**3GPP TSG-SA3 Meeting #123 *S3-25xxxx***

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Cisco Systems**

**Title: Discussion of enhancements for SNPN cellular hotspots**

**Document for: Discussion**

**Agenda Item: Conference Calls on inputs to 6G study and SID preparation**

# 1 Decision/action requested

***It is proposed to endorse the proposal of this discussion paper.***

# 2 References

[1] 3GPP LS S3-221740: "Facilitating roaming adoption across 3GPP NPN deployments".

[2] 3GPP TS 23.501, "System Architecture for 5G System; Stage 2"

[3] 3GPP TS 22.261, "Service requirements for the 5G system; Stage 1"

[4] 3GPP TS 33.310, "Network Domain Security (NDS), Authentication Framework (AF)".

# 3 Rationale

SA3 received an LS from the Wireless Broadband Alliance [1] on "Facilitating roaming adoption across 3GPP NPN deployments". Wireless Broadband Alliance specifies and operates OpenRoaming. OpenRoaming is a cloud federation–based framework that opens Wi-Fi roaming to a broad community of Identity Providers (IdPs) and Access Network Providers (ANPs). Figure 1 shows the high-level architecture. The OpenRoaming federation was established by the Wireless Broadband Alliance in 2020 as an industry solution to enable scalable, seamless, and secure authentication between user devices provisioned with OpenRoaming profiles and their Identity Providers (IdPs), who manage the user's credentials while those user's devices are roaming onto the access networks of organizations that have joined the federation. OpenRoaming defined a legal framework within which the federation operates, a technical framework that covers the automatic establishment of secured signaling between ANPs and IdPs, federation-wide automatic network selection, and closed access group-based policy enforcement implemented by ANPs and IdPs.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 1: OpenRoaming architecture (source: WBA Website)

SA plenary advised that the most appropriate way for initiating related work in 3GPP is via SA1. This resulted in Study on Interconnect of SNPN (FS\_ISN) in SA1, which led to the specification of the following requirements to support Stand-alone Non-Public Network (SNPN) cellular hotspots [3]:

- R1: Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to be able to interconnect with a large number of SNPN Credential Providers with which the SNPN might not have preconfigured information detailing the IP addresses used by these SNPN Credential Providers to interconnect with the SNPN.

- R2: Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN Credential Provider to be able to interconnect with a large number of SNPNs with which the SNPN Credential Provider might not have preconfigured information detailing the IP addresses used by these SNPNs to interconnect with the SNPN Credential Provider.

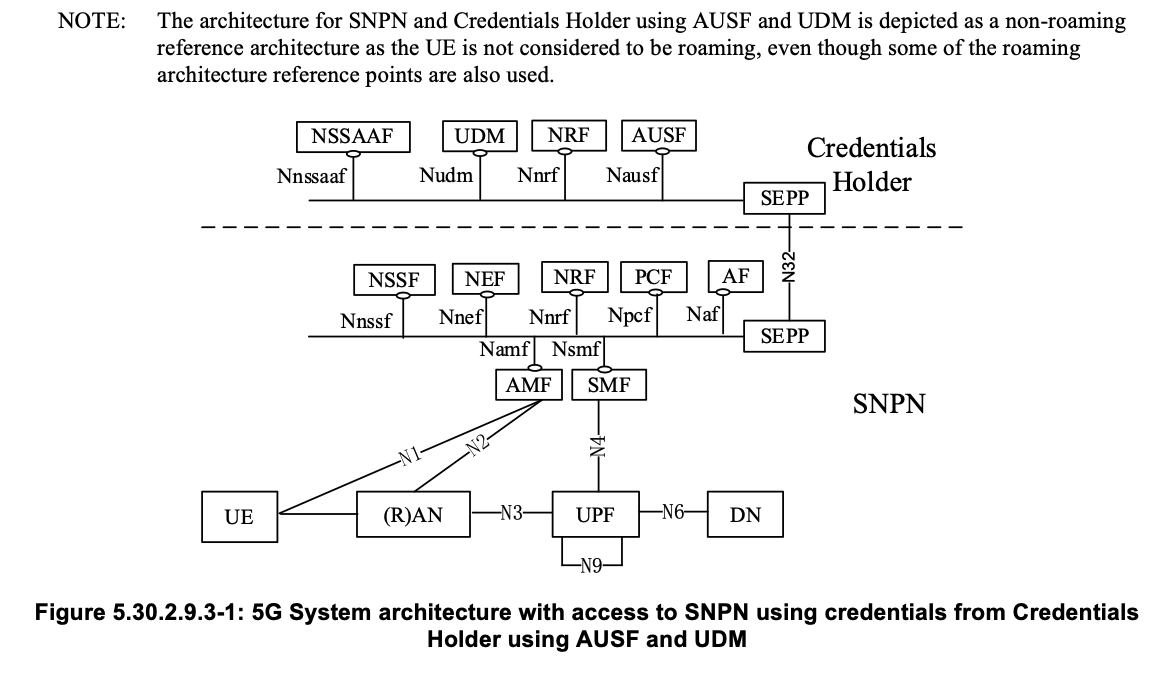
- R3: Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to be able to determine how to connect to an SNPN Credential Provider capable of verifying the identity presented by a user attempting to connect to that SNPN.

