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

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Algorithm identifier values for 256-bit algorithms |
|  |  |
| ***Source to WG:*** | KDDI |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TBD |  | ***Date:*** | 2024- |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 canbe 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 valuse for 256-bit encyrpiton 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 gives changes for new algorithm identifier values for 256-bit encryption and integirity protection algorithms. |
|  |  |
| ***Consequences if not approved:*** | 256-bit algorithms will not be used. |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*START OF 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;

"10012" 256-NEA4 256-bit Snow 5G based algorithm;

"10102" 256-NEA5 256-bit AES-256 based algorithm; and

"10112" 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.

#### 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;

"10012" 256-NIA4 256-bit Snow 5G based algorithm;

"10102" 256-NIA5 256-bit AES-256 based algorithm; and

"10112" 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\*\*\*

# 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\*\*\*

# 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\*\*\*