**3GPP TSG-SA3 Meeting #115adhoc-e *S3-241401r1***

**Emeeting, 15-19 April 2024**

**Source: Apple**

**Title: Security assumption on Ambient IoT**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve the pCR to TR 33.713***

# 2 References

None

# 3 Rationale

This contribution proposes security assumption for TR 33.713.

In SA2 spec TR 23.700-13 defined Ambient IoT devices as an IoT devices powered by energy harvesting with limited energy storage capability. In some use cases listed in SA1 spec TR 22.840, A-IoT devices are usually battery-free or with limited energy storage capability, which indicates those Ambient IoT device also have limited computing capabilities and it is difficult for them to support complicate security mechanisms, e.g. primary authentication, PDCP security functionality, etc.

Current 5G authentication procedure and signalling security protection are all based on long-term keys in the USIM, and the long-term key(s) of the subscription credential(s) (i.e. K) shall be confidentiality protected within the UE using a tamper resistant secure hardware component. If A-IoT devices can not support UICC or complex security protocols and algorithm computation, the security solution design will be totally different with current 5G. It should be a pre-assumption at the beginning.

This should be a pre-assumption in the beginning of the study.

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

## 4.Y Security Assumptions

In SA2 spec TR 23.700-13 defined Ambient IoT devices as an IoT devices powered by energy harvesting with limited energy storage capability. In some use cases listed in SA1 spec TR 22.840, A-IoT devices are usually battery-free or with limited energy storage capability, which indicates those Ambient IoT device also have limited computing capabilities and it is difficult for them to support complicate security mechanisms, e.g. primary authentication, PDCP security functionality, etc.

Current 5G authentication procedure and signalling security protection are all based on long-term keys in the USIM, and the long-term key(s) of the subscription credential(s) (i.e. K) shall be confidentiality protected within the UE using a tamper resistant secure hardware component.

If A-IoT devices can not support UICC or complex security protocols and algorithm computation, the security solution design will be totally different with current 5G. It should be a pre-assumption at the beginning.

* + 1. ~~Considering the limited capability of Ambient IoT devices, they may or may not contain UICC(s). Security solution design should include technical approaches for both kinds of A-IoT devices with or without UICC.~~

Editor’s Note: It depends on SA2 and RAN’s decisions whether Ambient IoT devices contain UICC.

\*\*\* End of 1st Change \*\*\*