**3GPP TSG-SA3 Meeting #118 *S3-24xxxx***

**Hyderabad, India, October 14 – 18, 2024**

**Source: OPPO**

**Title: Solution for AIoT Lightweight Authentication Based on 5G-AKA**

**Document for: Approval**

**Agenda Item: X.X**

# 1 Decision/action requested

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

# 2 References

[x] TS 33.501 Security architecture and procedures for 5G System

[y] TR 38.769 Study on solutions for Ambient IoT (Internet of Things) in NR

[z] TS 33.102 3G security; Security architecture

# 3 Rationale

This contribution proposes a 5G-AKA[x] based authentication solution for Key Issue #5.

According to the following scopes in TR 38.769[y], there are constrains such as power consumption etc.

*The overall objective of the SI is to study a harmonized air interface design with minimized differences (where necessary) for Ambient IoT to enable the following devices:*

*i. ~1 µW peak power consumption, has energy storage, initial sampling frequency offset (SFO) up to 10X ppm, neither DL nor UL amplification in the device. The device’s UL transmission is backscattered on a carrier wave provided externally.*

*ii. ≤ a few hundred µW peak power consumption has energy storage, initial sampling frequency offset (SFO) up to 10X ppm, both DL and/or UL amplification in the device. The device’s UL transmission may be generated internally by the device, or be backscattered on a carrier wave provided externally.*

For 5G-AKA, the generation of AV uses functions f1~f5 described in 3GPP TS 33.102.



Figure 7: Generation of authentication vectors

*f1：Message authentication function used to compute MAC*

*f2：Message authentication function used to compute RES and XRES*

*f3：Key generating function used to compute CK*

*f4：Key generating function used to compute IK*

*f5：Key generating function used to compute AK in normal procedure*

For R19 Ambient IoT device, it’s unlikely able to support so many calculations due to the power constrain. So, this solution proposes a lightweight authentication solution for Ambient IoT service.

# 4 Detailed proposal

SA3 is suggested to approve the following pCR.

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

6.X Solution #X: AIoT Authentication solution based on 5G-AKA

### 6.X.1 Introduction

The assumption of this solution is AIoT device and network sharing a long-term root key[x] K.

MAC/XMAC is used for device authenticating network. MAC is calculated by network side with the K, XMAC is calculated by AIoT device side with the K.

Optionally, RES/XRES is used for network authenticating device. XRES is calculated by network side with the K, RES is calculated by device side with the K.

To provide the freshness of the authentication vectors, RAND is also used to calculate MAC/XMAC and optioanlly RES/XRES.

### 6.X.2 Details

MAC/XMAC is used for device authenticating network. MAC is calculated by network side with the K, XMAC is calculated by AIoT device side with the K.

Optionally, RES/XRES is used for network authenticating device. XRES is calculated by network side with the K, RES is calculated by device side with the K.

To provide the freshness of the authentication vectors, RAND is also used to calculate MAC/XMAC and optioanlly RES/XRES.



Figure 6.X.2-1 AIoT Authentication based on 5G-AKA

Based on 5G-AKA, AIoT authentication solution has the following steps:

1. AIoT NF sends autneitication vector request to UDM/ARPF for AIoT device.
2. UDM/ARPF calculates MAC with K (e.g. the root key of AIoT device) and RAND.
3. Optionally, UDM/ARPF calculates XRES with K, if network wants to authenticate AIoT device.
4. UDM/ARPF sends RAND, MAC, device ID and optionally XRES to AIoT Authentication Function.
5. AIoT Authentication Function sends Authentication Request including RAND, MAC, device ID to AIoT NF.

If SEAF may verify XRES in the latter step, then AUSF would optionally send XRES to SEAF. If AUSF may verify XRES in the latter step, AUSF would not send XRES.

1. AIoT NF sends Authentication Request including RAND, MAC, device ID to Reader.
2. Reader sends Authentication Request including RAND and MAC to AIoT device.
3. AIoT device calculates XMAC with RAND and K.
4. Optionally, AIoT device calculates RES with K.
5. AIoT device verifies XMAC=MAC, then the network authentication is successful.
6. AIoT device sends Authentication Reponse to Reader, this message optionally including RES if network wants to authenticate AIoT device.

NOTE: whether step 7 and step 11 can be mapped into inventory procedure is to be aligned with RAN2 or SA2 procedure.

1. Reader sends Authentication Reponse to AIoT NF.
2. Optionally, AIoT NF sends Uplink Authentication Request including RES to AIoT Authentication Function.
3. Optionally, AIoT Authentication Function verifies XRES=RES, then the AIoT device Authentication is successful.

Editor’s Note: Network function used to derive authentication vector is FFS in this solution.

### 6.X.3 Evaluation

TBA.

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

#  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".

[2] 3GPP TS 22.369: "Service Requirements for ambient power-enabled IoT".

[3] RP-244058, RAN New SID for Study on Solution for Ambient IoT in NR.

[4] 3GPP TR 23-700-13: "Study on Architecture Support of Ambient power-enabled Internet of Things".

[x] TS 33.501 Security architecture and procedures for 5G System

[z] TS 33.102 3G security; Security architecture

\*\*\* End of 2nd Change \*\*\*