**3GPP TSG-SA3 Meeting #102-e *S3-210451***

**e-meeting, 18 - 29 January 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.434** | **CR** | **0003** | **rev** | **1** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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:*** | CR for correction in clause 5.2.4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** | Samsung | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SEAL | | | | |  | ***Date:*** | | | 2020-12-31 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | To clarify that access token uniquely identifies the user of VAL service or key management service. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Step6 is updated as follows:  Step 6: SIM-S sends an OpenID Connect Token Response to the UE containing an ID token and an access token (each which uniquely identify the user of the VAL service or key management service). The ID token is consumed by the UE to personalize the VAL client for the VAL user, and the access token is used by the UE to communicate and authorize the identity of the VAL user to the VAL server(s) and the VAL services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The procedure in clause 5.2.4 is incomplete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

***\*\*\*\*\*Start of Change\*\*\*\*\****

### 5.2.4 Authentication framework

Figure 5.2.4-1 describes the VAL Authentication Framework using the OpenID Connect protocol. It describes the steps by which a VAL UE authenticates to the SIM-S, resulting in a set of credentials delivered to the UE uniquely identifying the VAL service ID(s). The authentication framework supports extensible user authentication solutions based on the VAL service provider policy (shown as step 3). User authentication methods in support of step 3 (e.g. biometrics, secureID, etc.) are possible but not defined here.



Figure 5.2.4-1: OpenID Connect (OIDC) flow supporting VAL user authentication

Step 1: VAL UE establishes a secure tunnel with the SIM-S.

Step 2: VAL UE sends an OpenID Connect Authentication Request to the SIM-S. The request may contain an indication of authentication methods supported by the UE.

Step 3: User Authentication is performed between VAL UE and the SIM-S.

NOTE: The primary credentials for user authentication (e.g. biometrics, secureID, OTP, username/password) are based on VAL service provider policy. The method chosen by the VAL service provider for authentication and authorization is neither defined nor limited by the present document, it depends on the Vertical services and authentication and authorization methods supported by it.

Step 4: SIM-S sends an OpenID Connect Authentication Response to the UE containing an authorization code.

Step 5: UE sends an OpenID Connect Token Request to the SIM-S, passing the authorization code.

Step 6: SIM-S sends an OpenID Connect Token Response to the UE containing an ID token and an access token (each which uniquely identify the user of the VAL service or key management service). The ID token is consumed by the UE to personalize the VAL client for the VAL user, and the access token is used by the UE to communicate and authorize the identity of the VAL user to the VAL server(s) and the VAL services.

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