**3GPP TSG-SA3 Meeting #108Adhoc-e S3-222469-r1**

**e-meeting, 10th – 14th October, 2022**

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

**Title:** **Requirement on TMGI protection**

**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 TS 23.003: "Numbering, addressing and identification".

[2] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification"

[3] 3GPP TS 23.247: "5G multicast-broadcast services; Stage 2".

# 3 Rationale

Based on the discussion in SA3-108e, the proposed requirement is revised accordingly.

# 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

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 may provide means to mitigate the privacy attack which infers the members of the MBS group by group paging with TMGI.

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