EPC API Security Framework

European Payments Council

European Payments Council AISBL,
Cours Saint-Michel 30 B-1040 Brussels
T +32 2 733 35 33
Enterprise N°0873.268.927
secretariat@epc-cep.eu

EPC164-22
Version 2.1
Date issued: 16 March 2026

Public

Approved

API Security Framework

Abstract	The present document provides the security requirements related to the use of APIs as part of an EPC scheme.
Document Reference	EPC164-22
Issue	Version 2.1
Date of Issue	16 March 2026
Reason for Issue	Updates related to the VOP scheme
Reviewed by	EPC
Produced by	EPC
Circulation	Publicly available

Table of Contents

1. Document information

1.1. References

This section lists documents referred to in this document. The convention used throughout is to provide the reference number only, in square brackets. Use of square brackets throughout is exclusively for this purpose.

	Document Number	Title	Issued by:
[1]	EPC012-22	SEPA Payment Account Access scheme rulebook	EPC
[2]	EPC014-20	SEPA Request-to -Pay scheme rulebook	EPC
[3]	EPC218-23	Verification Of Payee scheme rulebook	EPC
[4]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels https://www.rfc-editor.org/info/rfc2119	S. Bradner
[5]	EPC127-25	EDS User Guide	EPC
[6]	ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles	ETSI
[7]	ETSI TS 119 495	Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking	ETSI
[8]	Directive (EU) 2015/2366	Payment Services Directive (PSD2)	EC
[9]	EPC342-08	Guidelines on cryptographic algorithms usage and key management: https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/yearly-update-guidelines-cryptographic-algorithms-usage-and-0	EPC

1.2. Defined terms or abbreviations

Term/Abbreviation	Definition
AISP	Account Information Service Provider
API	Application Programming Interface
API client	The party that sends the API request for a specific service or data to an API server
API server	The party that accepts the API request, processes it and sends the response information

ASPSP	Account Servicing Payment Service Provider
EDS	EPC Directory Service
EPC	European Payments Council
OSM	Operational Scheme Manager
Participant	An entity that accepted to be a part of the scheme in accordance with this scheme's rulebook
PISP	Payment Initiation Service Provider
Proxy	A "proxy" acts as a message gateway which remains transparent from a scheme perspective; also see definitions of RTSP and RVM below
PSD2	Payment Services Directive
QSealC	Qualified certificates for electronic seals These qualified certificates can be used to protect data and documents from tampering and to identify the origin of the data
QTSP	Qualified Trust Service Provider A QTSP has government-issued qualifications to issue qualified digital certificates under the trust services defined by the EU eIDAS regulation (see "QWAC"). The list of Trust Services Providers able to provide eIDAS certificates is available by the European Commission (EU Trust service dashboard).
QWAC	Qualified Web Authentication certificates: A QWAC is a qualified digital public key certificate under the trust services defined by the EU eIDAS regulation. Within the context of this document, QWAC for website authentication apply; as defined in the European Standard ETSI EN 319 412-4.
QWAC PSD2 / PSD2 QWAC	Qualified Web Authentication certificates issued for use in the PSD2 Open Banking context. A "PSD2 QWAC" is: - A QWAC certificate according the "ETSI TS 119 495" standard - Based on a QCstatement for Open Banking as specified in the ETSI TS 119 495 standard section 5.1, i.e. including ▪ A service provider role ▪ The name of the NCA (National Competent Authority) ▪ A PSP identifier as defined in GEN-5.2.1-3 of the ETSI specification: i.e. starting with 'PSD' and containing the PSP Authorization Number
RoP	Register of Participants
PSP	Payment Service Provider
RTP	Request-to-Pay
RTSP	Referenced Technical Solution Provider SRTP homologated "hub" or "proxy" acting as a message gateway which remains totally "transparent" from a scheme perspective.

RVM	Routing and/or Verification Mechanism in the VOP Scheme. An agent legally authorized to act on behalf of a Participant; transparent from a scheme perspective, and not having any final customers (Payer or Payee) in this role of RVM.
SEPA	Single Euro Payment Area
SPAA	SEPA Payment Account Access
SRTP	SEPA Request to Pay
TLS	Transport Layer Security
TLS EV / EV TLS	Extended Validation (EV) TLS/SSL Certificate An EV Certificate ensures the certificate holder has undergone extensive vetting and identity checks to certify that it is authentic and legitimate
TPP	Third Party Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.3. Background

The use of APIs for the exchanges between scheme Participants will be either mandatory or a feasible option, depending on the EPC schemes.

Since API related security matters are essential and support the actual API exchange, the purpose of this document is to define an API security framework based on widely available European or international security standards, listing the minimum-security related requirements applicable, regardless of the scheme, to scheme Participants using APIs.

The schemes in the current scope are SRTP, SPAA and VOP.