- R4: Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to be able to securely interconnect with an SNPN Credential Provider in deployments where the required security information is not preconfigured.

- R5: Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to enable an SNPN Credential Provider to securely notify events (e.g., a user’s subscription ending) to the SNPN.

NOTE 1: SNPN hotspot refers to a connectivity hotspot based on 3GPP 5G network technology that provides services in a similar way as provided by WLAN hotspots. Charging requirements are considered out of scope for this functionality.

3GPP has a capability to enable Non-Public Network (NPN) deployments of 5G-based systems. In Release 17, the 3GPP architecture [2] was enhanced to enable a Credentials Holder (CH) responsible for authenticating User Equipment (UE) to be decoupled from the operator of the SNPN, as shown below in Figure 2. The CH equates at an SNPN Credentials Provider in the 3GPP Stage 1 requirements.

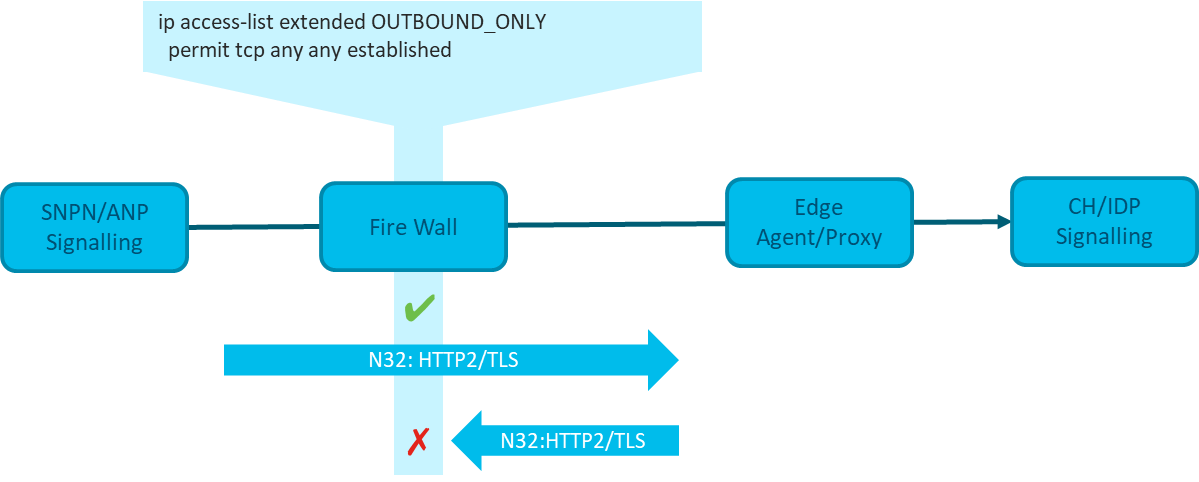


**Figure 2: 5G System Architecture with access to SNPN credentials from CH.**

**Observation 1:** From Figure 2, OpenRoaming architecture fits into 3GPP SNPN Rel-17 architecture where IdP and ANP act as CH and SNPN, respectively.

