**3GPP TSG-SA3 Meeting #115 S3-24w16**

**Athens, February 26 – March 01, 2024**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Introductory text to AES based 256-bit Algorithm Conformance Test Data.**

**Document for: Approval**

**Agenda Item: 4.5**

# 1 Decision/action requested

***SA3 is kindly asked to approve the proposed text for the introcution, the scope, and the Definitions and Terms.***

# 2 References

[1] S3-24w7 TS 35.245 Skeleton for the AES based 256-bit Algorithm Conformance Test Data.

# 3 Rationale

This pCR proposes the description text for the introduction, the scope and the Definition of Terms of [1].

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# Introduction

The present document is one of three, which between them form the entire specification set of the confidentiality and integrity protection algorithms, entitled:

- 3GPP TS 35.243: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  
Document 1: Algorithm Specification ".

- 3GPP TS 35.244: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  
Document 2: Implementation Test Data".

- 3GPP TS 35.245: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  
**Document 3: Design Conformance Test Data".**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 1 Scope

The present document contains the design conformance test data of the encryption and integrity protection function 256-NEA5, 256-NIA5 and the combined authenticated encryption 256-NCA5 protection function for 3GPP systems.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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].

## 3.2 Symbols

void

## 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].

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*