These schemes may rely on a directory service, called EPC Directory Service (EDS), managed by the Operational Scheme Manager (OSM). The registration in and the use of the EDS is under the responsibility of each scheme. Refer to the EDS User Guide [5] for further details.

The security requirements are independent of the API functionality and technical implementation and are applicable to all the schemes using API's and to all the API specifications (market or EPC) used by a scheme Participant, whether the scheme Participant chooses to send and receive messages directly, or whether it chooses to use mutualised services of a Proxy (technical solution provider) acting as a message gateway.

The SPAA, SRTP and VOP schemes are all managed by the EPC and were designed to use APIs for the communication between scheme Participants. Although there are some differences related to how the schemes operate, as well as a difference in maturity between them, and differences in naming the Participants and stakeholders, they are sufficiently similar as messaging schemes to justify a joint effort in defining a common API security framework.

Wherever there is a difference in a scheme that justifies a different approach in the security framework, that difference will be highlighted.

Note:
The capitalized keywords "MUST", “MAY", "SHOULD" and their variants, should be interpreted as defined in RFC 2119 [4].

2. Scope

For the details related to the schemes in scope of this document (i.e., the SPAA, the SRTP and the VOP schemes), please refer to their respective rulebook ([1], [2], [3]).

The purpose of this document is to describe the requirements of an API Security Framework, including:

- The security-related requirements based on widely available European or international security standards. The recommended security measures shall be proportionate and affordable.
- The list of operational requirements that an Operational Scheme Manager (OSM) should provide to ensure a smooth functioning of the framework.

The requirements laid out in this framework only relate to the interaction between the scheme Participants. The interaction between the scheme Participants and their customers as well as between the scheme Participants and the EDS is outside the scope of the framework.

The specifications of these requirements will be the responsibility of each API specification that uses them. In the case of SPAA that would be any API initiative defining a technical specification of the SPAA Scheme Rulebook. In the case of the SRTP and VOP schemes, it would be the responsibility of each scheme respectively to define the content for its own API specifications. In addition, the SRTP scheme shall define the scope of the homologation process related to the below requirements. It is also possible that different API initiatives define the content of other API specifications for SRTP or VOP. In any case, none of those specifications will be a part of this document.

The integration of each specification of the requirements laid out in this framework will be a responsibility of the scheme for which those specifications are intended. Furthermore, the obligation to implement any given specification by a scheme Participant, will also be the responsibility of each scheme.

Although most of the requirements are common and applicable to all schemes, there are some specificities for each of the schemes that will be indicated accordingly.

The requirements in this document are about securing the API itself as an “envelope”, not about securing each piece of information inside each individual message exchanged through the API. Messages may contain information that could lead to fraud if insufficiently secured, such as a Payee’s IBAN. If such information, inside messages, is to be protected, it is the role of Schemes to describe how. The current framework will only ensure that the messages flow correctly between identified, authenticated and authorised Participants, ensuring confidentiality, and that the content of the message was not tampered with in transport. The framework does not look at the content of the messages.

As indicated above, this version of the document includes details for the SPAA, SRTP and VOP schemes. In case other schemes would introduce new APIs, the document will be revised and updated accordingly.

3. Actors and Roles

3.1. Operational Scheme Manager

The Operational Scheme Manager, through the EDS, will collect, validate, maintain and when applicable, make available additional data related to the scheme Participants to ensure an effective functioning of the schemes.
The scheme Participants' requirements related to this role are described in chapter 13.
The requirements applicable to the OSM and EDS are specified in a separate document [5].

3.2. SPAA scheme – Actors and Roles

Please refer to section 1.3 of the SPAA scheme rulebook [1].

For the EDS End-to-End flow, please refer to the EDS User Guide [5].

3.3. SRTP Scheme – Actors and Roles

Please refer to section of 1.3 of the SRTP scheme rulebook [2].

For the EDS End-to-End flow, please refer to the EDS User Guide [5].

3.4. VOP Scheme – Actors and Roles

Please refer to section 2.1 of the VOP scheme rulebook [3].

For the EDS End-to-End flow, please refer to the EDS User Guide [5].

4. Identification

4.1. API server/API client

The SRTP/SPAA related API specifications cover the SRTP/SPAA related messages exchanged between the Payee's SRTP Service Provider/ Asset Broker and the Payer's SRTP Service Provider/Asset Holder, in both directions. The two technical roles being API client or API server depending on the situation. Since some interactions may not be completed synchronously, a call back possibility has been set to send back asynchronous responses.

In the VOP scheme, the Responding PSP provides the API server and the Requesting PSP has the API client role. As clarified above, an RVM can operate one or either of these roles on behalf of the PSP.

