European Payments Council

Verification Of Payee
Inter-PSP API Specifications

EPC103-24 / 2024 Version 1.0.1 / Date issued: 15 November 2024 / Date effective: 05 October 2025

Public

SEPA Single Euro Payments Area

Verification Of Payee API Specifications

European Payments Council

EPC103-24
2024 Version 1.0.1
Date issued: 15 November 2024
Date effective: 05 October 2025

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

Table of Contents

0 Document Information

0.1 Reference

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

	Document Number	Title	Issued by:
[1]	EPC218-23	Verification Of Payee Scheme Rulebook	EPC
[2]	ISO 13616	Financial services - International bank account number (IBAN) -- Part 1: Structure of the IBAN	ISO
[3]	To be defined	Guide to the VOP Scheme Adherence Process	EPC
[4]	EPC409-09	EPC list of countries and territories included in the SEPA Schemes' geographical scope	EPC
[5]	SEPA Regulation	Regulation (EU) 260/2012 establishing technical and business requirements for credit transfers and direct debits in euro, as amended by Regulation (EU) 2024/886 (Instant Payments Regulation (IPR))	EU
[6]	EPC288-23	EPC Recommendations for the Matching Processes under the VOP Scheme Rulebook	EPC
[7]	Directive (EU) 2015/2366	Payment Services Directive (PSD2)	EC
[8]	EPC164-22	API Security Framework	EPC
[9]	Funds Transfer Regulation	Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds (FTR)	EU
[10]	To be defined	References to EDS specifications or requirements	EPC
[11]	EPC217-08	SEPA REQUIREMENTS FOR AN EXTENDED CHARACTER SET (UNICODE SUBSET) BEST PRACTICES	EPC

0.2 Change History

Issue number	Dated	Reason for revision
1.0	31/10/2024	First Version – approved by Verification Of Payee Task Force
1.0.1	15/11/2024	Amendments as per Errata List (see Annexe A)

0.3 Purpose of Document

The EPC Verification Of Payee (VOP) Scheme ("Scheme") is a set of rules, practices and standards to achieve interoperability for the provision and operation of verifying Payment Account Numbers and Names of the Payment Counterparties, between Participants of the Scheme prior to initiating an Account-based Payment within SEPA. A Participant is any Payment Service Provider (PSP) as defined in [7] and [5] that is eligible to participate in the Scheme in accordance with Rulebook.

The objectives of these API Specifications are :

- To define the rules to be applied: establish standards and rules for using and integrating the API, including data formats, calling conventions and response codes.
- To define the authentication and authorisation mechanisms (OAuth, JWT, API keys) to protect the data exchanged via the API.

0.4 About the EPC

The purpose of the EPC, as one representative of the European Payment Service Providers' (PSP) sector, is to support and promote European payments integration and development, notably the Single Euro Payments Area ("SEPA").

The mission of the EPC is to contribute to safe, reliable, efficient, economically balanced and sustainable, convenient payments supporting an integrated European economy, its end-users' needs as well as its competitiveness and innovation goals:

- Through the development and management of pan-European payment and payment-related schemes and the formulation of positions and proposals on European payment issues;
- In constant dialogue with other stakeholders and regulators at European level; and
- Taking a strategic and holistic perspective.

The EPC offers one focal point and voice for the PSP sector on all European payment and payment-related issues, driven by a single vision.

The EPC shall, among other things, be responsible for the performance of functions relating to Scheme Management, as set out in the relevant governance documents, including amongst others the VOP scheme Rulebook. The EPC is the owner and manager of various payment and payment-related Schemes.

1 Introduction

This document describes the Application Programming Interface (API) specifications for the Verification Of Payee (VOP) scheme.

It defines the rules for implementing VOP requests and corresponding response messages in the inter-PSP space. These specifications facilitate an API technology that uses ISO 20022 resource elements. This document describes the technology used and the prerequisites needed to send requests and receive responses.

