**3GPP TSG- Meeting #**

**, , -**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The current requirements are not clear for cases when unauthorized information is removed from reported payloads. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | There is a requirement that the unauthorized information not be delivered to the LEA. This CR adds requirements clarifying that when unauthorized information is removed from a payload, the authorized information is unchanged and able to be properly decoded. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The requirements will remain unclear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS 33.126 CRs 0030, 0029 | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | CR 0030 (S3i230299) is the release 16 mirror of this CR. CR 0029 (S3i230298) is the release 17 mirror of this CR. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | s3i230273 | | | | | | | | |

## \*\*\*\* START OF FIRST CHANGE \*\*\*

## 6.4 Delivery

**R6.4 – 10 LI Service Scope** - The CSP shall only deliver Interception Product relating to specific CSP services which are specified implicitly or explicitly in the warrant.

**R6.4 - 15 Delivery of Multiple Services** - The CSP shall be able to deliver Interception Product of multiple services (e.g., CSP provided voice, messaging services, internet access) for a single target.

**R6.4 - 20 Context Correlation -** The CSP shall be able to deliver information such that the LEA can correlate all CC and IRI to the Context of Communications.

**R6.4 - 30 IRI to IRI Correlation -** The CSP shall be able to deliver information such that all the IRI can be correlated with related IRI of the same Target Communication.

**R6.4 - 40 CC to CC Correlation -** The CSP shall be able to deliver information such that all the CC can be correlated with related CC of the same Target Communication.

**R6.4 - 50 IRI and CC Correlation -** The CSP shall be able to deliver information such that the related IRI and CC of the same Target Communication can be correlated.

**R6.4 - 60 POI Identification -** The CSP shall be able to report to the LEA the POI source(s) of the Interception Product.

**R6.4 - 70 Delivery Reliability -** The CSP shall be able to employ mechanisms (e.g. buffering) to limit the effect of delivery network failures or limitations to prevent loss of Interception Product.

**R6.4 - 80 Delivery Latency -** The CSP shall ensure that the Interception Product is delivered to the LEA without undue delay as defined by mutual agreement between the CSP and the LEA.

**R6.4 - 90 Timestamping at Capture -** The CSP shall timestamp the Interception Product (both IRI and CC) at capture (at the POI) with a timestamp of precision, resolution, and accuracy commensurate with the performance of the intercepted service.

**R6.4 - 100 Timestamping at Delivery -** The CSP shall provide, where required for correlation purposes, the timestamp of the Interception Product (both IRI and CC) at the Mediation and Delivery Function (MDF) as sent to the LEMF, with a timestamp of precision, resolution, and accuracy commensurate with the performance of the intercepted service.

**R6.4 - 110 UTC -** The CSP shall provide all timestamps in UTC (including local offset).

**R6.4 - 120 Trusted Time -** The CSP shall utilise a trusted time source for all LI related functions.

**R6.4 - 130 Separate delivery of services** - The CSP shall be able to support delivering Interception Product for a particular service separately from other services' Interception Product (e.g. delivering SMS Interception Product independent of CS Voice Interception Product).

**R6.4 - 140 Ordering -** The CSP shall provide a means to enable the LEA to order the events of an intercepted service.

**R6.4 - 150 Duplication -** The CSP shall endeavour to limit duplicate delivery of Interception Product.

**R6.4 - 160 Encryption -** The CSP shall remove any encryption it provides or manages before delivery of the Interception Product to the LEA, or shall provide the LEA the information necessary to decrypt the intercepted communications (e.g. keys, algorithms, parameters) included with the Interception Product.

**R6.4 - 170 CSP provided Encryption Keys -** If the CSP provides encryption keys to the target, but is not involved in the encryption service, the CSP shall provide the keys to the LEA.

**R6.4 – 175** **CSP provided cryptographic parameters in roaming** – When a home CSP’s subscriber is roaming, independently of whether or not the subscriber is an LI Target in the VPLMN, the home CSP shall provide to the visited CSP the means to decrypt user services which are encrypted between the ME and an entity outside the visited CSP and using cryptographic parameters established in the home CSP.

**R6.4 - 180 Retroactive Decryption -** The CSP shall ensure that the crypto keys, algorithm and parameters delivered to the LEA enable the LEA to decrypt encrypted Target Communications retroactively.

**R6.4 - 190 Mid Communication Interception -** The CSP shall retain sufficient key material for the duration of any communications such that it is possible to decrypt already on going communications, when using CSP provided or managed encryption.

**R6.4 - 200 Encryption Key Material Lifecycle - Destruction** – Once key material specifically retained for LI purposes is no longer required, the CSP shall securely delete this key material.

**R6.4 - 210 Encoding -** The CSP shall be able to remove any specific CSP-controlled encoding before delivery to the LEA, or provide the LEA the information necessary to decode the intercepted communications concurrently with delivery of LI product.

**R6.4 - 220 Compression -** The CSP shall be able to remove any specific CSP-controlled compression before delivery to the LEA, or provide the LEA the information necessary to decompress the intercepted communications concurrently with delivery of LI product.

**R6.4 -230 Target Identifier Provenance** – The CSP shall be able to indicate, for each target identifier provided to the LEA in the Interception Product, the provenance of the identifier, specifically, whether the identifier was provided to the CSP by the LEA (in the initial warrant), whether it was observed in the intercepted communications, whether it was matched on by the function performing the isolation of communications, and whether it was associated with the target.

**R6.4 - 240 Redaction -** The CSP shall be able to redact information not authorized by the warrant from Target Communications such that the authorized information is not altered for delivery as Interception Product.

## \*\*\*\* END OF ALL CHANGES \*\*\*