**SA WG2 Meeting #163S2-2406064**

**Jeju, Korea, May 27 – 31, 2024**

**Source: Samsung, KPN N.V.**

**Title: KI#2: New Solution on Multiple Temporary Identifiers for AIoT Devices**

**Document for: Approval**

**Agenda Item: 19.14**

**Work Item / Release:** **FS\_AmbientIoT / Rel-19**

*Abstract of the contribution: This pCR proposes a new solution on Multiple Temporary Identities for AIoT Devices*

# 1 Discussion

This pCR proposes a new solution on Multiple Temporary Identities for AIoT Devices

# 2. Proposal

It is proposed to adopt the following text in TR 23.700-13.

\*\*\* Start of 1stchange \*\*\*

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
|  | Key Issues |
| Solutions | Key Issue #1 | Key Issue #2 | Key Issue #3 |
| #1 |  | X |  |
| #2 |  | X |  |
| #3 | X | X | X |
| #4 | X | X | X |
| #5 |  | X | X |
| #6 | X | X | X |
| #7 | X | X |  |
| #8 | X | X |  |
| #9 | X | X | X |
| #10 | X | X |  |
| #11 |  |  | X |
| #12 | X | X | X |
| #13 |  | X |  |
| #14 |  | X |  |
| #15 |  | X | X |
| #16 |  | X |  |
| #17 | X | X | X |
| #18 |  |  | X |
| #19 | X |  | X |
| #20 | X | X | X |
| #21 | X | X | X |
| #22 | X | X | X |
| #23 |  |  | X |
| #24 |  | X |  |
| #X |  | X |  |

\*\*\* Start of 2nd change (all new text) \*\*\*

## 6.X Solution #X: Multiple Temporary Reusable Identities for AIoT Devices

### 6.X.1 Description

This solution addresses KI#2 and tackles the problem of efficiently and securely identifying an AIoT device while preserving the limited AIoT device computing resources. This is accomplished by providing the AIoT device with a set of temporary identifiers, as explained below.

Similarly to the rationale for employing temporary identifiers for a UE, it is assumed that a new temporary identifier (e.g. 5G-GUTI) is required after every paging procedure and before the release of the NAS connection for an AIoT device as it is currently the requirement in 5GS, so as to minimize the ability of a rogue entity to track a user. If for example an AIoT device uses the same temporary identity after being paged twice, then a rogue entity may be able to track the device’s location based on the unmodified temporary identity. Furthermore, AIoT devices are expected to be limited in terms of power resources. It is therefore inefficient to allocate a new temporary identity after every paging procedure. Using local algorithms in the AIoT device and the network, where the algorithm generates a new temporary identity, has drawbacks in terms of power since each generation of a new identity would require compute power. With AIoT devices being very limited in power, this procedure can lead to increase power use if multiple paging procedures are performed for an AIoT device. Instead of computing power, this solution would require storage of the multiple identifiers in the AIoT device.

Additionally, AIoT devices are expected to be deployed in large numbers in the network, to have limited activity due to the power and resource constraints, and might leave the network without notice. Thus, for scalability considerations, a mechanism is needed to revoke the allocated temporary IDs in case of e.g. a prolonged inactivity period and re-allocate them to other devices.

The proposed solution can be summarized as follows:

- The network should allocate and provide more than one temporary identity to the UE, say N identities together with authentication information.

- The N allocated identities together with the authentication information can be sent to the UE in one message.

- The UE and the network will use one identity at time such that both entities know ahead of time which identity would be used next as will be described later.

- The ID combined to authentication information (e.g. tokens, encryption keys) are used to authenticate the device for each exchanged message.

NOTE: Mechanisms for authentication information generation, exchange and update are to be defined by SA WG3.

* The temporary IDs can be revoked from the AIoT device and re-allocated to another device e.g. in case of a pre-determined period of inactivity.
* When re-allocating the one or more ID(s) to another device, new authentication information is provided.

Note that the temporary identity may refer to any temporary identity which may be used in the 3GPP system or in the 5GS such as 5G-GUTI, or any identity that may be defined for AIoT devices.

