**3GPP TSG-SA3 Meeting #116 *draft\_S3-242449-r1***

Jeju, South Korea, 20th - 24th May 2024 merger of S3-242202 and S3-241873

**Source: Ericsson, CableLabs?, Charter Communications?**

**Title: Analysis of backwards compatibility**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is proposed to add the following Annex to the TR 33.700-41[1].***

# 2 References

[1] 3GPP TR 33.700-41 "Study on enabling a cryptographic algorithm transition to 256-bits"

# 3 Rationale

# 4 Detailed proposal

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

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

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

Annex X: Analysis of backwards compatibility

# X.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. Some deployments will not support the new algorithms at all. This is nothing new.

Table X.1-1 summarizes the possible scenarios of mixed cryptographic capabilities/policies, assuming that supporting/using only 256-bit crypto algorithms is allowed. It classifies scenarios into four categories, including authentication and key agreement (AKA), access security (AS), non-access security (NAS), and key derivation (KD). The three possible capabilities (128-bit only, 128-bit and 256-bit, and 256-bit only) are numbered by 1, 2, and 3 respectively. The label of a scenario is denoted as: <Category><UE capability>.<Network capability>. For example, AKA1.2 represents the case of authentication and key agreement where USIM/UE supports only 128-bit crypto algorithm, and network function (AUSF/UDM) supports both 128-bit and 256-bit crypto algorithms.

NOTE: it is assumed that AUSF and UDM will be upgraded at the same time and share the same crypto capabilities.

Table X.1-1 Scenarios of mixed crypto capabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | gNB | AMF/SEAF | AUSF/UDM |
|  |  | 128-bit | 128-bit &256-bit | 256-bit | 128-bit | 128-bit &256-bit | 256-bit | 128-bit | 128-bit &256-bit | 256-bit |
| USIM | 128-bit | N/A | N/A | N/A | N/A | N/A | N/A | AKA1.1 | AKA1.2 | AKA1.3 |
| 128-bit &256-bit | N/A | N/A | N/A | N/A | N/A | N/A | AKA2.1 | AKA2.2 | AKA2.3 |
| 256-bit | N/A | N/A | N/A | N/A | N/A | N/A | AKA3.1 | AKA3.2 | AKA3.3 |
| ME | 128-bit | AS1.1 | AS1.2 | AS1.3 | NAS1.1 | NAS1.2 | NAS1.3 | KD1.1 | KD1.2 | KD1.3 |
| 128-bit &256-bit | AS2.1 | AS2.2 | AS2.3 | NAS2.1 | NAS1.2 | NAS2.3 | KD2.1 | KD2.2 | KD2.3 |
| 256-bit | AS3.1 | AS3.2 | AS3.3 | NAS3.1 | NAS1.3 | NAS3.3 | KD3.1 | KD3.2 | KD3.3 |

There are already today a set of algorithms specified for 5G (128-NEA-1,2,3 and 128-NIA-1,2,3), where not all systems support all algorithms (only 1 and 2 are required). Still 5G works because it was designed with this in mind. 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). In fact, if this was not the case, there would be a vulnerability in the existing algorithm negotiation process.

The purpose of this Annex is to discuss the different aspects of introducing 256-bit algorithms and its potential impact to the 5G system.

The current mechanisms allow for introducing new algorithms. That would work as described below. It does not ensure 256-bit security for the system.

# X.2 256-bit security

One aspect of using algorithms with larger key size is to improve security i.e. getting approximately 256-bits of security instead of the approximately 128-bits of security.

NOTE: Although an algorithm can be proven to have x-bits of security, it is more difficult to say that an entire system has an exact level of security. Hence the usage of "approximately" above.

Since 128-bit key algorithms are still considered as being secure [XX], there is no immediate need to replace them with 256-bit variants in the 5G system for security purposes. Rather, the introduction of 256-bit algorithms should be understood as an enhancement driven by the need of increased throughput and explicitly not a need to repair a security vulnerability in the current 3GPP system. The approach taken in this study is to take it stepwise and study how 256-bit algorithms can coexist with 128-bit algorithms in 5G. However, this does not mean that the target is to achieve approximate 256-bit security for the entire 5G system when the new algorithms are used. Therefore any security improvements were not considered relevant.

It was decided that 256-bit key algorithms as any new algorithms that can be used together with the existing ones in 5G.

# X.3 Long-term key and key hierarchy

The long-term key(s) (LTK) of the subscription credential(s) can be either 128 or 256 bits, see clause 6.3.7 of TS 33.501 [2].

It may seem like a straightforward requirement to state that 256-bit algorithms need to be used together with 256-bit LTKs. However, this is not necessary unless the aim is to increase the security. When a 128-bit LTK is used to authenticate the UE (or rather subscription identifier), the resulting keys that are output from the authentication (CK, IK) are both of size 128. These keys are not used separately, but always in the concatenated form CK || IK. The concatenated keys are used as the key in the key derivation function (KDF) as defined in in Annex A.2 of TS 33.501 [2]. The output of the KDF is the 256-bit long KAUSF. In fact, all of the keys further down in the key hierarchy (clause 6.2 or TS 33.501 [2]) are of length 256-bits and can be used together with 256-bit algorithms.

As mentioned above, 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 key is used, and when n=256, all of the bits are used. This means that the existing key truncation works even if n = 256.

The above illustrates that even if the root key K (the LTK) is of size 128-bit, it is possible to reuse existing key hierarchy without any modifications when using it together with 256-bit key algorithms.

# X.4 Impact on AS and NAS protocols

It was agreed that 128-bit algorithms are still sufficiently secure and that 256-bit algorithms are just a set of additional algorithms, then NAS and AS negotiation algorithms can be used without any changes to the mechanisms.

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.

# X.5 Impact on Dual connectivity

 In Dual connectivity 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 confidentiality protection is activated on one access, it needs to be active on the other access as well. There is no rule that the two access need to use the same confidentiality algorithm, see the NOTE in clause 6.10.3.3 of TS 33.501 [2].

It was agreed that 128-bit algorithms are secure and that 256-bit algorithms are just a set of additional algorithms, then 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.

# X.6 Impact on Handovers and Interworking

If it can be accepted that 128-bit algorithms are secure 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.

After a handover from one network that does not support the new algorithms (e.g. a 4G network) to a network supporting the one or more of the new algorithms, the AMF of the latter can run a new NAS SMC with UE to switch to the newer (256-bit key) 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.

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