3GPP TSG-SA WG2#162 S2-2405130

Changsha, China, 15-19 April 2024 (was S2-2403924)

**Source: Qualcomm Incorporated**

**Title: Addressing open issues for Solution 3**

**Document for: Discussion/Approval**

**Agenda Item: 19.14**

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

*Abstract of the contribution: This contribution addresses open issues for Solution 3 and provides a new Annex for TR 23.700-13 to provide an overview of the Electronic Product Code.*

# 1. Text proposal

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

>>>>BEGINNING OF CHANGES<<<<

# 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 nonspecific.

- 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] 3GPP RP-234058: "New SID: Study on solutions for Ambient IoT (Internet of Things) in NR".

[4] 3GPP TS 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[5] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[6] 3GPP TS 23.503: "Policies and Charging control framework for the 5G System; Stage 2".

[7] 3GPP TR 38.848: "Technical Specification Group Radio Access Network; Study on Ambient IoT (Internet of Things) in RAN".

[8] 3GPP TR 38.769: "Study on solutions for Ambient IoT (Internet of Things) in NR".

[9] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[10] GS1 TDS Release 2.1: "EPC Tag Data Standard".

[X1] GS1 Organisation: The Global Language of Business. Available at: https://www.gs1.org/

[X2] GS1: Standards in the Healthcare Supply Chain. Available at: https://www.gs1.ch/de/media/1117

# 3 Definitions of terms 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].

**Ambient IoT Device:** An Ambient IoT device is an IoT device powered by energy harvesting, with limited energy storage capability. The other characteristics of the Ambient IoT device are defined in TR 38.769 [8].

NOTE 1: The final decision on the term name is to be determined in TR conclusion or normative phase.

**Ambient IoT Services:** The functionalities and procedures to support Ambient IoT use cases.

NOTE 2: the functionalities and procedures for Ambient IoT Services are left to outcome of the study. The Ambient IoT use case(s) can be referred to TR 38.848 [7] and TS 22.369 [2].

NOTE 3: The final definition on the term is to be determined in TR conclusion or normative phase.

**Device-originated - device-terminated triggered (DO-DTT):** The device originated traffic is triggered by the device terminated traffic or signalling.

**Device-terminated (DT):** The traffic is terminated at the AIoT device.

**Electronic Product Code:** A universal identifier that provides a unique identity for any physical object as defined by GS1 in the EPC Tag Data Standard [10] and used for identification needs of various business domains.

## 3.2 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].

AIoT Ambient IoT

DO-A Device-originated - autonomous

DO-DTT Device-originated - device-terminated triggered

DT Device-terminated

EPC Electronic Product Code

>>>>NEXT CHANGE<<<<

## 6.3 Solution #3: Lightweight Ambient IoT system

### 6.3.1 Description

#### 6.3.1.1 Introduction

This solution proposes a lightweight Ambient IoT system.

#### 6.3.1.2 Definitions

- **Command:** Refers to an instruction sent by an AF to an AIoT Device. The following instructions may be supported:

- Read: Reading data from an AIoT Device;

- Write: Writing data to an AIoT Device;

- Disable: Disable an AIoT Device temporarily or permanently.

- **Command Response:** Refers to the message sent by an AIoT Device in response to a Command. This may include an acknowledgement and optionally data (e.g. in case of the Read operation).

- **Enrichment Data**: Additional information that a Reader may include when providing Inventory information or a Command Response to the AIoT Controller. Enrichment Data may include information about the signal strength for each detected Device ID and the location of the Reader (if known).

- **Filter Criteria**: Criteria to limit an Inventory or Command to AIoT Devices that match certain criteria. Filter Criteria may consist of the following:

- an EPC as defined by GS1 in the EPC Tag Data Standard [10] and optionally a bitmask.Editor's note: Other Filter Criteria are FFS.

NOTE: The term Filter Criteria can be revisited to avoid clashes with existing terminology.

