**3GPP TSG-SA3 Meeting #123 S3-253054-r2**

**Goteborg, Sweden, 25 – 29 August 2025**

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

**Response to: S3-252509 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:** **CT1**

**Contact Person:**

#### Name: Zander Lei

E-mail Address: lei.zhongding@huawei.com

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

**Attachments: S3-253053**

**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 29.510: to add a note in the definition of producerSnssaiList in Table 6.3.5.2.4-1, indicating this attribute includes the slices requested and authorized during Access Token Request verification by NRF.**

[SA3] TS 29.510 is within the purview of the 3GPP CT1 working group.

**• 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, the following have been specified in clause 13.4.1.1.2 (**step 2 of case 1a**):

* “*The NRF shall additionally verify the S-NSSAIs of the NF Service Consumer and check whether there are restrictions on the NF Service Consumer to access NF Service Producers' services of a specific NF type depending on the slices for which they offer their services.* ... *For example, the NRF may verify that the NF Service Consumer can serve a slice which is included in the allowed slices for the NF Service Producer of a specific NF type. If the NF Service Consumer is authorized, the NRF shall then generate an access token with appropriate claims included*.”
* *“The claims may include a list of S-NSSAIs or NSI IDs for the expected NF Service Producer instances...”.*
* *“NOTE 1: If the claims do not include a list of NSSAIs or NSI IDs for the target NF type, it implies the token can be used to access expected NF services of all expected NF Service Producers of the NF type based on local configuration and operator policy.”*

In other words, 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, a NOTE 0 has been added 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). It is understood that the NRF only includes authorized slices/NSSAIs in the token claim. In order to keep consistence for the case 1a and the case 1b, clause 13.4.1.1.2 and 13.4.1.2.2 are thus updated to include additional text, similar to those in the second and the third bullet points above. The details of the updated text are shown in the CR attached for your easy reference.

**2. Actions:**

**To GSMA CVD PoE**

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

**3. Date of Next TSG-SA WG3 Meetings:**

SA3#124 13 - 17 Oct 2025 Wuhan, China

SA3#125 17 – 21 Nov 2025 Dallas, United States