests IMS Emergency services

In this scenario, the UE has a valid subscription and is authenticated when it registers with the network.

b) A UE in RM-REGISTERED state initiates a PDU Session request to setup an IMS Emergency Session

In this scenario, the UE is already registered with the network and share a security context with the AMF. The UE initiates a session management message to setup a new bearer for emergency services. The request for emergency services is sent protected by the current security context. The AMF may decide to re-authenticate the UE.

If there is a redirection of the UE to EUTRAN for IMS Emergency services, the redirect command from the gNB to the UE shall be protected by the UE's AS security context. The AMF shall send the 'NG AP UE Initial Context setup' message to enable the AS security context set up.

10.2.1.2 UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services

The UE shall first initiate a normal initial registration procedure to register with the 5G network. Upon successful normal registration, the UE initiates the UE requested PDU session establishment procedure to establish a PDU Session to receive emergency services as specified in TS 23.502 [8].

At the time of registration, the security mode control procedure shall be applied to authenticate the UE and setup NAS and AS security. Thus, integrity protection (and optionally ciphering) shall be applied to the emergency bearers as for normal bearers.

If authentication fails for any reason, it shall be treated the same way as any registration. Once the IMS Emergency Session is in progress with NAS and AS integrity protection (and optionally ciphering) applied, failure of integrity checking or ciphering (for both NAS and AS) is an unusual circumstance and shall be treated as in the case of a normal bearer.

10.2.1.3 UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services

The UE initiates the UE requested PDU session establishment procedure to receive emergency services as specified in clause 5.16.4 in TS 23.501 [2]. Since the UE already has a current 5G security context when it attempts to set up an IMS Emergency Session, the UE shall use this 5G security context to protect NAS, RRC and UP traffic. If the AMF successfully validates the PDU Session request for emergency bearer services using the current 5G security context, the AMF may accept this request and setup a PDU session.

If the AMF attempts to re-authenticate the UE after receiving a correctly integrity protected request for emergency bearer services based on the current NAS security context and the authentication failed and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF shall proceed as for the initial registration error scenario as described in clause 6.1.3.

If the AMF attempts to re-authenticate the UE after receiving a correctly integrity protected request for emergency bearer services based on the current NAS security context and the authentication failed and the serving network policy allows unauthenticated IMS Emergency Sessions, then the set up of the emergency bearers shall proceed in one of the two ways:

a) The set-up proceeds according to clause 10.2.2. In this case, there is no need for the UE to re-attach, and the AMF requests the use of the NULL ciphering and integrity algorithms in the same way as described in clause 10.2.2.2 for the case of Emergency registration by UEs in limited service state.

NOTE 1: If the authentication failure is detected in the AMF then the UE is not aware of the failure in the AMF, but still needs to be prepared, according to the conditions specified in TS 24.301, to accept a NAS SMC from the AMF requesting the use of the NULL ciphering and integrity algorithms.

NOTE 2: Regardless of if the authentication failed in the UE or in the AMF, the AMF can assume that the UE will accept that NULL integrity and ciphering algorithms are selected in the security mode control procedure

b) The UE and the AMF continues using the current security context as described below for the case when primary authentication is executed while setting up a PDU session for emergency services.

If primary authentication procedure is executed while setting up a PDU Session for emergency bearer services, the AMF and UE shall behave as follows:

UE behavior:

- Upon successful authentication verification in the UE, the UE shall continue using the current security context.

- Alternatively, upon authentication verification failure in the UE, the UE shall send a failure message to the AMF and shall continue using the current security context. If the UE receives a NAS security mode command selecting NULL integrity and ciphering algorithms, the UE shall accept this as long as the IMS Emergency session progresses.

AMF behavior:

- If the serving network policy allows unauthenticated IMS Emergency Sessions, the AMF, after the unsuccessful authentication verification of the UE, should not send a reject an Authentication Reject message and continue using the current security context with the UE.

- After receiving both, the EC Indication and the failure message from the UE, the AMF shall continue using the current security context with the UE for establishing an emergency bearer.

10.2.2 Unauthenticated IMS Emergency Sessions

10.2.2.1 General

There are many scenarios when an unauthenticated Emergency Session may be established without the network having to authenticate the UE or apply ciphering or integrity protection for either AS or NAS. For example:

a) UEs that are in Limited service state UEs, as specified in clause 3.5 in TS 23.122

b) UEs that have valid subscription but SN cannot complete authentication because of network failure or other reasons

TS 23.401 clause 4.3.12.1 identifies four possible network behaviours of emergency bearer support. Amongst these, the following two cases are applicable for unauthenticated emergency sessions:

a. **IMSI required, authentication optional**. These UEs shall have a SUPI. If authentication fails, the UE is granted access and the unauthenticated SUPI retained in the network for recording purposes. The PEI is used in the network as the UE identifier. PEI only UEs will be rejected (e.g. UICCless UEs).

b. **All UEs are allowed**. Along with authenticated UEs, this includes UEs with a SUPI that cannot be authenticated and UEs with only an PEI. If an unauthenticated SUPI is provided by the UE, the unauthenticated SUPI is retained in the network for recording purposes. The PEI is used in the network to identify the UE.

The network policy is configured to one of the above, and accordingly determine how emergency requests from the UE are treated.

If the ME receives a NAS SMC selecting NIA0 (NULL integrity) for integrity protection, and NEA0 (NULL ciphering) for encryption protection, then:

- the ME shall mark any stored native 5G NAS security context on the USIM /non-volatile ME memory as invalid; and

- the ME shall not update the USIM/non-volatile ME memory with the current 5G NAS security context.

These two rules override all other rules regarding updating the 5G NAS security context on the USIM/non-volatile ME memory, in the present document.

If NIA0 is used, and the NAS COUNT values wrap around, and a new K_{AMF} has not been established before the NAS COUNT wrap around, the NAS connection shall be kept.

NOTE: For unauthenticated IMS emergency sessions, NIA0, i.e., null integrity algorithm, is used for integrity protection. Additionally, as the NAS COUNT values can wrap around, the initialization of the NAS COUNT values are not crucial. Uplink and downlink NAS COUNT are incremented for NAS message that use NIA0, as for any other NAS messages.

A UE without a valid 5G subscription shall at an IRAT handover to 5G, when an IMS Emergency Service is active, be considered by the AMF to be unauthenticated. In such a scenario, EIA0 shall be used in 5G after handover if the target network policy allows unauthenticated IMS Emergency Sessions.

A handover from 5G to another RAT, of an unauthenticated IMS Emergency Session, shall result in an unauthenticated IMS Emergency Session in the other RAT.

10.2.2.2 UE sets up an IMS Emergency session with emergency registration

UEs that are in limited service state (LSM) request emergency services by initiating the Registration procedure with the indication that the registration is to receive emergency services, referred to as Emergency Registration.

UEs that had earlier registered for normal services but now cannot be authenticated by the serving network, shall initiate Emergency Registration procedure to request emergency services.

It shall be possible to configure whether the network allows or rejects an emergency registration request and whether it allows unauthenticated UEs to establish bearers for unauthenticated IMS emergency sessions or not.

The AMF may attempt to authenticate the UE after receiving the emergency registration request.

If authentication failed in the UE during an emergency registration request, the UE shall wait for a NAS SMC command to set up an unauthenticated emergency bearer.

If authentication failed in the serving network and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF shall proceed as with the normal initial registration requests. The AMF shall reject the unauthenticated emergency bearer setup request from the UE.

If authentication failed in the serving network and if the serving network policy allow unauthenticated IMS Emergency Sessions, then the AMF shall support unauthenticated emergency bearer setup and the behaviours of the UE and the AMF are as described below.

a) UE behaviour:

After sending Emergency Registration request to the serving network the UE shall know of its own intent to establish an unauthenticated IMS Emergency Session.

The UE shall proceed as specified for the non-emergency case in except that the UE shall accept a NAS SMC selecting NEA0 and NIA0 algorithms from the AMF.

NOTE: In case of authentication success the AMF will send a NAS SMC selecting algorithms with a non-NULL integrity algorithm, and the UE will accept it.

b) AMF behavior:

After receiving Emergency Registration request from the UE, the AMF knows of that UE's intent to establish an unauthenticated IMS Emergency Session.

- If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.
- After the unsuccessful verification of the UE, the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.
- After the receiving of both, the Emergency Registration request and the failure message from the UE, the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

Editor's Note: Error message depend on the primary authentication method used. It is ffs which message is used by the UE to indicate authentication failure.

10.2.2.3 Key generation for Unauthenticated IMS Emergency Sessions

10.2.2.3.1 General

An unauthenticated UE does not share a complete 5G NAS security context with the network as there has been no successful primary authentication run between the UE and the AMF. When the UE and the AMF does not share the security context the only possibility for an AMF that allows unauthenticated IMS Emergency Sessions is to run with the NULL integrity algorithm NIA0 and the NULL ciphering algorithm NEA0.

When there has been no successful run of Primary authentication of the UE, the UE and the AMF independently generate the K_{AMF} in an implementation defined way and populate the 5G NAS security context with this K_{AMF} to be used when activating a 5G NAS security context. All key derivations proceed as if they were based on a K_{AMF} generated from a successful Primary authentication run.

Even if no confidentiality or integrity protection is provided by NIA0 and NEA0, the UE and the network treat the 5G security context with the independently generated K_{AMF} as if it contained a normally generated K_{AMF}.

10.2.2.3.2 Handover

When UE attempts to make Xn/N2 handover, UE and gNB derive and transfer the keys as normal to re-use the normal handover mechanism. Since the derived keys have no ability to affect the output of the NULL algorithms it is irrelevant that the network and the UE derive different keys. This implies that source gNB will forward UE 5G security capability which contains NIA0 and NEA0 only to target gNB. So the target gNB can only select NIA0 for integrity protection and NEA0 for confidential protection. If the UE does not receive any selection of new AS security algorithms during a intra-gNB handover, the UE continues to use the same algorithms as before the handover (see TS 38.331 [22]).

11 Security procedures between UE and external data networks via the 5G Network

11.1 EAP based secondary authentication by an external DN-AAA server

11.1.1 General

This sub-clause specifies support for optional to use secondary authentication between the UE and an external data network (DN).

The EAP framework specified in RFC 3748 [27] shall be used for authentication between the UE and a DN-AAA server in the external data network. The SMF shall perform the role of the EAP Authenticator. In the Home Routed deployment scenario, the H-SMF shall perform the role of the EAP Authenticator and the V-SMF shall transport the EAP messages exchanged between the UE and H-SMF. It shall rely on the external DN-AAA server to authenticate and authorize the UE's request for the establishment of PDU sessions.

Between the UE and the SMF, EAP messages shall be sent in the SM NAS message. This message is received at the AMF over N1 and delivered to the SMF over N11 using either the Nsmf_PDUSession_CreateSMContext service operation or the Nsmf_PDUSession_Update SM Context service operation, as specified in TS23.502 [8]. The SMF that takes the role of the EAP authenticator communicates with the external DN-AAA over N4 and N6 via the UPF.

The SMF invokes the Namf_Communication_N1N2MessageTransfer service operation to transfer the N1 NAS message containing the EAP message, towards the UE via the AMF.

Following clauses describe the procedures for initial Authentication and Re-Authentication with the external DN-AAA server.

11.1.2 Authentication

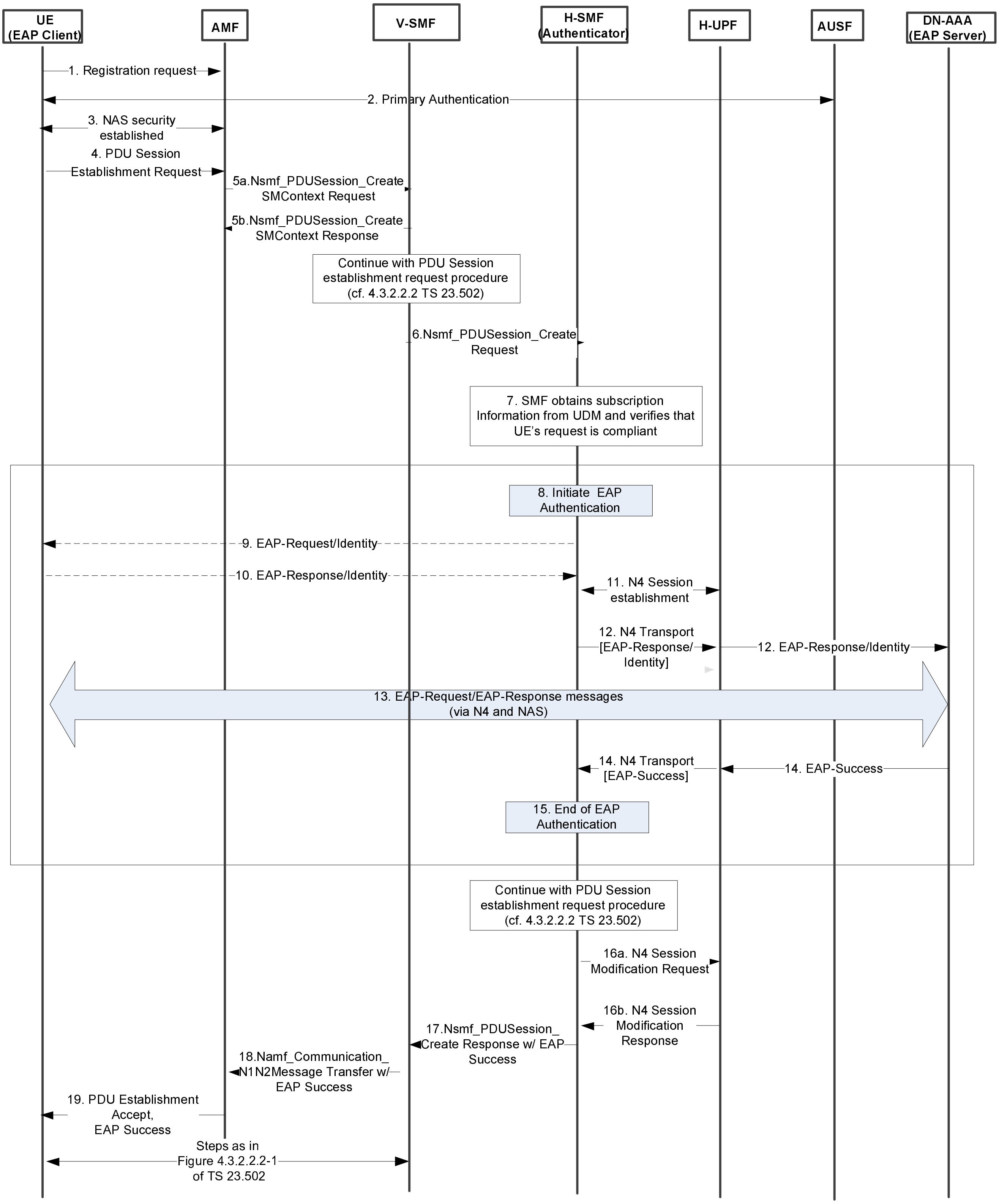
UE (EAP Client)
AMF
V-SMF
H-SMF (Authenticator)
H-UPF
AUSF
DN-AAA (EAP Server)
1. Registration request
2. Primary Authentication
3. NAS security established
4. PDU Session Establishment Request
5a.Nsmf_PDUSession_Create SMContext Request
5b.Nsmf_PDUSession_Create SMContext Response
Continue with PDU Session establishment request procedure (cf. 4.3.2.2.2 TS 23.502)
6.Nsmf_PDUSession_Create Request
7. SMF obtains subscription Information from UDM and verifies that UE's request is compliant
8. Initiate EAP Authentication
9. EAP-Request/Identity
10. EAP-Response/Identity
11. N4 Session establishment
12. N4 Transport [EAP-Response/ Identity]
12. EAP-Response/Identity
13. EAP-Request/EAP-Response messages (via N4 and NAS)
14. N4 Transport [EAP-Success]
14. EAP-Success
15. End of EAP Authentication
Continue with PDU Session establishment request procedure (cf. 4.3.2.2.2 TS 23.502)
16a. N4 Session Modification Request
16b. N4 Session Modification Response
17.Nsmf_PDUSession_ Create Response w/ EAP Success
18.Namf_Communication_ N1N2Message Transfer w/ EAP Success
19. PDU Establishment Accept, EAP Success
Steps as in Figure 4.3.2.2.2-1 of TS 23.502

Figure 11.1.2-1: Initial EAP Authentication with an external AAA server

The following procedure is based on sub-clauses 4.3.2.2.1 and 4.3.2.3 in TS 23.502 [8].

NOTE 1: Steps 1-6 are borrowed from clause 4.3.2.2.1 TS 23.502 and are for information only. Steps 7 to 15are related to authentication and are normative text.

1-3. The NG-UE registers with the network performing primary authentication with the AUSF/ARPF based on its network access credentials and establishes a NAS security context with the AMF.

4. The UE initiates establishment of a new PDU Session by sending a NAS message containing a PDU Session Establishment Request within the N1 SM container, slice information (identified by S-NSSAI) , PDU session ID and the PDN it would like to connect to (identified by DNN).

The PDU Session Establishment Request may contain SM PDU DN Request Container IE containing information for the PDU session authorization by the external DN.

5a. The AMF selects a V-SMF and sends either Nsmf_PDUSession_CreateSMContext Request or Nsmf_PDUSession_UpdateSMContext Request with the N1 SM container as one of its payload. It also forwards SUPI PDU Session ID, the received S-NSSAI, and the DNN.

5b. The V-SMF sends an Nsmf_PDUSession_CreateSMContext Responseor Nsmf_PDUSession_UpdateSMContext Response correspondingly to the AMF.

In case of a single SMF being involved in the PDU session setup, e.g. non-roaming or local breakout, that single SMF takes the role of both V-SMF and H-SMF. In this case, steps 6 and 17 are skipped.

6. The V-SMF sends an Nsmf_PDUSession_Create Request to the H-SMF.

7. The H-SMF obtains subscription data from the UDM for the given SUPI obtained from the AMF in step 5. The SMF checks whether the UE request is compliant with the user subscription and with local policies. If not, the H-SMF will reject UE's request via SM-NAS signalling and skip rest of the procedure. The SMF may also check whether the UE has been authenticated and/or authorized by the same DN, as indicated DNN in step 5, or the same AAA server in a previous PDU session establishment. The SMF may skip steps 8 to 15 if positive.

NOTE 2: The information on a successful authentication/authorization between a UE and an SMF may be saved in SMF and/or UDM.

8. The H-SMF shall trigger EAP Authentication to obtain authorization from an external DN-AAA server.

9. The H-SMF shall send an EAP Request/Identity message to the UE.

10. The UE shall send an EAP Response/Identity message contained within the SM PDU DN Request Container of a NAS message. The SM PDU DN Request Container includes its DN-specific identity complying with Network Access Identifier (NAI) format and PDU session ID.

To avoid the additional round-trip in steps 9 and 10, the secondary authentication identity may be sent by the UE in step 4.

11. The H-SMF selects a UPF and establishes an N4 Session with it. The SM PDU DN Request Container, if provided by the UE, is forwarded to the UPF. The H-SMF identifies the DN AAA server based on the SM PDU DN Request Container provided by the UE and on local configuration.

12. The UPF shall forward the SM PDU DN Request Container containing EAP Response/Identity message to the DN AAA Server.

13. The DN AAA server and the UE shall exchange EAP messages, as required by the EAP method, contained in the SM PDU DN Request Containers. In addition, it may send additional authorization information as defined in TS 23.501 clause 5.6.6.

14. After the successful completion of the authentication procedure, DN AAA server shall send EAP Success message to the H-SMF.

15. This completes the authentication procedure at the SMF. The SMF may save the DN-specific ID and DNN (or DN's AAA server ID if available) in a list for successful authentication/authorization between UE and an SMF. Alternatively, the SMF may update the list in UDM.

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 [8].

16a-16b. The SMF initiates a N4 Session Modification procedure with the selected UPF as in steps 9.a and 9.b of Fig 4.3.2.2.1-1 in TS 23.502 [8].

17. The H-SMF sends an Nsmf_PDUSession_Create Response to the V-SMF. This message shall include EAP Success to be sent to the UE to V-SMF.

18. The V-SMF sends an Namf_Communication_N1N2MessageTransfer to the AMF as in step 11 of Figure 4.3.2.2.1-1 in TS 23.502 [8]. This message shall include EAP Success to be sent to the UE within the NAS SM PDU Session Establishment Accept message.

19. The AMF forwards NAS SM PDU Session Establishment Accept message along with EAP Success to the UE as described in steps 12 and step 13 of Figure 4.3.2.2.1-1 in TS 23.502 [8].

The UE-requested PDU Session Establishment proceeds further as described in sub-clause 4.3.2.3 in TS 23.502 [8].

