**3GPP TSG-SA3 Meeting #107Adhoc -e S3-221414-r2**

**e-meeting, 27th June – 1st July, 2022**

**Source:**  **Huawei, HiSilicon**

**Title:** **Key issue on security protection for UEs in RRC inactive state**

**Document for: Approval**

**Agenda Item: 5.23**

# 1 Decision/action requested

***It is proposed to approve the key issue described in this document.***

# 2 References

[1] 3GPP TR 23.700-47: " Study on architectural enhancements for 5G multicast-broadcast services ".

# 3 Rationale

In the SA2’s study on MBS phase 2[1], enabling UEs to receive Multicast MBS Session data in RRC Inactive state is currently being studied, which would be beneficial for serving large number of UEs. Supporting UE receiving Multicast MBS Session data in RRC Inactive might require enhancements to the key management mechanisms and hence needs further study.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[xx] 3GPP TR 23.700-47: " Study on architectural enhancements for 5G multicast-broadcast services ".

[yy] 3GPP TS 33.501: " Security architecture and procedures for 5G system".

\*\*\* END OF 1st CHANGE\*\*\*

\*\*\* 2nd CHANGE \*\*\*

## 5.X Key issue: security protection for UEs in RRC inactive state

### 5.X.1 Key issue details

In order to provide MBS service to more UEs in a cell, NG RAN could enable UEs within an MBS multicast session to receive MBS session data while in CM-CONNECTED with RRC Inactive state. As documented in TR 23.700-47[xx], MBS assistance information will be provided from 5GC to RAN. RAN nodes will determine the switching for the UEs belonging to MBS session from CM-CONNECTED state to CM-CONNECTED with RRC Inactive state.

As specified in clause W.4 of TS 33.501[yy], the key update procedure may trigger the switch of UEs from RRC Inactive state to RRC connected state. For example, when the MSK is updated in control-plane procedure, 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 procedure.

### 5.X.2 Security threats

For the MSK update in control-plane procedure, when the updated MSK being taken in to use in MBSTF is not specified. The MSK update may require more time for UEs in RRC inactive state. If the MBSTF activates the updated MSK earlier than the UEs obtains the updated MSK, then this will disrupt the services for UEs that did not receive the new keys in time.

### 5.X.3 Potential security requirements

\*\*\* END OF 2nd CHANGE\*\*\*