Chapter 2 gives an overview of how the API works by drawing the flow in a sequence diagram and presenting the main use cases. A section introduces the trust model (authentication and authorisation model) for the VOP API.

Chapter 3 defines the character sets and data type supported by all services and notations used within all services definitions.

Chapter 4 goes into more depth by presenting the technical specifications and the data model to be used. In this chapter, we provide examples of API messages for the most common use cases, as described in the Verification Of Payee scheme Rulebook [1].

These API specifications constitute a binding supplement to the Rulebook [1].

2 API Overview

2.1 Sequence Diagram

In the Inter-PSP Space, a VOP Request from the Requesting PSP concerns a single Request combining the Payment Account Number (IBAN) and the Name of the Payment Counterparty only or potentially includes a data element, other than the Name of Payment Counterparty, which unambiguously identifies the Payment Counterparty (identification code) as well. If the Requester submits several Payment Account Numbers to be verified, the Requesting PSP must then send several VOP Requests in the Inter-PSP Space for each Payment Account Number concerned [5].

In this sequence diagram, the workflow for the Verification Of Payee is described.

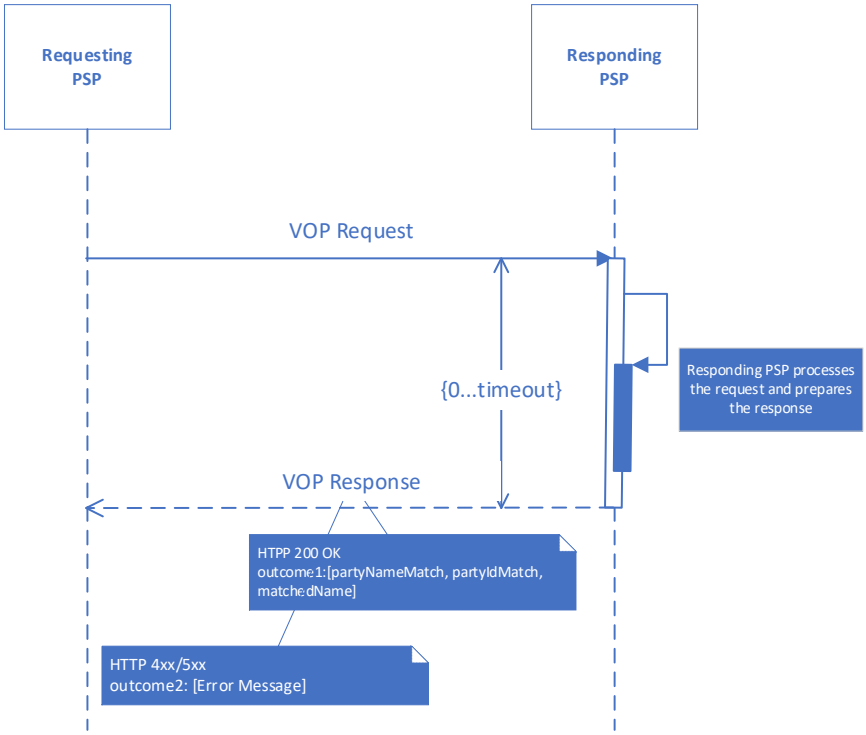

Figure 1 : Verification of Payee Sequence Diagram

The Requesting PSP prepares the request and submits it to the Responding PSP. After validation of the request, the Responding PSP prepares the response which is returned to the Requesting PSP. The response must be given within a Maximum Execution Time. The "Maximum Execution Time" rule is described in the chapter 3.3.2 of the Verification Of Payee Scheme Rulebook [1].

2.2 VOP Scheme high-level flow

The overall Verification Of Payee (VOP) API diagram, including the main interactions, endpoints and data flows (i.e. the EPC Directory Service (EDS) interactions), will be further described in the EDS requirements [10]. This document comes in complement to the VOP Scheme Rulebook [1], VOP API Specifications, API Security Framework [8] and provides a complete overview of the architecture, and the end-to-end view.