11.1.3 Re-Authentication

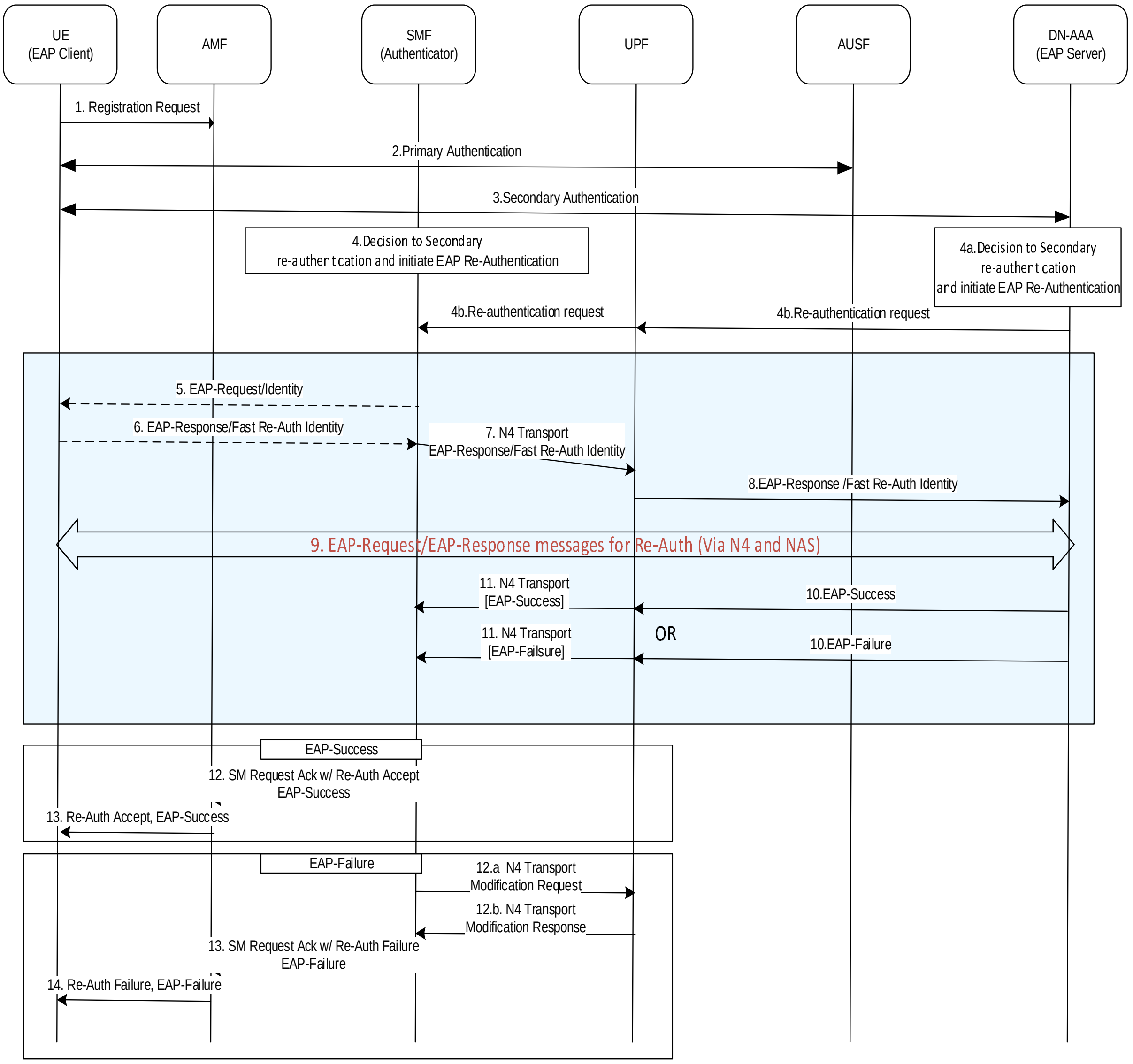
UE
(EAP Client)
AMF
SMF
(Authenticator)
UPF
AUSF
DN-AAA
(EAP Server)
1. Registration Request
2.Primary Authentication
3.Secondary Authentication
4.Decision to Secondary
re-authentication and initiate EAP Re-Authentication
4a.Decision to Secondary
re-authentication
and initiate EAP Re-Authentication
4b.Re-authentication request
4b.Re-authentication request
5. EAP-Request/Identity
6. EAP-Response/Fast Re-Auth Identity
7. N4 Transport
EAP-Response/Fast Re-Auth Identity
8.EAP-Response /Fast Re-Auth Identity
9. EAP-Request/EAP-Response messages for Re-Auth (Via N4 and NAS)
11. N4 Transport
[EAP-Success]
10.EAP-Success
OR
11. N4 Transport
[EAP-Failsure]
10.EAP-Failure
EAP-Success
12. SM Request Ack w/ Re-Auth Accept
EAP-Success
13. Re-Auth Accept, EAP-Success
EAP-Failure
12.a N4 Transport
Modification Request
12.b. N4 Transport
Modification Response
13. SM Request Ack w/ Re-Auth Failure
EAP-Failure
14. Re-Auth Failure, EAP-Failure

Figure 11.1.3-1: EAP Re-Authentication with an external AAA server

1-3 Secondary Authentications has been established according to procedures specified in clause 11.1.2, Initial EAP Authentication with an external AAA server.

Secondary Re-authentication may either be initiated by SMF or the external DN/AAA server. If Re-authentication is initiated by SMF, the procedure proceeds with step 4 (skipping steps 4a and 4b). If Re-authentication is initiated by the external DN/AAA server, the procedure proceeds with the alternative steps 4a and 4b.

4. The SMF decides to initiate Secondary Re-Authentication.

4a. The DN AAA server decides to initiate Secondary Re-Authentication.

4b. The DN AAA shall send a Secondary Re-Authentication request to UPF and the UFP forwards to SMF.

5. The SMF shall send an EAP Request/Identity message to the UE.

6. The UE shall respond with an EAP Response/Identity message (with Fast-Reauth Identity).

7. The SMF forwards the EAP Response/Identity to UPF, selected during initial authentication, over N4 interface.

This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.

8. The UPF shall forward the EAP Response/Identity message to the DN AAA Server.

9. The DN AAA server and the UE shall exchange EAP messages as required by the EAP method.

10. After the completion of the authentication procedure, DN AAA server either sends EAP Success or EAP Failure message to the SMF.

11. This completes the Re-authentication procedure at the SMF.

12-13. If the authorization is successful, EAP-Success shall be sent to UE.

12-14. If authorization is not successful, the SMF notifies failure to UPF. Upon completion of a N4 Session Modification procedure with the selected UPF, SMF sends EAP-Fail to UE via AMF.

12 Security aspects of Network Exposure Function (NEF)

12.1 General

In the 5G system, the Network Functions securely expose capabilities and events to 3rd party Application Functions via NEF. The NEF also enable secure provision of information in the 3GPP network by authenticated and authorized Application Functions.

Requirements on security aspects of NEF are captured in clause 5.9.2.3.

12.2 Mutual authentication

For authentication between NEF and an Application Function that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates shall be performed between the NEF and AF using TLS.

Certificate based authentication shall follow the profiles given in 3GPP TS 33.310 [17], clauses 6.1.3a and 6.1.4a. The structure of the PKI used for the certificate is out of scope of the present document.

12.3 Protection of the NEF – AF interface

TLS shall be used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the Application Function. The support of TLS is mandatory.

Security profiles for TLS implementation and usage shall follow the provisions given in TS 33.310 [17], Annex E.

12.4 Authorization of Application Function’s requests

After the authentication, NEF determines whether the Application Function is authorized to send requests for the 3GPP Network Entity. The NEF shall authorize the requests from Application Function using OAuth-based authorization mechanism, the specific authorization mechanisms shall follow the provisions given in RFC 6749 [43].

12.5 Support for CAPIF

When the NEF supports CAPIF for external exposure as specified in clause 6.2.5.1 in TS 23.501[2], then CAPIF core function shall choose the appropriate CAPIF-2e security method as defined in the sub-clause 6.5.2 in TS 33.122[53] for mutual authentication and protection of the NEF – AF interface.

13 Service Based Interfaces (SBI)

13.1 Protection at the network or transport layer

All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.

The TLS profile shall follow the profile given in Annex E of TS 33.310 [5] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

TLS shall be used for transport protection within a PLMN unless network security is provided by other means.

NOTE a: Regardless whether TLS is used or not, NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5] can be used for network layer protection.

NOTE b: In case interfaces are trusted (e.g. physically protected), there is no need to use cryptographic protection.

If there are no IPX entities between the SEPPs, TLS shall be used between the SEPPs. If there are IPX entities between SEPPs, application layer security on the N32 interface between SEPPs is needed for protection between the SEPPs. Application Layer Security solutions is specified in clause 5.6.3 (requirements) and clause 13.2 (procedures).

NOTE 1: Void

NOTE 2: Void.

13.2 Application layer security on the N32 interface

Editor's Note: This sub-clause is to include solutions satisfying the requirements on e2e security in clause 5.6. It is ffs whether the work performed by GSMA FASG DESS on e2e security for selected DIAMETER AVPs can be somehow utilized here. It is to also take into account solutions 10.1 and 10.2 in clause 5.10.4 of TR 33.899. When the solution(s) involve a Public Key Infrastructure then details of the use of the PKI are to be provided, e.g. by reference to TS 33.310.

13.2.1 General

The internetwork interconnect allows secure communication between service-consuming and a service-producing NFs in different PLMNs. Security is enabled by the Security Edge Protection Proxies of both networks, henceforth called cSEPP and pSEPP respectively. The SEPPs enforce protection policies regarding application layer security thereby ensuring integrity and confidentiality protection for those elements to be protected.

It is assumed that there are interconnect providers between cSEPP and pSEPP. The interconnect provider the cSEPP's operator has a business relationship with is called cIPX, while the interconnect provider the pSEPP's operator has a business relationship with is called pIPX. There could be further interconnect providers in between cIPX and pIPX, but they are assumed to be transparent and simply forward the communication.

A NF on the consumer side sends a message to a NF on the producer side. If this communication is across PLMN operators, as shown in Figure 13.2.x-1 below, the cSEPP receives the message and applies application layer protection, as defined in the present specification. The pIPX and cIPX can offer services that require modifications of the messages transported over the interconnect interface. These modifications are appended to the message and reflect the desired changes. The pSEPP, which receives the message, validates the message, extracts the original message and applies the patches by intermediaries. The pSEPP then forwards the message to the destination NF if the validations succeed.

The N32 interface consists of

- N32-c connection, for management of the N32 interface, and

- N32-f connection, for sending of JOSE protected messages between the SEPPs.

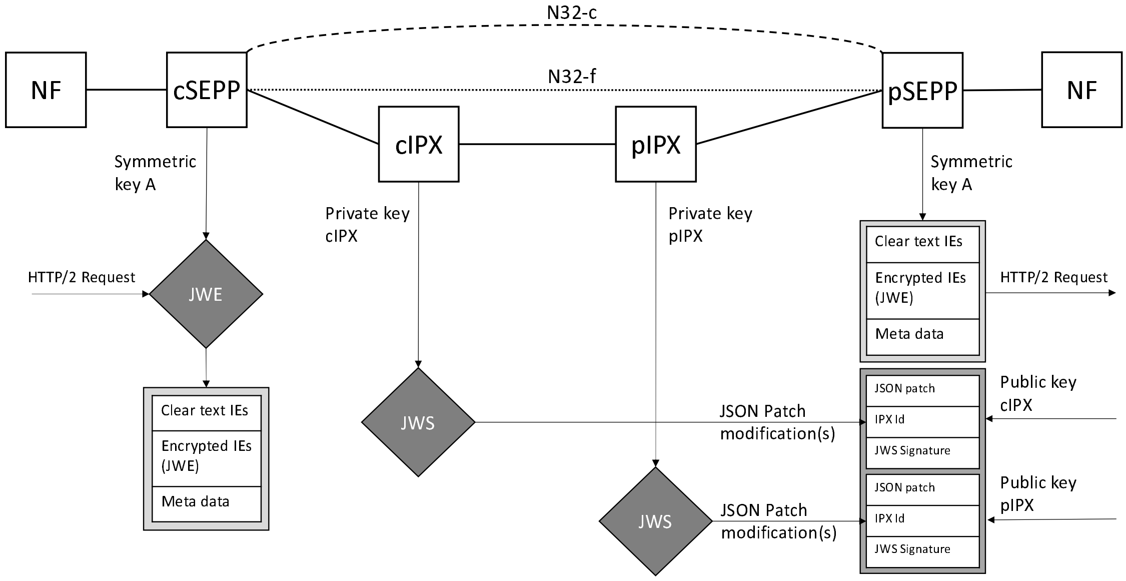

Figure 13.2.1-1: Overview of N32 Application Layer Security

13.2.2 N32-c connection between SEPPs

13.2.2.1 General

When the SEPPs have mutually authenticated each other and when the negotiated the security mechanism to use over N32 is Application Layer Security, the SEPPs use the established TLS connection (N32-c connection) to negotiate the N32 specific associated security configuration parameters.

The N32-c connection is used for the following:

- Key agreement: The SEPPs independently export keying material associated with the established N32-c connection between them and use it as the pre-shared key for generating the shared session key required. This is based on RFC 5705 [59] for TLS 1.2. For TLS 1.3, the exporter described in section 7.5 of [60] is used.

- Parameter exchange: The SEPPs exchange security related configuration parameters that are needed by the SEPPs to protect HTTP messages exchanged between the two Network Functions (NF) in their respective networks.

- Error handling: The receiving SEPP sends an error signalling message to the peer SEPP when it detects error on the N32 interface.

The following security related configuration parameters may be exchanged between the two SEPPs:

a. Modification policy – Modification policy, as specified in clause 13.2.z.4, indicates which IEs can be modified by an IPX provider of the sending SEPP.

b. Cipher suites for confidentiality and integrity protection when Application layer security is used to protect HTTP messages between them.

c. N32-f precontext identifier values, that's used by each SEPP to identify the set of security related configuration parameters, when it receives a protected message from a SEPP in a different PLMN.

Editor's Note: Whether supported confidentiality protection and integrity protection methods need to be negotiated is FFS.

13.2.2.2 Procedure for Key agreement and Parameter exchange

1. The two SEPPs perform a cipher suite negotiation to agree on a cipher suite to use for protecting NF service related signalling over N32-f.

    1a. The SEPP which initiated the TLS connection sends a Parameter Exchange Request message to the responding SEPP including the initiating SEPP's supported cipher suites. The cipher suites are ordered in initiating SEPP's priority order. The SEPP provides a N32-f precontext ID for the responding SEPP. The precontext IDs are 32-bit random integers, represented as 0-left padded strings of hexadecimal digits

    1b. The responding SEPP compares the received cipher suites to its own supported cipher suites and selects, based on its local policy, a suite, which is supported by both initiating SEPP and responding SEPP.

    1c. The responding SEPP sends a Parameter Exchange Response message to the initiating SEPP including the selected cipher suite for protecting the NF service related signalling over N32. The responding SEPP provides a N32-f precontext ID for the initiating SEPP.

    1d. The SEPPs create the N32-f context Id as follows:

    Initiater's N32-f precontext ID | responder's N32-f precontext ID

2. The two SEPPs may perform exchange of Data-type encryption policies and Modification policies. Both SEPPs shall store the protection policies sent by peer SEPP:

    2a. The SEPP, which initiated the TLS connection, sends a Parameter Exchange Request message to the responding SEPP including the initiating SEPP's protection policies listed in clause 13.2.z.

    2b. The responding SEPP shall store the policies if sent by the initiating SEPP.

    2c. The responding SEPP sends a Parameter Negotiation Response message to the initiating SEPP with the selected values for the parameters sent in step 5a and responding SEPP's suite of protection policies.

    2d. The initiating SEPP shall store the protection policy information if sent by the responding SEPP,

3. The two SEPPs shall exchange IPX security information lists.

4. The two SEPPs export keying material from the TLS session established between them using the TLS export function as specified in RFC 5705 [61] for TLS 1.2. For TLS 1.3, the exporter described in section 7.5 of [60] is used. The exported key shall be used as the master key to derive session keys and IVs for the N32-f context as specified in clause 13.2.4.4.1.

5. The two SEPPs start exchanging NF to NF service related signalling over N32-f and keep the TLS session open for:

    - any further N32-c communication that may occur over time while application layer security is applied to N32-f, or

    - any further N32-c and N32-f communication, if TLS is used to protect N32-f.

Editor's Note: The exact message names are FFS.

13.2.2.3 Procedure for Error detection and handling in SEPP

Errors can occur on an active N32-c connection or on one or more N32-f connections between two SEPPs.

When an error is detected, the SEPP shall map the error to an appropriate cause code. A signalling message is created to inform the peer SEPP, with cause code as one of its parameters.

The N32-c connection shall be used to send the signalling message to the peer SEPP.

If the error occurred in the processing of the one or more N32-f message(s), the corresponding Message Id (s), included in the metadata section of the N32-f message, shall be included as a parameter in the signalling message. This allows the peer SEPP to identify the source message (HTTP Request or Response) on which the error was found in the other SEPP.

NOTE: Local action taken by either SEPP is out of 3GPP scope.

13.2.2.4 N32-f Context

13.2.2.4.0 N32-f parts

The N32-f context consists of the following main parts also illustrated in Figure 13.2.2.4.0-1:

1. N32-f context ID
2. N32-f peer information
3. N32-f security context
4. N32-f context information

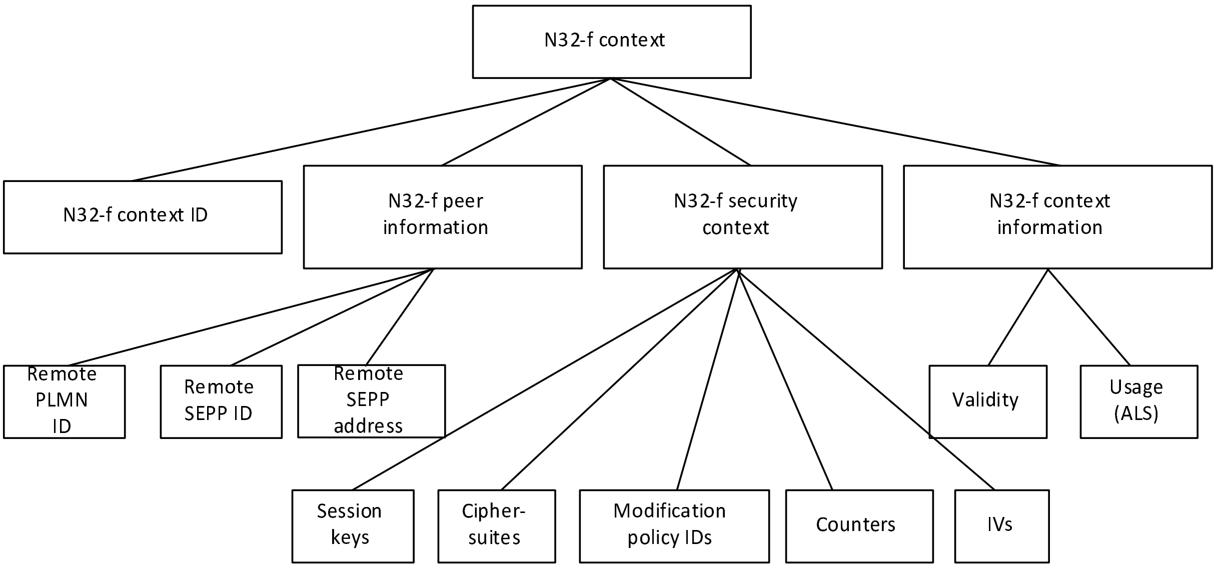

Figure 13.2.2.4.0-1: N32-f context overview

13.2.2.4.1 N32-f context ID

The N32-f context ID is used to refer to an N32-f context. The N32-f context ID is created during the N32-c negotiation and used over N32-f to inform the reveiving peer which security context to use for decryption of a received message.

To avoid collision of the N32-f context ID value, the ID shall be selected as a random value during the exchange over N32-c.

During transfer of application data over N32-f, the N32-f context ID shall be contained in a separate IE in the payload part of the JSON structure, see clause 13.2.a.2.1. The receiving part shall use this information to apply the correct key and parameters during decryption and validation.

13.2.2.4.2 N32-f peer information

The N32 "connection" between SEPPs is bidirectional and consists of the two SEPP endpoints and possibly up to two IPX providers. The SEPPs are identified by the PLMN ID and additionally a SEPP ID to distinguish between several SEPPs in the same PLMN. The remote SEPP address is necessary for routing the messages to the correct destination. The N32 peer information consists of the following parameters:

- Remote PLMN ID;
- Remote SEPP ID;

- Remote SEPP address.

13.2.2.4.3 N32-f security context

The N32-c initial handshake establishes session keys, IVs and negotiated cipher suites. Counters are used for replay protection. Modification policies are identified by modification policy IDs, to be able to verify received messages that have undergone IPX modifications. The N32 security context consists of the following parameters:

- Session keys
- Negotiated cipher suites
- Modification Policy IDs (if IPXs are used)
- Counters
- IVs
- List of security information of the IPX providers connected to the SEPPs (IPX security information list)
    - IPX provider identifier
    - List of raw public keys or certificates for that IPX

13.2.2.4.4 N32-f context information

The N32 context information consists of the following parameters:

- Validity
- Usage (application layer solution)

13.2.3 Protection policies for N32 application layer solution

13.2.3.1 Overview of protection policies

The protection policy suite is comprised of a data-type encryption policy and a modification policy. Together, these policies determine which part of a certain message shall be integrity protected, which part of a certain message shall be confidentiality protected, and which part of a certain message shall be modifiable by IPX providers. For application layer protection of messages on the N32 interface, the SEPP shall apply message protection policies.

There are two protection policies, namely:

- Data-type encryption policy that specifies which data types need to be confidentiality protected;
- A modification policy that specifies which IEs are modifiable by intermediaries

In addition, there is a mapping between the data-types in the data-type encryption policy and the IEs in NF API descriptions which is given in a NF-API data-type placement mapping.

13.2.3.2 Data-type encryption policy

The SEPP shall contain an operator controlled protection policy that specifies which types of data shall be encrypted. The data-types defined at this moment are the following:

- Data of the type 'SUPI'
- Data of the type 'location data'
- Data of the type 'key material'
- Data of the type 'authorization token'

This policy shall be on a per roaming partner basis.

The policy shall contain an identifier that identifies the policy and a release number referring to the release it is applicable for.

The Data-type encryption policies in the two partner SEPPs shall be equal in order to enforce a consistent ciphering of IEs on N32.

13.2.3.3 NF API data-type placement mapping

Each NF API data-type placement mapping shall contain the following:

- Which IEs contain data of the type 'IMSI' or type 'NAI'.
- Which IEs contain data of the type 'location data'.
- Which IEs contain data of the type 'key material'.
- Which IEs contain data of the type 'authorization token'.

Where the location of the IEs refers to the location of the IEs after the SEPP has rewritten the message for transmission over N32.

An NF API data-type placement mapping shall furthermore contain data that identifies the NF API, namely

- The name of the NF;
- The version;
- An identifier;
- The release version.

NOTE: Larger networks can contain multiple NFs with the same API, e.g. three AMFs. The NF API policy applies to all NFs with the same API.

The NF API data-type placement mapping resides in the SEPP.

13.2.3.4 Modification policy

The SEPP shall contain an operator-controlled policy that specifies which IEs can be modified by the IPX provider directly related to this particular SEPP. These IEs refer to the IEs after the sending SEPP has rewritten the message.

Each PLMN-operator shall agree the modification policy with the IPX provider it has a business relationship with prior to establishment of an N32 connection. Each modification policy applies to one individual relation between PLMN-operator and IPX provider. In order to cover the complete N32 connection both involved roaming partners exchange their modification policies. Both complementary modification policies comprise the overall modification policy for this specific N32 connection.

NOTE 1: In order to validate modifications for messages received on the N32 interface, the operator’s roaming partners will have to know the overall modification policy.

NOTE 2: Modification includes removal and addition of new IE. IEs therefore may not be present in the rewritten message.

The IEs that the IPX is allowed to modify are specified in a list giving an enumeration of JSON paths within the JSON object created by the SEPP. Wildcards may be used in specifying paths.

