3GPP TSG-SA WG2#163 S2-2406414r01

May 27th – May 31th , Jeju, Korea

**Source: China Telecom, NEC, CATT**

**Title: Address Open Issues and Update Procedure for Solution 10**

**Document for: Approval**

**Agenda Item: 19.14**

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

*Abstract of the contribution: This contribution addresses open issues and updates procedures in solution 10.*

# 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 IMPI with PLMN info, PEI, and GPSI as identifications for 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 access control, identification, and routing steering purposes. The solution introduces a new device ID. It can be treated as IMPI. The device ID is kept internally in 5GS and ambient IoT devices for access control, identification, and route steering purposes. It will not be exposed to the third AF.

The format of the device ID is Operator ID + Group ID + Instance ID. The Operator ID prefers to leverage existing MCC and MNC to define one specific MNO operator; the Group ID can represent the Company information.

The solution has a default device ID concept. The Instance ID is set to zero in the default device ID during the pre-configuration phase. Once the AF-triggered registration procedure is performed successfully, the 5GC will generate a new device ID with a unique and non-zero instance ID to replace the default device ID in the ambient IoT device.

In order to keep a competitive solution compared to the RFID solution, it is possible to trigger not only one or a few ambient IoT devices defined by the TID list but also numerous unregistered ambient IoT devices in the whole serving zone in the AF-triggered registration procedure. Then, it is possible to perform an automatic AF-triggered registration procedure for unregistered ambient IoT devices in the whole zone during the middle of the night without human resources involved. However, ambient IoT devices are not allowed to keep dedicated status info. How is the ambient IoT device aware of the registered or unregistered status in this case? In the solution, if the instance ID in the device ID is set to zero, such as the default device ID mentioned above, it will be implicit to show an unregistered status.

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 derived from the default device ID to realize different networking architectures.

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. It will not be exposed to the third AF.

- The ambient IoT device and Credential holder are pre-configured with the default ambient IoT device ID, 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.

8. Determine credential holder based on the default Device ID

AMF or New

Ambient IoT NF

6. The NG-RAN Reader performs AF triggered Registration operations with Ambient IoT Devices based on the Operator ID list and TID list info; Matched ambient IoT devices perform registration procedures with the default device ID, TID, and default credential. If the TID list is not carried in the message, it means all unregistered Ambient IoT devices matched with the operator ID list in the NG-RAN reader’s serving location need to execute registration.

3. AF Triggered Registration Request (Transaction ID, TA list, Operator ID list, TID list, Aggregation indication, time, periodical indication…)

Ambient AF

fd

UDM

NEF

NG-RAN

Reader

Ambient IoT

Devices

1. AF Triggered Registration Request (Transaction ID, TID list, Operator ID list, Location, AF ID, Aggregation indication, time, periodical indication …)

0.a pre-configuration

4.Obtain targeted NG-RAN Reader based on TA lists

5. AF Triggered Registration Request (Transaction ID, Operator ID list, TID list, time, periodical indication …)

10. Store Device ID, TID, Status, and so on in UDM/AMF or New Ambient IoT NF

12. AF triggered Registration Response (Transaction ID，TID, TID，Status, …)

2.AF authentication and authorization.

operator ID list check

7. AF Triggered Registration Response (Transaction ID, Default Device ID, TID, and default credential, …)

Credential

Holder

0.b pre-configuration

re-configuration

9. Authentication based on TID and default credential and Produce real Device ID and new credential

11. Sync up new Device ID and new credential with Ambient IoT devices

Figure 6.10.2-1 AF triggered Registration Procedure for Topology 1

0.a The Ambient IoT devices are pre-configured with default AIoT device ID and default credentials. TID (See GS1 TDS Release 2.1 [10]) is configured by AIoT manufacturers in advance. The instance ID value in the default AIoT device ID is set to zero. The ambient IoT device will implicitly know its active or inactive status based on the instance value in the solution.

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, 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. If the TID list is carried in the message, it means AF wants to trigger one or a few ambient IoT devices defined by the TID list to perform the registration procedure. If the TID list is not carried in the message, it means AF wants to trigger all unregistered Ambient IoT devices in this location to perform the registration procedure. The ambient IoT device will implicitly know its registered or unregistered status based on the instance value in the device ID. If the instance has all zero values in the device ID, then the ambient IoT device has an unregistered status.

- 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 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 the AF triggered registration request to the NG-RAN reader, including the 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 TID list and Operator ID list to perform the registration procedure with the default device ID, TID, and default credentials. If the TID list is not carried by the NG-RAN reader, all unregistered ambient IoT devices that match the operator ID list have to execute the registration procedure. The ambient IoT device will implicitly know its registered or unregistered status based on the instance value in the device ID. If the instance has all zero values in the device ID, then the ambient IoT device has an unregistered status. 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 default device ID, TID, and default credentials to AMF.