2.3 Use Cases (positive flows)

Three major use cases as positive flows are identified and supported. They correspond to the different combinations supported by the VOP scheme (see chapter 3.2 of the VOP Scheme Rulebook [1]).

2.3.1 Name/IBAN check

- **Prerequisite**: Beneficiary = natural person or legal person
- VOP Request: Name/IBAN check
- VOP Response:
    1. Match (MTCH), No Match (NMTC), Close Match (CMTC) with name indication, Not Applicable (NOAP)
    2. Error Message HTTP 4xx/5xx

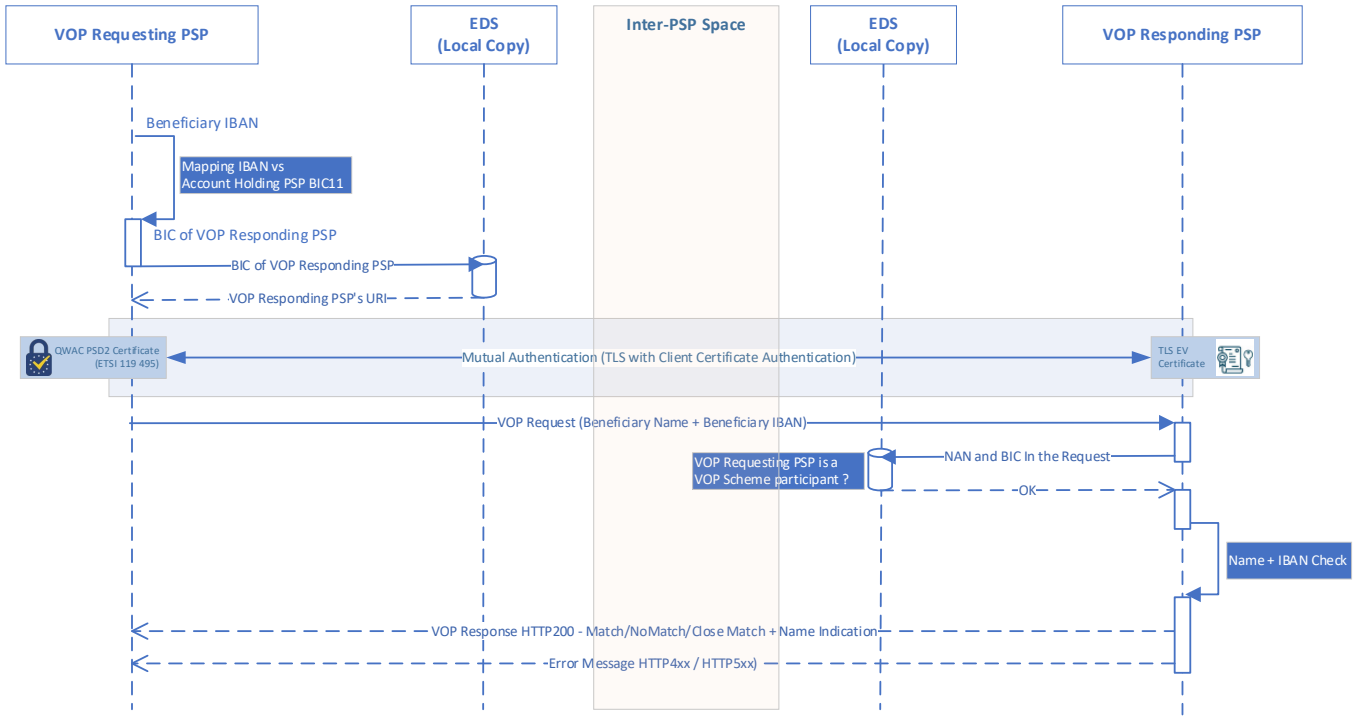

Figure 2 : Name / IBAN Check Process

2.3.2 Identification code (LEI or VAT number...)/IBAN check

- **Prerequisite**: Beneficiary = legal person
- VOP Request: Identification code/IBAN check
- VOP Response:
    1. Match (MTCH), No Match (NMTC), Not Applicable (NOAP)
    2. Error Message HTTP 4xx/5xx

