**SA WG2 Meeting #161S2-2403486**

**Athens, February 26th–March 1st, 2024 (revision of S2-2403202)**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Solution for KI#2, and KI#3: Unique User Identifier for a Human User and how it is used in 3GPP procedures to associate the Human User with a UE**

**Document for: Approval**

**Agenda Item: 19.8**

**Work Item / Release: FS\_UIA\_ARC / Rel-19**

*Abstract of the contribution: solution addressing KI#2*

# 1 Discussion

This document describes a solution addressing KI#2. The solution introduces a unique User Identifier, which uniquely identifies potential human Users that may use a UE. Considering that at a given time only one of the human Users is active with the UE, the solution specifies how the unique User Identifier of the active human User is associated with a UE. The main scope is to re-use existing procedures and to adapt them to cover the dynamic association aspects on authentication and authorization when one of the human Users gets active with the UE.

Additionally, it covers some aspects related to KI#3 when information is exposed to define which human Users are allowed to use the UE.

# 2 Proposal

It is proposed to update TR 23.700-32 as follows.

\* \* \* \* First change \* \* \* \*

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |
| --- | --- | --- |
| Solutions |  |  |
|  | <Key Issue #1> | <Key Issue #2> | <Key Issue #3> | <Key Issue #4> |
| #X: |  | X | X |  |
|  |  |  |  |  |

\* \* \* \* Next change (All new text) \* \* \* \*

## 6.X Solution #X: Unique User Identifier for a Human User and how it is used in 3GPP procedures to associate the Human User with a UE

### 6.X.1 Introduction

This solution addresses and KI#2 “Authentication and Authorization of Users and Restrictions on Users”.

The solution introduces a new unique User Identifier and specifies how the unique User Identifier is used in 3GPP procedures to associate a Human User with a UE dynamically.

### 6.X.2 Functional Description

This solution is based on dedicated User profiles for the human Users and a UE Subscription profile for the UE (containing a USIM card). It is assumed that the potential human Users and the User owning the UE have individual contracts with a single MNO to ensure that the User profiles and the UE Subscription belongs to the same MNO domain. Figure 4.X.2-1 shows how the solution is embedded in the 3GPP architecture and provides an overview how multiple human Users can use a single UE.

Figure 6.X.2-1: Solution Overview

When a human User login to a UE, the UE initiates the registration of the human User to the 5GS via the UE. During the registration the User profile of the human User is associated with the UE subscription as follows:

* Only one human User profile is associated with the UE subscription at a given time. The UE subscription is dedicated to the USIM owner, who provided the USIM in the UE.

Editor’s Note1: Detailed behaviour when a User initiates a registration at the UE but another User with a different User Identifier is already registered is ffs. This includes for example, the consideration of Security aspects and the decision if UE or CN initiated deregistration is preferred.

* When the MNO allows the association of multiple human User(s) with a UE subscription, a human User, preferable the one that owns the USIM card in the UE should be enabled to provide the information, which human User is allowed to use the UE. For this purpose, the MNO may limit the number of potential User profiles that can be associated to the UE with the UE Subscription.

It is up the MNO to offer methods to manage potential human User associations with a UE subscription. For example, the respective information may be part of the contract processes and the result is deployed UE subscription data and User profile data via OAM services. Alternatively, the MNO may offer an Application Server that allows a human User to provide the potential human User to UE subscription information dynamically via a Web Interface. Details of such solutions are out of scope in SA2 but may require following respective guidelines on security and privacy from SA3 group. From SA2 perspective it is important that following new information for the authorization check is available in the UE subscription:

* + MaxNumber of potential human User profiles that can be assigned with the UE subscription.
	+ List of potential UE profiles that are allowed for the UE subscription. The List cannot exceed the MaxNumber of potential human User profiles.

Editor’s Note2: Additional parameters and the handling of the parameters involving link/unlink via AF/NEF are ffs.

* When the UE subscription allows that the human User (identified by the User Identifier) is allowed for the UE, the UDM initiates the dynamic association of the human User with the UE and generates the temporary merged (generated or intersection) Subscription data containing UE Subscription data and User Profile data according to a defined MNO policy.

Subscriber/subscription information of the UE will not be moved into the User profile of a human User and information from the User profile of a human User should not override information of the UE subscription. This can be achieved by merging the UE subscription data with the User profile data in the UDM. How this merging is processed may be subject of a Mobile Network Operator MNO policy, which defines which information has precedence, however the MNO policy shall not consider using the User profile data to override the UE subscription data. For example, if UE subscription doesn’t contain voice services and the User profile allows them, the human User shall not be able to use voice services if the human User is associated with the UE.

