**3GPP TSG-SA3 Meeting #100e *S3-201959***

**e-meeting, 17 - 28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **2** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | TS 33.434 clean up | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung, Motorola Solutions | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SEAL | | | | |  | ***Date:*** | | | 23-07-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | 16 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In TS 33.434, there is no clause for VAL service authorization. This CR introduces new clause 5.2.X specifically for VAL service authorization.  There are some places in TS 33.434, where “VAL service” is mentioned as “SEAL service”. SEAL is only an enabler for verticals not a service. To avoid confusion among readers, this CR corrects or replaces the term “SEAL service” to “VAL service” in the following places (highlighted): 5.2.5 Authorization framework Authorization framework is shown in figure 5.2.5-1. A secure HTTP tunnel using HTTPS between VAL UE and VAL server shall be established before SEAL service authorization. Subsequent SEAL service authorization messaging make use of this tunnel. The service clients in the VAL UE present the access tokens to the SEAL service server over HTTP. The SEAL service server authorizes the user for the requested services on if the access token is valid. The procedures may be repeated as necessary to obtain additional SEAL user authorizations. 5.3.1 General To enable security for SEAL services, a SEAL KM client (located in either a SEAL UE or VAL server) may request key material applicable to a particular SEAL service, VAL client or user.  This CR also, corrects a minor editorial in clause 5.2.2 and 5.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 5.2.X VAL service authorization The VAL service authorization procedure shall validate the VAL user authorized to access the VAL services.  In order to gain access to VAL services, the VAL client shall present an access token to the VAL server for each VAL service of interest (see clause 5.2.5). If the access token is valid, then the VAL client shall be granted use of the requested VAL service. 5.2.5 Authorization framework Authorization framework is shown in figure 5.2.5-1. A secure HTTP tunnel using HTTPS between VAL UE and VAL server shall be established before VAL service authorization. Subsequent VAL service authorization messaging make use of this tunnel. The service clients in the VAL UE present the access tokens to the VAL server over HTTP. The VAL server authorizes the user for the requested services on if the access token is valid. The procedures may be repeated as necessary to obtain additional VAL user authorizations. 5.3.1 General To enable security for VAL services, a SEAL KM client (located in either a SEAL UE or VAL server) may request key material applicable to a particular VAL service, VAL client or user.  In clause 5.2.3 “- Shall be provisioned into the SEAL Key management server (SKM-S) and mapped to UE specific key material.” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misleads the procedures defined in specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.X (new), 5.2.2, 5.2.5, 5.3.1, 5.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

*\*\*\*\*\*First Change\*\*\*\*\**

### 5.2.X VAL service authorization

The VAL service authorization procedure shall validate the VAL user authorized to access the VAL services.  In order to gain access to VAL services, the VAL client shall present an access token to the VAL server for each VAL service of interest (see clause 5.2.5). If the access token is valid, then the VAL client shall be granted use of the requested VAL service.

### 5.2.2 SEAL service authorization

SEAL Service Authorization procedure shall validate the VAL user to access the SEAL services. In order to gain access to SEAL services, the SEAL client shall present an access token to the SEAL server for each service of interest. If the access token is valid, then the client shall be granted to use the service.

*\*\*\*\*\*Second Change\*\*\*\*\**

### 5.2.3 Identity management functional model

The SEAL Identity Management Server (SIM-S) and the SEAL Identity Management Client (SIM-C) provide the endpoints for VAL user authentication as shown in the SEAL Identity Management functional model in figure 5.2.3-1.

The reference point IM-UU utilizes Uu reference point as described in 3GPP TS 23.401 [7] and 3GPP TS 23.501 [8]. IM-UU shall support OpenID Connect 1.0 [5] and OAuth 2.0 [9] for VAL user authentication.



Figure 5.2.3-1: Functional model for SEAL Identity Management

In order to support VAL user authentication, the SIM-S shall be provisioned with the VAL user ID and VAL service IDs (usage of VAL user ID and VAL service ID is described in clause 7 of TS 23.434 [2]). A mapping between the VAL user ID and VAL service ID(s) shall be created and maintained in the SIM-S. When a VAL user wishes to authenticate for the VAL services, the VAL user ID and credentials are provided via the UE Identity management client to the SIM-S as per OpenID Connect 1.0 [5]. The SIM-S receives and shall verify the VAL user ID and credentials. If verification is successful, then the SIM-S returns an ID token, refresh token and access token to the UE Identity management client. The SIM-C shall learn the user's VAL service ID(s) from the ID token. Table A shows the SEAL specific tokens and their usage.

