3GPP TSG SA WG5 Meeting 137-e TDoc S5-213446

electronic meeting, online, 10 - 19 May 2021

**Title:** LS on Reply LS on slicing management aspects in relation to SEAL

**Response to:** LS S5-213037 on slicing management aspects in relation to SEAL from SA6

**Release:** Release 17

**Work Item:**

**Source:** SA5 #137-e

**To:** SA6

**Cc: SA,** SA2

**Contact person:** Jan Groenendijk

jan.groenendijk@ericsson.com

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

**Attachments:** None

# 1 Overall description

SA5 thanks SA6 for the liaison regarding a possible role for SEAL in exposure of network slicing to third party applications in relation to existing work in SA5 on slicing management and the SID proposal from SA6, S6-210708.

On the question for SA5to provide views about a possible role for SEAL (TS 23.434) in exposure of network slicing to third party applications in relation to existing work in SA5 on slicing management and the SID proposal in S6-210708, SA5 would like to make the following observations:

- In TS 23.434, SA6 has defined the support of SEAL services based and complementing the existing Core Network capabilities, e.g. Network Exposure Function (NEF) to support vertical applications.

- Regarding the existing work in SA5 on management capability exposure, it is about management capability exposure to a vertical customer (via a general feature for Management capability exposure governance (MCEG)) with interactions of management systems, especially based on SLA signed between the vertical (plays role of network slice customer, NSC/NOP) and an operator (plays role of network slice provider). Management capabilities are exposed through OSS/BSS to support appropriate exposure and accountability. e.g. product ordering, charging, tenant identification, authentication and authorization, etc.). Together with SDOs working for management plane, e.g. TMF, ETSI ZSM, SA5 (including OAM and Charging) is studying and specifying the use case and solution for management capability exposure.  According to existing scope and architecture of SEAL defined in TS 23.434, SA5 doesn’t see any role in this chain (NSC, MCEG, NSP, etc.) could be played by SEAL. (the last sentence is to answer question of SA6 in the LS regarding SA5 views about a possible role for SEAL (TS 23.434) in exposure of network slicing)

- SA5 specifies management services (MnSs) that enable network operators and service providers to manage and orchestrate their 3GPP networks and services. The details of what is managed for a 5G network (5GC and 5G RAN) is specified in the Network Resource Model [TS 28.541](https://www.3gpp.org/DynaReport/28541.htm).

- Exposure of management capability in the context of [TS 28.557](https://www.3gpp.org/DynaReport/28557.htm) (not 28.857) is about access to management services provided by an NPN-SP (NPN Service Provider) and accessed by an NPN-SC (NPN Service consumer), while FS\_MNSAC is about authentication and authorization of an consumer that wants to access the MnS provided by an MnS producer.

- SA5 scope does not include application layer functions (AF) for control/signalling plane which could be the scope of SA2 and SA6. FS\_MNSAC is focused on capability exposure of the management plane to an external vertical customer, especially based on SLA between a vertical and an operator.

.

# 2 Actions

**To SA6**

**ACTION:** SA5 asks SA6 to take note of the provided information

# 3 Dates of next TSG SA WG 5 meetings

SA5#138-e 23 - 31 August 2021 electronic meeting