**SA WG2 Meeting #160 S2-2313743**

**November 13 – 17, 2023, Chicago, USA (Revision of S2-2312377)**

**Source: InterDigital Inc.**

**Title: New Study on Enhancement of Usage of User Identifiers in the 5G System**

**Document for: Approval**

**Agenda Item: 30.1**

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 the Enhancement of Usage of User Identifiers in the 5G System

Acronym: FS\_eUUI5

Unique identifier:

Potential target Release: Rel-19

# 1 Impacts

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

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

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 780004 | Study on a Layer for User Centric Identifiers and Authentication | SA1 study on requirements for User Identifiers |
| 800012 | User Identities and Authentication | SA1 normative work on requirements for User Identifiers |
| 880041 | Study on Personal IoT Networks | SA1 study on Personal IoT Networks |
| 930029 | Personal IoT and Residential Networks | SA1 normative work on Personal IoT Networks; requirements for User Identifiers apply to Personal IoT Networks |
| 940065 | Study on Personal IoT Networks | SA2 study on Personal IoT Networks |
| 980011 | Personal IoT Networks | SA2 normative work on Personal IoT Networks |
| 950005 | Study on Localized Mobile Metaverse Services | SA1 study on metaverse services |
| 1000028 | Mobile Metaverse Services | SA1 normative work on metaverse services |

# 3 Justification

By enhancing the 5G System to allow for the creation and utilization of user-specific identities, operators will be able to provide enhanced user experience, optimized performance, and offer services to devices and users that are not part of the operator’s 3GPP network. For example, network settings can be adapted and services can be offered to users according to users’ needs, different from the subscription identifier that is used by the user to establish the connection.

In the context of this work, the user to be identified could be an individual human user using a UE with a certain subscription, an application running on or connecting via a UE, or a device (e.g., a PINE) behind a gateway UE (e.g., a PEGC).

Use cases are thoroughly discussed in TR 22.904 and include:

* One or more users (i.e., humans) sharing one UE,
* One or more users (i.e., devices) behind one gateway UE, and
* One or more users (i.e., gaming applications) running on the same UE and each is treated as a different user.

The reason for utilizing operator user-specific identities in the 3GPP network is to allow the operator to charge and provide service differentiation based on the user identifier.

Support for the identification of non-3GPP devices that communicate via a gateway UE may also enable use cases such as the deployment of a 5G Mobile VPN that is managed by the network. A 5G Mobile VPN that can provide a secure and reliable connection between an enterprise’s equipment, which includes non-3GPP devices, and authorized UEs that are located off-premises. In Rel-18, as part of 5WWC\_Ph2, support was added for AUN3 devices behind a 5G-RG. Support for AUN3 devices requires that each device has its own SUPI, its own subscription data, and that a separate NAS context be maintained by the AMF and 5G-RG for each AUN3. Furthermore, the 5G-RG establishes a separate PDU Session on behalf of each AUN3 device. A goal of this work is to enable the non-3GPP devices to be identified and to use only the subscription of the UE or RG to access the 5GC.

Support for associating an identifier with traffic of a UE may enable charging and service differentiation by an RG’s home network operator for users whose non-3GPP device(s) connect to the 5GC via the RG.

NOTE: Charging is in the remit of SA WG5.

# 4 Objective

The objectives of this SA2 study are to study how the 5G System can be enhanced to allow the operator to utilize user-specific identities in the 3GPP network.

This work is based on the normative requirements for the support of user identities that were added to TS 22.101 and TS 22.115 as part of the UIA (SP-180328) work item.

The focus is on two use cases. In both use cases one or more user identifiers may be associated with the subscription (i.e., identified by a SUPI) of a UE or RG and the users require different treatment (i.e., service differentiation).

The first use case is the scenario where the user identifier is used to identify the traffic that is sent to/from the UE. For example, this applies to the case where the user identifier identifies traffic to/from a UE application or all traffic to/from the UE (i.e., the human user case). The first use case is the focus of Work Tasks 1.x and Work Tasks 2.x. The first use case also includes exposure aspects. For example, an operator can provide User Authentication Service and third parties can request operator for authentication/authorization for a particular user.

The second use case is the scenario where an identifier identifies a non-3GPP device behind a UE or RG. The second use case is the focus of Work Tasks 4.x.

NOTE 1: To ensure backwards compatibility, the User Identifier is an optional feature in 5GS.

NOTE 2: Credentials need to be provisioned in the non-3GPP device by an operator, human user or a 3rd party. However, how a user identifier and any associated credentials are provisioned in a non-3GPP device, UE, or application is not in scope of this study. Also, application layer interaction between an application client of the UE and application server is out of scope.

NOTE 3: As much as possible, solutions should be based on existing procedures.

NOTE 4: The identifier of the non-3GPP devices in WT#4 might not be called a “user identifier” but solutions to WT#4 might reuse some aspects of WT#1 and WT#2 solutions.

The objectives of this study are not to move subscriber information into a user profile and information from the user profile should not be used to override information in a subscription. For example, the slices and DNNs that are available to the UE do not change based on the user of the UE.

Work Tasks 1.x focuses on supporting the use case where the user identifier of a human or application is associated with traffic that is to/from the UE:

* WT#1.1: Define the architectural assumptions that are necessary to support identifying the user identifier that is associated with a UE’s traffic.

NOTE A: When the user identifier applies to a human, only a single user identifier is associated with the UE at a given time and it is assumed that the user identifier is associated with all of services that the UE access during the time that the user identifier and UE are associated.

