**3GPP TSG-SA3 Meeting #123 S3-252934**

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

**Source: NTT DOCOMO**

**Title: pCR on aligning with SA plenary guidance**

**Document for: Approval**

**Agenda item: 4.1.1**

**Spec: 33.369**

**Version: 0.2.0**

**Work Item: AmbientIoT-SEC**

**Comments**

In SA#108, SA sent an LS (SP-250852) to SA2, SA3 and CT1, which provide a guidance for AIoT device credentials storage which is included in SP-250851:

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.

Based on the guidance provided by SA, in Rel-19, the AIoT system is defined as an SNPN without PLMN interaction. This guidance needs to be reflected in TS 33.369

\* \* \* Begin Change \* \* \* \*

|  |  |
| --- | --- |
| 3GPP TS 33.369 V0.2.0 (2025-05) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Security aspects of Ambient IoT service for isolated private networks  (Release 19) | |
|  | |
|  |  |

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

# 1 Scope

The present document specifies the security and privacy aspects of AIoT services in the 5G System (5GS), complying to the requirements in TS 22.369 [4], applicable to the AIoT Device types, traffic types, use cases and connectivity topologies defined in TS 38.300 [3], and based on the architecture defined in TS 23.369 [2].

The AIoT system is defined as private network, i.e. isolated network deployment that does not interact with a public network, e.g. an SNPN.

Security features for AIoT services include:

1. Network Layer Authentication between AIoT device and 5G core

a. AIoTF is the endpoint in the 5G core

b. Credentials are securely stored in the ADM on the network side

NOTE 1: The credentials are assumed to be stored in a secure environment in the ADM. How this is realized is left to implementation. The requirements will reflect this.

c. Secure storage and processing of credentials in the AIoT device.

NOTE 2: For SNPN deployment the storage of the credentials of non-AKA based methods is out of scope as described in TS 33.501[5] Annex I 2.2.

d. Security aspects of the storage of the credentials at the ADM

2. Confidentiality, anti-replay and integrity protection of information during AIoT service communication

3. Privacy of AIoT device identifiers using the AIoT Temp ID.

4. Security to protect the permanent disabling RF transmission capabilities of AIoT device(s).

Editor’s Note: Further refinement is FFS.

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

### 4.2.1 Requirements on the device

Editor’s Note: This clause contains the security requirement on the device, including secure storage and processing of credentials.

#### 4.2.1.1 Secure storage and processing of credentials

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.

The long term credentials shall be protected against physical and logical attacks when stored and processed.

In the present document, 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 means that no interconnection exists between AIoT systems and PLMNs.

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

Editor’s note: Further requirements are FFS

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