**3GPP TSG-SA WG2 Meeting #162 S2-2404490**

**Changsha, China, 2024-04-15 – 2024-04-19 (Revision of S2-240xxxx)**

**Title: [Draft] LS on Clarification of requirements for Ambient IoT**

**Response to: -**

**Release:** **Rel-19**

Work Item: FS\_AmbientIoT

Source: Ericsson (will be SA2)

To: SA1, SA3

Cc: -

Contact Person: Peter Hedman

E-mail Address: peter (dot) hedman (at) ericsson (dot) com

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:** -

# 1 Overall description

While progressing the study on Ambient IoT, SA2 discussed some of the SA1 requirements in TS 22.369 and SA2 would like to ask SA1 the following questions:

**Question 1:** Are the requirements in TS 22.369 the only service requirements that apply for Ambient IoT devices or are requirements, e.g. for support of an unalterable equipment identification, e.g. IMEI also valid for Ambient IoT devices?

**Question 3** The scope of TS 22.369 states that the document includes e.g. "Overview of Ambient IoT service and operation", but it is not clear to SA2 what constitutes the Ambient IoT services and what are the Ambient IoT operations. Further, clause 4.3 discusses use cases while it is stated in clause 6: "Ambient IoT service can be categorized into 4 categories, namely inventory, sensor data collection, tracking and actuator control" i.e. differences between services, operations and use cases in TS 22.369 is not clear. SA2 therefore assumes that TS 22.369 addresses use cases and SA2 can address each of those with one or more procedures including one or more Ambient IoT operations. Can SA1 confirm SA2 understanding?

Further, SA2 discussed the **security requirements** in TS 22.369 chapter 5.2.6 i.e.:

*The 5G system shall enable security protection suitable for Ambient IoT,* ***without compromising overall 5G security protection****.*

*The 5G system shall be able to provide a mechanism* ***to protect the privacy of information (e.g., location and identity****) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.*

*Based on subscription and operator policies, the 5G system shall authorize an Ambient IoT capable UE to communicate with a specific Ambient IoT device or with a group of Ambient IoT devices.*

**Question 4:** Inventory is meant to retrieve identifier associated to the Ambient IoT device and possibly retrieve more information e.g. device capabilities, status, measurement results and/or location (FFS whether additional information from the Ambient IoT device is to use a separate read command).While SA2 acknowledges the requirements on security and privacy in TS 22.369, SA2 would like to understand whether all the information need to be protected (integrity and/or confidentiality) or whether some information can be sent unprotected?

SA2 assumes that information that is essential for routing of the messages to an entity that can perform device authentication does not need to be confidentiality protected.

**Question 5:** SA2 would like to understand whether authentication, integrity and confidentiality protection is to be mandated for Ambient IoT devices using 3GPP access?

# 2 Actions

**To SA1**

**ACTION:** SA2 kindly asks SA1 to provide answers to the questions 1, 2, 3, 4, and 5.

**To SA3**

**ACTION:** SA2 kindly asks SA3 to provide answers to the question 4 and 5.

# 3 Date of next TSG SA WG SA2 meetings

SA2#163 2024-05-27 – 2024-05-31 Jeju, Korea

SA2#164 2024-08-19 – 2024-08-23 Maastricht, NL

# Annex: To help reader/discussions i.e. remove before sending LS

-------------------- Copy of TS 22.101 - remove before submission ------------------------

14 Types of features of UEs

3GPP specifications should support a wide variety of user equipment, i.e. setting any limitations on terminals should be avoided as much as possible. For example user equipment like hand-portable phones, personal digital assistants and laptop computers can clearly be seen as likely terminals.

In order not to limit the possible types of user equipment they are not standardised. The UE types could be categorised by their service capabilities rather than by their physical characteristics. Typical examples are speech only UE, narrowband data UE, wideband data UE, data and speech UE, etc.

In order to enhance functionality split and modularity inside the user equipment the interfaces of UE should be identified. Interfaces like UICC-interface, PCMCIA-interface and other PC-interfaces, including software interfaces, should be covered by references to the applicable interface standards.

UEs have to be capable of supporting a wide variety of teleservices, multimedia services and applications provided in PLMN environment. Limitations may exist on UEs capability to support all possible teleservices, multimedia services and information types (speech, narrowband data, wideband data, video, etc.) and therefore functionality to indicate capabilities of a UE shall be specified.

The basic mandatory UE requirements are:

- Support for USIM. Optional support of GSM phase 2, 2+, 3GPP Release 99 and Release 4 SIM cards [34]. Phase 1, 5V SIM cards shall not be supported. Support for the SIM/ISIM is optional for the UE, however, if it is supported, the mandatory requirements for SIM/ISIM shall be supported in the UE;

Note 1: There is no Release 5 specification for the SIM, and therefore references to "SIM" apply to earlier releases.

Note 2: It is strongly recommended that manufacturers implement SIM support on terminals supporting GERAN until the population of SIMs in the market is reduced to a low level.

- Home environment and serving network registration and deregistration;

- Location update;

- Originating or receiving a connection oriented or a connectionless service;

- An unalterable equipment identification; IMEI, see 3GPP TS 22.016 [12];

- Basic identification of the terminal capabilities related to services such as; the support for software downloading, application execution environment/interface, MExE terminal class, supported bearer services.

