**SA WG2 Meeting #S2-161 S2-240xxxx**

**26 Feb - 1 March, 2024, Athens, GR**

**Source: Apple, ??**

**Title: KI#3: New Sol: User Identity profile exposure**

**Document for: Approval**

**Agenda Item: 19.8**

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

***Abstract of the contribution:****This paper proposes a new solution to the KI#3 in 23.700-32 v0.1.0*

# 1 Discussion

The Rel-19 User Identities and Authentication Architecture study has agreed on the Key Issue #3 pertaining to “Exposure of User Identity Profile Information”.

This pCR proposal aims to address the following questions of Key Issue #3

* what and how User Identity Profile information and functionality are exposed (e.g., exposure of the content of the User Identity Profile, exposure of authorization/authentication results, authenticating users, and linking a User Identifier with a 3GPP subscription).

# 2 Proposal

It is proposed to adopt the following changes into TR 23.700-32 v0.1.0.

##

|  |
| --- |
| **\* \* \* \* 1st Change (revision marked)** |

## 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> | <Key Issue #5> |
| #X |  |  | X |  |  |

 **\* \* \* \* 2nd Change (all text new) \* \* \* \***

## 6.X Solution #X: User Identity profile exposure

### 6.X.1 Key Issue mapping

This solution addresses KI#3 “Exposure of User Identity Profile Information”.

### 6.X.2 Description

This solution assumes the following:

- The procedures for configuring User Identifiers in 5GC and provisioning them to UE are out of SA2 scope (for example, obtaining Blinded tokens through application layer, provisioning though USIM Application).

- How the user instructs UE to use a particular User Identifier is up to UE implementation (for example, biometrics based identification)

The solution is based on the following principles:

The UE subscription data in the UDM is enhanced with the following:

- One or more User Identifiers, optionally associated with one or more GPSI (if not explicitly associated, User Identifiers are applicable for all GPSIs in the UE subscription data)

- Each User Identifier can be associated with

- one or more non-3GPP identifiers, optionally associated with one or more AF Identifiers.

The same User Identifier could be configured as part of multiple UE subscription data.

A User Identifier could be for one-time use or can be reused multiple times.

PCC Rules may additionally contain:

- one or more user identifiers.

 UE policy may additionally contain:

- information specific to user identifiers.

### 6.X.3 Procedures

#### 6.X.3.1 Verification of User Identifier associated with a subscription

Exposure of User Identity Profile information is realized as a NEF service. An AF only requests NEF to verify contents of User Identity Profile and NEF would respond with a ‘Verified Successfully’ or ‘Not Verified’ answer. No part of user identity profile is exposed to AF through the NEF service.

The intention of AF is to use 5GC as an identity provider. User Identifier (or an associated non-3GPP identifier specific to the AF) acts as the unique identifier provided by the identity provider after the UE has successfully registered with the 5GC and linked the User Identifier to the UE’s 3GPP subscription.



**Figure 6.X.3.1‑1 User Identifier verification by 5GC**

1. User, through the application client in the UE, has provided Application Function with its own identifier (this could be either a User Identifier linked to their 3GPP subscription during registration in 5GC or an AF specific non-3GPP identifier).

2. AF decides to verify the presented identity with the 5GC.

3. AF invokes NEF Nnef\_VerifyIdentifier service with the identifier (i.e., a AF specific non-3GPP identifier or User Identifier) and UE information (e.g., IP Address, GPSI).

4. If the provided UE information is the IP Address, NEF may optionally use the same steps as in UEId Service to get UE’s SUPI.

5. NEF invokes the UDM Nudm\_VerifyIdentifer service with AF provided identifier and SUPI.

6. UDM checks whether the AF provided identifier is currently linked to the UE’s 3GPP subscription. If the AF has provided non-3GPP identifier, UDM checks whether this is one of the configured non-3GPP identifiers associated with User Identifier currently linked to the UE’s 3GPP subscription.

7. UDM responds to the NEF with the result of the verification.

8. NEF responds with a success or failure indication indicating whether 5GC was able to successfully confirm if the AF provided identifier is indeed associated with the UE’s 3GPP subscription.

If the AF requests to validate any other part of the user profile information associated with that UE’s 3GPP subscription, it can invoke the NEF service and provide the inputs along with User Identifier it wants 5GC to verify.

#### 6.X.3.2 Exposure of Authentication Results

The above procedure can also be used by the AF to obtain the results of an authentication procedure of a User Identifier. The NEF VerifyIdentifier service also provides subscribe and notify service operations allowing an AF to subscribe to be notified of User Identifier authentication results.

The User Identifier authentication may be performed using any of the solutions to Key Issue#2.



1. AF subscribes to the NEF VerifyIdentifier service for notifications on authentication results, and provides the associated notification endpoint of the AF by sending Nnef\_VerifyIdentifier Subscribe request to NEF:

* 1. User ID.
	2. UE addressing information (e.g. GPSI, or SUPI)
	3. Authorization/authentication results.

2. NEF performs the necessary authorization control and translation of internal-external information (e.g. the mapping between GPSI and SUPI if AF is in the untrusted domain).

3. The NEF subscribes to notifications about User Identifier authorization/authentication results, and provides the associated notification endpoint of the NEF to UDM by sending Nudm\_VerifyIdentifier Subscriber request to UDM

4. UDM detects the event occurs and sends the event report, by means of Nudm\_VerifyIdentifier Notify message to the associated notification endpoint of the NEF. The UDM includes the corresponding authentication results in the event report.

5. NEF forwards the received the event report to AF.

Editor’s Note: Exposure of other information related to User Identity profile is FFS.

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

NEF: Provides a service to

Verify whether a User Identifier or components of User Identity Profile is linked to 3GPP subscription of the UE (identified by a UE IP address or GPSI).

monitor authentication results of a User Identifier with the given UE.

UDM: Provides a service to

verify an identifier or components of user identity profile is linked to the UE’s (identified by SUPI) subscription.

monitor authentication results of a User Identifier with the given UE.

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