**3GPP TSG-SA3 Meeting #121 S3-25crypt2**

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

**Source: Nokia, Nokia Shanghai Bell**

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

**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] "PKI basics – A Technical Perspective", November 2002, <http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf>.

[x2] 3GPP TS 33.180, “Security for the Mission Critical (MC) service”

[x3] 3GPP TS 33.122, “Security aspects of Common API Framework (CAPIF) for 3GPP”

[x4] 3GPP TS 33.222, “Access to network application functions using Hypertext Transfer Protocol over TLS (HTTPS)”

[x5] 3GPP TS 33.127, “Lawful Interception architecture and functions”

\* \* \* 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].

API Application Programming Interface

CAPIF Common API Framework

LI Lawful Interception

MC Mission Critical

PKI Public Key Infrastructure

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

## 4.4 Detailed Protocol List

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

### 4.4.x PKI

A Public Key Infrastructure is designed to provide this trust. Using a data element called a digital certificate or public key certificate, which binds a public key to identifying information about its owner, the infrastructure is designed to create the binding, and manage it for the benefit of all within the community of use [x1].

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

 Introduction to Public Key Infrastructure (PKI) (see Clause 4 of TS 33.310 [3])

 Certificate based authentication for mission critical services (see Clause 6 of TS 33.180 [x2]) which is mainly
 referencing to TS 33.310 [3].

 Introduction to Inter-Operator PKI (see Clause 5.6.1 of TS 33.210 [2]) which is mainly referencing to TS 33.310 [3].

 Introduction to Common API Framework (CAPIF) (see Clause 6.3.1 of TS 33.122 [x3]) which is mainly referencing
 to TS 33.310 [3].

 Introduction of client and root certificates used for both identity verification and establishing encrypted communications between LI components [x5], but without explicit mentioning of PKI.

 Introduction of subscriber certificates used for certificate-based mutual authentication between UE and an application server (see Annex B of TS 33.222 [x4]) which is mainly referencing to TS 33.310 [3].

PKI employs hash algorithms which refer to symmetric cryptography, signature algorithms and public key algorithms which refer to asymmetric cryptography.

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