**3GPP TSG-SA3 Meeting #113 *S3-23xxxx***

**Chicago, USA 06 - 10 November 2023** (revision of S3-yyxxxx)

**Source: Huawei, HiSilicon**

**Title: R19 SID discussions for security enhancement of network slicing**

**Document for: Discussion**

**Agenda Item: 6**

# 1 Decision/action requested

***Provide information for R19 study on network slicing.***

# 2 References

[1] 3GPP TS 33.501

[2] 3GPP TS 23.502

[3] 3GPP TS 38.300

[4] 3GPP TR 33.874

[5] 3GPP TS 23.502

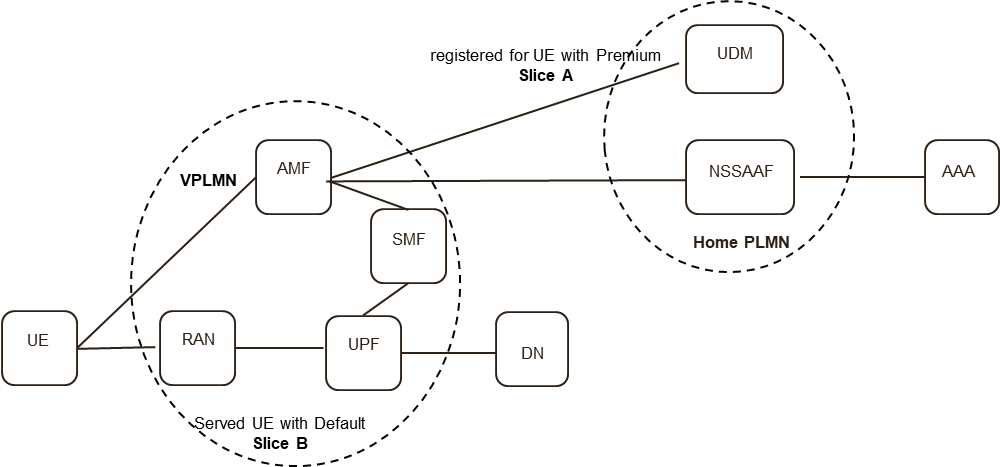
# 3 Rationale

Since Release 15, SA2 and SA3 have introduced various functional and security features relevant to network slicing. Amongst them, the following are observed to contain inconsistence issues or security implications. They deserve to be studied further in Release 19.

## 3.1 Home control to a roaming UE

In Release 15, theincreased home control is introduced and specified during Primary Authentication in TS33.501 [1]to prevent certain types of fraud, e.g. fraudulent registering a UE's serving AMF in UDM that the UE is not actually present in the visited network. The home control is realized through that the AUSF in the Home obtains confirmation that the UE has been successfully authenticated (cf. sub-clauses 6.1.3.1, 6.1.3.2, 6.1.4.1a of TS33.501 [1]). The Home AUSF can verify which PLMN a roaming UE is being served during primary authentication and the Home UDM can store authentication results (timestamp and PLMN name etc.).

However, there is no such home control feature during the UE’s slice authentication, i.e NSSAA procedure. Specifically, the Home does NOT know whether VPLMN provides UE with services of specific slices since the UDM does not store NSSAA results and VPLMN name is not verified by the Home. This may potentially cause a similar fraud as during Primary authentication, e.g. fraudulent registering a UE's serving AMF for slice A, but the UE is actually not registered or served by the slice in the visited network.



**Observation 1:** it is worthwhile investigating whether and how to provide consistent home control so that the Home may verify the real network slices being used to serve its roaming UE.

## 3.2 Network Slice Access Stratum Group (NSAG)

The NSAG information, as specified in TS23.502[2]/TS38.300[3] in Release 17, is an identifier of a group of network slices. The NSAG values are broadcasted (part of SIB1/SIB16) by gNBs for UE to perform Cell Reselection for the associated network slices. SA3 has concluded in TR33.874 [4] that including NSAG in a SIB will not cause security issues provided that the NSAG is defined properly.



However, the NSAG has not been used in the registration procedure due to lack of study on whether NSAG may leak sensitive slice information during initial AS registration.

**Observation 2:** Whether including NSAG in the registration request message causes any security issues should be studied so that UE can utilize NSAG to fast access to the slice in the NSAG.

## 3.3 Network Slice Simultaneous Registration Group (NSSRG)

The NSSRG information has been specified in TS23.501[5] and TS23.502[2] since the Release 17 in the UE’s subscription/configuration. It is used to restrict UE not to register to network slices in different NSSRG simultaneously. In other words, UE is allowed to register multiple slices within the same NSSRG at the same time but register slices from different NSSRG one at a time.

However, the UE’s security context for slices in different NSSRG could be shared even if the UE is registered to one slice after de-registered another. For example, a UE can register to Slice A at first. After the UE is switched off and deregistered from Slice A, the UE can be switched on again and registered to another Slice B. In this case, UE will share the same security context based on the current specification in TS33.501 [1], irregardless whether Slice A and Slice B are in the same NSSRG group. In addition, UE is sharing security context by default for slices within the same NSSRG. This may not be desirable in some scenarios where it is preferable not to allow security context sharing due to requirements from operators/applications.

**Observation 3**: SA3 should investigate whether restriction should be applied to network slices to avoid security context sharing.

# 4 Detailed proposal

It is proposed to study potential security enhancements to network slicing for R19, specifically,

**1:** whether and how to provide consistent home control so that the HPLMN can verify the real network slices being used to serve its roaming UE.

**2:** whether including NSAG in the registration request message causes any security issues so that UE can utilize NSAG to fast access to the slice in the NSAG.

**3**: whether restriction should be applied to network slices to avoid security context sharing.