**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211500-r2***

e-meeting, 17 - 28 May 2021

**Title: Alternative 3 DRAFT Response LS on 256-bit Milenage**

**Response to: LS S3-211408 / SAGE (21) 01 on 256‑bit Milenage**

**Source: SA3**

**To: ETSI SAGE**

**Cc:**

**Contact person: Tim Evans**

 **Tim.evans1@vodafone.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:**

# 1 Overall description

SA3 thanks ETSI SAGE for their LS on design approaches for Milenage-256. SA3 has discussed the points raised and has come to the following conclusions:

**ETSI SAGE question\_1**: What is SA3's view on the potential security requirements R1-R8?

**SA3 response\_1:**

* SA3 believes that it is wise to aim for a high security level for Milenage-256, providing resilience against future attacks, and allowing for use in future generations. SA3 therefore favours a design approach that can satisfy the security requirements R1 – R4 and R6 – R8 identified in SAGE’s LS. R5 is less important, as noted by SAGE.

**ETSI SAGE question\_2:** What is SA3 preference on Options 1, 2, and 3? In particular, if SAGE should see a need **to** use Option 3 to meet expectations on security when basing the construction on AES-128-256, does Option 2 still rank as the least preferred.

**SA3 response\_2**:

* Two design options considered in the SAGE LS satisfy the above set of requirements: Option 2 (Rijndael-256-256) and Option 3 (AES-128-256 with Feistel construction). Although a design based on Option 2 would be more efficient, SA3 has a strong preference for reusing existing implementations of AES-128-256, and judges that the performance of a design based on Option 3 would be acceptable.
* SA3 therefore favours a design following Option 3 (AES-128-256 with Feistel construction).

**ETSI SAGE question\_3:** Please provide any additional information which may suggest that SAGE's view on side-channel protection mechanisms is incorrect, or confirm that SAGE's understanding is correct.

**SA3 response\_3:**

* Globally SAGE’s understanding on side-channel protection is correct. The countermeasure cited as an example by SAGE more refers to software implementation, and to first-order side channel attacks. Hardware implementation may be different, because the subbytes operation might be implemented as the real composition of field inversion with affine transformation. Moreover, according to the state of the art, secure implementations might also be protected against fault attacks and high-order side channel threats, which may make the overhead brought by countermeasures more important.

# 2 Actions

**To ETSI SAGE**

**ACTION:** SA3 kindly asks ETSI SAGE to proceed with the specification of Milenage-256 based on Option 3.

# 3 Dates of next TSG SA WG 3 meetings

SA3#103Bis-e 5 - 9 ~July 2021 Electronic meeting (TBC)

SA3#104-e 16 - 27 August 2021 Electronic meeting