|  |
| --- |
| 3GPP TR 33.701 V1.1.0 (2024-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on mitigations against bidding down attacks(Release 19) |
|   |
|  | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Key issues 8

4.1 Key Issue #1: Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN 8

4.1.1 Description 8

4.1.2 Threats 8

4.1.3 Potential requirements 9

5 Solutions 9

5.1 Solution #1: Securely notification to UE when the GERAN/UTRAN networks are decommissioned 9

5.1.1 Introduction 9

5.1.2 Details 9

5.1.3 Evaluation 9

5.2 Solution #2: Provisioning of information on restricted RAT types using NAS message 10

5.2.1 Introduction 10

5.2.2 Details 10

5.2.3 Evaluation 10

5.3 Solution #3: Mitigation against bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN 11

5.3.1 Introduction 11

5.3.2 Details 12

5.3.3 Evaluation 13

5.4 Solution #4: Solution for mitigating GERAN UTRAN bidding down attack 13

5.4.1 Introduction 13

5.4.2 Details 13

5.4.3 Evaluation 14

5.5 Solution #5: Solution for access restrictions to decommissioned UTRAN and GERAN 15

5.5.1 Introduction 15

5.5.2 Details 15

5.5.3 Evaluation 16

5.6 Solution #6: Using allowlist to avoid bidding down attack from LTE/NR to decommissioned GERAN/UTRAN 16

5.6.1 Introduction 16

5.6.2 Details 16

5.6.3 Evaluation 16

5.7 Solution #7: Registration-based provisioning of decommissioned system list 16

5.7.1 Introduction 16

5.7.2 Details 16

5.7.3 Evaluation 17

5.8 Solution #8: UPU-based provisioning of decommissioned system list 18

5.8.1 Introduction 18

5.8.2 Details 18

5.8.3 Evaluation 19

5.9 Solution #9: Reuse SoR procedure for bidding down attack mitigation 19

5.9.1 Introduction 19

5.9.2 Details 19

5.9.3 Evaluation 20

5.10 Solution #10: Solution for configured operator indication 20

5.10.1 Introduction 20

5.10.2 Details 20

5.10.3 Evaluation 21

5.11 Solution #11: Solution to prevent GERAN/UTRAN bidding down attack using UICC Configuration 21

5.11.1 Introduction 21

5.11.2 Details 21

5.11.3 Evaluation 21

5.12 Solution #12: Solution to prevent bidding down to GERAN/UTRAN by restricting inter RAT handover 21

5.12.1 Introduction 21

5.12.2 Solution details 22

5.12.3 Evaluation 23

5.13 Solution #13: Solution to prevent bidding down by restricting UE access to GERAN/UTRAN in its location 23

5.13.1 Introduction 23

5.13.2 Solution details 23

5.13.3 Evaluation 25

5.14 Solution #14: configuration in UE per country 25

5.14.1 Introduction 25

5.14.2 Details: 26

5.14.3 Evaluation 26

5.15 Solution #15: Mitigation of Roaming Attack based on UE Implementation 27

5.15.1 Introduction 27

5.15.2 Solution details 27

5.15.2.1 PLMN Selection Logic 27

5.15.2.2 Mitigation of Attack Scenario 1 27

5.15.2.3 Mitigation of Attack Scenario 2 28

5.15.3 Evaluation 28

5.16 Solution #16: configuration in UE 28

5.16.1 Introduction 28

5.16.2 Details: 28

5.16.3 Evaluation 29

6 Conclusion 29

Annex <A> (informative): Guidance for legacy devices 30

A.1 Description 30

A.2 Approaches 30

A.2.1 Approach #1: Raising user awareness 30

A.2.x Approach #x: <Title of the proposal> 30

Annex <X> (informative): Change history 32

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

# 1 Scope

The present study focuses on mitigating bidding down attack, i.e. how to prevent UEs that are currently connected to LTE/5G from establishing a connection with a GERAN/UTRAN FBS considering for example the decommissioning of GERAN and UTRAN networks. In particular, the study aims at:

* Identifying attack scenarios and threats in the context of decommissioning of GERAN and UTRAN networks, e.g. cell (re)selection or forced handovers on GERAN or UTRAN once LTE and 5G signalling are blocked when GERAN/UTRAN networks are decommissioned; and
* Documenting solutions for the identified security threats and requirements.

# 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".

[2] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[4] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[5] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[6] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

AMF Access and Mobility management Function

AUSF AUthentication Server Function

CSS Cell Site Simulator

FBS False Base Station

GSMA GSM Association

NR New Radio

SMC Security Mode Command

SoR Steering of Roaming

TAI Tracking Area Identifier

UDM Unified Data Management

UICC Universal Integrated Circuit Card

UPU UE Parameter Update

# 4 Key issues

## 4.1 Key Issue #1: Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN

### 4.1.1 Description

The GERAN and UTRAN decommissions are part of a global trend. Operators are currently decommissioning legacy infrastructure from their networks. Decommissioning is a phased approach which entails legacy infrastructure is gradually phased out from the network.

As GERAN and UTRAN uses weak encryption between the base station and the UE, the communication can be cracked in real time by an attacker to intercept calls or text messages. Known vulnerabilities of 2G are: one way authentication, 2G algorithms such as A5/0 (no confidentiality), compromised algorithms A5/1 and A5/2 (GSMA deprecated in 2006), no inherent integrity protection over the air, and authentication and ciphering over the air are optional to implement. In terms of 3G, known vulnerabilities are: IMSI is still sent in clear text in initial RRC connection request; also, if TMSI is not recognized by the network, then UE is forced to reveal IMSI in clear text, user plane is not integrity protected, messages sent before Security Mode Command (SMC) are not integrity protected, etc.

In a scenario where the operator has decommissioned GERAN and UTRAN networks, the UE cannot determine on its own that such radio access networks are no longer available in certain areas. Therefore, if 5G-NR and LTE networks are being blocked by an attacker, the UE can fall back to selecting and connecting to false UTRAN and GERAN base stations.

