.

**3GPP TSG- Meeting # *s3i240049r1***

**, , -**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **2** | **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:***  |  and MSBR |
|  |  |
| ***Source to WG:*** | SA3LI (Ministère Economie et Finances) |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***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 canbe 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:*** | Specific LEA requirements related to NTN, Location Dependent Interception ‘(see 3GPP TR 22.926 Guidelines for Extraterritorial 5G Systems;Stage 1 R18).LEA requirements related to Mobile Base Station Relay(MBSR)  |
|  |  |
| ***Summary of change:*** | Requirements of Location Dependent Interception (LDI), its management, its delivery based on location and context. |
|  |  |
| ***Consequences if not approved:*** | Regulatory diffculties of NTN/MBSR developments. |
|  |  |
| ***Clauses affected:*** | 3.2; 6.3; 6.4; 6.5 |
|  |  |
|  | **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:*** | s3i240009, s3i240049 |

\*\*\* First Change \*\*\*

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

ADMF Administration Function

CAT Customized Alerting Tone

CC Content of Communication

CRS Customized Ringing Signal

CSP Communications Service Provider

gNB 5G NodeB

GUTI Globally Unique Temporary Identifier

HeNB Home eNodeB

H(e)NB HNB and HeNB

HNB Home NodeB

IRI Intercept Related Information

LALS Lawful Access Location Services

LDI Location Dependent Interception

LEA Law Enforcement Agency

LEMF Law Enforcement Monitoring Facility

LI Lawful Interception

MBSR Mobile Base Station Relay

MC Mission Critical

MCPTT Mission Critical Push to Talk

MDF Mediation and Delivery Function

NTN Non Terrestrial Network

POI Point Of Interception

SUCI SUbscription Concealed Identifier

SUPI SUbscription Permanent Identifier

ULI User Location Information

UTC Coordinated Universal Time

\*\*\* End of First Change \*\*\*

\*\*\* Second Change \*\*\*

## 6.3 Detect and Capture

**R6.3 - 10 Access Level Interception -** The CSP shall be able to perform network access level interception in both the core and on the edge of the network (e.g. IP-CAN level interception).

**R6.3 - 20 Service Level Interception -** The CSP shall be able to perform service level interception in both the core and on the edge of the network (e.g. IMS based VoIP).

**R6.3 - 30 Multi Party Service Interception -** CSP shall be able to report the multi-party service Interception Product of targeted group communications and its users.

**R6.3 - 40 Third Party Assisted Services -** If a CSP uses Third Parties as part of its service provision, the CSP shall be responsible for ensuring that the overall service complies with applicable LI regulations and requirements.

**R6.3 - 50 Third Party ME or UE Interception** - To the extent that a CSP manages a Third Party ME or UE, the CSP shall be able to report communications of such Third Party ME or UE (e.g. status of devices with a relay or forward function).

**R6.3 - 60 Third Party ME or UE Users Interception** - To the extent that a CSP manages Third Party ME or UE, the CSP shall be able to report communications of the end users connected to the CSP network via a Third Party ME or UE that is managed by the CSP (e.g. status of users communicating via ME or UE with a relay or forward function).

**R6.3 - 70 Modification of services** – Any change to any target service settings, as known to the CSP, shall be able to be reported.

**R6.3 - 80 Multiple Services Per target -** The CSP shall be able to simultaneously perform LI for multiple services for a given target.

**R6.3 - 90 Multiple Targets -** The CSP shall be able to simultaneously perform intercepts on multiple independent targets.

**R6.3 - 100 Multiple LEAs -** The CSP shall be able to simultaneously perform independent intercepts for any given target under different warrants.

**R6.3 - 110 Roaming Targets -** The visited CSP shall be able to perform interception of inbound roaming targets.

**R6.3 - 120 Roaming – Outbound -** The CSP shall be able to notify the LEA whenever the CSP becomes aware that the target has left, or entered, a visited network.

**R6.3 - 130 Roaming – Inbound -** The CSP shall be able to notify the LEA whenever the CSP becomes aware that the inbound roaming target has entered, or has left, the network.

**R6.3 - 140 Serving CSP change -** When the target changes serving CSP, the CSP that is served the warrant shall be able to provide the LEA with the identity of the new CSP if known.

**R6.3 - 141 Serving CSP change / returning to HPLMN** - When the target returns to the HPLMN, the home CSP that is served the warrant shall be able to provide the LEA with the identity of the VPLMN from which the target has returned if known.

**R6.3 - 150 Roaming Identifiers Visited CSP -** The visited CSP shall be able to obtain and validate the long term 3GPP identifiers of all inbound roamers from the home CSP regardless of the use of privacy mechanisms (based on roaming agreements).

**R6.3 - 160 Roaming Identifiers Home CSP -** The home CSP shall provide the long term 3GPP identifiers to the visited CSP for outbound roamers (based on roaming agreements).

**R6.3 - 170 Outbound Roaming Home Network** - CSPs shall be able to intercept its outbound roamers, if the communication pass through the home CSP's network.

