**3GPP SA WG2 Meeting #161 S2-2403204**

**Athens, February 26 – March 1, 2024**

**Source: Ericsson**

**Title: KI#2+3: New solution, User Identity Profile Server based control**

**Document for: Approval**

**Agenda Item: 19.8**

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

*Abstract of the contribution: The contribution discusses and proposes to include principles of a new solution to address key issues 2 and 3.*

**Proposal**

It is proposed to agree the following changes to 3GPP TR 23.700-32 v0.1.0:

\* \* \* Start of Changes \* \* \* \*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

UIP User Identity Profile

\* \* \* Next Change \* \* \* \*

# 6 Solutions

## 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> |
| #1 |  |  |  |  |
| #2 |  |  |  |  |
| #x |  | X | X |  |

\* \* \* Next Change (all new text) \* \* \* \*

## 6.X Solution #X: User Identity Profile Server based control

### 6.X.1 Key Issue mapping

This solution addresses KI#2 and KI#3.

### 6.X.2 Description

#### 6.x.2.1 User Identity Profile

The User Identity Profiles (UIPs) are stored in a UIP Server. The principles for the UIP Server are as follows:

1. The UIPs can be managed, e.g. created, updated, and removed, by the PLMN operator;

2. The UIPs can be managed, e.g. created, updated, and removed by trusted server (Portal) or by the UE/user, and in such case the PLMN operator authorizes the management operations;

3. All UIP management procedures are performed from an authorized and authenticated entity.

4. The UIP information is pushed by the UIP Server to the 5GC, optionally via the NEF.

Editor's note: Further principles and the information included in the UIP is FFS and dependent on the use cases to be addressed.

#### 6.x.2.3 Architecture

The architecture below shows an architecture for roaming (Figure 6.x.2.3-1) and one for non-roaming (Figure 6.x.2.3-2).

The interface between the UE and the Portal is assumed to be an application layer interface out of scope of 3GPP.

The interface between the UIP Client and the UIP Server is assumed to be on application layer and not standardized by SA2.

Editor's note: Whether and how to ensure that the UIP Client is in the UE and/or actual human user is using the UE is FFS.

Editor's note: Whether the UIP Client and the UIP Server protocol is standardized in 3GPP e.g. in SA6 is FFS.

The Portal is a trusted entity from the HPLMN perspective, and can e.g. be managed by the HPLMN operator or a trusted partner.



Figure 6.x.2.3-1: High-level roaming architecture



Figure 6.x.2.3-2: High-level non-roaming architecture

#### 6.x.2.5 Authentication and Authorization

The UIP management procedures are performed from an authorized and authenticated entity.

The User Identifier associated with the UIP is authenticated at the UIP management procedures e.g. for creating, removing an Identifier Link (link and unlink), and activating an Identifier Link.

NOTE: Security requirements are to be addressed by SA3.

### 6.X.3 Procedures

Editor's note: The high-level procedures and information flows for the solution is FFS.

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

Editor's note: Further impacts is FFS including which NFs are to receive UIP information.

UIP Server: A new server containing the User Identity Profiles, outside the 5GC.

5GC NF/NEF: Possible impacts to (new or existing) service operations to transfer User Identity Profile information from the UIP server to the 5GC.

UE: Support of client to update the User Identity Profiles in the UIP Server.

\* \* \* End of changes \* \* \* \*