**3GPP TSG-SA3 Meeting #104-e *S3-212463-r9***

e-meeting, 16 - 27 August 2021 was *S3-211527-r3*

**Title: Reply LS to GSMA on prevention of attacks on sliced core network**

**Response to: LS S3-212420 from GSMA FSAG**

**Release: N/A**

**Work Item: N/A**

**Source:** **SA3#104-e**

**To: GSMA**

**CC: SA2, CT4**

**Contact person: Tao Wan**

 **t.wan@cablelabs.com**

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

**Attachments:** none

# 1 Overall description

# SA3 thanks GSMA FSAG for their LS on "Prevention of attacks on sliced core network". SA3 would like to provide the following clarifications on the attacks discussed in the GSMA LS.

First, we would like to suggest that the assumption of these attacks appears very strong that an NF in the core network could be compromised. Note that an AMF contains the security contexts of all user equipment (UE) it serves, thus a comprised AMF would lead to more serious data breaches. We next provide clarification on each of the three attacks:

**Theft of Access Token** – this attack could be mitigated if the NRF authorizes the NF service consumer to obtain tokens only for authorized slice(s), as stated in clause 13.4.1.1.2 (step 1) of TS 33.501, *“The NRF checks whether the NF Service Consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the NRF shall then generate an access token with appropriate claims included".* SA3 is investigating if further clarification or additional enhancement to the current authorization procedures in TS 33.501 is needed.

**OCI mis-usage** – this attack as described in GSMA LS is not realistic since 3gpp-Sbi-Oci is used by a recipient NF to mark the overload of the sending NF who created the header. In the described attack, the attacking NF, which is the sender of the 3gpp-Sbi-Oci header, would be marked by the shared network function as overload. Further, OCI scope is on the level of NF instance or NF set, not on the slice level. Even if the S-NSSAI is in the header, it indicates that NF instance or NF set serving the particular slice is overloaded, not implying that the entire slice is overloaded. SA3 concluded that no additional enhancement to 3GPP specifications is needed for this issue.

**User Location Information Acquisition** – this attack could be mitigated if the shared network function (NF Service Producer) checks whether the NF Service Consumer can access the slice that the UE is currently registered to, e.g., by verifying the consistency between the producer NSSAI in the access token provided by the NF Service Consumer and the UE’s allowed NSSAI. Note that SUPIs are encrypted when being transmitted over radio channels, thus cannot be easily obtained in 5G. SA3 is investigating if further clarification or additional enhancement to 3GPP specifications is needed.

# 2 Actions

**To: GSMA FSAG**

**ACTION:** SA3 ask GSMA please take the above information into account.

# 3 Dates of next TSG SA WG 3 meetings

The next TSG SA WG3 meetings are available here:

https://www.3gpp.org/DynaReport/Meetings-S3.htm