When UE is in an area with no coverage of 5G-NR or LTE, an attacker capable of mounting a false UTRAN/GERAN in the same area will be successful in making the 5G-NR and LTE UE camp on the false UTRAN/GERAN based on the signal strength. Further, in GERAN there is no authentication of the base station to the device, which means that anyone can seamlessly impersonate as a legit GERAN base station. Therefore, if 5G-NR and LTE networks are being blocked by an attacker, a UE can fall back (bid-down) to selecting and connecting to false GERAN/UTRAN base stations.

### 4.1.2 Threats

One such attack scenario is, if the MNO is only 5G-NR operator, then the UE camping on the GERAN Cell Site Simulator (CSS) mounted by an attacker may provide the IMSI in clear, which allows the attacker to bind the UE and the IMSI to track the UE location in the 5G network (if the home network has configured "null-scheme" to be used).

Further, UE connecting to a UTRAN or GERAN FBS is vulnerable to bidding down attacks, e.g. fraudulent SMS or phone calls, which could cause significant financial losses for subscribers.

The FBS can also make use of a PLMN-ID that is different from the home operator, while at the same time blocking the UE from accessing the home network operator's PLMN. This means, that the radio interface of the UE experiences a roaming scenario without actually moving.

### 4.1.3 Potential requirements

UE and the EPS/5GS should support mechanisms to mitigate bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN by an attacker over the air interface.

# 5 Solutions

## 5.1 Solution #1: Securely notification to UE when the GERAN/UTRAN networks are decommissioned

### 5.1.1 Introduction

This solution addresses the security requirement in key issue#1 on securely notification to UE when the GERAN or UTRAN networks are decommissioned.

### 5.1.2 Details

The UE performs the registration procedure when it is connecting to the LTE or 5G network. During this procedure, the network indicates to the UE about the information on whether GERAN or UTRAN is decommissioned in a secure message, i.e., Registration Accept.

The current Registration Accept message content is referring to Clause 8.2.7 in TS 24.501[6]. With the new indication, the new Registration Accept message is as below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Registration accept message identity | Message type9.7 | M | V | 1 |
|  | 5GS registration result | 5GS registration result9.11.3.6 | M | LV | 2 |
| 77 | 5G-GUTI | 5GS mobile identity9.11.3.4 | O | TLV-E | 14 |
| …… |
| 13 | List of PLMNs to be used in disaster condition | List of PLMNs to be used in disaster condition9.11.3.83 | O | TLV | 2-n |
| TBD | List of decommissioned RAT | List of decommissioned RAT | O | TLV | 2-n |

This service is supposed to be provided for all the UEs when operators enable it. The UE ensures that no connection is established with decommissioned RATs.

Editor’s Note: How UE ensures this is FFS.

### 5.1.3 Evaluation

This solution addresses the security requirement in key issue#1 with the impact only on UE and AMF. This solution applies to both LTE and 5G networks. The network uses a Registration Accept message to send the list of decommissioned RATs to the UE during a general UE Registration Procedure.

This solution clarifies that the UE establishes a secure connection with the network using active RATs not on the decommissioned list.

This solution is not applied to legacy UEs.

## 5.2 Solution #2: Provisioning of information on restricted RAT types using NAS message

### 5.2.1 Introduction

This solution addresses the security requirement of key issue#1. As the decommissioning can be performed in a phased manner by the MNO, this solution details a mechanism to inform the UE whether in that particular region (Tracking Area (TA)) network supports GERAN and/or UTRAN.

### 5.2.2 Details

In this solution, the network notifies the UE during Attach/Registration procedure (for the TAI/list of TAIs included in the Attach/Registration accept message or for the entire PLMN).



**Figure 6.2.2-1: UE is notified about the restricted RAT types (GERAN/UTRAN) in Attach/Registration accept message**

During attach or registration procedure the network indicates to the UE about the information on restricted RAT types (i.e., GERAN/UTRAN) in attach or registration accept message for the TAI or included list of TAIs or for the entire PLMN, as shown in Figure 6.2.2-1. The restricted RAT types are excluded in any follow-up procedures by the UE.

### 5.2.3 Evaluation

This solution addresses key issue#1 to prevent UE from bidding down attack from fake GERAN/UTRAN.

Impacts:

1. The solution has impact on the UE and the AMF/MME.
2. This solution does not address the problem for legacy devices
3. This solution works even in roaming scenarios.
4. This solution uses TA for information on decommissioned RATs, when the network performs decommissioning in a phased manner.

## 5.3 Solution #3: Mitigation against bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN

### 5.3.1 Introduction

This solution proposes the following:

* When UE sends NAS registration request to the 5G core network, after successful NAS security context establishment with serving network, the serving network sends decommissioned RATs information to the UE along with registration accept message.
	+ In case of LTE, similar information can be included along with successful response to attach message.
* When UE receives this information about decommissioned RATs, it updates the cell search criteria to ensure that decommissioned RATs are not selected during cell search.
* After this information is available with the UE, till it moves to another serving network where such decommissioned RATs information is either empty or different, UE can ignore any redirection message to move the UE to any of the decommissioned RATs.
* When UE moves to another serving network, if it receives an empty list or a different list of decommissioned RATs, it updates the cell search criteria accordingly.

### 5.3.2 Details



Figure 6.3.1-1: Message flow showing steps to avoid UEs from connecting to decommissioned RATs

In the above message flow, the message flow till NAS Security context establishment is as per legacy procedures. This message flow includes the possible scenario when, as soon as UE powers on, UE connects with a FBS which can perform bidding down attack to a decommissioned RAT.

* After NAS registration is complete, as part of NAS registration accept, the serving network informs the UE about the decommissioned RATs.

UE updates the cell search criteria according to the list of decommissioned RATs to ensure that it does not select any cell belonging to those RATs.

* After UE moves to RRC Idle state, when it goes through the RRC connection procedure again and if it receives RRC redirection message attempting to redirect the UE to 2G/3G RAT, it can ignore that message.

NOTE: The UE gets the information about decommissioned RATs and uses it to prevent insecure downgrades. How the UE does this is up to the implementation.

Editor's Note: whether an FBS can redirect the connected victim UE to 2/3G RATs is FFS.