- **Inventory:** Refers to determining the identity of all or a subset of AIoT Devices in range of a reader.

#### 6.3.1.3 Assumptions

This solution makes the following assumptions:

- Commands and Command Responses are end-to-end protected between AF and AIoT Device.

NOTE 1: Details of the end-to-end protection of Commands and Command Results are assumed to be addressed by SA WG3.

- Commands and Command Responses are transparent to the AIoT Controller and the Reader, i.e. the AIoT Controller and Reader are not aware of the contents of Commands and Command Responses.

- AIoT Devices are assumed to be pre-provisioned with a Device ID and the security material for the end-to-end protection of Commands and Command Results. The EPC as defined by GS1 in the EPC Tag Data Standard [10] is used as the Device ID.

NOTE 2: Whether also dynamic (re-)provisioning of Ambient IoT Devices can be supported is up to SA WG3.

- The radio configuration (frequency bands, etc.) of the Reader is assumed to be configured through an OAM system, which is beyond the scope of SA WG2.

#### 6.3.1.4 Reference architecture

This solution proposes the reference architecture depicted in Figure 6.3.1.4-1.



Figure 6.3.1.4-1: Ambient IoT system architecture

The Ambient IoT system according to Figure 6.3.1.4-1 can support different deployment options. For example, the Reader may be co-located with a 3GPP UE so that the communication between Reader and AIoT Controller uses a PDU Session. Alternatively, Readers may be deployed independent of 3GPP UEs, i.e. as stand-alone base stations.

NOTE: The AIoT controller is assumed to be a 3GPP core network entity that enables Ambient IoT scenarios in the context of 5G. Other 5GC network functions are not assumed to be needed.

Editor's note: Whether NEF can potentially be reused for exposure (e.g. AF authorization, etc.) to the AF is FFS.

Editor's note: Further details how the architecture enables topology 1 and 2 are FFS. In case of topology 2, whether AMF is needed in 5GS core network is FFS.

#### 6.3.1.5 Network function description

##### 6.3.1.5.1 Reader

The Reader supports the following functionality:

- Supports the A-Uu air interface towards Ambient IoT Devices.

- Registers with an AIoT Controller.

- Supports the following functionality based on requests from an AIoT Controller:

- Perform one-time or periodic Inventory, deliver Inventory result to AIoT Controller.

- Delivers Commands from an AIoT controller to an AIoT Device.

- Delivers Command Responses received from an AIoT Device to an AIoT Controller.

##### 6.3.1.5.2 AIoT Controller

The AIoT Controller supports the following functionality:

- Register Readers.

- Authenticate and authorize AFs.

- Based on requests from an AF:

- Verify whether an AF is entitled to issue a specific Inventory Request.

- Select Readers to fulfil Inventory or Command request by AFs.

- Forward Inventory request to Readers and deliver Inventory result to AF.

- Forward Command to Readers and Command Responses to AF.

- Optionally collect usage data per AF, e.g. for charging purposes.

- Store last known Reader information for AIoT Devices.

Editor's note: Further details of exposure and charging are FFS.

##### 6.3.1.5.3 AF

The AF is assumed to support the following functionality:

- Authenticate towards the AIoT Controller.

- Send Inventory and Command Requests.

- Receive Inventory Responses and Command Responses.

Editor's note: It is FFS how AF can discover the responsible AIoT controller.

#### 6.3.1.6 Protocol Stacks

##### 6.3.1.6.1 Protocol Stack between Reader and AIoT Controller



**Legend:**

- **Reader Application Protocol (R-AP):** Application Layer Protocol between the Reader and the AIoT Controller.

- **Service-based Interface (SBI) Protocol Stack:** The protocol stack for service-based interfaces as defined in TS 29.500 [9].

Figure 6.3.1.6.1-1: Control Plane between Reader and AIoT Controller

NOTE 1: Whether an SBI protocol stack (consisting of IP/TCP/HTTP2/JSON) as defined in TS 29.500 [9] or an SCTP-based stack will be used will be decided in coordination with RAN3.

