**3GPP TSG-SA3 Meeting #117 *S3-24sid1***

Maastricht, Netherlands, 19th - 23rd Aug 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **DRAFT** | **rev** | **-** | **Current version:** | **18.X.Z** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network | **X** | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Adaptation of 256-bit algorithm for AS and NAS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | FS\_CAT256 | | | | |  | ***Date:*** | | | 2024-08-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | AS and NAS procedure is adapted with 256 bit algorithm during negotiation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Requirements for UE, gNB and AMF updated with 256 bit algorithm.  RRC security, NAS and UP security mechanishm is updated along with detailed inputs and outputs for 256 bit ciphering, integrity algorithm. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 256 bit algorithm cant be used without this change. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2, 5.3, 5.5, 5.11, 6.5, 6.6, 8.4, D.2, D.3, D.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS/TR 24.501,38.331 CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\* START OF CHANGES\*\*\*\*\*\*\*\*\*\*

# 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 for 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] Void

[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] Void

[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] Void.

[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 9113: "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] Void

[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] IETF 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".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] IETF RFC 9190: "EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3".

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

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] RFC 2818: "HTTP Over TLS".

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[94] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition".

[95] 3GPP TS 29.502: "5G System; Session Management Services".

[96] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services".

[97] 3GPP TS 23.402: "Authentication enhancements for non-3GPP accesses".

[98] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[99] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[100] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

[101] General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>.

[102] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[103] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services".

[104] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[105] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[106] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2.

[107] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1.

[108] 3GPP TS 26.502: "5G multicast–broadcast services; User Service architecture".

[109] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

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

[111] IETF RFC 4555 (2006-06): "RFC IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[112] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[x1] 3GPP TS 35.240: "Specification of the Snow 5G based 256-bits algorithm set: specification of the 256-NEA4 encryption, the 256-NIA4 integrity, and the 256-NCA4 authenticated encryption algorithm for 5G; Document 1: algorithm specification".

[x2] 3GPP TS 35.244: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G; Document 1: algorithm specification".

[x3] 3GPP TS 35.245: "Specification of the ZUC based 256-bits algorithm set: Specification of the 256-NEA6 encryption, the 256-NIA6 integrity, and the 256-NCA6 authenticated encryption algorithm for 5G; Document 1: algorithm specification".

[x4] 3GPP TS 35.241: "Specification of the Snow 5G based 256-bits algorithm set: Specification of the 256-NEA4 encryption, the 256-NIA4 integrity algorithm, and the 256-NCA4 authenticated encryption algorithm for 5G; Document 2: implementation test data".

[x5] 3GPP TS 35.244: Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G; Document 2: implementation test data".

[x6] 3GPP TS 35.247: Specification of the ZUC based 256-bits algorithm set: Specification of the 256-NEA6 encryption, the 256-NIA6 integrity, and the 256-NCA6 authenticated encryption algorithm for 5G; Document 2: implementation test data".

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 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] with the following additional requirement(s):

- The UE shall support the use of integrity protection with the ng-eNB over the Uu interface if it supports E-UTRA connected to 5GC.

- The UE shall indicate its support of integrity protection with the ng-eNB if it supports E-UTRA connected to 5GC.

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-NEA2,256-NEA1, 256-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 and 256-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 support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

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, 256-NIA1, 256-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3, 256-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 [22] 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 assessment 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 NG-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 Home Network Public Key Identifier shall be stored in the USIM.

The SUCI calculation indication, either USIM or ME calculating the SUCI, shall be stored in 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 SUCI calculation 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, Home Network Public Key Identifier, protection scheme identifier, Routing Indicator, and SUCI calculation indication 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, Home Network Public Key Identifier, protection scheme identifier, and SUCI calculation indication is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism. Routing Indicator can be updated, e.g., by OTA or as defined in clause 6.15.

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].

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 5.3 Requirements on the gNB

### 5.3.1 General

The security requirements given in this clause 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, 256-NEA1, 256-NEA2 as defined in Annex D of the present document.

The gNB may implement the following ciphering algorithm:

- 128-NEA3,256-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, 256-NIA1, 256-NIA2 as defined in Annex D of the present document.

