**3GPP TSG-SA1 Meeting #106 *S1-241335***

**Jeju, Korea (Republic Of), 27th May 2024 - 31st May 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.3* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **22.261** | **CR** | **0771** | **rev** | **2** | **Current version:** | **18.13.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network | **x** | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Alignment for Smart Energy Infrastructure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung, China Telecom, Huawei | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SEI | | | | |  | ***Date:*** | | | 2024-05-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Some requirements added to TS 22.261 were not supported in Release 18 stage 2 and stage 3 standardization. To align all 3GPP specifications, these unfulfilled requirements are removed from the Release 18 version of the specification. Other requirements have been satisfied in Release 18, mainly in TS 28.318. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Text in specific clauses is removed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | This specification will remain incompletely aligned with other 3GPP specifications for Release 18. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.10.2, 6.14.2, 6.23.2, 6.28.1, 6.28.2.2, 8.9 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

FIRST CHANGE

### 6.10.2 Requirements

The following set of requirements complement the requirements listed in 3GPP TS 22.101 [6], clause 29.

Based on operator policy, a 5G network shall provide suitable APIs to allow a trusted third-party to create, modify, and delete network slices used for the third-party.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party to monitor the network slice used for the third-party.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party to define and update the set of services and capabilities supported in a network slice used for the third-party.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party to configure the information which associates a UE to a network slice used for the third-party.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party to configure the information which associates a service to a network slice used for the third-party.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party to assign a UE to a network slice used for the third-party, to move a UE from one network slice used for the third-party to another network slice used for the third-party, and to remove a UE from a network slice used for the third-party based on subscription, UE capabilities, and services provided by the network slice.

The 3GPP network shall be able to provide suitable and secure means to enable an authorized third-party to provide the 3GPP network via encrypted connection with the expected communication behaviour of UE(s).

NOTE 1: The expected communication behaviour is, for instance, the application servers a UE is allowed to communicate with, the time a UE is allowed to communicate, or the allowed geographic area of a UE.

The 3GPP network shall be able to provide suitable and secure means to enable an authorized third-party to provide via encrypted connection the 3GPP network with the actions expected from the 3GPP network when detecting behaviour that falls outside the expected communication behaviour.

NOTE 2: Such actions can be, for instance, to terminate the UE's communication, to block the transferred data between the UE and the not allowed application.

The 5G network shall be able to provide secure means for providing communication scheduling information (i.e. the time period the UE(s) will use a communication service) to an NPN via encrypted connection. This communication scheduling information is used by the 5G network to perform network energy saving and network resource optimization.

The 5G network shall provide a mechanism to expose broadcasting capabilities to trusted third-party broadcasters' management systems.

Based on operator policy, a 5G network shall provide suitable APIs to allow a trusted third-party to manage this trusted third-party owned application(s) in the operator's Service Hosting Environment.

Based on operator policy, the 5G network shall provide suitable APIs to allow a third-party to monitor this trusted third-party owned application(s) in the operator's Service Hosting Environment.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party to scale a network slice used for the third-party, i.e. to adapt its capacity.

Based on operator policy, a 5G network shall provide suitable APIs to allow one type of traffic (from trusted third-party owned applications in the operator's Service Hosting Environment) to/from a UE to be offloaded to a Service Hosting Environment close to the UE's location.

Based on operator policy, the 5G network shall provide suitable APIs to allow a trusted third-party application to request appropriate QoE from the network.

Based on operator policy, the 5G network shall expose a suitable API to an authorized third-party to provide the information regarding the availability status of a geographic location that is associated with that third-party.

Based on operator policy, the 5G network shall expose a suitable API to allow an authorized third-party to monitor the resource utilisation of the network service (radio access point and the transport network (front, backhaul)) that are associated with the third-party.

Based on operator policy, the 5G network shall expose a suitable API to allow an authorized third-party to define and reconfigure the properties of the communication services offered to the third-party.

The 5G system shall support the means for disengagement (tear down) of communication services by an authorized third-party.

Based on operator policy, the 5G network shall expose a suitable API to provide the security logging information of UEs, for example, the active 3GPP security mechanisms (e.g. data privacy, authentication, integrity protection) to an authorized third-party.

