**3GPP TSG-SA1 Meeting #92e *S1-204043***

**Electronic Meeting, 10 September - 19 September 2020** *(revision of S1-20XXXX)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **22.261** | **CR** |  | **rev** |  | **Current version:** | 18.0.0 |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Addition of requirements on Data Integrity in 5GS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China Unicom,Spreadtrum Communications | | | | | | | | | |
| ***Source to TSG:*** | SA1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | DUMMY | | | | |  | ***Date:*** | | | 2020-11-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Verticals, such as supply chain finance and insurance, have strict requirements for IoT data integrity, e.g. environment data including temperature and windspeed data, and agricultural insurance and warehouse data (e.g. number and weight of goods) for inventory financing. Those services require to guarantee data integrity from UE to a 3rd party/SP (Service Provider).  An example use case:  During the transportation of vaccines/drugs, vaccines/drugs containers in cold chain logistics may be equipped with IoT sensors which send data to the vehicles. Those vehicles connect to a 3rd party/SP platform by 3GPP network for data gathering and processing. Real-time monitoring is very critical since the products in the container may exceptionally sensitive to changes in pH, temperature and even light conditions.  Ensuring the data integrity of the collected environment data in each container/sensor is necessary to the service in order to guarantee the vaccine/drug’s status.  In this use case, the requirements are to achieve the data integrity for the environmental data from IoT sensors to the 3rd party/SP. If problems arose, the 3rd party/SP (hospital or vaccine company) would claim to trace all the environment data during transportation afterwards and the data integrity may be non-real-time.  While data integrity methods are provided within the 3GPP network, there are gaps in ensuring end-to-end data integrity from UE to 3rd party/Service Providers using the 3GPP Network.  Therefore, data integrityof IoT UE for certain vertical services is required. Enterprise customers of mobile telecommuncations would benefit from a standardized means to achieve data integrity.  MNOs will be able to providedata integrity for communications with their service users as a fundamental service enabler. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | To add requirements on Data Integrity between the 5GS and 3rd party AFs to the 5GS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Data integrity from 5GS to 3rd party/SP cannot be guaranteed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.2 and 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:*** | |  | | | | | | | | |

---Start of the First Change---

8. Security

8.2 General

The 5G system shall support a secure mechanism to store cached data.

The 5G system shall support a secure mechanism to access a content caching application.

The 5G system shall support a secure mechanism to access a service or an application in an operator's Service Hosting Environment.

The 5G system shall enable support of an access independent security framework.

The 5G system shall support a mechanism for the operator to authorize subscribers of other PLMNs to receive temporary service (e.g. mission critical services).

The 5G system shall be able to provide temporary service for authorized users without access to their home network (e.g. IOPS, mission critical services).

The 5G system shall allow the operator to authorize a third-party to create, modify and delete network slices, subject to an agreement between the third-party and the network operator.

Based on operator policy, a 5G network shall provide suitable means to allow a trusted and authorized third-party to create and modify network slices used for the third-party with appropriate security policies (e.g. user data privacy handling, slices isolation, enhanced logging).

The 5G system shall support a secure mechanism to protect relayed data from being intercepted by a relay UE.

Subject to HPLMN policy as well as its service and operational needs, any USIM able to access EPS instead of a 5G USIM may be used to authenticate a user in a 5G system to access supported services according to the user‘s subscription.

The 5G system shall provide integrity protection and confidentiality for communications between authorized UEs using a 5G LAN-type service.

The 5G LAN-VN shall be able to verify the identity of a UE requesting to join a specific private communication.

The 5G system shall provide suitable means to allow use of a trusted third-party provided encryption between any UE served by a private slice and a core network entity in that private slice.

The 5G system shall provide suitable means to allow use of a trusted and authorized third-party provided integrity protection mechanism for data exchanged between an authorized UE served by a private slice and a core network entity in that private slice.

The 5G system shall provide suitable means to allow use of a trusted and authorized third-party provided integrity protection mechanism for data exchanged between an authorized UE served by a non-public network and a core network entity in that non-public network.

The 5G system shall support a mechanism to provide data integrity protection for communication between a UE and an Application Server offered by a 3rd party/ Service Provider.

---End of the Change---

---Start of the Second 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.

The 5G system shall support a mechanism to provide data integrity protection for communication between a UE and an Application Server offered by a 3rd party/Service Provider both in real time and after a period of time.

NOTE: Real time in this context means the 3rd party/SP verifies the data integrity when it obtains the data from the UE, e.g. real time monitoring services. After a period of time means the 3rd party/SP verifies the integrity of the data a period of time after it has been transferred to the SP, e.g. for insurance claim reviews.

Subject to regional or national regulatory requirements and based on operator policy, a 5G network shall provide suitable mechanisms to allow service providers, e.g. other MNOs/third-parties, to verify the integrity of the data sent from a UE to a Service Provider.

---End of the Change---