**3GPP TSG-CT WG4 Meeting #101-bis-eC4-210198**

**E-meeting, 25th January – 29th January 2021**

Title: [Draft]LS on Identification of source PLMN-ID in SBA

Release: Rel-17

Work Item: SBIProtoc17

Source: CT4

To: SA3, GSMA 5GJA

Cc:

**Contact Person:**

Name: Jesus de Gregorio

Tel. Number: +34646004863

E-mail Address: jesus.de.gregorio@ericsson.com

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

Attachments: -

**1. Overall Description:**

During CT4#101e and CT4#101e-bis meetings, CT4 has discussed mechanisms to allow an NF Service Producer (NFp) to be able to receive information about the source PLMN of incoming SBA messages, in inter-PLMN scenarios.

It is CT4's understanding, based on the normative requirements stated in TS 33.501, that the pSEPP (i.e. the SEPP placed in the PLMN of the NFp) is assumed to have enough information to verify that a given incoming message from a remote PLMN contains valid PLMN-ID information in the received messages. As indicated in clause 13.2.4.8 of TS 33.501:

"The pSEPP further verifies that the PLMN-ID contained in the message is equal to the "Remote PLMN-ID" in the related N32-f context."

CT4 has observed that the PLMN-ID information in the N32-f context is obtained from the list of PLMN-IDs signalled by the SEPP in the PLMN of the NF Service Consumer (cSEPP) during the N32-c connection setup. (Note that this is only true from Rel-16 onwards, and that in Rel-15 the pSEPP does not have such PLMN-ID information; instead, it only has the domain name in the TLS certificate presented by the cSEPP).

During these discussions held in CT4, several scenarios have been brought up by some companies, where CT4 could not conclude on whether they are supported by 3GPP, and whether the assumption above (in which the pSEPP verifies the PMLN-ID information) can always be fulfilled.

These scenarios are:

1. One cSEPP serves a given PLMN, and such PLMN has multiple PLMN-IDs. It is not clear whether the same N32-c connection is used for all possible PLMN-IDs, or whether a separate N32-c connection is used for each PLMN-ID.
2. One cSEPP serves multiple PLMNs, each one with its own PLMN-ID(s). This scenario was called "SEPP Hub" by operators. It was questioned how the trust model applies to this case, and whether a SEPP outsourced to, say, an IPX provider can still be considered trusted or not, and the implications of that.
3. A scenario in which there may be further SEPPs, not only the cSEPP and pSEPP, but also potentially "intermediate SEPPs". This was called as "chained SEPPs". This applies to use case when the NFc and the NFp are located in PLMNs that are not immediately adjacent, i.e. if the message from NFc has to traverse more than one PLMNs to reach NFp.

Some companies in CT4 believed that the current 3GPP security architecture defined by SA3 does not fully support these models (in particular, scenarios 2 and 3 above), but there was no consensus. CT4 would highly appreciate feedback from SA3 with regards to these scenarios.

Another point worth mentioning concerns the scenario when OAuth2 is deployed. CT4 discussed whether the usage and presence of Oauth2 access tokens (potentially including a claim with the PLMN-ID of the requesting NF Service Consumer) could be of any help. CT4 observed that the access token is generated by the Home NRF (in the PLMN of the NFp) based simply on the information provided on the JSON request body of the AccessTokenRequest message sent by the Visited NRF (in the PLMN of the NFc). So, again, it is unclear how the pSEPP could verify that the "source PLMN" information received in such message is valid and correct (in particular, in those cases where a cSEPP may serve multiple PLMN-IDs).

**2. Actions:**

**To SA3, GSMA 5GJA groups.**

**ACTION:** CT4 kindly requests SA3 and GSMA 5GJA to provide feedback on the validity of the above scenarios, and whether SA3 believes that the current frozen releases (Rel-15 and Rel-16) can support them. Also, in case any of those scenarios is considered as not currently supported, CT4 would appreciate any indication on whether SA3 has plans to cover any of them in a further release.

**3. Date of Next CT4 Meetings:**

3GPP TSG CT4#102e 02/2021 E-Meeting