Editor’s Note3: How merged User profile data and UE Subscription data, the MNO policy, and the association of the UE subscription with the UE profile are memorized is ffs.

The User Identifier is provided by the MNO to the human User and may be based on following parameters and considerations:

* The human User Identifier should be based on the Network Access Identifier (NAI) specifications in RFC 7542. As the human Users need to be on the same MNO domain as the UE subscription, it needs to be unique per MNO only. An MNO may use any of the following examples for the User Identifier:
	+ Name.MCCMNC.RoutingID@domain.com, or alternatively
	+ string.routingID@domain.com. or
	+ Name@domain.com, where domain is built out of the MCC/MNC of the MNO and the RoutingID i.e. domain may be RIDxx.MNCyy.MCCzz.

In the examples Name can be any string or number and RoutingID is used to determine the right UDM/UDR group storing the User profile.

### 6.X.3 Procedures

The dynamic association of a human User profile with a UE Subscription requires to extend the existing procedures defined in TS 23.502 by adding the new user identification User Identifier (UserID) to the procedures.

#### 6.X.3.1 Registration procedure

In a first step, it is proposed to adapt the Registration procedure as specified in TS 23.502, Figure 4.2.2.2.2-1 to perform the association of the UE subscription with the User profile. The adapted Registration procedure builds then the basis to generate the temporary merged Subscription data containing UE Subscription data and User Profile data according to a defined MNO policy.

It is to be noted that there could be operator deployments that may consists of multiple UDMs in the network; in such a case there could be scenarios that the UE and the User Identifier linked to a specific UE be part of different UDMs.



Figure 6.X.3.1-1: User Registration of Human Users using a UE

Figure 6.X.3 shows how the Registration procedure as defined in TS 23.502, clause 4.2.2.2.2 is modified when a UE is enabled to serve multiple Human Users.

 As prerequisite it is assumed that the UE contains a USIM which is associated with the UE Subscription in 5GS while the User has a dedicated User profile. Both, UE Subscription and User profile belong to the same Operator domain and doesn’t require roaming functionality.

0 The human User initiates the User Registration procedure at the UE i.e., human User can login at the UE. For this purpose, an App can be defined (that may use a UE provided API). Once the user logs in, the UE provides his/her user credentials that are dedicated to the User Identifier. How this is done is out of scope in SA2.

1/3 UE sends NAS registration request that include SUCI/GUTI of the UE and the UserIndication, which provides the information that a human User requests to register via the UE to 5GS.

6/9 AMF ensures per existing procedures that the UE and User are authenticated (if needed involving an AUSF and steps 8, 9 of TS 23.502, Figure 4.2.2.2.2-1). When the AMF recognizes the UserIndication for a human User it derives the User Identifier in steps 6-9 of TS 23.502, Figure 4.2.2.2.2-1 considering the NAS Authentication and Security principles for User Identifier in the same way as for the UE. At the end of this step the AMF has the SUPI of the UE used by the human User and the User Identifier of the human User. EIR check (steps 11, 12 of TS 23.502, Figure 4.2.2.2.2-1) may also be carried out.

 As the AMF has received from the UE the User Identifier of User, the AMF enforces a user authentication for the UE and the User. The Authentication may be required to cover security aspects in situations where the UE is already registered with a different User Identifier. Important is to consider that a previous registration of the UE and a User is cancelled and all corresponding resources (at SMSF, PCF, SMF, CHF etc…) are released to meet the architectural assumption and requirement that only a single User Identifier is active with a UE subscription at a given time.

14a.1 When the AMF issues Nudm\_UECM\_Registration request, the AMF provides both the SUPI and the User Identifier to UDM that is responsible to handle the UE Subscription. The UDM checks in the UE’s Subscription if the User Identifier is allowed for the UE; if this is not the case it rejects the UECM\_Registration.

 This assumes a new UDR table indexed by the SUPI that contains all User Identifier (s) allowed for this SUPI.

14a.2 Based on the User Identifier (e.g. routing identifier part), the UDM of the UE identifies the UDM of the User and asks the UDM of the User for readiness to associate the human User (User Identifier) with the UE (SUPI).