The gNB may support the following integrity protection algorithm:

- 128-NIA3, 256-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 [22] 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 [5] 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

The following requirements apply:

- 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

The following requirements apply:

- 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 long term 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 implementations, 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.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 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, 256-NEA1, 256-NEA2 as defined in Annex D of the present document.

The AMF may support the following ciphering algorithm:

- 128-NEA3, 256-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, 256-NIA1, 256-NIA2 as defined in Annex D of the present document.

The AMF may support the following integrity protection algorithm:

- 128-NIA3, 256-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.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 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:

"00002" NEA0 Null ciphering algorithm;

"00012" 128-NEA1 128-bit SNOW 3G based algorithm;

"00102" 128-NEA2 128-bit AES based algorithm; and

"00112" 128-NEA3 128-bit ZUC based algorithm.

"01002" 256-NEA1 256-bit SNOW 5G based algorithm;

"01012" 256-NEA2 256-bit AES based algorithm; and

"01102" 256-NEA3 256-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]).

256-NEA1 is based on SNOW 5G (see TS 35.240 [x1]).

256-NEA2 is based on 256-bit AES (see TS 35.243 [x2]).

256-NEA3 is based on 256-bit ZUC (see TS 35.246 [x3]).

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:

"00002" NIA0 Null Integrity Protection algorithm;

"00012" 128-NIA1 128-bit SNOW 3G based algorithm;

"00102" 128-NIA2 128-bit AES based algorithm; and

"00112" 128-NIA3 128-bit ZUC based algorithm.

"01002" 256-NIA1 256-bit SNOW 5G based algorithm;

"01012" 256-NIA2 256-bit AES based algorithm; and

"01102" 256-NIA3 256-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]).

256-NIA1 is based on SNOW 5G (see TS 35.240 [x1]).

256-NIA2 is based on 256-bit AES (see TS 35.243 [x2]).

256-NIA3 is based on 256-bit ZUC (see TS 35.246 [x3]).

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 user plane (to be used between UE and 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.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

### 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 / 256-bit integrity algorithms as described in Annex D shall be set as follows.

The KEY input shall be equal to the KNASint 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 / 256-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.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

### 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 / 256-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, KNASenc, 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 / 256-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.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 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 / 256-NIA algorithms are specified in Annex D.

The input parameters to the 128-bit / 256-bit NIA algorithms as described in Annex D are the RRC message as MESSAGE, an 128-bit / 256-bit integrity key KRRCint 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 / 256-NEA algorithms are specified in Annex D.

The input parameters to the 128-bit / 256-bit NEA algorithms as described in Annex D are a 128-bit / 256-bit cipher Key KRRCenc 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.

### 6.5.3 RRC UE capability transfer procedure

The network should activate AS security (i.e., perform a successful AS SMC procedure) before running the RRC UE capability transfer procedure.

With the exception of unauthenticated emergency calls and the UEs using Control plane CIoT optimization,, if the network had acquired UE capabilities using RRC UE capability transfer procedure before AS security activation, then the network shall not store them locally for later use and shall not send them to other network entities. In that case, the network shall re-run the RRC UE capability transfer procedure after a successful AS SMC procedure.

NOTE 1: For UEs without AS security (e.g., UEs using Control Plane CIoT optimization), RRC UE radio capability transfer procedure cannot be protected.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 6.6 UP security mechanisms

### 6.6.1 UP security policy

The SMF shall provide UP security policy for a PDU session to the ng-eNB/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 ng-eNB/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 ng-eNB/gNB shall not overrule the UP security policy provided by the SMF. If the ng-eNB/gNB cannot activate UP confidentiality and/or UP integrity protection when the received UP security policy is "Required", the ng-eNB/gNB shall reject establishment of UP resources for the PDU Session and indicate reject-cause to the SMF. If the received UP security policy is "Not needed ", then the establishment of the PDU Session shall proceed as described in TS 23.502 [8]. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the ng-eNB can activate UP integrity protection.

