**3GPP TSG-SA3 Meeting #124 S3-253286-r1**

**Wuhan, China, 13 – 17 October 2025**

**Source: Nokia**

**Title: Pseudo-CR on Change to MIKEY-SAKKE**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This pCR if for refinement of the text related to the Key-Issue for Mickey-Sakke, specifically, it can be assumed this protocol will not be updated by IETF, ergo, the 3GPP must study and prepare the necessary solutions. For further details please refer to [1].

It is further proposed to remove the Editor’s Note.

[1] S3-253285, “Discussion on KI for MIKEY-SAKKE”

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

### 7.1.2 Protocol #2: MIKEY-SAKKE key exchange

MIKEY-SAKKE is a key exchange method specified in the IETF RFC 6509 [6]. As described in TR 33.938 [2], it is used in the 3GPP system to securely transport cryptographic keys for Mission Critical Services [3]. It employs asymmetric cryptography for key distribution.

Since the MIKEY-SAKKE will not be updated by IETF with PQC algorithms, SA3 assumes it should study alternative solutions for the MIKEY-SAKKE due to post-quantum threats to existing signature schemes.

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