256bit Algorithm Discussion, May 9th 2023

1. 256 WID proposal/S3-23xxxx - was S3-230695 - New WID on Addition of 256 bit UP security Algorithms

[VF] presents and gives clarification on new algorithm(s), output, regulation, etc.

[Huawei] comments on dates, Mar 2023 needs correction.

[QC] comments.

[Ericsson] comments the regulation problem should be solved, it is happened in 3G/4G era. It needs to be solved.

[SAGE] asks whether 256 bit algorithms needs to written in those 6 specifications or not. All algorithms are record in ETSI specifications.

[Ericsson] comments on last paragraph of objective.

Chair tries to clarify Ericsson’s comments as asking whether it is mandated to support 256 algorithm in 5G from Rel-19 onwards

[Huawei] asks why to emphasize user plane, why control plane excluded.

[VF] clarifies there is bigger risk for user plane. If control plane need to be included, happy to include it.

Chair clarifies there is no way to distinguish CP and UP algorithm separately currently, there is only one negotiation applicable for both.

[QC] supports to have control plane at same time.

[SAGE] comments on tag length.

[Huawei] prefers to have new algorithm for both CP and UP.

[Apple] (no show)

[Huawei] proposes to remove “user plane” in objective.

Chair asks to pay attention on Ericsson’s comment about deploying 256bit algorithm in 5G.

[VF] replies.

[Ericsson] replies.

[QC] comments about time to implement the support in specifications, but asks not to mandate deployment.

[NIST] shares same view with QC.

Chair suggests to consider the comments and submit for SA plenary workshop on Rel-19.

1. SID from KDDI/S3-230834

[KDDI] presents.

[VF] comments it is dealing about the deployment issues while the WID proposal was just about the algorithm adoption.

[Ericsson] comments, agree with 1st objective, but don’t understand the point for 2nd objective and 3rd objective.

[Nokia] asks whether 256bit algorithm is strong enough for quantum computers or 128bit (symmetric) is good enough.

[KDDI] clarifies it is about deploying 128 and 256bit algorithms together, in a inconsistent manner.

[Ericsson] replies, deployment of 256bit algorithms should be a sperate issue, doesn’t see the need for immediate need.

[Huawei] has question whether AEAD mode is in scope of this study, not specifically mentioned.

[KPN] questions for clarification: is the SID only for symmetric algorithm or also include asymmetric algorithm?

[KDDI] clarifies only symmetric algorithm

[VF] comments the study should consider asymmetric algorithm.

Chair clarifies asymmetric algorithms we use are in IETF defined protocols and we would depend IETF to enhance these protocols. We will adopt in specifications, when IETF updates them.

[KDDI] clarifies.

[Apple] is fine 1st objective, but has questions to 2nd and 3rd objectives, does it mean evaluation of SAGE algorithms?

[Huawei] comments 3rd objective, does it contradict the WID work, if new algorithms are considered?

[KDDI] clarifies.

[QC] comments the 1st bullet is tightly bound with WID,

[Nokia] comments on necessity about the objective if 256bits is mandatory.

[KDDI] clarifies.

[Apple] comments about requirement for algorithm design. It should be evaluation to be added.

[VF] has concern on last sentence of objective, clashes with the WID.

[CMCC] comments to make 1st object at first, asks what is the risk when 128/256 deployed in parallel, any clear risk identified yet?

1. Information on AEAD mode of ZUC-256

[CATT] presents.

[SAGE] comments it does not support short tag.

1. Reply LS to ETSI SAGE on Specification of the 256-bit air algorithms

Presents. SA3 kindly asked ETSI SAGE to proceed with the specification of Milenage-256 based on AES-128-256 with Feistel construction , this was not considered by SAGE. Having two options for Milenage-256, one based on AES-128 and one based on Rijndael-256, is not recommended since it would create market fragmentation.

[SAGE]: Feistel construction was not feasible. Having a 3rd option for Milenage-256 is a good security practice, why opposing a good security practice.