NOTE 2: The R-AP protocol is assumed to be defined by RAN3 in coordination with SA2.

NOTE 3: The motivation to propose the R-AP protocol instead of reusing NGAP is that (a) NGAP terminates on the AMF, while AMF is not assumed to be used by this solution and (b) that most of the underlying concepts of NGAP (existence of UE contexts at RAN nodes, PDU Sessions, support of UE mobility, etc.) do not apply to AIoT in this solution.

Editor's note: Whether instead of a new R-AP protocol a simplified version of NGAP can be defined to support AIoT scenarios is FFS and can be discussed with RAN WG3.

Editor's note: Further details of using an SBI protocol stack-based interface between a Reader function co-located with a UE and the AIoT Controller over the PDU Session are FFS.

##### 6.3.1.6.2 Protocol Stack between AIoT Device and Application Function



**Legend:**

- **Reader Application Protocol (R-AP):** Application Layer Protocol between the Reader and the AIoT Controller.

- **Service-based Interface (SBI) Protocol Stack:** The protocol for service-based interfaces as defined in TS 29.500 [9].

- **AIoT API:** The API between AIoT Controller and Application Function to support Inventory and Command Procedures.

- **Command Protocol:** Application Layer Protocol between AIoT Device and Application Function to support Commands and Command Responses.

Figure 6.3.1.6.2-1

NOTE 1: The AIoT API is assumed to be defined by SA2 (Stage 2 aspects) and CT3 (Stage 3 aspects).

NOTE 2: The Command Protocol is assumed to be defined by SA2 (Stage 2 aspects) and CT1 (Stage 3 aspects).

### 6.3.2 Procedures

#### 6.3.2.1 Inventory procedure

Figure 6.3.2.1: Inventory procedure

1. The AF sends an Inventory Request to the AIoT controller. The AF may optionally include the following information:

- Filter Criteria to limit the inventory to AIoT Devices matching those criteria;

NOTE: If the AF does not provide Filter Criteria, then a full inventory of all AIoT devices reachable by the Reader(s) will be performed.

- a list of reader IDs to limit the inventory to specific Readers;

- a periodicity value to request the inventory to be performed periodically.

As part of the Filter Criteria an AF may provide an EPC and optionally a bitmask. This enables the AF to trigger a targeted inventory:

- For example, an AF may want to inventory complete shipments only (identified by AIoT devices attached to the pallets that carry the shipment), without having to unnecessarily inventory also all AIoT devices which may be located on the pallets. This can be achieved by limiting the inventory to AIoT devices that carry an EPC based on the Serial Shipping Container Code EPC scheme. To do so, the AF may provide a bitmask that only matches on the Header value of the EPC and an EPC value that contains the standardized Header value for the Serial Shipping Container Code EPC scheme. (See Annex X for further details on EPC schemes and EPC Header values.).

- Another example is an AF that may only want to inventory individual items from a specific company. This can be achieved by limiting the inventory to AIoT devices that carry an EPC that is based on the Serialised Global Trade Item Number (SGTIN) EPC scheme and where the GS1 Company Prefix contained in the SGTIN matches the company prefix of the specific company that the AF is interested in. To do so, the AF may provide a bitmask matching on the Header value of the EPC and the bits of the GS1 Company Prefix contained in the Serialised Global Trade Item Number (SGTIN) EPC scheme and may provide an EPC that contains the standardized Header value for the Serialised Global Trade Item Number (SGTIN) and the Company Prefix value of the company that the AF is interested in.

2. The AIoT controller verifies whether the AF is entitled to make the received Inventory Request, e.g. the AIoT controller verifies whether the AF is allowed to issue an Inventory Request with the specified Filter Criteria or without any Filter Criteria, without providing reader IDs, etc.