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 ng-eNB/gNB to the target ng-eNB/gNB, the source ng-eNB/gNB shall include in the HANDOVER REQUEST message, the UE's UP security policy. If the UP security policy is ‘Required’, the target ng-eNB/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 ng-eNB/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 ng-eNB/gNB. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

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 ng-eNB/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 ng-eNB/gNB shall send the UE's UP security policy and corresponding PDU session ID received from the source ng-eNB/gNB to the SMF. The SMF shall verify that the UE's UP security policy received from the target ng-eNB/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 ng-eNB/gNB. This UP security policy information, if included by the SMF, is delivered to the target ng-eNB/gNB in the Path-Switch Acknowledge message. The SMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm.

If the target ng-eNB/gNB receives UE's UP security policy from the SMF in the Path-Switch Acknowledge message, the target ng-eNB/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 ng-eNB/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 ng-eNB/gNB receives both UE security capability and UP security policy, then ng-eNB/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 ng-eNB/gNB.

At an N2-handover the SMF shall send the UE's UP security policy to the target ng-eNB/gNB via the target AMF. The target ng-eNB/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 ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

At interworking-handover from EPS to 5GS, the SMF+PGW-C provides the UE's UP security policy to the target ng-eNB/gNB via the target AMF. The target ng-eNB shall determine from the UP security policy received from the AMF together with the UE indication that it supports user plane integrity protection with ng-eNB in UE EPS security capabilities (i.e. bit EIA7), whether to activate user plane integrity protection with the UE or not. The target ng-eNB/gNB shall reject all DRBs for which it cannot comply with the corresponding UP integrity protection policy in the UP security policy and indicate the reject-cause to the source MME via the target AMF. For all other DRBs, the target ng-eNB/gNB shall activate UP integrity protection per DRB according to the used UP security policy. Only if the UE indicates that it supports use of user plane integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection. If the target AMF detects in a Registration procedure following interworking-handover from EPS to 5GS, and becomes aware of that there is a mismatch between the UE EPS security capabilities received from the source MME and the one received from the UE, and that the target ng-eNB may not have the UE capability indicating UP IP support in UE EPS security capabilities, then the AMF shall send an N2 CONTEXT MODIFICATION REQUEST message to inform the target ng-eNB about the correct UE EPS security capabilities and target ng-eNB shall take the new UE EPS security capabilities into account.

### 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/ng-eNB as defined in Clause 6.6.1.



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/ng-eNB 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/ng-eNB does not have KUPint, the gNB/ng-eNB shall generate KUPint and UP integrity protection for such DRBs shall start at the gNB/ng-eNB. Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB/ng-eNB does not have KUPenc, the gNB/ng-eNB shall generate KUPenc and UP ciphering for such DRBs shall start at the gNB/ng-eNB.

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 KUPint, the UE shall generate KUPint 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 KUPenc, the UE shall generate KUPenc 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/ng-eNB.

If UP integrity protection is not activated for DRBs, the gNB/ng-eNB 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/ng-eNB 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 NG-RAN, shall be responsible for user plane data confidentiality protection.

The use and mode of operation of the 128-bit / 256-bit NEA algorithms are specified in Annex D.

The input parameters to the 128-bit / 256-bit NEA algorithms as described in Annex D are the message packet, an 128-bit / 256-bit cipher key KUPenc 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

#### 6.6.4.1 General

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

#### 6.6.4.2 UP integrity mechanisms between the UE and the gNB

The use and mode of operation of the 128-bit NIA / 256-bit NIA algorithms are specified in Annex D.

The input parameters to the 128-bit NIA / 256-bit NIA algorithms as described in Annex D are, the message packet, a 128-bit / 256-bit integrity key KUPint 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.

#### 6.6.4.3 UP integrity mechanisms between the UE and the ng-eNB

If the UE supports E-UTRA connected to 5GC, the UE shall indicate support of integrity protection by setting the EIA7 algorithm bit in 5G UE Security Capability IE (see clause 9.11.3.54 of TS 24.501 [35]) to indicate that the UE supports user plane integrity protection with an ng-eNB.

If the 128-NIA / 256-NIA algorithm is signalled by the ng-eNB to the UE, clause 6.6.4.2 applies.

