|  |
| --- |
| 3GPP TR 33.700-41 V0.3.0 (2024-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on enabling a cryptographic algorithm transition to 256-bits(Release 19) |
|   |
|  | 3GPP-logo_web |
|  |
| 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 16Internethttp://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.© 2022, 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 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Assumptions 8

5 Key issues 8

6 Solutions 8

7 Conclusions 8

Annex A (Informative): Considerations on 256-bit security 9

Annex B (Informative): Analysis of backwards compatibility 9

B.1 Introduction 9

B.2 Long-term key and key hierarchy 9

B.3 Impact on AS and NAS protocols 10

B.4 Impact on Dual connectivity 10

B.5 Impact on RRC Connection Re-establishment 10

B.6 Impact on Handovers and Interworking 11

Annex C: Change history 11

# 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

Thepresentdocument aims to address key requirements for introducing support for 256-bit symmetric algorithms into the 5G System as well as the coexistence of 128-bit and 256-bit cryptographic algorithms. Considering findings and conclusions from preceding work, the following points should be addressed as part of the present document:

Studying key issues and candidate solutions concerning the negotiation (selection) of key sizes between UE and network, including:

- Potential risks and impacts to the current system when supporting both 128-bit and 256-bit algorithms in parallel and the adoption of 256-bit algorithms in existing deployments where 128 bits is already supported, e.g. handover scenarios within 5G system

- How to prioritise the use of 256-bit algorithms and mitigate bidding-down attacks when negotiating key sizes;

- How to ensure 256-bit security is achieved concerning varying levels of support for 256-bit algorithms by different UEs and within the network; potential dependencies in key-length selection of AS and NAS layers

- Study the implications and requirements for the key hierarchies to support 256-bit cryptographic algorithms

- Study the implications and requirements to AKA procedures.

# 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 33.501: "Security architecture and procedures for 5G system".

[4] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS)".

[5] UK NCSC, "Next steps in preparing for post-quantum cryptography"
<https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography>

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

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

AES Advanced Encryption Standard

SMC Security Mode Command

ZUC Zu Chongzhi

# 4 Assumptions

The 5G System supports already procedures for the selection and activation of the AS and NAS security based on the UE security capabilities and network configuration.

The UE security capabilities IE is defined in TS 24.501 [4] clause 9.11.3.54. The IE includes already space for the introduction of new 5G algorithms, 4 for each type of algorithm (ciphering or integrity protection).

The NAS and AS SMC procedures described in TS 33.501 [3] in clauses 6.7.2 and 6.7.4 respectively enable the network and the UE to securely select and activate NAS and AS security based on the UE security capabilities and network configuration. Using NAS and AS SMC procedures to indicate UE the use of new 256-bit ciphering and integrity algorithms requires assigning an identity to these algorithms (which will then need to be reflected in the relevant specifications).

The UE security capabilities are sent to the network in an initial NAS message that can be unprotected. This is the reason why the 5G System supports a mechanism to protect against bidding down attacks by a man-in-the-middle tampering with the initial NAS message as pointed out in NOTE 1 of clause 6.7.2 of TS 33.501 [3]. This is the reason the UE security capabilities are replayed in the NAS SMC message.

# 5 Key issues

Void

# 6 Solutions

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Void

# 7 Conclusions

During the study, the following aspects on introducing new 256-bit encryption and integrity protection algorithms were discussed:

- 256-bit security,

- relation with the long-term key and key hierarchy,

- impacts on Access Stratum (AS) and Non-Access Stratum (NAS) protocols,

- impacts on Dual Connectivity,

- impacts on RRC-Reconnection,

- impacts on handover and interworking mechanisms, and

- backward compatibility.

