ETSI TS 133 122 V17.0.0 (2022-04)

LTE;
5G;
Security aspects of Common API Framework (CAPIF)
for 3GPP northbound APIs
(3GPP TS 33.122 version 17.0.0 Release 17)

Reference
RTS/TSGS-0333122vh00

Keywords
5G,LTE,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the security architecture i.e., the security features and the security mechanisms for the common API framework (CAPIF) as per the architecture and procedures defined in 3GPP TS 23.222 [3].

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".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Symbols

For the purposes of the present document, the following symbols apply:

AEF_{PSK} Pre-Shared Key for AEF

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
TLS	Transport Layer Security

4 Security requirements

4.1 General

Architectural requirements pertaining to CAPIF security are found in 3GPP TS 23.222 [3]. The following are CAPIF derived security requirements.

4.2 Common security requirements

Security requirements that are applicable to all CAPIF entities are:

- [CAPIF-SEC-4.2-a] The CAPIF shall provide mechanisms to hide the topology of the PLMN trust domain from the API invokers accessing the service APIs from outside the PLMN trust domain.
- [CAPIF-SEC-4.2-b] The CAPIF shall provide mechanisms to hide the topology of the 3rd party API provider trust domain from the API invokers accessing the service APIs from outside the 3rd party API provider trust domain.
- [CAPIF-SEC-4.2-c] The CAPIF shall provide authorization mechanism for service APIs from the 3rd party API providers.
- [CAPIF-SEC-4.2-d] The CAPIF shall support a common security mechanism for all API implementations to provide confidentiality and integrity protection.
- [CAPIF-SEC-4.2-e] API invoker authentication and authorization shall support all deployment models listed in 3GPP TS 23.222 [3].
- [CAPIF-SEC-4.2-f] The API invoker and CAPIF should enforce the result of the authentication for the duration of communications (e.g. by integrity protection or implicit authentication by encryption with a key that is derived from the authentication and is unknown to the adversary).

4.3 Security requirements on the CAPIF-1/1e reference points

The CAPIF-1/1e reference points between the API invoker and the CAPIF core function shall fulfil the following requirements:

- [CAPIF-SEC-4.3-a] Mutual authentication between the API invoker and the CAPIF Core function shall be supported.
- [CAPIF-SEC-4.3-b] The transport of messages over the CAPIF-1 and CAPIF-1e reference points shall be integrity protected.

- [CAPIF-SEC-4.3-c] The transport of messages over the CAPIF-1 and CAPIF-1e reference points shall be protected from replay attacks.
- [CAPIF-SEC-4.3-d] The transport of messages over the CAPIF-1 and CAPIF-1e reference points shall be confidentiality protected.
- [CAPIF-SEC-4.3-e] Privacy of the 3GPP user over the CAPIF-1 and CAPIF-1e reference points shall be protected.
- [CAPIF-SEC-4.3-f] The CAPIF core function shall authorize the API invoker prior to the API invoker accessing the AEF.
- [CAPIF-SEC-4.3-g] The CAPIF core function shall authorize the API invoker prior to accessing the discover service API.
- [CAPIF-SEC-4.3-h] The CAPIF core function shall authenticate the API invoker's onboarding request.
- [CAPIF-SEC-4.3-i] The CAPIF core function shall authenticate the API invoker's offboarding request.

4.4 Security requirements on the CAPIF-2/2e reference points

The CAPIF-2/2e reference points between the API invoker and API exposing function shall fulfil the following requirements:

- [CAPIF-SEC-4.4-a] Mutual authentication between the API invoker and the API exposing function shall be supported.
- [CAPIF-SEC-4.4-b] The transport of messages over the CAPIF-2 and CAPIF-2e reference points shall be integrity protected.
- [CAPIF-SEC-4.4-c] The transport of messages over the CAPIF-2 and CAPIF-2e reference points shall be protected from replay attacks.
- [CAPIF-SEC-4.4-d] The transport of messages over the CAPIF-2 and CAPIF-2e reference points shall be confidentiality protected.
- [CAPIF-SEC-4.4-e] Privacy of the 3GPP user over the CAPIF-2 and CAPIF-2e reference points shall be protected.
- [CAPIF-SEC-4.4-f] The API exposing function shall determine whether API invoker is authorized to access service API.