The following table provides an overview of the role of the Participants for each of the Schemes:

Scheme	Service Type	API client	API server
SPAA	Regular	Asset Broker	Asset Holder
	Call-back	Asset Holder	Asset Broker
SRTP	Regular	Payee's SRTP Service Provider	Payer's SRTP Service Provider
	Call-back	Payer's SRTP Service Provider	Payee's SRTP Service Provider
VOP	Regular	Requesting PSP	Responding PSP

4.2. API client Customer (dedicated to SPAA scheme)

This will be covered in the SPAA specificities (see Annex 1).

4.3. Scheme Participants Identification requirements

Purpose: unambiguously identify a scheme Participant from a "machine readable" perspective.

Requirement: each Participant MUST have at least one identifier.

Identifiers are given under the responsibility of the Operational Scheme Manager (OSM), which must ensure their unicity per identifier type (the same identifier cannot be given twice) and unambiguousness (it identifies without ambiguity a single scheme Participant).

The OSM may let scheme Participants use identifiers they already have, provided they are compliant with the unicity and unambiguousness requirement (e.g., PSD2 identifier, LEI, VAT number etc…). This allows potential re-use of existing infrastructure for those scheme Participants.

When a scheme Participant does not have such existing identifier, the OSM must provide one.

Identifiers of scheme Participants are the key to fetch other information about the scheme Participants, and for authentication and authorisation.

API client

Following certificates must be used for identification of the API client.

Scheme	Service Type	API client	Comments
SPAA	Regular	QWAC - Qualified Web Authentication Certificate	Profile based on the European Standard ETSI EN 319 412-4 [6]; the extensions defined by ETSI TS 119 495 [7] may also be used
	Call-back	EV TLS	The asset holder can use his EV TLS server side certificate for the call back
SRTP	Regular & Call-back	QWAC - Qualified Web Authentication Certificate	Profile based on the European Standard ETSI EN 319 412-4 [6]; the extensions defined by ETSI TS 119 495 [7] may also be used
VOP	Regular	QWAC PSD2[1] - Qualified Web Authentication Certificate issued for use in the PSD2 Open Banking context	Profile based on the European Standard ETSI EN 319 412-4 [6]; the extensions defined by ETSI TS 119 495 [7] **must** be used

Remark: by construction of those qualified certificates, the following would apply:

- When a scheme Participant wants to use several, different, identifiers (e.g., BIC codes), it MUST present a certificate for each of its identifier, which may be the same certificate.
- When a scheme Participant wants to use different domains for different, or the same, services, it MUST present a certificate for each of its domains.

API server

The API server does not need a QWAC, it can use a standard website certificate. To ensure a sufficient high level of authentication, an EV TLS certificate is required.

Remarks

- It is possible that a Participant in an API server role uses the same certificate as API client for call-backs. In this case the field extendedKeyUsage in the certificate SHALL contain both attributes clientAuth and serverAuth.
- The scheme Participants should be able to receive, and act upon, the broadcasted emergency messages issued by the OSM.

[1] A QWAC PSD2 certificate already owned by a Participant may be reused

5. Scheme Participants Information requirement

Purpose: additional information that is required from a scheme Participant to establish a secure connection.

- Scheme Participant Roles

  Role's definition depends on the scheme. When a unique type of role (e.g. SRTP Participant) exists, this section is void and does not specify any requirement because being identified and authenticated means that the Participant has the single role defined in the scheme. When several roles are defined in the scheme, being authorised to a type of role can limit the set of APIs available at an endpoint.

- When a scheme Participant intends to serve Payers, then:
  - Finding the API's endpoint (the URL) of an identified scheme Participant is **necessary** to be able to call the said API.
  - Finding the API documentation (at least URL) is **necessary**. In the case this is the default API proposed by the scheme, this indication is sufficient. When this is an API proposed by an API Initiative, the link to the specification is sufficient.
- The commercial name ("human readable") of a scheme Participant might be **useful** if that name is to be presented to the Payers or the Payees.

6. Scheme Participants Authentication requirements

Purpose: proof the identity for a scheme Participant.

When calling another scheme Participant's API's endpoint, the Participants MUST perform mutual authentication. This authentication serves to prove the identity of the Participants: see chapter 4.

The mutual authentication is done by applying TLS (including client authentication) and referred to as '**TLS with Client Authentication**'.

The TLS version, key length and algorithms MUST comply with the standard recommended by the EPC – PSSG [9] that is currently applicable and as mentioned in the respective Risk Management Annex of each scheme for the securing of data transport.

7. Secured communication between Scheme Participants requirements

Purpose: avoid eavesdropping and tampering of communication.

The TLS layer discussed at the Authentication chapter (chapter 6) covers this requirement.

8. Authorisation requirements

8.1. Client authorisation principles

Authorisation is the process by which an API server will decide to allow or deny an API client request. In case of denial, the API server will answer with an HTTP 403 (Forbidden) response.

