3GPP TSG-SA WG2#164 S2-240xxxx

Aug 19th – Aug 23th , Maastricht, NL was S2-2407809

**Source: China Mobile**

**Title: Solution 10 – updating AF triggered registration procedures with read-only operations**

**Document for: Approval**

**Agenda Item: 19.14**

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

*Abstract of the contribution: This contribution updates AF triggered registration procedure with read-only operations.*

# 1. Text proposal

It is proposed to agree the following changes to TR 23.700-13:

>>>>BEGINNING OF CHANGES<<<<

## 6.10 Solution #10: Registration procedure for Ambient IoT Devices

### 6.10.1 Description

This solution is for Key Issue #2 "Identification, Subscription, Registration and Connection management".

As depicted in Architecture Requirements, the DT and DO-DTT traffic types will be studied in this stage. The Ambient IoT devices could be driven by the network for Topology1 or UE for topology 2 before registering to the network. This proposal proposes one potential mechanism for identification, subscription, registration management, and registration procedures as well.

As we know, 5GS uses SUPI with PLMN info, PEI, and GPSI as identifications for device ID based access control, identification, authentication, routing steering, and service purposes. However, due to cost and power consumption, most ambient IoT devices may not have these kinds of IDs. Referencing the RFID solution, most likely, the ambient IoT device has the following IDs:

1) TID (See GS1 TDS Release 2.1 [10]): The AIoT manufacturer configures the tag ID in advance. It is only readable. It can be treated as PEI in the ambient IoT solution.

2) EPC (See GS1 TDS Release 2.1 [10]): Electrical Product Code. The ID can be used to flexibly define one or a group of ambient IoT devices in the ambient IoT service procedure. It can be treated as GPSI in the ambient IoT solution.

Unfortunately, neither TID nor EPC has the operator ID information. Therefore, they are not suitable for device ID based access control, identification, and routing steering purposes. The solution introduces a new device ID. It can be treated as SUPI. The device ID is either allocated by 5GC or the third party. This ID need to be kept internally in 5GS and ambient IoT devices for access control, identification, and route steering purposes. The format of the device ID is Operator ID + Group ID + Instance ID.

Editor's note: Detailed information carried in Operator ID and Group ID is FFS.

To simplify the pre-configuration procedure, only Operator ID and Group ID will be pre-configured in the ambient IoT device. Instance ID doesn’t need to be pre-configured in the ambient IoT devices. Once the AF-triggered registration procedure is performed successfully based on TID and default credentials, the 5GC will generate a new entire device ID with a unique instance ID or will obtain the entire unique device ID from the third party. The device ID’s registration status and binding association with TID are kept in the 5GC. The new device ID will not be synced with the ambient IoT device to realize an AF-triggered registration procedure with read-only operations.

In the subsequent ambient IoT service operations, the ambient IoT will send TID info to 5GC, which will get the actual device ID based on the binding association between the device ID and TID. This is why only the operator ID and group ID are pre-configured in the ambient IoT device, and the newly generated device ID is not synced with the ambient IoT device; however, the 5GC still can get the correct ambient IoT device ID and can perform the access control based on it.

furthermore, EPC ID can also be pre-configured in the ambient IoT device. In the solution, full or partial EPC can be used to match one specific ambient IoT device or a group of ambient IoT devices flexibly. Matched ambient IoT devices will respond with TID and credentials for authentication purposes.

Besides, the credential holder can be flexibly placed in the serving operator, roaming operator, enterprise, or third AF based on Operator ID and Group ID to realize different networking architectures.

As the Ambient IoT Devices for supply chain services possibly move anywhere, it is difficult to authenticate and authorize the devices in the serving network. That is because the serving network cannot acquire the credentials or subscription data if there is no roaming agreement between the home network and the serving network. What’s more, the serving network is not aware of the home network if the information of home PLMN is not contained in the operator ID or signaling message. Thus, for supply chain service the credential holder can be placed in the third AF. To support the supply chain service or registration for the whole serving zone, the AF should sign SLA with the Operator. It is supposed that AF can enforce authentication and authorization by itself or with the help of other AF.

The principles/assumptions are given below:

- A new network function named Ambient IoT NF may be adopted to manage Ambient IoT devices and procedures. If not, this relevant function can be supported by AMF.

- In 5GC, each Ambient IoT device has a unique device ID that consists of the Operator ID, group ID, and Instance ID.

- The device ID is kept internally in 5GS and ambient IoT devices for access control, identification, and route steering purposes.

The ambient IoT device is pre-configured with the EPC, Operator ID + Group ID, TID, and default credentials. For ambient IoT devices applied in the supply chain, the Operator ID+Group ID field can be filled with a specific value, e.g., 999.

