**SA WG2 Meeting #163 S2-2407285**

**27 May – 31 May, 2024, Jeju, Korea (Revision of S2-2406284)**

**Source: InterDigital Inc.**

**Title: New WID on User Identities and Authentication Architecture**

**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: User Identities and Authentication Architecture

Acronym: UIA\_ARC

Unique identifier: TBD

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

|  |  |
| --- | --- |
|  | Study  |
|  | Normative – Stage 1 |
| x | 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 |
| 1020063 | Study on User Identities and Authentication Architecture | SA2 Study on User Identities and Authentication Architecture |

# 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 a device behind a gateway UE/5G-RG.

Use cases are thoroughly discussed in TR 22.904 and include:

* One or more users (i.e., devices) behind one gateway UE

.

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.

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

This work item will implement the following objective as concluded in the study User Identities and Authentication Architecture. Exact conclusion contents of normative work for the objective shall be based on the conclusions in clause 8.4 of TR 23.700-32.

Objective #1: Support for Identifying non-3GPP Devices Connecting behind a UE or 5G-RG.

Under this objective it is assumed that Authentication for the non-3GPP deviceis performed by UE or 5G-RG, which is not in the scope of 3GPP.

A Device Identifier will be specified. A Device Identifier is a permanent identifier and will be a generic string, and the allocation of the Device Identifier is out of scope of 3GPP.

The objective is that the 5GC is able to associate the traffic from each individual non-3GPP device with a Device Identifier and use the Device Identifier to obtain QoS Settings for the traffic.

For non-3GPP devices requiring QoS differentiation, Device Identifiers and their corresponding QoS/Policies associated with a UE/5G-RG subscription are provisioned into the UDR by the AF.

NOTE 1: The connection between non-3GPP devices and UE/5G-RG is not impacted.

NOTE 2: The UE/5G-RG shall support the traffic from non-3GPP devices that are not linked with a Device Identifier. Non-3GPP devices that do not need to be identified by 5GC can use the QoS Flow(s) established using Rel-18 Connectivity Group ID mechanisms.

* Once a UE/5G-RG binds the Device Identifier to a non-3GPP device, QoS differentiation can be performed within a PDU Session (using different QoS Flows) or between PDU Sessions. In the case of non-3GPP devices sharing a PDU Session, QoS Flows are provisioned in the UE/5G-RG using PDU Session Modification procedures. Based on the application-layer mechanisms out of 3GPP scope between UE/5G-RG and AF, an AF session with required QoS may be implemented as per clause 4.15.6.6 of TS 23.502 for the corresponding non-3GPP device.

NOTE 3: How UE/RG binds Device Identifier to non-3GPP device is out of scope of 3GPP. When a non-3GPP device connects to the UE/5G-RG, the UE/5G-RG can, based on locally configured policies, bind the traffic from the non-3GPP device to a Device Identifier. For non-3GPP devices with Device Identifiers whose traffic need to be differentiated, in case of NAT, UE/5G-RG will ensure that it does not NAT the traffic from different non-3GPP devices to the same IP address and port number range combination.

NOTE 4: Who (the UE/5G-RG and/or the AF) decides to request for change of QoS Flows will be discussed and documented during the normative stage.

For non-3GPP devices requiring QoS differentiation, it will be specified that the UE/5G-RG may send the Device Identifier and user plane address of the non-3GPP device to the SMF in a NAS-SM message, and the SMF will forward the Device Identifier and user plane address to the PCF. The PCF will take it into account for policy decisions based on the Device Identifier information retrieved from the UDR. Device Identifier is used as a data key to retrieve the information from the UDR.

* When using an IP PDU Session Type, the user plane address is the UE IP Address(es) / Port Number(s) that carry the non-3GPP device’s traffic. When using an Ethernet PDU Session Type, the user plane address is the MAC address and/or the VLAN tag ID that is associated with the non-3GPP device’s traffic.
* For non-3GPP devices requiring QoS differentiation, UE/5G-RG may also send the Device Identifier of the non-3GPP device to the SMF in DHCPv6 message to associate the Device Identifier with the user plane address.

NOTE 5: The details of this DHCPv6 based solution will be discussed and clarified as part of the normative stage.

The optional restriction within the 5GS on max number of simultaneously active Device Identifiers per UE/5G-RG for devices whose traffic need to be differentiated will be handled as part of this work.

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| N/A |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| *23.501* | *Updates to the 5G System architecture to support User Identities* | SA #106(December 2024) |  |
| *23.502* | *Updates to the 5G System architecture to support User Identities* | SA #106*(December 2024)* |  |
| *23.503* | *Updates to the 5G System architecture to support User Identities* | SA #106*(December 2024)* |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Michael Starsinic, Interdigital <Michael.Starsinic@Interdigital.com>

# 7 Work item leadership

SA2

# 8 Aspects that involve other WGs

Security aspects will be covered by SA3.

Charging aspects will be covered by SA5.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| AT&T - ? |
| Broadcom - ? |
| BT plc - ? |
| CableLabs |
| Cisco - ? |
| China Mobile - ? |
| China Unicom - ? |
| Comcast - ? |
| Deutsche Telekom - ? |
| Dish Network - ? |
| Futurewei - ? |
| HiSilicon - ? |
| Huawei - ? |
| InterDigital Inc. - ? |
| KPN - ? |
| Lenovo - ? |
| MATRIXX Software - ? |
| MediaTek - ? |
| NEC - ? |
| OPPO - ? |
| Philips International B.V. - ? |
| Samsung - ? |
| Telecom Italia - ? |
| Vodafone - ? |
| Xiaomi - ? |