**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *S3-234360***

**Berlin, Germany, 22-26 May 2023 was S3-234300**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.122** | **CR** | **0036** | **rev** | **-**  | **Current version:** | **18.0** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | CR on security for resource owner aware northbound access to APIs  |
|  |  |
| ***Source to WG:*** | NTT DOCOMO, Nokia, Nokia Shanghai Bell, Lenovo, Qualcomm, Huawei, Xiaomi, Samsung, Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SNAAPPY |  | ***Date:*** | 2023-08-20 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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-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 updates to the individual reference points. |
|  |  |
| ***Consequences if not approved:*** | Resource owner aware northbound access to APIs is not secured |
|  |  |
| ***Clauses affected:*** | 2, 3.3, 4.8, 5, new clause 6.5.Y2e |
|  |  |
|  | **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:*** | Editor's notes are there for later alignment with CT specifications |
|  |  |
| ***This CR's revision history:*** | Draft provided to SA3#112, updated by S3-234297, S3-234298, S3-234299 |

++++++ First 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 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[3] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

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

[5] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[6] IETF RFC 7519: "JSON Web Token (JWT)".

[7] IETF RFC 7515: "JSON Web Signature (JWS)".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] Void

[10] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[XX] IETF RFC 7636: " Proof Key for Code Exchange by OAuth Public Clients".

++++++ 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].

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 ++++++

## 4.8 Security requirements on the CAPIF-8/8e reference points

CAPIF-8/8e interface is not in scope of 3GPP. Nevertheless, integrity and confidentiality protection, protection against replay attacks, privacy of the resource owner, authentication between the resource owner and the CCF need to be addressed by mechanism(s) which are out of 3GPP scope.

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

# 5 Functional security model

## 5.1 General functional security model

Figure 5.1-1 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 5.1-1: CAPIF functional security model

## 5.2 Functional security model supporting RNAA

Figure 5.2-1 shows the functional security architecture of CAPIF when RNAA is supported. The authorization function itself is a part of the CCF. The Oauth client and the CCF shall communicate using https.



Figure 5.2-1: CAPIF supporting RNAA functional security model

Editor's note: the above figure will need alignment with SA6.

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

### 6.5.Y2e Authentication and authorization for RNAA

#### 6.5.Y2e.1 General

RNAA shall use token-based authorization using OAuth 2.0 framework with the following roles:

- The API invoker has the role of the OAuth 2.0 client.

- The CCF has the role of the OAuth 2.0 authorization server, i.e., providing the access token used for RNAA.

- The AEF has the role of the resource server.

The access tokens used for RNAA can contain the resource owner identity claim and other claims.

The resource owner can be the user of the UE or the owner of the subscription depending on the use case and regulations. The present document does not specify the resource owner, but the resource owner ID is specified as the GPSI of the corresponding UE if the resource is related to a UE.

The access token shall include the resource owner ID and the API invoker ID. GPSI is used as identifier for the resource owner. The token issuer ID is the CCF ID. The API invoker ID binds the token to the API invoker. To avoid privacy issues, GPSI needs to be different from MSISDN, SUPI etc.

Editor's Note: The details of access tokens used for RNAA need to be aligned with stage 3 (e.g., claim versus scope).

AEF shall do the authorization check of the API invocation request. AEF checks the request against the token, including the resource owner identity. As the token includes resource owner identity, there is no need for additional UE authentication in API invocation. Moreover, the token should be able to restrict the API invoker to a specific resource (e.g., location, QoS, PDN connectivity status).

For Oauth flows involving redirection, authentication between CCF/AUF and UE should be performed after API Invoker redirects the UE to CCF/AUF.

In case of an external AF (i.e., not the application on the UE) being the API invoker, for mutual authentication of API invoker AF and API exposing function, the authentication methods of clause 6.4 and 6.5.2 are reused.

For authorization, the following flows can be used:

- Client credential flow (according to RFC 6749 [4]),

- Authorization code flow (according to RFC 6749 [4]), or

- Authorization code flow with PKCE (according to RFC 7636 [XX]).

Editor's Note: How to choose the flow is left to stage 3.

CCF shall give service authorization which subscribers or users can use RNAA.

NOTE: In this specification, only a UE accessing its own resources is considered if the API invoker is on a UE.

#### 6.5.Y2e.2 Authorization using oauth client credential flow

If client credential flow is used for authorization of the API invoker by the AEF, the procedures in RFC 6749 [4] shall be followed with the following profile:

- The access token request message may include the resource owner ID.

NOTE 1: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

Editor’s note: the mapping of API Invoker ID and GPSI is left for stage 3.

- The CCF shall check whether the API invoker is entitled to consume the API and allowed to access the resources of the resource owner, by using authorization information available in the CCF.

- If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources. If the API invoker is an AF not on a UE, the check is omitted.

Editor's Note: Further details of the token are left for stage 3, this includes how to differentiate RNAA and legacy tokens

NOTE 2: How to get the authorization from the resource owner and store it in the CCF is out of scope of the present document.

#### 6.5.Y2e.3 Authorization using authorization code (optional PKCE) flow

If authorization code flow, optionally with PKCE, is used by the AEF for authorization of the API invoker, the procedures in RFC 6749 [4] and optionally RFC 7636 [XX] shall be followed, with the following profile:

- The authorization token and/or authorization request may include the resource owner ID.

Editor’s Note: Whether and how the token and/or authorization request can include resource owner ID is left to stage 3.

NOTE: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

Editor's note: the mapping of API Invoker ID and GPSI is left for stage 3.

- The resource owner dynamically allows the API invoker to access the resource owner's resources as described in RFC 6749 [4] and optionally RFC 7636 [XX]

- If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources. The access token shall contain the resource owner ID (i.e. GPSI) and the API invoker ID. If the API invoker is an AF not on a UE, the check is omitted.

Editor's Note: further details of the token are left for stage 3, this includes how to differentiate RNAA and legacy tokens

#### 6.5.Y2e.4 Revocation

API Exposing Function needs to be informed about revocation if this is necessary to ensure correct handling of revocation.

Editor's note: this clause describes the revocation procedure, unless this is taken care of by SA6 as it is for non RNAA use cases.

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