The URI requested by an API client may be subject to different access modalities for scheme Participants:

1. All schemes apply a closed access model to the API with authentication
   - A prerequisite registration of the API client with the scheme is mandatory and subject to some conditions.
   - The registration conditions of an API client may include:
     - A participation to a scheme (e.g.: SRTP, VOP, SPAA).
     - Registration in a directory (e.g.: EDS for VOP).
     - For SPAA, following additional conditions for the registration of the API client apply:
       - A contractual relationship between both legal entities, on API client and API server sides (currently only applicable to the SPAA scheme) must exist.
       - A legal role, e.g.: PISP, AISP roles as specified by PSD2 (currently only applicable to the SPAA scheme) must be defined.
   - The API client must authenticate when accessing the server's URI.
     For SPAA, closed access with authentication and explicit authorisation applies: the API client must also get the consent from the data owner. The consent could for example result in the provision of an authorisation token to the API client, for instance using OAuth2 (RFC 6749).

8.2. Schemes closed access with client authentication

This use-case will apply:

- to all the SRTP-API interactions
- to some of the SPAA transactional assets
- to the VOP Scheme.

In these cases, the registration will be subject to the participation of the API client to the relevant EPC scheme. In the case of the SPAA Scheme, this registration must be completed by the PISP role of the API client.

8.2.1. Mandatory Basic approach

To allow or deny the access to the API client, the API server must perform the following steps:

1. Authenticate the API client based on its certificate (cf. chapter 6)
2. Extract the subsequent identity of the API client from the certificate (cf. chapter 4)
3. Check the participation of the API client to the relevant scheme (in the RoP or a directory (e.g., the EDS))
4. Check the legal role of the API client if needed (not applicable to SRTP and VOP)
5. Check the access right of the API client to the API resources that are accessed through the URI (not applicable to VOP).

The last step is critical to avoid an unauthorised access, for instance to a resource that was submitted by another API client:

- A SEPA Request-To-Pay or a Cancellation Request in case of SRTP
- A Payment Initiation Request in case of SPAA

As the whole authorisation process may be repeatedly executed by the API server for each API client request, it is also possible to optimise this process through a pre-enrolment of the API client.

8.2.2. Additional Optional optimised approach

The below is mentioned as an example for possible future development subject to bilateral agreements, but is not yet used in any scheme.

Pre-enrolment

This pre-enrolment could allow the API server to get and store some characteristics of a given API client:

- Names, logos
- Certificates or public keys
- Call-back and redirect URIs
- Requested grants and scopes
- …

These characteristics may be complemented by information extracted and regularly refreshed from external repositories

- Scheme participation and roles
- EPC directories
- Legal roles
- …

The pre-enrolment process will usually provide the API client with a client id that is linked to the usage context specified by the provided information. If needed, an API client may execute, with the same API server, several pre-enrolments for different specialised usage contexts.

An example for an enrolment protocol is proposed by the IETF in the OAuth2 context (RFC 7591 & 7592).

Client id usage

The client id may be used to get an authorisation token, for instance using OAuth2 (RFC 6749).

The API server can execute some of the authorisation steps at once before providing the authorisation token to the API client.

8.3. API server identification and authorisation

This use-case currently only applies to the VOP Scheme.

To verify the identity of the API server, the API client must perform the following steps:

1. Retrieve the URI of the API server of the Responding PSP for the VOP API from the EDS. The fact the API Server is present in the EDS, implicitly proves the adherence of this participant to the scheme.
2. Authenticate the API server based on its certificate (cf. chapter 7) through standard TLS authentication.

9. Scheme Participants sealing/signing requirements

Purpose: providing the proof that an API client has indeed submitted a given request and vice versa an API server has indeed provided a given response.

Note: This section is only relevant when the scheme has required that some messages, or part of the messages, must be protected by sealing. So far, this is only foreseen for the SRTP scheme. The corresponding message (or part of it) must then be signed.

The identity of the signee is represented by certificates for sealing (QSealC). Those certificates SHALL be based on the profile defined by the European Standard ETSI EN 319 412-4 [6]. The owner is always a legal person acting as either the API client or the API server. If needed the extensions defined by ETSI TS 119 495 [7] may also be used for these certificates.

Those certificates can be provisioned through the same list of Certification Authorities already mentioned above.

Key length and algorithms MUST comply with the EPC – PSSG recommendation [9] for sealing.

The exact protocol to transport the seal along with the message not being an undisputed European or international standard, it is up to the API used to specify that protocol in the API documentation.

10. Availability requirements

Availability of the infrastructures (including protection against DDOS), liabilities, emergency plans and minimal standardisation of the solutions in accordance with the respective scheme rulebooks.

The system MUST ensure high availability of services in accordance with the adopted classification of criticality, in particular through redundancy of components, backing up data and software as well as automatic maintenance of system continuity.

11. Security conformance and testing

The Scheme may require scheme Participants to prove that security requirements among other requirements have been met during the homologation process and to confirm that it is maintained on a regular basis to the OSM. In this case Scheme Participants should provide a testing environment, test data or any other evidence requested as part of the homologation process.