This policy shall be specific per roaming partner and per IPX provider that is used for the specific roaming partner.

The modification policy resides at the SEPP

For each roaming parter, the SEPP shall be able to store a policy for sending in addition to one for receiving.

A basic modification policy that shall be applied irrespective of the exchanged policy is that IEs requiring encryption shall not be inserted at a different location in the JSON object.

13.2.3.5 Provisioning of the policies in the SEPP

The SEPP shall contain an interface that the operator can use to manually configure the protection policies in the SEPP.

The SEPP shall be able to store and process the following policies for outgoing messages:

- A generic data-type encryption policy;
- Roaming partner specific data-type encryption policies that will take precedence over a generic data-type encryption policy if present;
- One NF API Data-type placement mapping;
- Multiple modification policies, to handle modifications that are specific per IPX provider and modification policies that are specific per IPX provider and roaming partner.

The SEPP shall also be able to store and process the following policies for incoming messages:

- Roaming partner specific data-type encryption policies;
- Roaming partner specific modification policies that specifies which fields can be modified by which IPX providers.

13.2.4 N32-f connection between SEPPs

13.2.4.1 General

The SEPP receives the HTTP/2 request/response messages from the Network Function. It performs the following actions on these messages before they are sent on the N32-f interface to the SEPP in the other PLMN:

a) It parses the incoming message and reformats it to produce the input to JWE (clause 13.2.4.3).

b) It applies JSON Web Encryption (JWE) [x] on the input created in a) to protect the reformatted message (clause 13.2.4.4).

c) It encapsulates the resulting JWE object into a HTTP/2 message (as the body of the message) and sends to the SEPP in the other PLMN over the N32-f interface.

The path between the two SEPPs may take them via the cIPX and pIPX nodes. These IPX nodes may modify messages as follows:

a) The IPX node recovers the unencrypted (cleartext) section of the HTTP message (in the JWE object), modifies it according to the modification policy, and calculates an "operations" JSON Patch object. It creates a temporary JSON object with "operations" and few other parameters for replay protection etc. (clause 13.2.4.5.1).

b) The temporary JSON object is input into JSON Web Signature (JWS) [45] to create a JWS object (clause 13.2.4.5.2).

c) The JWS object is appended to the received message and sent to the next hop.

The JWS objects generated by the two IPX providers form an auditable chain of modifications that are applied to the parsed message at the receiving end after verifying that the patches conform to the modification policy.

Encryption of IEs take place end to end between cSEPP and pSEPP.

13.2.4.2 Overall Message payload structure for message reformatting at SEPP

A HTTP message received from an internal Network Function is reformatted into two temporary JSON objects that will be intput to JWE:

a. The **dataToIntegrityProtect** containing information that is only integrity protected. It contains the following:

- clearTextEncapsulationMessage – contains the complete original HTTP message, excluding parts which require encryption and, including the pseudo-header fields, HTTP headers and HTTP message body.
- metadata – contains SEPP generated information i.e. authorizedIPX ID, Message ID and N32-f context Id.

b. The **dataToIntegrityProtectAndCipher** containing parts of original message that require both encryption and integrity protection.

```
{
   ‶dataToIntegrityProtect″ : {
      ‶clearTextEncapsulatedMsg″ : {
          ‶Pseudo-Headers″ : {
             ‶Method″ : {},
             ‶Scheme″ : {},
             ‶Authority″ : (},
             ‶Path″ : {},
             ‶Query&Fragment″ : {}
          },
          ‶HTTP_Headers″ : {
             ‶Hdr1″: {},
             ‶Hdr2″:{‶encBlockIdx″: 0}
          },
          ‶Payload″ : {
             ‶IE1″ :{},
             ‶IE2″ :{‶encBlockIdx″: 1},
             ‶IE3″ :{},
             ‶IE4″ :{}
          }
      },
      ‶metaData″ : {
         ‶Message Id″ : {},
          ‶authorizedIPX Id″ : {},
          ‶N32-f Context Id″ : ()
      }
   },
   ‶dataToIntProtectAndCipher″ : [
       Hdr2,
       IE2
   ]
}
```

Figure 13.2.4.2-1 Example of JSON representation of a reformatted HTTP message

Editors Note: Reformatting of Multipart HTTP messages (with JSON + binary payload) to be aligned with CT4 once available.

13.2.4.3 Message reformatting in sending SEPP

13.2.4.3.1 dataToIntegrityProtect

13.2.4.3.1.1 clearTextEncapsulatedMessage

This is a JSON object that contains the non-encrypted portion of the original message and consists of the following objects:

1.a) Pseudo_Headers – the JSON object that includes all the Pseudo Headers in the message.

- For HTTP Request messages, the object contains entry each for the ":method", ":path", ":scheme" and ":authority" pseudo headers.

NOTE: If the "path" pseudoheader contains multiple parts separated by a slash (/) or includes a query parameter (following a "?"), an array is used to represent :path, with one element per part of the path (i.e. per "directory"). This enables ciphering individual element of the path (e.g. if SUPI is passed).

- For HTTP Response messages, the object contains the ":status" pseudo header.

1.b) HTTP_Headers - All the headers of the request are put into a JSON object (map) called HTTP_Headers, with the header name as "key" and the header value as "value".

1.c) Payload – the JSON object that includes the content of the payload of the HTTP message. Each attribute or IE in the payload shall form a single entry in the Payload JSON object. If there is any attribute value that requires encryption, it shall be moved into the **dataToIntegrityProtectAndCipher** JSON object (clause 13.2.a.3.2), and the original value in this element shall be replaced by the index in the form {"encBlockIdx": <num>} where "num" is the index of the corresponding entry in the **dataToIntegrityProtectAndCipher** array.

13.2.4.3.1.2 metadata

The JSON object containing information added by the sending SEPP. It contains:

a) **Message Id**: Unique identifier (64 bit integer) representing a HTTP Request/Response transaction between two SEPPs.

b) **authorizedIPX Id**: string identifying the first hop IPX (cIPX or pIPX) that is authorized to update the message. This field shall always be present. When there is no IPX that’s authorized to update, the value of this field is set to "NULL".

c) **N32-f Context Id**: Unique identifier representing the N32-f context information used for protecting the message.

13.2.4.3.2 dataToIntegrityProtectAndCipher

The dataToIntegrityProtectAndCipher is a JSON array that contains all the attribute values that require both encryption and integrity protection. Attribute values can come from any part of the original HTTP message – Pseudo_Headers, HTTP_Headers and Payload.

The JSON array shall contain one array entry per attribute value that needs encryption. Each array entry represents the value of the attribute to be protected, and the index in the array is used to reference the protected value within the dataToIntegrityProtect block. This associates each attribute in the dataToIntegrityProtectAndCipher block with the original attribute in the dataToIntegrityProtect block. This is needed to reassemble the original message at the receiving SEPP.

13.2.4.4 Protection using JSON Web Encryption (JWE)

Protection of reformatted HTTP messages between SEPPs shall use JSON Web Encryption (JWE) as specified in IETF RFC 7516 [59]. All encryption methods supported by JWE are AEAD methods that encrypt, and integrity protect "plaintext" in one single operation and can additionally integrity protect additional data.

The dataToIntegrityProtectAndCipher and dataToIntegrityProtect blocks shall be input to JWE as plaintext and JWE Additional Authenticated Data (AAD) respectively. The JWE AEAD algorithm generates JWE encrypted text (ciphertext) and a JWE Authentication Tag (Message Authentication Code). The ciphertext is the output from symmetrically encrypting the plaintext, while the authentication tag is a value that verifies the integrity of both the generated ciphertext and the Additional Authenticated Data.

If the dataToIntegrityProtectAndCipher is not present in the rewritten HTTP message, the JWE plaintext shall be set to the string "NULL". The JWE AEAD algorithm will generate ciphertext and an authentication tag, but the ciphertext will not contain meaningful information.

The Flattened JWE JSON Serialization syntax shall be used to represent JWE as a JSON object.

The session key shared between the two SEPPs, as specified in clause 13.2.a.4.1, shall be used as the Content Encryption Key (CEK) value to the algorithm indicated in the Encryption algorithm ("enc") parameter in the JOSE header. The algorithm ("alg") parameter in the JOSE header denoting the key exchange method shall be set to "dir", i.e. "Direct use of a shared symmetric key as the CEK".

The 3GPP profile for supported cipher suites in the "enc" parameter is described in clause 13.2.4.9.

If AES GCM is used for AEAD the security considerations in 8.4 of [59] shall be taken into account. In particular, the same key shall not be used more than 2^{32} times and an IV value shall not be used more than once with the same key.

The generated JWE object is transmitted on the N32-f interface in the payload body of a SEPP to SEPP HTTP/2 message.

13.2.4.4.1 N32-f key hierarchy

The N32-f key hierarchy is based on the N32-f master key generated during the N32-c initial handshake by TLS key export. Each run of the N32-f key derivation creates two pairs of session keys and IV salts. The two pairs are used in two different HTTP/2 sessions. In one Session the N32-c initiatior acts as the HTTP client and in the second the N32-c responder acts as the client.

If the exported master secret is reused to set up multiple HTTP sessions or to set up new HTTP sessions on stream ID exhaustion, a new, unique, Context ID shall be generated to avoid key and IV re-use.

The master key is obtained from the TLS exporter. The export function takes 3 arguments: Label, Context, Length (in octets) of desired output. For the N32 Master key derivation, the label shall be "EXPORTER_3GPP_N32_MASTER", the Context shall be "" (the empty string) and the Length shall be 64.

Editor’s Note: The exporter label for this usage should be registered with IANA

The N32 key derivation function N32-KDF is based on HKDF [62] and uses only the HKDF-Expand function as the initial key material has been generated securely:

N32-KDF (label, L) = HKDF-Expand (N32-f master key, "N32" || N32-Context-ID || label, L),

where

- label is a string used for key separation,
- L is the length of output keying material in octets.

There are two pairs of session keys and IV salts to be derived.

NOTE: In AES-GCM re-use of one IV may reveal the integrity key (Joux’s Forbidden attack). The binding of session keys and IV salts to context IDs and different HTTP sessions is essential to protect against inadvertent use of the same key with a repeated IV.

The labels for the JWE keys are:

- "parallel_request_key"
- "parallel_response_key"
- "reverse_request_key"
- "reverse_response_key"

The keys derived with labels starting parallel are to be used for request/responses in an HTTP session with the N32-c initiating SEPP acting as the client (i.e. in parallel to the N32-c connection). The keys derived with the labels starting reverse are used for an HTTP session with the N32-c responding SEPP acting as the client.

To generate the IV salts, the length is 4 and the labels are:

- "parallel_request_iv_salt"
- "parallel_response_iv_salt"
- "reverse_request_iv_salt"
- "reverse_response_iv_salt"

The 96-bit nonce for AES_GCM shall be constructed as the concatenation of the IV salt (4 octets, 32-bits) and the sequence counter, SEQ, as defined in 8.2.1 of [63]. The sequence counter shall be a 64-bit unsigned integer that starts at zero and is incremented for each invocation of the encryption. A different sequence counter shall be maintained for each IV salt.

```
Nonce = IV salt | SEQ
```

13.2.4.5 Message modifications in IPX

13.2.4.5.1 modifiedDataToIntegrityProtect

```
modifiedDataToIntegrityProtect =
{
   ″Operations″ : JSON Patch that captures
         IPX provider modifications,
   ″Identity″ : ″IPX1",
   ″Tag″ : JWE Tag generated by sending
         SEPP
}
```

Figure 13.2.4.5.1-1 Example of JSON representation of IPX provider modifications

This is a temporary JSON object generated by an IPX provider as it modifies the original message. It contains the following:

a) **Operations** - This is a JSON string element that captures IPX modifications based on RFC 6902 [64]. If no patch is required, the operations element is set to NULL.

b) **Identity** - This is the Identity of the IPX performing the modification.

c) **Tag** – A JSON string element to capture the “tag” value (JWE Authentication tag) in the JWE object generated by the sending SEPP. This is required for replay protection.

NOTE: Since there is no central registry that can ensure unique IPX Identities, it is expected that an IPX will include its Fully Quantified Domain Name (FQDN) in the JSON modification object.

13.2.4.5.2 Modifications by IPX

NOTE: It is assumed that operators act as a certification authority for IPX providers they have a direct business relationship with. In order to authorize N32-f message modifications, operators sign a digital certificate for each of these IPX providers and provide it to both the IPX provider itself as well as their roaming partners to enable them to validate any modifications by this IPX provider.

Only cIPX and pIPX shall be able to modify messages between cSEPP and pSEPP. In cases of messages from cSEPP to pSEPP, the cIPX is the first intermediary, while the pIPX is the second intermediary. In cases of messages from pSEPP to cSEPP the pIPX is the first intermediary, while the cIPX is the second intermediary.

The first intermediary shall parse the encapsulated request (i.e. the clearTextEncapsulationMsg in the dataToIntegrityProtect block) and determine which changes are required. The first intermediary creates an “operations” JSON document to describe the differences between received and desired message, taking the syntax and semantic from RFC 6902 [64] (JSON patch), such that, when applying the JSON patch to the encapsulated request the result will be the desired request. If no patch is required, the operations element is NULL.

NOTE: It is necessary to create a JWS object even if no patch is required to prevent deletion of modifications.

The first intermediary creates a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.a.5.1. It includes its identity and the JWE authentication tag, which associates this update by the intermediary with the JWE object created by the sending SEPP.

The modifiedDataToIntegrityProtect JSON object is input to JWS to create a JWS object. The generated JWS object is appended to the payload in the HTTP message. The message is then sent to the next hop.

The second intermediary parses the encapsulated request, applies the modifications described in the JSON patch appended by the first intermediary and determines further modifications required for obtaining the desired request. These modifications are recorded in an additional JSON patch against the JSON object resulting after application of the first intermediary's JSON patch. If no patch is required, the operations element for the second JSON patch is NULL

The second intermediary creates a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.a.5.1. It includes its identity and the JWE authentication tag, which associates this update by the second intermediary with the JWE object created by the sending SEPP.

The modifiedDataToIntegrityProtect JSON object is input to JWS to create a JWS object. The generated JWS object is appended to the payload in the HTTP message. The message is then sent to the receiving SEPP.

13.2.4.6 Protecting IPX modifications using JSON Web Signature (JWS)

Protection of IPX provider modified attributes shall use JSON Web Signature (JWS) as specified in IETF RFC 7515 [45]. The mechanism described in this clause uses signatures, i.e. asymmetric methods, with private/public key pairs.

When an IPX node modifies one or more attributes of the original HTTP message and creates a modifiedDataToIntegrityProtect to record its modifications, it shall use JWS to integrity protect the modifiedDataToIntegrityProtect object.

The private key of the IPX provider shall be used as input to JWS for generating the signature representing the contents of the patchRequest.

The "alg" parameter in the JOSE header indicates the chosen signature algorithm. The 3GPP profile for supported algorithms is described in clause 13.2.a.9.

The Flattened JWS JSON Serialization syntax shall be used to represent JWS as a JSON object.

13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP shall decrypt the JWE ciphertext using the shared session key and the following parameters obtained from the JWE object – Initialization Vector, Additional Authenticated Data value (clearTextEncapsulatedMessage in “aad”) and JWE Authentication Tag (“tag”).

The content encryption algorithm checks the integrity and authenticity of the clearTextEncapsulatedMessage and the encrypted text by verifying the JWE Authentication Tag in the JWE object. The algorithm returns the decrypted plaintext (dataToIntegrityProtectAndCipher) only if the JWE Authentication Tag is correct.

The receiving SEPP refers to the NF API data-type placement mapping table to re-construct the original reformatted message by updating corresponding entries in clearTextEncapsulatedMessage with values in the dataToIntegrityProtectAndCipher array.

The receiving SEPP shall next verify IPX provider updates by verifying JWS signatures added by the intermediaries. For modifications by IPX provider that the receiving SEPP’s operator does not have a business relationship with, the SEPP shall verify the JWS signature, using the corresponding raw public key or certificate that is contained in the IPX provider’s security information list obtained as part of the N-32 security context setup. It then checks that the raw public key or certificate of the JWS signature IPX's Identity in the modifiedDataToIntegrity block matches to the IPX provider referred to in the "authorizedIPX Id" field added by the sending SEPP, based on the information given in the IPX provider security information list.

The receiving SEPP checks whether the modifications performed by the intermediaries were permitted by the respective modification policies. If this is the case, the receiving SEPP applies the patches in the “operations” field in order, performs plausibility checks, and creates a new HTTP request according to the "patched" clearTextEncapsulatedMessage.

13.2.4.8 Procedure

The following clause illustrates the message flow between the two SEPPs with modifications from cIPX and pIPX.

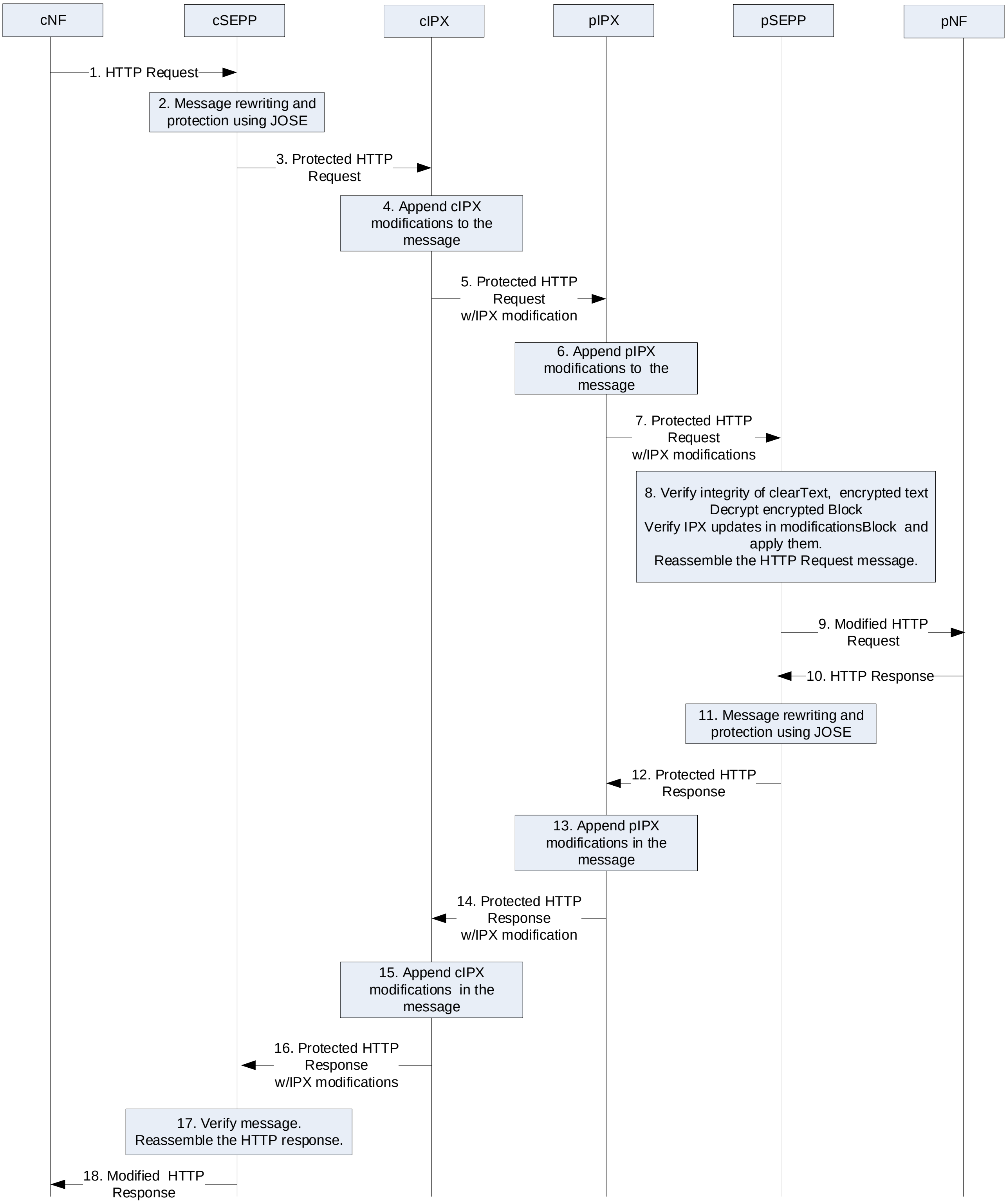
cNF
cSEPP
cIPX
pIPX
pSEPP
pNF
1. HTTP Request
2. Message rewriting and protection using JOSE
3. Protected HTTP Request
4. Append cIPX modifications to the message
5. Protected HTTP Request w/IPX modification
6. Append pIPX modifications to the message
7. Protected HTTP Request w/IPX modifications
8. Verify integrity of clearText, encrypted text Decrypt encrypted Block Verify IPX updates in modificationsBlock and apply them. Reassemble the HTTP Request message.
9. Modified HTTP Request
10. HTTP Response
11. Message rewriting and protection using JOSE
12. Protected HTTP Response
13. Append pIPX modifications in the message
14. Protected HTTP Response w/IPX modification
15. Append cIPX modifications in the message
16. Protected HTTP Response w/IPX modifications
17. Verify message. Reassemble the HTTP response.
18. Modified HTTP Response

Figure 13.2.4.8-1 Message flow between two SEPPs

1. The cSEPP receives an HTTP request message from a network function.

2. The cSEPP shall begin reformating the HTTP Request message

    a. Generating blocks for integrity protected data and encrypted data, and protecting them:

The cSEPP encapsulates the HTTP request into a clearTextEncapsulatedMessage block containing the following child JSON objects:

- Pseudo_Headers
- HTTP_Headers with one element per header of the original request.
- Payload that contains the message body of the original request.

For each attribute that requires e2e encryption between two SEPPs, the attribute value is copied into a dataToIntegrityProtectAndCipher JSON object and the attribute's value in the clearTextEncapsulatedMessage is replaced by the index of attribute value in the dataToIntegrityProtectAndCipher block.

A metadata block is created that contains the N32-f context Id, Message Id generated by SEPP for this request/response transaction and next hop identity.

The cSEPP protects dataToIntegrityProtect block and dataToIntegrityProtectAndCipher block as per clause 13.2.a.4. This results in a single JWE object representing the protected HTTP Request message.

b. Generating payload for the SEPP to SEPP HTTP message

The JWE/JWS becomes the payload of the new HTTP message generated by cSEPP.