If the 128-EIA / 256-NIA algorithm is signalled by the ng-eNB to the UE, the following applies:

- The use and mode of operation of the 128-EIA / 256-EIA algorithms are specified in Annex B of TS 33.401 [10].

- The input parameters to the 128-bit / 256-bit EIA algorithms as described in Annex B of TS 33.401 [10] are, the message packet, a 128-bit / 256-bit integrity key KUPint 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, time and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

NOTE: The ng-eNB decides whether to signal 128-NIA / 256-NIA or 128-EIA / 256-EIA algorithm (cf. clause 5.3.1.2 of TS 36.331 [69]).

If the ng-eNB 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.

UE and the ng-eNB (or the ng-eNB acting as the MN) shall derive UP integrity key as specified in Annex A.7 of TS 33.401 [10], with the KeNB set to KgNB.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

#### 6.9.2.3 Key derivations during handover

##### 6.9.2.3.1 Intra-gNB-CU handover and intra-ng-eNB handover

The gNB shall have a policy deciding at which intra-gNB -CU handovers the KgNB can be retained and at which a new KgNB needs to be derived. At an intra-gNB-CU handover, the gNB shall indicate to the UE whether to change or retain the current KgNB in the HO Command message. Retaining the current KgNB shall only be done during intra-gNB-CU handover.

NOTE: The option of retaining the KeNB at intra-ng-eNB handover is not supported in ng-eNB.

If the current KgNB is to be changed, the gNB/ng-eNB and the UE shall derive a KNG-RAN\* as in Annex A.11/A.12 using target PCI, its frequency ARFCN-DL/EARFCN-DL, and either NH or the current KgNB depending on the following criteria: the gNB shall use the NH for deriving KNG-RAN\* 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 KNG-RAN\* from the current KgNB (this is referred to as a horizontal key derivation). The gNB shall send the NCC used for the KNG-RAN\*derivation to UE in HO Command message. The gNB/ng-eNB and the UE shall use the KNG-RAN\* as the KgNB, after handover.

If the current KgNB is to be retained, the gNB and the UE shall continue using the current KgNB, after handover.

NOTE 1: 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.

NOTE 2: The key derivation mechanism described in this clause is also applicable to CHO defined in TS 38.300[52].

##### 6.9.2.3.2 Xn-handover

In Xn handovers the source gNB/ng-eNB shall perform a vertical key derivation in case it has an unused {NH, NCC} pair. The source gNB/ng-eNB shall first compute KNG-RAN\* from target PCI, its frequency ARFCN-DL/EARFCN-DL, and either from currently active KgNB in case of horizontal key derivation or from the NH in case of vertical key derivation as described in Annex A.11/A.12.

Next, the source gNB/ng-eNB shall forward the { KNG-RAN\*, NCC} pair to the target gNB/ng-eNB. The target gNB/ng-eNB shall use the received KNG-RAN\* directly as KgNB to be used with the UE. The target gNB/ng-eNB shall associate the NCC value received from source gNB/ng-eNB with the KgNB. The target gNB/ng-eNB shall include the received NCC into the prepared HO Command message, which is sent back to the source gNB/ng-eNB in a transparent container and forwarded to the UE by source gNB/ng-eNB.

When the target gNB/ng-eNB 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 KAMF 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/ng-eNB in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The target gNB/ng-eNB 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 KAMF, 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 KgNB from the new KAMF 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 KgNB with a new NCC value equal to zero. Then, the AMF shall use {the derived new initial KgNB, 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/ng-eNB shall in this case set the value of *keySetChangeIndicator* field to true in further handovers. The gNB/ng-eNB should in this case perform an intra-gNB-CU/intra-ng-eNB handover immediately .

NOTE 1: 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/ng-eNB knows the target gNB/ng-eNB keys. The target gNB/ng-eNB can immediately initiate an intra-gNB-CU/intra-ng-eNB handover to take the new NH into use once the new NH has arrived in the PATH SWITCH REQUEST ACKNOWLEDGE message.

NOTE 2: The key derivation mechanism described in this clause is also applicable to CHO defined in TS 38.300[52].

