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

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.

* **Theft of Access Token** – this attack can be mitigated if the NRF verifies the slide ID in the Nrf\_AccessToken\_Get request against the authoritative information such as NF profile or NF certificate.
* **OCI mis-usage** – this attack 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.
* **User Location Information Acquisition** – this attack may be possible if the shared network function does not cross check the SUPI in a request against the slice ID of the NF consumer, or if the shard network function does not have sufficient information to cross check. A simple way to mitigate such attack is to avoid sharing network functions across slices if strict slice isolation is required.

SA3 would like to acknowledge that SA3 specifications could be further improved to allow more rigorous validation of requesting parameters against authoritative information.

# 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#103Bis-e 5 - 9 ~July 2021 Electronic meeting (TBC)

SA3#104-e 16 - 27 August 2021 Electronic meeting