3GPP TSG SA WG 3 Meeting SA3#103e TDoc draft\_S3-211523-r4

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**

**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 understands that the LS is asking if it is okay for UE belonging to PLMN\_Disaster to trust PLMN\_Alive’s SI message indicating that UEs belonging to PLMN\_Disaster are welcome to roam to PLMN\_Alive. SA3 also understands that the LS is referring to solutions #5, #12, #13, #14, #16, #21, #22, #28, #39, #46 in TR 24.811.

It is difficult for SA3 to analyze these wide array of 10 solutions and comment on each. Therefore, 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. Therefore, it is important that MINT feature cannot be misused by a false base station.

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

**A2**:

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.

SA3 wants to ask CT1 if the core network of PLMN\_Disaster is still up and running?

* If the assumption is that only the RAN is down and the core network is still available, then UE shall perform a fresh registration procedure (triggering primary authentication and NAS/AS SMC) towards PLMN\_Alive. In other words, UE shall not simply camp on PLMN\_Alive's cell.
* Instead, if the assumption is that even the core network is down, then UE has to blindly trust the PLMN\_Alive (no mutual authentication, no NAS/AS SMC). Then the situation is similar to unauthenticated emergency call. It should be noted that a conscious decision is made in this case to prioritize availability and security is unavailable.

SA3 also wants to ask CT1 how roamers are intended to be handled. Could it happen an incoming roamer has no allowable PLMN list (and of course PLMN\_Disaster is not available in a foreign country)? If so, then it could become easier for attacker to lure these incoming roamers.

# 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