**3GPP TSG-SA3 Meeting #115 e-adhoc *draft\_S3-241469-r2***

Online, 15th April – 19th April 2024

**Source: Xiaomi**

**Title: New solution for mitigating GERAN UTRAN bidding down attack**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***It is proposed to approve the pCR to TR 33.701 V0.1.0.***

# 2 References

[1] 3GPP TR 33.701 Study on mitigations against bidding down attacks

# 3 Rationale

This contribution proposes a new solution for TR 33.701 [1].

# 4 Detailed proposal

\*\*\* Start of the Change \*\*\*

## 5.y Solution #y: Solution for mitigating GERAN UTRAN bidding down attack

### 5.y.1 Introduction

This solution addresses the key issue of bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN

In this solution, the network sends the list of 2G/3G supporting PLMNs, list of 2G/3G decommissioning PLMNs, and 2G/3G decommissioning information of home PLMN to the UE.

The aforementioned information is delivered to the UE via registration accept message/UPU procedure.

### 5.y.2 Details



Figure 5.Y.2-1: Procedure for mitigating false base station in 2G/3G decommissioning scenarios

1. The core network function may send a list of 2G/3G supporting PLMNs (list-1), or a list of 2G/3G decommissioning PLMNs (list-2), or 2G/3G decommissioning information of the home network to the UE.

- List-1: the list of 2G/3G supporting PLMNs contains the identities of the PLMNs that still deploy and maintain the radio access technologies of GERAN/GSM and/or UTRA.

* If provided by the HPLMN, the list can contain all the PLMNs that have roaming agreement with the HPLMN and still support 2G/3G. The list may also contain the HPLMN of the UE if the HPLMN still maintains 2G/3G.
* If provided by the serving PLMN, the list can indicate that the serving PLMN which the UE is attached to still maintains 2G/3G.

Editor's Note: Wether List-1 is sent to UE is FFS

- List-2: the list of 2G/3G decommissioning PLMNs contains the identities of the PLMNs that have decommissioned the radio access technologies of GERAN/GSM and/or UTRA.

* If provided by the HPLMN, the list can contain all the PLMNs that have roaming agreement with the HPLMN and have decommissioned 2G/3G. The list may also contain the home PLMN of the UE if the HPLMN has decommissioned 2G/3G.
* If provided by the serving PLMN, the list can indicate that the serving PLMN which the UE is attached to has decommissioned 2G/3G.

- If the home network has decommissioned 2G/3G access technologies, the 2G/3G decommissioning information may include the indication that 2G/3G has been decommissioned in the home network or the indication that UE shall not select all the GERAN/GSM/UTRA cells.

The message in step 1 may be delivered to the UE via the registration accept message or UPU procedure.

1. If the UE receives the list of 2G/3G supporting PLMNs, the UE shall only select the GSM/GERAN/UTRA cells broadcasting the PLMN IDs in list-1 (because the GSM/GERAN/UTRA cell broadcasting the PLMN ID not in list-1 is considered to be forged by a false base station).

If the UE receives the list of 2G/3G decommissioning PLMNs, the UE shall not select the GSM/GERAN/UTRA cells broadcasting the PLMN IDs in list-2 (because the GSM/GERAN/UTRA cell broadcasting the PLMN ID in list-2 is considered to be forged by a false base station).

NOTE 1: In case the false base station forges a GSM/GERAN/UTRA cell broadcasting the PLMN ID not in the list-2, the combination of list-1 and list-2 can be used by the UE to detect the fake cell.

If the UE receives the 2G/3G decommissioning information of the home network, the UE shall not select the GSM/GERAN/UTRA cell (because the HPLMN does not support a successful 2G/3G AKA for the UE).

NOTE 2: The information received by the UE for mitigating false base stations takes precedence over the information of PLMN/access technologies combination infromation configured in the UICC.

### 5.y.3 Evaluation

This solution is not work for legacy UEs.

This solution has impacts on UE.

* The UE may receive list of 2G/3G supporting PLMNs (i.e. list-1).
* The UE may receive the list of 2G/3G decommissioning PLMNs (i.e. list-2)
* The UE may receive the 2G/3G decommissioning information of home PLMN
* If home PLMN has completed the 2G/3G decommissioning, the UE shall not select the GSM/GERAN/UTRA cell (because the HPLMN does not support a successful 2G/3G AKA for the UE).
* If the UE receives the list of 2G/3G supporting PLMNs, the UE shall only select the GSM/GERAN/UTRA cells broadcasting the PLMN IDs in list-1
* If the UE receives the list of 2G/3G decommissioning PLMNs, the UE shall not select the GSM/GERAN/UTRA cells broadcasting the PLMN IDs in list-2

This solution has impacts on registration procedure or UPU procedure.

The list of 2G/3G supporting PLMNs, list of 2G/3G decommissioning PLMNs, and the HPLMN 2G/3G decommission information may be delivered to the UE via UPU procedure or registration accept message.

If UPU is used, this solution only works in 5G.

\*\*\* End of the Change\*\*\*