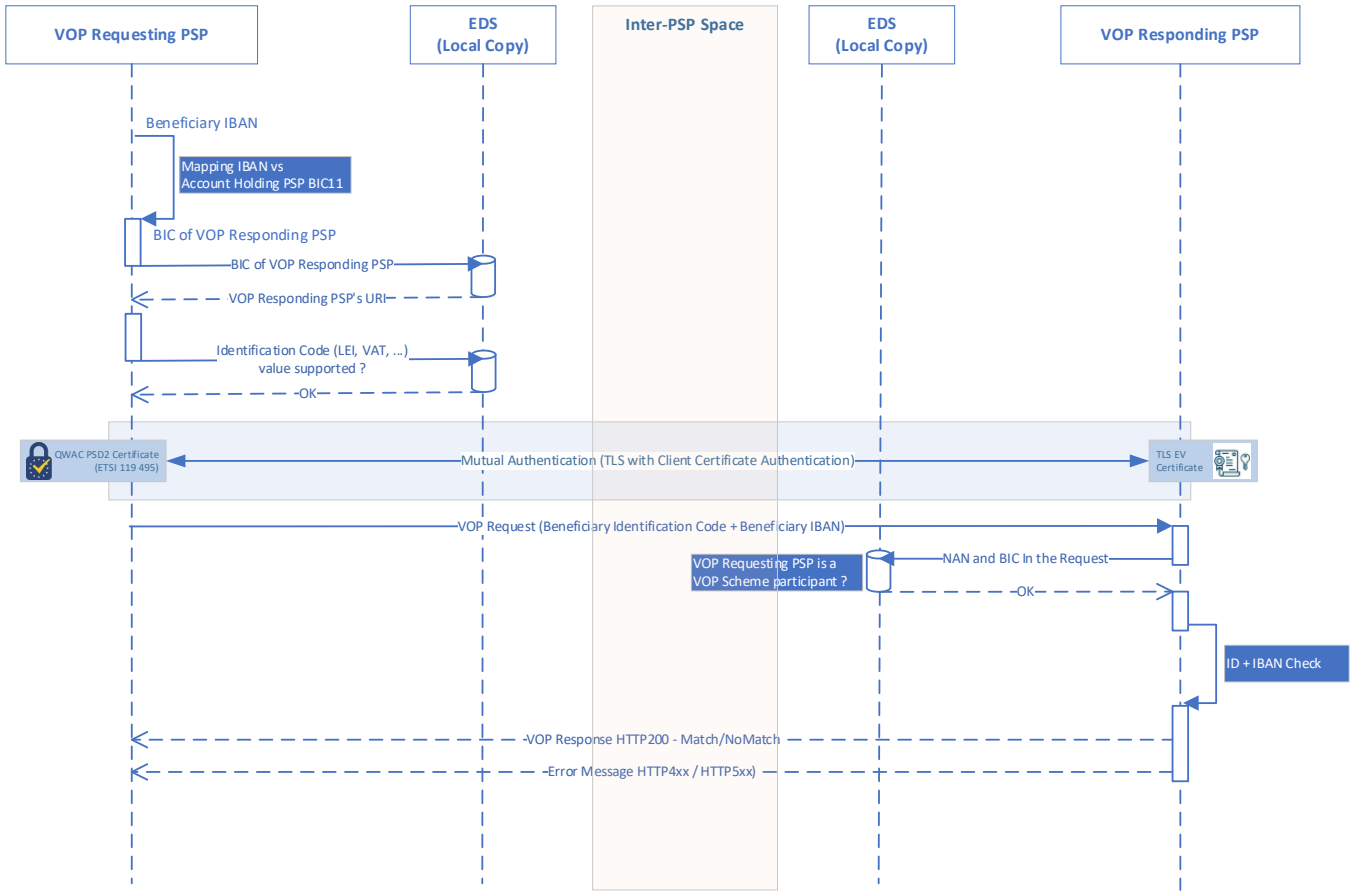

Figure 3 : Identification Code / IBAN Check Process

2.3.3 Name (or Identification code) + additional attribute (C007)/IBAN check

- **Prerequisite**: Beneficiary = natural or legal person
  AND additional information needed to identify the payment counterparty for example: Beneficiary PSP = e-money institution or payment institution
- VOP Request: Name/IBAN check or Identification code/IBAN check
- VOP Response:
  1. In case of Name+IBAN : Match (MTCH), No Match (NMTC), Close Match (CMTC) with name indication, Not Applicable (NOAP)
     In case of IBAN+Identification code : Match (MTCH), No Match (NMTC), Not Applicable (NOAP)
  2. Error Message HTTP 4xx/5xx

