**3GPP TSG-CT3 Meeting #116e C3-21xxxx**

**E-Meeting, 19th – 28th May 2021 (Revision of C3-213193)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.486** | **CR** | **0055** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  |
| *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:***  | CAPIF support |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | eV2XAPP |  | ***Date:*** | 2021-05-01 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  Rel-17 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | TS 23.286 specifies the CAPIF adaptation for VAE server. The corresponding stage 3 description should also be added. |
|  |  |
| ***Summary of change:*** | Add CAPIF description. |
|  |  |
| ***Consequences if not approved:*** | Missing the CAPIF description. |
|  |  |
| ***Clauses affected:*** | 2, 3.3, X (new), X.1 (new), X.2 (new) |
|  |  |
|  | **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 openAPI file. |
|  |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* 1st Change \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[3] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[4] 3GPP TS 23.286: "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows".

[5] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[6] OpenAPI: "OpenAPI Specification Version 3.0.0", <https://spec.openapis.org/oas/v3.0.0>.

[7] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[8] 3GPP TR 21.900: "Technical Specification Group working methods".

[11] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[12] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[13] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[14] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[15] IETF RFC 7233: "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".

[16] IETF RFC 7234: "Hypertext Transfer Protocol (HTTP/1.1): Caching".

[17] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[18] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[19] 3GPP TS 29.116: "Representational state transfer over xMB reference point between Content Provider and BM-SC".

[20] 3GPP TS 29.572: "5G System; Location Management Services; Stage 3".

[21] IETF RFC 6455: "The Websocket Protocol".

[22] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[23] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[24] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[TS23222] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs; Stage 2".

[TS29222] 3GPP TS 29.222: "Common API Framework for 3GPP Northbound APIs; Stage 3".

[TS33122] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

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

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

CAPIF Common API Framework

V2X Vehicle-to-Everything

VAE V2X Application Enabler

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

# X Using Common API Framework

## X.1 General

When CAPIF is used with a VAE service, the VAE server shall support the following as defined in 3GPP TS 29.222 [TS29222]:

- 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 [TS23222], 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.

## X.2 Security

When CAPIF is used for external exposure, before invoking the API exposed by the VAE server, the NF service consumer (e.g. V2X application specific server) as API invoker shall negotiate the security method (PKI, TLS-PSK or OAUTH2) with CAPIF core function and ensure the VAE server has enough credential to authenticate the NF service consumer (e.g. V2X application specific server), see 3GPP TS 29.222 [TS29222], clause 5.6.2.2 and clause 6.2.2.2.

If PKI or TLS-PSK is used as the selected security method between the NF service consumer (e.g. V2X application specific server) and the VAE server, upon API invocation, the VAE server shall retrieve the authorization information from the CAPIF core function as described in 3GPP TS 29.222 [TS29222], clause 5.6.2.4.

As indicated in 3GPP TS 33.122 [TS33122], the access to the VAE APIs may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [23]), using the "Client Credentials" authorization grant, where the CAPIF core function (see 3GPP TS 29.222 [TS29222]) plays the role of the authorization server.

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

If OAuth2 is used as the selected security method between the NF service consumer (e.g. V2X application specific server) and the VAE server, the the NF service consumer (e.g. V2X application specific server), prior to consuming services offered by the VAE APIs, shall obtain a "token" from the authorization server, by invoking the Obtain\_Authorization service, as described in 3GPP TS 29.222 [TS29222], clause 5.6.2.3.2.

The VAE APIs do not define any scopes for OAuth2 authorization. It is the VAE server responsibility to check whether the NF service consumer (e.g. V2X application specific server) is authorized to use an API based on the "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 NF service consumer (e.g. V2X application specific server) has full authority to access any resource or operation for the invoked API.

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

\*\*\* End of Changes \*\*\*