**R6.3 – 180 Access Network Identity -** The CSP shall provide the LEA the identity of the 3GPP or non 3GPP Access Network as known by the CSP.

**R6.3 - 190 Location -** The CSP shall be able to obtain and report the location of the target.

**R6.3 - 200 Location Triggers -** The CSP shall be able to obtain and report the target location at certain network events associated with the target.

**R6.3 - 210 Communication Location Reporting -** The CSP shall be able to obtain and report the target location at start and end of communication, as well as during the communication including periodically and per event.

**R6.3 - 220 Location Reporting** - The CSP shall be able to obtain and report the target location for both active and idle MEs or UEs triggered either by UE-Action (e.g. UE cell site change) or on a periodic basis or on demand by the LEA.

**R6.3 - 230 Location Reporting Independency -** Location information may be reported as part of interception of a service (e.g. VoLTE, RCS), or independently.

**R6.3 - 240 Location Accuracy -** The CSP shall report the most accurate target location available to the CSP.

**R6.3 - 245 Radiolocation Assistance -** The CSP shall be able to provide information to assist the LEA to perform radiolocation of target UEs.

**R6.3 - 250 Multiple Location Sources -** The CSP shall be able to report the source of each location information report provided to the LEMF (e.g. cell ID, GPS).

**R6.3 - 260 Location Positioning Methods -** The CSP shall be able to report the positioning method used to obtain location information (e.g. network-based, UE-based, access-based).

**R6.3 - 270 Additional Location Information -** If the CSP has additional location information of the target beyond cell site identifier (e.g. altitude, civic address, geo-coordinates), the CSP shall be able to provide this.

**R6.3 – 275 Location Translation –** If the CSP provides a logical location information (e.g. cell ID) or a non-standard position format (e.g. a local cartesian coordinate system with an indeterminate origin), the CSP shall be able to either provide off-line means for this location to be converted to a standard geo-location, or provide the converted geo-location in one of the standard TS 33.128 formats in the same report.

**R6.3 – 276 Moving Cell Identifier** – The CSP shall indicate which kind of cell identifier is available in the User Location Information (ULI) in case of NTN or MBSR. A cell identifier is either an earth-fixed one, that cover continuously the same geographical areas all the time, either an earth-moving one.

**R6.3 - 277 Mapping of Moving Cell Identifier** – The CSP shall provide the related mapping of a moving cell identifier to geographical coordinates.

**R6.3 - 280 Location Senescence -** The CSP shall provide information that indicates when the location was determined (e.g. age of location, timestamp).

**R6.3 - 290 Trusted/Untrusted Location** - The location information reported to the LEMF shall be location information trusted by the 3GPP network (i.e. the location information is either 3GPP network derived or verified), if available. The CSP shall also be able to report target location information from untrusted sources (e.g. user provided) in addition to or in absence of the trusted location information.

**R6.3 - 300 Location Trust Indication -** The CSP shall be able to indicate to the LEA whether the location information is trusted or untrusted.

**R6.3 - 310 Projected Location -** The CSP shall be able to indicate to the LEA whether the location information of the target is measured or possible.

**R6.3 - 320 Non 3GPP access -** For non 3GPP access the CSP shall be able to provide the identity and location of the non 3GPP access function serving the UE as known by the CSP.

**R6.3 - 330 Roaming Location -** In the case of inbound roaming, the visited CSP that was served a warrant shall be able to provide location information without assistance from the home CSP.

**R6.3 - 340 Location Changes in the Visited Network -** In the case of roaming, the home CSP that was served a warrant shall be able to provide location information as visible in the home network.

**R6.3 - 350 Location Requests -** The home CSP shall be able to provide notification of target-related location information requests received from outside the home network when these requests are visible to the home network as part of normal network operations.

**R6.3 – 360 LCS Use** - The CSP shall be able to use LCS, if available, in support of LALS for an LCS-targetable UE (with or without target LCS subscription).

**R6.3 – 370 LALS Reporting** – The CSP shall be able to provide on-demand and periodic LALS reports of the target's location independent of the target's communication state.

**R6.3 - 380 Up-to-date LALS location** - LALS shall report either the current (updated) location, or if the current location is unavailable the last known location of a target's UE.

**R6.3 - 390 LALS failure notification** - If the location is unavailable, LALS shall be able to report a failure reason, as to why the location is unavailable.

**R6.3 - 400 Target specificity -** The CSP shall ensure no communications are intercepted other than those of, or associated with, the target's equipment, facilities or services.

**R6.3 - 410 Service specificity -** The CSP shall ensure that only the communication services specified by the warrant are intercepted.

**R6.3 – 420 Service Scope** - All CSP based services shall be in scope of LI including mission critical services and non-mission critical services.

**R6.3 - 430 Service Activation** - The CSP shall report service activation.

**R6.3 - 440 Service** **Invocation** - The CSP shall report service invocation.

**R6.3 - 450 Service Modification** - The CSP shall report service modifications (e.g., changes to content, content descriptors, timing descriptors, group participation, copy of service content).