3. The cSEPP shall use HTTP POST to send the HTTP message to the first intermediary.
4. The first intermediary (e.g. visited network's IPX provider) creates a new modifiedDataToIntegrityProtect JSON object with three elements:

a. The operations JSON element contains modifications performed by the first intermediary as per RFC 6902[64].

b. The intermediary includes its own identity in the Identity field of the patchRequest element.

c. The "tag" element, present in the JWE object generated by cSEPP, is copied into the modifiedDataToIntegrityProtect object. This acts as a replay protection for updates made by the first intermediary.

The intermediary executes JWS on the modifiedDataToIntegrityProtect JSON object and appends to the message.

5. The first intermediary sends the modified HTTP message request to the second intermediary (home network's IPX) as in step 3.
6. The second intermediary performs further modifications if required. The second intermediary executes JWS on the modifiedDataToIntegrityProtect JSON object and appends it to the message.
7. The second intermediary sends the modified HTTP message to pSEPP as in step 3.

Note: The behaviour of the intermediaries is not normative, but the hSEPP assumes that behaviour for processing the resulting request.

8. The pSEPP receives the message and does the following:

- It extracts the serialized values from the components of the JWE object.
- Invokes JWE decrypt function to check the integrity of the message and decrypt the dataToIntegrityProtectAndCipher block. This results in entries in the encrypted block becoming visible in cleartext.
- The pSEPP updates the clearTextEncapsulationMessage block in the message by replacing the references to the dataToIntegrityProtectAndCipher block with the referenced decrypted values from the dataToIntegrityProtectAndCipher block.
- It then verifies IPX provider updates of the attributes in the modificationsArray. It checks whether the modifications performed by the intermediaries were permitted by policy.
- The modified values of the attributes are updated in the clearTextEncapsulationMessage in order.

The pSEPP re-assembles the full HTTP Request from the contents of the clearTextEncapsulationMessage.

9. The pSEPP shall send the HTTP request resulting from step 8 to the home network's NF.

10.-18.These steps are analogous to steps 1.-9.

13.2.4.9 JOSE profile

SEPPs shall follow the JWE profile defined in TS 33.210 with the restriction that it shall only use AES GCM with a 128-bit or 256-bit key.

SEPPs and IPXs shall follow the JWS profile as defined in TS 33.210 with the restriction that it shall only use ES256 algorithm.

13.3 Authentication and static authorization

13.3.1 Authentication and authorization between network functions and the NRF

NRF and NF shall authenticate each other during discovery, registration, and access token request. If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.

If the PLMN does not use protection at the transport layer, mutual authentication of NRF and NF may be implicit by NDS/IP or physical security (see clause 13.1).

When NRF receives message from unauthenticated NF, NRF shall support error handling, and may send back an error message. The same procedure shall be applied vice versa.

After successful authentication between NRF and NF, the NRF shall decide whether the NF is authorized to perform discovery and registration.

In the non-roaming scenario, the NRF authorizes the Nnrf_NFDiscovery_Request based on the profile of the expected NF/NF service and the type of the NF service consumer, as described in clause 4.17.4 of TS23.502 [8].In the roaming scenario, the NRF of the NF Service Provider shall authorize the Nnrf_NFDiscovery_Request based on the profile of the expected NF/NF Service, the type of the NF service consumer and the serving network ID.

If the NRF finds NF service consumer is not allowed to discover the expected NF instances(s) as described in clause 4.17.4 of TS 23.502[8], NRF shall support error handling, and may send back an error message.

NOTE 1: When a NF accesses any services (i.e. register, discover or request access token) provided by the NRF , the OAuth 2.0 access token for authorization between the NF and the NRF is not needed.

13.3.2 Authentication and authorization between network functions

Authentication between network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between NFs.
- If the PLMN does not use protection at the transport layer, authentication between NFs within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

When an NF receives message from other unauthenticated NF, the NF shall support error handling, and may send back an error message.

If the PLMN uses token-based authorization, the network shall use protection at the transport layer as described in clause 13.1.

Depending on whether token-based authorization is used or not, authentication between network functions shall be performed in one of the following ways:

- If token-based authorization is used within one PLMN, the service consumer NF shall authenticate the service producer NF at transport layer before trying to access the service API. The service producer NF may authenticate the service consumer NF at transport layer.

NOTE 1: Authentication of the service consumer NF towards the service producer NF will be implicit by authorization, which can only be granted after successful authentication of the service consumer NF towards the NRF.

- If token-based authorization is not used within one PLMN, service consumer NF and service producer NF shall mutually authenticate before performing access to the service API. The service producer NF shall additionally check authorization of the service consumer NF based on local policy before granting access to the service API.

NOTE 2: Authentication between network functions in different PLMN is implicit by authentication between NF-SEPP as in clause 13.3.3, SEPP-SEPP as in clause 13.2 and SEPP-NF as in clause 13.3.3.

When local policy check is failed, NF service provider shall support error handling, and may send back an error message

13.3.3 Authentication and authorization between SEPP and network functions

NOTE 1: This clause also describes authentication and authorization between SEPP and NRF, because the NRF is a network function.

Authentication between SEPP and network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between SEPP and NFs.

- If the PLMN does not use protection at the transport layer, authentication between SEPP and NFs within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

A network function and the SEPP shall mutually authenticate before the SEPP forwards messages sent by the network function to network functions in other PLMN.

13.3.4 Authentication and authorization between SEPPs

Authentication and authorization between SEPPs in different PLMN is defined in clause 13.2.

13.4 Authorization of NF service access

13.4.1 OAuth 2.0 based authorization of Network Function service access

13.4.1.0 General

The authorization framework uses the OAuth 2.0 framework as specified in [43]. Grants shall be of the type Client Credentials Grant, as described in clause 4.4. of [43]. Access tokens shall be JSON Web Tokens as described in [44] and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in [45].

The authorization framework described in clause 13.4.1 is mandatory to support for NRF and NF.

13.4.1.1 Service access authorization within the PLMN

OAuth 2.0 roles, as defined in clause 1.1 of [43], are as follows:

a. The Network Resource Function (NRF) shall be the OAuth 2.0 Authorization server.

b. The NF service consumer shall be the OAuth 2.0 client.

c. The NF service producer shall be the OAuth 2.0 resource server.

OAuth 2.0 client (NF service consumer) registration with the OAuth 2.0 authorization server (NRF)

The NF service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], shall be used to register the OAuth 2.0 client (NF service consumer) with the OAuth 2.0 Authorization server (NRF), as described in clause 2.0 of [43]. The client id, used during OAuth 2.0 registration, shall be the NF Instance Id of the NF.

Access token request before service access

The following procedure describes how the NF service consumer obtains an access token before service access to NF service producers of a specific NF type.

Pre-requisite:

a. The NF Service consumer (OAuth2.0 client) is registered with the NRF (Authorization Server).

b. The NRF and NF service producer share the required credentials when token validation is performed by the NF service producer.

c. The NRF and NF have mutually authenticated each other.

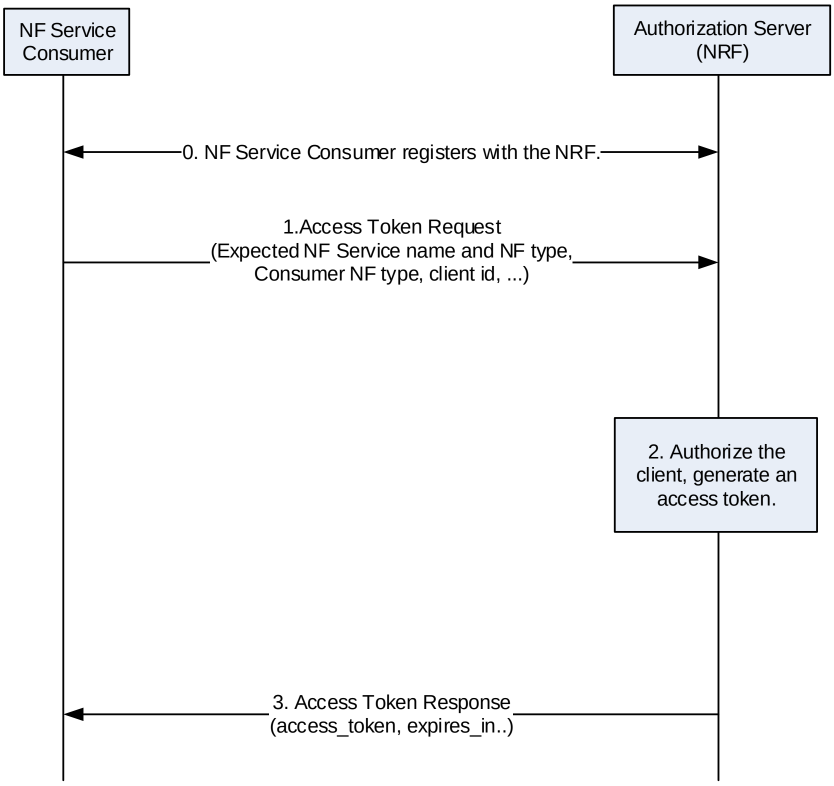
NF Service Consumer
Authorization Server (NRF)
0. NF Service Consumer registers with the NRF.
1.Access Token Request (Expected NF Service name and NF type, Consumer NF type, client id, ...)
2. Authorize the client, generate an access token.
3. Access Token Response (access_token, expires_in..)

Figure 13.4.1.1-1: NF service consumer obtaining access token before NF service access

1. The NF service consumer requests an access token from the NRF in the same PLMN using the Nnrf_AccessToken_Get request operation. The message includes the NF Instance Id of the NF service consumer, expected NF service name(s), NF type of the expected NF producer instance and NF consumer.

2. The NRF optionally authorizes the NF service consumer. It shall then generate an access token with appropriate claims included. The NRF shall digitally sign the generated access token based on a shared secret or private key as described in [45].

   The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF type of the producers (audience), expected service name(s) (scope) and expiration time (expiration).

3. If the authorization is success,the NRF sends access token to the NF service consumer in the Nnrf_AccessToken_Get response operation. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC6749[43].

Editor's Note: The service names need to be aligned with CT4 definitions in TS 29.510

Access token request for a specific NF Producer/NF Producer service instance

The NF service consumer shall request an access token from the NRF for a specific NF Producer instance/NF Producer service instance. The request includes the NF Instance Id of the requested NF Producer, the expected NF service name and NF Instance Id of the NF service consumer.

The NRF optionally authorizes the NF service consumer to use the requested NF Producer instance/NF Producer service instance, and then proceeds to generate an access token with the appropriate claims included.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF Instance Id of the requested NF Service Producer (audience), service name (scope) and expiration time (expiration). The token is included in the Nnrf_AccessToken_Get response sent to the NF service consumer.

Service access request based on token verification

The following figure and procedure describe how authorization is performed during Service request of the NF service consumer.

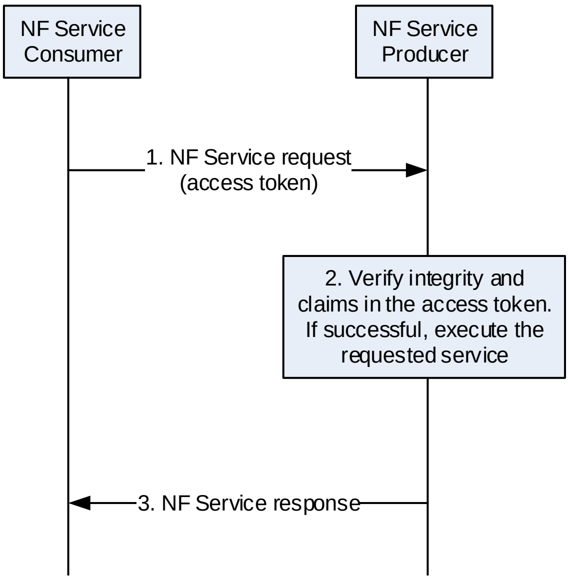
NF Service Consumer
NF Service Producer
1. NF Service request (access token)
2. Verify integrity and claims in the access token. If successful, execute the requested service
3. NF Service response

Figure 13.4.1.1-2: NF service consumer requesting service access with an access token

Pre-requisite: The NF service consumer is in possession of a valid access token before requesting service access from the NF Service producer.

1. The NF Service consumer requests service from the NF service producer. The NF Service Consumer includes the access token.

   The NF Service consumer and NF service producer authenticate each other following clause 13.3.

2. The NF Service producer verifies the token as follows::

   - The NF Service producer verifies the integrity of the token by verifying the signature using NRF's public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service producer verifies the claims in the token as follows:

- It checks that the identity of the issuer of the access token (NRF) in the issuer claim in the access token, matches the subject in the NRF certificate.
- It checks that the subject claim within the access token, matches the subject in the NF consumer certificate.

NOTE: This can be done only in intra-PLMN scenarios where NF consumer and NF producer mutually authenticate each other with TLS certificates (clause 13.3.2).

- It checks that the audience claim in the access token matches its own identity or the type of NF service producer.
- If scope is present, it checks that the scope matches the requested service operation.
- It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

3. If the verification is successful, the NF Service producer executes the requested service and responds back to the NF Service consumer. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC6749 [43].

13.4.1.2 Service access authorization in roaming scenarios

In the roaming scenario, OAuth 2.0 roles are as follows:

a. The visiting Network Resource Function (vNRF) shall be the OAuth 2.0 Authorization server for vPLMN and authenticates the NF service consumer.

b. The home Network Resource Function (hNRF) shall be OAuth 2.0 Authorization server for hPLMN and generates the access token.

c. The NF service consumer in the visiting PLMN shall be the OAuth 2.0 client.

d. The NF service producer in the home PLMN shall be the OAuth 2.0 resource server.

OAuth 2.0 client (NF service consumer) registration with the OAuth 2.0 authorization server (NRF)

Same as in the non-roaming scenario in 13.4.1.1.

Obtaining access token independently before NF service access

The following procedure describes how the NF service consumer obtains an access token for NF service producers of a specific NF type for use in the roaming scenario.

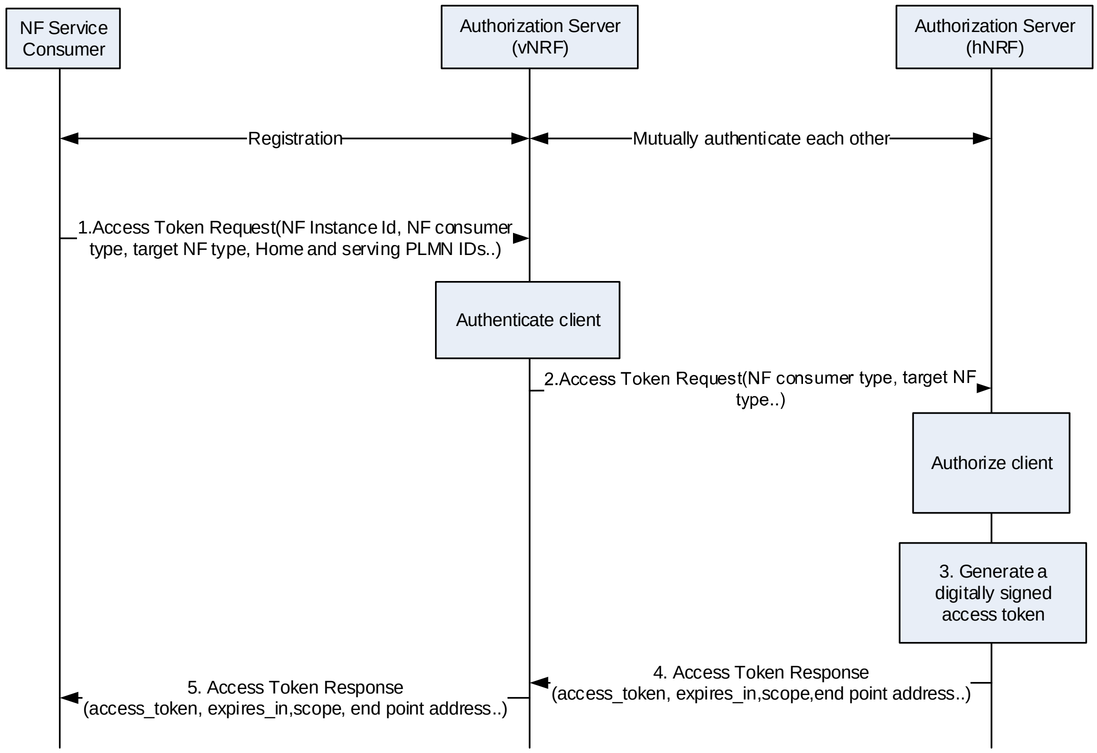
NF Service Consumer
Authorization Server (vNRF)
Authorization Server (hNRF)
Registration
Mutually authenticate each other
1.Access Token Request(NF Instance Id, NF consumer type, target NF type, Home and serving PLMN IDs..)
Authenticate client
2.Access Token Request(NF consumer type, target NF type..)
Authorize client
3. Generate a digitally signed access token
4. Access Token Response (access_token, expires_in,scope,end point address..)
5. Access Token Response (access_token, expires_in,scope, end point address..)

Figure 13.4.1.2-1: NF service consumer obtaining access token before NF service access (roaming)

Pre-requisite:

a. The NF Service consumer (OAuth2.0 client) is registered with the NRF (Authorization Server).

b. The NRF and NF service producer share the required credentials when token validation is performed by the NF service producer.

c. The two NRFs have mutually authenticated each other.

d. The NRF in the serving PLMN and NF service consumer have mutually authenticated each other.

1. The NF service consumer invokes Nnrf_AccessToken_Get Request (NF Instance Id of the NF service consumer, expected NF service Name (s), NF Type of the expected NF Producer instance, NF type of the NF consumer, home and serving PLMN IDs) from NRF in the same PLMN.

2. The NRF in serving PLMN identifies the NRF in home PLMN (hNRF) based on the home PLMN ID, and requests token from hNRF as described in clause 4.17.5 of [8]. The vNRF forwards the parameters it obtained from the NF service consumer, including NF service consumer type, to the hNRF.

3. The hNRF optionally authorizes the NF service consumer and shall generate an access token with appropriate claims included. The hNRF shall digitally sign the generated access token based on a shared secret or private key as described in [45].

   The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF type of the NF Service Producer (audience), expected services name(s) (scope) and expiration time (expiration).

4. If the authorization is success, the access token is included in Nnrf_AccessToken_Get Response message to the vNRF. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC6749 [43].

5. The vNRF forwards the Nnrf_AccessToken_Get Response or error message to the NF service consumer.

Editor’s Note: The service names need to be aligned with CT4 definitions in TS 29.510

Obtain access token for a specific NF Producer/NF Producer service instance

The NF service consumer shall request an access token from the NRF for a specific NF Producer instance/NF Producer service instance. The request includes the NF Instance Id of the requested NF Producer, the expected NF service name and NF Instance Id of the NF service consumer.

The NRF in the visiting PLMN forwards the request to the NRF in the home PLMN

The NRF optionally authorizes the NF service consumer to use the requested NF Producer instance/NF Producer service instance, and then proceeds to generate an access token with the appropriate claims included.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF Instance Id of the requested NF Service Producer (audience), service name (scope) and expiration time (expiration). The token is included in the Nnrf_AccessToken_Get response sent to the NRF in the visiting PLMN. The NRF in the visiting PLMN forwards the Nnrf_AccessToken_Get response message to the NF service consumer.

Service access request based on token verification

Same as in the non-roaming scenario in 13.4.1.1.

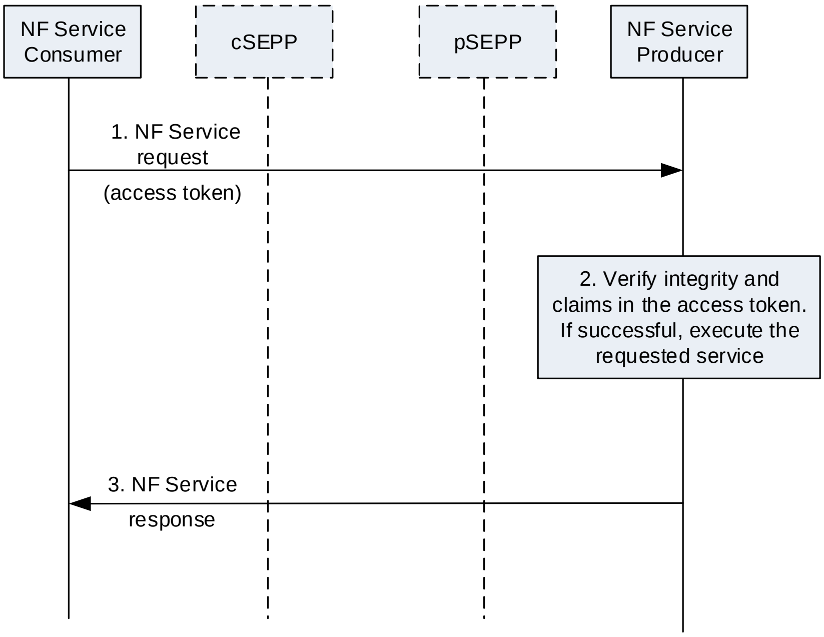

Figure 13.4.1.2-2: NF service consumer requesting service access with an access token in roaming case

13.5 Security capability negotiation between SEPPs

The security capability negotiation allows the SEPPs to negotiate which security mechanism to use for protecting NF service related signalling over N32. There shall be an agreed security mechanism between a pair of SEPPs before conveying NF service related signalling over N32.

When a SEPP notices that it does not have an agreed security mechanism for N32 protection with a peer SEPP or if the security capabilities of the SEPP have been updated, the SEPP shall perform security capability negotiation with the peer SEPP in order to determine, which security mechanism to use for protecting NF service related signalling over N32. Certificate based authentication shall follow the profiles given in 3GPP TS 33.310 [17], clauses 6.1.3a and 6.1.4a.

A mutually authenticated TLS connection as defined in clause 13.1 shall be used for protecting security capability negotiation over N32. The TLS connection shall provide integrity, confidentiality and replay protection.

