**SA WG2 Meeting #161S2-2403203**

**February 26th – March 2nd, 2024; Athens revision of S2-2402847**

**Source: Samsung**

**Title: KI#2, KI#3 New Sol: Exposing user authentication result to 3rd parties**

**Agenda Item: 19.8**

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

*Abstract of the contribution: Solution for Authentication and exposure of authentication result to 3rd parties*

# 1 Discussion

Solution discusses KI#2 and KI#3 as described in TR 23.700-32.

# 2 Proposal

It is proposed to add this solution to TR 23.700-32 FS\_UIA\_ARC.

\* \* \* Start of 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> |
| #1 |  |  |  |  |
| #2 |  |  |  |  |
| #X |  | X | X |  |

\* \* \* Second Change : All new text \* \* \* \*

6.X Solution #X: Exposing user authentication result to 3rd parties

6.X.1 Key Issue mapping

This solution maps to KI#2 (Authentication of users) and KI#3 (Exposure of user identity functionality).

6.X.2 Description

#### 6.X.2.1 Scenario and use cases

The following solution discusses the scenario as per the use case 5.2 as mentioned in TR 22.904.

Use case involves a 3rd party entity (e.g. a bank) requesting for an authentication service (or second-factor authentication) via operator.

Using traditional SMS-OTP for second factor authentication provided security risk. SMS-OTP solutions are prone to phishing attacks. Whereas using a UE’s already established connection to perform user authentication further provides trust that the user is using its own UE (to which it’s user ID was linked securely be the operator) and using it’s own HPLMN.

The procedure described below can also be used a primary login (and signing up) for 3rd party services using operator’s user identifier. This provides operator to leverage their infrastructure and offer secure authentication solutions to third party applications.

#### 6.X.2.2 Entities

**User Information Database Function (UIDF):** This NF can store the specific aspects related to a User ID. The user profile for a particular User ID also store a reference to the UE subscription(s) (i.e SUPI(s)) that are linked to the particular User ID. It is essential that the User profile is stored separately from the UDM (that is separately from the subscription data of the SUPI), since User ID(s) and SUPI(s) can be dynamically linked and unlinked, and at a particular point of time possible no SUPI may be linked to a user profile.

#### 6.X.2.2 Solution summary

Consider the case when a user is (using a UE) is using 3rd party application (e.g. Bank) which requires 2nd factor authentication

In order to get verification, for the corresponding user identified by the User ID; 3rd party request the Operator (via NEF) to start user authentication and verify whether an actual human user is using the particular User ID or not.

It is assumed that linking between the particular User ID (say UID-1) and the SUPI (say IMSI-A) has already been performed by the operator (i.e. IMSI-A subscription stores the association of the UID-1 and/or the User profile for UID-1 stores the association for IMSI-A).

6.X.3 Procedures



Figure 6.X.3-1 3rd party application requesting User authentication

1. A User which has credentials for UID-1 and has access to the particular UE (which is identified by IMSI-A to the operator). The user logs-in to the application using bank id and password. The bank application requests for secondary authentication, so the user provides UID-1 and optionally the operator’s name to the Bank application. The interaction between user and the application is out of 3GPP scope.

Note: The device from which the user accesses the application (e.g. bank application) may not be the same as the UE (which is associated to IMSI-A). 3rd party server asks the operator to check whether the particular User has the possession of the particular UE which is linked to that User ID (i.e. possession factor) and operator verifies it by invoking the User to perform authentication for the particular User ID at that particular UE.

1. AF to NEF : Nnef\_UserVerify Request (User ID)

An AF (operated by the application server of Step 1) sends the request to NEF to verify authentication for the particular User ID.

1. NEF to User Profile: Request to get User Profile for User ID

User profile checks the profile for the provided User ID (UID-1 in our example) and returns the associated SUPI (IMSI-A in our example) to the NEF.

Note: It is assumed that linking between the particular User ID and the SUPI has already been performed by the operator.

In case an AAA-server is used for authentication, User profile may additionally provide the AAA server address of the entity which is responsible for authenticating the corresponding User ID

1. User Profile to NEF (SUPI/GPSI linked with User ID, AAA server address)
2. NEF to UDM: Nudm\_UserAuthenticate request (SUPI/GPSI, User ID, AAA server address)

Now in order to trigger the particular UE (via it’s AMF), UDM has to check the UE registration and find the particular AMF which is serving the UE.

UDM checks the subscription data for the provided SUPI and checks if the provided User ID is linked with User ID or not.

If the User ID is linked with the SUPI, UDM decides to trigger the authentication for the User ID at the particular UE identified by SUPI).

Note: If the UE (corresponding to the SUPI linked to the User Identifier) is not registered to the network, UDM may end the procedure and send failure notification of the UE.

EN: Steps 6 to Step 11 describes the Authentication procedure after a 3rd party has invoked the network to perform user authentication for the particular User ID. What exact method, is used, will be decided by SA WG 3.

1. UDM to AMF (SUPI, User ID, AAA-server Address)

UDM request the particular AMF which is serving the UE to trigger UE to perform user authentication.

1. AMF to UE NAS message (Authentication trigger for User ID)
2. UE operation

Upon receiving the received NAS message, based on UE implementation User may have to perform some invocation (e.g. an app is invoked, or provide the password corresponding to the User ID)

1. UE to AMF : NAS message (User ID, Authentication related message (e.g. EAP message))

As per any User invocation (e.g. passwords received from the User, or per configured credentials), UE sends NAS message to the AMF corresponding to the User ID (as received in Step 7).

1. Authentication for the particular User ID between the UE and the Auth server.

NSSAAF based secondary authentication may be reused.

1. AMF to UDM (SUPI, User ID, Authentication success/failure).
2. UDM to NEF: Nudm\_UserID auth Response(User ID, Authentication success/failure)
3. NEF to AF : Nnef\_UserVerify response(User ID, Authentication success/failure)
4. Upon receiving success of the user authentication, Bank application (server) now allow UE the access to it’s services.

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

* NEF impacts
  + on new service for verification for user authentication
* UDM impacts
  + handling NEF request for User authentication at a particular UE and triggering the authentication for a User ID at the particular UE.
* UE impacts
  + for providing the credentials related to a particular User ID to the network and performing authentication
* UIDR : new NF for User profile storage.