- Terminals capable for emergency calls shall support emergency call without a SIM/USIM/ISIM.

- Support for the execution of algorithms required for encryption, for CS and PS services. Support for non encrypted mode is required;

- Support for the method of handling automatic calling repeat attempt restrictions as specified in 3GPP TS 22.001 [4];

- At least one capability type shall be standardised for mobile terminals supporting the GERAN,UTRAN and E-UTRAN radio interfaces.

- Under emergency situations, it may be desirable for the operator to prevent UE users from making access attempts (including emergency call attempts) or responding to pages in specified areas of a network, see 3GPP TS 22.011 [11];

- Ciphering Indicator for terminals with a suitable display;

- The ciphering indicator feature allows the UE to detect that the 3GPP radio interface ciphering (user plane) is not switched on and to indicate this to the user. The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. The default terminal behaviour shall be to take into account the operator setting data in the SIM/USIM. However, terminals with a user interface that can allow it, shall offer the possibility for the user to configure the terminal to ignore the operator setting data in the SIM/USIM. If this feature is not disabled by the SIM/USIM or if the terminal has been configured to ignore the operator setting data in the SIM/USIM, then whenever a user plane connection is in place, which is, or becomes un-enciphered, an indication shall be given to the user. In addition, if this feature is not disabled by the SIM/USIM or if the terminal has been configured to ignore the operator setting data in the SIM/USIM, then additional information may also be provided about the status of the ciphering. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;

- Support for PLMN selection.

- Support for handling of interactions between toolkits concerning the access to UE MMI input/output capabilities;

- Whenever an application (e.g. a SAT/MExE/WAP application) requires the access to the UE MMI input/output capabilities (e.g. display, keyboard,… ), the UE shall grant this access subject to the capabilities of the UE. This shall not cause the termination of any other applications (e.g. WAP browser or MExE/SAT application) which were previously using these UE resources. The UE shall give the user the ability to accept or reject the new application. In the case that the application request is rejected, the access to the UE MMI input/output capabilities is returned to the applications which were previously using these UE resources. If the user decides to continue with the new application, then when this new application is terminated, the access to the UE MMI input/output capabilities shall be returned to the UE to be re-allocated to applications (e.g. the preceding application which was interrupted). Subject to the capabilities of the UE, the user shall have the ability to switch the MMI input/output capabilities between applications.

NOTE: Rejecting a request to access the UE MMI input/output capabilities by an application does not necessarily mean that it is terminated, but only that the access to the UE MMI input/output capabilities are not granted to this application. Handling of rejection (termination, put on hold,…) is the responsibility of the application.

Annex A describes a number of features which may optionally be supported by the UE.

-------------------- Copy of TS 22.369 - remove before submission ------------------------

### 5.2.6 Security and privacy

The 5G system shall enable security protection suitable for Ambient IoT, without compromising overall 5G security protection.

The 5G system shall be able to provide a mechanism to protect the privacy of information (e.g., location and identity) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.

Based on subscription and operator policies, the 5G system shall authorize an Ambient IoT capable UE to communicate with a specific Ambient IoT device or with a group of Ambient IoT devices.

------------ 22.261-------------

6.14.2 Requirements

An IoT device which is able to access a 5G PLMN in direct network connection mode using a 3GPP RAT shall have a 3GPP subscription.

The 5G system shall allow the operator to identify a UE as an IoT device based on UE characteristics (e.g. identified by an equipment identifier or a range of equipment identifiers) or subscription or the combination of both.

The 5G system shall be able to provide mechanisms to change the association between a subscription and address/number of an IoT device (e.g. changing the owner and subscription information associated with the IoT device) within the same operator and in between different operators in an automated or manual way.

The 5G system shall be able to support identification of subscriptions independently of identification of IoT devices. Both identities shall be secure.

An IoT device which is able to connect to a UE in direct device connection mode shall have a 3GPP subscription, if the IoT device needs to be identifiable by the core network (e.g. for IoT device management purposes or to use indirect network connection mode).

Based on operator policy, the 5G system shall support a mechanism to provision on-demand connectivity (e.g. IP connectivity for remote provisioning). This on-demand mechanism should enable means for a user to request on-the-spot network connectivity while providing operators with identification and security tools for the provided connectivity.

The 5G system shall support a secure mechanism for a home operator to remotely provision the 3GPP credentials of a uniquely identifiable and verifiably secure IoT device.

The 5G system shall support a secure mechanism for the network operator of an NPN to remotely provision the non-3GPP identities and credentials of a uniquely identifiable and verifiably secure IoT device.

Based on MNO and NPN policy, the 5G system shall support a mechanism to enable MNO to update the subscription of an authorized UE in order to allow the UE to connect to a desired NPN. This on-demand mechanism should enable means for a user to request on-the-spot network connectivity which is authorized by its MNO.

Based on operator policy, the 5G system shall provide means for authorised 3rd parties to request changes to UE subscription parameters for access to data networks, e.g., static IP address and configuration parameters for data network access.