**3GPP TSG-SA3 Meeting #117 *S3-24xxxx***

Maastricht, Netherlands, 19th - 23th August 2024

**Title: LS on aggregation and other N32 topics in the context of mediated roaming**

**Response to: LS S3-242364 on the introduction of the domain "ipxnetwork.org" from GSMA 5GMRR**

**Release: Rel-18**

**Work Item: <work\_item\_name> (<work-item\_code>)**

**Source:** **<current\_meeting\_identity>**

**To: GSMA 5GMRR**

**Cc: CT4**

**Contact person: Andreas Pashalidis**

 **Andreas.pashalidis AT bsi.bund.de**

 **<phone\_of\_tdoc\_requestor>**

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

**Attachments:** DocNumber(s) [Description e.g.. Draft TS 29.414 v0.1.0].
**!! WARNING !!** Do not insert the file directly as an object in this Word document.

# 1 Overall description

SA3 thanks GSMA 5GMRR for their LS reply (S3-242364) on the introduction of the domain ipxnetwork.org, and would like to provide the following responses and clarifications.

"*In the context of N32-s and N32-p, but also in the context of N32-f as specified in 3GPP, from the perspective of Roaming Intermediaries it is desirable to use “aggregation”, i.e. to carry the signalling for multiple roaming relations (i.e. multiple pairs of roaming partners) over a single TLS connection.*

*While such aggregation appears to be impossible over N32-c and N32-f/TLS, it remains somewhat unclear whether it is conformant with N32-f/PRINS as specified in 3GPP.*"

Clarification: In order to maintain the possibility of trust anchoring with high granularity as well as better isolation of signalling traffic flows, SA3 discourages the use of aggregation. Despite this, the specifications do not forbid aggregation in the context of PRINS. More specifically, according to Note 3 of clause 5.9.3.2 of TS 33.501, if a given PLMN uses a Roaming Hub (RH) for the purposes of roaming with multiple other PLMNs, then a single TLS connection between the PLMN's SEPP and the RH can be used for carrying N32-f PRINS signalling for some or all the other PLMNs.

"*If PLMN IDs must be included in leaf certificates, then a potentially large number of PLMN IDs would need to be included in the TLS certificate in the context of aggregation, undermining the purpose of trust anchoring with the granularity of single PLMNs. More precisely, if the PLMN IDs are required in the leaf certificate used for N32-f/PRINS, then all the PLMN IDs of all roaming partners reachable through a given N32-f TLS (PRINS) connection appear in the certificate SAN fields. In situations with a chain of two Roaming Intermediaries this may include PLMN IDs of roaming partners that are not a customer of the given Roaming Intermediary, but a customer of the other Roaming Intermediary in the chain. Moreover, because N32-c is established E2Es it will only contain the PLMN IDs of a single roaming partner while the N32-fTLS (PRINS) certificate would contain the PLMN IDs of all roaming partners served through the Intermediary.*"

Clarification: Trust anchoring for the TLS connection for N32-f/PRINS is currently outside the scope of 3GPP specifications. However, SA3 believes that PLMN-ID based trust anchoring as specified for N32-c in TS 33.501 and tested according to clause 4.2.5 of TS 33.517 can be used for N32-f/PRINS, even under the circumstances described above. Firstly, if PLMN-IDs are encoded as (sub-)subdomains within a roaming intermediary's SAN entries, for example as in mnc001.mcc001.example.ipxnetwork.org, then PLMN-ID based trust anchoring can be applied in a consistent manner across all connections, as the requirement that any given PLMN-ID can appear in at most one trust anchor can be upheld (since the mapping using the certificate will work). This prevents situations in which multiple intermediaries are configured to be trusted as TLS endpoints (for PRINS) of any given roaming partner. (This would be an insecure configuration under the assumption that, for any given mediated roaming relation, there exists one specific "next-hop" intermediary that serves that relation.) Secondly, a form of "privilege escalation" is prevented, whereby signalling for superfluous PLMNs is added to the N32-f flow; cross-checks can be defined to ensure consistency between representing PLMN-IDs as per certificate and individual signalling messages. Such cross-checks would complement the check that each received N32-f message belongs to some N32-f context previously established via N32-c. Thirdly, it remains unclear why encoding PLMN-IDs as (sub-)subdomains of "ipxnetwork.org" in intermediary certificates appears to be undesirable. Within the context of an appropriate Certificate Practice Statement, SA3 does not see an issue with this, even though intermediaries have not been assigned themselves such IDs, and even if the encoded PLMN-ID is not a direct customer of a given intermediary. Instead, SA3 believes that such encoding would increase transparency of roaming relation management and hence enables better security controls both at roaming intermediaries and PLMNs. Fourthly, encoding PLMN-IDs into TLS certificates for N32-f/PRINS enables PLMNs to use a common trust anchor resolution for N32-c, N32-f/TLS and for N32-f/PRINS (although SA3 does not recommend this in the context of aggregation).

