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

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

**Source: KDDI**

**Title: Pseudo-CR on 3GPP Cryptographic Inventory for EAP-TLS**

**Document for: Approval**

**Agenda item: 5.20**

**Spec: 3GPP TR 33.938**

**Version: 0.1.0**

**Work Item: FS\_CryptoInv**

**Comments**

This document proposes a detailed text of EAP-TLS protocol for Study on 3GPP Cryptographic Inventory.

\* \* \* 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] IETF, "EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3", RFC 9190.

[x2] IETF, “HMAC-based Extract-and-Expand Key Derivation Function (HKDF) “, RFC 5869.

[x3] IETF, "The EAP-TLS Authentication Protocol", RFC 5216.

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

### 4.4.x EAP-TLS

EAP-TLS [x1, x2] is used in 5G system in standalone mode to realise the following:

Mutual authentication between UE and AUSF (see Annex B of TS 33.501 [4])

Mutual authentication between UE and AAA (see Annex I of TS 33.501 [4])

Mutual authentication between N5GC and AUSF (see Annex O of TS 33.501 [4])

The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in clause 6.2 of TS 33.210 [2]. The 3GPP profile of TLS certificates is specified in clause 6.1.3a of TS 33.310 [3].

EAP-TLS employs asymmetric cryptography for authentication and key agreement.

#### 4.4.x.1 Key Hierarchy

After a successful authentication, session keys will be derived based on the master secret.

When EAP-TLS is used with TLS version 1.3[x1], Hashed Message Authentication Code (HMAC)-based key derivation function (HKDF) [x2] is used with a hash algorithm in the cipher suite.

When EAP-TLS is used with TLS version 1.2[x3], a pseudo random function based on HMAC\_SHA-256 is used to derive session keys.

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