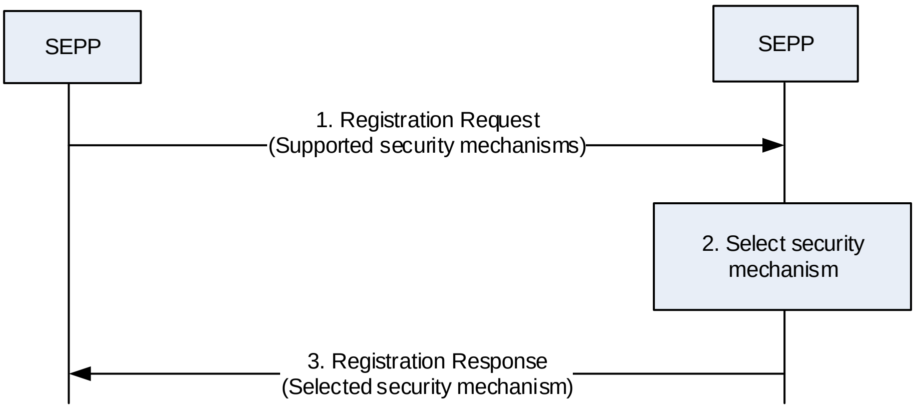
SEPP
SEPP
1. Registration Request
(Supported security mechanisms)
2. Select security mechanism
3. Registration Response
(Selected security mechanism)

Figure 13.5-1 Security capability negotiation

1. The SEPP which initiated the TLS connection sends a Registration Request message to the responding SEPP including the initiating SEPP's supported security mechanisms for protecting the NF service related signalling over N32 (see table 9.3.1.X-1). The security mechanisms are ordered in initiating SEPP's priority order.

2. The responding SEPP compares the received security capabilities to its own supported security capabilities and selects, based on its local policy, a security mechanism, which is supported by both initiating SEPP and responding SEPP.

3. The responding SEPP sends a Registration Response message to initiating SEPP including selected security mechanism for protecting the NF service related signalling over N32.

Editor's Note: The exact message names are FFS.

Table 13.5-1: NF service related signalling traffic protection mechanisms over N32

N32 protection mechanism	Description
Mechanism 1	N32 Application Layer Secuity
Mechanism 2	TLS
Mechanism n	Reserved

If the selected security mechanism is N32 Application Layer Security the SEPPs shall behave as specified in clause 13.2.

If the selected security mechanism is TLS (i.e. there are no IPX entities between the SEPPs) the SEPPs shall forward the NF service related signalling over N32 using the existing TLS connection as specified in clause 13.1.

If the selected security mechanism is based on a mechanism other than the ones specified in Table 13.5-1, the two SEPPs shall terminate the TLS connection.

14 Security related services

14.1 Services provided by AUSF

14.1.1 General

The AUSF provides UE authentication service to the requester NF by Nausf_UEAuthentication. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. Clause 9.6.2 describes the Nausf_UEAuthentication_Authenticate service operation. The services listed here are used in procedures that are described in clause 6 of the present document.

Since AUSF is completely security-related, all service operations are described in the present document. TS 23.501 [2], clause 7.2.7, only lists the services and TS 23.502 [8], clause 5.2.10, provides the reference to the present document.

14.1.2 Nausf_UEAuthentication service

Service operation name: Nausf_UEAuthentication_authenticate.

Description: Authenticate the UE and provides related keying material.

Input, Required: One of the options below.

1. In the initial authentication request: SUPI or SUCI, serving network name.
2. In the subsequent authentication requests depending on the authentication method:
   a. 5G AKA: Authentication confirmation message with RES* as described in clause 6.1.3.2 or Synchronization Failure indication and related information (i.e. RAND/AUTS).

   b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

Input, Optional: None.

Output, Required: One of the options below.

1. Depending on the authentication method:
   a. 5G AKA: authentication vector, as described in clause 6.1.3.2 or Authentication confirmation acknowledge message.

   b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.
2. Authentication result and if success the master key which are used by AMF to derive NAS security keys and other security key(s).

Output, Optional: SUPI if the authentication was initiated with SUCI.

14.1.3 Nausf_SoRProtection service

The following table illustrates the security related services for SoR that AUSF provides.

Table 14.1.3-1: NF services for SoR provided by AUSF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nausf_SoRProtection	Protect	Request/Response	UDM

Service operation name: Nausf_SoRProtection.

Description: The AUSF calculates the SoR-MAC-I$_{AUSF}$ as specified in the Annex A.17 of this document using UE specific home key (K$_{AUSF}$) along with the steering information received from the requester NF and delivers the SoR-MAC-I$_{AUSF}$ and Counter$_{SoR}$ to the requester NF. If the ACK indication is set to ‘true’ by the UDM in the SoR Header, then the AUSF shall compute the SoR-XMAC-I$_{UE}$ and return the computed SoR-XMAC-I$_{UE}$ in the response. The details of the SoR header is specified in TS 24.501 [35].

Input, Required: Requester ID, SUPI, service name, list of preferred PLMN/access technology combinations or 0x00, ACK indication.

Input, Optional: None.

Output, Required: SoR-MAC-I$_{AUSF}$, Counter$_{SoR}$ or error (counter_wrap).

Output, Optional: SoR-XMAC-I$_{UE}$ (if ACK indication is set to ‘true’ in the Input, then the SoR-XMAC-I$_{UE}$ shall be computed and returned).

14.2 Services provided by UDM

14.2.1 General

UDM provides within Nudm_UEAuthentication service all authentication-related service operations, which are Nudm_UEAuthentication_Get (clause 9.7.2.1) and Nudm_UEAuthentication_ResultConfirmation (clause 9.7.2.2).

The complete list of UDM services is defined in TS 23.501 [2], clause 7.5.1, and further refined in TS 23.502 [8], clause 5.2.3.1.

14.2.2 Nudm_UEAuthentication_Get service operation

Service operation name: Nudm_UEAuthentication_Get

Description: Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

Inputs, Required: SUPI or SUCI, serving network name.

Inputs, Optional: Synchronization Failure indication and related information (i.e. RAND/AUTS).

Outputs, Required: Authentication method and corresponding authentication data for a certain UE as identified by SUPI or SUCI input.

Outputs, Optional: SUPI if SUCI was used as input.

14.2.3 Nudm_UEAuthentication_ResultConfirmation service operation

Service operation name: UEAuthentication_ResultConfirmation

Description: Requester NF informs UDM about the result of an authentication procedure with a UE.

Inputs, Required: SUPI, timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

Inputs, Optional: None.

Outputs, Required: None.

Outputs, Optional: None.

14.3 Services provided by NRF

14.3.1 General

NRF provides within Nnrf_OAuth2Auth services, which includes Nnrf_OAuth2Auth_AccessTokenGet (clause 13.4.1.1) and Nnrf_OAuth2Auth_AccessTokenAuthorization(clause 13.4.1.1) two service operation.

The following table illustrates the security related services for OAuth 2.0 that NRF provides.

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnrf_AccessToken	Get	Request/Response	AMF, SMF, PCF, NEF, NSSF, SMSF, AUSF

The complete list of NRF services is defined in TS 23.501 [2], clause 7.2.6, and further refined in TS 23.502 [8], clause 5.2.7.

14.3.2 Nnrf_AccessToken_Get Service Operation

Service Operation name: Nnrf_ AccessToken_Get.

Description: NF consumer request NRF to provide Access Token.

Known NF Consumers: AMF, SMF, PCF, NEF, NSSF, SMSF, and AUSF.

Inputs, Required: the NF Instance Id of the NF service consumer, expected NF service name(s), NF types of the expected NF producer instance and NF consumer.

Inputs, Optional: Home and serving PLMN IDs.

Outputs, Required: Access Token with appropriate claims, where the claims shall include NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF type of the producers (audience), expected service name (scope) and expiration time (expiration).

Outputs, Optional: None.

15 Management security for network slices

15.1 General

The creation, modification, and termination of a Network Slice Instance (NSI) is part of the Management Services provided by the 5G management systems. A management service is accessed by management service consumers via standardized service interfaces given in 3GPP TS 28.533 [54]. The typical service consumers for the above NSI provisioning and NSI provisioning exposure are operators and vertical industry respecitively, as described in 3GPP TS 28.531 [55]. These management services are securely protected through mutual authentication and authorization below.

15.2 Mutual authentication

If a management service consumer resides outside the 3GPP operator's trust domain, mutual authentication shall be performed between the management service consumer and the management service producer using TLS, based on either 1) the client and server certificates with the profiles given in 3GPP TS 33.310 [17], clauses 6.1.3a and 6.1.4a or 2) pre-shared keys with TLS-PSK following RFC 4279 [56]. The structure of the PKI used for the certificates is out of scope of the present document. The key distribution of TLS-PSK is up to the operator's security policy and out of scope of the present document.

15.3 Protection of management interactions between the management service consumer and the management service producer

TLS shall be used to provide integrity protection, replay protection and confidentiality protection for the interface between the management service producer and the management service consumer residing outside the 3GPP operator's trust domain. Security profiles for TLS implementation and usage shall follow the provisions given in TS 33.310 [17], Annex E.

15.4 Authorization of management service consumer's request

After the mutual authentication, the management service producer determines whether the management service consumer is authorized to send requests to the management service producer. The management service producer shall authorize the requests from the management service consumer using the one of the following two options: 1) OAuth-based authorization mechanism following RFC 6749 [43]; 2) based on the local policy of the management service producer.

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

A.1.1 General

All key derivations (including input parameter encoding) for 5GC shall be performed using the key derivation function (KDF) specified in TS 33.220 [28]. This clause specifies how to construct the input string, S, to the KDF (which is input together with the relevant key). For each of the distinct usages of the KDF, the input parameters S are specified below.

A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [28], FC values allocated for the present document are in range of 0x69 – 0x76.

A.2 K_{AUSF} derivation function

This clause applies to 5G AKA only.

When deriving a K_{AUSF} from CK, IK and the serving network name when producing authentication vectors, and when the UE computes K_{AUSF} during 5G AKA, the following parameters shall be used to form the input S to the KDF.

- FC = 0x6A,
- P0 = serving network name,
- L0 = length of the serving network name (variable length as specified in 24.501 [35]),
- P1 = SQN ⊕ AK
- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06)

The exclusive or of the Sequence Number (SQN) and the Anonymity Key (AK) is sent to the UE as a part of the Authentication Token (AUTN), see TS 33.102. If AK is not used, AK shall be treated in accordance with TS 33.102, i.e. as 000…0.

The serving network name shall be equal to the concatenation of the service code set to '5G' and the SN Id according to sub-clause 6.1.1.4 "Construction of serving network name".

The input key KEY shall be equal to the concatenation CK || IK of CK and IK.

A.3 CK' and IK' derivation function

When deriving a CK' and IK' , the KDF of TS 33.402 [11] clause A.2 shall be used with the following exception: the serving network name shall be used as the value of access network identity (P0).

The serving network name shall be equal to the concatenation of the service code set to '5G' and the SN Id according to sub-clause 6.1.1.4 "Construction of serving network name".

A.4 RES* and XRES* derivation function

When deriving RES* from RES, RAND, and serving network name in the UE and when deriving XRES* from XRES, RAND, and the serving network name in the ARPF, the following parameters shall be used to form the input S to the KDF.

- FC = 0x6B,
- P0 = serving network name,
- L0 = length of the serving network name (variable length as specified in 24.501 [35]),
- P1 = RAND,
- L1 = length of RAND (i.e. 0x00 0x10) ,
- P2 = RES or XRES,
- L2 = length RES or XRES (i.e. variable length between 0x00 0x04 and 0x00 0x10) .

The input key Key shall be equal to the concatenation CK || IK of CK and IK.

The serving network name shall be equal to the concatenation of the service code set to '5G' and the SN Id according to sub-clause 6.1.1.4 "Construction of serving network name".

The (X)RES* is identified with the 128 least significant bits of the output of the KDF.

A.5 HRES* and HXRES* derivation function

When deriving HRES* from RES* in the SEAF and when deriving HXRES* from XRES* in the AUSF the following parameters shall be used to form the input S to the SHA-256 hashing algorithm:

- P0 = RAND,
- P1 = XRES*,

The input S shall be equal to the concatenation P0||P1 of the P0 and P1.

The H(X)RES* is identified with the 128 least significant bits of the output of the SHA-256 function.

A.6 K_{SEAF} derivation function

When deriving a K_{SEAF} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x6C,
- P0 = <serving network name>,
- L0 = length of <serving network name>

Editor's note: It is FFS if other parameters are needed.

The input key KEY shall be K_{AUSF}.

A.7 K_{AMF} derivation function

A.7.0 Parameters for the input S to the KDF

When deriving a K_{AMF} from K_{SEAF} the following parameters shall be used to form the input S to the KDF.

- FC = 0x6D

- P0 =SUPI,
- L0 = length of SUPI
- P1 = ABBA parameter
- L1 = length of ABBA parameter

The input key KEY shall be the 256-bit K_{SEAF}.

For ABBA parameter values please refer to clause A.7.1.

A.7.1 ABBA parameter values

ABBA parameter is provided to the UE from SEAF and shall be used as an input parameter for KAMF derivation. To support flexible set of security features ABBA parameter is defined when security features change. To ensure forward compatibility, the ABBA parameter is a variable length parameter.

The SEAF shall set the ABBA parameter to 0x0000. The UE shall use the ABBA parameter provided by the SEAF in the calculation of K_{AMF}.

The following values have been defined for this parameter.

ABBA parameter value	Description
0x0000	Initial set of security features defined for 5GS.

Table A.7.1-1: ABBA parameter definitions

A.8 Algorithm key derivation functions

When deriving keys for NAS integrity and NAS encryption algorithms from K_{AMF} in the AMF and UE or ciphering and integrity keys from K_{gNB} in the gNB and UE, the following parameters shall be used to form the string S.

- FC = 0x69
- P0 = algorithm type distinguisher
- L0 = length of algorithm type distinguisher (i.e. 0x00 0x01)
- P1 = algorithm identity
- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm type distinguisher shall be N-NAS-enc-alg for NAS encryption algorithms and N-NAS-int-alg for NAS integrity protection algorithms. The algorithm type distinguisher shall be N-RRC-enc-alg for RRC encryption algorithms, N-RRC-int-alg for RRC integrity protection algorithms, N-UP-enc-alg for UP encryption algorithms and N-UP-int-alg for UP integrity protection algorithms (see table A.8-1). The values 0x00 and 0x07 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

Table A.8-1: Algorithm type distinguishers

Algorithm distinguisher	Value
N-NAS-enc-alg	0x01
N-NAS-int-alg	0x02
N-RRC-enc-alg	0x03
N-RRC-int-alg	0x04
N-UP-enc-alg	0x05
N-UP-int-alg	0x06

The algorithm identity (as specified in clause 5) shall be put in the four least significant bits of the octet. The two least significant bits of the four most significant bits are reserved for future use, and the two most significant bits of the most significant nibble are reserved for private use. The entire four most significant bits shall be set to all zeros.

For the derivation of integrity and ciphering keys used between the UE and gNB, the input key shall be the 256-bit K_{gNB}. For the derivation of integrity and ciphering keys used between the UE and AMF, the input key shall be the 256-bit K_{AMF}.

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

A.9 K_{gNB} and K_{N3IWF} derivation function

When deriving a K_{gNB} from K_{AMF} and the uplink NAS COUNT in the UE and the AMF the following parameters shall be used to form the input S to the KDF.

- FC = 0x6E
- P0 = Uplink NAS COUNT
- L0 = length of uplink NAS COUNT (i.e. 0x00 0x04)
- P1 = Access type distinguisher
- L1 = length of Access type distiguisher (i.e. 0x00 0x01)

The values for the access type distinguisher are defined in table A.9-1. The values 0x00 and 0x03 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

The access type distinguisher shall be set to the value for 3GPP (0x01) when deriving KgNB. The access type distinguisher shall be set to the value for non-3GPP (0x02) when deriving K_{N3IWF}.

Table A.9-1: Access type distinguishers

Access type distinguisher	Value
3GPP access	0x01
Non 3GPP access	0x02

The input key KEY shall be the 256-bit K_{AMF}.

This function is applied when cryptographically protected 5G radio bearers are established and when a key change on-the-fly is performed.

A.10 NH derivation function

When deriving a NH from K_{AMF} the following parameters shall be used to form the input S to the KDF.

- FC = 0x6F
- P0 = SYNC-input
- L0 = length of SYNC-input (i.e. 0x00 0x20)

The SYNC-input parameter shall be the newly derived K_{gNB} for the initial NH derivation, and the previous NH for all subsequent derivations. This results in a NH chain, where the next NH is always fresh and derived from the previous NH.

The input key KEY shall be the 256-bit K_{AMF}.

A.11 K_{NG-RAN}* derivation function for target gNB

When deriving a K_{NG-RAN}* from current K_{gNB} or from fresh NH and the target physical cell ID in the UE and NG-RAN for handover purposes the following parameters shall be used to form the input S to the KDF.

- FC = 0x70
- P0 = PCI (target physical cell id)
- L0 = length of PCI (i.e. 0x00 0x02)
- P1 = ARFCN-DL (target physical cell downlink frequency)
- L1 = length of ARFCN-DL

The input key KEY shall be the 256-bit NH when the index in the handover increases, otherwise the current 256-bit K_{gNB}(when source is gNB) or K_{eNB} (when source is ng-eNB).

A.12 K_{NG-RAN}* derivation function for target ng-eNB

When deriving a K_{NG-RAN}* from current K_{gNB} or from fresh NH and the target physical cell ID in the UE and NG-RAN for handover purposes the following parameters shall be used to form the input S to the KDF.

- FC = 0x71
- P0 = PCI (target physical cell id)
- L0 = length of PCI (i.e. 0x00 0x02)
- P1 = EARFCN-DL (target physical cell downlink frequency)
- L1 = length of EARFCN-DL (i.e. 0x00 0x03)

The input key KEY shall be the 256-bit NH when the index in the handover increases, otherwise the current 256-bit K_{gNB} (when source is gNB) or K_{eNB} (when source is ng-eNB)K_{gNB}.

A.13 K_{AMF} to K_{AMF}' derivation in mobility

Derivation of K_{AMF}' from K_{AMF} during mobility shall use the following input parameters.

- FC = 0x72
- P0 = DIRECTION
- L0 = length of DIRECTION (i.e. 0x00 0x01)
- P1 = COUNT,
- L1 = length of COUNT (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

When K_{AMF}' is derived in handover, DIRECTION shall be 0x01 and COUNT shall be the downlink NAS COUNT of the 3GPP access.

When K_{AMF}' is derived in idle mode mobility (i.e., mobility registration update), DIRECTION shall be 0x00 and COUNT shall be the uplink NAS COUNT of the 3GPP access used in the Registration Request.

A.14 K_{AMF} to K_{ASME}' derivation for interworking

A.14.1 Idle mode mobility

This input string is used when there is a need to derive K'_{ASME} from K_{AMF} during mapping of security contexts from 5G to EPS at idle mode mobility. The following input parameters shall be used.

- FC = 0x73
- P0 = NAS Uplink COUNT value
- L0 = length of NAS Uplink COUNT value (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

A.14.2 Handover

This input string is used when there is a need to derive K_{ASME}' from K_{AMF} during mapping of security contexts from 5G to EPS at handovers. The following input parameters shall be used.

- FC = 0x74
- P0 = NAS Downlink COUNT value
- L0 = length of NAS Downlink COUNT value (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

A.15 K_{ASME} to K_{AMF}' derivation for interworking

A.15.1 Idle mode mobility

This input string is used when there is a need to derive K_{AMF}' from K_{ASME} during mapping of security contexts from EPS to 5G at idle mode mobility. The following input parameters shall be used.

- FC = 0x75
- P0 = NAS Uplink COUNT value
- L0 = length of NAS Uplink COUNT value (i.e. 0x00 0x04)

The input key KEY shall be K_{ASME}.

A.15.2 Handover

This input string is used when there is a need to derive K_{AMF}' from K_{ASME} during mapping of security contexts from EPS to 5G at handovers. The following input parameters shall be used.

- FC = 0x76
- P0 = NH value
- L0 = length of NH value (i.e. 0x00 0x20)

The input key KEY shall be K_{ASME}.

A.16 Derivation of K_{SN} for dual connectivity

This input string is used when the MN and UE derive K_{SN} during dual connectivity. The following input parameters shall be used:

- FC = 0x79
- P0 = Value of the SN Counter as a non-negative integer
- L0 = length of the SN Counter value (i.e. 0x00 0x02)

The input KEY shall be $K_{ng\text{-}eNB}$ when the MN is an ng-eNB and K_{gNB} when the MN is a gNB.

A.17 SoR-MAC-I_{AUSF} generation function

When deriving a SoR-MAC-I_{AUSF} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x77,
- P0 = SoR header ,
- L0 = length of SoR header
- P1 = $Counter_{SoR}$
- L1 = length of $Counter_{SoR}$
- P2 = PLMN ID and access technology list
- L2 = length of PLMN ID and access technology list

The input key Key shall be K_{AUSF}.

PLMN ID and access technology list parameter is included for SoR-MAC-I_{AUSF} generation only if the value of the “List indication” is set to ‘1’ in the SoR Header (see TS 24.501[35]), otherwise P2 and L2 are not included.

The SoR-MAC-I_{AUSF} is identified with the 128 least significant bits of the output of the KDF.

A.18 SoR-MAC-I_{UE} generation function

When deriving a SoR-MAC-I_{UE} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x78,
- P0 = 0x01 (SoR Acknowledgement: Verified the Steering Information List successfully)
- L0 = length of SoR Acknowledgement (i.e. 0x00 0x01)
- P1 = $Counter_{SoR}$
- L1 = length of $Counter_{SoR}$

The input key Key shall be K_{AUSF}.

The SoR-MAC-I_{UE} is identified with the 128 least significant bits of the output of the KDF.

Annex B (informative): Using additional EAP methods for primary authentication

B.1 Introduction

The present annex describes an example of the usage of additional EAP methods for primary authentication in private networks using the 5G system as specified in TS 22.261 [7]. It is provided as an example on how the 5G authentication framework for primary authentication can be applied to EAP methods other than EAP-AKA' The additional EAP methods are only intended for private networks or with IoT devices in isolated deployment scenarios, i.e. roaming is not considered, as specified in TS 22.261 [7].

When the 5G system is deployed in private networks, the SUPI and SUCI should be encoded using the NAI format as specified in TS 23.501 [2]. UE always includes the realm part in the NAI for routing to the correct UDM.

B.2 Primary authentication and key agreement

B.2.1 EAP TLS

B.2.1.1 Security procedures

EAP-TLS is a mutual authentication EAP method that can be used by the EAP peer and the EAP server to authenticate each other. It is specified in RFC 5216 [38]. The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in TS 33.310 [5], and should be followed when EAP-TLS is used in 3GPP networks.

EAP-TLS supports several TLS versions, and the negotiation of the TLS version is part of EAP-TLS. The main principle of negotiation goes as follows. The EAP server indicates the support for EAP-TLS in the EAP-Request. If the peer chooses EAP-TLS, it responds with an EAP-Response indicating in the ClientHello message which TLS versions the peer supports. The EAP server chooses the TLS version, and indicates the chosen version in the ServerHello message.

