3GPP TSG SA WG 3 Meeting SA3#103e TDoc draft\_S3-211523-r12

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:** Yes, there might be security risks because the broadcast information is not protected. For example, a false base station may impersonate PLMN offering disaster roaming or PLMN with disaster condition.

**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 when UE is out of coverage of or cannot access any allowed PLMNs .

Secondly, it must be ensured that, except for emergency calls, unauthenticated network access (i.e. without primary authentication and NAS/AS SMC with null integrity algorithm) to the PLMN offering disaster roaming is not allowed. This prevents a UE lured by a false base station from using any impersonated PLMN as mutual authentication and security setup will fail. If this is ensured, SA3 regards the impact of impersonation security risks as no worse than denial of service to the UE (e.g., MINT service not available).

Therefore, CT1 needs to decide if above mechanisms can be ensured and unavailability of MINT feature in absence of security setup are acceptable. If so, no additional security enhancement seems to be needed for now, but SA3 would like to look at the overall security of this feature again after the conclusions have progressed.

# 2 Actions

**To CT1**

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

# 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