3GPP TSG SA WG5 Meeting 138-e TDoc S5-214515d1

electronic meeting, online, 23 - 31 August 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 #138-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**](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:

- The work in SA5 on management capability exposure to third party applications leverages a management capability exposure governance feature (TS 28.533). This exposure requires the interactions between the network slice provider’s management system (BSS/OSS) and the network slice customer’s management system. Solutions for these interactions are still subject to SA5 internal discussion. This means that management capabilities are to be exposed to third party through BSS.

- 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). SA5 assumes that any entity can access an MnS as long as it has authorization to do so. Therefore, with the right authorization the application layer should be able to use an MnS specified by SA5 where it makes sense for the use case to do so.

The application layer should be able to use the MnSs provided by SA5 where it makes sense for the use case to do so.

# 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#139-e 11 - 20 October 2021 electronic meeting

SA5#140-e 15 - 24 November 2021 electronic meeting