**3GPP TSG-SA3 Meeting #107-e *S3-220958-r2***

e-meeting, 16 - 20 May 2022

**Title: draft Reply LS on Clarification on MBS Security Context (MSK/MTK) Definitions**

**Response to: LS C4-222303 on LS on Clarification on MBS Security Context (MSK/MTK) Definitions from CT4**

**Release: Rel-17**

**Work Item: 5MBS**

**Source:** **Ericsson (to be SA3)**

**To:** **CT4**

**Cc: CT1**

**Contact person: Markus Hanhisalo**

**Markus.hanhisalo@ericsson.com**

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

**Attachments:** None

# 1 Overall description

SA3 would like to thank CT4 for the LS C4-222303 on Clarification on MBS Security Context (MSK/MTK) Definitions.

In C4-222303, CT4 request following clarifications from SA3:

”CT4 is developing support of MBS Keys distribution via control place procedure as specified in Annex W of 3GPP TS 33.501, and would like to request following clarifications from SA3:

**Observation 1:** It is CT4's understanding that MBS Key Material sent by MBSF consists of a list of {*Key Domain ID, MSK ID, MSK, MTK ID, MTK*} per MBS Session. This is based on following information in Clause 6.3.2.1A:

*…*

*The UE shall receive the following information via the User Service Discovery / Announcement procedures if protection of the MBMS User Service is applied:*

*…*

*…*

*- Identifiers of the MSKs needed for the User Service.*

*For each MSK, the identifiers that shall be included are Key Domain ID and MSK ID. The Key Number part of each MSK ID shall be set to 0x0 to denote the current MSK. The Key Number values in the Service Announcement shall be ignored by the UE, since they may change over time and Key Group part of MSK ID is sufficient to identify the MSKs, see clause 6.3.2.1.*

*- Mapping information how the MSKs are used to protect the different RTP sessions or FLUTE channels.*

*…*

Hence, the information needs to contain a plural number of the above MBS Keys Sets each containing {*Key Domain ID, MSK ID, MSK, MTK ID, MTK*} per MBS Session.

**Question 1:** CT4 kindly requests SA3 to confirm if above understanding is correct?

**Observation 2:** 3GPP TS 33.246 Clause 6.3.2.1 specifies that Key domain ID is defined as:

*Key Domain ID = MCC || MNC and is 3 bytes long.*

**Question 2:** How is Key Domain ID encoded in case of SNPN?

**Question 3:** Is it mandatory to encode Key Domain ID using MCC/MNC only?”

**Question 4:** Can SA3 confirm that the Key Domain ID shall be sent together with the MBS keys from the MBSF towards the MB-SMF (and then SMF and UEs).

**Answers:**

**Answer 1:** SA3 confirms that above CT4 understanding is correct.

**Answer 2:** In case of SNPN, ***Key Domain ID = MCC || MNC***, the Key Domain ID used for SNPNs is not required to be unique.

**Answer 3:** Key Domain ID is recommended to be encoded using MCC and MNC in case of SNPN

.

Answer 4: Yes. The Key Domain ID shall be sent together with the MBS keys from the MBSF towards the MB-SMF.

# 2 Actions

**To CT4**

**ACTION:** SA3 would like to asks CT4 to take the above information into account.

# 3 Dates of next TSG SA WG 3 meetings

SA3#107e-Bis 27 June - 1 July 2022 electronic meeting

SA3#108e 22 -26 August 2022 Goteborg, Sweden