**3GPP TSG-CT WG1 Meeting #132-eC1-21XXXX**

**E-meeting, 11-15 October 2021**

**Source: Lenovo, Motorola Mobility**

**Title: Correction of event triggered network slice adaptation procedure**

**Spec: 3GPP TS 24.549 V0.1.0**

**Agenda item: 17.2.23**

**Document for: Agreement**

**1. Introduction**

Error in procedures and reference and extra "and" remain in the spec.

**2. Reason for Change**

Client and server procedures for event triggered network slice adaptation have flaws and need to be corrected and completed.

A reference needs to be updated since it is obsolete.

Subclause 6.2.2.2 has a superfluous "and" after bullet b) which needs to be removed.

**3. Conclusions**

<Conclusion part (optional)>

**4. Proposal**

It is proposed to agree the following changes to 3GPP TS 24.549.

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows;".

[3] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[4] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification;".

[5] OMA OMA-TS-XDM\_Group-V1\_1\_1-20170124-A: "Group XDM Specification".

[6] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[7] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[8] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[9] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

\* \* \* Next Change \* \* \* \*

#### 6.2.2.2 Client procedure

In order to request for network slice adaptation, the SNSCM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 7231 [7]. In the HTTP POST request message, the SNSCM-C:

a) shall set the Request-URI to the URI identifying the SNSCM-C appended with VAL service identity and the value "/UE-triggered-slice-adaptation";

b) shall set the "Host" header field to the URI identifying of SNSCM-S and the port information;

c) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [8]; and

d) shall include the parameters for VAL UE list and requested S-NSSAI as specified in table A.1.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [9]; and

e) may include the parameters for requested DNN and slice adaptation cause as specified in table A.1.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [9].

\* \* \* Next Change \* \* \* \*

#### 6.2.2.3 Server procedure

Upon receipt an HTTP POST request from the SNSCM-C for network slice adaptation, the SNSCM-S shall determine the identity of the sender as specified in clause 6.2.1.1 to confirm whether the sender is authorized or not. If:

a) the sender is not an authorized user, the SNSCM-S shall respond with an HTTP 403 (Forbidden) response message and avoid the rest of steps; or

b) the sender is an authorized user, the SNSCM-S:

1) shall attempt to update the network slice for one or more VAL UEs with the identities listed in the VAL UE list for for the VAL service, identified by VAL service ID by using the parameters for requested S-NSSAI, requested DNN and slice adaptation cause from the HTTP POST request message;

Editor's note: How the SNSCM-S updates the network slice for one or more VAL UEs for a VAL service, needs to be specified.

2) shall send the updated network slice and any new DNN to the PCF, if the update is successful, 3GPP TS 23.434 [2]; and

3) shall send an HTTP 200 response message containing the successful or failure status of the requested network slice adaptation to the SNSCM-C.

<Proposed change in revision marks>

\* \* \* Next Change \* \* \* \*

## A.1.2 Client side parameters

The SNSCM-C uses the parameters shown in table A.1.2-1 to trigger network slice adaptation for a VAL application.

Table A.1.2-1: Client side parameters for network slice adaptation trigger

|  |  |
| --- | --- |
| Parameter | Description |
| VAL UE List | REQUIRED. Represents a space-separated list of VAL UE Ids within the VAL service, for which the network slice adaptation trigger applies. |
| VAL service ID | REQUIRED. The VAL service ID of the VAL application |
| Requested S-NSSAI | REQUIRED. The new S-NSSAI which is requested |
| Requested DNN | OPTIONAL. The new DNN which is requested |
| Slice adaptation cause | OPTIONAL. Indicates the cause for the slice adaptation. |