**3GPP TSG-CT WG1 Meeting #133e-bisC1-220191**

**E-meeting, 17-21 January 2022**

**Source: Lenovo, Motorola Mobility**

**Title: Resolving EN**

**Spec: 3GPP TS 24.549v1.0.0**

**Agenda item: 17.2.23**

**Document for: Agreement**

**1. Introduction**

<Introduction part >

**2. Reason for Change**

There is an EN for how the SNSCM-S updates network slices of a VAL service for a VAL-UE, which should be resolved.

**3. Conclusions**

Added text and referred to cluase 4.15.6.10 in TS 23.502, where there is a description how an eSEAL server can act as an application function and update application traffic by moidifying the URSP rules and thereby the network slices.

**4. Proposal**

It is proposed to agree the following changes to 3GPP TS <TS number and version>.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next 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".

[10] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*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 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;

NOTE: To update the application traffic, the SNSCE-S can act as an AF and use the reference point N33 as shown in 3GPP TS 23.434 [2] to influence a VAL UE's URSP rules for the application traffic by providing a guidance on the route selection parameters S-NSSAI and DNN as described in clause 4.15.6.10 of 3GPP TS 23.502 [10].

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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*