**3GPP SA3LI#85e-a *S3i220244***

**eMeeting, 25-29 April 2022**

Title: LS on Inter-PLMN Handover of VoLTE calls and idle mode mobility of IMS sessions

Response to:

Release: Release 18

Work Item:

Source: SA3LI

To: SA2, CT1

Cc: SA3, CT4

**Contact Person:**

Name: Koen Jaspers

E-mail Address: k.b.jaspers@minjenv.nl

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

Attachments: None

**1. Overall Description:**

Guidance – Include the document reference if this responds to an incoming LS.

Guidance – Inform clearly what is the oldest release for which this LS needs to be considered by the destination group(s)

Guidance – Inform clearly if the LS is only for information or ACTION [see 2. below]

SA3-LI has identified that the handover between PLMNs using home routing for ongoing IMS-sessions (calls) created issues for LI.

For home routing the regulators in general require the IMS-encryption to be switch off for roamers to allow lawful interception in the VPLMN without involvement of the HPLMN.

The assumption was that after roaming registration IMS-sessions would be started and full capture of an IMS-session was possible. The use of inter-PLMN handover will not provide full IMS-session information needed for effective lawful interception in the VPLMN. SA3-LI needs to make additional information to be available for an effective lawful interception.

This LS focusses on the VoLTE IMS roaming for both VoLTE/EPC and VoNR/5G Core. IMS for VoNR has not fully been specified yet. If IMS is specified for VoNR this home routing issue for inter-PLMN handover of IMS session needs also to captured as well.

The following list states the requirements related to inter PLMN handover of IMS-sessions:

1. There is a need to intercept an ongoing call of a user even if it is inbound roaming to a PLMN.

2. There needs to be a mechanism to ensure that the HPLMN can turn off IMS-encryption when a user roams to a VPLMN which requires it to be turned off. In addition the HPLMN might also require the IMS-encryption to be back on when a user is returning to the HPLMN.

3. It needs to be ensured that the VPLMN lawful interception system has access to the relevant identifiers to be able to perform lawful interception of IMS services as given in the stage 2 and stage 3 SH8R/N9HR details.

1. 3GPP access level identifiers (MSISDN, IMSI, IMEI).
2. IMS level identifiers (IMPU, IMPIs) of local served party and IMPU of remote end point user.
3. SDP information for media stream (Codec etc.).

4. The law enforcement monitoring facilities must be able to decode / interpret any intercepted media it receives after the inter-PLMN handover (as at any other time!).

5. The network needs to support the lawful interception system in the HPLMN detecting that a user has moved to different country (e.g. so that it can suspend interception if legally required). This may be applied to the content of the communication only or to signaling information and content.

6. The network needs to support the lawful interception system in the HPLMN detecting that a user has moved back to the HPLMN from different country (e.g. so that it can start interception if legally required).

7. The requirements 5 and 6 would need to apply in the case of non-terrestrial networks (NTNs) as well.

8. The VPLMN lawful interception system needs to be able to detect whether the HPLMN has correctly configured the IMS session (e.g. encryption off). Any action resulting from such detection is a CSP policy issue.

SA3-LI is looking forward to discuss the set of information that needs to be provided at inter PLMN handover and the most appropriate way to make the information available.

1. What changes are needed so the IMS can make the required information available.
2. What is the preferred mechanism to get the IMS-information provided to the VPLMN (e.g. as part of the registration process)?
3. Are changes needed for the HPLMN to be able to deactivate or activate the IMS-encryption during inter-PLMN handover?
4. Are changes needed for the VPLMN to detect if the correct configurations for roamers to allow lawful interception at the VPLMN?

Taking the regulatory, process and technical aspects into account offers to have dedicated Go 2 Meeting on this subject with some delegates from SA2 and CT1 (and if requested SA3 and CT4).

**2. Actions:**

**To CT WG1 and SA WG2 group.**

**ACTION:** SA3-LI asks CT WG1 and SA WG2 group to take the requirement in this LS into account.

 SA3-LI asks CT WG1 and SA WG2 group to if a G2M will be useful.

 SA3-LI asks CT WG1 and SA WG2 group to responses to the questions after the G2M if performed or directly if no G2M is needed.

Guidance – Provide clear information on what the other groups must do, and by when

**3. Date of Next SA3-LI Meetings:**

SA3#85-LI-e-b TBD July 2022 Electronic meeting

SA3#86-LI-b 30th August - 2nd September 2022 Sophia Antipolis, France

SA3#87-LI-e-a 3rd - 5th October 2022 Electronic meeting

SA2#87-LI-b 1st - 4th November 2022 US TBC