##### 6.9.2.3.3 N2-Handover

Upon reception of the NGAP HANDOVER REQUIRED message, if the source AMF does not change the active KAMF (meaning no horizontal KAMF 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 KAMF 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 KAMF 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 KAMF, different from the 5G NAS security context on which the currently active 5G AS security context is based, but has not yet performed a UE Context Modification procedure, the Namf\_Communication\_CreateUEContext Request message shall in addition contain an indication that the KAMF sent by source AMF to target AMF is not in sync with the current KgNB used between the UE and the source gNB (i.e., keyAmfChangeInd) which means that AS key re-keying is required at the UE. Further, the source AMF shall derive a new KgNB associated with NCC=0 using the new KAMF and the uplink NAS COUNT from the last successful NAS SMC procedure with the UE and provide the {NH= newly derived KgNB, NCC=0} pair to the target AMF in the Namf\_Communication\_CreateUEContext Request message.

The source AMF uses its local policy to determine whether to perform horizontal KAMF derivation on currently active KAMF. If horizontal KAMF derivation is performed, the Namf\_Communication\_CreateUEContext Request shall contain an indication (i.e., keyAmfHDerivationInd ) that the new KAMF has been calculated, an indication (i.e., keyAmfChangeInd) that AS key re-keying is required at the UE, and the downlink NAS COUNT used in the horizontal derivation of the sent KAMF. The ngKSI for the newly derived KAMF key has the same value and the same type as the ngKSI of the current KAMF. Further, the source AMF shall derive a new KgNB associated with NCC=0 using the newly derived KAMF and the uplink NAS COUNT value of 232-1 as defined in Annex A.9. The source AMF shall include the{NH=newly derived KgNB, NCC=0} pair and the ngKSI for the newly derived KAMF key in the Namf\_Communication\_CreateUEContext Request as well.

NOTE a: The uplink NAS COUNT value for the initial KgNB derivation is set to 232-1. The reason for choosing such a value is to avoid any possibility that the value may be used to derive the same KgNB again.

The source AMF shall always increment the downlink NAS COUNT by one after sending the Namf\_Communication\_CreateUEContext Request message to the target AMF.

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 KAMF derivation (i.e., keyAmfHDerivationInd), it shall derive the NAS keys from the received KAMF 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 KAMF 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 KNASint key. The input parameters to the NAS 128-bit / 256-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 KNASint;

- COUNT : it shall be set to 232-1;

- 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 the value of the NAS connection identifier for 3GPP access.

The use of the 232-1 as the value of the COUNT for the purpose of NAS MAC calculation/verification does not actually set the NAS COUNT to 232-1. The reason for choosing such a value not in the normal NAS COUNT range, i.e., [0, 224‑1] 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 KAMF 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 ng-eNB/gNB. The purpose of this NASC could be compared to a NAS SMC message. If the target AMF receives the keyAmfChangeInd, it shall further send the received {NCC, NH} pair and the New Security Context Indicator (NSCI) to the target ng-eNB/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 1a: VoidNOTE 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 KAMF and {NH, NCC} pair received from the source AMF and then send the received {NH, NCC} pair to the target ng-eNB/gNB within the NGAP HANDOVER REQUEST message.

Upon receipt of the NGAP HANDOVER REQUEST message from the target AMF, the target ng-eNB/gNB shall compute the KNG-RAN\* to be used with the UE by performing the key derivation defined in Annex A.11 and A.12 with the {NH, NCC} pair received in the NGAP HANDOVER REQUEST message and the target PCI and its frequency ARFCN-DL/EARFCN-DL. The gNB uses the KNG-RAN\* corresponding to the selected cell as KgNB. The ng-eNB uses the KNG-RAN\* corresponding to the selected cell as KeNB. The target ng-eNB/gNB shall associate the NCC value received from AMF with the KgNB/KeNB. The target ng-eNB/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 ng-eNB/gNB had received the NSCI, it shall set the *keySetChangeIndicator* 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-CU, intra ng-eNB, Xn, or N2 with the exception that during intra-gNB-CU handover, the UE may retain the same key based on an indication from the gNB. The UE behaviour is also same in case of conditional handover, as specified in TS 38.300 [52], i.e., the UE shall use the parameters of the selected target cell in KNG-RAN\* derivations.

