|  |
| --- |
| 3GPP TR ab.cde Vx.y.z (yyyy-mm) |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects<Title>(Release 20) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttps://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 7

3 Definitions and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Use of cryptographic algorithms on 5G air interface 9

4.1 NAS Security 9

4.2 AS Security 9

5 Introduction to AEAD 10

5.1 Protection provided by AEAD 10

5.2 Algorithm inputs and outputs 10

5.3 Order of operations 10

6 Procedures and protocols impacted by AEAD 12

6.1 Creation and Handling of algorithm inputs 12

6.1.1 Cryptographic keys 12

6.1.2 Nonce 12

6.1.3 Associated Data 12

6.2 Impact to AS and NAS security 13

6.2.1 AEAD algorithm selection 13

6.2.2 Order of ciphering and integrity protection 13

6.3 Interworking scenarios 14

7 Potential Requirements 15

8 Conclusion 16

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

This study aims to identify potential challenges and requirements for supporting AEAD algorithms [1, 2, 3] for NAS and AS security (including control and user plane security) in the 6G System, including the following:

* Impact to AS and NAS security
* Key hierarchy and management to support AEAD algorithms
* Negotiation of encryption and/or integrity protection when using AEAD algorithms
* Creation and handling of AEAD algorithm inputs, such as Nonce and Associated Data

Co-existence of AEAD-compatible systems and legacy deployments and algorithms (i.e., only AEAD algorithms or both AEAD and standalone algorithms) should be taken into account.

# 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 33.331 “NR; Radio Resource Control (RRC); Protocol specification”

[2] 3GPP TS 38.323: “NR; Packet Data Convergence Protocol (PDCP) specification”.

[3] 3GPP TS 35.240 Specification of the Snow 5G based 256-bits algorithm set

[4] 3GPP TS 35.243 Specification of the AES based 256-bits algorithm set

[5] 3GPP TS 35.246 Specification of the ZUC based 256-bits algorithm set

[6] Antoine Joux, Authentication Failures in NIST version of GCM

[7] Mihir Bellare, Chanathip Namprempre, Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm

[8] Hugo Krawczyk, The Order of Encryption and Authentication for Protecting Communications (Or: How Secure is SSL)

[9] RFC 5116, “Authenticated Encryption with Associated Data”

[10] S3-241495, “Reply LS on request to change integrity algorithm of 256-NIA3/256-NCA3”

[11] S3-242733, “Recent Attack on polynomial based MACs with short tag”

# 3 Definitions and abbreviations

## 3.1 Terms

Void

## 3.2 Symbols

Void

## 3.3 Abbreviations

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

AE Authenticated Encryption

AEAD Authenticated Encryption with Associated Data

EtM Encrypt-then-MAC

E&M Encrypt & MAC

MtE MAC-then-Encrypt

SMC Security Mode Command

# 4 Use of cryptographic algorithms on 5G air interface

## 4.1 NAS Security

The Non-Access Stratum (NAS) protocol protects Control Plane communication between the UE and the Core Network using separate ciphering and integrity protection algorithms. The supported ciphering and integrity protection algorithms are sent as part of the UE security capabilities from the UE to the AMF as part of the initial NAS message. These capabilities are then compared with two separate, prioritized lists of algorithms supported by the network –one for ciphering algorithms, one for integrity protection algorithms– that are stored in the AMF. After determining the ciphering and integrity protection algorithms to be used as per the network’s priority, the AMF sends this selection to the UE as part of the NAS Security Mode Command (SMC) message.

Similar to the algorithm negotiation, the activation of NAS security also happens separately for ciphering and integrity protection. First, the AMF initiates downlink integrity protection before sending the NAS SMC message to the UE. Afterwards, it also activates NAS uplink deciphering. Following the receipt and validation of the NAS SMC message, the UE activates uplink and downlink ciphering as well as integrity protection and responds to the AMF with a NAS Security Mode Complete message. Finally, the AMF also activates downlink ciphering.

Both operations use separate cryptographic keys for ciphering and integrity protection. Besides this secret key, KEY (KNASenc or KNASint), other inputs to the NAS security algorithms include BEARER, DIRECTION, and COUNT. If both ciphering and integrity protection are activated, the NAS protocol specifies that messages are first encrypted and then integrity protected (Encrypt-then-MAC) [1].

