**3GPP TSG-CT WG4 Meeting #110-eC4-223302**

**E-Meeting, 12th – 20th May 2022**

**Title: LS on Clarification on MBS Security Keys**

**Response to:**

**Release:** **Rel-17**

Work Item: 5MBS

Source: CT4

To: SA3

cc: CT1, CT3, SA2

Contact Person: Varini Gupta

E-mail Address: Varini.gupta@samsung.com

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

**Attachment: None**

**1. Overall Description:**

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 the multicast session security context distributed by MBSF to MB-SMF, SMF and UE consists of MBS Service Key (MSK) and MBS Traffic Key (MTK) and the corresponding Key IDs, where MSK is used to protect the MTK. This is based on following highlighted text in 3GPP TS 33.501 Annex W.4.1.2:

*The multicast session security context consists of the MBS session ID, MBS keys and the corresponding key ID. The MBS keys include MBS Service Key (MSK) and MBS Traffic Key (MTK). MBS traffic is protected with the MTK. The MSK is used to protect the MTK when the MTK is delivered to the UE. The identification for every MSK and MTK are determined as specified in Clause 6.3.2.1 and clause 6.3.3.1 of TS 33.246 [102].*

*…*

*…*

*In the multicast session join and session establishment procedure, the SMF interacts with the MB-SMF to obtain the multicast session security context. Absence of the multicast security context indicates that security protection is not applied for the MBS session. The SMF shall provide the multicast session security context to the UE if received from the MB-SMF and the UE is authorized to use the required multicast service. The UE shall use the MTK in the received multicast session security context, to process the protected MBS traffic until it receives a new MTK update over the user-plane.*

**Question 1:** Are (or can) MSK and MTK delivered simultaneously when using Control Plane procedure?

**Question 2:** If the answer to Question 1 is Yes, is it a potential security flaw that the key which is used to protect MTK is delivered along with it?

------------

**Observation 2:** 3GPP TS 33.501 Annex W.4.1.2 specifies that:

*The MBSF determines whether security protection to be applied or not for the MBS session based on locally configured policy or based on the information provided by the AF. If security protection to be applied, then the MBSF shall create the multicast session security context by generating the MSK and its key ID for a MBS session. Afterwards, the MBSF distributes the MSK with MBS session ID and its key ID to the MB-SMF and MBSTF. The MBSF shall also distribute them to MB-SMF either upon request by the MB-SMF (i.e., pull) or when a new MSK is generated (i.e., push). The MBSF may also include the MSK lifetime when it distributes the MSK to MBSTF.*

*…*

*…*

*The MSK may be updated based on the request from MB-SMF or AS (e.g., due to the change of authorization information) or based on the local policy (e.g., key lifetime expiration). When the MSK is updated, the MBSF shall send the new MSK with MBS session ID and its key ID to the MB-SMF and then the MB-SMF shall trigger the session update as specified in clause 7.2.6 in TS 23.247 [103]. The MSK with MBS session ID and the corresponding key ID are delivered to the UEs that has joined the multicast session. The MBSF shall also send the new MSK with MBS session ID and its key ID to the MBSTF. The MBSTF may request a MSK to the MBSF when it does not have a valid MSK (e.g., due to the current MSK expiration).*

The highlighted part indicates that MSK lifetime is included when it is distributed to the MBSTF.

**Question 3:** How is following scenario handled:

* MSK lifetime expires in MBSTF
* MBSTF requests and receives updated MSK from MBSF
  + MBSF forwards updated MSK to the UE via MB-SMF
* MBSTF generates and distributes new MTK to MBSF
  + MBSF forwards updated MTK to the UE via MB-SMF or MBSTF sends MTK to the UE using MIKEY over UDP

At this moment, how does UE know as to "when" to start using the new MSK/MTK? Is there a possibility that MBSTF starts using updated MTK sooner than UE?

------------

**Observation 3:** CT4 has discussed some CRs (not yet agreed though) on handling of disabling security for an MBS session when it was enabled before. CT4 would like to know whether MBSF can send an update to MBSTF/MB-SMF indicating that the security is no longer applicable for an MBS Session.

**Question 4:** Can security for an MBS session be disabled when it was enabled before, and vice versa, when the MBS Session is active?

**2. Actions:**

**To SA3:**

**ACTION:** CT4 kindly requests SA3 to provide responses to above questions.

# 3. Dates of next CT4 meetings

The upcoming CT4 meetings can be found in the [CT4 Meetings calendar](https://www.3gpp.org/dynareport/Meetings-C4.htm?Itemid=294)