**3GPP SA3#94-LI *s3i240475***

**9-12 June 2024, Amsterdam, Netherlands (NL)**

**Title: Reply LS** **on enhancement to the protocol stack of IMS Data Channel**

**Response to:** **S4-241373 [LS on enhancement to the protocol stack of IMS Data Channel]**

**Release: Rel-18**

**Work Item: 5G\_MEDIA\_MTSI\_ext**

**Source: SA3-LI**

**To: SA4**

**Cc: SA3**

**Contact person:**

Name: Tyler Hawbaker

E-mail Address: thawbaker@fbi.gov

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

# 1 Overall description

SA3-LI thanks SA4 for the LS on enhancement to the protocol stack of IMS Data Channel. SA3-LI provides the following response:

**Question 1**: Would it be beneficial to be able to activate/deactivate IMS media plane encryption from lawful interception perspective?

**Answer 1**: The capability to activate/deactivate IMS media plane confidentiality protection is mandatory from a lawful interception perspective. In roaming cases, this disabling applies on a per roaming agreement basis, meaning that the entirety of the IMS traffic flow regardless of LI targeting is not confidentiality protected when the roaming agreement requires. Current S8/N9 Home routed roaming LI capabilities defined in TS 33.127/33.128 require media plane encryption [confidentiality protection] of IMS to be turned off due to the current IMS security architecture design limiting capability to provide hop-by-hop media protection. SA3-LI has responded to similar questions from GSMA NG/UPG (see LS out s3i240070, attached in this response) pointing to the continued requirement for IMS Data Channel.

From a general sense, SA3-LI maintains the requirement that, when present, media shall be delivered either in unencrypted format, or with the means and instructions to decrypt the encrypted media and communications related information. If current protocol stack design does not allow the latter, then the CSP shall have the means to disable such encryption.

For SA4’s awareness, it is also worth noting that there are additional LEA requirements in the case of non-roaming interoperability set up (e.g. agreement between CSP of two different countries) that may prohibit the use of media encryption between such CSPs (e.g. confidentiality protection controlled by the originating network) to enable LI in the terminating network.

SA3-LI has also concluded that while encryption includes both confidentiality and integrity protection, SA3-LI only requires confidentiality protection disabling mechanisms while preserving integrity protection.

# 2 Actions

**To SA4**

**ACTION:** SA3-LI kindly asks SA4 to take the answer into account when determining protocol stack enhancements.

# 3 Dates of next SA3-LI meetings

SA3#95-LI 29 October – 1 November 2024 Las Vegas, NV (US)

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