**3GPP TSG-SA3 Meeting #123 S3-253037-r1**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Huawei, HiSilicon**

**Title: Pseudo-CR on MIKEY-SAKKE protocol**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This contribution identifies the MIKEY-SAKKE protocol is not expected to be updated by other SDO to use PQC.

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

### 7.1.X Protocol #X: MIKEY-SAKKE key exchange

MIKEY-SAKKE is a key exchange method specified in the IETF RFC 6509 [x1]. As described in TR 33.938 [x2], it is used in the 3GPP system to securely transport cryptographic keys for Mission Critical Services [x3]. It employs asymmetric cryptography for key distribution. It may be vulnerable to quantum computing if not updated using Post Quantum Cryptography (PQC).

Editor’s Note: It is ffs whether the IETF will update it to use PQC in the near future, and if not, how the potential risk can be addressed.

\* \* \* Next 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".

[x1] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''.

[x2] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

[x3] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

\* \* \* 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].

MIKEY-SAKKE Multimedia Internet KEYing – Sakai-Kasahara Key Encryption

PQC Post Quantum Cryptography

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