3GPP TSG SA WG4 Meeting #122 TDoc S4-230196

Athens, Greece, 20th–24th February 2023

**Title: Reply LS on security architecture for 5G multicast–broadcast services**

**Response to: S4-230013 | S3-223919**

**Release: Rel-17**

**Work Item: 5MBUSA**

**Source:** **3GPP SA4**

**To:** **3GPP SA3**

**Cc: 3GPP SA2, 3GPP CT4**

**Contact person: Richard Bradbury**

**richard dot bradbury at bbc dot co dot uk**

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

**Attachments:** S4-230040

# 1 Overall description

SA4 acknowledges SA3's LS response to SA2 on the topic of the security architecture for 5G multicast/broadcast and thanks SA3 for amending clause W.4.1.3 of TS 33.501 in line with SA2's recommendation to respecify the User Plane security procedure in more neutral terms (i.e., referring to the MBS Security Function). This change unblocks the completion of this aspect of the MBS User Services architecture by SA4 in TS 26.501.

However, SA4 observes that this change in TS 33.501 V17.8.0 introduces an architectural inconsistency between the Control Plane procedure and the User Plane procedure in the case of GBA-based security (per TS 33.246), as summarised in the table below:

|  |  |  |
| --- | --- | --- |
|  | Control Plane security procedure *TS 33.501 clause W.4.1.2* | User Plane security procedure *TS 33.501 clause W.4.1.3* |
| Assignment of session encryption key (MSK) | MBSF | MBS Security Function |
| Assignment of traffic encryption key (MTK) | MBSTF | MBS Security Function |

SA4 notes that TS 23.247 clause 6.13 specifies that the MBS Security Function is applicable to both Control Plane security procedures and User Plane security procedures. It is SA4's strong preference that this be reflected in TS 33.501 as follows to avoid constraining implementations of the Control Plane security procedure unnecessarily:

|  |  |  |
| --- | --- | --- |
|  | Control Plane security procedure *TS 33.501 clause W.4.1.2* | User Plane security procedure *TS 33.501 clause W.4.1.3* |
| Assignment of session encryption key (MSK) | MBS Security Function | MBS Security Function |
| Assignment of traffic encryption key (MTK) | MBS Security Function | MBS Security Function |

Besides, SA4 has agreed to add support of User Plane procedure as attached CR and leave the Nmb2 interaction to implementation. If the MBSSF can be introduced into the Control Plane procedure for the MSK and MTK allocation and management, the interaction among the MBSF, MBSTF and MBSSF would be left to implementation in Rel-17.

# 2 Actions

**To SA3**

**ACTION:** SA4 reminds SA3 that detailed functional architecture of the MBSF and MBSTF has been delegated by SA2 to SA4 and kindly asks SA3 to make a similar change to clause W.4.1.2 of TS 33.501 in Release 17, i.e. to describe the Control Plane security procedure in more neutral terms also, in particular by specifying that both the MSK and MTK are assigned by the MBS Security Function.

# 3 Dates of next TSG SA WG 4 meetings

SA4#123-e 17th–21st April 2023 Electronic

SA4#124 22nd–26th May 2023 Berlin, Germany