**3GPP TSG-CT WG4 Meeting #111-eC4-224xxx**

**E-Meeting, 18th – 26th August 2022**

Title: Reply LS on PLMN ID used in Roaming Scenarios

Response to: LS (S3-221214) on PLMN ID used in Roaming Scenarios from SA3

Release: Rel-17

Source: CT4

To: SA3

Cc: SA2

**Contact Person:**

Name: Bruno Landais

Tel. Number:

E-mail Address: bruno.landais@nokia.com

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

Attachments: 29.500 CR on Asserted Source Network ID

**1. Overall Description:**

CT4 thanks SA3 for their LS on PLMN ID used in Roaming Scenarios (S3-221214).

CT4 has agreed the following principles regarding the insertion of the 3gpp-Sbi-Asserted-Network-Id header in requests sent towards a target PLMN:

1. A Rel-17 5GC NF (NFc and NFp) originating an HTTP request shall insert the header.

1. For legacy NFs or cSEPP:
	* a Rel-17 SCP, cSEPP and pSEPP shall insert the header if the HTTP request message does not include the header and the SCP, cSEPP and pSEPP can determine the PLMN ID of the source PLMN.
	* For a source PLMN supporting multiple PLMN IDs, it is a deployment issue how the cSEPP determines the source PLMN ID. See example solutions below.
	* It is a deployment issue how the pSEPP determines the source PLMN ID to insert towards the target NF, if the incoming message to the pSEPP does not include the header and the source PLMN ID cannot be uniquely determined. See example solutions below.

Regarding the editor's notes asked by SA3:

1st editor's note:

*The context is related to the case of one operator having support for multiple PLMN-IDs. In roaming scenarios where one SEPP serves a given PLMN, and such PLMN has multiple PLMN-IDs, and uses the same N32 connection for all PLMN-IDs, the editor's notes from S3-221213 still need to be addressed:*

*"Editor's Note: It is FFS what should be the asserted PLMN-ID if the NF has not included the PLMN-ID header and the SEPP serves multiple PLMN-IDs."*

CT4 answer:

cSEPP may determine the source PLMN ID e.g. using the following approaches:

1. cSEPP may derive the source PLMN ID from the PLMN ID indicated in the TLS certificate (if present in the TLS certificate) received from the sending NF (with direction communication between the sending NF and cSEPP).
2. When using indirect communication between the sending NF and cSEPP, the SCP in the source PLMN may derive the source PLMN ID from the PLMN ID indicated in the TLS certificate received from the sending NF (if present in the TLS certificate) and insert the header in the outgoing HTTP request it sends towards cSEPP.

Alternatively, in network deployments where a different SCP would be deployed per PLMN ID, and where a sending NF supporting a certain PLMN ID only interacts with an SCP supporting the same PLMN ID, the SCP may insert the PLMN ID it is serving in the outgoing HTTP request towards the sending SEPP.

1. cSEPP may derive the source PLMN ID from topological network information (e.g. source IP address of the incoming HTTP request);
2. If cSEPP cannot determine the source PLMN ID, cSEPP may be configured to insert one default PLMN ID. In this case, if the request message body carries a PLMN ID, then the default PLMN ID may not be the same.
3. A different cSEPP may be deployed per source PLMN ID. Each cSEPP advertises one source PLMN ID to pSEPP per N32 connection. The sending NF or SCP discovers and selects the cSEPP based on the source PLMN ID of the HTTP request.

Likewise, the pSEPP can determine the source PLMN ID to insert in the header (if none is received in the HTTP request) e.g. using the following approaches:

1. using the PLMN ID received in the TLS certificate received from the cSEPP, or locally configured in pSEPP, or received from cSEPP in the N32-c handshake request;
2. If pSEPP cannot determine the specific source PLMN ID to insert, for an N32 connection supporting multiple source PLMN IDs (of a given PLMN), pSEPP may be configured per operator policies to insert one default source PLMN ID (of that PLMN). In this case, if the request message body carries a PLMN ID, then the default PLMN ID may not be the same.

2nd editor's note:

*"Editor's Note: It is FFS which PLMN ID an NF will include in case the NF serves multiple PLMN IDs."*

CT4 answer:

1. The sending NF should include the PLMN ID on behalf of which the HTTP request is sent.

For instance, an AMF or SMF that supports multiple PLMN IDs should indicate the serving core network operator PLMN ID, i.e. the PLMN ID signaled by the AMF to the SMF in the servingNetwork IE (see TS 29.502).

CT4 would also like to point out that it has renamed the 3gpp-Sbi-Asserted-Plmn-Id header to 3gpp-Sbi-Asserted-Source-Network-Id and extended its ABNF definition to enable encoding a source PLMN ID or SNPN ID, since CT4 expects this header to apply more generally to all N32 scenarios (not limited to roaming scenarios) and N32 can also be used between an SNPN and another SNPN or PLMN (e.g. see clause 5.30.2.9.3 of TS 23.501 on Credentials Holder using AUSF and UDM for primary authentication and authorization).

CT4 has agreed the attached 29.500 CR on Asserted Source Network ID.

**2. Actions:**

**To SA3 group.**

**ACTION:** CT4 kindly asks SA3 to take the above information into account and to finalize the 33.501 CR (draftCR S3-221213).

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

3GPP TSG CT4#112e 10/2022 E-Meeting