**3GPP TSG-SA3 Meeting #107Adhoc -e S3-221396-r2**

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

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

**Title:** **Key issue 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

According to TS 23.003 [1] and TS 38.331 [2], 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 [3]).

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, infer members of the MBS group presence in the paging area, track the UEs belonging to a particular MBS group, and infer when service activation is underway. In addition to the privacy attack, the DoS attack may also be possible.

As discussed in S3-220537, SA3 agreed that SA3 will study the issue further and keep SA2 informed if more progress is made.

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

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

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

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

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

## 5.X Key issue: TMGI Protection

### 5.X.1 Key issue details

According to TS 23.003 [xx] and TS 38.331 [yy], 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 [zz]).

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.X.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.X.3 Potential security requirements

TBA

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