**Observation 2:** From Figure 2, CH and SNPN communicate using SEPP over the N32 reference point.

Today's PLMNs have a centralized database of IP addresses of all operator nodes that connect to the inter-PLMN IP backbone network, including AAA servers/proxies. This information is used for firewall and border gateway configuration. Signaling connections between VPLMN and HPLMN are long-lived (Diameter and N32f) and support bidirectional signaling. However, for SNPNs, there is no centralized IP address database. SNPNs configure the firewall to enable outbound connections to IdP/CH. In this case, signaling connections between SNPN and CH are short-lived. Signaling connections between SNPN and CH can be terminated if no signaling needs to be exchanged. Figure 3 shows a simplified firewall configuration allowing outbound connections to arbitrary addresses and the resulting failure of a new inbound connection from IdP (CH) to ANP (SNPN) with today's architecture.

****

**Figure 3: Firewall and SNPN deployment using N32**

**Observation 3:** Due to scalability considerations, the deployment of SNPN cellular hotspots means signaling connection between SNPN and CH over N32 can terminate if no signaling needs to be exchanged between a pair of SNPN and CH.

R1 and R2 capture the need for a scalable solution for connections between a CH and an SNPN.

N32 SBA architecture uses HTTP as the protocol for bi-directional signaling exchanges. HPLMN initiated subscription for notifications to a callback URI is required from consumer NF in VPLMN to a producer NF in HPLMN. Producer NF uses callback URI received in a service request to connect with consumer NF if any data is available (e.g. changes in the user’s identity profile). In current N32 SBA architecture, the HPLMN initiated signalling to a callback URI may require a separate firewall rule configuration (e.g., when the callback URI is a different 5-tuple).

R5 captures the need for the CH to be able notify events to the SNPN.

**Observation 4:** Enhancements to N32 that permit the CH-initiated signaling towards an SNPN to reuse the same outbound socket as SNPN-initiated signaling towards the CH should be studied to minimize the firewall and border gateway configuration of the SNPN.

The N32 reference points have been defined to support the signaling between public networks, dimensioned to enable support between VPLMNs with country-wide geographical coverage and HPLMNs with 10s of millions of subscribers. These scaling requirements have led to the definition of roaming architecture reference points that use long-lived forwarding connections between VPLMNs and HPLMNs. In contrast, an SNPN typically covers a much smaller area, and a single CH may only support a small number of UEs. Consequently, the volume of traffic between the SNPN and CH is much less and more likely to be torn down due to inactivity.

**Observation 5:** N32 reference point is currently designed to support 10s of millions of subscribers using a long-lived connection between VPLMN and HPLMNs.

Some forecasts predict there will be 1 million SNPNs in Europe by the end of the decade - a 1000 times increase compared to the number of public networks. As LS S3-221740 from the Wireless Broadband Alliance indicates, signaling scaling from roaming using non-public Wi-Fi networks can experience signaling scaled at 1/1000th of the load experienced by public networks. Hence, one future scenario has the N32 reference points being required to support 1000 times more networks, each with 1/1000th of the signaling scale of a conventional public network. Such scaling requirements are radically different from those that led to the specification of long-lived forwarding connections between VPLMNs and HPLMNs and have not been studied.

**Observation 6:** N32 reference points will be required to support 1000 times more networks, each with significantly less signaling scale of conventional public network. Such requirements lead to short-lived forwarding connections between VPLMNs and HPLMNs that needs to be studied.

R4 states the need for an SNPN to be able to securely interconnect with CH in deployments where the required security information is not preconfigured. Network domain security in the 5GS is achieved via cross-certification, as defined in TS 33.310 clause 4.2 [4]. This functionality was defined with the assumption of bilateral roaming agreements between PLMNs and does not apply to or scale for SNPNs. The challenge to do this by any means other than manual configuration is described in TS 33.310 Appendix B.3. [4].

**Observation 7:** Network domain security via cross-certification does not apply to or scale for SNPNs. A suitable solution to secure connections between CH and SNPN needs to be studied.

