**3GPP TSG-SA3 Meeting #124 Draft\_S3-253806r3**

Wuhan, China, 13 – 17 October 2025 revision of 3449, 3516, 3575

**Title: (Draft) LS reply on LI requirements on IMS Data Channel**

**Response to: LS S3-253119/S2-2507657 on LI requirements on IMS Data Channel from SA2**

**Release: Rel18**

**Work Item: NG\_RTC\_SEC**

**Source: SA3**

**To: SA2, SA3-LI**

**Cc: SA4, CT1**

**Contact person: Jing Ping**

**Jing.ping@nokia-sbell.com**

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

**Attachments:** N/A

# 1 Overall description

SA3 thanks SA2 for the LS regarding LI requirements on IMS Data Channel.

SA3 would like to give feedback for below scenario:

1) Roaming cases with S8HR / N9HR model: SA2 would like to ask SA3 to study how the VPLMN decrypts the Data Channel content when any UE is in roaming state.

Feedback from SA3: The S8HR/N9HR are direct interfaces between a roaming UE and its HPLMN and LI Requirements on the S8HR/N9HR imply that these interfaces shall not be confidentiality protected. It is possible to VPLMN have access to a copy of the DC content without confidentiality protection by using DTLS1.2 in DC protocol stack and setting NULL cipher for DTLS1.2. However, it’s not recommended in security point of view because of following reasons:

* NULL cipher is not possible for DTLS1.3 and is not recommended in DTLS1.2.
* DTLS1.3 is recommended since Rel19.
* The downgrade security configuration is applied to all UEs of the HPLMN to avoid LI being detectable.
* Regulation such as Cyber Resilience Act (CRA) mandates that data in transit and storage by default should be encrypted using state-of -the-art mechanisms

2) Interoperability case between two CSPs, or in direct communications between two users P2P: When the MF acts as "HTTP Proxy", the P2A, P2A2P Data Channels are always terminated in the MF which can provide a copy of the IMS Data Channel content after decryption for LI. To support the LI requirements for P2P data channel, the serving IMS network can be configured to anchor the P2P Data Channel of the target UE or all UEs in the MF which acts as "DC Application Proxy". The MF can provide a copy of the IMS Data Channel content after decryption.

When the MF acts as a “UDP Proxy”, LI requirements cannot be fulfilled

Feedback from SA3:

SA3 would like to point out that according to TS 23.228 the “DC Application Proxy" is applicable only to the case that the network initiates the P2P session. SA3 would like to request for clarifications whether SA2 considers the "DC Application Proxy" to be applicable for fulfilling LI requirements for the UE initiated P2P.

3) Interoperability between two CSPs, in which one is using IMS Data Channel and the other is using IMS without any IMS Data Channel feature: If the target UE is using the IMS without any Data Channel, and interworking between the DCMTSI UE and MTSI UE (i.e., the LI target) for specific DC application is required (as specified in clause AC.7.9 of TS 23.228), the IMS data channel content from the DCMTSI UE is terminated in the MF or DC AS. The MF or DC AS may support the interworking with the MTSI UE via IMS video flow or other existing mechanism (e.g. SMS, HTTP via Internet DN. It is assumed that LI for such interworking scenarios (IMS video, SMS, Internet) with the MTSI UE is supported by existing specifications. SA2 has not identified any gaps in supporting LI for these scenarios.

Feedback from SA3: Since SA2 has not identified any gaps in supporting LI for these scenarios, SA3 will not explore them further.

SA3 kindly asks SA2, SA3-LI take the above answer for the scenario 1 into account and asks SA2 confirm question on the scenario 2.

# 2 Actions

**To SA2, SA3-LI**

**ACTION:** SA3 kindly asks SA2, SA3-LI take the above answer for scenario 1 into account and asks SA2 confirm question on the scenario 2.

# 3 Dates of next TSG SA WG 3 meetings

SA3#125 17 – 21 November 2025 Dallas, US

SA3#126 9 – 13 February 2026 India (TBD)