### 5.3.3 Evaluation

This solution ensures that when UE is roaming, it receives the list of decommissioned RATs from the serving network. UE uses this information to update the cell search criteria, and hence, this ensures that the UE does not connect to decommissioned RATs. Also, UEs can use this information to ignore redicrection messages.

This solution does not address the problem for legacy devices.

This solution impacts UEs and Core Network entities (serving AMF). Also, operators need to configure the decommissioned RAT information in serving AMFs according to the areas where older RATs are decommissioned.

## 5.4 Solution #4: Solution for mitigating GERAN UTRAN bidding down attack

### 5.4.1 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.

### 5.4.2 Details



Figure 5.4.2-1: 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.

Editor's Note: it is FFS whether it is practical for an operator to maintain a list of decommissioned networks for all roaming partners

Editor's Note: it is FFS whether it is practical for a network to provide this huge list to the UEs.

Editor’s Note: Whether and how a serving PLMN should have an agreement with the PLMNs that have a roaming agreement with HPLMN is FFS.

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).

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 1: 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.

Editor’s Note: Whether and how the list can be maintained effectively such that a complete list of all roaming partners is available to the UE at the right time is FFS.

### 5.4.3 Evaluation

This solution is not work for legacy UEs.

This solution has impacts on UE.

Sending one or more of the lists impacts both the UE and the network. In particular, it impacts the UE and the AMF and the UDM function in the core network

* 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
* Including information on whether the serving PLMN supports 2G/3G in List-1 is optional.
* 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.

In other words, the AMF includes in the Registration Accept message, one or more lists and sends it to the UE. After the UE receives the list, it can decide to establish a PDU session based on the list. Similarly, the information collected from the HPLMN may impact the UE routing parameter in the UDM of the VPLMN/SPLMN when the UE is visiting a different PLMN. The UE routing parameter information in the UDM may be sent to the UE via the AMF using the UE Parameter Update procedure. Once received, the UE will store the Updated Routing Parameter in the UICC.

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

## 5.5 Solution #5: Solution for access restrictions to decommissioned UTRAN and GERAN

### 5.5.1 Introduction

This solution address KI#1.

### 5.5.2 Details

The solution describes how a UE is provisioned with decommissioned UTRAN and GERAN access restriction information to avoid UTRAN/GERAN selection (e.g., when NR/LTE signal is unavailable). The UTRAN and GERAN access restriction information (i.e., list of restricted RAT specific to decommissioned UTRAN, decommissioned GERAN) can be sent to the UE in any NAS message following the establishment of NAS security.

The UDM/UDR based on operator’s local policy manages GERAN and UTRAN access restriction information for the UE(s) (e.g., in the subscription data as part of UE Access and mobility context).

NOTE 2: The UDM/UDR already manages Mobility restrictions and RAT restriction information for the UE(s) in the subscription data as part of UE Access and mobility context (described in TS 23.501 [4] Clause 5.3.4.1). It is upto the normative work to determine if the decommissioned UTRAN and GERAN access restriction can be managed along with the existing information, as part of UE Access and mobility context or any new information category is needed. Further any additional granularity of information if any needed as part of UTRAN and GERAN access restriction information can be upto the normative work.

During UE registration, the AMF fetches the GERAN and UTRAN access restriction information (i.e., using Nudm\_SDM\_Get/response as in TS 23.502 [2] step 14b in clause 4.2.2.2.2 or using any Nudm service), which indicates UTRAN access restriction/not allowed, and GERAN access restriction/not allowed information.

The AMF stores the received network access restriction information as part of UE context and provides the network access restriction information to UE in a secured NAS message (i.e., such as Registration Accept messaage).

#As alternative way, the AMF based on operator local policy can be configured with GERAN and UTRAN access restriction information, in such case UDM involvement described above is not applicable.

The UE stores the received information (if it can process i.e., if it is not a legacy device) and determines not to select the UTRAN or GERAN access based on the received network access restriction information.

NOTE 3: Legacy UEs cannot understand this new information, so it may be dropped with no action from the UE.

### 5.5.3 Evaluation

The solution addresses KI#1 by reusing the principles of existing access restrictions and includes the following impact:

Network: Solution provides 2 options, i.e., option-1 which impacts UDM and AMF; option-2 which impacts only AMF on the network side i.e., to fetch and provide UE with the network access restriction information that includes UTRAN and GERAN access restrictions for the decommissioned networks.

UE: The UE on receiving network access restriction information determines not to select decommissioned UTRAN and GERAN.

This solution does not address the problem for legacy devices.

## 5.6 Solution #6: Using allowlist to avoid bidding down attack from LTE/NR to decommissioned GERAN/UTRAN

### 5.6.1 Introduction

This solution addresses the security requirement in Key Issue #1: Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN.

### 5.6.2 Details

During the registration procedure of a UE registering 5G network, the network provides the UE the allowlist of networks, i.e., the allowed RAT types of the current serving PLMN, in the Registration Accept message. If the operator has decommissioned GERAN and UTRAN networks, only 4G and/or 5G networks are listed.

Upon receiving the message, UE does not connect to the network whose RAT types are not in the allowlist of the networks.

### 5.6.3 Evaluation

This solution has impacts on AMF and UE and does not address the problem for legacy devices.

Impacts on the AMF:

* The AMF needs to add a new information element indicating the allowlist of available networks to the Registration Accept message.

Impacts on the UE:

* The UE does not connect to the networks that are not in the allowlist of the networks.

## 5.7 Solution #7: Registration-based provisioning of decommissioned system list

### 5.7.1 Introduction

This solution addresses key issue #1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN". The solution introduces a new IE in the registration accept message to signal to the UE the list of decommissioned systems.

### 5.7.2 Details

It is assumed that the AMF is pre-configured with a list of 3GPP radio technologies that the PLMN does no longer support. Based on this configuration and once a registration procedure is successfully completed, the AMF includes a new parameter in the Registration Accept message to indicate to the UE which 3GPP access technologies to no longer select as long as the UE is registered in the current PLMN. Since the Registration Accept is sent after NAS security establishment, there are no risks that the indication is tampered with. This new parameter which is referred to as the List of Decommissioned 3GPP Access Technologies (LDAT) in the procedure below contains a list of RATs that are decommissioned and hence no longer supported by the serving PLMN. In this context, the LDAT includes GERAN or UTRAN or both.

