



Study on enabling a cryptographic algorithm transition to 256-bits

KDDI, NEC, Samsung, Deutsche Telekom, BSI, Lenovo,
NSA, KPN



Outline

- Background
- Justification
- Objectives
- Summary
- Appendix: Takeaways from SA3 conference call on 256-bit algorithms



Background

- 📶 3GPP SA3 has previously performed a study on the support of 256-bit algorithms for 5G in TR 33.841 (Rel.16, March 2019)
 - Conclusion: *`... it is proposed for evaluation of new algorithms [by ETSI SAGE] to start now`*
- 📶 ETSI SAGE finalized their evaluation on AES-256, SNOW-V, ZUC-256 ([S3-230642](#))
- 📶 Final version of TR 33.841 contains a number of unresolved Editor's notes
- 📶 SA3 has been discussing the transition to 256-bit algorithms
 - WID proposal presented at SA3#110: Introduction of 256-bit algorithms ([S3-230695](#))
 - Earlier version of this SID, presented at SA3#110 ([S3-230834](#))
 - Offline call on 256-bits was held May 9th (Refer to Appendix)

Note: The WID aims to create the required TSs and CRs to TS 33.501 to adopt 256-bit algorithm variants. The SID aims to resolve practical challenges related to the transition to those algorithms.



Justification

- 🌿 TR 33.841 leaves a number of important questions unanswered and practical challenges not covered associated with the transition to 256-bit algorithms
- 🌿 KDDI foresees challenges that require further study, including but not limited to:
 - Security risks associated to parallel support for 128 and 256-bit algorithms
 1. Risk of inconsistent key sizes being used at different points of the network
 2. Similar risk identified in 5G NSA deployment scenarios
 3. Ensuring sufficient entropy in long-term keys for 256-bit AS/NAS security algorithms
 - Other open questions
 1. Negotiation of MAC lengths between the UE and network as well as system and performance impacts associated with use of MAC tags longer than 32 bits
 2. Negotiation of key lengths between the UE and network as well as expected ABBA parameter values in context of transition



Objectives

-  This study aims to address open questions and practical challenges related to the transition of symmetric cryptographic algorithms in the 3GPP System to 256-bit:
- Study key issues and candidate solutions concerning the negotiation of key sizes between UE and network incl.:
 - Potential risks supporting 128-bit and 256-bit algorithms in parallel
 - If and how to utilize ABBA parameter
 - Study key issues and candidate solutions concerning the negotiation of MAC lengths between UE and network:
 - System and performance impacts associated with use of longer MACs
 - Secure negotiation of MAC lengths between UE and network
 - Study key issues and candidate solutions concerning varying levels of support for 256-bit algorithms in the UE and network:
 - Ensuring consistent use of 256-bit algorithms
 - Ensuring effective key length equals the key bit length



Summary

-  KDDI and its supporters see a need for further study on 256-bit cryptographic algorithms due to the following:
- Unanswered questions in current version of study on the support of 256-bit algorithms; TR 33.841
 - Potential security risks foreseen in the transition to 256-bits
 - Timely for a study as ETSI SAGE also just finalized their evaluation on 256-bit cryptographic algorithms



Appendix



Comments from 256-bit offline call (May 9th)

- Given the rising interest in 256-bit algorithms, SA3 held a conference call on the topic (contributions, meeting minutes can be found [on the 3GPP FTP server](#))
- Key takeaways regarding the proposed SID by KDDI:
 - SID proposed by KDDI is independent from the WID proposal on the adoption of 256-bit algorithms in 3GPP standards ([S3-230695](#))
 - Several IMs voiced support for proposal 1 in [S3-230834](#) on studying security challenges and candidate solutions concerning negotiation of key size & MAC length between UE and network
 - Worth studying the possibility of longer MACs, as suggested previously by ETSI SAGE ([S3-202851](#))
 - This SID intends to cover symmetric algorithms only