Based on operator policy, the 5G system shall provide suitable means to allow a trusted and authorized third-party to consult security related logging information for the network slices dedicated to that third-party.

Based on operator policy, the 5G network shall be able to acknowledge within 100 ms a communication service request from an authorized third-party via a suitable API.

The 5G network shall provide suitable APIs to allow a trusted third-party to monitor the status (e.g. locations, lifecycle, registration status) of its own UEs.

NOTE 3: The number of UEs could be in the range from single digit to tens of thousands.

The 5G network shall provide suitable APIs to allow a trusted third-party to get the network status information of a private slice dedicated for the third-party, e.g. the network communication status between the slice and a specific UE.

The 5G system shall support APIs to allow the non-public network to be managed by the MNO's Operations System.

The 5G system shall provide suitable APIs to allow third-party infrastructure (i.e. physical/virtual network entities at RAN/core level) to be used in a private slice.

A 5G system shall provide suitable APIs to enable a third-party to manage its own non-public network and its private slice(s) in the PLMN in a combined manner.

The 5G system shall support suitable APIs to allow an MNO to offer automatic configuration services (for instance, interference management) to non-public networks deployed by third parties and connected to the MNO's Operations System through standardized interfaces.

The 5G system shall be able to:

- provide a third-party with secure access to APIs (e.g. triggered by an application that is visible to the 5G system), by authenticating and authorizing both the third-party and the UE using the third-party's service.

- provide a UE with secure access to APIs (e.g. triggered by an application that is not visible to the 5G system), by authenticating and authorizing the UE.

- allow the UE to provide/revoke consent for information (e.g., location, presence) to be shared with the third-party.

- preserve the confidentiality of the UE's external identity (e.g. MSISDN) against the third-party.

- provide a third-party with information to identify networks and APIs on those networks.

The 5G system shall provide a means by which an MNO can inform authorised 3rd parties of changes in the

- RAT type that is serving a UE;

- cell ID.

NEXT CHANGE

### 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 configuration parameters for data network access.

NEXT CHANGE

### 6.23.2 Requirements

The 5G system shall provide a mechanism for supporting real-time E2E QoS monitoring within a system.

NOTE 1: The end points in E2E are the termination points of the communication service within the boundary of the 5G system.

The 5G system shall support combined QoS monitoring for a group of UEs.

NOTE 1A: Combined monitoring stands for the monitoring of several UEs for which the monitoring results are reported together. An example for combined QoS monitoring is that the 5G networks monitors the service bit rates of all connections associated with the group of UEs.

The 5G network shall provide an interface to an application for QoS monitoring (e.g. to initiate QoS monitoring, request QoS parameters, events, logging information).

The 5G system shall be able to provide real time QoS parameters and events information to an authorized application/network entity.

NOTE 2: The QoS parameters to be monitored and reported can include latency (e.g. UL/DL or round trip), jitter, and packet loss rate.

The 5G system shall be able to log the history of the communication events.

NOTE 3: The communication history may include timestamps of communication events and position-related information. Examples of such information are the positions of UEs and of radio base stations associated with communication events. Communication events include instances when the required QoS is not met.

The 5G system shall support different levels of granularity for QoS monitoring (e.g. per flow or set of flows).

The 5G system shall be able to provide event notification upon detecting an error that the negotiated QoS level cannot be met/guaranteed.

The 5G system shall be able to provide information that identifies the type and the location of a communication error (e.g. cell ID).

The 5G system shall be able to provide notification of communication events to authorized entities per pre-defined patterns.

NOTE 4: An example for a communication event is that the service bit rate drops below a pre-defined threshold for QoS parameters. When such an event occurs, the authorized entity is notified, and the event is logged.

The 5G system shall support event-based QoS monitoring.

NOTE 5: An example for a triggering event is a position change of the pertinent UE. A position change can, for instance, be inferred from a 5G position service that tracks the UE.

The 5G system shall be able to respond to a request from an authorized entity to provide real-time QoS monitoring information within a specified time after receiving the request (e.g., within 5 s).

NOTE 6: The response time can be specified by the user.