3. The AIoT controller sends the Inventory Request to the Readers identified by the Reader IDs or to all readers, includes the Filter Criteria and periodicity information, if provided by the AF.

4. Each Reader that received the Inventory Request from the AIoT Controller performs the Inventory procedure according to the Filter Criteria, if provided. If the Filter Criteria contain an EPC and optionally a bitmask, then the Reader sends the EPC and the bitmask as part of the inventory request. The Readers either perform a one-time inventory or perform the inventory periodically according to the received periodicity.

NOTE: The details of the EPC are transparent to the Reader.

5. If the Inventory Request contains an EPC, then the AIoT Device compares the received EPC with its Device ID, i.e., the locally stored EPC. If the Inventory Request also contains a bitmask, then the AIoT Device only compares the relevant bits according to the bitmask.

6.

NOTE: This enables the case if an AF wants to perform a full inventory.

If the Inventory Request contains an EPC and optionally a bitmask and the received EPC matches the locally stored EPC as described in the previous step, then the AIoT Device responds to the Reader. The AIoT Device includes its Device ID in the Inventory Response.

7. The Readers collects the received Device IDs and provides the Device IDs to the AIoT Controller. The Readers may optionally include Enrichment Data.

8. For each reported Device ID, the AIoT Controller stores the reader ID that reported the Device ID together with a timestamp. The timestamp enables the AIoT controller to purge outdated last known Reader information; the details of this are up to AIoT Controller implementation.

9. The AIoT Controller provides the Device IDs and optionally the Enrichment Data to the AF.

NOTE: The AIoT Controller provides the Device IDs as received to the AF, i.e., the AIoT Controller is not assumed to verify Device IDs.

Editor's note: Whether the AIoT Controller additionally provides the Reader ID for each Device ID (i.e. the last known Reader ID for each Device ID) to the AF is FFS.

#### 6.3.2.2 Command procedure



Figure 6.3.2.2: Command procedure

1. The AF issues a Send Command request, which includes the Command to be sent and either:

- a list of Device IDs that the Command is destined to, or;

- Filter Criteria that identify the AIoT Devices that are supposed to act upon the Command.

In addition, if the AF provides Filter Criteria, the AF may additionally include a list of reader IDs to use for sending the Command.

NOTE: Including the list of reader IDs enables the AF to limit sending of the Command to a specific area.

2. The AIoT Controller determines the list of Readers to use for sending the Command taking the Reader IDs (if provided by the AF) and any stored information about the last known Reader for specific Device IDs into account. The details of determining candidate Readers are up to AIoT Controller implementation.

3. The AIoT Controller provides the Command and the Device IDs or Filter Criteria (whichever has been provided by the AF) to the Readers.

Editor's note: Whether the Reader needs to perform an Inventory before sending the command to the AIoT devices is FFS.

4. Each Reader that receives the Send Command request from the AIoT Controller, sends the Command to the AIoT Devices identified by the Device IDs or to the AIoT Devices identified by the Filter Criteria (whichever has been provided by the AIoT Controller).

Editor's note: The details of how the Filter Criteria are applied during the Command procedure are FFS.

Editor's note: Failure handling, e.g. if an AIoT device is not reachable is FFS.

5. The AIoT Device(s) respond to the Reader and provide the Command Response.

6. The Readers send the received Command Response(s) to the AIoT Controller. The Readers may optionally include Enrichment Data.

7. The AIoT Controller sends the received Command Response(s) and optionally Enrichment Data to the AF.

NOTE: Support of sending the same Command to multiple AIoT Devices requires support of group security for the Command (e.g. group keys for protecting the Command), which depends on SA WG3.

### 6.3.3 Impacts on services, entities and interfaces

New network entities and interfaces are proposed.