No key issues were identified. Introduction of 256-bit key encryption and integrity protection algorithms was agreed. The algorithm identifier values for encryption and integrity protection algorithms based on AES-256, SNOW-5G and ZUC-256 are to be assigned in the normative work. It was concluded that there are currently no security threats to 128-NIA1,128-NIA2, 128-NIA3, 128-NEA1, 128-NEA2, 128-NEA3 specified in TS33.501[3] for the 5G System. The algorithm negotiations specified in TS33.501[3] already supports the adoption of new algorithms.

# Annex A (Informative): Considerations on 256-bit security

Several clarifications on the purpose of this study are provided here.

First, this study of introducing 256-bit of crypto algorithms is not intended to achieve 256-bit of security for an entire 5G system. Although a 256-bit symmetric crypto algorithm may be proven to have 256-bit of security in theory, it is difficult to claim such level of security in practice for a large system such as 5G, since many factors (e.g., key length) may affect security level.

Second, the purpose of this study is not intended to obsolete 128-bit crypto algorithms, since 128-bit crypto algorithms are still considered secure [5]. Rather, this study intends to introduce 256-bit crypto algorithms to coexist with existing 128-bit algorithms in 5G.

Third, since 128-bit crypto algorithms are still considered secure [5], no security threat has been identified from the introduction of 256-bit algorithms to coexist with 128-bit algorithms. Thus, no key issue is needed for this study.

# Annex B (Informative): Analysis of backwards compatibility

# B.1 Introduction

Introduction of any new algorithm into the 5G system will have a certain amount of impact. The deployment of the new algorithms will not take place everywhere all at once.

There are already today a set of algorithms specified for 5G (128-NEA-1,2,3 and 128-NIA-1,2,3). For AS and NAS protocols there are negotiation mechanisms in place that will help both peers of a connection to find a set of algorithms (one for confidentiality and one for integrity) that they share. The network operator is in control of the prioritization of the algorithms. The algorithm with the highest priority that both endpoints can agree on gets selected.

If the introduction of 256-bit key algorithms is considered as introduction of any new algorithms, it is a fair assumption that current mechanisms can be reused and provide equally strong negotiation protection for the 256-bit algorithms just by adding possibility to negotiate the new algorithms (i.e. define new algorithm identifiers/code points).

The purpose of this Annex is to discuss the different aspects of introducing 256-bit algorithms and its potential impact to the 5G system, especially in terms of backward compatibility when 128-bit and 256-bit algorithms are co-existed in the 5G system.

The current mechanisms allow for introducing new algorithms. That would work as described below.

The impact to key derivation and AS/NAS protocols will be described in clauses B.2 and B.3. For more detailed analysis of the impact to AS protocols, the impact to dual connectivity, RRC-reconnection, and handovers and interworking will be discussed in clauses B.4, B.5 and B.6.

# B.2 Long-term key and key hierarchy

The Key (or long-term key(s) of the subscription credential(s)) can be either 128 or 256 bits, see clause 6.2.2 of TS 33.501 [2]. If a 128-bit long-term key is used for authenticating the UE, all output keys in the 5G key hierarchy are 256 bits, which means that they need truncation to be used in 128-bit algorithms. The truncation is defined in Annex A.8 of TS 33.501 [2] as:

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

According to the above, when n=128, the 128 least significant bits of the output key are used, and when n=256, all of the bits of the output key are used.

It was confirmed that the existing key derivation function and truncation for generating keys for NAS, UP and RRC work for both 128-bit and 256-bit algorithms without any changes to the mechanisms.

# B.3 Impact on AS and NAS protocols

Clause 6.4.6 of TS 33.501 [2] defines the protection of initial NAS message, and one of the information elements in the initial NAS message is UE security capabilities. Therefore, the initial NAS message can carry the list of supported 256-bit algorithms if algorithm identifier values are assigned.

In clause 6.7.2 of TS 33.501 [2], the information element for NAS Security Mode Command is defined. Mandatory elements are the replayed UE security capabilities, the selected NAS algorithms, and the ngKSI for identifying the KAMF. H The key length is not involved in this procedure, and NAS Security Mode Command can be applied for 256-bit algorithms if corresponding algorithm identifier values are assigned to 256-bit algorithms.

