|  |
| --- |
| 3GPP TR 33.870 V0.3.0 (2022-07) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study of privacy of identifiers over radio access; (Release 18) |
|   |
|  | 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.© 2022, 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 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Architectural considerations 7

5 Key issues 7

5.1 Key issue #1: Privacy aspects of variable length user identifiers 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.X Key issue #X: 8

5.X.1 Key issue details 8

5.X.2 Threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.A Solution #A: <Solution Title> 8

6.A.1 Introduction 8

6.A.2 Solution details 8

6.A.3 Evaluation 8

7 Conclusions 8

Annex A: List of 3GPP identifiers. 8

Annex <X> : Change history 9

# 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

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The present document achieves the following objectives:

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, including technical remedies, security guidance, to the identified and feasible privacy attacks; the analysis should consider newer methodologies such as those involving AI/ML

Recommendations to the identified and feasible privacy attacks. Recommendations may include but are not limited to non-technical remedies, architectural recommendations, and procedural fixes.

# 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 24:501: “Non-Access-Stratum (NAS) protocol for 5G System (5GS)”.

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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>

# 4 Architectural considerations

###

# 5 Key issues

## 5.1 Key issue #1: Privacy aspects of variable length user identifiers

### 5.1.1 Key issue details

Some networks may decide to allow user identifiers with variable length, e.g. in case SUPI of type NAI. If an attacker can learn something about the length, this will reduce the size of the anonymity set.

The length can become visible to an attacker in case a length preserving encryption scheme is being used for identifier concealment.

Editor's Note: Usage scenarios of variable length user identifiers in 5GS deployments is FFS

### 5.1.2 Security threats

An attacker on the air interface can identify and track subscribers with unusual lengths of the username field of variable-length SUPI in NAI format even if it is confidentiality protected (e.g., relatively short or long SUPIs).

Note: NAIs can be used for any EAP method.

If such an unusual length of the username field is unique to a single subscriber, an adversary may be able to uniquely attribute it to that subscriber.

If there is a group of subscribers with unusual lengths of username fields in their SUPIs, the attacker may be able to infer the membership of those subscribers in such group.

Editor's Note: Further threats are FFS

### 5.1.3 Potential security requirements

 The 5G system should protect against anonymity set reduction based on identifier length.

Editor's Note: Further requirements are FFS

## 5.2 Key Issue #2: Users Identified by Priority Access

### 5.2.1 Key Issue Details

During connection establishment, a UE selects an RRC establishment cause value according to its access identity and access category based on the rules specified in table 4.5.6.1 and table 4.5.6.2 in TS 24.501[2]. The establishment cause value is sent in the clear over-the-air in RRC Setup Request messages. UEs assigned access identities 11-15, will send establishment cause “highPriorityAccess”, which affords them admission benefits when accessing the network. NR also supports two new establishment causes, “mps-PriorityAccess” and “mcs-PriorityAccess”, which indicate that UEs assigned access identity 1 and 2 are permitted to use multimedia priority services and mission critical services, respectively. The priority access cause values are different and can be distinguished from the values used by ordinary UEs assigned access identity of 0. UEs with access identity 0 use establishment causes which include: “mt-Access”, “emergency”, “mo-Signalling”, “mo-SMS”, “mo-VoiceCall”, etc.

Similarly, when a UE resumes a suspended connection it sends an RRC resume cause in the RRC Resume Request message. The options for the resume cause values are the same as for the establishment cause values. The resume cause is also sent in the clear over-the-air.

The establishment cause and resume cause can also be linked to other identifiers that appear during a data session. For example, the TMSI is sent in the same RRC Setup Request message as the establishment cause. This allows the attacker to associate the establishment cause to the TMSI and trace the user throughout their data session.

Editor’s Note: How and which identifiers can be linked with each other by exploiting the RRC establishment/resume cause is FFS.

As a result, priority users are easily distinguishable from other subscriber groups based on the RRC establishment cause and resume cause. The exposed establishment cause and resume cause reveal private user information and introduce privacy threats. This information leakage makes it possible to infer the group membership of priority users, the general location of priority users (e.g., localize users to specific cells), the number of priority users (e.g., as distinguished by different TMSIs), and the type of priority users (e.g., as distinguished by different priority establishment/resume causes).

### 5.2.2 Security Threats

TBD

### 5.2.3 Potential Security Requirements

TBD

## 5.X Key issue #X:

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Solutions

## 6.A Solution #A: <Solution Title>

### 6.A.1 Introduction

### 6.A.2 Solution details

### 6.A.3 Evaluation

# 7 Conclusions

Annex A:
List of 3GPP identifiers.

The following table provides a non-exhaustive list of 3GPP identifiers and parameters transmitted over the air. These identities are provided for information only (e.g., inclusion neither suggests that the identity is in the scope of study nor that there is a privacy issue with that identity).

|  |  |  |  |
| --- | --- | --- | --- |
| No | Name of 3GPP Identifier  | Description | Specified in 3GPP document |
| 1 | SUCI  | SUbscription Concealed Identifier | TS 23.003 [aa], TS 23.501 [bb] |
| 2 | S-NSSAI | Single Network Slice Selection Assistance Information | TS 23.003 [aa], TS 23.501 [bb] |
| 3 | 5G-GUTI | 5G Globally Unique Temporary Identifier5G-GUTI provides an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity.5G-GUTI has two main components:- one that identifies the AMF(s) which allocated the 5G-GUTI; and- one that uniquely identifies the UE within the AMF(s). | TS 23.003 [aa] |
| 4 | CAG Identifier | A Closed Access Group (CAG) within a PLMN is uniquely identified by a CAG-Identifier | TS 23.003 [aa], TS 23.501 [bb] |
| 5 | C-RNTI | Cell Radio Network Temporary IdentifierC-RNTI is a unique identifier dedicated to a particular UE and used for identifying RRC Connection and scheduling. C-RNTI can be reallocated when a UE accesses a new cell with the cell update procedure. | TS 38.300 [cc], TS 38.321 [dd] |
| 6 | Establishment Cause | RRC establishment cause value maps to an access identity. This value is sent in RRC Setup Request messages when establishing a connection. | TS 24.501 [ee] |
| 7 | Resume Cause | RRC resume cause value maps to an access identity. This value is sent in RRC Resume Request messages when resuming a suspended connection. | TS 38.331 [ff] |
|  |  |  |  |
|  |  |  |  |

Annex <X> :
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA3#106-e | S3-220514 |  |  |  | Skeleton | 0.0.1 |
| 2022-02 | SA3#106-e | S3-220515 |  |  |  | Scope | 0.0.1 |
| 2022-02 | SA3#106-e | S3-220516 |  |  |  | Annex A | 0.0.1 |
| 2022-05 | SA3#107-e | S3-221180 |  |  |  | Key Issue #1: Privacy aspects of variable length user identifiers | 0.2.0 |
| 2022-07 | SA3#107-e Ad Hoc | S3-221642 |  |  |  | New key issue on users identified by Priority Access | 0.3.0 |