Note 1: Considering the NG-RAN reader sequence scanning behavior, 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 location of the credential holder. Based on local configurations related to operator ID and/or group ID derived from the default device ID, it is flexible to steer authentication messages to the serving operator’s credential holder, roaming operator’s credential holder, or the third AF-owned credential holder.

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, a Real device ID with a unique and non-zero instance ID will be produced. The procedure may replace default credentials with new credentials produced by the credential holder.

10. 5GC stores the new device ID, TID, status (active), and so on in UDM, AMF/New AIoT NF. The status information will be used in the Ambient IoT service procedures to verify the Ambient IoT device.

11. AMF/New AIoT NF will sync up new device IDs and credentials with relative ambient IoT devices.

12. The AMF/New AIoT NFreturns AF Triggered Registration Response to the AF via NEF.

#### 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.

AMF/New

Ambient IoT NF

7. Fixed UE Readers or UE Reader-matched UE GPSI perform AF-triggered Registration operations with Ambient IoT Devices matched on the Operator ID list and TID list info; Matched ambient IoT devices will perform registration requests with the default device ID, TID, and default credentials. If the TID list is not carried in the message, it means all unregistered Ambient IoT devices in the UE reader’s serving location must perform the registration procedure.

needed

4. AF Triggered Registration Request (Transaction ID, TA lists, Operator ID list, TID list, location list, AF ID, Store ID, Aggregation indication, Time, Periodical indication, UE GPSI…)

5. Obtain targeted fixed UE readers based on TA lists, Location list, AF ID, and Store ID. Or Obtain UE reader based on UE GPSI

Ambient AF

fd

UDM

NEF

UE

Reader

Ambient IoT

Devices

2. AF Triggered Registration Request (Transaction ID, location list, TID list, Operator ID list, aggregation indication, AF ID, Store ID, Time, Periodical indication, UE GPSI …)

1.UE Reader performs registration Procedure with UE read type indication – Fixed or Mobile, location, AF ID, Store ID

6. AF Triggered Registration Request (Transaction ID, Operator ID list, TID List, Aggregation indication, Time, Periodical indication…)

9. Sync up new Device ID and new credential with Ambient IoT devices.

10. AF triggered Registration Response (Transaction ID,TID, TID Status, …)

3. AF authentication and authorization/ Operator ID list check

8. AMF/New AIoT NF Determine credential holder based on the default Device ID; Credential holder does authentication based on TID and default credential and produces new Device ID and credentials. New Device ID, TID, Status, and so on are stored in UDM and AMF/ New Ambient IoT NF.

Credential

Holder

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, precise location, AF ID, and Store ID.
2. AF sends an AF Triggered Registration Request to NEF with the following parameters: Transaction ID, TID list, Operator ID list, location, AF ID, Store 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, store 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.

1. 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.

1. The NEF sends AF Triggered Registration Request to the AMF/Ambient IoT NF, including the Transaction ID, Operator ID list, TID list ID, TA list, AF ID, Store ID, aggregation indication, time, periodical indication, UE GPSI and so on.
2. If UE GPSI isn't included in the message, the AMF/Ambient IoT NF selects the fixed-type UE readers based on the Location list, AF ID, and Store ID. Alternatively, if UE GPSI is carried in the message, the AMF/Ambient IoT NF selects the designated UE reader based on UE GPSI.
3. 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 TID list, Operator ID list, time, periodical indication, and so on.
4. the fixed-type UE readers or the designated GPSI UE reader activate one or a few targeted ambient IoT devices that match both the TID list and Operator ID list to perform the registration procedure with the default device ID, TID, and default credentials. If the TID list is not carried in the message, all unregistered ambient IoT devices in the fixed-type UE readers’ or the designated GPSI UE reader’s serving area that match the operator ID list have to execute the registration procedure. The ambient IoT device will implicitly know its registered or unregistered status based on the instance value in the device ID. If the instance has all zero values in the device ID, then the ambient IoT device has an unregistered status. 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 2: 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.

1. AMF/New AIoT NF Determines the credential holder based on the default Device ID; the credential holder authenticates the ambient IoT device based on the TID and default credential. If authentication is successful, 5GS produces a new Device ID and credentials. 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
2. AMF/New AIoT NF will sync up new device IDs and credentials with relative ambient IoT devices.
3. 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, AF ID, and store 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 default AIoT device ID and default credentials and updates the device ID and credentials if the registration procedure is performed successfully.

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

>>>>END OF CHANGES<<<<