**3GPP TSG-SA5 Meeting #156 *S5-244585***

**Maastricht, Netherlands, 19 - 23 August 2024**

**Title: LS Reply on Internal 5G Core information expose to trusted AF**

**Response to: (S6-242714/S2-2407354) LS on Clarification related to Internal 5G Core information expose to trusted AF**

**Release: Release 18**

**Work Item: NSCALE**

**Source: SA5**

**To: SA6, SA2**

**Cc: SA3**

**Contact person: Yushuang Hu**

**huyushuang@chinamobile.com**

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

**Attachments:** N/A

# 1 Overall description

SA5 would like to thank SA6,SA2 for the LS on Clarification related to Internal 5G Core information expose to trusted AF.

Based on the latest LS from SA2(S2-2407354), for the following clarification request from SA6 about the information exposed by the 5GC to NSCE server: “As described in TS 33.501 clause 5.9.2.3, NEF and the AF shall fulfil the security requirements that include that “Internal 5G Core information such as DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain.”

The questions from SA6 to consult SA2 and SA3’s view are as following:

*Whether a trusted AF of an 3GPP operator is considered within the operator’s domain; If yes, whether it is possible to expose Internal 5G Core information such as DNN, S-NSSAI, etc. to a trusted AF (e.g., a NSCE server). Whether the NSI (i.e., Network Slice Instance) and/or NSI ID can be exposed to the trusted AF.*

* *Whether a trusted AF of an 3GPP operator is considered within the operator’s domain;*
  + *If yes, whether it is possible to expose Internal 5G Core information such as DNN, S-NSSAI, etc. to a trusted AF (e.g., a NSCE server).*
* *Whether the NSI (i.e., Network Slice Instance) and/or NSI ID can be exposed to the trusted AF.*

**The first question is already replied by SA2,** based on the statements that *“In SA2’s view, trusted AFs of a 3GPP operator are owned and operated by the 3GPP operator. Thus, it is considered within the operator’s domain.*

* + ***Follow-up question:*** *If yes (to Question 1), whether it is possible to expose Internal 5G Core information such as DNN, S-NSSAI, etc. to a trusted AF (e.g., a NSCE server).*
  + *[****SA2 Reply****] SA2 needs to further investigate whether the Internal 5G Core information such as DNN, S-NSSAI might be exposed to the trusted AF(s) of an 3GPP operator.*

**Therefore, for the Question 2**:*Whether the NSI (i.e., Network Slice Instance) and/or NSI ID can be exposed to the trusted AF?*

**[SA5 Reply]:** We respect SA2's conclusion that *“In SA2’s view, trusted AFs of a 3GPP operator are owned and operated by the 3GPP operator. Thus, it is considered within the operator’s domain.* and would like to provide further clarification from the SA5 perspective.

A NetworkSlice instance represents a Managed Object Instance (MOI) of NetworkSlice IOC (see clause 6 in TS 28.541). A NetworkSlice instance can be uniquely identified by a Distinguished Name (DN). For further details on DN, see clause 4.2.1 in TS 32.158.

With regards to using NSI and NSI ID, SA5 would like to make the following clarifications:

* NSI has been used interchangeably with NetworkSlice instance in TS 28.541. So both mean the same in the context of that specification.
* NSI ID is not defined in 3GPP SA5. For NetworkSlice instance identification purposes, DN is used instead.

The decision to expose NetworkSlice instance information (including DN) to trusted AFs is based on the operator’s policy. It is up to the operator to decide whether a trusted AF can (or cannot) consume this information, by making the trusted AF become an authorized (or non-authorized) MnS consumer.

# 2 Actions

**To SA6, SA2**

**ACTION: SA5 kindly requests SA6 and SA2 to take the information above into account and inform SA5 if further clarifications are needed**

# 3 Dates of next TSG SA WG 5 meetings

SA5#157 14 October - 18 October 2024 Hyderabad, India

SA5#158 18 November- 22 November2024 Orlando, US