**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *S3-23xxxx***

**Electronic meeting, Online, 17 - 21 April 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | draft CR on resource owner aware northbound acces to APIs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | NTT DOCOMO | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2023-04-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 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:*** | | The CR provides security for resource owner aware northbound access to APIs | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The CR provides the architecture enhancement required for securing resourcer owner aware northbound access to APIs.  In addition, it provides the detailed updates to the individual reference points. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Resource owner aware northbound access to APIs is not secured | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Draft provided to SA3#110-adhoc-e | | | | | | | | |

++++++ First 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].

AEF API Exposing Function

API Application Programming Interface

CAPIF Common API Framework

JSON JavaScript Object Notation

JWT JSON Web Token

KDF Key Derivation Function

PKI Public Key Infrastructure

PSK Pre-Shared Key

RNAA Resource owner-aware northbound API access

TLS Transport Layer Security

++++++ Next Change ++++++

# 5 Functional security model

## 5.1 General functional security model

Figure 5-1 shows the functional security model for the CAPIF architecture. The interfaces CAPIF-1, CAPIF-1e, CAPIF-2, CAPIF-2e, CAPIF-3, CAPIF-4, CAPIF-5, CAPIF-3e, CAPIF-4e, CAPIF-5e, CAPIF-7 and CAPIF-7e are defined in 3GPP TS 23.222 [3] and support the CAPIF functionality defined in 3GPP TS 23.222 [3]. CAPIF-1, CAPIF-2, CAPIF-3, CAPIF-4, CAPIF-5 and CAPIF-7 are interfaces that lie within the PLMN trust domain while the CAPIF-1e , CAPIF-2e, CAPIF-3e, CAPIF-4e, CAPIF-5e and CAPIF-7e interfaces are CAPIF core and AEF access points for API Invokers outside of the PLMN trust domain.

Security for the CAPIF-1, CAPIF-2, CAPIF-3, CAPIF-4, CAPIF-5 and CAPIF-7 interfaces support TLS and are defined in subclauses 6.2, 6.4 and 6.6 of the present document. Security for the CAPIF-1e, CAPIF-2e and CAPIF-7e interfaces support TLS, and are defined in subclause 6.3, subclause 6.5, and subclause 6.9 respectively.

Security for the CAPIF-3e, CAPIF-4e and CAPIF-5e interfaces support NDS/IP security to secure communication between different IP security domains. This avoids multiple secure connections between API provider domain and CAPIF core domain by leveraging the NDS/IP security procedures specified in TS 33.210 [2].

Authentication and authorization are required for both API invokers that lie within the PLMN trust domain and API invokers that lie outside of the PLMN trust domain. For an API invoker that is outside of the PLMN trust domain, the CAPIF core function in coordination with the API exposing function utilizes the CAPIF-1e, CAPIF-2e and the CAPIF-3 interfaces to onboard, authenticate and authorize the API invoker prior to granting access to CAPIF services. Security flow diagrams for onboarding security, CAPIF-1e security and CAPIF-2e security can be found in Annex B. When the API invoker is within the PLMN trust domain, the CAPIF core function in coordination with the API exposing function perform authentication and authorization of the API invoker via the CAPIF-1, the CAPIF-2 and the CAPIF-3 interfaces prior to granting access to CAPIF services. Authentication and authorization of API invokers (both internal and external to the PLMN trust domain) is specified in clause 6 of the present document.



Figure 5-1: CAPIF functional security model

## 5.2 Functional security model supporting RNAA

tbd

++++++ Next Change ++++++

## 6.5 Security procedures for CAPIF-2e reference point

### 6.5.Y2e Authentication and authorization for RNAA

Editor's note: this clause provides the detailed flow required for authorizing an RNAA access. For oAuth based authorization, this includes the oAuth flow.

+++++ End of Changes +++++