NOTE B: When the user identifier applies to an application, more than one user identifier can be associated with the UE at a given time and it is assumed that support of this use case will be limited to session management impacts.

* WT#1.2: What information is stored as part of the user profile (e.g., a user identifier, associated security credentials, associated devices, user specific settings, charging details and parameters). Including how user profiles are acquired, stored, and updated in the 5GC.
* WT#1.3: Whether and how user identifiers are linked and unlinked (i.e., associated) with 3GPP subscriptions in an operator-controlled manner.
* WT#1.4: Whether and what user specific settings and parameters (e.g., QoS) need to be taken into account by the 3GPP system in order to provide service differentiation when providing communication services.

Work Tasks 2.x builds on the human / application use case of Work Tasks 1.x. The focus of this work task is on how users are authenticated and authorized, how user identifier related functionality and information is exposed, and how the network restricts user identifiers.

* WT#2.1: How are users authenticated and authorized and what user profile information and functionality is exposed to 3rd parties (e.g., exposure of the content of the user profile, exposure of authorization/authentication results, authenticating users, and linking a user identifier with a subscription).

NOTE 5: Privacy protections (e.g., privacy of information in the user profile) may be considered by SA WG3.

NOTE 6: Aspects of this work task will depend on interaction with SA WG3. For example, authentication and Authorization methods are in the remit of SA WG3. Also, privacy questions related to exposure of user profile information need to be coordinated with SA WG3.

NOTE 7: Some exposure aspects (e.g., what functionality needs to be exposed) may depend in interaction with SA WG6.

* WT#2.2: How the network restricts the usage of user identifiers, including in roaming scenarios (e.g., how the operator restricts the number of simultaneously active user identifiers per SUPI (i.e., per subscription), restricts the usage of a user identifier in roaming scenarios, and suspends usage of the user identifier based on operator policy or location).

Work Tasks 3.x are void.

Work Tasks 4.x focuses on the case where non-3GPP devices behind a UE or RG need to be identified. The focus of this work task is how an identifier is used by the network to control and identify the traffic to/from UE or RG when the traffic is associated with the non-3GPP devices. This objective differs from existing support for AUN3 devices in TS 23.316 because the objective is to enable the non-3GPP devices to be identified and to use only the subscription of the UE or RG to access the 5GC (i.e., the UE or RG should have to maintain only a NAS Context itself and not for each non-3GPP device). Also, it may be possible for the non-3GPP devices to share a PDU Session.

* WT#4.1: When non-3GPP devices communicate via a UE or RG, whether and how the network is aware of the non-3GPP devices connecting to the UE and controls the traffic to/from UE or RG when the traffic is associated with the non-3GPP devices and what configuration information the network can provide to the UE related to non-3GPP access link (e.g., configuration information for the control of IP Address allocation for the non-3GPP devices behind the UE or RG).
* WT#4.2: Void.
* WT#4.3: Whether and how to provide 5GC identification and policy control of individual non-3GPP devices connecting behind a UE or RG. Including whether and how to trigger policy control for the individual non-3GPP devices via PCF and NEF APIs.

NOTE 8: Changes to the layer 1 or layer 2 protocols of non-3GPP devices are not in scope of this study. It is assumed that the non-3GPP device does not support 5G authentication nor NAS behaviour.

NOTE 9: Conclusions related to an RG should be shared with the Broadband Forum (BBF) and CableLabs.

NOTE 10: Solutions for Ethernet PDU Session should either work in the presence of randomized MAC addresses or state that it only applies to the case where MAC addresses are not randomized.

Work Tasks 5.x are void.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Work Task ID** | **TU Estimate****(Study)** | **TU Estimate****(Normative)** | **RAN Dependency****(Yes/No/Maybe)**  | **Inter Work Tasks Dependency**  |
| WT#1 |  |  |  | WT#1 is Self-Contained |
| WT#1.1 | 1.5 | 0.5 | No |  |
| WT#1.2 | 0.5 | 0.5 | No |  |
| WT#1.3 | 0.5 | 0.5 | No |  |
| WT#1.4 | 1 | 1 | No |  |
| WT#2 |  |  |  | Depends on WT#1 |
| WT#2.1 | 1.5 | 0.5 | No | Depends on WT#1.2 (i.e., what is in the user identity profile) |
| WT#2.2 | 0.5 | 0.5 | No |  |
| WT#3.x | Void | Void | N/A |  |
| WT#4 |  |  |  | May depend on WT#1 and WT#2 |
| WT#4.1 | 1 | 1 | No |  |
| WT#4.2 | Void | Void | N/A |  |
| WT#4.3 | 1 | 1 | No |  |
| WT#5 | Void | Void | N/A |  |

**Total TU estimates for the study phase: 7.5**

**Total TU estimates for the normative phase: 5.5**

**Total TU estimates: 7.5 + 5.5 = 13**

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| Internal TR | 23.7xy | Study on the Enhancement of Usage of User Identifiers in the 5G System | SA#103(March 2024) | SA#104 (June 2024) |  |

# 6 Work item Rapporteur(s)

# 7 Work item leadership

SA2

# 8 Aspects that involve other WGs

Security aspects will be covered by SA3.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| InterDigital Inc. |
| Deutsche Telekom |
| Futurewei |
| NEC |
| Huawei |
| HiSilicon |
| AT&T |
| KPN |
| Philips International B.V. |
| Comcast |
| CableLabs |
| Dish Network |
| Charter Communications, Inc. |
| Samsung |
| Xiaomi |
| Broadcom |
| Vodafone |
| China Mobile |
| China Unicom |
| Telecom Italia |
| BT plc |