Figure 5.7.2-1 illustrates the impact on the current registration procedure. The step description is included below



**Figure 5.7.2-1: Registration procedure including provisioning of LDAT parameter**

1. The AMF is preconfigured with a List of Decommissioned 3GPP Access Technologies (LDAT).
2. The UE initiates the procedure by sending a Registration Request message.
3. The AMF potentially triggers a primary authentication and establishes NAS security with the UE. From this step onwards, all NAS traffic is confidentiality and integrity protected.
4. The remaining steps of the registration procedure are performed as specified in TS 23.502 [2] with no changes for this solution except for the last message as described in step 4.
5. The AMF concludes the procedure by sending a Registration Accept message including the LDAT information.

NOTE: Details of the LDAT parameters such as whether it is a simple list of 3GPP radio access technologies or more granular e.g. a list per tracking area, is left to CT1 group.

1. The UE stores the LDAT information and removes any previously received one (if any). The stored LDAT information is bound to the PLMN. The UE acts on it accordingly during 3GPP access selection as long as the UE is registered over 3GPP access in that PLMN.

### 5.7.3 Evaluation

The solution addresses the requirement of key issue #1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN".The solution does not provide a mechanism to address backward compatibility issues with UEs not supporting this additional NAS IE.

The solution is not limited to a specific technology and can achieve the same effect irrespective of the target 3GPP access technology.

Since the LDAT information is under the control of the AMF, the solution works even in roaming scenarios.

Depending on the LDAT format (see NOTE in clause 5.7.2), the extent of impact and complexity especially on the UE side may vary considerably.

The solution has impact on UE and AMF and does not solve the problem for legacy devices.

## 5.8 Solution #8: UPU-based provisioning of decommissioned system list

### 5.8.1 Introduction

This solution addresses key issue #1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN". The solution introduces a new IE in the UPU data to signal to the UE the list of decommissioned systems.

### 5.8.2 Details

It is assumed that the UDM is pre-configured with a list of 3GPP radio technologies that the PLMN does no longer support. Based on this configuration and once a registration procedure is successfully completed, if the UDM invokes the UPU procedure, it can include a new parameter in the UPU data to indicate to the UE which 3GPP access technologies to no longer select as long as the UE is registered in the current PLMN. Since the UPU Data is transported over NAS after successful security establishment, there are no risks that the indication is tampered with. This new parameter which is referred to as the List of Decommissioned 3GPP Access Technologies (LDAT) in the procedure below contains a list of RATs that are decommissioned and hence no longer supported by the serving PLMN. In this context, the LDAT includes GERAN or UTRAN or both.

Figure 5.8.2-1 below illustrates the impact on the current UE parameter update procedure. The step description is included below



**Figure 5.8.2-1: UE parameter update procedure including provisioning of LDAT parameter**

1. The UDM is preconfigured with a List of Decommissioned 3GPP Access Technologies (LDAT). the details on the LDAT data storage in UDM/UDR are left out of scope of this solution (can be clarified during the normative work or left to stage 2/3 details).
2. The UE and the network completes a successful registration procedure including Primary authentication and NAS security establishment.
3. If the UDM decides to invoke the UE parameter procedure of clause 6.15 of TS 33.501 [3], based on operator policy, the UDM includes the LDAT information in the UPU data, alongside the other parameters.

NOTE: Details of the LDAT parameters such as whether it is a simple list of 3GPP radio access technologies or more granular e.g. a list per tracking area, is left to CT1 group.

1. The remaining steps of the UE parameter update procedure are unchanged.
2. The UE stores the LDAT information and removes any previously received one (if any). The stored LDAT information is bound to the PLMN. The UE acts on it accordingly during 3GPP access selection as long as the UE is registered over 3GPP access in that PLMN. The UE does not select any RAT that is included in the stored LDAT information when served by that PLMN.

### 5.8.3 Evaluation

The solution addresses the requirement of key issue #1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN".

The solution does not provide a mechanism to address backward compatibility issues with UEs not supporting this additional IE.

The solution requires that UPU is deployed which is not necessarily the case on the network side.

The solution is not limited to a specific technology and can achieve the same effect irrespective of the target 3GPP access technology.

Since the LDAT information is under the control of the UDM, the solution works only for non-roaming scenarios.

Depending on the LDAT format (see NOTE in clause 5.8.2), the extent of impact and complexity especially on the UE side may vary considerably.

The solution has impact on UE, AMF and UDM and does not solve the problem for legacy devices.

The solution does not address the issue for EPS.

This solution cannot be used in Roaming, unless the solution is updated to support the UDM gets the LDT list of visiting networks.

## 5.9 Solution #9: Reuse SoR procedure for bidding down attack mitigation

### 5.9.1 Introduction

The solution addresses the key issue #1 “Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN”.

The solution proposes to reuse the existing SoR procedure to inform the UE of the network status (whether the RAT is valid or invalid), and introduces UE-side control so that users can choose to enable or disable this feature.

### 5.9.2 Details

Steering of roaming (SoR) allows the HPLMN to update the "Operator Controlled PLMN Selector with Access Technology" list in the UE by providing the HPLMN protected list of preferred PLMN/access technology combinations via NAS signalling, which is described in Annex C (normative) in TS 23.122 [5].

After the operator has decommissioned the GERAN or UTRAN, they can reuse the existing SoR procedures to notify the UE to update the "Operator Controlled PLMN Selector with Access Technology," which indicates the PLMN list and whether the related access technology is valid or invalid. The SoR transparent container is described in 9.11.3.51 in TS 24.501 [6].

The UE will use this list for PLMN selection, as outlined in clause 4.4.3.1.1 in TS 23.122 [5]. The order of priority for PLMN selection is: 1) available HPLMN or EHPLMN; 2) user-controlled list; 3) operator-controlled list (updated by the SoR procedure); 4) other PLMN/RAT with high quality; 5) other PLMN/RAT in order of decreasing signal quality; 6) disaster condition (only if UE support MINT).