12. Audit trail requirements

These requirements are applicable to all scheme Participants, both on the server and client sides.

As a basic audit requirement, the audit log must be always enabled, and must include all the information that is legally required.

In additional, it is strongly recommended that entries (logEntry) include the following objects/fields:

- logName: The resource name of the log
- timestamp: The time the event described by the log entry occurred
- serviceName: the name of the service used/invoked
- uniqueID: A unique identifier for the log entry
- httpRequest: Information about the HTTP request associated with this log entry.
    - URL
    - Headers
    - Payload if any
- httpResponse: Information about the HTTP response associated with this log entry
    - HTTP return code
    - Headers
    - Payload if any

Audit trails must be protected from data manipulation to ensure integrity.
It is recommended to keep the audit trail information at least for six months or according to the applicable legal requirements.

13. Operational Scheme Manager (OSM) related requirements

The EDS will be the practical tool of the OSM. The EDS will collect, validate, maintain and when applicable, make available additional data related to the scheme Participants to ensure an effective functioning of the schemes. Please refer to the EDS User Guide [5].

These data will be included in the EDS, only accessible to scheme Participants in a secured way (in a push or pull mode). Only the modified data must be updated in the publication.

It is the responsibility of the Participants to download a current version of the EDS as a local copy, as detailed in the EDS User Guide [5].

Annex 1: SPAA scheme specificities

User Identification and Authentication – SPAA Scheme

In the SPAA scheme, the user would be the Asset Owner (AO) or somebody rightfully acting on his behalf. The user identification is a key-feature that must be properly completed before going further with authentication and any business processes (transactional or data assets).

The purpose of identification is to make sure that the user is the relevant one and that no-one else will be annoyed by any notification or request.

This purpose might go beyond the strict identification of the user by also specifying a usage context. Some Asset Holders may know a same user with different profiles (private access, delegated access, business access etc.), according to scenarios listed below:

- Private access on his/her own account
  - E.g., the user wants to access his own banking account
- Delegated private access
  - E.g., the user wants to access his mother's banking account
- Company access on his/her own account
  - E.g., the user wants to access to his professional banking account
- Delegated company access
  - E.g., the user wants to access the banking account of their employer

So, SPAA functionality has to allow to manage the above cases where necessary in order to distinguish different usage context and simplify the Identification process of the customer between Asset Broker and Asset Holder.

Thus, the recognition process must provide an unambiguous result for a single couple of Asset Broker and Asset Holder, i.e., the identification key, upon which each actor of the value chain can rely.

In the context of an API, this identification key must be sharable between the API client (i.e., the Asset Broker) and the API server (i.e., the Asset Holder).

On one hand, this identification key shall reasonably be as stable as possible within time although identification process may evolve and change their identification keys and mechanisms. On the other hand, the identification key is not meant to provide any additional information (e.g., personal address, phone number, email address…) by itself.

However, according also to GDPR rules adopted by each Participant's country, it is still possible to use some of these pieces of data as identification key. Moreover, the identification key can also be used to retrieve additional information when possible. The possible identification keys will be defined in the different API specifications according to what is mandated by PSD2.

Annex 2: SRTP scheme specificities

Referenced Technical Solution Provider's attribution

'Referenced Technical Solution Provider' is a label given by the Homologation Body in the SRTP scheme.

Purpose: a scheme Participant's proxy acts as a gateway to expose or consume other scheme Participant's APIs.

A proxy can either be technically transparent, or visible (at the level of mutualised certificates). It is not an actor as it is always legally transparent because the liabilities and obligations stay at the level of each scheme Participant.

For auditability purpose, the proxy MUST be given an identity by the OSM. The OSM MUST manage these entities as having an infrastructure's role: proxy. Other constraints might apply to the proxy depending on the scheme (such as a special kind of homologation).

A scheme Participant can also act as an infrastructure proxy.

The proxy MUST provision its own QWAC authenticating itself toward callers and callees of APIs.

The proxy only acts as a gateway in the communication, but does not have, in its proxy role, any final customers (e.g., Payers or Payees).

When the use of proxies is made possible by the scheme, the Identification of the scheme Participant MUST be provided at the scheme level in the message (e.g., attributes AT-N001 and AT-E005 for the SRTP scheme).

Although this indication in the message is redundant when a direct route API is used, it is RECOMMENDED to always populate this information even when the scheme makes it optional.

When a scheme Participant wants to use a proxy as its entry or exit point, this route MUST be declared and managed by the OSM.

Scheme Participants making use of visible proxies (at certificate level) MUST indicate to the OSM that their messages are signed by the proxy instead of themselves. In such case, the proxy must also provision a QSealC as explained in the "non-repudiation" section (chapter 11).

The communication and non-repudiation mechanism between the proxy and the scheme Participants it represents must comply with the same security requirements, however implementations are left to private/commercial relationship between the proxy and the scheme Participants.