>>>>NEXT CHANGE<<<<

# Annex X: Overview of the Electronic Product Code

The EPC Tag Data Standard [10], issued and maintained by the GS1 organisation [X1], defines the Electronic Product Code as follows:

*The EPC is a universal identifier that provides a unique identity for any physical object. The EPC is designed to be unique across all physical objects in the world, over all time, and across all categories of physical objects. It is expressly intended for use by business applications that need to track all categories of physical objects, whatever they may be.*

In line with this definition, it is important to emphasize that the EPC Tag Data Standard [10] defines EPC as a means for unique identification of physical objects independently of any technology for storing and transmitting such EPC information. In other words, EPCs can be used independently of existing RFID tags.

Despite the word "product" that is an integral part of the term Electronic Product Code, EPCs are not only used for instance for retail items. Instead, the EPC Tag Data Standard [10] defined identification schemes for various business domains to enable identification of

- individual trade items based on the Serialised Global Trade Item Number (SGTIN) EPC scheme;

- logistics handling units (e.g., a pallet load) based on the Serial Shipping Container Code (SSCC) EPC scheme;

- returnable assets such as boxes, pallets and casks based on the Global Returnable Asset Identifier (GRAI);

- aircraft parts based on the Aerospace and Defense Identifier (ADI) EPC scheme;

- patients and the services provided to them based on the Global Service Relation Number (GSRN) EPC scheme (see also [X2] for more information on the use of EPC in the healthcare supply chain);

- etc.

The reason that EPCs are unique despite being used by independently operating organizations in many different domains is the typical structure of the underlying EPC schemes, which typically include an organizational identifier.

For example, as illustrated in Fig. X.1, the Serial Shipping Container Code (SSCC) as defined in clause 6.3.2 of the EPC Tag Data Standard [10], consists of a GS1 Company Prefix and a Serial Reference. The GS1 Company Prefix number space is managed by the GS1 organization, which assigns GS1 Company Prefix numbers to individual organizations. The serial reference is then assigned by the organization itself. Together this yields a unique EPC.

|  |  |
| --- | --- |
| GS1 Company Prefix | Serial Reference |

Fig X.1: Serial Shipping Container Code EPC scheme.

The EPC Tag Data Standard [10] follows the same approach also for other EPC schemes, e.g., the Serialised Global Trade Item Number (SGTIN), which is used for individual trade items such as an instance of a specific product (e.g., an individual TV). As depicted in Fig. 2, the SGTIN also contains a unique GS1 Company Prefix. In addition, the SGTN contains the Item Reference (to differentiate different object classes) and a Serial number, which are assigned by the organization identified by the company prefix.

|  |  |  |
| --- | --- | --- |
| GS1 Company Prefix | Item Reference | Serial Number |

Fig X.2: Serialised Global Trade Item Number (SGTIN) EPC scheme.

In clause 14, the EPC Tag Data Standard [10] also defines a binary encoding of the EPC schemes, i.e., the standard also defines how EPCs are serialized as a string of bits, e.g., for storage on tags.

As shown in Fig. 3, the key idea is that a binary representation of an EPC starts with a header value that indicates the EPC scheme followed by the bitwise representation of a particular encoding scheme. For instance, SSCC-96 defines how the GS1 Company Prefix and the Serial Reference of the Serial Shipping Container Code are represented as a string of bits. The typical size of EPCs, e.g., for the Serialised Global Trade Item Number using the SGTIN-96 coding scheme is 96 bits (including the Header value).

|  |  |  |
| --- | --- | --- |
| EPC scheme | Header value | Coding scheme specific bits |
| Serial Shipping Container Code (SSCC) | 0011 0001 | SSCC-96 as defined in clause 14.6.2.1 of [10] |
| Serialised Global Trade Item Number (SGTIN) | 0011 0000 | SGTIN-96 as defined in clause 14.6.1.1 of [10] |

Fig X.3: The EPC binary representation consists of the header value that identifies the EPC scheme and coding scheme specific bits, e.g. SSCC-96 for the Serial Shipping Container Code as defined in [10]. (Note: This table shows a subset only.)

>>>>END OF CHANGES<<<<