"*5GMRR also informs 3GPP that there exists a trusted relationship with non-PLMN entities in the mobile ecosystem,(e.g. Roaming intermediaries, RVAS providers,…). These entities have not been assigned any PLMN IDs by a regulatory body.*"

Clarification: SA3 is aware that a trusted relationship exists between PLMN and roaming intermediaries. The role of intermediaries is, however, separated from that of PLMNs, without any of the two roles being more trusted than the other. For example, clause 4.2.2.2 of TS 33.517 requires that IPX provider's keys are not accepted for N32-c, and that PLMN keys are not accepted for JSON patch signature verification.

"*For the PRINS security mechanism PLMN IDs* ***are******not*** *required in the leaf certificates used by the Roaming Intermediary to set up the TLS connections for N32-f/PRINS. In this case, 3GPP is asked to explain how the security threats are mitigated for N32-f TLS connections with the Roaming intermediaries, and how the responding SEPP would decide whether an incoming TLS connection is for N32-c (and therefore trust anchor selection according to PLMN ID is applicable) or for N32-f (and therefore it is not applicable).*"

Clarification: As explained above, while SA3 recommends to encode PLMN-IDs as (sub-)subdomains of "ipxnetwork.org" in order to increase transparency of roaming relation management and enable PLMN-ID-based trust anchor resolution, this is currently outside the scope of 3GPP specifications. If PLMN-ID based trust anchor resolution is not applicable for N32-f/PRINS, then a SEPP can listen to TLS for PRINS on a dedicated port and signal this using the senderN32fPortList (if initiating) or senderN32fPort (if responding) information element of the SecNegoatiateReqData or SecNegoatiateRspData structure, respectively (see clause 6.1.5 of TS 29.573).

"*Alternatively, for the PRINS security mechanism PLMN IDs* ***are*** *required in the leaf certificates used by the Roaming Intermediary to set up the TLS connections for N32-f/PRINS. And which PLMN IDs need to be added to the leaf certificates used by the Roaming Intermediary.*"

Clarification: As explained above, while currently outside the scope of 3GPP specifications, SA3 recommends to encode PLMN-IDs of all the PLMN IDs of all roaming partners reachable through a given N32-f TLS (PRINS) connection.

"*5GMRR would like to inform 3GPP that it specified a variant of the N32 interface stipulating that Roaming Intermediaries operate SEPPs rather than PRINS proxies. In this variant, there may exist more than two SEPPs in a chain between two roaming partners, and there is no Application Layer Security as in PRINS; as security associations fully terminate at each SEPP, this represents a hop-by-hop security approach. In this variant, the communication leg between a PLMN and a Roaming Intermediary uses the GSMA-defined "N32-s" variant of N32, and the communication leg between two Roaming Intermediaries uses the GSMA-defined “N32-p” variant of N32.*

[…]

 *Provide any feedback on how to handle the coexistence of N32-c/N32-f as specified in 3GPP, and N32-s/N32-p as specified in GSMA 5GMRR and outlined above.*"

SA3 thanks GSMA 5GMRR for informing on this development. While SA3 understands that deploying and maintaining a hop-by-hop security solution may appear to be more cost-effective than one where ALS mechanisms provide attributability to PLMNs and roaming intermediaries alike, the reasons behind this development remain unclear. This is because SA3 believes that the security properties provided by PRINS, notably the possibility to attribute message content to their originators, is representative of current state of the art and therefore, in the medium to long-term, fosters trust in the industry as a whole. SA3 also believes that the lack of ALS represents a structural weakness that is bound to be exploited.

SA3 welcomes technical contributions and active participation in 3GPP meetings from GSMA members that aim to address the remaining technical obstacles, if any, of the currently specified solutions for N32 with ALS. While SA3 currently does not see the need to take specific actions in order to handle the coexistence GSMA-defined N32-s and N32-p alongside with 3GPP specifications, it is grateful for being kept informed about developments in this area.

# 2 Actions

**To GSMA 5GMRR:**

**ACTION:** SA3 kindly asks GSMA 5GMRR to take into account the above clarifications and feedback.

# 3 Dates of next TSG SA WG 3 meetings

SA3#118 14 - 18 October 2024 TBD (India)

SA3#119 2025 TBD