Table 5.2.3-1: VAL UE authentication token

|  |  |  |
| --- | --- | --- |
| Token Type | Consumer of the Token | Description |
| ID token | VAL UE client(s) | Contains the VAL service ID for at least one authorized VAL service. |
| Access token | SKM-S, SEAL service server(s) | Short-lived token (definable in the SIM-S) that conveys the UE's identity. This token contains the VAL service ID for at least one authorized service. |
| Refresh token | SIM-S (Authorization Server) | Allows VAL UE to obtain a new access token without forcing user to log in again. |

To support the VAL service identity functional model, the VAL service ID(s):

- Shall be provisioned into the SEAL Identity management database and mapped to VAL UE IDs.

- Shall be provisioned into the SEAL Key management server (SKM-S) and mapped to UE specific key material.

*\*\*\*\*\*Third Change\*\*\*\*\**

### 5.2.5 Authorization framework

Authorization framework is shown in figure 5.2.5-1. A secure HTTP tunnel using HTTPS between VAL UE and VAL server shall be established before VAL service authorization. Subsequent VAL service authorization messaging make use of this tunnel. The service clients in the VAL UE present the access tokens to the VAL server over HTTP. The VAL server authorizes the user for the requested services only if the access token is valid. The procedures may be repeated as necessary to obtain additional VAL user authorizations.

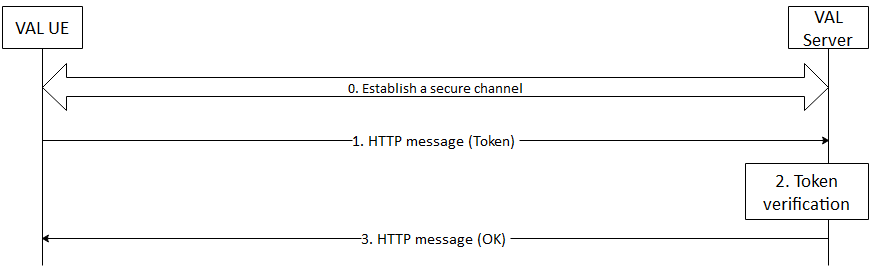


Figure 5.2.5-1: VAL User Service Authorization

After the VAL UE establishing a secure connection with the VAL server, the VAL UE sends an HTTP message containing the access token to the VAL server where service authorization is requested. The VAL server receives the message and validates the access token. If the access token is valid, The VAL server positively acknowledges the request. The VAL server may provide service related information to the VAL UE at this time.

*\*\*\*\*\*Fourth Change\*\*\*\*\*\**

## 5.3 SEAL key management procedure

### 5.3.1 General

To enable security for VAL services, a SEAL KM client (located in either a SEAL UE or VAL server) may request key material applicable to a particular VAL service, VAL client or user.

Prior to making a key management request to the SEAL KMS (SKM-S), the VAL client or VAL user shall be authenticated by the SEAL identity management service (clause 5.2). In addition, secure connections shall be established between the SEAL client and the SKM-S (reference point KM-UU) and the VAL server and the SKM-S (reference point KM-S) prior to any associated key management requests.

As a result of the SEAL identity management authentication procedure, an access token scoped for key management services is provisioned to the SEAL UE. This access token is provided with each and every key management request to the SKM-S.

A VAL server is provisioned with an access token scoped for SEAL key management services and is provided with each and every key management request to the SKM-S. The method for provisioning this access token into the VAL server is out of scope of the present document.

Figure 5.3.1-1 shows the SEAL key management procedure. A SKM client may send a SEAL KM Request message to the SKM-S. The SKM-S validates and processes the request and responds with a SEAL KM Response message. The response contains key management material specific to the SEAL service or the VAL server request, or alternatively, an error code if the SKM-S encounters a failure condition.



Figure 5.3.1-1: SEAL key management procedure

The procedure in figure 5.3.1-1 is described here:

1. The SKM-C establishes a direct HTTPS connection to the SKM-S. Steps 2 and 3 are within this secure connection.

2. The SKM-C sends a SEAL KM Request message to the SKM-S. The request contains the authorization credentials obtained during authentication and message content specified in clause 5.3.2.

3. The SKM-S authorizes the request and if valid, sends a SEAL KM Response message containing the requested key material (or error code) as specified in clause 5.3.3.

As a successful result of this procedure, the VAL UE or VAL Server has securely obtained service specific key material for use within the VAL system.

*\*\*\*\*\*End Change\*\*\*\*\**