**3GPP TSG SA WG 1 Meeting #108 S1-244439**

**Orlando, Florida, USA, 18-22 Nov 2024** *(revision of S1-244413, 4317)*

**Source: Nokia, AT&T, T-Mobile US, Telefonica, KPN**

**Title: New WID on Fraud detection in CDRs**

**Document for: Approval**

**Agenda Item: 4**

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: Fraud detection in CDRs

{Free text. It has to be the same as in the "Title:" section above. Studies have to start by "Study on"}

Acronym: CDRFraud

{Propose an acronym. Final acronym to be confirmed at the plenary. The sign "-" is a level separator between (Feature)-(Building Block)-(Work Task). The sign "\_" can be freely used. Studies have to start by "FS\_". Each acronym level has to be simple and short, 7 characters max recommended}

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-20

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

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

**\* Other = e.g. testing**

## 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) |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

{List here other Work Items which relate to the proposed one, such as a Work Item in an earlier Release if further enhancing the feature from the previous Release)}

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text}  |

**Dependency on non-3GPP (draft) specification:**

# 3 Justification

Recently there have been TDoS (Telephony Denial Of Service) and DDoS attacks on telecommunication systems particularly on emergency systems – e.g., as described in the below research papers:

1. <https://www.cisa.gov/sites/default/files/2023-02/Cyber%20Risks%20to%20911%20TDoS_6.4.2020%20-%20%28508c%29_1.pdf>
2. <https://ieeexplore.ieee.org/document/7961982>

In such situations, fraudsters use botnets which randomly generate subscriber and device identities like IMSI and IMEI and make emergency calls, thereby rendering the emergency systems out of service.

The randomly generated subscriber and device identities e.g. IMSI. MSISDN and IMEI may or may not be valid ones. These identities are further used by network entities like GMLC and PSAP to fetch location information for the corresponding subscribers. Here if the identities are invalid then their location information would also be invalid. So in order to prevent location information retrieval for invalid identities, the subscriber and device identities need to be validated and only those that are determined to be valid, should be used for location information retrieval. The invalid ones should not be used and the network element should make a decision either to discard them or to respond with error message.

In non-emergency calls too, fraudsters could use devices with spoofed identities to commit identity frauds. For example, the device identity could be spoofed or blacklisted or stolen. Also since EIR is not widely deployed by many service providers, the device identity is usually not checked.

Traditionally, service providers need to monitor location performance for their emergency and commercial services related to 4G and 5G. The location performance data is then used to generate reports to regulators, e.g. FCC – compliance for 911 calls, location monitoring accuracy and LBS traffic. Service providers make use of the CDRs and other input sources for correlating location data and generating reports to local regulators. The CDR parameters like subscriber and device identities, cell-id and location information are some of the fields used for location information correlation and data filtering.

Currently, operators have implemented STIR/SHAKEN to validate and verify caller identity to prevent spoofed calls, but device identity spoofing is not addressed yet (not supported by STIR/SHAKEN).

Also, TS 22.261 has defined fraud protection requirements in cl. 8.7, although focused on stolen devices.

In general, the subscriber and device identities contained in CDRs can be invalid – spoofed, malformed, or incorrect. Using invalid identities for location information correlation would lead to erroneous results and waste of resources. Furthermore, use of invalid identities for data filtering will not help any purpose.

The occurrence of spoofed identities in CDRs could cause significant impact for the external sources that use them, e.g.

* Location performance reporting tools that some operators are currently using
* CDR analysis tools that law enforcement agencies use to detect suspicious activity in a particular area or during particular time.
* Revenue loss for operators due to use of spoofed identities

So, in order to make sure the devices used in communications are legitimate and not spoofed and also to provide better protection to telecommunication systems, it is essential to attest and sign the device identities – just like caller identity is attested and signed.

It is thus proposed to introduce requirements to identify invalid identities in 3GPP.

There is no expected impact on 3GPP security mechanisms related to add e.g. further security to charging records (already secured objects in operator networks) or to their secure transport within networks. There is no intention to attest or sign explicitly the device caller identity.

# 4 Objective

This work item proposes new requirements related to handling invalid identities in charging information. It includes the following aspects:

* Identify identities or other parameters in charging information as invalid
* Prevent invalid identities from being used for location information correlation or data filtering
* Expose to regulators information about the use of invalid identities and parameters in charging information.

# 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 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| 22.261 | Introduce new requirements to support the handling of invalid identities in charging information | TSG#106 |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Goix, Laurent-Walter, Nokia, laurent-walter.goix@nokia.com

# 7 Work item leadership

SA WG1

# 8 Aspects that involve other WGs

# 9 Supporting Individual Members

{At least 4 supporting Individual Members are needed. There is an expectation that these companies will provide resources to progress the work. Note that having 4 supporting companies is a necessary but not sufficient condition: the usual TSG approval process by consensus is needed for the WID approval}

|  |
| --- |
| Supporting IM name |
| Nokia |
| AT&T |
| T-Mobile US |
| Telefonica |
| KPN |
|  |