R3 states the need for an SNPN to be able to determine how to connect to a CH capable of verifying the identity presented by a user attempting to connect to that SNPN.

In the view of the authors, this requirement is already resolved in the existing specification, as implied by the following excerpt from TS 23.501 clause 5.30.2.3:

*A subscription of an SNPN is either:*

*- identified by a SUPI containing a network-specific identifier that takes the form of a Network Access Identifier (NAI) using the NAI RFC 7542 [20] based user identification as defined in clause 28.7.2 of TS 23.003 [19]. The realm part of the NAI may include the NID of the SNPN; or*

*- identified by a SUPI containing an IMSI.*

*NOTE 3: As to route network signalling to AUSF and UDM instances serving the SNPN-enabled UE, the UE can be configured with Routing Indicator locally or updated with Routing Indicator using the UE Parameters Update via UDM Control Plane procedure defined in clause 4.20 of TS 23.502 [3]. When the SNPN credential is stored in the USIM, the Routing Indicator is provisioned in the USIM, when the SNPN credential is stored in the ME, the Routing Indicator is provisioned in the ME.*

*In the case of access to an SNPN using credentials owned by a Credentials Holder as specified in clause 5.30.2.9.2 and clause 5.30.2.9.3, the SUPI shall also contain identification for the Credentials Holder (i.e. the realm in the case of Network Specific Identifier based SUPI or the MCC and MNC in the case of an IMSI based SUPI). In the case of access to an SNPN using credentials owned by a Credentials Holder using AAA-S as specified in clause 5.30.2.9.2, only Network Specific Identifier based SUPI is supported.*

Regardless of the fact that the signalling connection between the SNPN and the CH might need to be established on the fly, the SUPI asserted by the user always includes information (i.e. the realm part) that allows the SNPN to retrieve the CH’s IP address.

**Observation 8:** The SUPI asserted by the user always includes information (i.e. the realm part) that allows the SNPN to retrieve the IP address of a CH capable of verifying the identity presented by a user attempting to connect to that SNPN.

# 4 Detailed proposal

The following observations are summarized from above:

**Observation 1:** From Figure 2, OpenRoaming architecture fits into 3GPP SNPN Rel-17 architecture where IdP and ANP act as CH and SNPN, respectively.

**Observation 2:** From Figure 2, CH and SNPN communicate using SEPP over the N32 reference point.

**Observation 3:** Due to scalability considerations, the deployment of SNPN cellular hotspots means signaling connection between SNPN and CH over N32 can terminate if no signaling needs to be exchanged between a pair of SNPN and CH.

**Observation 4:** Enhancements to N32 that permit the CH-initiated signaling towards an SNPN to reuse the same outbound socket as SNPN-initiated signaling towards the CH should be studied to minimize the firewall and border gateway configuration of the SNPN.

**Observation 5:** N32 reference point is currently designed to support 10s of millions of subscribers using a long-lived connection between VPLMN and HPLMNs.

**Observation 6:** N32 reference points will be required to support 1000 times more network, each with significantly less signaling scale of conventional public network. Such requirements lead to short-lived forwarding connections between VPLMNs and HPLMNs that needs to be studied.

**Observation 7:** Network domain security via cross-certification does not apply to or scale for SNPNs. A suitable solution to secure connections between CH and SNPN needs to be studied.

**Observation 8:** The SUPI asserted by the user always includes information (i.e. the realm part) that allows the SNPN to retrieve the IP address of a CH capable of verifying the identity presented by a user attempting to connect to that SNPN.

It is proposed to agree the new SID proposal [S3-24yyyy] with the aim to study potential enhancements and security aspects that facilitate deployments by SNPN cellular hotspots, the requirements for which are provided in TS 22.261 clause 6.25.4 [3].

The SID proposal is focused on security aspects of SNPN cellular hotspots. It is the understanding of the proponents of this SID that the Stage 1 requirements on Groups of Interconnected SNPNs does not necessitate work in SA3.

Use cases of emergency services and public safety may be considered as well, including but not limited to IMS.