**3GPP SA WG2 Meeting #151E S2-2204643**

**Elbonia, May 16 - 20, 2022 (was S2-220xxxx)**

**Source: Nokia, Nokia Shanghai Bell**

**Title:** **Discussion on the SA3LI LS on Inter-PLMN Handover of VoLTE calls and idle mode mobility of IMS sessions**

**Document for: Discussion**

**Agenda item: 4.1**

**Work Item / Release:**

*Abstract of the contribution: This paper discusses the LS from SA3LI on inter-PLMN VoLTE HO, potential technical implications and proposes a way forward.*

# 1. Background

SA3LI has sent LS S3i220244 on Inter-PLMN Handover of VoLTE/VoNR calls and idle mode mobility of IMS sessions to SA2 and CT1 (Cc to SA3 and CT4). The LS discusses the use case where an IMS user roams into a VPLMN (e.g., from the HPLMN), S8HR/N9HR roaming architecture is used, the UE is registered at the home IMS or has even an ongoing call (i.e., inter-PLMN handover happens for the ongoing call) and the VPLMN requires de-activation of IMS confidentiality protection while in the serving PLMN (HPLMN) confidentiality protection is active. In the same way it should be possible to activate confidentiality protection if the user moves to a PLMN (e.g., moves from VPLMN to HPLMN) requiring confidentiality. In addition to de-activation or activation of confidentiality protection, the VPLMN also requires information about user identities and other call related data.

The LS is listing a number of requirements related to inter PLMN handover and idle mode mobility of IMS-sessions that need to be fulfilled for an effective interception of inbound roamers:

1. For any ongoing call, following handover, it must be possible to intercept that S8HR call in the new PLMN.

2. In order to support the above, a mechanism shall exist to ensure that the HPLMN can turn off IMS confidentiality protection when any UE roams to a VPLMN. In addition, a mechanism may be required to support turning on the IMS confidentiality protection when the UE 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 HPLMN shall have a mechanism to detect that a user has roamed into and back from a different country.

1. The HPLMN may be required to suspend the lawful interception for any targeted outbound roamer (including NTNs). 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.

b) When the HPLMN is required to suspend lawful interception for any targeted outbound roamer, the HPLMN shall have the mechanism to detect that the UE has moved back to the home country in order to start/resume the lawful interception of that UE when required.

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

Turning-off IMS confidentiality protection when a UE moves into a VPLMN requires the IMS in HPLMN

 a) to be aware of the PLMN change (addressing bullet 4 above),

 b) based on local policies trigger a re-REGISTER from the UE,

 c) during re-registration indicate to the UE that NULL scheme encryption shall be used,

 d) tear-down old Security Associations (SAs) and take new ones with no encryption in use.

For a) existing mechanisms can be re-used, namely that P-CSCF subscribes to PLMN\_change (see TS 29.214) and PCRF/PCF inform P-CSCF via Rx about the new PLMN ID based on information received from SMF/PGW via Gx/N7. This needs to be performed for all UEs of the HPLMN roaming into a different PLMN. It needs to be checked whether this existing procedure is fully applicable for the use case or some (minor) changes are required. For example, currently the procedure is only invoked when the UE performs initial REGISTER, and it is used to report the PLMN ID but not really to notify about PLMN changes.

For b) the S-CSCF must be informed by the P-CSCF about the PLMN change. This can be done by sending a SIP MESSAGE from P-CSCF to S-CSCF. This message is currently sent from P-CSCF to AS but needs now also be possibly sent from P-CSCF to S-CSCF. When receiving the SIP MESSAGE, the S-CSCF triggers a re-authentication per existing procedure in TS 24.229, 5.4.1.6 by sending a SIP NOTIFY (reg-event) to the UE. Alternatively, the UE can also send a re-REGISTER once it is aware of the PLMN change (such behavior might have UE impact). In any case, based on internal policies, the network might need to de-register the UE.

For c) the UE sends a re-REGISTER and the S-CSCF indicates to the UE in the response to the re-REGISTER the new encryption algorithm, which is NULL scheme, to turn-off confidentiality protection. If the UE has not indicated support of NULL scheme in the re-REGISTER, the registration will fail. As a side note, the HPLMN must also be able to determine whether or not turn off the confidentiality protection when a PLMN change happens. For example, when national regulations do not require a PLMN to intercept voice services of inbound roamers.

For d) both UE and P-CSCF shall start using the new set of IPSec SAs (without encryption) once they are established for any SIP communication and tear-down the existing set of IPSec SAs once their lifetime has expired.

Turning-on IMS confidentiality protection again when the UE moves back from the VPLMN to the HPLMN (or another PLMN requiring confidentiality) follows the same steps as indicated before but with selecting a security algorithm unequal to NULL in step c.

This procedure would work independently whether the UE is within a SIP session or not. However, for an ongoing session fulfilling requirement 3 in the SA3LI LS, it is not sufficient to just turn off IMS confidentiality as described. The VPLMN is lacking access to IMS level identifiers (IMPU, IMPI) or SDP information (used codec) associated with the call as the next SIP message within the session may not be required to carry such information. Also, it is possible that no SIP signalling messages are exchanged except the BYE. Even if the UE sends a re-INVITE or the network sends a re-INVITE to trigger SDP offer/answer, it needs to be ensured that the same identifiers and SDP information is available as for the original INVITE. As per current procedures, the re-INVITE usually will not carry all the session identities required for LI. Therefore, stage 3 needs to analysis possible implications of such in-call scenarios and make necessary changes to specifications. Significant impacts to network and UE are very likely and it is even not clear at this point whether a suitable solution fulfilling all LI requirements can be found.

Another aspect that needs to be considered is the potential use of media plane security between UE and P-CSCF/IMS-ALG. If media plane security is in use, it might be needed to implement mechanisms allowing to switch it off or on in the serving PLMN.

# 2. Conclusion

Based on the analysis above we conclude that making the home IMS in S8HR scenarios aware of a PLMN change and based on the PLMN ID turning off or on IMS confidentiality protection can be implemented with rather minor changes in the network and most probably no changes in the UE. This works also when the UE is in the middle of a session. Changes may be doable as Cat-F CRs to Rel-17 specifications.

However, providing IMS identifiers and SDP information related to an ongoing session to the VPLMN has significant impact to the network and UE. From our point of view these impacts need to be carefully studied in the context of a new work item in close coordination with CT WGs and SA3, triggered by service requirements defined by SA1 (which excludes a solution in Rel-17). Therefore, until a mechanism is discovered to transport the IMS identifiers in SIP messages for ongoing IMS sessions, the mid-call interception of an established IMS session in the VPLMN may not be possible.