**3GPP TSG-SA3 Meeting #104-e *S3-212463r1***

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**

**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 has already been compromised. It is hard to achieve unless this is an insider attack from within the 5GC. For example, an AMF, as cited in the attacks, contains the security context of all user equipment (UE) it serves. A comprised AMF would lead to data breaches for all served UEs, which is much more devastating than the impact of the attacks themselves. Specifications and protocols may not be able cover all scenarios arising out of an insider attack. This is applicable for 5G as well as previous 4G/3G etc. Usually defense-in-depth principles are applied to cover such scenarios. This would have larger impacts to the 3GPP systems. We next provide clarification on each of the three attacks:

* **Theft of Access Token** – this attack could only be possible if the NRF authorizes the compromised NF service consumer to obtain tokens for unauthorized slice(s). This is against the principle of the 3GPP specification, as stated in clause 13.4.1.1.2 (step 1) of TS33.501, *“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 whether additional clarification to the authorization procedure is necessary to avoid any ambiguity.

**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 assumed the sender, would provide overload information the shared network function. Further, ociScope is on the level of NF instance or NF sets, not on the slice level. Even the slide ID is in the header, it indicates that NF instances or NF sets on the particular slide is overloaded, not the entire slice overloaded.

# **User Location Information Acquisition** – this attack has an even stronger assumption that the compromised NF can obtain the SUPI of the victim UE. It is noted that SUPI is only available in few NFs, e.g. UDM, UDR, or AMF. This assumption may not be valid in the 5G setting. Firstly, SUPI is encrypted by the SUCI at all time when being transmitted over wireless channels. Secondly, all the service-based interfaces between NFs using for SUPI transmission are security protected. The compromised NF-2 not serving the victim UE will not be able to obtain its SUPI. Further, with this assumption, the attack could only happen if the shared network function (NF service producer) does not check whether the SUPI in a service request is served by the requesting (i.e. compromised) NF service consumer. In addition, even if SUPI is somehow available at the compromised NF, which can send the request to AMF, AMF with the mapping between the SUPI and the allowed slice-ID is able to reject the request after verifying allowed slice-ID with the slice-ID included in the access token. SA3 is investigating whether clarification is required to the 3GPP specifications to avoid any ambiguity.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

SA3#105-e 8 - 12 November 2021