**3GPP TSG-SA3 Meeting #121 S3-25crypt1**

**Goteborg, Sweden, 7 - 11 April 2025**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Pseudo-CR on Technical Details on the ECIES**

**Document for: Approval**

**Agenda item: 5.20**

**Spec: 3GPP TR 33.938**

**Version: 0.1.0**

**Work Item: 3GPP Cryptographic Inventory**

**Comments**

For the cryptographic inventory the ECIES should be described in more detail in the detailed protocol list. This pCR is providing the proposed changes.

\* \* \* First Change \* \* \* \*

# 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 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[4] 3GPP TS 33.501: “Security architecture and procedures for 5G system”.

[x1] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

[x2] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>

\* \* \* Next Change \* \* \* \*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

ICB Initial Counter Block

SECG Standards for Efficient Cryptography

SUPI Subscription Permanent Identifier

\* \* \* Next Change \* \* \* \*

## 4.4 Detailed Protocol List

Editor’s Note: This detailed protocol list is expected to finalize first.

### 4.4.x ECIES

ECIES is used in 5G system in standalone mode for the following:

 Concealment of the SUPI (see Annex C.3 of TS 33.501 [4])

The ECIES profiles follow the terminology and processing specified in SECG version 2 [x1] and [x2]. The security profiles for the ECIES implementation and usage in 3GPP is given in clause C.3.4 of TS 33.501 [4].

ECIES employs symmetric cryptography for the confidentiality protection of the Ephemeral encryption key and ICB, while the elliptic curve profiles refer to asymmetric cryptography.

\* \* \* End of Changes \* \* \* \*