**R6.3 - 460 Service Deactivation** - The CSP shall report service deactivation.

**R6.3 - 470 Service Up/Download** - The CSP shall report service related uploading or downloading.

**R6.3 - 480 Service Access Method** - The CSP shall report the access method used by the target to interact with the service (e.g., via ME, UE or web).

**R6.3 - 490 Early media** - The CSP shall be able to intercept early media (e.g., CAT, CRS).

**R6.3 - 500 Context Comprehensibility -** The CSP shall include in Interception Product information that allows the LEA to establish the Context of Communications.

**R6.3 - 510 Service Indication -** The CSP shall include in Interception Product an indication of the communication service as known by the CSP network.

**R6.3 - 520 Interdependency of IRI and CC -** The CSP shall ensure IRI containing CC metadata is delivered in a timely and accurate manner such that it shall be possible to decode CC in real time.

**R6.3 - 530 Reporting Post Session Established Digits** - The CSP shall support extracting and reporting dialled digits after the session is established (e.g. user dialled, signalled) via the CSP services, on a per-warrant basis.

**R6.3 - 540 Post Session Established Digit Reporting for IRI and CC Intercepts -** The CSP shall be able to support extracting and reporting digits after the session is established for IRI-only intercepts, as well as for intercepts that report both IRI and CC.

**R6.3 - 550 Toggle for Post Session Established Digit Extraction -** The CSP shall support the Post Session Established Digit Extraction capability with a toggle feature that can activate/deactivate this capability, per warrant.

**R6.3 - 560 Charging -** The 3GPP system shall be able to generate LI charging event records.

***R6.3 – 600  Location Verification for NTN*** *–* The CSP shall be able to verify the GNSS coordinated reported by the UE with the network.

***R6.3 – 700    Location Accuracy for NTN*** *-* The granularity of the network verified location information shall be at least comparable to terrestrial network ones.

\*\*\* End of Second Change \*\*\*

\*\*\* Third 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 (e.g. 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.

**R6.4 – 250 Delivery Of Location Dependent Interception (LDI) -** The CSP shall be able to suspend the delivery of LDI when the user moves outside the authorised area(s).

**R6.4 – 260 Delivery of Location Dependent Interception to different LEAs** -The CSP shall be able to deliver LDI to the requesting LEA, or to another agreed LEA, or be able to suspend LDI based on LEA requirements.

**R6.4 – 270 Delivery Based on Country Registration of a Target Device or Facility** - The CSP shall be able to enable or suspend the delivery of intercepted information based on the country of registration for a target device or facility.

**\*\*\* End of Third Change \*\*\***

**\*\*\* Start of Fourth Change \*\*\***

## 6.5 Lawful compliance

**R6.5 - 10 Interception Time Period -** The CSP shall ensure that Lawful Interception is performed only for the time period as specified in the warrant.

**R6.5 - 20 Interception Temporary Reduction -** The CSP shall be able to both suspend (e.g. when roaming outbound internationally) and resume all or a portion of the obligated Interception Product during the Interception Period.

**R6.5 - 30 LI Activation -** The CSP shall be able to notify the LEA of interception activation.

**R6.5 - 40 LI Changes -** The CSP shall be able to notify the LEA of changes related to interception (e.g., suspend or resume).

**R6.5 - 50 LI Deactivation -** The CSP shall be able to notify the LEA of interception deactivation.

**R6.5 - 60 Warrant correlation -** The CSP shall ensure all the Target Communications can be correlated with the warrant.

**R6.5 - 70 Recordkeeping -** The CSP shall create and implement a record retention policy such that it is able to document the handling of the intercepts.

**R6.5 - 80 Technological I****nvariance -** The CSP shall be able to comply with the LI requirements in the present document regardless of network implementation technology or architectural options.

**R6.5 - 90 Location Dependent Interception -** LDI principles are conditional and based on geographical aeras. The CSP shall be able within its service area to intercept the traffic usages of a specific target based on location, and/or extra context information such the country registration of a vessel within border(s), the subscription, or of extra territorial requirements (e.g. international maritime and aeronautical zones, or above other countries).

**R6.5 – 100 Location Dependent Interception Management -** When a target is in an area to be on monitored (i.e. aera declared as a LEA’s geographical authorized country(ies)), then CSP intercepts all the target traffic and send it to the applicable jurisdiction (warrant issueing) or to another agreed LEA than the requesting one. Other extra requirements may apply such as CSP’s own subscriber traffic selection or type of communications.

**R6.5 – 200 Location Dependent Interception Monitoring -** The CSP shall monitor permanently a target’s location during on-going communications or for any mobility management event detected in the core network which includes a target’s location change or update, in order to manage both the interception of the target communications and the delivery of them to the designated LEA.

**R6.5 - 300 Location for Non Terrestrial Network** - The CSP shall be able to locate each target in a verifiable, trusted, reliable and accurate manner in order to determine the policy and the nature of applied jurisdiction that applies based from location and/or context (e.g. flag of a vessel or an airplane).

**\*\*\* End of FourthChange \*\*\***

**\*\*\* End of Last Change \*\*\***