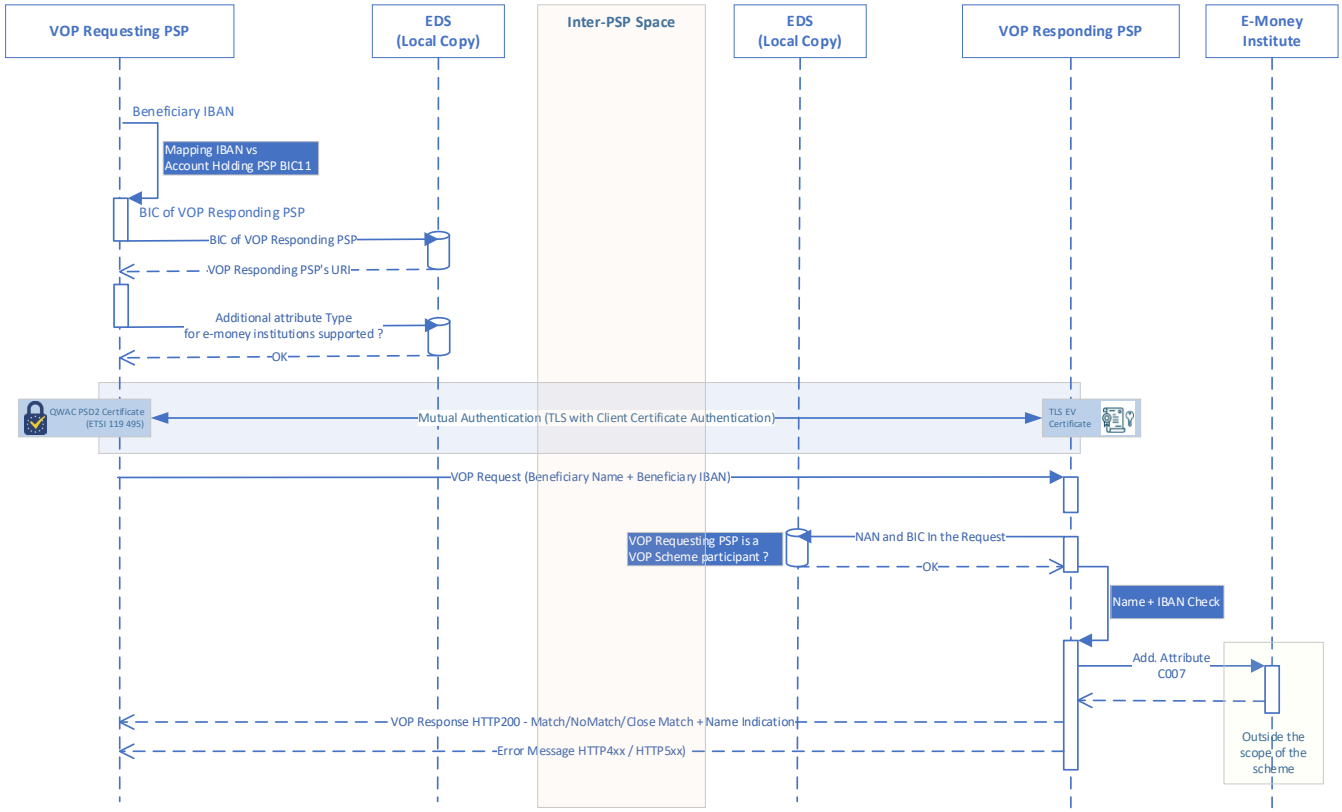

Figure 4 : Name / IBAN + Additional Attribute Check Process

2.4 API Authentication and authorisation

This section provides a description of the trust model (authentication and authorisation model) for the VOP API. The model and its specifications are integrated and described in detail within the overall API Security Framework issued by the EPC (see [8]).