Annex 3: VOP scheme specificities

Clarifications concerning the use of QWAC PSD2 certificates on client side

The specifications of the QWAC PSD2 certificate are defined in the ETSI Technical Standard (TS) 119 495 1.7.1 here.

This document specifies (section 5.3, Note 3) that a QWAC PSD2 can be issued to support both server and client-side authentication; this is indicated in the certificate's Extended Key Usage (EKU): extKeyUsage including id-kp-serverAuth and id-kp-clientAuth.

Therefore, any QWAC PSD2 certificate to be used by a PSP to for client authentication in VOP must include the Client Authentication EKU.

Google's update to its Root Program Policy mandates that by June 15, 2026, public TLS server certificates can no longer include the Client Authentication EKU. As a consequence, large international CA (Globalsign, Digicert, SSL.com) have recently announced they will gradually stop issuing public TLS certificates with the client authentication option, including QWAC certificates.

It is worthwhile to note that the ETSI TS builds on the guidelines and requirements defined by the Certification Authority Browser Forum (CA/B Forum). The CA Browser Forum Baseline Requirements still allow the Client Authentication EKU.

VOP APIs don't require browser support and the QWAC PSD2 certificates are in general not intended to be used by browsers. Changing the principles of these certificates would not only impact VOP, but also existing PSD2 services.

In conclusion: the authentication principles defined for the VOP API remain applicable and when requesting a QWAC PSD2, PSPs will need to ensure their QTSP still supports issuing QWAC PSD2 certificates that include the value id-kp-clientAuth, in the EKU extension.

An overview of QTSP can be found on the EIDAS Dashboard.

The EPC does not intend to define its own specifications to validate client certificates but for the authentication of the VOP Requester (API-client) using QWAC PSD2 certificates, encourages the usage of the authentication principles put in place for Open Banking under PSD2.

The EPC recommends to integrate the full list of qualified root Certification Authorities (CAs) and their intermediate CAs in the trust list of the VOP API-Server, as the VOP API Servers need to accept valid QWAC PSD2 certificates from any valid QTSP (Qualified Trust Service Provider).

The API-client is not expected to provide the entire certificate trust chain (i.e. including intermediate certificates) when they present the QWAC PSD2 certificate during the TLS handshake to the API-server - this is the recommended approach.

The API-server needs to consider the intermediate CA that issued the QWAC certificate that is in the trusted list as a "trust anchor" (which therefore does not need to be validated further). If the CA that issued the QWAC is not in the API-server's trusted list, the validation will follow the certificate chain until it finds the intermediate CA that is in the trusted list. The QWAC certificate must include by default the AIA extension which enables this.

Resources:

- The EIDAS dashboard provides access to the lists of QTSP and other documentation: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

- The EIDAS API documentation can be found here: https://eidas.ec.europa.eu/efda/swagger-ui/index.html
- https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/tl-info: trusted list summary including all country trusted lists and a meta-list pointing to the various lists (ec.europa.eu/tools/lotl/eu-lotl.xml)

Clarifications concerning the use of EV-TLS certificates on server side

As above-mentioned in this document, an EV-TLS certificate for authentication on the API server-side (Responding PSP or its RVM) is required.

To verify an EV-TLS certificate, the API-client (Requesting PSP or its RVM) requires the root certificate of the corresponding Certification Authority (CA) that issued the EV certificate to be included in its trust store, since there is no onboarding between the VOP Requesting PSP (or RVM) and VOP Responding PSP (or RVM) .

Note:

1. The ASF does not specify which CAs can issue EV TLS certificates for VOP.
2. No single public source is available listing the root certificates of CAs issuing EV-TLS certificate.

The EPC recommends:

1. API-servers (VOP Responding PSPs and RVMs) obtain their EV-TLS certificate from a “commonly known CA” in the European financial industry.
2. API-clients (VOP Requesting PSPs and RVMs) integrate in their trust store the commonly used CAs that are used to obtain EV-TLS certificates.
3. API-servers provide the trust chain (i.e. including intermediate certificates) to the API-client when they present the EV certificate during the TLS handshake (an existing general practice).
4. When a VOP Responding Server deploys a certificate of a new CA, it is recommended to inform other RVMs and PSPs which have to take this new CA not account. To this end, the EPC provides a contact list.

A non-exhaustive list of the CA used in VOP, based on the URI included in EDS is available, for indicative purposes only, on the EPC website.

For information, here is the link to the Common CA Database (CCADB); a common repository of public root CAs. It provides the lists of trusted root certificates for the major browser’s root stores (e.g. Mozilla’s Root Store). It is worth noting that these lists include all commonly used root and intermediate CAs for EV TLS certificates that are being used in the context of VOP, at the time of this publication.

Authentication in case of RVM

This following chapter describes the Authentication model for VOP in more detail.