In the following, it is described new capabilities that are required in the network and/or AIoT device to support the above functionality

In terms of new functionality, the solution requires a new capability for multiple temporary identifiers to indicate its support for receiving, handling, and storing multiple temporary identifiers at a time. The AIoT device may also indicate how many identities it can receive at a given time, where this may be based on memory or resources in the device. The UE may determine the number of identifiers which it can receive based on several factors, e.g. the total available memory in the UE, the length or size of the identifier, a combination of available resources, etc. Furthermore, the network then may determine to allocate a number N of temporary identities to a UE based on the capability indication provided by the UE and other factors. The transmission of the set of identities should occur using a secured message.

### 6.X.2 Procedures

#### 6.X.2.1 Temporary Reusable ID Allocation



Figure 6.X.2-1: Procedure to support allocation of multiple temporary identities to AIoT devices

The procedure in Figure 6.X.2-1 to support allocation of multiple temporary identities to AioT devices is described step by step below.

1. The AioT device sends a registration/validation request to the AMF (or AioT NF). The request includes a capability indication for receiving multiple temporary identifiers. Optionally, the request may also include the maximum number of temporary identifiers that can be stored at the AioT device.

2. The AMF (or AioT NF) allocates a set of temporary identifiers and authentication information to the AioT device with N entries. The allocation may be performed based on device capability, subscription, or local policy.

3. A registration/validation response is sent by the AMF (or AioT NF) to the AioT device including the set of allocated temporary identifiers with N entries together with the authentication information.

4. The AioT device stores the set of N temporary identifiers in the same order they were received in step 3. For example, if N identifiers were received, they should be stored so that the first identifier to be used is Temp ID#1, then Temp ID#2…, and lastly Temp ID#N.

5. A paging is sent from AMF (or AioT NF) to the AioT device via the RAN reader including the first temporary identifier, i.e. Temp ID#1.

6. A NAS response message is provided by the AioT device including the temporary identifier contained in step 5, i.e. Temp ID#1 and the corresponding authentication information.

7. The temporary identifier in steps 5 and 6 is deleted locally both at the AioT device (see step 7a) and AMF (or AioT NF, see step 7b). In both cases, the next temporary identifier is set to be the next one in the set received in step 3, i.e. Temp ID#2.

8. The connection with the AioT device is released or the transaction/service is completed.

9. Steps 5 to 9 are repeated upon a new need for paging. Both the AioT device and the AMF (or AioT NF) locally delete any temporary identifier that has been used.

10. Once the full set of identifiers have been used and deleted, the procedure is repeated from step 2 with a new set of temporary identifiers being allocated by the AMF/AioT NF to the AioT device before the connection is released.

#### 6.X.2.2 Temporary Reusable ID Revocation and Re-Allocation

The temporary reusable IDs may be revoked and re-allocated as described below:

* One or more temporary IDs can be revoked from the AIoT device and re-allocated to another device e.g. in case of a pre-determined period of inactivity after which the device is assumed to have left the network. A revocation notification may be sent to the device.
* When re-allocating the one or more ID(s) to another device, new authentication information is associated with the new allocation. The authentication information from a pre-defined number of previous allocations is also temporarily stored in the CN NF.
* It is assumed that an AIoT device may not have received the revocation notification from the network and may communicate again at a later time by responding to a paging for the same ID that has been re-allocated to another device.

#### 6.X.2.3 Temporary Reusable ID Conflict Detection and Resolution

If a device from which the ID had been previously revoked attempts to communicate again with the network by responding to the paging from the network, the following conflict detection and resolution mechanisms are performed:

- When the returning device responds to paging from the network using the temporary ID and the authentication information from a previous ID association, the network can determine that the device is using an ID which has been re-assigned, and identify it using the authentication information from the previous association.

### - If the device is still authorized to communicate with the network, new temporary IDs and new authentication material are allocated to the device.6.X.3 Impacts on services, entities and interfaces

Impacts on existing entities:

CN NF (AMF or AIoT NF):

- Support handling and allocation of multiple temporary reusable identifiers for AIoT devices.

- Support revocation and conflict detection and resolution for temporary reusable IDs for AIoT devices.

AIoT device:

- Support for multiple temporary identifiers capability indication.

- Handling the allocation of multiple temporary identifiers from the network.

\*\*\* End of 2nd change \*\*\*