The TLS procedure described in the RFC 5216 [38] is TLS 1.1 [39]. However, the use of TLS 1.1 is not recommended in 3GPP networks [5], and should be disabled also in the EAP server if EAP-TLS is used. A newer version, TLS 1.2 is defined in RFC 5246 [40]. The basic protocol procedures for TLS 1.1 and TLS 1.2 are the same. The major changes are in security capability, pseudorandom function (PRF) and cipher suites. The details of changes can be found in section 1.2 of RFC 5246. The EAP server should always choose the highest TLS version that is supported on both endpoints.

The procedure below is based on the unified authentication framework from the present document, procedures from TS 23.502 and RFC 5216 [38]. The procedure is presented here as an example, and other potential procedures are possible, e.g. if TLS resumption is used.

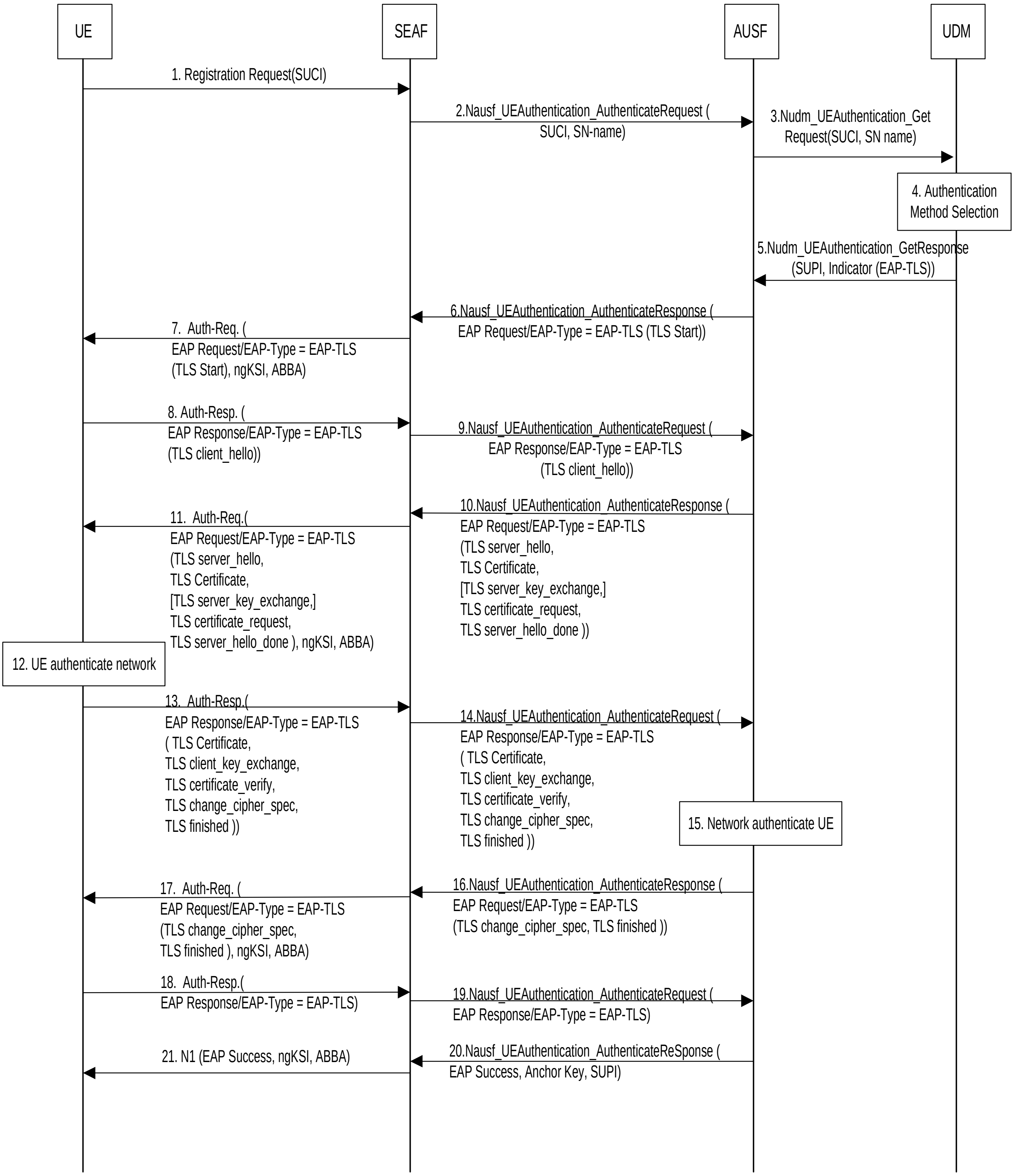
UE
SEAF
AUSF
UDM
1. Registration Request(SUCI)
2.Nausf_UEAuthentication_AuthenticateRequest (SUCI, SN-name)
3.Nudm_UEAuthentication_Get Request(SUCI, SN name)
4. Authentication Method Selection
5.Nudm_UEAuthentication_GetResponse (SUPI, Indicator (EAP-TLS))
6.Nausf_UEAuthentication_AuthenticateResponse (EAP Request/EAP-Type = EAP-TLS (TLS Start))
7. Auth-Req. (EAP Request/EAP-Type = EAP-TLS (TLS Start), ngKSI, ABBA)
8. Auth-Resp. (EAP Response/EAP-Type = EAP-TLS (TLS client_hello))
9.Nausf_UEAuthentication_AuthenticateRequest (EAP Response/EAP-Type = EAP-TLS (TLS client_hello))
10.Nausf_UEAuthentication_AuthenticateResponse (EAP Request/EAP-Type = EAP-TLS (TLS server_hello, TLS Certificate, [TLS server_key_exchange,] TLS certificate_request, TLS server_hello_done))
11. Auth-Req.(EAP Request/EAP-Type = EAP-TLS (TLS server_hello, TLS Certificate, [TLS server_key_exchange,] TLS certificate_request, TLS server_hello_done), ngKSI, ABBA)
12. UE authenticate network
13. Auth-Resp.(EAP Response/EAP-Type = EAP-TLS (TLS Certificate, TLS client_key_exchange, TLS certificate_verify, TLS change_cipher_spec, TLS finished))
14.Nausf_UEAuthentication_AuthenticateRequest (EAP Response/EAP-Type = EAP-TLS (TLS Certificate, TLS client_key_exchange, TLS certificate_verify, TLS change_cipher_spec, TLS finished))
15. Network authenticate UE
16.Nausf_UEAuthentication_AuthenticateResponse (EAP Request/EAP-Type = EAP-TLS (TLS change_cipher_spec, TLS finished))
17. Auth-Req. (EAP Request/EAP-Type = EAP-TLS (TLS change_cipher_spec, TLS finished), ngKSI, ABBA)
18. Auth-Resp.(EAP Response/EAP-Type = EAP-TLS)
19.Nausf_UEAuthentication_AuthenticateRequest (EAP Response/EAP-Type = EAP-TLS)
20.Nausf_UEAuthentication_AuthenticateReSponse (EAP Success, Anchor Key, SUPI)
21. N1 (EAP Success, ngKSI, ABBA)

Figure B.2.1.1-1: Using EAP-TLS Authentication Procedures over 5G Networks for initial authentication

1. The UE sends the Registration Request message to the SEAF, containing SUCI. If the SUPI is in NAI format, only the username part of the NAI is encrypted using the selected protection scheme and included in the SUCI, together with the realm part in the NAI needed for UDM routing.

   Privacy considerations are described in Clause B.2.2.

2. The SEAF sends Nausf_UEAuthentication_Authenticate Request message to the AUSF. The SUCI and the serving network name (as described in clause 6.1.1.4) are included in the message.

3. AUSF sends the the Nudm_UEAuthentication_Get Request, containing SUCI and the serving network name, to UDM. The general rules for UDM selection applies.

4. The SIDF located within the UDM de-conceals the SUCI to SUPI if SUCI is received in the message. The UDM then selects the primary authentication method.

5. If the UDM chooses to use EAP-TLS, it sends the SUPI and an indicator to choose EAP-TLS to AUSF in the Nudm_UEAuthentication_Get Response.

6. With the received SUPI and the indicator, the AUSF chooses EAP-TLS as the authentication method. The AUSF sends thea Nausf_UEAuthentication_Authenticate Response message containing EAP-Request/EAP-TLS [TLS start] message to the SEAF.

7. The SEAF forwards the EAP-Request/EAP-TLS [TLS start] in the Authentication Request message to the UE. This message also includes the ngKSI and the ABBA parameter. In fact, the SEAF shall always include the ngKSI and ABBA parameter in all EAP-Authentication request message. ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1.

8. After receiving the EAP-TLS [TLS-start] message from SEAF, the UE replies with an EAP-Response/EAP-TLS [client_hello] to the SEAF in the Authentication Response message. The contents of TLS client_hello are defined in the TLS specification of the TLS version in use.

NOTE1: The EAP framework supports negotiation of EAP methods. If the UE does not support EAP-TLS, it should follow the rule described in RFC 3748 [27] to negotiate another EAP method. In 5G system, UDM typically knows which EAP method and credentials are supported by the subscriber, and consequently EAP based negotiation may never be used.

9. The SEAF forwards the EAP-Response/EAP-TLS [client hello] message to AUSF in the Nausf_UEAuthentication_Authenticate Request.

10. The AUSF replies to the SEAF with EAP-Request/EAP-TLS in the Nausf_UEAuthentication_Authenticate Response, which further includes information elements such as server_hello, server_certificate, server_key_exchange, certificate_request, server_hello_done. These information elements are defined in the RFCs for the corresponding TLS version in use.

11. The SEAF forwards the EAP-Request/EAP-TLS message with server_hello and other information elements to the UE through Authentication Request message. This message also includes the ngKSI and the ABBA parameter .The SEAF shall set the ABBA paremeter as defined in Annex A.7.1.

12. The UE authenticates the server with the received message from step 11.

NOTE 2: The UE is required to be pre-configured with a UE certificate and also certificates that can be used to verify server certificates.

13. If the TLS server authentication is successful, then the UE replies with EAP-Response/EAP-TLS in Authentication Response message, which further contains information element such as client_certificate, client_key_exchange, client_certificate_verify, change_cipher_spec, client_finished etc. Privacy considerations are described in Clause B.2.1.2.

14. The SEAF forwards the message with EAP-Response/EAP-TLS message with client_certificate and other information elements to the AUSF in the Nausf_UEAuthentication_Authenticate Request.

15. The AUSF authenticates the UE based on the message received. The AUSF verifies that the client certificate provided by the UE belongs to the subscriber identified by the SUPI. If there is a miss-match in the subscriber identifiers in the SUPI, the AUSF does not accept the client certificate. If the AUSF has successfully verified this message, the AUSF continues to step 16, otherwise it returns an EAP-failure.

NOTE 2: The AUSF is required to be pre-configured with the root or any intermediary CA certificates that can be used to verify UE certificates. Deployment of certificate revocation lists (CRLs) and online certificate status protocol (OCSP) are described in clause B.2.2.

16. The AUSF sends EAP-Request/EAP-TLS message with change_cipher_spec and server_finished to the SEAF in the Nausf_UEAuthentication_Authenticate Response.

17. The SEAF forwards EAP-Request/EAP-TLS message from step 16 to the UE with Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1.

18. The UE sends an empty EAP-TLS message to the SEAF in Authentication Response message.

19. The SEAF further forwards the EAP-Response/EAP-TLS message to the AUSF in the Nausf_UEAuthentication_Authenticate Request.

20. The AUSF uses the first 256 bits of EMSK as the K_{AUSF} and then calculates K_{SEAF} from K_{AUSF} as described in Annex A.6. The AUSF sends an EAP-Success message to the SEAF together with the SUPI and the derived anchor key in the Nausf_UEAuthentication_Authenticate Response.

21. The SEAF forwards the EAP-Success message to the UE and the authentication procedure is finished. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1. Then the SEAF derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7, and provides the ngKSI and the K_{AMF} to the AMF.

    On receiving the EAP-Success message, the UE derives EMSK and uses the first 256 bits of the EMSK as the K_{AUSF} and then calculates K_{SEAF} in the same way as the AUSF. The UE derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7.

NOTE 3: Step 21 could be NAS Security Mode Command.

NOTE 4: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

B.2.1.2 Privacy considerations

B.2.1.2.1 EAP TLS without subscription identifier privacy

For EAP TLS, if the operator determines to not provide subscription identifier privacy for the UE in TLS layer (e.g., in TLS 1.2 without privacy option), the subscription identifier protection in NAS layer, i.e., in Step 1 of Figure B.2.1-1, becomes ineffective privacy-wise. Therefore, the operator may just choose that UE uses "null-scheme" for calculation of SUCI which is sent in NAS layer. However, the operator may anyway use other than null-schemes (e.g., one of ECIES schemes) for simplification of having single scheme for all UEs in NAS layer even though privacy is not enhanced in this particular case.

The operator could also determine not to provide subscription identifier privacy for the UE in NAS layer even though the TLS layer inherently provides subscription identifier privacy (e.g., in TLS 1.3). In such case, the operator may just choose that UE uses "null-scheme" for calculation of SUCI which is sent in NAS layer.

B.2.1.2.2 EAP TLS with subscription identifier privacy

For EAP TLS, if the operator determines to provide subscription identifier privacy for the UE in TLS layer, the the EAP TLS server needs to support privacy either inherently (e.g., in TLS 1.3) or via separate privacy option (e.g., in TLS 1.2). If privacy is an option in TLS layer, then the operator needs to configure UE with the information that privacy-on-TLS layer is enabled. Further, following considerations need to be taken.

In Step 1 of Figure B.2.1-1, it is important that calculation of SUCI, which is sent in NAS layer, is done using schemes other than "null-scheme". Otherwise, the subscription identifier protection provided by TLS layer becomes ineffective privacy-wise. Nevertheless, the "null-scheme" could be used in NAS layer while still preserving subscription identifier privacy, by omitting the username part from NAI as described in RFC 4282 clause 2.3 [y]. It would be analogous to using anonymous identifier in EAP, meaning that only realm part from NAI is included in SUCI which is sent in NAS layer. Thus formed SUCI can still be used to route the authentication request to AUSF.

In Step 13 and 14 of Figure B.2.1-1, when TLS 1.2 is used, the UE would need to behave as described in "Section 2.1.4. Privacy" of RFC 5216 [38] where instead of sending the client certificate in cleartext over the air, the UE first sends TLS certificate (no cert) and only later sends TLS certificate after a TLS is setup.

B.2.2 Revocation of subscriber certificates

Subscriber certificates that are used with EAP-TLS typically include static validity times. A certificate revocation list (CRL) as specified in RFC 5280 [48] and online certificate status protocol (OCSP) as specified in RFC 6960 [49] are means for the issuing certificate authority (CA) to revoke the certificates before their scheduled expiration date. In 5G security architecture, the UDM/ARPF is responsible for such subscriber status information. EAP-TLS peers and servers may also support Certificate Status Requests (OCSP stapling) as specified in RFC6066 [50] which allows peers to request the server's copy of the current status of certificates.

The deployment of CRLs is demonstrated in figure B.2.2-1. When the UDM/ARPF maintains the CRLs, the lists may be periodically updated to AUSFs, and stored locally in AUSF.

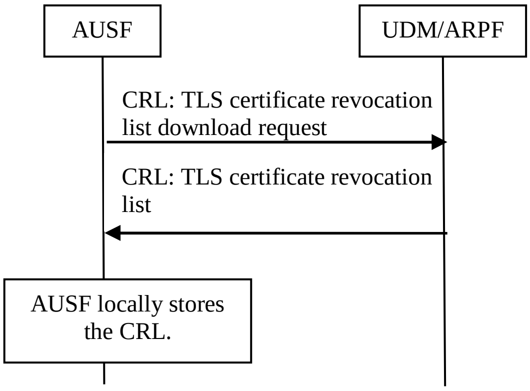
AUSF
UDM/ARPF
CRL: TLS certificate revocation list download request
CRL: TLS certificate revocation list
AUSF locally stores the CRL.

Figure B.2.2-1: AUSF requests CRL from UDM/ARPF

The deployment of OSCP is demonstrated in figure B.2.2-2. When the UDM/ARPF supports OCSP, the AUSF may check the certificate status online.

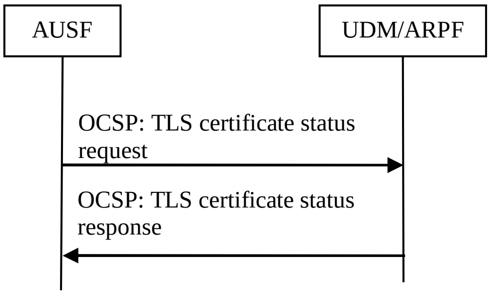
AUSF
UDM/ARPF
OCSP: TLS certificate status request
OCSP: TLS certificate status response

Figure B.2.2-2: AUSF requests the status of TLS certificate from UDM/ARPF

B.3 Key derivation

When EAP methods are used with 5G system, the serving network name is always bound to the anchor key derivation as required in clause 6.1.1.3. When SEAF acts as a pass-through EAP authenticator, it always includes the serving network name into the authentication request to the AUSF. In the same as the initial authentication procedure specified in clause 6.1.2, AUSF verifies that the SEAF is authorized to use the serving network name, and uses the serving network name when calculating the K_{SEAF} from the K_{AUSF} as described in Annex A.6. The AUSF always uses the first 256 bits of EMSK as the K_{AUSF}.

When EAP-TLS [38] is used for authentication, key materials are derived during authentication and key agreement procedure, which are further split into MSK and EMSK. Both UE and AUSF share a 512 bits EMSK key and the first 256 bits of the EMSK is used as the K_{AUSF}. The K_{SEAF} is derived based on the rules specified in Annex A.6.

Annex C (normative): Protection schemes for concealing the subscription permanent identifier

C.1 Introduction

The present Annex specifies the protection schemes for concealing the subscription permanent identifier. Each protection scheme is identified using a 4-bit identifier. The defined values are:

null-scheme	0x0;
Profile <A>	0x1;
Profile <B>	0x2.

The values 0x3 - 0xB are reserved for future standardized protection schemes. The values 0xC - 0xF are reserved for propietary protection schemes.

Care should be taken when using unique schemes for small groups of users, as this may impact the effectiveness of the privacy scheme for these users.

Each protection scheme has scheme-output with following sizes:

null-scheme size of input, i.e., size of username used in case of NAI format or MSIN in case of IMSI;

Profile <A> total of 256-bit public key, 64-bit MAC, and size of input;

Profile <B> total of 264-bit public key, 64-bit MAC, and size of input.

The maximum size of scheme-output for proprietary protection schemes shall be <X>.

Editor's Note: The value of <X> is FFS and stage 3 spec needs to be referenced here.

C.2 Null-scheme

The null-scheme shall be implemented such that it returns the same output as the input, which applies to both encryption and decryption.

When using the null-scheme, the SUCI does not conceal the SUPI and therefore the newly generated SUCIs do not need to be fresh.

NOTE 1: The reason for mentioning the non-freshness is that, normally, in order to attain unlinkability (i.e., to make it infeasible for over-the-air attacker to link SUCIs together), it is necessary for newly generated SUCIs to be fresh. But, in case of the null-scheme, the SUCI does not conceal the SUPI. So unlinkability is irrelevant.

NOTE 2: The null-scheme provides no privacy protection.

C.3 Elliptic Curve Integrated Encryption Scheme (ECIES)

C.3.1 General

The use of ECIES for concealment of the SUPI shall adhere to the SECG specifications [29] and [30]. Processing on UE side and home network side are described in high level in clauses C.3.2 and C.3.3.

C.3.2 Processing on UE side

The ECIES scheme shall be implemented such that for computing a fresh SUCI, the UE shall use the provisioned public key of the home network and freshly generated ECC (elliptic curve cryptography) ephemeral public/private key pair according to the ECIES parameters provisioned by home network. The processing on UE side shall be done according to the encryption operation defined in [29]. with the following changes to Section 3.8 and step 5 and 6 of Section 5.1.3.

- generate keying data K of length *enckeylen* + *icblen* + *mackeylen*.
  - Parse the leftmost enckeylen octets of K as an encryption key EK, the middle icblen octets of K as an ICB, and the rightmost mackeylen octets of K as a MAC key MK.

The final output shall be the concatenation of the ECC ephemeral public key, the ciphertext value, the MAC tag value, and any other parameters, if applicable.

NOTE: The reason for mentioning "any other parameter, if applicable" in the final output is to allow cases, e.g. to enable the sender to send additional sign indication when point compression is used.

The Figure C.3.2-1 illustrates the UE's steps.

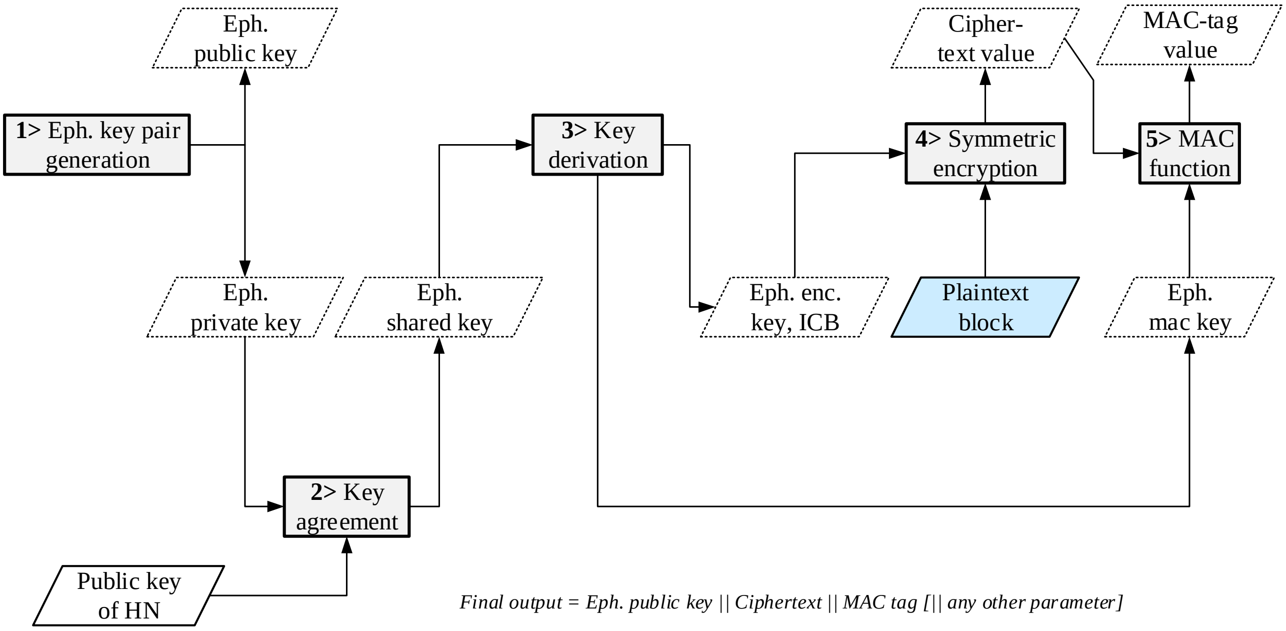

Figure C.3.2-1: Encryption based on ECIES at UE

C.3.3 Processing on home network side

The ECIES scheme shall be implemented such that for deconcealing a SUCI, the home network shall use the received ECC ephemeral public key of the UE and the private key of the home network. The processing on home network side shall be done according to the decryption operation defined in [29]. with the following changes to Section 3.8 and step 6 and 7 of Section 5.1.4.