- The credential holder is pre-configured with TID and default credentials.

- The solution is based on an operator-controlled Ambient IoT device.

### 6.10.2 Procedures

#### 6.10.2.1 Procedures for AF triggered Registration for Topology 1

The following figure presents a procedure of AF triggered registration for Topology 1.

A screenshot of a document

Description automatically generated

Figure 6.10.2-1: AF triggered Registration Procedure for Topology 1

0.a. The Ambient IoT devices are pre-configured with operator ID and group ID and default credentials and/or EPC. TID (See GS1 TDS Release 2.1 [10]) is configured by AIoT manufacturers in advance.

NOTE 1: How information is configured into ambient IoT device is out of scope of 3GPP.

0.b Meanwhile, the 5GC or the third credential holder is also pre-configured with the TID, default credentials, status (inactive), and so on.

1. AF sends an AF Triggered Registration Request to NEF with the following parameters: Transaction ID, EPC or TID list, Operator ID list, location, AF ID, Aggregation indication information, time, periodical indication, and so on.

- Operator ID list: This information is used to define the targeted ambient IoT devices from the operator's perspective, supporting multiple operator ambient IoT device access. It could be one specific operator or a list of operators.

- TID list: The information can be used to define one or a few targeted ambient IoT devices.

- EPC: The information can be used to define one or a group of targeted ambient IoT devices.

- Aggregation indication: It is used to tell the 5GS how to handle the response messages - aggregation response or not.

- Time: when the service will be carried out exactly. This parameter is only carried in the AF-triggered whole unregistered ambient IoT devices performing registration procedure scenarios.

- Periodical indication: whether the service operation will be executed periodically. This parameter is only carried in the AF-triggered whole unregistered ambient IoT devices performing registration procedure scenarios.

2. NEF will perform the below actions towards the third Ambient AF

- Perform authentication to the third Ambient AF to decide whether it is allowed to access 5GS or not.

- Check the authorization to determine whether the third Ambient AF is allowed to perform an AF triggered registration operation or not.

- Check the authorization to determine whether operators in the operator list ID are allowed or not.

- Converting location information to TA List information.

The NEF obtains serving AMF or Ambient IoT NF based on the TA list.

3. The NEF sends AF Triggered Registration Request to the AMF/Ambient IoT NF, including the EPC or TID list ID, Transaction ID, Operator ID list, TA list, aggregation indication, time, periodical indication, and so on.

4. The AMF/Ambient IoT NF selects the NG-RAN reader based on the TA list.

5. The AMF/Ambient IoT NF forwards AF triggered the registration request to the NG-RAN reader, including the EPC or TID list, Operator ID list, time, periodical indication, and so on.

6. NG-RAN activates one or a few targeted ambient IoT devices that match both the EPC or TID list and Operator ID list to perform the registration procedure with the operator ID , group ID, TID, and default credentials. A receiving limit time may be configured on NG-RAN. Once timeout, the message received after this time will be discarded by NG-RAN.

7. The NG-RAN reader forwards the registration messages with the operator ID, group ID , TID, and default credentials to AMF/New Ambient IoT NF.

NOTE 2: Considering the NG-RAN reader sequence scanning behaviour, don't suggest that NG-RAN perform a response aggregation operation during the interactive authentication procedure between ambient IoT devices and 5GC. Aggregation operations may only be performed in 5GC in this scenario.

8. Upon receiving the registration message from NG-RAN, AMF/New AIoT NF can determine the targeted credential holder based on local configurations related to operator ID and/or group ID . AMF/New AIoT NF may forward authentication requests to AF for supply chain scenarios.

9. Perform an authentication operation based on TID as username and default credentials between AMF/New AIoT NF and the credential holder. Once authentication is successful, 5GC or a third party will produce a Real full device ID with a unique instance ID internally. The device ID consists of operator ID + group ID + instance ID.

10. 5GC stores the new device ID, TID, and status (active) in UDM, AMF/New AIoT NF, and sets the device status as active. The status information will be used in the Ambient IoT service procedures to verify the Ambient IoT device. The new device ID and status information will not be synced with the ambient IoT device to realize the whole procedure with read-only operations.

11. The AMF/New AIoT NF returns AF Triggered Registration Response to the AF via NEF.

NOTE 3: Security related mechanisms will be in the remit of SA WG3.

#### 6.10.2.2 Procedures for AF triggered Registration for Topology 2

The registration may be triggered by AF via the UE reader. The UE reader interacts with AMF /New Ambient IoT NF via NG-RAN, which could be regarded as an AF triggered registration procedure for topology 2.