14a.3 The UDM of the User sends a positive response when the association of the human User and the UE is possible and a negative response when not. This may be the case when the human User is already associated with another UE.

14a.4 Nudm\_UECM\_Registration response. If the User Identifier is not allowed for the UE the UDM rejects the AMF request with a cause that allows the AMF to reject the UE registration with a proper cause telling the user that this specific User Identifier is not allowed to use this UE.

14b.1 In step 14b of TS 23.502 Figure 4.2.2.2.2-1, when the AMF issues the Nudm\_SDM\_Get request, the AMF provides both the SUPI and the User Identifier to UDM that is responsible to handle the UE subscription.

14b.2/3 Based on the User Identifier (e.g. routing identifier part), the UDM of the UE identifies the UDM of the User and gets User profile data.

14b.4 the UDM merges the UE subscription data and the User profile data (possibly retrieved from different UDRs) according to a MNO policy to create the merged subscription data result. If the User profile is not compatible with the UE subscription, it rejects the AMF request with a cause that allows the AMF to reject the registration with a proper cause (telling the User that User profile is not compatible with the UE subscription).

 The merged Subscription data may induce to use the user’s User Identifier (s) additionally, while the merged Subscription data result also contains codes and further 3GPP parameters including the new User Identifier.

14b.5 Nudm\_SDM\_Get response with the merged Subscription data result.

21 Further steps 14c-19c of TS 23.502, Figure 4.2.2.2.2-1 are carried out leading to the AMF sending a NAS registration accept/reject based on the merged Subscription information result.

#### 6.X.3.2 Registration procedure supporting SMS over NAS

The AMF may run the procedure of TS 23.502 Figure 4.13.3.1-1: Registration procedure supporting SMS over NAS. To support multiple Human Users of a UE this procedure is modified as shown in Figure 6.X.3-2.



Figure 6.X.3.2-1: Registration procedure supporting SMS over NAS for Human Users using a UE

1+2 Follows Step 0 - 14 of Registration procedure in Figure 6.X.3-1.

3 The AMF discovers and selects an SMSF to serve the human User (User Identifier) via the UE as described in TS 23.502 Figure 4.13.3.1-1.

4 Follows Step 15 - 20 of Registration procedure in Figure 6.X.3-1

5 When the AMF invokes Nsmsf\_SMService\_Activate service operation from the SMSF User Identifier shall be included along with the SUPI (and possibly the Group Id of the UDM/UDR of the UE/User).

6 The SMSF discovers an UDM based on the SUPI and User Identifier (and possibly the Group Id of the UDM/UDR of the UE/User). The UDM merges (based on operator policy) the SMS related User Profile data and the SMS related UE subscription data (possibly retrieved from different UDR) to create merged SMS subscription data.

7.a It is assumed that it is not required to re-check the readiness for the association of the human User and the UE.

7b.5 The merged SMS subscription data result is sent to the SMSF.

 Once SMSF has received the subscription data result, the SMSF behaviour to handle SMS is as defined in existing specifications.

#### 6.X.3.3 Further procedures

Editor’s Note4: The new User Identifier parameter identifying a Human User of a UE may be needed in other procedures e.g., PDU Session Establishment/Modification as well. The identification of these procedures is ffs.

### 6.X.4 Impacts on services, entities, and interfaces

UE:

* Distinguish human Users and provide User Identifier of active human User in procedures.
* Receive merged Subscription data results (result code information) and inform human User.

AMF:

* Receive and forward User Identifier of active human User in procedures.
* Initiate Authentication/Security for UE and User Identifier and provide results to UE via (R)AN.
* Receive merged Subscription data results from SMSF and UDM of User and forward to (R)AN.

SMSF:

* Receive and forward User Identifier of active human User in procedures.
* Receive merged Subscription data results and forward to AMF.

UDM of UE (UE Subscription):

* Discover UDM of User based on User Identifier of active human User and get User profile data of User Identifier.
* Authorize User Identifier of active human User for UE.
* Check compatibility of User profile data and UE subscription data and build merged Subscription data result.
* Initiate storage and forwarding of merged Subscription data result.

UDM of User (User Profile):

* Provide User profile for User Identifier of active human User in procedures to UDM of UE.
* Notify UDM/UDR of UE when User profile changes.

Multiple UDM deployments may result in UE and the User Identifier linked to the UE being part of different UDMs.

\* \* \* \* End of Changes \* \* \* \*