The RVM acts as a gateway to expose or consume API’s on behalf of the Scheme Participants it represents. For information: a scheme Participant can also act as an infrastructure RVM for other Participants.

RVMs are not considered as Participants in the scheme; it is always legally transparent because the liabilities and obligations stay at the level of each scheme Participant.

The use of an RVM may not be technically transparent for the other scheme Participants even if the liabilities remain on the scheme Participants.

Please refer to the EDS User Guide [5].

Requesting site verification

- The VOP Request will contain the BIC of the Requesting PSP, regardless if the VOP request was sent by the Requesting PSP itself, or via an RVM.
- The API Client authenticates via a QWAC PSD2 certificate.
- The API Server (Responding PSP) will verify in the EDS if the combination of the BIC of the Requesting PSP and the Authorisation Number retrieved from the QWAC PSD2 certificate, are present; this is regardless of the actual sender of the message (Requesting PSP or RVM acting on its behalf). This way it is transparent for the Responding PSP if the requesting API gateway is operated by a RVM or directly by the Requesting PSP.

Responding site verification:

- The Requesting PSP derives the BIC of the Responding PSP (Account holding PSP BIC) based on the IBAN to validate and it retrieves the URI of the VOP API for this BIC from the EDS.
- For information: the fact the BIC is available in the EDS, implicitly confirms the adherence of the Responding PSP to the VOP scheme.
- It is transparent for the Requesting PSP if the responding API gateway is operated by a RVM or the Responding PSP itself.
- The Requesting PSP authenticates the Responding server by validating if the certificate is a valid EV certificate. A RVM can use an EV certificate of the Responding PSP or can use its own certificate for authentication on behalf of the Participants it represents.
- The standard TLS authentication by the Requesting PSP verifies the server certificate.

Possible use cases and examples

This paragraph lists the different set-up combinations of PSP and RVM that can occur in the EDS; each case is illustrated with an example of 2 fictive PSP:

As Responding PSP

- **Case 1: directly connected PSP**
  - Each PSP operates its own responding API gateway, exposing its EV certificate

Key in EDS (BIC11)	Responding URI in EDS[2]
ABCDLLCC123	'https://api.ABCD.com'
EFGHLLCC123	'https://api.EFGH.com'

- **Case 2: PSP connected through an RVM using distinct URIs**
  - The RVM applies a unique URI per PSP, exposing its EV certificate

[2] We only mention the URI scheme ('https') and URI host; to obtain the full URI, the API resource path will be added but as this is a fixed text ('vop/v1/payee-verifications'), it is not mentioned in the table. Example of a full API URI: 'https://api.EFGH.com/vop/v1/payee-verifications'.

Key in EDS (BIC11)	Responding URI in EDS
IJKLLLCC123	'https://api.rvm.com/IJKLLLCC123'
MNOPLLCC123	'https://api.rvm.com/MNOPLLCC123'

- **Case 3: PSP connected through an RVM using a common URI**
  - The RVM applies a common URI for all PSP, exposing its EV certificate

Key in EDS (BIC11)	Responding URI in EDS
QRSTLLCC123	'https://api.rvm.com'
UVWXLLCC123	'https://api.rvm.com'

As Requesting PSP

- **Case 1: directly connected PSP**
  - Each PSP operates its own responding API gateway, exposing its QWAC PSD2 certificate

Key in EDS (BIC11)	Identifier in client certificate
ABCDLLCC123	ID-ABCD-12345
EFGHLLCC123	ID-EFGH-67890

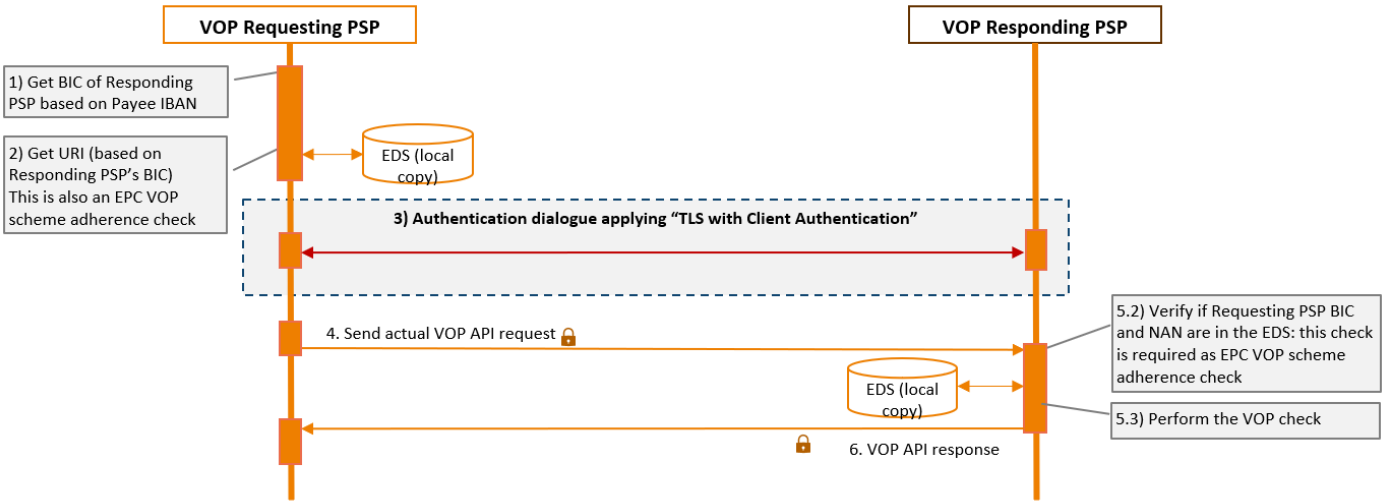
- **Case 2: PSP connected through an RVM using PSP QWAC PSD2**
  - Each PSP uses its own QWAC PSD2 certificate through the RVM