- generate keying data K of length *enckeylen* + *icblen* + *mackeylen.*
  - Parse the leftmost *enckeylen* octets of *K* as an encryption key *EK*, the middle *icblen* octets of *K* as an ICB, and the rightmost *mackeylen* octets of *K* as a MAC key *MK*.

NOTE: Unlike the UE, the home network does not need to perform a fresh ephemeral key pair generation for each decryption. How often the home network generates new public/private key pair and how the public key is provisioned to the UE are out of the scope of this clause.

The Figure C.3.3-1 illustrates the home network's steps.

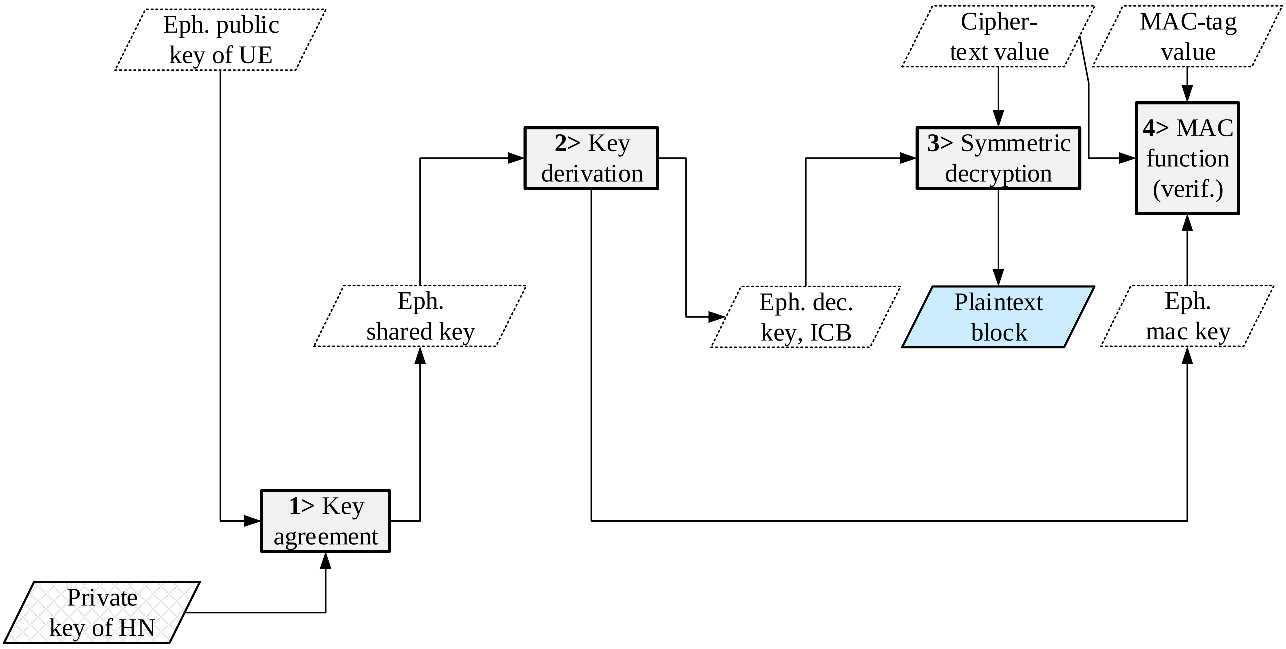

Figure C.3.3-1: Decryption based on ECIES at home network

C.3.4 ECIES profiles

C.3.4.0 General

Unless otherwise stated, the ECIES profiles follow the terminology and processing specified in SECG version 2 [29] and [30]. The profiles shall use "named curves" over prime fields.

For generating successive counter blocks from the initial counter block (ICB) in CTR mode, the profiles shall use the standard incrementing function in section B.1 of NIST Special Publication 800-38A [16] with m = 32 bits. The ICB corresponds to T_1 in section 6.5 of [16].

Profile A shall use its own standardized processing for key generation (section 6 of RFC 7748 [46]) and shared secret calculation (section 5 of RFC 7748 [46]). The Diffie-Hellman primitive X25519 (section 5 of RFC 7748 [46]) takes two random octet strings as input, decodes them as scalar and coordinate, performs multiplication, and encodes the result as an octet string. The shared secret output octet string from X25519 shall be used as the input Z in the ECIES KDF (section 3.6.1 of [29]).

Profile B shall use point compression to save overhead and shall use the Elliptic Curve Cofactor Diffie-Hellman Primitive (section 3.3.2 of [29]) to enable future addition of profiles with cofactor $h \neq 1$. For curves with cofactor $h = 1$ the two primitives (section 3.3.1 and 3.3.2 of [29]) are equal.

The profiles shall not use backwards compatibility mode (therefore are not compatible with version 1 of SECG).

C.3.4.1 Profile A

The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:

- EC domain parameters	: Curve25519 [46]
- EC Diffie-Hellman primitive	: X25519 [46]
- point compression	: N/A
- KDF	: ANSI-X9.63-KDF [29]
- Hash	: SHA-256
- SharedInfo$_1$	: $\overline{R}$(the ephemeral public key octet string – see [29] section 5.1.3)

- MAC : HMAC–SHA-256
- mackeylen : 32 octets (256 bits)
- maclen : 8 octets (64 bits)
- SharedInfo$_2$: the empty string
- ENC : AES–128 in CTR mode
- enckeylen : 16 octets (128 bits)
- icblen : 16 octets (128 bits)
- backwards compatibility mode : false

C.3.4.2 Profile B

The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:

- EC domain parameters : secp256r1 [30]
- EC Diffie-Hellman primitive : Elliptic Curve Cofactor Diffie-Hellman Primitive [29]
- point compression : true
- KDF : ANSI-X9.63-KDF [29]
- Hash : SHA-256
- SharedInfo1 : $\overline{R}$ (the ephemeral public key octet string – see [29] section 5.1.3)
- MAC : HMAC–SHA-256
- mackeylen : 32 octets (256 bits)
- maclen : 8 octets (64 bits)
- SharedInfo2 : the empty string
- ENC : AES–128 in CTR mode
- enckeylen : 16 octets (128 bits)
- icblen : 16 octets (128 bits)
- backwards compatibility mode : false

Annex D (normative): Algorithms for ciphering and integrity protection

D.1 Null ciphering and integrity protection algorithms

The NEA0 algorithm shall be implemented such that it generates a KEYSTREAM of all zeroes (see sub-clause D.2.1). The length of the KEYSTREAM generated shall be equal to the LENGTH input parameter. The generated KEYSTREAM requires no other input parameters but the LENGTH. Apart from this, all processing performed in association with ciphering shall be exactly the same as with any of the ciphering algorithms specified in this Annex.

The NIA0 algorithm shall be implemented in such way that it shall generate a 32 bit MAC-I/NAS-MAC and XMAC-I/XNAS-MAC of all zeroes (see sub-clause D.3.1). Replay protection shall not be activated when NIA0 is activated. All processing performed in association with integrity (except for replay protection) shall be exactly the same as with any of the integrity algorithms specified in this annex except that the receiver does not check the received MAC.

NOTE 1: The reason for mentioning the replay protection here is that replay protection is associated with integrity.

The NIA0 shall not be used for signalling radio bearers (SRBs) except for unauthenticated emergency sessions for unauthenticated UEs in LSM.

The NIA0 shall not be used for data radio bearers (DRBs).

NOTE 2: A UE with a 2G SIM is considered to be in LSM in NR.

NOTE 3: NEA0 and NIA0 provide no security.

D.2 Ciphering algorithms

D.2.1 128-bit Ciphering algorithms

D.2.1.1 Inputs and outputs

The input parameters to the ciphering algorithm are a 128-bit cipher key named KEY, a 32-bit COUNT, a 5-bit bearer identity BEARER, the 1-bit direction of the transmission i.e. DIRECTION, and the length of the keystream required i.e. LENGTH. The DIRECTION bit shall be 0 for uplink and 1 for downlink.

Figure D.2.1.1-1 illustrates the use of the ciphering algorithm NEA to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

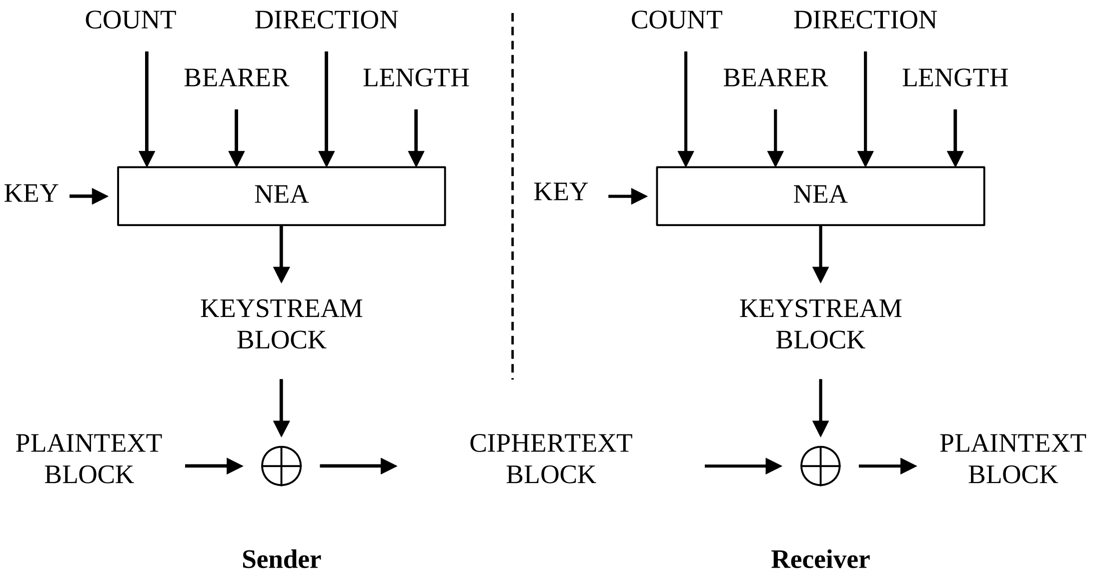

Figure D.2.1.1-1: Ciphering of data

Based on the input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

D.2.1.2 128-NEA1

128-NEA1 is identical to 128-EEA1 as specified in Annex B of TS 33.401 [10].

D.2.1.3 128-NEA2

128-NEA2 is identical to 128-EEA2 as specified in Annex B of TS 33.401 [10].

D.2.1.4 128-NEA3

128-NEA3 is identical to 128-EEA3 as specified in Annex B of TS 33.401 [10].

D.3 Integrity algorithms

D.3.1 128-Bit integrity algorithms

D.3.1.1 Inputs and outputs

The input parameters to the integrity algorithm are a 128-bit integrity key named KEY, a 32-bit COUNT, a 5-bit bearer identity called BEARER, the 1-bit direction of the transmission i.e. DIRECTION, and the message itself i.e. MESSAGE. The DIRECTION bit shall be 0 for uplink and 1 for downlink. The bit length of the MESSAGE is LENGTH.

Figure D.3.1.1-1 illustrates the use of the integrity algorithm NIA to authenticate the integrity of messages.

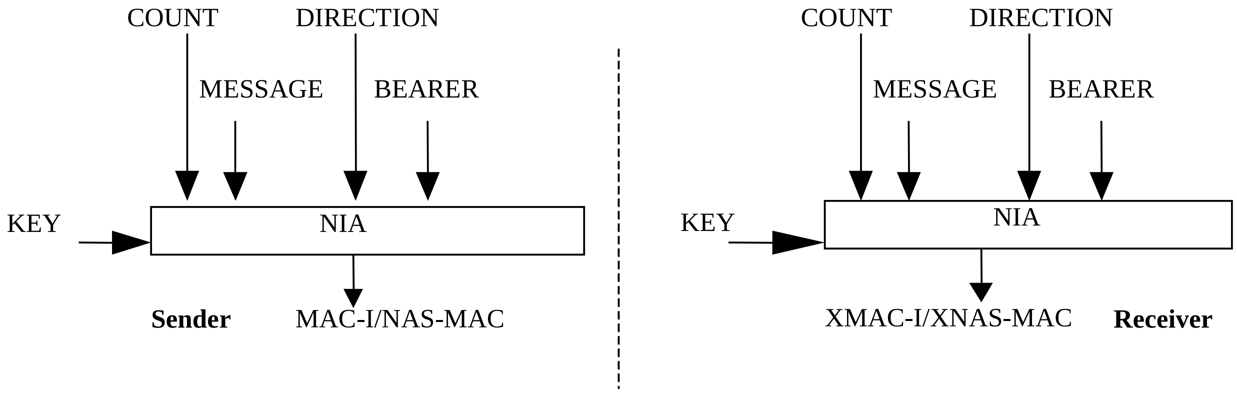

Figure D.3.1.1-1: Derivation of MAC-I/NAS-MAC (or XMAC-I/XNAS-MAC)

Based on these input parameters the sender computes a 32-bit message authentication code (MAC-I/NAS-MAC) using the integrity algorithm NIA. The message authentication code is then appended to the message when sent. For integrity protection algorithms, the receiver computes the expected message authentication code (XMAC-I/XNAS-MAC) on the message received in the same way as the sender computed its message authentication code on the message sent and verifies the data integrity of the message by comparing it to the received message authentication code, i.e. MAC-I/NAS-MAC.

D.3.1.2 128-NIA1

128-NIA1 is identical to 128-EIA1 as specified in Annex B of TS 33.401 [10].

D.3.1.3 128-NIA2

128-NIA2 is identical to 128-EIA2 as specified in Annex B of TS 33.401 [10].

D.3.1.4 128-NIA3

128-NIA3 is identical to 128-EIA3 as specified in Annex B of TS 33.401 [10].

D.4 Test Data for the security algorithms

D.4.1 General

Annex D.4 contains references to the test data for each of the specified algorithms.

D.4.2 128-NEA1

For 128-NEA1 is the test data for UEA2 in TS 35.217 [36] can be reused directly as there is an exact, one-to-one mapping between UEA2 inputs and 128-NEA1 inputs.

D.4.3 128-NIA1

For 128-NIA1 is the test data for 128-EIA1 in clause C.4 of TS 33.401 [10] can be reused directly as there is an exact, one-to-one mapping between 128-EIA1 inputs and 128-NIA1 inputs.

D.4.4 128-NEA2

For 128-NEA2 is the test data for 128-EEA2 in clause C.1 of TS 33.401 [10] can be reused directly as there is an exact, one-to-one mapping between 128-EEA2 inputs and 128-NEA2 inputs.

D.4.5 128-NIA2

For 128-NIA2 is the test data for 128-EIA2 in clause C.2 of TS 33.401 [10] can be reused directly as there is an exact, one-to-one mapping between 128-EIA2 inputs and 128-NIA2 inputs.

D.4.6 128-NEA3

For 128-NEA3 is the test data for 128-EEA3 in TS 35.223 [37] can be reused directly as there is an exact, one-to-one mapping between 128-EEA3 inputs and 128-NEA3 inputs.

D.4.7 128-NIA3

For 128-NIA3 is the test data for 128-EIA3 in TS 35.223 [37] can be reused directly as there is an exact, one-to-one mapping between 128-EIA3 inputs and 128-NIA3 inputs.

Annex E (informative): UE-assisted network-based detection of false base station

E.1 Introduction

The UE in RRC_CONNECTED mode sends measurement reports to the network in accordance with the measurement configuration provided by the network. These measurement reports have security values in being useful for detection of false base stations or SUPI/5G-GUTI catchers. The network, in an implementation specific way, could choose UEs or tracking areas or duration for which the measurement reports are to be analysed for detection of false base station. The present Annex gives examples of how measurement reports from UEs could be used for detection of false base station, and some actions thereafter.

E.2 Examples of using measurement reports

The received-signal strength and location information in measurement reports can be used to detect a false base station which attract the UEs by transmitting signal with higher power. They can also be used to detect a false base station which replays the genuine MIB/SIB without modification.

In order to detect a false base station which replays modified version of broadcast information to prevent victim UEs from switching back and forth between itself and genuine base stations (e.g. modifying neighbouring cells, cell reselection criteria, registration timers, etc. to avoid the so called ping-pong effect), information on broadcast information can be used to detect inconsistency from the deployment information.

Further, a false base station which uses inconsistent cell identifier or operates in inconsistent frequency than the deployment of the genuine base stations, can be detected respectively by using the cell identifier or the frequency information in the measurement reports.

Measurement reports collected from multiple UEs can be used to filter out incorrect reports sent by a potential rogue UE.

Upon detection of the false base station, the operator can take further actions, e.g. informing legal authorities or contacting the victim UE.

Annex F (normative): 3GPP 5G profile for EAP-AKA'

F.1 Introduction

The present annex describes the 3GPP 5G profile for EAP-AKA' described in RFC 5448 [12], and RFC 4187 [21].

NOTE: This annex (or a part of it) can be removed e.g. if RFC 5448 is updated in the IETF and a reference to the new RFC is added. Alternatively, some of the content may be moved to relevant 3GPP stage 3 specification.

F.2 Subscriber privacy

EAP-AKA' includes optional support for identity privacy mechanism that protects the privacy against passive eavesdropping. The mechanism is described in RFC 4187 [21] clause 4.1.1.2, and it uses pseudonyms that are delivered from the EAP server to the peer as part of an EAP-AKA exchange. The privacy mechanism described in [21] corresponds to the privacy provided by 5G-GUTI, however, assignment of 5G-GUTI is done outside the EAP framework in 5GS.

TS 33.501 assumes that the SUCI is sent outside the EAP messages, however, the peer may still receive EAP-Request/Identity or EAP-Request/AKA-Identity messages. Table F.2-1 specifies how the 5G UE shall behave when receiving such requests.

Table F.2-1: 5G UE behaviour when receiving EAP identity requests

REQUEST	5G UE RESPONSE
EAP-Request/Identity	EAP-Response/Identity SUCI$^{1)}$
EAP-Request/AKA-Identity AT_PERMANENT_REQ	EAP-Response/AKA-Client-Error with the error code "unable to process packet" $^{2)}$
EAP-Request/AKA-Identity AT_FULLAUTH_REQ	EAP-Response/AKA-Identity AT_IDENTITY=SUCI $^{3)}$

EAP-Request/AKA-Identity
AT_ANY_ID_REQ
	EAP-Response/AKA-Identity
	AT_IDENTITY=fast re-auth identity OR
	AT_IDENTITY=SUCI $^{4)}$

1) RFC 3748 [27] allows the peer to respond with abbreviated Identity Response where the peer-name portion of the NAI has been omitted. The 5G UE responds with SUCI where the peer name has been encrypted.

2) RFC 4187 [21] allows the peer to respond with a pseudonym (cf. 5G-GUTI) or the permanent identity (i.e. SUPI). The 5G UE follows the "conservative" policy that has been described in RFC 4187 [21] clause 4.1.6 (Attacks against Identity Privacy) for the pseudonym based privacy, i.e. the peer shall not reveal its permanent identity. Instead, the peer shall send the EAP-Response/AKA-Client-Error packet with the error code "unable to process packet", and the authentication exchange terminates. The peer assumes that the EAP-Request/AKA-Identity originates from an attacker that impersonates the network, and for this reason refuses to send the cleartext SUPI.

3) RFC 4187 [21] allows the peer to respond with a pseudonym (cf. 5G-GUTI) or the permanent identity (i.e. SUPI). The 5G UE responds with SUCI.

4) RFC 4187 [21] allows the peer to respond with a fast re-authentication identity, pseudonym (cf. 5G-GUTI) or the permanent identity (i.e. SUPI). If the 5G UE supports fast re-authentication, it responds with the fast re-authentication identity, and if the 5G UE does not support fast re-authentication, it responds with SUCI.

F.3 Subscriber identity and key derivation

EAP-AKA' uses the subscriber identity (Identity) as an input to the key derivation when the key derivation function has value 1 (i.e. MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)). RFC 4187 [21] clause 7 describes that the Identity is taken from the EAP-Response/Identity or EAP-Response/AKA-Identity AT_IDENTITY attribute sent by the peer. This principle is not applied to the 5GS.

If the AT_KDF_INPUT parameter contains the prefix "5G:", the AT_KDF parameter has the value 1 and the authentication is not related to fast re-authentication, then the UE shall use SUPI as the Identity for key derivation. This principle applies to all full EAP-AKA' authentications, even if the UE sent SUCI in NAS protocol or if the UE sent SUCI in the respose to the EAP identity requests as described in Table F.2-1 or if no identity was sent because the network performed re-authentication. The only exception is fast re-authentication when the UE follows the key derivation as described in RFC 5448 [12] for fast re-authentication.

NOTE: The fast re-authentication is not supported in 5GS.

F.4 Void

Annex G (informative): Application layer security on the N32 interface

G.1 Introduction

The SEPP as described in clause 4.X is the entity that sits at the perimeter of the network and performs application layer security on the HTTP message before it is sent externally over the roaming interface.

The application layer traffic comprises all the IEs in the HTTP message payload, sensitive information in HTTP message header and Request URI. Not all the IEs get the same security treatment in SEPP. Some IEs require e2e encryption, some only require e2e integrity protection, while other IEs may require e2e integrity protection but modifiable by intermediate IPX provider while in-transit.