## 4.2 AS Security

Access Stratum (AS) security, protecting Control Plane and User Plane communication between the UE and the RAN, is provided by the Packet Data Convergence Protocol (PDCP) protocol. As for NAS security, ciphering and integrity protection are ensured by separate ciphering and integrity protection algorithms selected during the AS SMC procedure.

AS Security activation also works similarly to NAS SMC. One difference is that uplink ciphering by the UE and uplink deciphering by the RAN is only activated after the Security Mode Complete message.

Both ciphering and integrity protection operations use separate cryptographic keys for Control Plane and User Plane, KRRCenc / KRRCint and KUPenc / KUPint respectively. The input parameters include the secret key, KEY, and the BEARER. Once ciphering and integrity protection are activated, the order of operations is opposite to that of NAS security. For each PDCP message, first a Message Authentication Code (MAC) tag is created for integrity protection, and then the message is encrypted (MAC-then-Encrypt) [2].

# 5 Introduction to AEAD

## 5.1 Protection provided by AEAD

Authenticated Encryption (AE) is an operating mode for cryptographic algorithms. The key characteristic of AE is that ciphering, and integrity protection are executed in a combined operation, producing both a ciphertext and a MAC tag. This way, data encryption and authentication can ideally be provided in a single pass. Authenticated Encryption with Associated Data (AEAD) additionally allows for input that is authenticated, but not encrypted. This can be leveraged in use cases where solely data integrity is required while the plain text remains visible for processing.

Additionally, AEAD algorithms allow selective ciphering and integrity protection as needed. If only ciphering is required, only the resulting ciphertext is used. If only integrity protection is required, only the plain text and the resulting MAC tag is used. Finally, it is also possible to combine both approaches and provide ciphering and integrity protection for one part of a message while another part is only integrity protected (e.g., because certain message contents need to be accessible in plain text).

The 256-bit cryptographic algorithms specified by ETSI SAGE are all based on AEAD1, which also allows for confidentiality protection, integrity protection, and a combined AEAD mode. ETSI SAGE has specified the below indicators for different algorithm options based on SNOW 5G, AES-256, and ZUC-256 [3] [4] [5].

|  |  |
| --- | --- |
|  | **Cryptographic algorithm** |
| **Snow 5G** | **AES-256** | **ZUC-256** |
| **Operating mode** | **Confidentiality**  | 256-NEA4 | 256-NEA5 | 256-NEA6 |
| **Integrity** | 256-NIA4 | 256-NIA5 | 256-NIA6 |
| **Authenticated Encryption with Associated Data (AEAD)** | 256-NCA4 | 256-NCA5 | 256-NCA6 |

**Table X: 256-bit cryptographic algorithms specified in by ETSI SAGE**

## 5.2 Algorithm inputs and outputs

The inputs required are the plain text, a single cryptographic key for encryption and integrity protection, a unique nonce, to ensure that the ciphertext does not leak information, and associated data.

The expected outputs vary on the performed of operations. If only encryption is applied, the output will be a ciphertext. If only integrity protection is applied, the output will be a MAC tag. In case both are performed, the expected output would be both the ciphertext and the MAC tag.

## 5.3 Order of operations

Depending on the concrete AEAD scheme, the combination of integrity protection and encryption can vary. The following approaches are commonly used:

- Encrypt-then-MAC (EtM): The plaintext is encrypted first, then a MAC is generated from the resulting ciphertext.

- Encrypt-and-MAC (E&M): A MAC is generated from the plaintext, which is then encrypted without the MAC.

- MAC-then-Encrypt (MtE): A MAC is generated from the plaintext, and both are encrypted to produce a ciphertext.

Note 1: AEAD1, the AEAD operating mode specified by ETSI SAGE, employs the EtM approach [3] [4] [5].

Note 2: "Order of operations" here refers specifically to the sequence in which integrity protection and encryption are applied (i.e., how they are combined, and which operation occurs first). It does not determine whether both operations are performed or whether they are applied selectively (e.g., encryption only or integrity protection only).

Note 3: There are publications that suggest Encrypt-then-MAC (EtM) is preferable from a security perspective [7][8]. EtM ensures integrity is verified before decryption, making it resilient to attacks like padding oracle and chosen-cyphertext attacks [7][8]. In contrast Mac-then-Encrypt (MtE) may not be generally secure, even when the encryption function is secure and the MAC unforgeable [8].

