**3GPP TSG-SA3 Meeting #123 S3-253059**

Goteborg, Sweden, 25 – 29 August 2025

**Source: Nokia**

**Title: Correction of TS to reflect the guidance from SA plenary regarding credential storage and processing**

**Document for: Approval**

**Agenda item: 4.1.1**

**Spec: 3GPP TS 33.369**

**Version: 0.2.0**

**Work Item: AmbientIoT-SEC**

**Comments**

This pCR proposes to correct the requirements in accordance with the guidance provided by the SA plenary.

*“*

*It is proposed that SA#108 endorses the following guidance for AIoT device credentials storage:*

*1) for Rel-19, the AIoT system is defined as private network (isolated network deployment that does not interact with a public network) e.g. SNPN, and the AIoT device credentials storage follows 3GPP defined requirements, the exact mechanism is out of scope of 3GPP (similar to Annex I.2.2 of TS 33.501). This bullet means that no interconnection exists between AIoT systems and PLMNs ;*

*2) For Rel-20, if the AIoT system is defined as public network i.e. PLMN, the AIoT device credentials storage shall use UICC.*

*NOTE 1: Revisiting the above requirements in bullet 1 and/or 2 can be anticipated in future releases following the normal working procedures including in Rel-20.*

*NOTE 2: In case UICC is used, the exact form factor and whether it is removable, non-removable or integrated is out of scope of 3GPP.*

**Proposed Changes**

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

4.2.1.1 Secure storage and processing of credentials

The requirements in this clause apply only to AIoT Devices where communications are triggered by the network. The long-term credentials used for authentication shall be securely stored and processed on the AIoT device.

The long term credentials shall be protected against cloning when stored or processed.

The long term credentials shall be confidentiality and integrity protected when stored and processed.

NOTE: UICC provides protection for long term credentials against physical and logical attacks.

\* \* \* End of Change \* \* \* \*