However, the UE can still select the PLMN/RAT not included in the operator-controlled list as for 4) and 5), which may lead to a bidding down attacks due to a potential decommissioned RAT and FBS. Thus, it is proposed that the user can configure the UE to support bidding down attack mitigation, and once it is activated, the UE shall not select the RATs that are invalid in the network according to the operator-controlled list, e.g. for the PLMN/RAT in case 4) and 5).

NOTE: It is left to UE implementation whether the user can configure the UE to support bidding down attack mitigation.

### 5.9.3 Evaluation

The solution addresses key issue #1 “Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN”.

The solution only has UE impact: enhancements on network/RAT selection if UE activates to support bidding down attack mitigation.

The solution reuses the existing SoR procedure to update the decommission PLMN/RAT information, and only enhances the PLMN/RAT selection on UE side based on received decommission information. The solution does not affect the network side. The solution requires SoR solution is deployed.

This solution does not address the problem for legacy devices.

This solution is working in 5G, and is not working in LTE.

Editor’s Note: Whether the solution can work in non-roaming case should be clarified and should be checked with CT1.

## 5.10 Solution #10: Solution for configured operator indication

### 5.10.1 Introduction

This solution addresses key issue #1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN". The solution focuses on the scenario where all GERAN and UTRAN has been decommissioned in a given PLMN.

### 5.10.2 Details

If all GERAN and UTRAN has been decommissioned in a PLMN, the operator configures an indication on the UE. The indication is bound to the operator's PLMN ID and indicates to the UE that GERAN and UTRAN access technologies have been decommissioned. Based on this indication and the location information inside ME, when the UE is in the area of those PLMNs, UE can avoid the connection to GERAN/UTRAN cells under those PLMNs.

When there is a false base station claiming to be a GERAN/UTRAN cell from other PLMN (i.e. not in the configured list of decommissioned RATs), UE can decline this cell based on the location information.

How the indication is configured on the UE is left to out of band mechanisms or to other solutions for provisioning such information from the network. Observe, that any such mechanisms need to be secure so that the UE is not mislead into selecting still available access technologies.

NOTE: For example, the out of band mechanisms can be OTA, or other offline configuration

### 5.10.3 Evaluation

The solution addresses the requirement of key issue #1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN".

The solution is limited to GERAN and UTRAN access technologies and is used only when all GERAN/UTRAN has been decommissioned.

The solution has only impact on the UE. Since the solution does not take stand on the provisioning mechanism, the impact on the network if any is for further study. In case the provisioning is left to out of band mechanisms, then network impact is limited. Furthermore, this would be beneficial even in roaming scenarios UE for serving PLMNs supporting similar out of band mechanisms.

Leaving the configuration to out of band mechanisms incurs an operational burden for the operator. Furthermore, for the roaming scenarios to work, the solution assumes an alignement of the so called out of band mechanisms. This, in practice, is very unlikely relying on a standardized mechanism.

This solution depends on the correctness and security of the location information, which is hard to be achieved by UE.

## 5.11 Solution #11: Solution to prevent GERAN/UTRAN bidding down attack using UICC Configuration

### 5.11.1 Introduction

This solution addresses the security requirement of key issue#1.

### 5.11.2 Details

If the HPLMN completed the decommissioning or network supports LTE and/or NR only, then the UICC is pre-configured with the information on restricted RAT types (i.e., GERAN/UTRAN) for the entire HPLMN. The UE excludes the combination HPLMN and restricted RAT types of the HPLMN for any PLMN/Cell (re)selection procedures.

### 5.11.3 Evaluation

This solution addresses key issue#1 to prevent UE from bidding down attack from fake GERAN/UTRAN.

Impacts:

1. The solution has impact on the UE to store and use the preconfigured information on restricted RAT types in the HPLMN.
2. This solution does not address the problem for legacy devices
3. The UICC configuration based solution is only limited to the non-roaming scenarios.

## 5.12 Solution #12: Solution to prevent bidding down to GERAN/UTRAN by restricting inter RAT handover

### 5.12.1 Introduction

The proposed solution addresses the security requirement of key issue#1 "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN". The security requirement states: " UE and the 5GS should *support mechanisms* to mitigate bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN by an attacker *over the air interface*."

The proposed solution introduces a *mechanism* where the AMF/MME provides guidance to the RAN for RAN to prevent UE's inter-RAT handover, thus prevents being lured to GERAN/UTRAN false base station operating at higher power (resulting into better RSRP) and with better quality signal (resulting into better RSRQ) to lure the UE.

### 5.12.2 Solution details

The AMF/MME in the Core Network (CN) maintains mapping of RAT per location. For example, this mapping could be a table comprising TAI and RAT information from 5.12.2-1.

The eNB/ ng-eNB nodes in the Radio Access Network (RAN) enforce the security policy for preventing bidding down by restriction inter-RAT handover to GERAN/UTRAN in location where PLMN has removed GERAN/UTRAN RAT.

The proposed solution does not inform about the absence of GERAN/UTRAN Radio Access Technologies (RAT) to UE. Instead, the CN informs the RAN so that the source ng-eNB/eNB decides not to let the inter RAT handover related procedures take place in the RAN where the UE is located.

1. The AMF/MME learns about UE's location based on UE's location update procedure.

 The CN maintains information about the availability of different RAT per location for example, by a table 5.12.2-1 that maps UE's location represented by Tracking Area Identity (TAI) with present/absent flag for GERAN/UTRAN.

2. If the GERAN/UTRAN is absent in UE's TAI, the AMF/MME informs eNB/ ng-eNB for eNB/ ng-eNB to decide to not let inter RAT mobility take place in UE's location represented by NCGI/ECGI in RAN.

The AMF/MME uses NGAP/S1AP protocol signaling to pass this information to RAN nodes.

NOTE: The solution does not provide specifics related to attack vectors that manifests into a security risk as to how source base station of a PLMN is manipulated to talk to potential False Base Station of an adversary operating in GERAN/UTRAN.



