**3GPP SA3#94-LI *s3i240708***

**29 October-1 November 2024, Las Vegas(US)**

**Title: RCS lawful intercept requirements**

**Response to:**

**Release: Rel-19**

**Work Item: LI19**

**Source: SA3-LI**

**To: GSMA**

**Cc: SA3**

**Contact person:**

Name: Pierre Courbon

E-mail Address: pierre.courbon[@]finances.gouv.fr

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** None

# Overall description

SA3-LI understands that GSMA is specifying use of end-to-end encryption (E2EE) for a carrier grade solution(s) in its Rich Communication Services (RCS), that may have to take LI regulations into account. SA3-LI requests support from GSMA to enhance 3GPP SA3-LI specifications.

The main requirements on LI related to encryption are in 3GPP TS 33.126:

* **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 ongoing 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.

SA3-LI is kindly requesting GSMA to confirm how LI requirements above can be met when E2EE with the highest-level security is used on any communications.

Actions

**To GSMA:**

**ACTION:** SA3-LI kindly requests GSMA to liaise on LI requirements related to its E2EE in RCS (future specification) and to inform SA3-LI on related developments.

# 3 Dates of next SA3-LI meetings

SA3#96-LI 28 – 31 January 2025 Sophia Antipolis, France

SA3#97-LI 29 Apr – 02 May 2025 Washington DC, US