**3GPP TSG-SA3 Meeting #109*AdHoc-e draft\_S3-230190-r1***

**16 - 20 January 2023**

**Source: Intel**

**Title: Add Usecases to Solution 10**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***This contribution proposes to remove EN related to use case for solution #10 in TR 33.858.***

# 2 References

# [1] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[2] 3GPP TR 23.700-08: "Study on enhanced support of Non-Public Networks; Phase 2".

# 3 Rationale

*This solution addresses Key Issue #2 (Authentication for UE access to hosting network). The proposed solutions use existing mechanisms in 33.535[3].*

*As per the conclusion in 23.700-08[2], clause 8.4, when UE accesses the Hosting network using the subscription/credentials of its Home network, only two cases are considered:*

*- If the Home network is PLMN, the Hosting network can be PNI-NPN or SNPN.*

*- If the Home network is SNPN, the Hosting network can be only SNPN.*

*In both cases, solutions to these scenarios can be considered in the following categories*

*- UE uses home network credentials to access the hosting network.*

*- UE uses credentials obtained using the onboarding procedure as defined in 33.501[1] Annex I.9("Security of UE onboarding in SNPNs" to access the hosting network.*

*- UE uses credentials provided by Home Network using existing 3GPP mechanisms.*

# 4 Detailed Proposal

It is proposed to approve the following changes for inclusion in TR 33.738.

\*\*\*Start of CHANGEs\*\*\*

6.10 Solution #10: Access to localized services using existing mechanisms

6.10.1 Introduction

This solution addresses Key Issue #2 (Authentication for UE access to hosting network). The proposed solutions use existing mechanisms in 33.501[4].

As per the conclusion in 23.700-08[2], clause 8.4, when UE accesses the Hosting network using the subscription/credentials of its Home network, only two cases are considered:

- If the Home network is PLMN, the Hosting network can be PNI-NPN or SNPN.

- If the Home network is SNPN, the Hosting network can be only SNPN.

In both cases, solutions to these scenarios can be considered in the following categories

- UE uses home network credentials to access the hosting network.

- UE uses credentials obtained using the onboarding procedure as defined in 33.501[4] Annex I.9("Security of UE onboarding in SNPNs" to access the hosting network.

Note: Onboarding procedures only provide connectivity to obtain credentials. The credentials provisioning protocol is out of scope.

Following clause details how UE can use existing mechanisms and methodologies to access localized services.

6.10.2 Solution details

6.10.2.1 Solution for access to localized services based on Home Network Credentials

To access the hosting network, the UE determines whether it can reuse home network credentials. As per 23.700-08[2], the UE concludes that a home network credential can be utilized if the SNPN ID of the hosting network is contained in the SNPN priority lists connected with the home network subscription and the hosting network shows support for CH credentials. Existing 33.501[4] primary authentication can be reused in this case. No normative work is needed from the SA3 WG perspective.

6.10.2.2 Solution for access to localized services based on Onboarding Mechanism

Figure 6.10.2.2-1 shows a general overview of the access to localized services based on the onboarding mechanism. If UE uses credentials other home network credentials, then credentials obtained using the onboarding procedure as defined in 33.501[4] Annex I.9("Security of UE onboarding in SNPNs" can be used to access the hosting network.

****

**Figure 6.10.2.2-1: Overview of Access to localized services based on Onboarding Mechanism per Annex I.9.2**

Figure 6.10.2.2-2 shows the procedures for access to localized services.

****

**Figure 6.10.2.2-2: Procedures to Access localized services based on Onboarding**

1. The Localized Service Provider (LSP) establishes a service agreement with the operator of a Hosting Network. The LSP also establishes a service agreement with the UE to enable the UE to receive the information needed to discover/access Hosting Network and the localized service. The hosting network is configured based on the service agreement, e.g., DNN/S-NSSAI configuration for access to localized service, QoS, number of end-users, time, location, whether home network services can be accessed via the hosting network, etc. The configuration of the Hosting Network is performed by means that are outside of the 3GPP scope. The UE performs the procedures defined in 3GPP TS 23.502 to get the 5GC network access.

NOTE: In figure 6.10.2.2-2, the same network takes the role of the Onboarding network and then of the hosting network. Also, DCS can be involved in step 1c for primary authentication or as a part of step 2(secondary authentication).

2. Localized service advertisements prompt UE's user using default credentials where UE authenticates with the DCS (e.g., per TS 33.501[4] Annex I.9.2). The procedures are similar to the existing 23.501[BB] clause 5.30.2.10.2. e.g., After a successful onboarding procedure, the LSP sends a Security Profile corresponding to the UE and LSP certificate to the LSP access. The Security Profile associated with the LSP contains all the necessary data to establish a TLS tunnel between the LSP and UE.

Note: Aspects related to information configuration, such as PVS IP address and PVS FQDN, depend on WG SA2’s conclusions.

3. After step 2, the UE needs to disconnect from the network (so far in the role of onboarding network) and reconnect again (now in the role of Hosting network). The user performs a selection of the Hosting Network. UE connects to the Hosting Network and is authenticated by the LSP in the role of Credential Holder (e.g., using a AAA server) using credentials downloaded in 2. UE requests a PDU Session and accesses the localized service of the LSP via the Hosting Network. Upon expiry of the time-restricted credentials, the LSP in the role of Credential Holder requests a release of the UE. When the localized service agreement is terminated, the Hosting Network removes the configured information by means that are outside of the 3GPP scope.

6.10.3 System Impact

For 6.10.2.1, We do not see any system impact on existing security architecture per 33.501[4].

For 6.10.2.2, , the existing UE onboarding procedure cannot be used as is for access to localized services. As per 23.501[6] clause 5.30.2.10.4.2 (Onboarding configuration for the UE), The PVS information, such as PVS IP address and PVS FQDN(s) provided by the onboarding network takes precedence over any such information stored in the UE. In contrast, the PVS information provided by the DCS takes precedence over the information stored in the onboarding network.

6.10.4 Evaluation

For 6.10.2.1, With the proposed solutions above, we do not see any system impact on the existing security architecture per 33.501[4]. The solution addresses key issue 2 and fulfils the requirements of mutual authentication between UE and the Hosting Network.

The solution considers two scenarios for UE access to the hosting network using the subscription/credentials of the home network:

- If the home network is a PLMN, the hosting network can be a PNI-NPN or a stand-alone network providing non-3GPP access (SNPN).

- If the home network is an SNPN, the hosting network can only be an SNPN.

In both cases, the UE has two options for accessing the hosting network:

- The UE can use home network credentials to access the hosting network, in which case existing primary authentication methods in TS 33.501 can be reused.

- The UE can use credentials obtained through an onboarding procedure defined in Annex I.9 of TS 33.501, which provides connectivity to obtain credentials. The credentials provisioning protocol is outside the scope of this solution.

The solution addresses both cases where if UE is preconfigured with PVS address information and the UE receives PVS address information from the SMF during the PDU Session Establishment Accept message; the UE can determine based on local configuration whether to apply or ignore the PVS address information provided by the SMF.

. \*\*\* END OF CHANGE \*\*\*