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 KAMF has been calculated (i.e., K\_AMF\_change\_flag is one),

- The UE shall compute the horizontally derived KAMF using the KAMF 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 KAMF. The UE shall further configure NAS security based on the horizontally derived KAMF 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 KAMF 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 verification of the NASC fails, the UE shall abort the handover procedure. Furthermore, the UE shall discard the new NAS security context if it was derived and continue to use the existing NAS and AS security contexts.

If *keySetChangeIndicator* 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 KAMF and the NAS COUNT value of 232-1 in the derivation of the temporary KgNB. The UE shall further process 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 ng-eNB/gNB via source ng-eNB/gNB is equal to the NCC value associated with the currently active KgNB/KeNB, the UE shall derive the KNG-RAN\* from the currently active KgNB/KeNB and the target PCI and its frequency ARFCN-DL/EARFCN-DL using the function defined in Annex A.11 and A.12.

- If the UE received an NCC value that was different from the NCC associated with the currently active KgNB/KeNB, 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 ng-eNB/gNB via the HO command message. When the NCC values match, the UE shall compute the KNG-RAN\* from the synchronized NH parameter and the target PCI and its frequency ARFCN-DL/EARFCN-DL using the function defined in Annex A.11 and A.12.

The UE shall use the KNG-RAN\* as the KgNB when communicating with the target gNB and as the KeNB when communicating with the target ng-eNB.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

## 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



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 .

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 KASME, 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 KAMF' key from the received KASME 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, 128-NEA2, 256-NEA4 and 256-NEA5 for NAS signalling ciphering, RRC signalling ciphering and UP ciphering;

b. 128-NIA1, 128-NIA2, 256-NIA4 and 256-NIA5 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., KNASenc and KNASint) from the new KAMF' 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 KAMF' key is defined such as the value is taken from the eKSI of the KASME key (i.e. included in the received EPS security context) and the type is set to indicate a mapped security context. The target AMF shall store the EPS NAS security algorithms received from the source MME in the mapped 5G security context. Similar to N2-Handover defined in Clause 6.9.2.3.3, the target AMF shall also set the NCC to zero and shall further derive the temporary KgNB using the mapped KAMF' key and the uplink NAS COUNT value of 232-1 as specified in Annex A.9.

The target AMF associates this mapped 5G Security context with ngKSI.

NOTE 3: The target AMF derives a temporary KgNB using the mapped KAMF' instead of using the {NH, NCC} pair received from the MME. The uplink NAS COUNT value for the initial KgNB derivation is set to 232-1. The reason for choosing such a value is to avoid any possibility that the value may be used to derive the same KgNB again.

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 KAMF' and the NCC value associated with the NH parameter used in the derivation of the KAMF'. 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 232-1.

The target AMF shall increment the downlink NAS COUNT by one after creating a NAS Container.

4. The target AMF requests the target gNB/ng-eNB 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 {NCC=0, NH=derived temporary KgNB}, the New Security Context Indicator (NSCI), and the UE security capabilities in the Handover Request message to the target gNB/ng-eNB. 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.

5. The target gNB/ng-eNB shall selects the 5G AS security algorithms from the list in the UE security capabilities

The target gNB/ng-eNB shall compute the KgNB to be used with the UE by performing the key derivation defined in Annex A.11 with the {NCC, NH} pair received in the Handover Request message and the target PCI and its frequency ARFCN-DL. The target gNB/ng-eNB shall associate the NCC value received from AMF with the KgNB.The target gNB /ng-eNB shall then derive the 5G AS security context, by deriving the 5G AS keys (KRRCint, KRRCenc, KUPint, and KUPenc) from the KgNB and the selected 5G AS security algorithm identifiers as described in Annex A.8 for gNB and in Annex A.7 in TS 33.401[10].

The target gNB/ng-eNB sends a Handover Request Ack message to the target AMF. Included in the Handover Request Ack message is the Target to Source Container, which contains the selected 5G AS algorithms, the *keySetChangeIndicator*, the NCC value from the received {NH, NCC} pair, and the NAS Container received from the target AMF. If the target gNB/ng-eNB had received the NSCI, it shall set the *keySetChangeIndicator* field to true, otherwise it shall set the *keySetChangeIndicator* field to false.