4.5 Security requirements on the CAPIF-3/4/5 reference points

The security requirements for CAPIF-3/4/5 reference points are:

- [CAPIF-SEC-4.5-a] The transport of messages over the CAPIF-3/4/5 reference points shall be integrity protected.
- [CAPIF-SEC-4.5-b] The transport of messages over the CAPIF-3/4/5 reference points shall be confidentiality protected.
- [CAPIF-SEC-4.5-c] The transport of messages over the CAPIF-3/4/5 reference points shall be protected from replay attacks.
- [CAPIF-SEC-4.5-d] The CAPIF core function shall be able to authenticate the service API publishers to publish and manage the service API information.
- [CAPIF-SEC-4.5-e] The CAPIF core function shall be able to authorize the service API publishers to publish and manage the service API information.
- [CAPIF-SEC-4.5-f] The CAPIF core function shall be able to request explicit grant of new API invoker’s onboarding.

- [CAPIF-SEC-4.5-g] The CAPIF core function shall be able to authenticate the API Management function's registration request for API Provider domain functions.
- [CAPIF-SEC-4.5-h] The CAPIF core function shall be able to authenticate the API Management function's registration update request for API provider domain functions.

4.6 Security requirements on the CAPIF-3e/4e/5e reference points

The security requirements for CAPIF-3e/4e/5e reference points are:

- [CAPIF-SEC-4.6 -a] The transport of messages over the CAPIF-3e/4e/5e reference points shall be integrity protected.
- [CAPIF-SEC-4. 6 -b] The transport of messages over the CAPIF-3e/4e/5e reference points shall be confidentiality protected.
- [CAPIF-SEC-4. 6 -c] The transport of messages over the CAPIF-3e/4e/5e reference points shall be protected from replay attacks.
- [CAPIF-SEC-4. 6 -d] The CAPIF core function shall be able to authenticate the service API publishers to publish and manage the service API information.
- [CAPIF-SEC-4. 6 -e] The CAPIF core function shall be able to authorize the service API publishers to publish and manage the service API information.
- [CAPIF-SEC-4. 6 -f] The CAPIF core function shall be able to request explicit grant of new API invoker's onboarding.
- [CAPIF-SEC-4.6-g] The CAPIF core function shall be able to authenticate the API Management function's registration request for API Provider domain functions.
- [CAPIF-SEC-4.6-h] The CAPIF core function shall be able to authenticate the API Management function's registration update request for API provider domain functions.

4.7 Security requirements on the CAPIF-7/7e reference points

The security requirements for CAPIF-7/7e reference points are:

- [CAPIF-SEC-4.7-a] The transport of messages over the CAPIF-7 and CAPIF-7e reference points shall be integrity protected.
- [CAPIF-SEC-4.7-b] The transport of messages over the CAPIF-7 and CAPIF-7e reference points shall be protected from replay attacks.
- [CAPIF-SEC-4.7-c] The transport of messages over the CAPIF-7 and CAPIF-7e reference points shall be confidentiality protected.
- [CAPIF-SEC-4.7-d] Privacy of the 3GPP user over the CAPIF-7 and CAPIF-7e reference points shall be protected.
- [CAPIF-SEC-4.7-e] The API exposing function (destination AEF handling service API) shall determine whether AEF that is topology hiding entity, is authorized to access service API.

5 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.

