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

Maastricht, The Netherlands, 19th - 23rd August 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | **18.6.0** |  |
|  | | | | | | | | |
| *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:*** | Algorithm identifier values for 256-bit algorithms | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | KDDI | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TBD | | | | |  | ***Date:*** | | | 2024-MM-DD |
|  |  | | | |  | |  | | |  |
| ***Category:*** | C |  | | | | | ***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:*** | | It was agreed in SA3 #116 to assign algorithm identifier values for 256-bit ciphering and integrity protection algorithms as the conclusion of FS\_CAT256. With new identifier values, UE can notify its support of 256-bit algorithms in UE security capability and 256-bit algorithms can be selected during NAS and AS security mode command. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This contribution specifies new algorithm identifier values for 256-bit encryption and integirity protection algorithms and defines their use as optional. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 256-bit cryptographic algorithms cannot not be used on the air interface. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.1.3, 5.2.2, 5.2.3, 5.3.2, 5.3.3, 5.5.1, 5.5.2, 5.11.1, 6.2.2.1, 6.2.2.2, 6.4.3.1, 6.4.4.1, 6.5.1, 6.5.2, 6.6.3, 6.6.4.2, 6.9.2.3.3, D.2, D.3, D.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... 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 CHANGE\*\*\*

# 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".

[A] 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".

[B] 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".

[C] 3GPP TS 35.242: "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 3: design conformance test data".

[D] 3GPP TS 35.243: "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".

[E] 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".

[F] 3GPP TS 35.245: "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 3: design conformance test data".

[G] 3GPP TS 35.246: "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".

[H] 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".

[I] 3GPP TS 35.248: "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 3: design conformance test data".

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF NEXT CHANGE\*\*\*

# 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 NG-RAN related to keys

The 5GC and NG-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 5GC and NG-RAN may allow for use of encryption and integrity protection algorithms for AS and NAS protection having keys of length 256 bits.

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

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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 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; and

256-NEA4, 256-NEA5, 256-NEA6 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 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; and

256-NIA4, 256-NIA5, 256-NIA6 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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 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; and

- 256-NEA4, 256-NEA5, 256-NEA6 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; and

- 256-NIA4, 256-NIA5, 256-NIA6 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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 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; and

- 256-NEA4, 256-NEA5, 256-NEA6 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; and

- 256-NIA4, 256-NIA5, 256-NIA6 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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;

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

"01002" 256-NEA4 256-bit Snow 5G based algorithm;

"01012" 256-NEA5 256-bit AES-256 based algorithm; and

"01102" 256-NEA6 256-bit ZUC-256 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-NEA4 is based on Snow 5G (see TS 35.240 [A]).

256-NEA5 is based on 256-bit AES-256 (see TS 35.243 [D]).

256-NEA6 is based on 256-bit ZUC-256 (see TS 35.246 [G]).

Full details of the algorithms are specified in Annex D.

NOTE: TS 35.240 [A], TS 35.243 [D], and TS 35.246 [G] respectively specify 256-NCA4, 256-NCA5, and 256-NCA6 authenticated encryption algorithms, and these algorithms are prepared for future use.

#### 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;

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

"01002" 256-NIA4 256-bit Snow 5G based algorithm;

"01012" 256-NIA5 256-bit AES-256 based algorithm; and

"01102" 256-NIA6 256-bit ZUC-256 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-NIA4 is based on Snow 5G (see TS 35.240 [A]).

256-NIA5 is based on 256-bit AES-256 (see TS 35.243 [D]).

256-NIA6 is based on 256-bit ZUC-256 (see TS 35.246 [G]).

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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF NEXT CHANGE\*\*\*

#### 6.2.2.1 Keys in network entities

***Keys in the ARPF***

The ARPF shall process the long-term key K and any other sensitive data only in its secure environment. 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 KAUSF 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 KAUSF from CK' and IK' for EAP-AKA' as specified in clause 6.1.3.1. In case that 5G AKA is used as authentication method, the UDM/ARPF shall generate the KAUSF as specified in clause 6.1.3.2.

The KAUSF may be stored in the AUSF between two subsequent authentication and key agreement procedures.

When the AUSF stores the KAUSF, the AUSF shall store the latest KAUSF generated after successful completion of the latest primary authentication. The authentication is considered as successful and the AUSF shall store the latest KAUSF or replace the old KAUSF with the new KAUSF (if the AMF(s) end up selecting the same AUSF instance for (re)authentication of the UE):

- in case 5G AKA is used as authentication method, when the RES\* and the XRES\* are equal (see clause 6.1.3.2.0, Step 11).

- in case EAP-AKA' is used as authentication method, when the AUSF sends an EAP-Success message to the SEAF (see clause 6.1.3.1, Step 10).

The AUSF shall generate the anchor key, also called KSEAF, 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, KSEAF, from the AUSF upon a successful primary authentication procedure in each serving network.

The SEAF shall never transfer KSEAF to an entity outside the SEAF. Once KAMF is derived KSEAF shall be deleted.

The SEAF shall generate KAMF from KSEAF immediately following the authentication and key agreement procedure and hands it to the AMF.

NOTE 1: This implies that a new KAMF, along with a new KSEAF, 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 KAMF from the SEAF or from another AMF.