The following diagram illustrates the security dialogue:

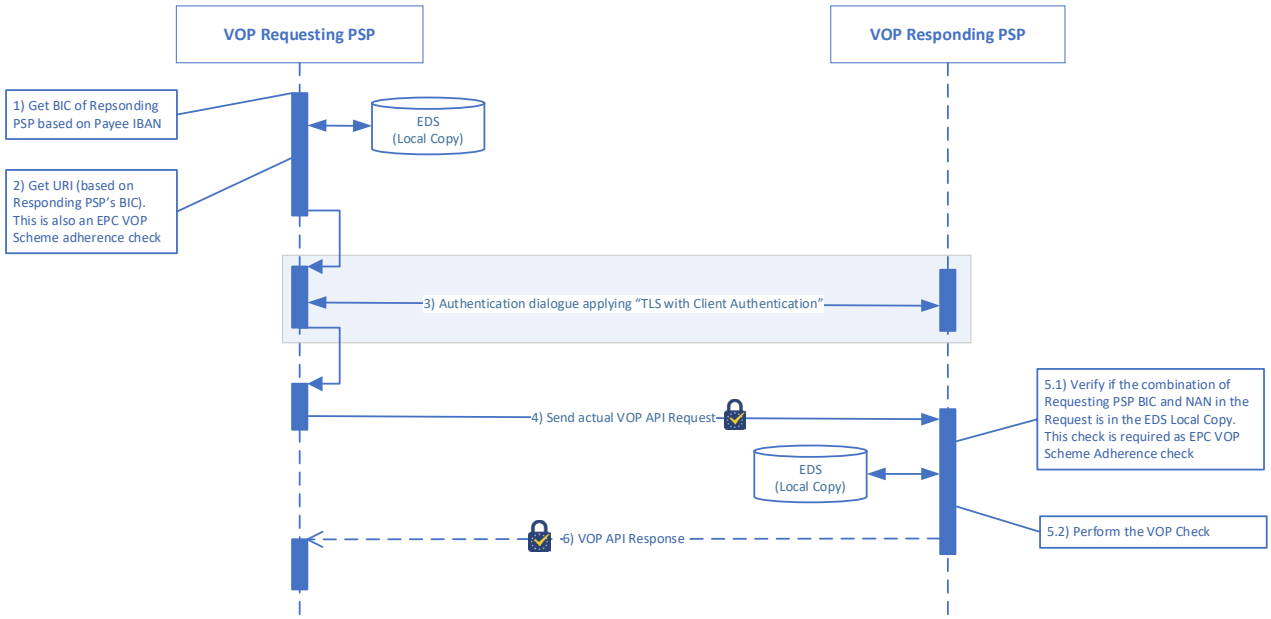

Figure 5 : Security Dialogue Diagram

2.4.1 Authentication

The Requesting PSP retrieves the Responding PSP's API end point ('URI') for the VOP Request from the local copy of the EDS. This implicitly confirms to the Requesting PSP that the Responding PSP adheres to the VOP scheme.

