3GPP SA3 Meeting #104-e draft\_S3-212462-r1

e-meeting, 17-27 August 2021 (revision of xx-yyxxxx)

**Source: Interdigital, Apple, AT&T, CableLabs, Futurewei, Verizon Wireless**

**Title: New** **WID for Study of privacy of Over the Air identities**

**Document for: Approval**

**Agenda Item: 7**

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 Over the Air identities

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 are either placing under doubt the efficacy of the adopted SA3 solutions using novel methods (e.g., AI/ML) for attacking privacy, proposing an additional, supplemental method for privacy preservation (<https://lnkd.in/euXaZaE> and S3-213003), or provide new and complex attack scenarios allowing linking of OTA identities with each-other and with other long-term identities.

Historically, SA3 was reactive in solving privacy attacks. That sometimes resulted in band-aid solutions that sometimes did not remedy the causes of privacy attacks and attempted to cover the symptoms only. A comprehensive study of various 3GPP identities, initially focusing of the OTA identities, and their potential use in different privacy attack scenarios is overdue in SA3.

This proposed Study is to focus on comprehensive investigation of various 3GPP identities, their privacy requirements, possible privacy attacks involving 3GPP identities, and potential attack remediations, while initially concentrating of the OTA identities, and their potential use in different privacy attack scenarios. The concrete examples of identities that require a comprehensive privacy evaluation include CAA-level UAV ID, S-NSSAI, 5G-GUTI.

# 4 Objective

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

Analysis of feasibility of privacy attacks including newer methodology involving AI/ML

Analysis of available countermeasures to identified and feasible privacy attacks including newer methodology involving AI/ML

Recommendations (e.g., remedies) to the identified and probably 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 OTA identities | ? | ? | 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 |
| TR 33.849  |

|  |
| --- |
| Study on subscriber privacy impact in 3GPP |
| Title: | Study on subscriber privacy impact in 3GPP |

 | Approved at plenary#SA#64 (June 2014) | Rel-12 StudyLast version 33849-020 from 2014/03/03  |
|  |  |  |  |

# 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 |
| Futurewei |
| Interdigital |
| Verizon Wireless |
|  |