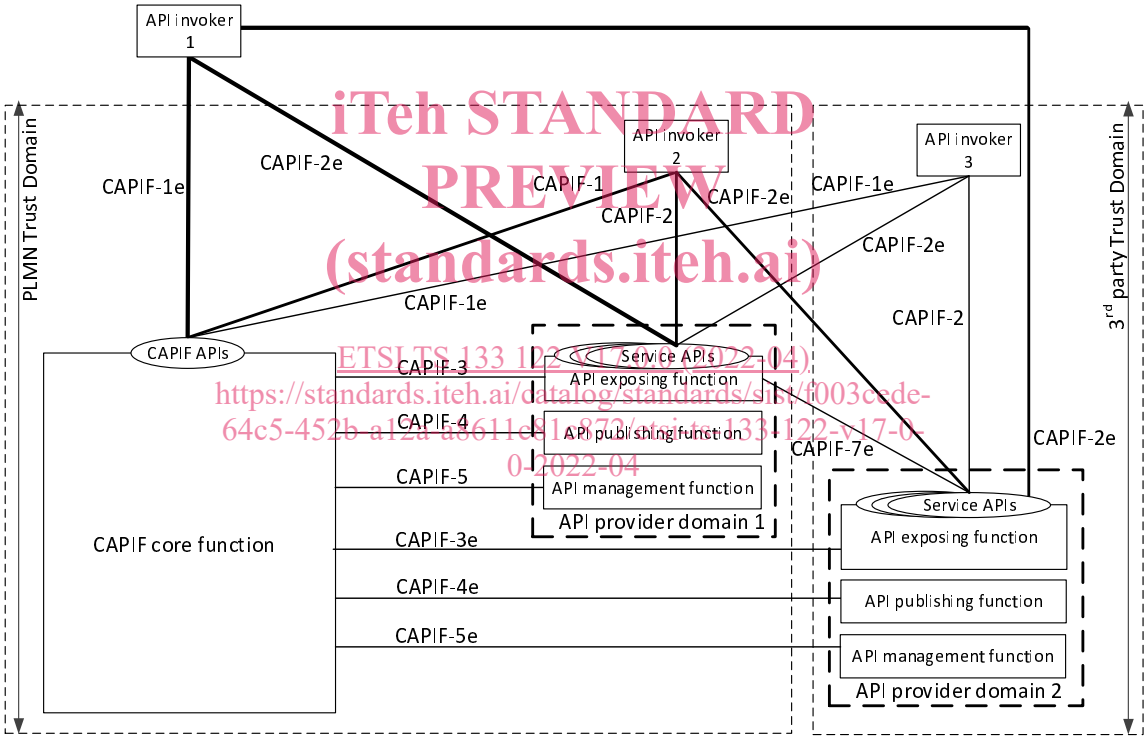

Figure 5-1: CAPIF functional security model

6 Security procedures

6.1 Security procedures for API invoker onboarding

The API invoker and the CAPIF core function shall follow the procedure in this subclause to secure and authenticate the onboarding of the API invoker to the CAPIF core function. The API invoker and the CAPIF core function shall establish a secure session using TLS. Security profiles for TLS implementation and usage shall follow the provisions given in TS 33.310 [2], Annex E .

With a secure session established, the API Invoker sends an Onboard API Invoker Request message to the CAPIF core function. The Onboard API Invoker Request message carries an onboard credential obtained during pre-provisioning of the onboard enrolment information, which may be an OAuth 2.0 [4] access token. When the OAuth 2.0 token based mechanism is used as the onboarding credential, the access token shall be encoded as JSON web token as specified in IETF RFC 7519 [6], shall include the JSON web signature as specified in IETF RFC 7515 [7], and shall be validated per OAuth 2.0 [4], IETF RFC 7519 [6] and IETF RFC 7515 [7]. Other credentials may also be used (e.g. message digest).

Figure 6.1-1 details the security information flow for the API invoker onboarding procedure. The OAuth 2.0 token based authentication credential is shown in this example.

