

Liaison Statement to 3GPP SA1



| | | |
|-----------------------|-------------------------------|-------------|
| Document Title | Liaison Statement to 3GPP SA1 | Page 1 of 2 |
|-----------------------|-------------------------------|-------------|

| | | | |
|---------------------------|---|---------------------|----------|
| Date | 4-October-2022 | Meeting Time | 8:00 PDT |
| WG / Project | WBA OpenRoaming Technical Standards Task Group | | |
| To | 3GPP SA1 | | |
| Project chaired by | Mark Grayson (Cisco), Betty Cockrell (Single Digits), Necati Canpolat (Intel) | | |
| Topic | Facilitating interconnect between SNPNs and Credentials Holder | | |
| Action ID Prefix | N/A | | |

Dear 3GPP SA1

In July 2022, WBA Liaised with 3GPP SA, SA3 and CT6 concerning aspects that may result in lowering the barriers to adoption of SNPN type systems ([SP-220730](#)). Four issues were raised in the original LS, two issues relating to operating the N32 reference point between SNPN and Credentials Holder (CH) and two issues relating to the management of credentials. Whereas 3GPP CT6 and 3GPP SA have responded to the issues related to credential management (e.g., [C6-220475](#)), 3GPP SA concluded ([SP-220985](#)) that the most appropriate way for initiating work in 3GPP to address the other issues highlighted is via the SA1 work group.

The issues related to operation of the N32 reference point have been identified by WBA as a result of its operation of a cloud-based federation designed to facilitate the interworking between non-public Wi-Fi networks and different credential holders. Within its first full year of operation, this federation has attracted over 1 million non-public networks to join the federation.

However, WBA also notes that similar use cases have been identified by 5G ACIA in its white paper on “5G Non-Public Networks for Industrial Scenarios” (https://5g-acia.org/wp-content/uploads/5G-ACIA_5G_Non-Public_Networks_for_Industrial_Scenarios_09-2021.pdf). In the paper, 5G ACIA describe deployment scenarios where there is a communication path between the SNPN and a PLMN protected by a firewall. 5G ACIA scenarios include the use of the firewall protected communication path to enable the SNPN operator to support “roaming” (interworking) agreements with one or more PLMNs.

The following considerations apply to existing 3GPP specifications with N32 reference point:

- 3GPP has re-used the N32 reference point to support interconnect between SNPN and CH, where the CH service can be provided by a private enterprise or be offered as a service by a PLMN.
- Business objectives of enterprises deploying SNPN may require interconnect to multiple different CHs.
- The N32 reference point has been designed to support inter-PLMN traffic.
- Today's PLMNs have a centralized database of IP addresses of all operator nodes that connect to the inter-PLMN IP backbone network, including Security Edge Protection Proxies. This information is used for firewall and border gateway configuration to enable operation of N32 reference points, as defined by GSMA.

Accordingly, WBA would like to draw 3GPP SA1's attention to the following issues as they relate to the deployment of interconnection between SNPN and Credentials Holder.

| | | | |
|-----------------|-------------------------------|-------------------|----------------|
| Filename | Liaison Statement to 3GPP SA1 | Version | 1.0 |
| Status | Final | Revised On | 4 October 2022 |

Liaison Statement to 3GPP SA1



| | | |
|-----------------------|-------------------------------|-------------|
| Document Title | Liaison Statement to 3GPP SA1 | Page 2 of 2 |
|-----------------------|-------------------------------|-------------|

- There may be SNPN and CH deployments where IP address information of endpoints is not available in advance of signalling establishment, e.g., 1) where the SNPN is operated behind a NAT, 2) where a CH instance is operated using a cloud provider using dynamic IP address assignment, or 3) where the interconnect is delivered as part of a third party defined confederation which does not operate a centralized database of IP addresses.
- Infosec policies of the enterprise operating the SNPN may prohibit accepting inbound socket connections from unknown IP addresses.

Given the unique attributes of SNPN and CH deployments, e.g., compared with conventional inter-PLMN signalling, the WBA OpenRoaming group kindly asks SA1 to consider defining service requirements for facilitating interconnect between SNPN and CH in particular, taking into account issues as described in the bullets above.

Proposed Action to 3GPP SA1

- WBA kindly asks 3GPP SA1 to consider defining, in the release 19 timeframe, service requirements for facilitating interconnect between SNPN and CH, in particular, considering the issues described above.

Thank you in advance and for any additional information please contact WBA PMO (pmo@wballiance.com).

The WBA OpenRoaming Technical Standards TG Chairs

Next WBA F2F Meetings:

- 17 – 20 October 2022, Amsterdam
- 31 January to February 2 2023, Singapore

| | | | |
|-----------------|-------------------------------|-------------------|----------------|
| Filename | Liaison Statement to 3GPP SA1 | Version | 1.0 |
| Status | Final | Revised On | 4 October 2022 |