Figure 5.12.2-1: CN instructs RAN not to let inter RAT mobility happen

|  |  |  |
| --- | --- | --- |
| TAI as AMF/MME sees UE location | NCGI/ECGI as RAN sees UE location | Policy Check at AMF/MME |
| PLMN | TAC | PLMN | NCI/ECI | GERAN/UTRAN presence/absent |
| MCC | MNC |   | MCC | MNC | gNB/eNB id | Cell id | RAT-Indicator |
| 234 | 99 | 1 | 234 | 99 | 123 | 10 | Y |
| 234 | 99 | 2 | 234 | 99 | 456 | 20 | Y |
| 234 | 99 | 3 | 234 | 99 | 789 | 30 | N |
| 208 | 34 | 1 | 208 | 34 | 123 | 40 | Y |
| 208 | 34 | 2 | 208 | 34 | 456 | 50 | Y |
| 240 | 99 | 3 | 240 | 99 | 777 | 60 | Y |

Table 5.12.2-1: CN policy table screening UE location

### 5.12.3 Evaluation

The solution prevents inter RAT handover of a UE by keeping RAT bidding down security policy enforcement in the RAN. It's the core network that provides guidance to the RAN to not let inter RAT handover to GERAN/UTRAN take place.

The solution assumes the UE is a registered UE in the PLMN.

The solution does not require changes to UE. The solution does not solve security requirement of KI#1 for legacy UE that only can access GERAN/UTRAN. Also, legacy UE would not have camped on ng-eNB/eNB to begin with.

The solution works for UE in CM-CONNECTED/RRC CONNECTED states, but not for UE in RRC IDLE/RRC INACTIVE/CM-IDLE modes where UE triggers mobility by cell (re)selection without involving the network.

The solution ties the UE's location and the available RAT absence absent/presence in an 'allowed list'. Thus, the solution prohibits inter RAT handover to GERAN/UTRAN where PLMN has removed GERAN/UTRAN, while still allowing inter RAT handover elsewhere.

The solution effectiveness to mitigate security risk may be impacted if the False Base Station operating in GERAN/UTRAN falsifies its location information.

Also, if the RAT is not in the list, the PLMN RAN will not let inter RAT mobility to any other RAT in UE's location. The solution scope could be expanded to non-3GPP RATs such as CDMA, CDMA-2000, W-CDMA, non-3GPP untrusted radio, WiMax etc.

The solution properties allow it to work in roaming scenarios if serving PLMN's CN and RAN interoperate to prevent inter RAT handover in a location where restricted RAT is not supposed to be operational in UE's reported location.

Impacted network functions/entities: AMF, MME, eNB, ng-eNB

Impacted 3GPP communication protocols: NGAP, S1AP

## 5.13 Solution #13: Solution to prevent bidding down by restricting UE access to GERAN/UTRAN in its location

### 5.13.1 Introduction

The proposed solution addresses the security requirement of key issue#1: "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN".

### 5.13.2 Solution details

The AMF/MME in the Core Network (CN) maintains the RAT availability information for GERAN/UTRAN presence/absence per location, for example in a table 5.13.2-1 that maps location represented by Tracking Area Identity (TAI) with present/absent flag for GERAN/UTRAN. Accordingly, the CN informs the UE, therefore subsequent action by the UE not accessing GERAN/UTRAN in its location if PLMN's GERAN/UTRAN does not exist in UE's location. The CN nodes AMF/MME learns about UE's location based on UE's location update.

The proposed solution addresses UEs both in CM-CONNECTED and CM-IDLE mode in UE's last known location.

If the UE is in CM-IDLE mode in the CN, means UE is in RRC IDLE mode in the RAN. In this mode, UE does not have RRC connection with the radio network and does not have active NAS signalling with CN. Therefore, the network uses paging to reach out to UEs in a location where GERAN/UTRAN is removed.

As shown in the figure 5.13.2-1;

1. AMF detects that change in UE configuration is needed for access and mobility management. AMF pages the UEs in CM-IDLE/RRC IDLE in a location where GERAN/UTRAN is removed. As a result, UEs are expected to transition to CM-CONNECTED state to receive information from the CN. Alternatively, the UE could already be in CM-CONNECTED/RRC CONNECTED state.

 If the GERAN/UTRAN is absent in UE's TAI, the AMF/MME informs the UE to only access allowed RATs in UE's registered last known location. The information is passed in the form of 'allowed RAT list' that comprises only NR/LTE in this case. The list could comprise any allowed RAT by the PLMN.

2a. As shown in the figure 5.13.2-1, the AMF sends an access and mobility instruction by a new IE in UE Configuration Update (UCU) Command in NAS signalling to pass this information to UE. The solution reuses existing UE Configuration Update procedure from TS 24.501 [6] and TS 23.502 [2], but with a new IE to carry allowed RAT information.

2b. The UE responds with a UCU Command Complete.

Once the UE is informed to only use allowed RATs, UE subsequently only accesses allowed RATs. It mitigates risk of UE selecting decommissioned GERAN/UTRAN since the allowed RAT will not include GERAN/UTRAN.

Specific internal processes that lead to UE's subsequent action of only accessing allowed RAT is left to implementation at the UE by OEM.



Figure 5.13.2-1: UCU procedure to update UE of GERAN/UTRAN removal

|  |  |  |
| --- | --- | --- |
| TAI as AMF/MME sees UE location | NCGI/ECGI as RAN sees UE location | Policy Check at AMF/MME |
| PLMN | TAC | PLMN | NCI/ECI | GERAN/UTRAN presence/absent |
| MCC | MNC |   | MCC | MNC | gNB/eNB id | Cell id | RAT-Indicator |
| 234 | 99 | 1 | 234 | 99 | 123 | 10 | Y |
| 234 | 99 | 2 | 234 | 99 | 456 | 20 | Y |
| 234 | 99 | 3 | 234 | 99 | 789 | 30 | N |
| 208 | 34 | 1 | 208 | 34 | 123 | 40 | Y |
| 208 | 34 | 2 | 208 | 34 | 456 | 50 | Y |
| 240 | 99 | 3 | 240 | 99 | 777 | 60 | Y |

Table 5.13.2- 1: Example correlation of available RAT per location in AMF

### 5.13.3 Evaluation

The solution informs UEs in CM IDLE mode and CONNECTED mode by network trigger.