When the Requesting PSP, or an RVM acting on its behalf, calls the Responding PSP API endpoint, both participants MUST perform an authentication of the other participant to prove each other's identity. This mutual authentication is done by applying TLS (including client authentication) and referred to as '**TLS with Client Authentication**' in [8].

TLS with Client Authentication is done through exchanging certificates issued by trusted parties. The following types of certificates are required in the context of authentication and authorisation of a VOP API Request:

'QWAC PSD2' or 'PSD2 QWAC'	A 'Qualified Web Authentication Certificate' (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.

	A 'QWAC PSD2' is a Qualified Web Authentication Certificate issued for use in the PSD2 Open Banking context. A "PSD2 QWAC" is defined as follows: - 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 PSP 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
'TLS EV' or 'EV TLS'	'Extended Validation' (EV) TLS/SSL Certificate An EV Certificate ensures the certificate holder has undergone an extensive level of vetting and identity checks to certify that the website is authentic and legitimate

2.4.2 Authorisation

Authorisation is the process by which an API server (= Responding PSP for VOP) will decide to allow or deny an incoming request. This authorization is implicitly granted to any authenticated client.

To authorise a VOP request, the Responding PSP **must** verify in the EDS if the Requesting PSP is adhering to the VOP EPC scheme. This is done by applying the following steps:

1. Once the Requesting PSP is authenticated, the Responding PSP can extract a National Authorization Number (NAN) from the QWAC PSD2 used in the request.
2. The Responding PSP will verify if the combination of the BIC (as received in the payload of the VOP request) and the NAN received via the QWAC PSD2 certificate of the Requesting PSP is present in the EDS.

This verification is mandatory; it's the responsibility of the PSP (or its proxy) to implement it at application level (EPC will not specify the technicalities).

3 Character Sets and Notations

3.1 Character Set and Data Types

The character set within the API Framework for parameters transported in HTTP bodies is UTF-8 encoded. This specification is only using the basic data elements "String", "Boolean", "ISODateTime", "ISODate", "UUID", “BIC”, “LEI” and "Integer" (with a byte length of 32 bits) and ISO based code lists. For codes defined by ISO, a reference to the corresponding ISO standard provided in the related section of this document.

Max35Text, Max70Text, Max140Text, Max256Text, Max500Text are defining strings with a maximum length of 35, 70, 140, 256, 500 characters respectively.

PSPs will accept for strings at least the following character set:

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
/ - ? : ( ) . , ' +
Space

Within the SEPA schemes, unless otherwise agreed, only a limited set of Latin characters may be exchanged. This restriction has been agreed in order to overcome the complexity that would result if all European language based characters were to be exchanged between all adhering banks. However banks by prior agreement may exchange additional characters such as through bilateral/multilateral agreements or via an agreed AOS (Additional Optional Service). See the “SEPA Requirements for an extended Character Set BEST PRACTICES” document for more details [11].

Complex data types and code lists are defined in section 4.2 of this document.

3.2 Notations

3.2.1 Notation for Requests

For API request calls, query parameters, HTTP header parameters and body content parameters are specified within this API Framework as follows:

Attribute	Type	Condition	Description
attribute tag	type of attribute	condition	description of the semantic of the attribute and further conditions.

The "Type" is referring to either basic or complex data types as introduced in Section 3.1. The following conditions may be used when describing data to be submitted by the client:

- Optional: The attribute is supported by the server, usage is optional for the client. The server may ignore the parameter if mentioned in the “Description” column of the table above.
- Conditional: The attribute is supported by the server and might be mandated by certain rules as defined in the “Description” column of the table above.
- Mandatory: The attribute is supported by the server and shall be used by the client.

3.2.2 Notation for Responses

For API call responses, parameters, HTTP header parameters and body content parameters are specified within the API Framework as follows:

Attribute	Type	Condition	Description
attribute tag	type of attribute	condition	description of the semantic of the attribute and further conditions.

