**3GPP TSG-SA3 Meeting #108-e draft\_S3-222066-r2**

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

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

**Title:** **Add threat and requirement to key issue on TMGI protection**

**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

TMGI is a temporary identity. However, since it is being utilized for MBS group paging and its value reused for paging different UEs, as well as being transmitted in cleartext, an eavesdropper may be able to infer the MBS UE group membership. The security threat and requirement are added to address this issue.

# 4 Detailed proposal

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

## 5.2 Key issue#2: TMGI Protection

### 5.2.1 Key issue details

According to TS 23.003 [4] and TS 38.331 [5], TMGI is defined as Temporary Mobile Group Identity. Temporary Mobile Group Identity (TMGI) is used within MBMS to uniquely identify Multicast and Broadcast bearer services. The TMGI is composed of MBMS Service ID, Mobile Country Code (MCC), and Mobile Network Code (MNC).

TMGI is used by the Core Network (CN) of MBS UEs and by MBS UEs as a temporary identity for monitoring of the Paging channel for CN paging if configured by upper layers for MBS multicast reception (e.g., see clause 7.2.5.2 of TS 23.247 [6]).

TMGI is a temporary identity. However, since it is being utilized for MBS group paging and its value reused for paging different UEs, as well as being transmitted in cleartext, the privacy attack and DoS attack may be possible.

### 5.2.2 Security threats

As the TMGI is paged with clear text and it is unchanged after group paging, the attacker can eavesdrop the TMGI which is paged before and spoof the UEs belonging to the group. The UE belongings to the corresponding MBS group may response to this fake group paging message. For example, the idle UEs in the MBS group will unnecessarily resume the connection, which is power consuming.

In addition, an attacker eavesdrop over the paging channel for MBS UEs may be capable of the following privacy attacks:

- inferring members of the MBS group presence in the paging area.

### 5.2.3 Potential security requirements

The 5G system should provide means to mitigate the spoofing attack in which the idle UEs in the MBS group unnecessarily resumes the connection.

The 5G system should provide means to mitigate the privacy attack which infers the members of the MBS group by group paging with TMGI.

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