**3GPP TSG-CT3 Meeting #134C3-242xxx**

**Changsha, China, 15th – 19st April 2024 was C3-242349**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.486** | **CR** | **0122** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | Corrections and updates to the security related provisions |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | NBI18 |  | ***Date:*** | 2024-04-18 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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 canbe 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The following issues have been identified:* Clause 7 should be voided and replaced with per-API "Security" clause that refer directly to TS 29.122. This will enable to align with how the new APIs defined in Rel-18 have been documented and the NBI TS skeleton. In addition, this clause may introduce confusion with clause 8 (especially clause 8.2) to the readers as it addresses similar aspects.
 |
|  |  |
| ***Summary of change:*** | This CR proposes to:* Address and correct the above-detailed issues.
 |
|  |  |
| ***Consequences if not approved:*** | * The above-detailed issues are not corrected and the quality of the specification is not enhanced.
 |
|  |  |
| ***Clauses affected:*** | 7, 8.1, 8.2 |
|  |  |
|  | **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 does not impact the OpenAPI descriptions of the APIs defined in this specification. |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* \* Start of changes \* \* \* \*

# 7 Security

TLS shall be used to support the security communication between the VAE Server and the VASS over the Vs interface, and also between different VAE Servers over the VAE-E interface as specified in 3GPP TS 33.536 [31] and 3GPP TS 33.501 [32]. The access to the VAE service APIs shall be authorized by means of OAuth2.0 protocol (see IETF RFC 6749 [23]), based on local configuration, using the "Client Credentials" authorization grant. If OAuth2.0 is used, a client, prior to consuming services offered by the VAE service APIs, shall obtain a "token" from the authorization server.

\* \* \* \* Next changes \* \* \* \*

## 8.1 General

When CAPIF is used with a VAE service, the VAE Server shall support the following as defined in 3GPP TS 29.222 [26]:

- the API exposing function and related APIs over CAPIF-2/2e and CAPIF-3/3e reference points;

- the API publishing function and related APIs over CAPIF-4/4e reference point;

- the API management function and related APIs over CAPIF-5/5e reference point; and

- at least one of the security methods for authentication and authorization, and related security mechanisms.

In a centralized deployment as defined in 3GPP TS 23.222 [25], where the CAPIF Core Function and API provider domain functions are co-located, the interactions between the CAPIF Core Function and API provider domain functions may be independent of CAPIF-3/3e, CAPIF-4/4e and CAPIF-5/5e reference points.

When CAPIF is used with a VAE service, the VAE Server shall register all the features for northbound APIs in the CAPIF Core Function.

\* \* \* \* Next changes \* \* \* \*

## 8.2 Security

When CAPIF is used for external exposure, before invoking the API exposed by the VAE Server, the service consumer, acting as a CAPIF API invoker, shall negotiate the security method (PKI, TLS-PSK or OAuth2.02) with the CAPIF Core Function and ensure that the VAE Server has enough credentials to authenticate the service consumer (e.g., VASS), see clauses 5.6.2.2 and 6.2.2.2 of 3GPP TS 29.222 [26].

If the PKI or TLS-PSK is used as the selected security method between the service consumer and the VAE Server, upon API invocation, the VAE Server shall retrieve the authorization information from the CAPIF Core Function as described in clause 5.6.2.4 of 3GPP TS 29.222 [26].

As indicated in 3GPP TS 33.122 [27], the access to the VAE Server APIs may be authorized by means of the OAuth2.0 protocol (see IETF RFC 6749 [23]), using the "Client Credentials" authorization grant, where the CAPIF Core Function (see 3GPP TS 29.222 [26]) plays the role of the authorization server.

NOTE 1: In this release of this specification, only the "Client Credentials" authorization grant is supported.

If OAuth2.0 is used as the selected security method between the service consumer and the VAE Server:

- the service consumer shall, prior to consuming the services offered by the VAE Server, obtain a "token" from the authorization server, by invoking the Obtain\_Authorization service as described in clause 5.6.2.3.2 of 3GPP TS 29.222 [26]; and

- the VAE Server APIs do not define any scopes for OAuth2.0 authorization. It is the VAE Server responsibility to check whether the service consumer is authorized to use an API based on the OAuth2.0 "token". Once the VAE Server verifies the "token", it shall check whether the VAE Server identifier in the "token" matches its own published identifier, and whether the API name in the "token" matches its own published API name. If those checks are passed, the service consumer has full authority to access any resources or operations of the invoked API.

NOTE 2: For the aforementioned security methods, the VAE Server needs to apply admission control according to access control policies after performing the authorization checks.

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