**3GPP TSG-SA3 Meeting #108Adhoc-e draft\_S3-222470-r3**

**e-meeting, 10th – 14th October, 2022 merger of S3-222855**

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

**Title:** **Security threat and requirement in MOCN network sharing scenario**

**Document for: Approval**

**Agenda Item: 5.23**

# 1 Decision/action requested

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

# 2 References

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

# 3 Rationale

In R17, the security protection for broadcast is provided in service layer. In R18, optimization is studied for the MOCN network sharing scenario. Similarly, the 5G system needs to protect the traffic in service layer in MOCN network sharing scenario.

# 4 Detailed proposal

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

### 5.1.1 Key issue details

In MOCN network sharing scenario, multiple CNs are connected to the same NG-RAN. As documented in TR 23.700-47 [2], the efficiency of resource utilization for the same broadcast content is studied. For the same broadcast content, the AF will set up multiple broadcast MBS sessions towards those CNs. Each CN will deliver the same content towards the same shared NG-RAN node. The NG-RAN node only delivers one copy of the broadcast content over the air.

As specified in clause W.4 of TS 33.501 [3], user-plane procedure is applicable for broadcast service. MBSTF may protect the traffic transmission with encryption and/or integrity. The security protection of MBS traffic is supported in service layer. In MOCN network sharing scenario, the multiple CNs may enable their own security towards the content. The UE will receive the MBS keys from their serving PLMN. However, the NR-RAN broadcasts only one copy of the content. The security impact needs analysis if security are activated for the same content to be provided to 5G MOCN network sharing scenarios. For example, UEs from PLMN1 may be unable to decipher the content if the NG-RAN node chooses to broadcast the ciphered content from the CN of PLMN2, since the MTK generated and distributed by the PLMN1 may be different from the MTK that will be used by the PLMN2 to protect the MBS traffic.

If the content is protected using CN-specific keys, which is not a serving PLMN for an UE in the shared RAN, then UEs not having the key will fail to properly process the content, should the network send only one of the copies.

### 5.1.2 Security threats

If the content is not protected by application (in another words, CA/DRM does not apply) then reusing the existing security procedure in service layer may cause processing failure in UEs in MOCN network sharing scenario. The UEs will be out of MBS if it is not served by the PLMN that is protecting the MBS traffic, as the UE does not have the appropriate MTK to handle the protected traffic.

### 5.1.3 Potential security requirements

The 5G system may support a mechanism to distribute the appropriate key (key that will be used to protect the MBS content at the service layer) to the UE to handle the protected MBS traffic over the MOCN deployment scenarios..

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