3GPP TSG SA WG 3 Meeting SA3#103e TDoc draft\_S3-211523-r6

Electronic meeting, Online, 17 - 28 May 2021

**Title: Reply LS to LS on broadcasting from other PLMN in case of Disaster Condition**

**Response to: LS C1-211189 on LS on broadcasting from other PLMN in case of Disaster Condition from CT1**

**Release: Rel-17**

**Work Item: FS\_MINT-CT**

**Source:** **SA3**

**To: CT1**

**Cc: RAN2**

**Contact person: Dongjoo Kim**

**dongjoo7.kim@lge.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:** **None**

# 1 Overall description

SA3 thanks CT1 for the LS (C1-211189/ S3-211372) on FS\_MINT-CT being studied in TR 24.811.

SA3 is giving general comments for the two questions in this LS:

**Q1:** Whether receiving and utilizing broadcast information as being studied in TR 24.811 from PLMNs other than the PLMN with Disaster Condition, which can be the home PLMN or a visited PLMN, pose any security risks; and

**A1:** If UE's actions are not specified carefully, there might be security risks because the broadcast information is not protected. For example, a false base station may impersonate PLMN\_Alive.

**Q2:** If the answer to Q1 is yes, then what would be SA3's recommendations from security perspective?

**A2**: Firstly, it must be ensured that the MINT feature is applicable only in absence of PLMN\_Disaster’s coverage. In other words, UE shall \*not\* use the MINT feature as long as the UE detects cells belonging to PLMN\_Disaster or any other allowable/equivalent PLMNs. This will make it difficult for an attacker to succeed in tricking UEs, because it has to nullify all other valid cells in the area.

Secondly, it must be ensured that the UE performs primary authentication and non-null integrity algorithms are activated by the PLMN\_Alive. This can prevent a UE lured by a false base station from registering to the impersonated PLMN as the authentication will fail. Thus, SA3 regards the impact of these security risks as no worse than denial of service to the UE (e.g., MINT service not available).

Therefore, it needs to be decided if these conditions can be met and the DoS threat is acceptable for CT1. If so, no additional security enhancement is needed.

# 2 Actions

**To CT1**

**ACTION:** SA3 kindly asks CT1 to take the above reply into consideration for their subsequent works.

# 3 Dates of next TSG SA WG 3 meetings

SA3#103bis-e 5 - 9 July 2021 Electronic meeting

SA3#104e 16 - 27 August 2021 Electronic meeting