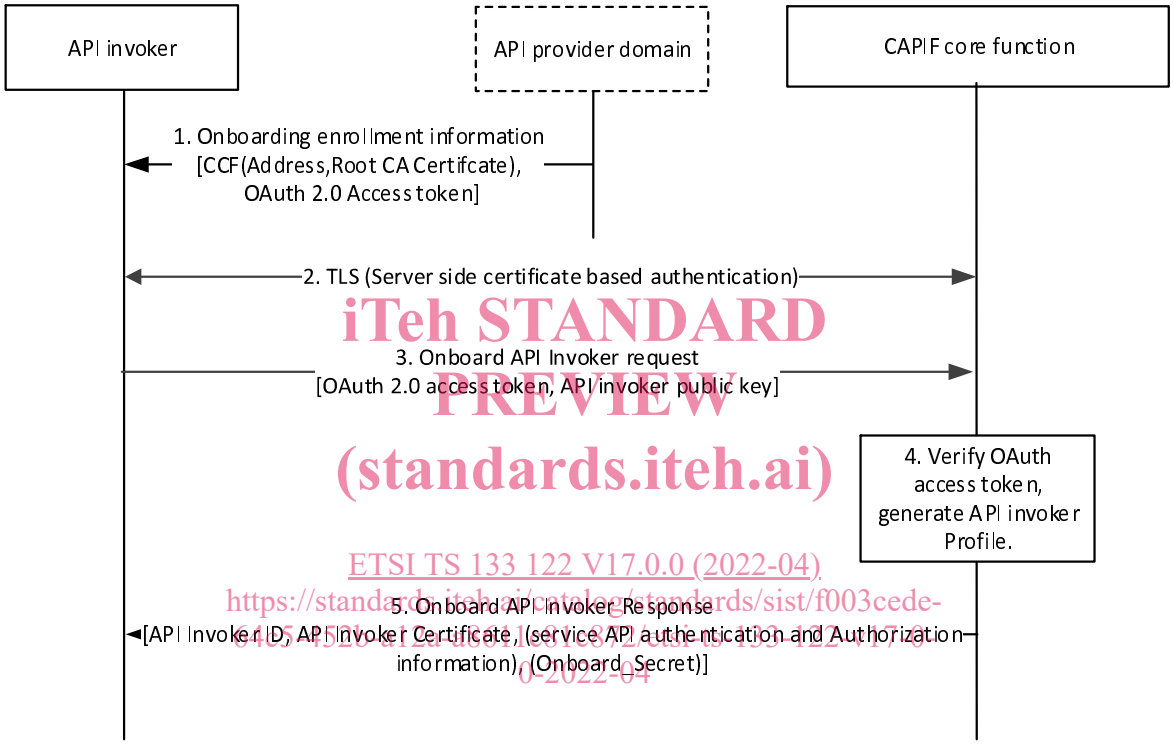

Figure 6.1-1: Security procedure for API invoker onboarding

1. As a prerequisite to the onboarding procedure, the API invoker obtains onboarding enrolment information from the API provider domain. The onboarding enrolment information is used to authenticate and establish a secure TLS communication with the CAPIF core function during the onboarding process. The enrolment information includes details of the CAPIF core function (Address, and Root CA certificate) and includes an onboarding credential (the OAuth 2.0 [4] access token).

NOTE 1: The procedure used to obtain the enrolment information by the API invoker is out of scope of the present document.

2. The API invoker and CAPIF core function shall establish a secure session based on TLS (Server side certificate authentication). The API invoker shall use the enrolment information obtained in step 1 to establish the TLS session with the CAPIF core function.

3. After successful establishment of the TLS session, the API invoker shall send an Onboard API invoker request message to the CAPIF core function along with the enrolment credential (OAuth 2.0 [4] access token). The API invoker generates the key pair {Private Key, Public key} and provides the public key along with the Onboard API invoker request.

4. The CAPIF core function shall validate the enrolment credential (OAuth 2.0 [4] access token). If validation of the credential (the OAuth 2.0 [4] access token in this example) is successful, the CAPIF core function shall