**3GPP TSG-SA3 Meeting #103-e *S3-211527-r3***

e-meeting, 17 - 28 May 2021

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

**Response to: LS S3-211383 from GSMA FSAG**

**Release: N/A**

**Work Item: N/A**

**Source:** **SA3#103-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 is strong that an NF could be compromised. 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). SA3 is investigating whether additional enhancement to authorization procedure is necessary to mitigate the threat.
* **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 would be marked by the shared network function as overload. 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. (explain with more details why this is not on the slice level). 29.500
* **User Location Information Acquisition** – this attack may be possible if the shared network function does not cross check the SUPI in a request belongs to the slice ID of the requesting NF service consumer, or if the shard network function does not have sufficient information to cross check. SA3 may further investigate this issue for 5G networks where shared network functions cannot be avoided.

# Attack could be mitigated if the shared network function (NF service producer) does check the SUPI in a request ~~is indeed served by (belongs to) the slice ID of~~ the requesting NF service consumer are being served by a common slice. SA3 is investigating if 3GPP specifications allow such check. 5.15 -TS 23.501 / 29.510/29.518 (AMF stage 3). 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#104-e 16 - 27 August 2021 Electronic meeting

SA3#104Bis-e 4 - 8 October 2021 Electronic meeting