.

**3GPP TSG- Meeting # *s3i240059***

**, , -**

|  |
| --- |
| *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 Moving Base Station |
|  |  |
| ***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 Moving Base Station (such 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/Moving Base Station developments. |
|  |  |
| ***Clauses affected:*** | 3.1; 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 \*\*\*

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**activation/deactivation:** The large time scale action (i.e. on the same order as subscription lifetimes, that encompass multiple sessions, e.g. subscribing to “call hold” service) that turns on/off a service or feature for a user so that it is ready to act or will no longer be available to act. In the case of lawful interception, this may apply to all or a particular subset of communications. (See also Invocation).

**Artificial Intelligence:** Artificial Intelligence is typically considered to be a system that performs some form of reasoning, planning or object management, using knowledge as well as perceived information that, in the past, required human intervention. (Definition from ATIS-I-0000068, White Paper "Evolution to an Artifical Intelligence Enabled Network" [8]).

**capture:** The action taken by the CSP to separate and copy the communications associated with a target identifier.

**Content of Communication (CC):** Information exchanged between two or more users of a communications service, excluding intercept related information. This includes information which may, as part of some communications service, be stored by one user for subsequent retrieval by another.

**context of communication:** Information needed to recreate the state known in the CSP's network of the Target Communication. For example the direction of initiation on communication (to or from), direction of data flow (to or from), direction association with the identifiers to and from addresses), actions taken by the CSP on behalf of the target or identity translations.

**Communication Service Provider (CSP):** The entity that owns or operates the network that provides a service to a subscriber.

**delivery:** The action taken by the CSP to perform the necessary correlation and processing of communications associated with a target, and delivering the result to the LEA.

**de-provisioning:** The action taken by the CSP, that may be in response to an interception termination request from the LEA, or automatically once the warrant period has expired, to remove from its network functions the information and reporting pertaining to the target.

**detection:** The action taken by the CSP to identify communications associated with a target identifier.

**edge interception:** Interception performed in less secure locations that could be at customer's premises e.g. H(e)NB, ProSe relays.

**group identifier:** A group identity provides a reference to a defined group of one or more users. The use of this group identity applies to all users in the group.

**interception:** The actions of Provisioning, Detection, Capture, Delivery, and De-Provisioning.

**interception product:** The Intercept Related Information (IRI) and/or Content of Communication (CC) generated as a result of isolating the target**'**s communications or identities for the purpose of delivery to the requesting LEA.

**Intercept Related Information (IRI):** Information or data associated with communication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data, and location information.

**Interception Aera:** Geographical aera where Location Dependent Interception (LDI) applies. It is defined by agreement between LEA(s) and the CSP.

**invocation:** The short, intra-session time scale action (i.e. the application of the hold feature in the middle of a call session) in which a service or feature is called to act. In the case of lawful interception, this may apply to all or a particular subset of communications. (See also Activation).

**Lawful Access Location Services (LALS):** A service provided by a CSP to an LEA in which action is performed by a CSP to obtain a target's location information by means of Location Services (LCS), and to provide that information to an LEA.

**Lawful Interception (LI):** Actions taken by the CSP that include: provisioning the target identity in the network to enable isolation of target communications (separating it from other users' communications), duplicating the communications for the purpose of sending the copy to the LEA, and handing over the Interception Product to the LEA that served the CSP with the warrant. An interception is associated with exactly one warrant.

**lawful interception identifiers:** Target identifying details as defined in ETSI TS 103 280 [5].

**LI delivery latency:** The time between isolation in the Point of Interception and delivery of the Product of Interception at the LEA at the agreed point of handover.

**Location Dependent Interception:** The interception is dependent on the target location and/or extra context information such as the country of registration of a vessel (if available), or extra territorial requirements (e.g. international maritime and aeronautical zones) in order to let the CSP system to determine the applicable jurisdiction for interception.

**location information:** Information relating to the geographic/ physical or logical location of a target.

**Mediation and Delivery Function (MDF):** Functions that convert the CSP internal formats and protocols to the agreed formats and protocols for handover from the CSP to the LEA.

**Moving Cell:** A cell for which the general area of coverage is moving in relation to the surface of the earth. For example, such cell may be in a moving facility such a train, a boat or an airplane or be generated by in a satellite.

**party role:** The role of a user identifies whether the user was for example the initiating party or the addressed party or intermediate addressed party in a communication.

**production: The actions of Detection, Capture, and Delivery.**

**provisioning: The action taken by the CSP to insert into its network functions information that identifies the target and the specific communication services of interest to the LEA, sourced from the LEA provided warrant.**

**target communication:** All communications, communication attempts (successful or not), and network interactions that originate from, are directed to, are controlled by, or are associated with, the target's identifiers, equipment, facilities or services, including actions taken by the network on behalf of the target, that are available in the CSP's network.

**target identity:** A network or service identity that uniquely identifies a target for interception from all other non-targets within one or more CSP services. One target may have one or several target identities. The target identity can be a long term subscription based identity, a short term network identity, a public identity or an internal (private) identity.

**third party:** A resource or entity which is not fully owned and fully controlled by the CSP.

**warrant:** The formal mechanism to require Lawful Interception from an LEA served to the CSP on a specific target. Depending on jurisdiction also known as: intercept request, intercept order, lawful order, court order or judicial order (in association with supporting legislation).

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

\*\*\* Second 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

IA Interception Area

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

MBS Moving Base Station

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

UTC Coordinated Universal Time

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

\*\*\* Third 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~~, whatever the technology or network type used (terrestrial or non-terrestrial).~~

**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 Mobile Cell Identification** – The CSP shall be able to report when a cell is capable of ,moving and what type off facilities the cell is located in.

**R6.3 – 277 Cell Movement Identification** – The CSP shall be able to report when the coverage location of a mobile cell changes in near real time.

**R6.3 – 278 Mapping of Moving Cell** – The CSP shall be able to provide the geographical location of mobile cells at the time of reported events on a periodic basis or on demand by the LEA.

**R6.3 – 279 Location of a moving cell** - If a base station is located on board ~~in~~ a vessel the geographical location of the vessel will be reported. If a base station is located on board ~~in~~ a high altitude platform the geographical location of the center of the footprint of the cell will be reported in combination with an ~~size~~ indication of the footprint size.

**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 provided or verified), if available. The CSP shall also be able to report and to verify where possible by the network location information from untrusted sources (e.g user equipment provided).

**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 when connected via NTN.

**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 Third Change \*\*\*

\*\*\* 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, or crossing Interception Area boundary in case of LDI) 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 – 100 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.~~

**~~R6.5 – 200 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. The CSP shall monitor permanently a target’s location during on-going communications or for any mobility management event.~~

**R6.5 – 90 Location Dependent Interception Management -** The CSP shall be able to continuously monitor the target’s location during on-going communications or for any mobility management event and deliver interception product to the applicable jurisdiction when the target is in the Interception Area (IA). For Location Dependent Interception situations mutual legal assistance treaties might apply between LEAs.

**R6.5 – 100 Lawfull Interception Policy based on Location and Context –** The CSP shall be able to locate ~~permanently~~ each target in a trusted (verifiable, reliable) manner ~~with sufficient accuracy in order~~ to determine the policy based on jurisdiction requirements. The applicable ~~ed~~ policy ~~is~~ can be defined based on the UE location~~, Network based location~~ and context (e.g. flag of a vessel or an airplane).

**R6.5 – 200 Location in Non Terrestrial Network** - The CSP shall be able to obtain and report UE locations with similar granularity ~~accuracy~~ as with terrestrial networks.

**\*\*\* End of fourth Change \*\*\***

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