**3GPP TSG-SA3 Meeting #124 S3-253799-r1**

Wuhan, China, 13 – 17 October 2025

**Title: Reply LS to GSMA on CVD-2025-0101**

**Response to: S3-253130 GSMA CVD-2025-0101 – Four critical vulnerabilities in the access control mechanism of the 5G core Network**

**Release: Release 19**

**Work Item: 5G\_eSBA**

**Source: SA3**

**To: GSMA**

**Cc: CT4**

**Contact person: Zander Lei**

 **lei.zhongding@huawei.com**

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

**Attachments: S3-253798**

# 1 Overall description

SA3 thanks GSMA CVD PoE for their LS on the potential vulnerabilities in the access control mechanism of the 5G core Network. SA3 would like to provide the following responses:

**• 3GPP TS 33.501: §13.4.1.1.2 could be more explicit about the exact conditions and content of the list of S-NSSAIs (producerSnssaiList) in the access token, including case 1b.**

[SA3] In TS 33.501, it has been specified in clause 13.4.1.1.2 (**step 2 of case 1a**) that the NRF only includes authorized slices/NSSAIs in the token claim. The NRF issues an access token without a list of NSSAIs in the claim only if all slices are authorized. Thus, an NF Consumer will not be able to use an access token to access services of unauthorized slices served by the NF Producer. For more clarity, NOTEs have been added in the clauses 13.4.1.1.2 and 13.4.1.2.2 as suggested.

As far as the“**1b case**”is of concern, similar behavior is specified for the NRF in clause 13.4.1.1.2 (similar normative text to the first bullet point above). The NRF only includes authorized slices/NSSAIs in the token claim. In order to keep consistence for the case 1a and the case 1b, clauses 13.4.1.1.2 and 13.4.1.2.2 are thus updated. The details can be found in the CR attached.

# 2 Actions

**To GSMA CVD**

**ACTION:** SA3 kindly asksGSMA CVD PoE to take above information into consideration

# 3 Dates of next TSG SA WG 3 meetings

SA3#125 17 – 21 November 2025 Dallas, US

SA3#126 9 – 13 February 2026 India (TBD)