The AS algorithms are selected between UE and gNB in the similar manner as NAS algorithms. Therefore, 256-bit AS algorithms can be adopted to AS algorithm selection.

It was agreed that 128-bit algorithms are still sufficiently secure for the 5G system and that no need to differentiate the security levels provided by128-bit and 256-bit algorithms. Therefore, from a specification perspective, 256-bit algorithms can be treated as an additional set of algorithms and the NAS and AS SMC procedures for negotiating algorithms between the UE and AMF and the UE and gNB respectively can be used.

What is needed is for the new algorithms to be assigned new identifiers in clause 5.11.1 of TS 33.501 [2] and that new code points are assigned in the UE security capability information element for the new encryption and integrity protection algorithms in stage 3 specifications.

# B.4 Impact on Dual connectivity

In NR-NR Dual Connectivity (NR-DC) the UE is simultaneously connected to more than one RAN node, a MN and a SN, see clause 6.10 of TS 33.501 [2].

The rules for setting up security contexts in Dual connectivity are very complex, but (very much simplified), it can be summarized so that if protection on the air interface is activated on one access, it needs to be active on the other access as well. There is no rule that the two accesses need to use the same air-interface security algorithms, see the NOTE in clause 6.10.3.3 of TS 33.501 [2].

It was confirmed that 128-bit algorithms are secure for the 5G system and that 256-bit algorithms are just a set of additional algorithms. Therefore, it is possible to use a 128-bit algorithm over one access and a 256-bit algorithm over the other access in Dual connectivity, reusing existing mechanisms.

# B.5 Impact on RRC Connection Re-establishment

When RRC connection is re-established, the same air-interface security algorithm as the source gNB can be selected between the UE and target gNB. However, this does not prohibit the algorithm negotiation between the UE and the target gNB, a new algorithm can be selected based on the UE security capability and the security policy of gNB.

When the new algorithm is to be selected between the UE and the target gNB, AS algorithm selection can be used. As discussed in B.3, AS algorithm selection can be used for both 128-bit and 256-bit algorithms if adequate algorithm identifier values are assigned.

It was confirmed that 128-bit algorithms are secure for the 5G system and that 256-bit algorithms are just a set of additional algorithms, then it is possible to use a 256-bit algorithm over one access and handover to an access that is using a 128-bit algorithm or vice versa.

# B.6 Impact on Handovers and Interworking

After a handover from one network that does not support the 256-bit air-interface security algorithms (e.g. a 4G network) to a network supporting one or more of the 256-bit algorithms, the AMF of the latter can run a new NAS SMC with UE to switch to the 256-bit algorithm. Hence, the UE does not "get stuck" in using the old type of algorithms, but the operator policy can take the UE's full UE security capability into account.

As discussed in B.3, NAS SMC can support both 128-bit and 256-bit algorithms if adequate algorithm identifier values are assigned.

It was confirmed that 128-bit algorithms are secure for the 5G system and that 256-bit algorithms are just a set of additional algorithms, then it is possible to use a 256-bit algorithm over one access and handover to an access that is using a 128-bit algorithm or vice versa. Therefore, there is no security issue identified for reusing the existing mechanisms in handovers and interworking scenarios.

Annex C:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-240330 |  |  |  | Document Skeleton | 0.0.1 |
| 2024-02 | SA3#115 | S3-241010 |  |  |  | Inclusion of the approved documents at SA3#115:S3-241008, S3-241009 | 0.1.0 |
| 2024-05 | SA3#116 | S3-242448 |  |  |  | Inclusion of the approved documents at SA3#116:S3-242447, S3-242450 | 0.2.0 |
| 2024-08 | SA3#117 | S3‑243655 |  |  |  | Inclusion of the approved documents at SA3#117:S3-242777, S3-242787, S3-243647, S3-243648 | 0.3.0 |
|  |  |  |  |  |  |  |  |