# 6 Procedures and protocols impacted by AEAD

## 6.1 Creation and Handling of algorithm inputs

### 6.1.1 Cryptographic keys

The existing key hierarchy of the 5G System uses separate encryption and integrity protection keys (i.e., KNASenc/KNASint, KRRCenc/KRRCint, KUPenc/KUPint). In contrast, as outlined in section 5.2, AEAD algorithms commonly use a single cryptographic key which is then used for both encryption and MAC calculation.

If the 6G System is to support combined encryption and integrity protection only in scenarios where both are required, it may be possible to simplify the key hierarchy by using a single key for both operations (i.e., KNASaead, KRRCaead, KUPaead). Alternatively, if the 6G System is to also support separate encryption and integrity protection algorithms (e.g., 256-NEA4 and 256-NIA5), it may still be necessary to maintain separate encryption and integrity protection keys. In that case, it needs to be specified which cryptographic key is to be used in scenarios when a combined AEAD-mode is selected (i.e., 256-NCA4, 256-NCA5, 256-NCA5). Given the existing key hierarchy, the following options are possible:

|  |  |
| --- | --- |
| **Option** | **Description** |
| 1) Reuse an existing key for AEAD operation | Designate either the existing encryption key or the existing integrity protection key (KNASenc/KNASint, KRRCenc/KRRCint, KUPenc/KUPint) to be used when AEAD-mode is selected.  |
| 2) Add a new dedicated key for AEAD operation | Introduce a new dedicated AEAD key (e.g., KNASaead, KRRCaead, KUPaead) in addition to the existing encryption and integrity protection keys (KNASenc/KNASint, KRRCenc/KRRCint, KUPenc/KUPint) to be used when AEAD-mode is selected. |

**Table Y: Cryptographic Key Options for AEAD Algorithm in 6G**

Changes to the key hierarchy may also impact related procedures, such as key refresh and key re-keying. As per the current specification, when KAMF and KgNB are updated, the NAS Security keys (KNASenc, KNASint) and the AS Security keys (KRRCenc/KRRCint, KUPenc/KUPint) derived from them are updated as well. While the mechanism of key refresh and key re-keying may not change with the introduction of AEAD, the cryptographic key used with these algorithms will need to be updated accordingly.

### 6.1.2 Nonce

AEAD algorithms commonly require a nonce that is not to be reused as it ensures the uniqueness and integrity of the ciphertext. When a nonce is misused, in other words, a nonce is repeated for a given key, an attacker may be able to exploit the repetition to a forgery attack [6]. Therefore, constructing a nonce that is guaranteed not to repeat within a given session is essential to uphold AEAD security guarantees.

One possible way to construct a unique Nonce is by using the existing COUNT, BEARER and DIRECTION parameters, in alignment to the ciphering and integrity algorithms used today. While this method appears sufficient enough, further parameters in the AEAD-mode algorithm design may be considered to enhance resilience against potential nonce misuse.

### 6.1.3 Associated Data

Associated Data provides a mechanism for authenticating input without encrypting it, making it suitable for scenarios where only integrity protection is required. This enables AEAD algorithms to provide various levels of protection, depending on the result of the algorithm selection between UE and network.

Note: In addition to providing integrity-only protection for an entire message, Associated Data may also be used to provide selective integrity-only protection for parts of a message that do not need to be encrypted. Such use cases in the 3GPP System are still TBD.

## 6.2 Impact to AS and NAS security

### 6.2.1 AEAD algorithm selection

The current 5G System uses dedicated algorithms for encryption (NEA0, NEA1, NEA2, NEA3) and integrity protection (NIA0, NIA1, NIA2, NIA3) which are selected independently. This means a given session may use the same or different algorithms for encryption and integrity protection (including NULL), on both AS and NAS layer. Even when using AEAD algorithms that combine encryption and integrity protection, the option to select the NULL algorithm may still be required to signal the use of encryption only or integrity protection only.

In scenarios when both encryption and integrity protection are required, one aspect that needs to be specified is whether separate algorithms are to be supported (e.g., 256-NEA4 and 256-NIA4), or whether the system should implicitly choose the combined AEAD algorithm in such cases (e.g., 256-NCA4). The same also applies in cases when different algorithms are selected for encryption and integrity protection (e.g., 256-NEA4 and 256-NIA5). Since the existing 256-bit integrity protection algorithms all use the same Mac5G framework based on GMAC [10][11], the MAC computation is fundamentally the same.
Having to support both separate and combined encryption and integrity protection may complicate implementations without a tangible security benefit. Additionally, providing encryption and integrity protection in a single pass may be preferable in terms of performance to running the same algorithm twice.

