**3GPP TSG-SA3 Meeting #124 draft S3-253824-r1**

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

**Source: Xiaomi, ZTE Corporation, OPPO, Huawei, HiSilicon, Nokia**

**Title: Key issue for authentication for DO-A capable AIoT devices**

**Document for: Approval**

**Agenda item: 5.2.11**

**Spec: 3GPP TR 33.714**

**Version: 0.0.0**

**Work Item: FS\_AIoT\_SEC\_Ph2**

**Comments**

This contribution proposes to introduce a new key issue for FS\_AIoT\_SEC\_Ph2, which discusses the authentication for DO-A capable AIoT devices.

Merger of S3-253172, S3-253302, S3-253374, S3-253558, S3-253341

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

## 5.X Key Issue #X: Authentication for AIoT devices

### 5.X.1 Key issue details

DO-A capable AIOT devices can inform the network of their presence and send data to the AIOTF autonomously. The TR 23.700-30 [x] studies the architecture framework and procedure for DO-A capable AIoT devices, including the device initiated registration-like procedure and data transfer procedure.

With the capability of providing information autonomously, the existing security mechanisms (e.g. authentication procedure) specified for DT capable AIoT devices need be enhanced to accommodate DO-A use cases. The authentication between the DO-A capable AIoT device and the network is required upon device-initiated communication to validate each other’s identities. Otherwise, the attacker may impersonate the victim device and send fake identification to the network side.

In addition, the security aspects of AIoT Device type 1 for public networks, e.g., authentication, should be studied to ensure the security of AIoT systems.

Therefore, it is necessary to study how to perform authentication between the AIoT device and network, addressing risks such as impersonation.

NOTE 1: For AIoT device credentials storage and processing in public networks, the AIoT device credentials storage will use UICC.

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.

### 5.X.2 Security threats

The attacker may impersonate the victim device.

The attacker may impersonate a legitimate network and communicate with the AIoT device.

### 5.X.1 Potential security requirements

The 5G system shall provide a means to perform mutual authentication between the AIoT device and the network.

Editor’s Note: Whether network authentication has to happen before the device communicates with the network is FFS.

\* \* \* Second Change \* \* \* \*

# 2 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".

[x] 3GPP TR 23.700-30: "Study on Architecture support of Ambient power-enabled Internet of Things (AIoT); Phase 2;".

…

\* \* \* Third Change \* \* \* \*

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

<ABBREVIATION> <Expansion>

DO-A Device-originated - autonomous

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