**3GPP TSG-SA3 Meeting #121 S3-XXXXXX**

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

**Source: NIST**

**Title: Pseudo-CR on 3GPP Cryptographic Inventory for MIKEY-SAKKE**

**Document for: Approval**

**Agenda item: 5.20**

**Spec: 3GPP TR 33.9xy**

**Version: 0.0.0**

**Work Item: FS\_CryptoInv**

**Comments**

This document presents an inventory of services that that make use of the MIKEY-SAKKE protocol in response to the work item 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".

[aa] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[ab] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''

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

## 4.4 Detailed Protocol List

### 4.4.X MIKEY-SAKKE

MIKEY-SAKKE is used in the 5G system to securely transport cryptographic keys for Mission Critical Services. It is used in the following scenarios:

Group Master Keys (GMKs) from a Group Management Server to a Group Management Client on a MC UE (see Annex E clause E.2 TS 33.180[aa])

Private Call Keys (PCKs) between MC UEs (see Annex E clause E.3 TS 33.180[aa])

Client-Server keys (CSKs) between MCX Server and MC client (see Annex E clause E.3 TS 33.180[aa])

Multicast Signalling Keys (MuSiK) from MCX Servers to MC clients (see Annex E clause E.3 TS 33.180[aa])

Security profiles for MIKEY-SAKKE are left for implementation.

MIKEY-SAKKE as defined in IETF RFC 6509 [ab]

MIKEY-SAKKE employs symmetric cryptography for key distribution.

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