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

NOTE 3: The precise rules for key handling in inter-AMF mobility can be found in clause 6.9.3.

The AMF shall generate keys KNASint and KNASenc dedicated to protecting the NAS layer.

The AMF shall generate access network specific keys from KAMF. In particular,

- the AMF shall generate KgNB 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 KN3IWF and transfer it to the N3IWF when KAMF is received from SEAF, or when KAMF' is received from another AMF.

***Keys in the NG-RAN***

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

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

***Keys in the N3IWF***

The N3IWF receives KN3IWF from the AMF.

The N3IWF shall use KN3IWF 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.

n in the figure 6.2.2-2 equals to the key length of the algorithm.



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

NOTE 4: The key derivation and distribution scheme for standalone non-public networks, when an authentication method other than 5G AKA or EAP-AKA' is used, is given in Annex I.2.3.

#### 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.

n in the figure 6.2.2-2 equals to the key length of the algorithm.



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 KAUSF 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.

The UE shall store the latest KAUSF or replace the old KAUSF with the latest KAUSF, after successful completion of the latest primary authentication . If the USIM supports 5G parameters storage, KAUSF shall be stored in the USIM. Otherwise, KAUSF shall be stored in the non-volatile memory of the ME.

In case 5G AKA is used as an authentication method, upon receiving the valid NAS Security Mode Command message from the AMF (to take the corresponding partial context derived from the newly generated KAUSF into use), the UE shall consider the performed primary authentication as successful and the UE shall store the newly generated KAUSF as the latest KAUSF or replace the old KAUSF with the latest KAUSF.

In case of any key generating EAP method in the present document (EAP-AKA'', EAP-TLS in Annex B, EAP methods in Annex I) is used as the authentication method for the primary (re)authentication, upon receiving the EAP-Success message, the primary authentication shall be considered as successful and the UE shall store the newly generated KAUSF as the latest KAUSF or replace the old KAUSF with the latest KAUSF.

The ME shall perform the generation of KSEAF from the KAUSF. 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 KAMF. If the USIM supports 5G parameters storage, KAMF 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 KAMF.

Any 5G security context, KAUSF and KSEAF 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.

When the ME is powered up and the USIM supports the 5G parameters storage but does not support the 5G parameters extended storage, and the USIM has a stored KAUSF, then the UE may delete the KAUSF and associated 5G security context that are stored at the USIM and set the KSI value of ngKSI to '111'.

NOTE A: The above handling can be used to prevent a stored CounterSoR and CounterUPU being associated with the wrong KAUSF. Further criteria for deleting the security information are left to the ME implementation.

NOTE 1: The key derivation and distribution scheme for standalone non-public networks, when an authentication method other than 5G AKA or EAP-AKA' is used, is given in Annex I.2.3.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF NEXT CHANGE\*\*\*

#### 6.4.3.1 NAS input parameters to integrity algorithm

The input parameters to the NAS 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 integrity algorithms are specified in Annex D.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF NEXT CHANGE\*\*\*

#### 6.4.4.1 NAS input parameters to confidentiality algorithm

The input parameters for the NAS 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 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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 integrity algorithms are specified in Annex D.

The input parameters to the integrity algorithms as described in Annex D are the RRC message as MESSAGE, an 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 ciphering algorithms are specified in Annex D.

The input parameters to the ciphering algorithms as described in Annex D are a 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF NEXT CHANGE\*\*\*

### 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 ciphering algorithms are specified in Annex D.

The input parameters to the ciphering algorithms as described in Annex D are the message packet, a 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 integrity algorithms are specified in Annex D.

The input parameters to the integrity algorithms as described in Annex D are, the message packet, a 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF NEXT CHANGE\*\*\*

##### 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 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: Void.

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 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.

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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 and the output from the 256-bit ciphering algorithm are the same as those of 128-bit ciphering algorithms except they take a 256-bit keys.

### D.2.2.2 256-NEA4

256-NEA4 is based on Snow 5G and specified in [A].

### D.2.2.3 256-NEA5

256-NEA5 is based on AES-256 and specified in [D].

### D.2.2.4 256-NEA6

256-NEA6 is based on ZUC-256 and specified in [G].

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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 and the output from the 256-bit integrity algorithm are the same as those of 128-bit integrity algorithms except they take a 256-bit keys.

### D.3.2.2 256-NIA4

256-NIA4 is based on Snow 5G and specified in [A].

### D.3.2.3 256-NIA5

256-NIA5 is based on AES-256 and specified in [D].

### D.3.2.4 256-NIA6

256-NIA6 is based on ZUC-256 and specified in [G].

\*\*\*END OF CHANGE\*\*\*

\*\*\*START OF 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

The test data for 256-NEA4 is given in [B] and [C].

## D.4.9 256-NEA5

The test data for 256-NEA5 is given in [E] and [F].

## D.4.10 256-NEA6

The test data for 256-NEA6 is given in [H] and [I].

## D.4.11 256-NIA4

The test data for 256-NIA4 is given in [B] and [C].

## D.4.12 256-NIA5

The test data for 256-NIA5 is given in [E] and [F].

## D.4.13 256-NIA6

The test data for 256-NIA6 is given in [H] and [I].

\*\*\*END OF CHANGE\*\*\*