Key in EDS (BIC11)	Identifier in client certificate
IJKLLLCC123	ID-IJKL-12345
MNOPLLCC123	ID-MNOP-67890

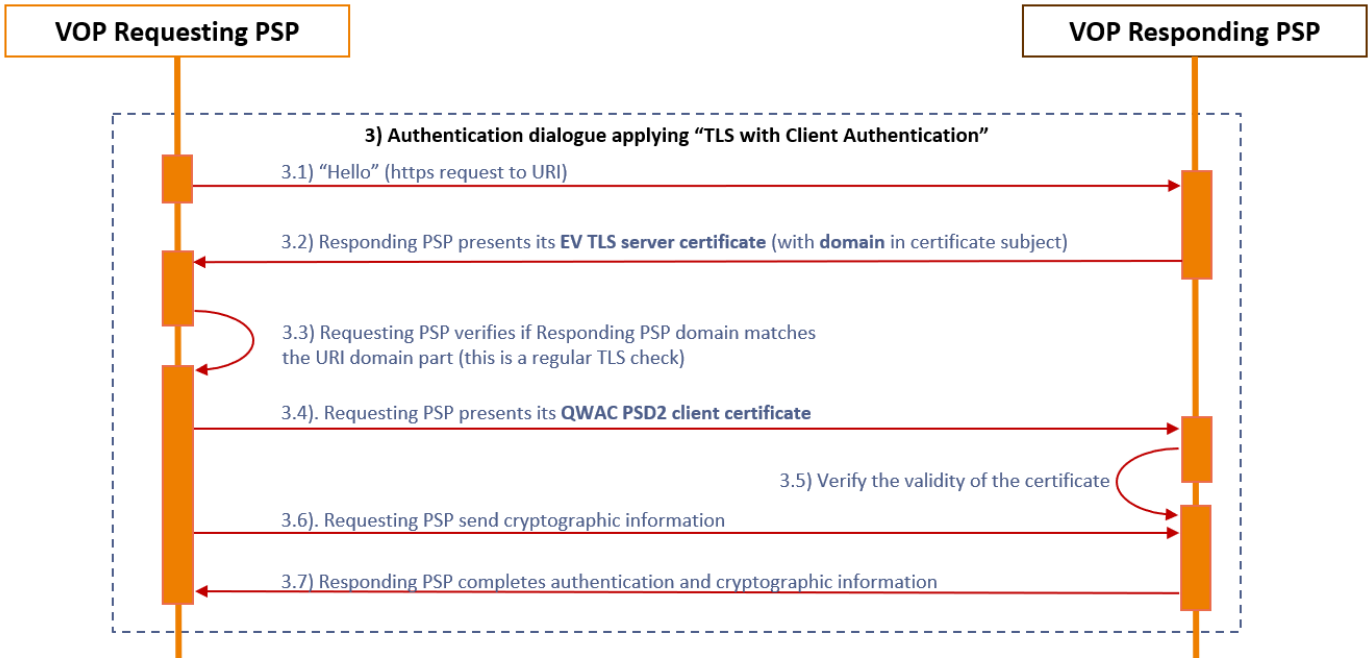
Authentication dialogue sequence diagrams

The authentication according the **TLS with Client Authentication** model is illustrated for information by the following sequence diagram:

- **Overall VOP Request workflow**



- **VOP "TLS with Client Authentication" process**


VOP Requesting PSP
VOP Responding PSP
3) Authentication dialogue applying "TLS with Client Authentication"
3.1) "Hello" (https request to URI)
3.2) Responding PSP presents its EV TLS server certificate (with domain in certificate subject)
3.3) Requesting PSP verifies if Responding PSP domain matches the URI domain part (this is a regular TLS check)
3.4). Requesting PSP presents its QWAC PSD2 client certificate
3.5) Verify the validity of the certificate
3.6). Requesting PSP send cryptographic information
3.7) Responding PSP completes authentication and cryptographic information