**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 17

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:**

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

With home routing roaming, PLMN operators are required to switch off the IMS-encryption for roamers in order to allow the lawful interception of roamers in the VPLMN without involvement of the HPLMN.

The assumption was that after roaming registration IMS-sessions would be started without IMS-encryption and full capture of an IMS-session was then possible. The use of inter-PLMN handover will not provide full IMS-session information needed for effective lawful interception in the new VPLMN. SA3-LI needs additional information to be made available for effective lawful interception.

The hitherto assumption SA3 LI had was that during the IMS registration, the IMS encryption would be turned off and as a consequence, a full capture of IMS session related signalling and media would be possible in the VPLMN for lawful interception purpose. When the inter-PLMN handover happens with an established IMS session for a roamer, without having the complete IMS session related information, an effective lawful interception of such roamers is not possible in the VPLMN. In order to have a non-compromised lawful interception in the VPLMN, complete information of IMS sessions shall be made available in the VPLMN.

This LS focusses on the Home Routed VoLTE IMS roaming for VoLTE/EPC but it is also applicable to VoNR/5G Core..

Even though the current SA3 LI finding focusses on the Home Routed VoLTE IMS roaming, note that the problem would also apply to VoNR IMS roaming.

The following list states the requirements related to inter PLMN handover and idle mode mobility 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.

Ongoing call interception of a user during handover even if that user becomes an inbound roamer to a PLMN shall be possible.

2. In order to support the above, a mechanism shall exist to ensure that the HPLMN can turn off IMS-encryption when a user roams to a VPLMN. In addition, the mechanism may be required to support turning on the IMS encryption when the user returns or roams back to the HPLMN.

3. The handover handling shall ensure that the VPLMN lawful interception system has access to the relevant identifiers to enable the lawful interception of IMS services of roamers. The relevant identifiers shall include at the minimum, the following:

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 (codec, PT, etc.) for the media stream.

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 a 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.

The HPLMN shall have a mechanism to detect that a user has roamed into a different country. The HPLMN may be required to suspend the lawful interception for outbound roaming. Such suspension, if executed, may include the suspension of lawful interception for the content of communications or the suspension of lawful interception of content of communication and the signaling.

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).

When the HPLMN is required to suspend lawful interception for outbound roamers, the HPLMN shall have the mechanism to detect that the user has moved back to the country in order to start the lawful interception of that user when required.

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

8. The lawful interception system in the VPLMN shall 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 detailed list of information that needs to be provided at inter PLMN handover/idle mode mobility and the most appropriate way to make the information available. For example:

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 are in use at the VPLMN?

Taking the regulatory process and technical aspects into account SA3-LI offers to have dedicated Go To Meeting based discussion 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 kindly asks CT WG1 and SA WG2 group to take the requirement in this LS into account.

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

 SA3-LI kindly asks CT WG1 and SA WG2 group to respond to the above questions (either after the G2M if performed or directly if no G2M is needed).

 SA3-LI kindly asks CT WG1 and SA WG2 group to provide their preferred solution(s) to the requirements (either after the G2M if performed or directly if no G2M is needed).

**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