6. The target AMF sends the Forward Relocation Response message to the source MME. The required security parameters obtained from gNB/ng-eNB 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 Container obtained from the target AMF in step 6.

8. The UE derives a mapped KAMF' key from the KASME in the same way the AMF did in step 3. It shall also derive the 5G NAS keys and KgNB corresponding to the AMF and the target gNB/ng-eNB in step 3 and step 5. The UE shall further set the selected EPS NAS security algorithms in the 5G security context to the NAS security algorithms used with the source MME. It associates this mapped 5G security context with the ngKSI included in the NAS Container. The UE shall verify the NAS MAC in the NAS Container.

If verification of the NAS MAC fails, the UE shall abort the handover procedure. Furthermore, the UE shall discard the new NAS security context if it was derived and continue to use the existing NAS and AS security contexts.

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/ng-eNB. This shall be ciphered and integrity protected by the AS keys in the current 5G security context.

10. The target gNB/ng-eNB 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 UE shall use the mapped 5G security context to protect the subsequent Registration Request message over 3GPP access. The target AMF shall validate the integrity of the Registration Request message using the mapped security context. Upon successful validation, the target AMF shall send a context request message to the old AMF and shall include the additional GUTI and an indication that the UE is validated. Upon receiving the context request message with the indication that the UE is validated, the old AMF shall skip the integrity check and transfer the native 5G security context to the target AMF.The AMF shall retrieve the native security context using the 5G GUTI. If the AMF determines to activate the native security context, the AMF shall perform a NAS SMC procedure.

NOTE 5: It is up to AMF when to activate the native 5G security context.

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.

If the AMF has no native 5G security context available when the UE performs the Registration Request (protected by the mapped 5G security context) following the handover procedure, then the AMF via the SEAF should run a primary authentication depending on local operator policy.

The handling of security contexts in the case of multiple active NAS connections in the same PLMN’s serving network is given in clasue 6.4.2.2.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

# 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.2.2 256-bit Ciphering algorithms

### D.2.2.1 Inputs and outputs

The input parameters to the ciphering algorithm are a 256-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.2.2.1-1 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.2.2.1-1: 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.2.2.2 256-NEA1

256-NEA4 is based on SNOW 5G.

### D.2.2.3 256-NEA2

256-NEA5 is based on 256-bit AES.

### D.2.2.4 256-NEA3

256-NEA3 is based on ZUC.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

# 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.3.2 256-Bit integrity algorithms

### D.3.2.1 Inputs and outputs

The input parameters to the integrity algorithm are a 256-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.3.2.1-1 illustrates the use of the integrity algorithm NIA to authenticate the integrity of messages.



Figure D.3.2.1-1: 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.3.2.2 256-NIA1

256-NIA4 is based on SNOW 5G.

### D.3.2.3 256-NIA2

256-NIA5 is based on 256-bit AES.

### D.3.2.4 128-NIA3

256-NIA6 is based on ZUC.

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE\*\*\*\*\*\*\*\*\*\*

# 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.

## D.4.8 256-NEA4

For 256-NEA4 is the test data for SNOW 5G based 256-bit algorithm in TS 35.241[x4].

## D.4.9 256-NIA4

For 256-NIA4 test data for SNOW 5G based 256-bit algorithm in TS 35.241[x4].

## D.4.10 256-NEA5

For 256-NEA5 is the test data for AES based 256-bit algorithm in TS 35.244[x5].

## D.4.11 256-NIA5

For 256-NIA5 test data for AES based 256-bit algorithm in TS 35.244[x5].

## D.4.12 256-NEA6

For 256-NEA6 is the test data for ZUC based 256-bit algorithm in TS 35.247[x6].

## D.4.13 256-NIA6

For 256-NIA6 test data for ZUC based 256-bit algorithm in TS 35.247[x6].

\*\*\*\*\*\*\*\*\*\* END OF CHANGES\*\*\*\*\*\*\*\*\*\*