The 5G system shall support an update/refresh rate for real time QoS monitoring with a specified value (e.g., at least one update per second).

The 5G system shall be able to provide statistical information of service parameters and error types while a communication service is in operation.

NOTE 7: The time span for collection and evaluation of statistical values can be specified by the user.

The 5G system shall provide information on the current availability of a specific communication service in a particular area (e.g. cell ID) upon request of an authorized entity.

The 5G system shall provide a means by which an MNO informs a third party of network events (failure of network infrastructure affecting UEs in a particular area, etc.).

Based on MNO policy, the 5G system shall provide a mechanism to automatically report service degradations, communications loss, and sustained connection loss in a specific geographic area (e.g., a cell sector, a cell or a group of cells) to a third party.

NOTE 8: These reports use a standard format. The specific values, thresholds, and conditions upon which alarms occur can include the measured values for end-to-end latency, service bit rate, communication service availability, end-to-end latency jitter, etc. for a UE, the UE’s location, and the time(s) during which the degradation occurred.

NOTE 9: What the MNO does with such reports is out of scope of 3GPP.

NEXT CHANGE

### 6.28.1 Description

The 5G system is expected to meet the service requirements for cyber-physical control applications in vertical domains.

A vertical domain is a particular industry or group of enterprises in which similar products or services are developed, produced, and provided. Automation refers to the control of processes, devices, or systems in vertical domains by automatic means. The main control functions of automated control systems include taking measurements, comparing results, computing any detected or anticipated errors, and correcting the process to avoid future errors. These functions are performed by sensors, transmitters, controllers, and actuators.

Cyber-physical systems are to be understood as systems that include engineered, interacting networks of physical and computational components. Cyber-physical control applications are to be understood as applications that control physical processes. Cyber-physical control applications in automation follow certain activity patterns, which are open-loop control, closed-loop control, sequence control, and batch control.

Communication services supporting cyber-physical control applications need to be ultra-reliable, dependable with a high communication service availability, and often require low or (in some cases) very low end-to-end latency.

Communication in automation in vertical domains follows certain communication patterns. The most well-known is periodic deterministic communication, others are a-periodic deterministic communication and Smart Grid.

Smart Grid is a term that refers to enhanced cyber-physical control of electrical grids and to related application. Smart Grid operation can cover power generation, transmission, distribution, and consumption, which can require high communication service availability and communication service reliability. 5G system functionalities can be used for Smart Grid control, monitoring, availability assurance, service security, isolation and etc. Communication for cyber-physical control applications supports operation in various vertical domains, for instance industrial automation and energy automation.

For more information about cyber-physical control applications in specific vertical domains, see clauses D.1 to D.4.

NEXT CHANGE

#### 6.28.2.2 Smart Grid

For the 5G system to support the Smart Grid, the 5G systems needs to fulfil at minimum the following requirements.

- 3GPP TS22.104, clauses 9 and A.4 for Smart Grid specific service requirements;

- 3GPP TS 22.261, clause 6.26 for requirements related to the support of secured communication between the 5G system and a trusted third-party;

- 3GPP TS 22.261, clauses 6.23 for the requirements related to information exchange between the 5G system and a trusted third-party;

NEXT CHANGE

## 8.9 Data security and privacy

The 5G system shall support data integrity protection and confidentiality methods that serve URLLC, high data rates and energy constrained devices.

The 5G system shall support a mechanism to verify the integrity of a message as well as the authenticity of the sender of the message.

The 5G system shall support encryption for URLLC services within the requested end-to-end latency.

Subject to regulatory requirements, the 5G system shall enable an MNO to provide end-to-end integrity protection, confidentiality, and protection against replay attacks between a UE and third-party application server, such that the 3GPP network is not able to intercept or modify the data transferred between a UE and third-party application server.

Subject to regulatory requirements and based on operator policy, the 5G system shall provide a mechanism to support data integrity verification service to assure the integrity of the data exchanged between the 5G network and a third-party service provider.

NOTE: This requirement could apply to mechanisms supported over the interface between 5G core network and an external application, with no impact on RAN and UE.

END OF CHANGES