3GPP SA3 Meeting #105-e S3-214296-r6

e-meeting, 08-19 November 2021 (revision of S3-213847)

**Source: Interdigital, Apple, AT&T, CableLabs, CATT, CISA ECD, Convida Wireless, Ericsson, Futurewei, Intel, Johns Hopkins University APL, Mavenir, Motorola Mobility, Nokia, Nokia Shanghai Bell, Peraton Labs, Phillips, Samsung, Telefonica, US NIST, US NSA, Verizon Wireless, Xiaomi, ZTE**

**Title: New** **WID for Study of privacy of identifiers over radio access**

**Document for: Approval**

**Agenda Item: 4.25**

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 of privacy of identifiers over radio access

Acronym: FS\_Id\_Prvc

Unique identifier:

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

Potential target Release: Rel-18

# 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 |  | X |  |
| No |  |  |  |  |  |
| Don't know | X |  | X |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a Study Item

{Tick one box. "**Feature** / **Building Block** / Work Task" form a hierarchical structure. E.g. no Building Block can be proposed without a corresponding parent Feature. The full structure of all existing Work Items is shown in the 3GPP Work Plan in ftp://ftp.3gpp.org/Information/WORK\_PLAN}

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 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 |
| FS\_SPI | Study on Subscriber Privacy Impact in 3GPP (SPI) | FS-SPI focused on privacy principles that should followed in 3GPP when designating new systems, security architectures and protocols. The proposed Study may use findings of FS\_SPI. |

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

# 3 Justification

Privacy is part of SA3 TOR since 2011 (“The 3GPP TSG SA WG3 has the overall responsibility for security and privacy in 3GPP systems. The WG will perform analysis of potential threats to these systems. Based on the threat analysis, the WG will determine the security and privacy requirements for 3GPP systems and specify the security architectures and protocols.”)

Recent publications have placed doubts on the efficacy of the adopted SA3 solutions. These publications use novel methods (e.g., AI/ML) for attacking privacy, proposing an additional, supplemental method for privacy preservation (https://arxiv.org/abs/2105.10440), or provide new and complex attack scenarios allowing the linking of identifiers transmitted over radio access with each-other and/or with other long-term identifiers.

SA3 should be proactive in preventing and solving attacks on user/subscriber privacy and avoid situations where the working group needs to quickly react to new attack scenarios with band-aid solutions. A comprehensive study of various 3GPP identifiers, initially focusing on the identifiers over radio access, and their potential use in different privacy attack scenarios is overdue in SA3.

This proposed Study is to result in a comprehensive investigation of various 3GPP identifiers (e.g., user, subscriber, access network, core network, etc.), their privacy requirements, possible privacy attacks involving 3GPP identifiers, and potential attack remediations, while initially concentrating on the identifiers over radio access, and their potential use in different privacy attack scenarios. This study does not intend to replace the existing CVD process. The concrete examples of identifiers that require a comprehensive privacy evaluation may include SUPI, SUCI, S-NSSAI, 5G-GUTI, etc.

# 4 Objective

Analysis of 3GPP identifiers that represent either targets of privacy attacks themselves or may aid adversaries in privacy attacks.

Analysis of the feasibility of privacy attacks; the analysis should consider newer methodologies such as those involving AI/ML

Analysis of available countermeasures to the identified and feasible privacy attacks; the analysis should consider newer methodologies such as those involving AI/ML

Recommendations (e.g., remedies) to the identified and feasible privacy attacks. Recommendations may include but are not limited to technical remedies, architectural recommendations, and procedural fixes.

# 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 33.8XX | Study of privacy of identifiers over radio access | ? | ? | Brusilovsky, Alec, Interdigital, alec.brusilovsky@interdigital.com |

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

|  |
| --- |
|  |
|  |  |

 |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Brusilovsky, Alec, Interdigital, alec.brusilovsky@interdigital.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Apple |
| AT&T |
| CableLabs |
| CATT |
| CISA ECD |
| Convida Wireless LLC |
| Ericsson |
| Futurewei |
| Intel |
| Interdigital |
| Johns Hopkins University APL |
| Mavenir |
| Motorola Mobility |
| Nokia |
| Nokia Shanghai Bell |
| Peraton Labs |
| Phillips |
| Samsung |
| Telefonica |
| US NIST |
| US NSA |
| Verizon Wireless |
| Xiaomi |
| ZTE |