A document with text and images

Description automatically generated

Figure 6.10.2-2: AF triggered Registration Procedure for Topology 2

1. The UE Reader performs the registration procedure, including the fixed or mobile type of UE reader, location, and AF ID.

2. AF sends an AF Triggered Registration Request to NEF with the following parameters: Transaction ID, EPC or TID list, Operator ID list, location, AF ID, Aggregation indication information, time, periodical indication, UE GPSI, and so on.

If UE GPSI is included in the message, the third AF wants to perform an AF-triggered registration procedure with a designated UE reader defined by UE GPSI. In addition, time and periodical indication parameters are not included in the message.

If UE GPSI isn't included in the message, the third AF wants to perform an AF-triggered registration procedure without designated UE readers. 5GS determines the involved UE readers based on input info from the third AF, such as location, AF ID, and so on. Considering UE reader posture, such as UE reader antenna pointing direction, only fixed-type UE readers will be involved in the procedure.

3. NEF will perform the below actions towards the third Ambient AF:

- Perform authentication to the third Ambient AF to decide whether it is allowed to access 5GS or not.

- Check the authorization to determine whether the third Ambient AF is allowed to perform an AF-triggered registration operation.

- Check the authorization to determine whether operators in the operator list ID are allowed or not.

- Converting location information to TA List information.

The NEF obtains serving AMF or Ambient IoT NF based on the TA list.

4. The NEF sends AF Triggered Registration Request to the AMF/Ambient IoT NF, including the Transaction ID, Operator ID list, EPC or TID list ID, TA list, AF ID, aggregation indication, time, periodical indication, UE GPSI and so on.

5. If UE GPSI isn't included in the message, the AMF/Ambient IoT NF selects the fixed-type UE readers based on the TA, Location list, and AF ID. Alternatively, if UE GPSI is carried in the message, the AMF/Ambient IoT NF selects the designated UE reader based on UE GPSI.

6. First, The AMF/Ambient IoT NF sets up the connection with targeted UE readers. Then, it forwards the AF-triggered registration request to the fixed-type UE readers or the designated GPSI UE reader, including the EPC or TID list, Operator ID list, time, periodical indication, and so on.

7. the fixed-type UE readers or the designated GPSI UE reader activate one or a few targeted ambient IoT devices that match both the EPC or TID list and Operator ID list to perform the registration procedure with the Operator ID, Group ID, TID, and default credentials. A receiving limit time may be configured on NG-RAN. Once timeout, the message received after this time will be discarded by NG-RAN.

NOTE: Considering the latency requirement and reader scanning capability, don't suggest that UE Reader performs a response aggregation operation during the interactive authentication procedure between ambient IoT devices and 5GC. Whether and when the UE Reader should engage the response aggregation should be decided on the service requirements and service scenario, e.g. when the latency exceeds the scanning speed or when the Topology 1 and Topology 2 are in one Registration request.

8. AMF/New AIoT NF Determines the credential holder based on the operator ID and group ID; the credential holder authenticates the ambient IoT device based on the TID and default credential. If authentication is successful, 5GS produces a new full Device ID, 5GC sets the device status as active. At the same time, new Device ID, TID, Status (active), and so on are stored in UDM and AMF/ New Ambient IoT NF. The status information will be used in the Ambient IoT service procedures to verify the Ambient IoT device. The new device ID and status information will not be synced with the ambient IoT device to realize the whole procedure with read-only operations.

9. The AMF/New AIoT NF returns AF Triggered Registration Response to the AF via NEF.

### 6.10.3 Impacts on services, entities and interfaces

**NEF:**

- Capability to authentication and authorization to the third ambient IoT AF.

- Capability to support verification on operator ID list.

**AMF/Ambient IoT NF:**

- The AMF/Ambient IoT NF selects the NG-RAN reader and/or UE reader based on the TA list, Location, and AF ID.

- Capability to aggregate the Ambient IoT devices' response.

- Capability to be aware of the Topology types.

**UDM/Credential holder:**

- The UDM stores the profile information of Ambient IoT devices.

- Authenticating the ambient IoT device and producing new device IDs.

**NG-RAN Reader:**

- The NG-RAN reader performs paging and receives responses from Ambient IoT devices in Topology 1.

**UE Reader:**

- The UE Reader performs paging and receives responses from Ambient IoT devices in Topology 2.

**Ambient IoT device:**

- The ambient IoT device stores the operator ID, group ID, and default credentials.

- Performing registration procedure once it is matched during the paging procedure.

>>>>END OF CHANGES<<<<