The solution addresses security requirements of KI#1 "Bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN", during coexistence of NR/LTE and GERAN/UTRAN, depending on UE's last known location, GERAN/UTRAN may or may not exist in PLMN RAN infrastructure. The solution enables UE to be selective by allowing access to PLMN's own GERAN/UTRAN in locations where it exists, and at the same time is restricting UE to only access NR/LTE in locations where PLMN has removed its own GERAN/UTRAN.

The information is protected in NAS because it is sent only after SMC in NAS.

It is up to operator policy to determine the paging occasions as to when to page UEs in a location where GERAN/UTRAN is removed. The solution does not advocate the use of additional paging but reuses existing paging occasions in accordance with UE Configuration Update procedure and session timers by AMF.

There is no additional overhead on AMF/MME with regards to maintaining location information and PLMN offered RAT type information because both pieces of information already are available via OAM in AMF/MME. The proposed solution combines these two pieces of information for AMF to make an informed decision of informing allowed RAT to the UE in its location. If there is a change of available RAT in UE's location, AMF again triggers UCU procedure with allowed RAT IE. Thus, the CN retains the control of updating the UE of allowed RAT in UE's location only when there is a change detected.

The solution does not address legacy UEs that could only access GERAN and/or UTRAN.

The solution could work in roaming scenarios if the serving PLMN has implemented the CN procedures of the proposed solution.

The solution scope could be expanded to other 3GPP RAT and non-3GPP RATs such as CDMA, CDMA-2000, W-CDMA, non-3GPP untrusted radio, WiMax etc.

The solution effectiveness to mitigate security risk may be impacted if the False Base Station operating in GERAN/UTRAN falsifies its location information.

Impacted NFs or network entities: UE, AMF, MME

Impacted 3GPP communication protocols/mediums: UCU

## 5.14 Solution #14: configuration in UE per country

This solution addresses the Key Issue #1.

### 5.14.1 Introduction

This solution prevents bidding down attacks and addresses roaming scenarios.

The solution relies only on information stored in the UE: configuration information stored on the USIM and location information known by the UE. The solution does not rely on information sent by a base station, as this base station could potentially be a false base station.

### 5.14.2 Details:

Initial conditions

* The USIM is configured with a list where each entry indicates one or several access technologies (e.g. UTRAN or GERAN) forbidden in a defined country. This list can also contain specific entries:
	+ To define one or several access technologies forbidden by default in case that the country, identified by the UE according to the location of the UE, is not listed.
	+ To define one or several access technologies forbidden when the location of the UE cannot be determined by the UE.
* For each entry of the list, it is possible to provide additional information on the policy to apply, e.g
	+ It could be indicated if the policy applies to either PLMN, or NPN, or both.
	+ It could be possible to determine a specific behavior of the UE in case that the technology is forbidden, e.g. to define a warning message to the user instead of blocking the access.
	+ It could be possible to define service types remaining allowed if the access technology is forbidden for a defined country, e.g. emergency calls.
* The ME supports GNSS (Global Navigation Satellite System) measurement capability.

During the network selection procedure, which takes place before registration,

* The UE determines the country where the UE is located thanks to GNSS measurement allowing the UE to determine its position. The ME may contain a map enabling to determine the country according to the GNSS measurement. the location information known by the UE.
* The UE checks that the proposed access technology to establish the communication is not forbidden by the list stored in the USIM. If the access technology is forbidden according to the list in the USIM, the UE does not consider this network as candidate for any further step, e.g. the network selection/reselection procedures and the network redirection procedure.

The content of this file is under the control of the home operator. The file could be updated by means of OTA mechanism.

The solution could also address non-roaming scenario. In case of non-roaming, the list in the USIM is limited to only one country, which corresponds to HPLMN.

### 5.14.3 Evaluation

This solution addresses the Key Issue #1 and roaming scenarios.

The solution relies only on information stored in the UE: configuration information stored on the USIM and location information determined by the UE.

The security of this solution depends on the correctness, reliability and security of the location information known by the UE. E.g. the GNSS is subjected to spoofing and jamming attacks. The solution puts burden on the operator to update the list.

The solution has impacts on the ME and the USIM.

Editor's Note: It is FFS whether the roaming is part of this document.

## 5.15 Solution #15: Mitigation of Roaming Attack based on UE Implementation

### 5.15.1 Introduction

This solution address key issue #1.

This solution focus on addressing the following attack:

Suppose the UE is roaming. The home PLMN of the UE is PLMN 1. The visited PLMN of UE is PLMN 2. If only serving or home network information (i.e. decommission policy of PLMN1 and PLMN2) is provisioned to the UE, the false base station can still broadcast PLMN ID irrelevant to serving PLMN/home PLMN (e.g., PLMN3). And the UE will connect to the false base station due to the lack of PLMN 3 knowledge.



**Figure 5.15.1-1: Roaming Attack**

### 5.15.2 Solution details

#### 5.15.2.1 PLMN Selection Logic

As outlined in clause 4.4.3.1.1 in TS 23.122 [5]. The order of priority for PLMN selection is: 1) available HPLMN or EHPLMN; 2) user-controlled list; 3) operator-controlled list (can be updated by the SoR or OTA procedure); 4) other PLMN/RAT with high quality; 5) other PLMN/RAT in order of decreasing signal quality; 6) disaster condition (only if UE support MINT).

PLMN in 1), 2) and 3) are stored in the USIM, while PLMN in 4), 5) and 6) are not stored in the USIM. The PLMN in 1), 2) and 3) are typically used for UE’s normal service, while PLMN in 4), 5) and 6) are typically used for UE’s abnormal service, e.g. emergency call, disaster condition.

So, to be specific, there are two attack scenarios:

1. FBS broadcasts the 2G/3G RAT of PLMN ID stored in USIM.

2. FBS broadcasts the 2G/3G RAT of PLMN ID not stored in USIM.

#### 5.15.2.2 Mitigation of Attack Scenario 1

Regarding scenario 1, the UE obtains the decommission policy and will no longer select a decommissioned RAT, once all PLMNs in the USIM have been decommissioned from 2G/3G networks, scenario 1 can be effectively resolved.

