**3GPP TSG-SA3 Meeting #108-e S3-222069**

**e-meeting, 22nd – 26th August, 2022**

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

**Title:** **Solution on security protection for UEs in MOCN network sharing scenario**

**Document for: Approval**

**Agenda Item: 5.23**

# 1 Decision/action requested

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

# 2 References

[1] 3GPP TR 33.883: " Study on security enhancements for 5G multicast-broadcast services phase 2".

# 3 Rationale

If the content is protected using different CN-specific keys, then UEs not having the key will fail to properly process the content, should the network send only one of the copies. To address the issue, the solution proposed that MBSF/NEF needs to decide send one or more copies based on security activation status and indicate to RAN node.

# 4 Detailed proposal

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

## 6.X Solution # X: security protection for UEs in MOCN network sharing scenario

### 6.X.1 Introduction

If the security protection of MBS traffic is required, confidentiality and integrity protection will be provided in service layer. However, for UEs in different PLMN, the content is protected using different CN-specific keys. If RAN nodes only send one of the copies in MOCN network sharing scenario, UEs not having the key will fail to properly process the content.

To address the issue, the solution proposed that MBSF/NEF needs to decide send one or more copies based on security activation status and indicate RAN node. If the security in service layer is not activated, the RAN can reuse the network resource based on the indication and send one copy to save the overhead. Otherwise, more copies are required.

If service layer security is used, then optimized radio resource utilization for MBS is not possible for MOCN network sharing scenario.

### 6.X.2 Solution details

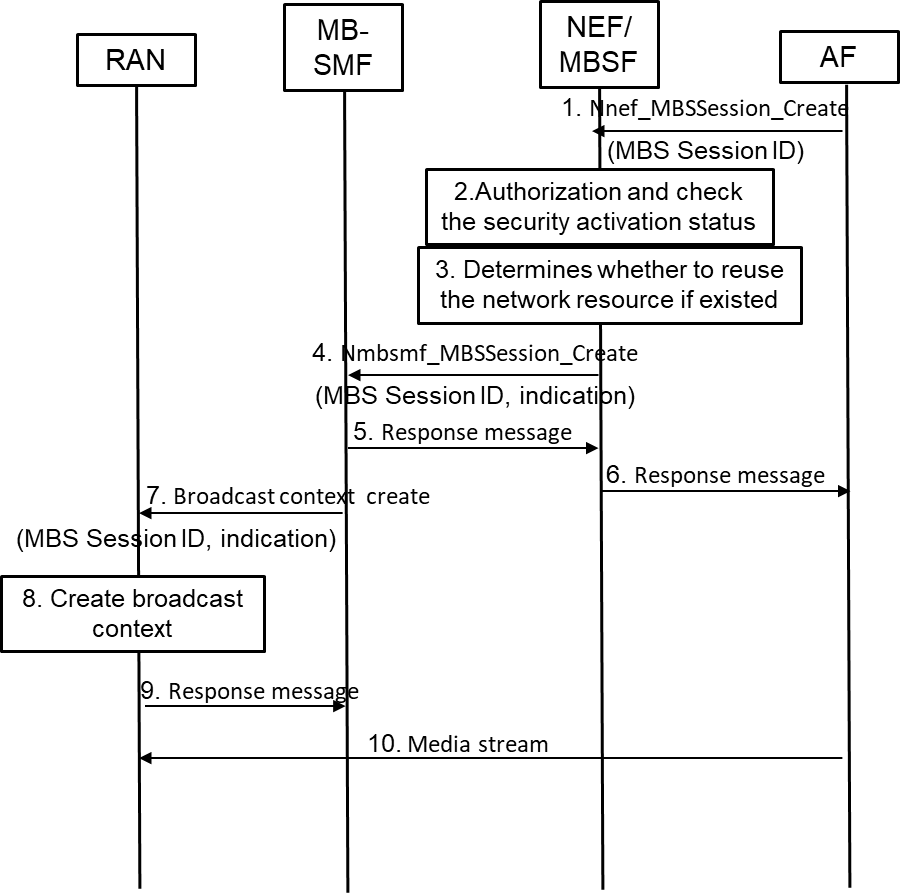


Figure 6.X.2-1 call flow of security protection for UEs in MOCN network sharing scenario

As show in the Figure 6.X.2-1, the details of security protection is summarized as following:

1. AF performs TMGI allocation and MBS session creation as specified in clause 7.1.1.2 or clause 7.1.1.3 of TS 23.247 [6].

2. NEF/MBSF checks authorization of AF. In addition, NEF/MBSF confirms the security activation status for the MBS session. The security activation status implies whether security protection is applied or not.

3. NEF/MBSF determines whether to reuse the network resource for the same service if alreay existed in RAN nodes as specified in TR 23.700-47 [2]. If the security protection is not activated, NEF/MBSF indicates to reuse the network resource. Otherwise, the indication implies to allocate new network resource.

4. NEF/MBSF further provides the indication to MB-SMF.

5-6. Continue the MBS session creation procedure.

7. MB-SMF invokes Namf\_MBSBroadcast\_ContextCreate Request with further including the indication in the N2 SM container received in step 1.

8. NG-RAN node creates a Broadcast MBS Session Context if the Broadcast MBS Session Context does not exist (i.e. the other PLMN network sharing the NG-RAN node has not requested for the same broadcast MBS service to be established at the NG-RAN node) as descripted in TR 23.700-47[2]. If the NG-RAN node already exists, then the NG-RAN node checks the indication.

The NG-RAN node determines whether to use the previously allocated radio resources of the MBS session as suggested by the received indication. When the NG-RAN node receives the DL MBS data of the requested MBS session afterwards, it will not send the received data in the air interface if reusing the network resource. Otherwise, the NG-RAN node treat the session as the newly request session and creates new Broadcast MBS Session Context.

Editor's Note: The description may be updated based on the conclusion of SA2 and RAN groups.

9-10. Continue the procedure as secified in TS 23.247 [6].

### 6.X.3 System impact

TBA

### 6.X.4 Evaluation

TBA

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