**3GPP TSG-SA3 Meeting #116 *S3-242453-r1***

Jeju, South Korea, 20th - 24th May 2024

**Title: Reply-LS on GSMA CVD-2023-0069 5G Core Network Attacks**

**Response to: LS S3-234135 CVD-2023-0069 – 5G Core Network Attacks**

**Release: Rel-18**

**Work Item: TEI18**

**Source: SA WG3**

**To: GSMA CVD**

**Cc: CT WG4**

**Contact person: lei.zhongding@huawei.com**

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

**Attachments:** S3-240895, S3-241948, S3-242451

# 1 Overall description

SA3 thanks GSMA for their LS on 5G Core Network Attacks. SA3 has analysed the attacks and would like to provide the following responses for the related Findings:

* **Related to Finding 1: Confused Producer Attack**

There are two types of access token requests specified for accessing services of NF Service Producersin clause 13.4 of TS33.501, i.e. one is “NF-type specific” (in terms of Service Producers) as described in (1a) while the other is “NF-instance specific” as in (1b) in clause 13.4.1.1. In the case of “NF-type specific” token requests, the NRF grants tokens without specifying instances of an NF Service Producer only if all instances of the requested NF type are authorized. In the “Confused Producer Attack” setup, the NRF will not grant C1 an access token without specifying instances since P2 is not authorized to serve C1.

Likewise, if a list of S-NSSAI is not included in the token claims, it implies all instances of NF Service Producers are authorized. In the case that NF Service Producers are slice-specific as in the “Confused Producer Attack” setup, the list of authorized slices (S-NSSAI) will be included in the claims.

Clarification text are added in clause 13.4.1.2 of TS 33.501 as shown in S3-240895.

* **Related to Finding 2: Token Reuse Attack**

The access token specified in clause 13.4 is a short-lived token where an expiration time is included to impose time limits on the access token in use. The expiration time is not specified but set based on the operator’s policy to allow flexibility and cost effectiveness, taking into consideration different threat situations and network complexities etc. In the current releases, token revocation is not supported.

A NOTE is added in clause 13.4.1.2 of TS 33.501 for clarification as shown in S3-241948.

* **Related to Finding 4: NFDiscovery Bypass Attack**

The NF profile is stored at the NRF after registration. The NRF needs to verify all parameters including “requesterSnssais” in the request message against the NRF-stored NF profile of the NF service consumer. It is misinterpretation that the NRF checks against the one in the request message of the consumer. Regarding NRF behaviour of handling the authorization check during the NF discovery, there are details already specified in the stage 3 specification TS 29.510, e.g. clauses 6.1.6.2.2, 6.2.3.2.3.1, and Annex C. Nevertheless, clarification text are added in the clauses 5.9.2.2 and 13.3.1.3 of TS 33.501 to avoid misunderstanding, as shown in S3-242451.

# 2 Actions

**To GSMA**

**ACTION:** SA3 kindly asks GSMA to take above information into account.

# 3 Dates of next TSG SA WG 3 meetings

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)

SA3#118 14 - 18 October 2024 Hyderabad (India)