So, the attack described in scenario 1 can be mitigated by most of solutions in this TR.

#### 5.15.2.3 Mitigation of Attack Scenario 2

Regarding scenario 2, it means that the PLMN ID stored in the USIM cannot be obtained by the UE for some reasons (e.g. the signal being blocked by attackers). Therefore, the UE begins to select PLMN IDs not stored in the USIM, as described in step 4), 5), and 6) in 5.15.2.1.

Typically, the primary purpose for a UE to access a PLMN not stored in the USIM is for abnormal services, such as emergency calls or disaster conditions, which are rare case in the real world. Therefore, a simple method to address attack scenario 2 can be implemented on the terminal side:

When the UE activates the function for prevention from bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN, the UE will stop searching for PLMN IDs not stored in the USIM after traversing the PLMNs stored in the USIM, even if it detects signals from these PLMNs. When the UE deactivates this function, the UE will follow the current logic for PLMN selection as described in 5.15.2.1.

Of course, enabling this function comes with some costs, so the terminal vendor should consider informing the user explicitly about the potential risks of enabling this function. For example, "If you activates this function, in some extreme cases (where there are no signals from PLMNs stored in the USIM in the vicinity), emergency calls and disaster conditions cannot be fulfilled. Still continued?"

### 5.15.3 Evaluation

The solution address key issue #1.

Specifically, the solution addresses the roaming attack as described in 5.15.1.

The solution divides the roaming attack into two attack scenarios.

In order to address attack scenario 1, most of solutions in this TR can be used, the system impact will follow the evaluations of those solutions.

In order to address attack scenario 2, it can be based on the UE implementations. Enabling this function may come with some costs.

## 5.16 Solution #16: configuration in UE

This solution addresses the Key Issue #1.

### 5.16.1 Introduction

This solution is a variant of solution #14.

The solution relies only on information stored in the ME, which limits itself to the allowed RATs, and on location information known by the UE. The solution does not rely on information sent by a base station, as this base station could potentially be a false base station. It is essentially geofencing RAT usage.

### 5.16.2 Details:

Initial conditions:

The ME is configured, e.g. by UPU from the home operator, with a list where each entry indicates one or several access technologies (e.g. UTRAN or GERAN) forbidden in a defined area. The area could be defined as a polygon in WGS84 coordinates, potentially with height limits to allow certain technologies in planes. This list can also contain specific entries:

* + To define one or several access technologies forbidden by default in case that the area, identified by the UE according to the location of the UE, is not listed.
	+ To define one or several access technologies forbidden when the location of the UE cannot be determined by the UE.
* For each entry of the list, it is possible to provide additional information on the policy to apply, e.g.
	+ It could be indicated if the policy applies to either PLMN, or NPN, or both.
	+ It could be possible to determine a specific behaviour of the UE in case that the technology is forbidden, e.g. to define a warning message to the user instead of blocking the access.
	+ It could be possible to define service types remaining allowed if the access technology is forbidden for a defined country, e.g. emergency calls.

Periodically, when the ME determines that it has moved sufficiently, or when there is no communication possible,

* The application determines the location where the UE is located and
* The application configures the modem with the acceptable access technologies

### 5.16.3 Evaluation

This solution addresses the Key Issue #1 and roaming scenarios.

The solution relies only on information stored in the ME.

The solution has impacts on the ME.

The security of this solution depends on the correctness and security of location information known by the UE. Communication of the list to the ME is done over UPU.

# 6 Conclusion

For this study, there was no agreement for normative work.

Annex <A> (informative):
Guidance for legacy devices

## A.1 Description

In a scenario where the operator has decommissioned GERAN or UTRAN networks, a legacy UE that cannot support any enhancements or upgrades cannot determine on its own that such radio access networks are no longer available in certain areas. Such UE is subject to the same attacks described in clause 4.1. Observe, that in this scenario the attack becomes less challenging since there is no interference and hence any need to jam genuine base station signals.

Legacy UEs are numerous and will remain in the field for a long period of time until they are eventually phased out or replaced by more capable ones. Such periods are typically measured in years. This provides more than a sufficient time window for attackers to mount their schemes by FBS using decommissioned radio technology.

The scope of this annex is any guidance or solution with no standard impact that can help mitigate the threat for such devices. This does not rule out for example reusing existing out of band mechanisms to increase awareness and trigger actions from the end user.

## A.2 Approaches

### A.2.1 Approach #1: Raising user awareness

Operators can use their PR channels to highlight events such as the decommissioning of UTRAN or GERAN networks. Whether it is through news posts or advertisements, operators can inform on the decommissioning of older generations or the completion of the transitions to newer ones to raise user awareness. The most aware user may start paying attention to the network indicators in the display.

### A.2.x Approach #x: <Title of the proposal>

Editor’s Note: This is the template for guidance proposal.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-240548 |  |  |  | TR skeleton | 0.0.0 |
| 2024-02 | SA3#115 | S3-240928 |  |  |  | Included changes from S3-240536 and S3-240919. | 0.1.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241513 |  |  |  | Included changes from S3-241516, S3-241524, S3-241533, S3241601, S3-241552, S3-241580, S3-241559, S3-241555, S3-241574, S3-241578 and S3-241634. | 0.2.0 |
| 2024-05 | SA3#116 | S3-242511 |  |  |  | Included changes from S3-242030, S3-242266, S3-242636, S3-242488, S3-242489, S3-242491, S3-242492, S3-242007, S3-242006, S3-242513, S3-242005, S3-242485, S3-242487, S3-242486 and S3-242493. | 0.3.0 |
| 2024-06 | SA#104 | SP-240651 |  |  |  | Presented for information | 1.0.0 |
| 2024-08 | SA3#117 | S3-243557 |  |  |  | Included changes from S3-243342, S3-243657, S3-243385, S3-243396, S3-243507, S3-243508, S3-243509, S3-243510, S3-243659, S3-243691. | 1.1.0 |