TSG SA Meeting #102 SP-231718

December 11 – 15, 2023, Edinburgh, Scotland

**Source: SA WG3**

**Title: New SID Proposal on mitigations against bidding down Attacks**

**Document for: Approval**

**Agenda Item: 6.1.3**

**3GPP TSG-SA3 Meeting #113S3-235096**

**Chicago, US, 6 - 10 November 2023** *revision of S3-234624*

**Source: Huawei, HiSilicon, Nokia, Nokia Shanghai Bell**

**Title: New SID Proposal on mitigations against bidding down Attacks**

**Document for: Approval**

**Agenda Item: 6.2**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on mitigations against bidding down attacks

Acronym: FS\_MiBiDA

Unique identifier: 1020043

Potential target Release: *Rel-19*

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  |  |  |
| No |  |  |  |  |  |
| Don't know | X |  | X | X |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study  |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| N/A | N/A | N/A |

# 3 Justification

 If a UE connects to a 2G/3G FBS from 4G or 5G, then it is vulnerable to bidding down attack, e.g. fraudulent SMS or phone call, which could cause significant financial losses for subscribers.

There are several procedures for UEs connected to 4G/5G to establish a connection with 2G/3G base station, i.e. interworking from 4G to 2G/3G (including inter RAT handover procedure and RAU procedure), CSFB procedure (including redirection from 4G to 2G/3G), SRVCC from 5G to 3G, and cell selection once 5G and 4G is unavailable.

Security solution for interworking from 4G to 2G/3G and SRVCC is already defined in TS 33.401 and TS 33.501 respectively. SA3 has also addressed unsecure redirection from 4G to 2G or 3G in release 15 and release 18 respectively.

SA3 has studied preventing UEs from connecting to 5G FBS from Release 16 to Release 18, and no conclusion is reached. However, SA3 does not study how to prevent UEs from selecting 2G/3G FBS when 5G/4G is blocked by an attacker.

It is worth noticing that throughout the history of mobile network deployments, as mobile network systems are continuously evolving and improving, operators periodically shift focus and investment to the newest generation network and obviously end up decommissioning older ones. This is in fact what is currently happening with many operators announcing the decommissioning of their 2G or 3G networks. In such circumstances, it is no longer appropriate to allow a UE supporting 2G or 3G networks to continue selecting such networks. In fact due to weaker protection in these generation, if UEs are tricked into selecting such networks, then they will be vulnerable to many known attacks pertaining to 2G and 3G.

Therefore, SA3 should consider generic and future proof methods to mitigate and if possible prevent such bidding down attacks in this context.

# 4 Objective

This study will focus on mitigating bidding down attack, i.e. preventing UE that is currently connected to 4G/5G is establishing a connection with 2G/3G FBS considering for example the decommissioning of 2G and 3G networks. The identified topics are:

WT1:

WT1.1: Identify attack scenarios and threats in the context of decommissioning of 2G and 3G networks, e.g. cell (re)selection or forced handovers on 2G or 3G once 4G and 5G signalling are blocked when 2G/3G networks are decommissioned;

WT12: Study solutions for the identified security threats and requirements.

## TU estimates

|  |  |  |
| --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) |
| WT1 | 1.5 | 0.5 |

Total TU estimates for the study phase: 1.5

Total TU estimates for the normative phase: 0.5

Total TU estimates: 2

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| TR | 33.701 | Study on mitigations against bidding down Attacks | TSG#103(Mar 2024) | TSG#104(June 2024) | Noamen Ben Henda, noamen.ben.henda@huawei.com |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A | N/A | N/A | N/A |

# 6 Work item Rapporteur(s)

Noamen Ben Henda, noamen.ben.henda@huawei.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Huawei |
| HiSilicon |
| Nokia |
| Nokia Shanghai Bell |
| Ericsson |
| OPPO |
| AT&T |