Note: The common design of the 256-bit integrity protection algorithms and thus, the lack in algorithm diversity may be considered a security risk, especially considering recent cryptanalysis targeting polynomial-based MAC constructions [11].

Depending on the way that AEAD algorithms are selected, the NAS and AS SMC procedures may also be impacted. One option would be the implicit selection of the combined AEAD algorithms as outlined in the previous paragraph. Alternatively, the NCA algorithms could also be selected explicitly during the SMC procedure. In that case, both UE and network would need to support a separate, prioritized list for combined encryption and integrity protection algorithms.

As outlined in section 4, integrity protection and encryption are enabled at different times during the NAS and AS SMC procedure. On the network side, integrity protection is enabled before the Security Mode Command message is sent, and encryption is initiated after. On the UE side, both encryption and integrity protection are enabled at the same time once the Security Mode Command message is verified. To replicate this behaviour with the new 256-bit algorithms, the Security Mode Command message would be inputted as Associated Data to produce a MAC. Once the NAS/AS SMC message is received and verified by the UE, the Security Mode Complete message would be inputted as plain text to provide both encryption and integrity protection. Enabling encryption on the AMF side happens in two steps: first, uplink decryption after the Security Mode Command message is sent, and second, downlink encryption after the Security Mode Complete message is received. As such, the combined AEAD modes (256-NCA4, 256-NCA5, 256-NCA6) may only be activated by the AMF after successful completion of the NAS SMC procedure.

### 6.2.2 Order of ciphering and integrity protection

The Packet Data Convergence Protocol (PDCP) as specified in TS 38.323 [2] is responsible for data protection between the UE and the NG-RAN within the AS. The protocol specification states that integrity protection is to be performed first, and encryption of the MAC and plaintext is performed second. In other words, the order is MAC-then-Encrypt (MtE). The order of operation for the 256-bit algorithms based on AEAD1 is the opposite. The plaintext encrypted first, and then a MAC is generated from the resulting ciphertext (Encrypt-then-MAC / EtM). Hence, when adopting of these algorithms for AS Security, the following options are possible:

|  |  |
| --- | --- |
| **Option** | **Description** |
| 1) Replicate MtE through executing algorithm twice | The AEAD algorithm is run twice, first for integrity protection only and then for encryption only to replicate MtE (No changes to the PDCP protocol required). |
| 2) Update PDCP protocol to follow EtM approach | Change the order of encryption and integrity protection operation in the PDCP protocol to EtM (Changes to the PDCP protocol required). |

**Table Z: Options for adopting AEAD algorithms for AS security**

There may be potential security and performance benefits to Option 2. As outlined in Section 5.3, EtM ensures integrity is verified before decryption, making it resilient to certain attacks. Additionally, Option 2 would enhance time efficiency, as it would allow for AEAD to perform parallel keystream generation and integrity protection, thereby decreasing the overall time as compared to sequential execution of these steps.

Since the NAS protocol already follows the same order of encryption and integrity protection (i.e., Encrypt-then-MAC), it aligns with the specification of the algorithms based on AEAD1. Therefore, the order of operation for NAS security should not be impacted by the introduction of AEAD.

## 6.3 Interworking scenarios

Assuming that the 6G System will support (AEAD-compatible) 256-bit algorithms only, the following is to be addressed to ensure seamless interworking with (AEAD-incompatible) legacy systems.

The predominant challenge is the lack of support for 256-bit algorithms in legacy systems. In the case of interworking between 5G and EPS, security contexts can be mapped because the ciphering and integrity protection algorithms are the same (albeit labelled by different abbreviations). For interworking scenarios between a 128-bit-only system and a 256-bit-only system, it needs to be determined whether a security context mapping between cryptographic algorithms of different key lengths is acceptable at all, and if so, how such mappings are to be performed. It should also be considered that moving from 6G to legacy systems could entail a shift from using a single, combined AEAD algorithm to separate ciphering and integrity protection algorithms and vice versa.

# 7 Potential Requirements

TBD

# 8 Conclusion

 TBD