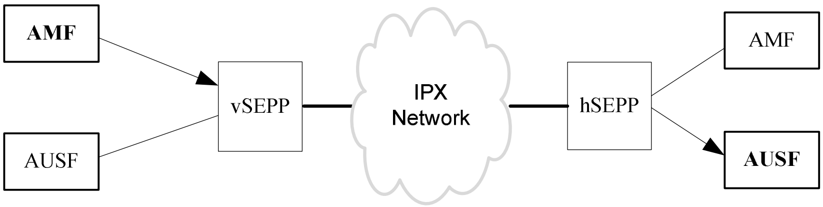

Figure G.1-1: Signaling message from AMF (vPLMN) to AUSF (hPLMN) traversing the respective SEPPs

In the above figure, an example is shown where the AMF NF in the visiting PLM network (vPLMN) invokes an API request on the AUSF NF in the home PLM network (hPLMN) using the following message flow:

- The AMF NF first sends the HTTP Request message to its local SEPP (i.e. vSEPP).
- The vSEPP applies Application Layer Security (ALS) and sends the secure message on the N32 interface to AUSF NF of the hPLMN.
- The hSEPP at the edge of the hPLMN, receives all incoming HTTP messages from its roaming partners. It verifies the message, removes the protection mechanism applied at the application layer, and forwards the resulting HTTP message to the corresponding AUSF NF.

To allow for the trusted intermediary IPX nodes to see and possibly modify specific IEs in the HTTP message, while completely protecting all sensitive information end to end between SEPPs, the SEPP implements application layer security in such a way that:

- Sensitive information such as authentication vectors are fully e2e confidentiality protected between two SEPPs. This ensures that no node in the IPX network shall be able to view such information while in-transit.
- IEs that are subject to modification by intermediary IPX nodes are integrity protected and can only be modified in a verifiable way by authorized IPX nodes.
- Receiving SEPP can detect modification by unauthorized IPX nodes.

G.2 Structure of HTTP Message

Following is a typical structure of the HTTP Message:

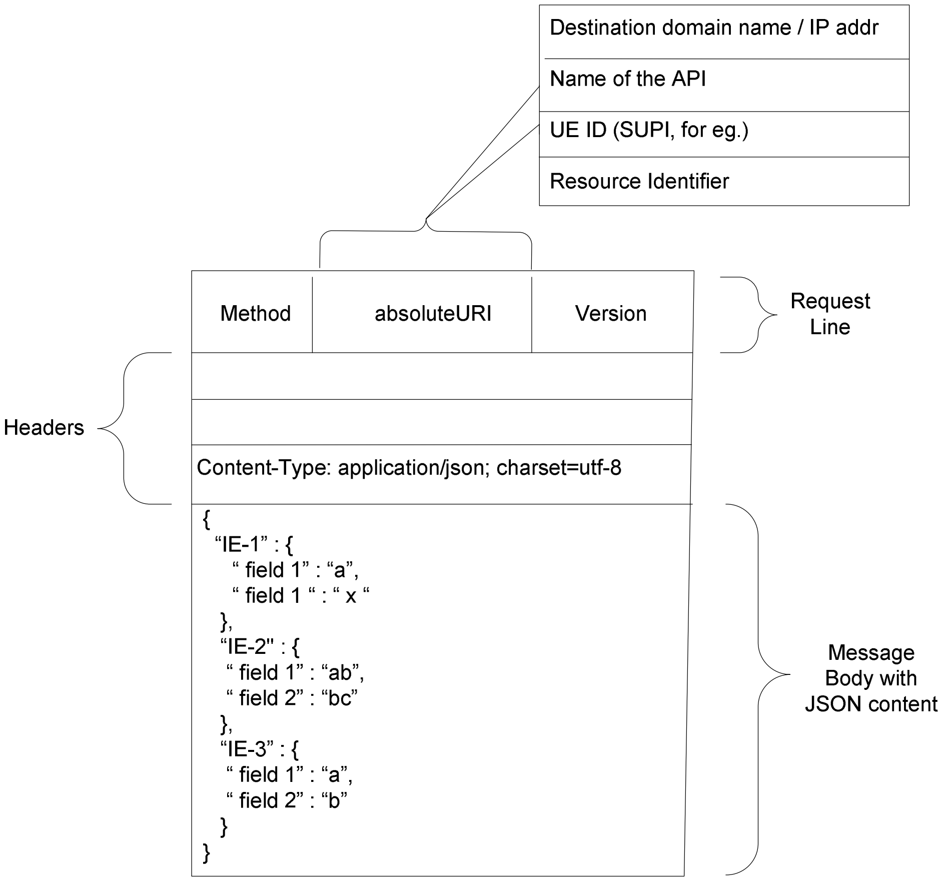

Figure G.2-1 Typical structure of the HTTP message received by SEPP

It consists of:

- HTTP Message payload with JSON based IEs
- HTTP Headers with or without sensitive elements
- HTTP Request-URI with or without sensitive elements such as SUPI.

In the outgoing direction, i.e. towards the N32 interface, the SEPP shall parse the HTTP message fully and apply protection on each part as required.

In the incoming direction, i.e. towards the Network Function, the SEPP shall verify the message, and if successful reassemble the original message and send it to the destined Network Function.

Annex H (normative): Hash functions

H.1 General

This Annex describes how to form the inputs of non-keyed hash calculations using the KDF described in TS 33.220 [28].

H.2 HASH$_{\text{AMF}}$ and HASH$_{\text{UE}}$

When the AMF and UE shall derive HASH$_{\text{AMF}}$ and HASH$_{\text{UE}}$ respectively using the following parameters as input to the KDF given in TS 33.220 [28].

- S = Initial NAS message,

NOTE: The order of packing the input, S, to hash algorithm is the same as the order of packing the UL NAS message to the AMF.

- Key = 256-bit string of all 0s

HASH_{AMF} or HASH_{UE} are the 64 least significant bits of the 256 bits of the KDF output.

Annex I (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2018-06	SA#80	SP-180452	0004	1	B	Rules on concurrent running of authentication and NAS SMC procedure	15.1.0
2018-06	SA#80	SP-180452	0007	2	F	Remove EN for initial NAS message protection	15.1.0
2018-06	SA#80	SP-180452	0012	1	F	Modification on UE's subscribe privacy requirement	15.1.0
2018-06	SA#80	SP-180452	0018	-	D	Editorial modification on reference	15.1.0
2018-06	SA#80	SP-180452	0030	1	F	Add condition for reset NAS COUNTs	15.1.0
2018-06	SA#80	SP-180452	0038	2	F	Editorials to 33.501	15.1.0
2018-06	SA#80	SP-180454	0046	2	B	The granularity of NF service discovery	15.1.0
2018-06	SA#80	SP-180452	0053	2	F	CR for Clause Security algorithm selection, key establishment and security mode command procedure	15.1.0
2018-06	SA#80	SP-180452	0064	4	F	Corrections to secondary authentication procedure	15.1.0
2018-06	SA#80	SP-180454	0066	2	F	Clarifications to clause UP security mechanisms	15.1.0
2018-06	SA#80	SP-180452	0075	1	C	F1-C Protection	15.1.0
2018-06	SA#80	SP-180452	0080	1	F	Corrections related to authentication related services	15.1.0
2018-06	SA#80	SP-180452	0081	1	F	Clarifications to: Linking increased home control to subsequent procedures	15.1.0
2018-06	SA#80	SP-180452	0084	1	F	Clarifications to: Initiation of authentication and selection of authentication method	15.1.0
2018-06	SA#80	SP-180452	0090	1	F	Clarifications to Idle mode mobility from 5GS to EPS	15.1.0
2018-06	SA#80	SP-180452	0095	2	F	Multiple NAS connections	15.1.0
2018-06	SA#80	SP-180452	0097	2	F	Clarifications to Mapping of Security Contexts	15.1.0
2018-06	SA#80	SP-180452	0104	1	F	KeNB derivation in 5GS to EPS handover	15.1.0
2018-06	SA#80	SP-180455	0105	3	F	Corrections and clarifications to Handover from EPS to 5GS over N26	15.1.0
2018-06	SA#80	SP-180455	0107	-	F	Delete Editor's Note in C.3.4.3	15.1.0
2018-06	SA#80	SP-180454	0111	2	F	Misleading title given to clause 6.13	15.1.0
2018-06	SA#80	SP-180455	0115	3	F	Clarifications to: Authentication procedures	15.1.0
2018-06	SA#80	SP-180453	0118	3	F	Clarifications to: Using additional EAP methods for primary authentication	15.1.0
2018-06	SA#80	SP-180454	0120	1	F	Clarifications on unused 5G authentication vectors, and remaning authentication data	15.1.0
2018-06	SA#80	SP-180453	0125	3	F	Generalization of key derivation in NG-RAN to cover both gNBs and ng-eNBs	15.1.0
2018-06	SA#80	SP-180455	0128	1		Emergency call redirection scenarios	15.1.0
2018-06	SA#80	SP-180453	0135	1	C	TS 33.501 Resolving Editors notes 5.10.1 Security Visibility	15.1.0
2018-06	SA#80	SP-180453	0143	3	F	Clarifications to: Key hierarchy, key derivation, and distribution scheme	15.1.0
2018-06	SA#80	SP-180455	0145	5	B	Clarification to Subscription identifier privacy	15.1.0
2018-06	SA#80	SP-180453	0147	3	B	Clarifications to: Protection at the network or transport layer, Authorization and authentication between network functions and the NRF	15.1.0
2018-06	SA#80	SP-180453	0149	3	F	Corrections in clause 6	15.1.0
2018-06	SA#80	SP-180453	0150	1	F	Reference corrections in clause 8	15.1.0
2018-06	SA#80	SP-180453	0152	3	F	Clarifications to: Definitions and Abbreviations	15.1.0
2018-06	SA#80	SP-180453	0153	1	F	Editorial changes to claus 10 and 12	15.1.0
2018-06	SA#80	SP-180453	0155	2	F	Clarifications to Annex A : Key derivation functions	15.1.0
2018-06	SA#80	SP-180453	0156	2	F	Clarifications to: Security contexts	15.1.0
2018-06	SA#80	SP-180453	0157	1	F	Clarifications to: Security handling in state transitions	15.1.0
2018-06	SA#80	SP-180455	0160	-	F	Corrections to Authentication Framework	15.1.0
2018-06	SA#80	SP-180453	0161	1	B	Clarifications to security requirements and features (clause 5)	15.1.0
2018-06	SA#80	SP-180453	0162	2	F	Corrections on SUCI protection schemes	15.1.0
2018-06	SA#80	SP-180453	0163	3	F	Clarifications to: Security handling in mobility	15.1.0
2018-06	SA#80	SP-180453	0164	-	F	Corrections on clause 6.5	15.1.0
2018-06	SA#80	SP-180453	0165	1	F	Clarifications on clause 7.2	15.1.0
2018-06	SA#80	SP-180455	0170	2	F	Correction for TS 33.501 subclause 4.1	15.1.0
2018-06	SA#80	SP-180455	0172	1	F	Correction for TS 33.501 subclause 5.11.2	15.1.0
2018-06	SA#80	SP-180455	0183	1	B	Security Negotiation for RRC INACTIVE	15.1.0
2018-06	SA#80	SP-180455	0184	1	B	Key handling at RRC-INACTIVE state transitions	15.1.0
2018-06	SA#80	SP-180454	0185	1	F	Security Procedures for Dual Connectivity	15.1.0
2018-06	SA#80	SP-180455	0189	1	F	Editorial correction to clause 6.12.5 on SIDF	15.1.0
2018-06	SA#80	SP-180454	0192	1	F	Correction to: 3GPP 5G profile for EAP-AKA'	15.1.0
2018-06	SA#80	SP-180455	0194	-	F	Corrections to section 4.1 Security domains	15.1.0
2018-06	SA#80	SP-180455	0196	1	F	Corrections to section 13.4.1.1	
2018-06	SA#80	SP-180454	0200	-	F	Resolving Editor's Note on USIM	15.1.0

2018-06	SA#80	SP-180455	0201	1	C	Addition of SBA security requirements for SEPP and NF	
2018-06	SA#80	SP-180454	0208	1	F	Clarification of the IPsec implementation requirements	15.1.0
2018-06	SA#80	SP-180454	0209	1	B	Protection of internal gNB interfaces	15.1.0
2018-06	SA#80	SP-180454	0210	1	B	Introduction of DTLS for protection of Xn-C and N2 interfaces	15.1.0
2018-06	SA#80	SP-180454	0211	-	F	Corrections of references to sub-clauses	15.1.0
2018-06	SA#80	SP-180454	0212	-	F	Corrections and clarifications to idle mode mobility from EPS to 5GS over N26	15.1.0
2018-06	SA#80	SP-180454	0213	-	F	Authorization of Application Function's requests	15.1.0
2018-06	SA#80	SP-180454	0214	1	B	Security Mechanism for Steering of Roaming	15.1.0
2018-06	SA#80	SP-180448	0215	-	B	CAPIF support for NEF external exposure interface	15.1.0
2018-06	SA#80	SP-180454	0216	-	F	Clarfication to 6.4.1 NAS security general	15.1.0

2018-06	SA#80	SP-180454	0217	-	F	Clarifications to Annex D.3 Integrity algorithms	15.1.0
2018-09	SA#81	SP-180709	0154	3	D	Editorial changes to clause 9	15.2.0
2018-09	SA#81	SP-180708	0221	1	F	Generic description of 5G security elements	15.2.0
2018-09	SA#81	SP-180708	0223	2	F	Update on SEAF requirements	15.2.0
2018-09	SA#81	SP-180708	0230	1	F	Clause 5.2.5 - Modification on subscriber privacy	15.2.0
2018-09	SA#81	SP-180706	0236	-	D	Clause 6.4.5 - Editorial modification on NAS COUNT handling	15.2.0
2018-09	SA#81	SP-180709	0238	1	F	Clause 6.6.2 - Modification on UP security activation mechanism	15.2.0
2018-09	SA#81	SP-180708	0239	1	F	Clause 6.7.3.2 - Modification on algorithm selection during N2 handover	15.2.0
2018-09	SA#81	SP-180706	0240	-	F	Clause 6.7.3.5 - Correct reference for RNA update procedure	15.2.0
2018-09	SA#81	SP-180708	0242	1	F	Mobility - Correcting AS re-keying and NAS re-keying in N2-handover	15.2.0
2018-09	SA#81	SP-180709	0249	1	F	Add rule for concurrent running of security procedures	15.2.0
2018-09	SA#81	SP-180709	0250	1	F	Modify rule for concurrent running of security procedures	15.2.0
2018-09	SA#81	SP-180708	0251	1	F	Annex C clarification on 'username'	15.2.0
2018-09	SA#81	SP-180706	0252	-	F	Deletion of Requester ID from 'Nausf_UEAuthentication_authenticate'	15.2.0
2018-09	SA#81	SP-180707	0253	1	F	Removal of KSEAF storage restriction	15.2.0
2018-09	SA#81	SP-180709	0257	1	F	Deletion of ENs in Clause 5.3 Requirements on the gNB	15.2.0
2018-09	SA#81	SP-180706	0258	-	F	Align NAS connection identifier with access type identifier	15.2.0
2018-09	SA#81	SP-180706	0259	-	F	Correct the encryption key in confidentiality clause	15.2.0
2018-09	SA#81	SP-180706	0260	-	F	Deletion of Editor Note in Annex D.2.1 Ciphering algorithm	15.2.0
2018-09	SA#81	SP-180709	0261	1	F	Add definition and values for ABBA parameter	15.2.0
2018-09	SA#81	SP-180706	0262	-	F	Deletion of EN in Caluse 10.2.1 Authenticated IMS Emergency Sessions	15.2.0
2018-09	SA#81	SP-180706	0268	-	F	Reference corrections in clause 6.10	15.2.0
2018-09	SA#81	SP-180709	0270	1	F	Algorithm Negotiation for Unauthenticated UEs in LSM	15.2.0
2018-09	SA#81	SP-180706	0272		F	AS SMC Handling Update	15.2.0
2018-09	SA#81	SP-180709	0273	1	F	Other security procedures for DC	15.2.0
2018-09	SA#81	SP-180707	0275	1	F	N32 related definitions	15.2.0
2018-09	SA#81	SP-180708	0276	1	F	Access Token Request updates	15.2.0
2018-09	SA#81	SP-180708	0277	1	F	Access Token Request for a specific NF service producer	15.2.0
2018-09	SA#81	SP-180709	0278	1	F	Editorial corrections to TS 33.501	15.2.0
2018-09	SA#81	SP-180709	0279	1	F	Corrections on primary authentication	15.2.0
2018-09	SA#81	SP-180706	0280	-	F	Delay the transmission of kseaf after home network verifies the RES	15.2.0
2018-09	SA#81	SP-180709	0284	1	F	Align AS SMC procedure with SA2 and RAN3	15.2.0
2018-09	SA#81	SP-180707	0287	1	F	Remove Editor's Note on additional claims in the access token	15.2.0
2018-09	SA#81	SP-180707	0288	1	F	Remove Editor's Note on additional parameters that may be required in step 1 of Figure 13.4.1.1-2	15.2.0
2018-09	SA#81	SP-180706	0290	-	B	CR-slice-management-security	15.2.0
2018-09	SA#81	SP-180706	0292	-	F	Authentication for token-based authorization	15.2.0
2018-09	SA#81	SP-180709	0295	1	F	DC - definition corrections	15.2.0
2018-09	SA#81	SP-180706	0301	-	F	DC - correcting reference	15.2.0
2018-09	SA#81	SP-180709	0302	1	F	Mobility - Clarification in intra-gNB-CU handover	15.2.0
2018-09	SA#81	SP-180708	0305	1	F	Mobility - Resolving EN and corrections in AS re-keying	15.2.0
2018-09	SA#81	SP-180708	0306	1	F	Mobility - Corrections for usage of local policy at AMF	15.2.0
2018-09	SA#81	SP-180708	0307	1	F	Mobility - Rectification of NAS MAC calculation for NAS Container	15.2.0
2018-09	SA#81	SP-180706	0309	-	F	Mobility - Correction of NAS COUNTs in N2-handover	15.2.0
2018-09	SA#81	SP-180706	0310	-	F	Mobility - Removing an EN in Xn-handover	15.2.0
2018-09	SA#81	SP-180706	0311	-	F	Mobility - Rectification of UE security capabilities in NAS Container	15.2.0
2018-09	SA#81	SP-180707	0313	1	F	Privacy - adding missing details to SUCI content and format	15.2.0
2018-09	SA#81	SP-180707	0314	1	F	Privacy - addressing ENs	15.2.0
2018-09	SA#81	SP-180709	0315	1	F	Update of definition of 5G AS security context for 3GPP access	15.2.0
2018-09	SA#81	SP-180708	0316	1	F	Use the old KRRCint for calculation of the security token in MSG3	15.2.0
2018-09	SA#81	SP-180707	0319	1	F	Removal of token validation by NRF	15.2.0
2018-09	SA#81	SP-180707	0323	-	F	Clarification of ngKSI and ABBA parameter in 5G-AKA	15.2.0
2018-09	SA#81	SP-180707	0324	1	F	Clarification for ngksi and ABBA parameter for EAP-AKA'	15.2.0
2018-09	SA#81	SP-180708	0327	1	F	Corrections and clarifications to interworking clauses	15.2.0
2018-09	SA#81	SP-180708	0328	1	F	Removal of editor's note on harmonization between inter and intra system handovers	15.2.0
2018-09	SA#81	SP-180708	0329	1	F	Clarifications related to the NAS Container calculation during inter system handover	15.2.0
2018-09	SA#81	SP-180706	0330	-	F	Addition of missing reference to RFC on DTLS over SCTP	15.2.0
2018-09	SA#81	SP-180709	0331	1	F	Correction of Note on physical protection for NDS/IP use	15.2.0
2018-09	SA#81	SP-180709	0334	1	F	Multiple NAS connections: taking a new security context into use on non-3GPP access	15.2.0
2018-09	SA#81	SP-180706	0336	-	F	Correction to Clause 5.11.2 Requirements for algorithm selection	15.2.0
2018-09	SA#81	SP-180709	0337	1	F	Removal of Note 2a on Kausf use case restriction	15.2.0
2018-09	SA#81	SP-180706	0339	-	D	Editorial correction to TS 33.501	15.2.0
2018-09	SA#81	SP-180707	0341	1	F	Clarification to key hierarchy	15.2.0
2018-09	SA#81	SP-180707	0342	1	F	Collection of editorial changes	15.2.0

2018-09	SA#81	SP-180708	0343	1	F	Addition of definitions and corrections to references	15.2.0
2018-09	SA#81	SP-180707	0344	1	F	Corrections to references and update on authentication vector text	15.2.0
2018-09	SA#81	SP-180707	0347	2-	F	Error handling for SBA authentication and authorization in service layer	15.2.0
2018-09	SA#81	SP-180707	0348	1	F	Clarification on authentication and authorization in SBA	15.2.0
2018-09	SA#81	SP-180709	0349	1	F	Adding OAuth related authorization services for SBA security	15.2.0
2018-09	SA#81	SP-180707	0354	1	F	Clarifications and editorials to clause 13.1 (Transport security for service based interfaces)	15.2.0
2018-09	SA#81	SP-180707	0355	-	F	Updates on Security Mechanism for Steering of Roaming	15.2.0
2018-09	SA#81	SP-180708	0360	1	F	Simplification of the UE handling of keys at handover	15.2.0
2018-09	SA#81	SP-180707	0362	1	F	CR on the registration procedure for mobility from EPS to 5GS	15.2.0
2018-09	SA#81	SP-180708	0363	1	F	CR on adding KAMF change flag in NAS SMC	15.2.0
2018-09	SA#81	SP-180708	0364	1	F	CR on corrections on the UP security policy confirmation	15.2.0
2018-09	SA#81	SP-180708	0365	1	F	CR on corrections on the UP security policy confirmation	15.2.0
2018-09	SA#81	SP-180708	0366	1	F	CR on corrections on the 5GS to EPS handover procedure	15.2.0
2018-09	SA#81	SP-180707	0367	-	F	Handling of initial value of CounterSoR	15.2.0
2018-09	SA#81	SP-180707	0368	-	F	Update on InactiveMAC-I calculation	15.2.0
2018-09	SA#81	SP-180707	0370	1	F	Clarification to the protection of attributes by the SEPP	15.2.0
2018-09	SA#81	SP-180707	0373	-	D	Editorial correction to 6.7.2 of 33.501	15.2.0
2018-09	SA#81	SP-180709	0374	-	B	Security mechanisms for non-SBA interfaces in 5GC	15.2.0
2018-09	SA#81	SP-180709	0375	-	F	Clarifications to 13.5	15.2.0
2018-09	SA#81	SP-180709	0376	-	B	Application layer security on the N32 interface	15.2.0

History

Document history		
V15.1.0	July 2018	Publication
V15.2.0	October 2018	Publication