The "Type" is referring to either basic or complex data types as introduced in Section 3.1. The following conditions can be set on data to be provided by the server:

- Optional: The attribute is supported optionally by the server
- Conditional: The attribute is supported by the server under certain conditions as indicated in the “Description” column of the table above.
- Mandatory: The attribute is always supported by the server.

3.2.3 Notations used for Requests as well as Responses

The following additional conditions apply to both, requests from the client to the server as well as responses from the server to the client:

Attribute	Type	Condition	Description
		{Or	
		Or	
		Or}	
		{Or – Optional	
		Or – Optional	
		Or – Optional}	

- {Or: The **first** element in a sequence of elements of which **exactly one** has to be included.
- Or: An element in a sequence of elements of which **exactly one** has to be included. The element is **neither the first nor the last** within this sequence.
- Or}: The **last** element in a sequence of elements of which **exactly one** has to be included.
- {Or – Optional: The **first** element in a sequence of elements of which **at most one** may be included.
- Or – Optional: An element in a sequence of elements of which **at most one** may be included. The element is **neither the first nor the last** within this sequence.
- Or – Optional}: The **last** element in a sequence of elements of which **at most one** may be included.

Note: Specifications for the API are accompanied by an interface description (as a YAML file). Within these API descriptions, elements with conditions "{Or", "Or", "Or}", "{Or – Optional", "Or – Optional", "Or – Optional}" will be treated as (pure) optional elements at the moment. It is the responsibility of the implementer to ensure the additional checks.

4 VOP API Definition

4.1 VOP API Technical Specifications

This chapter contains information about the header, request body and response body required to execute a successful request with the Verification Of Payee API.

4.1.1 API Access Methods

Endpoint	Method	Condition	Description
/vop/v1/payee-verifications	POST	Mandatory	Submit a Verification Of Payee Request

The approach taken was to develop the Verification of Payee API specifications based on ISO standards applied in a RESTful JSON format.

4.1.2 Request Parameters

4.1.2.1 Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	The Requesting PSP's reference number of the VOP Request
X-Request-Timestamp	ISODateTime	Mandatory	Time Stamp of the VOP Request. [AT-T056]

Note : The X-Request-Timestamp header must contain a valid ISO 8601 timestamp string, expressed in either UTC time format (YYYY-MM-DDThh:mm:ss.sssZ) or local time with UTC offset format (YYYY-MM-DDThh:mm:ss.sss+/-hh:mm), milliseconds included, as defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" (https://www.w3.org/TR/xmlschema-2/) which is aligned with ISO 8601.

4.1.2.2 Request Body

Element	Type	Condition	Description
party	Party Type	Mandatory	Provide information about the identification of the Payee
partyAccount	Account Type	Mandatory	Provide information about the Account of the Payee
partyAgent	Agent Type	Mandatory	Identification of the Responding PSP Referring to Rulebook [1] - Responding Agent [AT-C002]
unstructuredRemittanceInformation	Array of Max140	Optional	Additional information about AT-C001 sent by the Requester

Element	Type	Condition	Description
			[AT-C007] Usage Rule : only one entry may be used
requestingAgent	Agent Type	Mandatory	Identification of the Requesting PSP Referring to Rulebook [1] - Requesting Agent [AT-D002]

4.1.3 Response Parameters:

4.1.3.1 Response Code

The HTTP response code equals 200 in case of successful API process.

4.1.3.2 Header

Element	Type	Condition	Description
X-Request-ID	UUID	Mandatory	The Requesting PSP's reference number of the VOP Request
X-Response-Timestamp	ISODateTime	Mandatory	Time Stamp of the VOP Response [AT-T061]

Note : The X-Response-Timestamp header must contain a valid ISO 8601 timestamp string, expressed in either UTC time format (YYYY-MM-DDThh:mm:ss.sssZ) or local time with UTC offset format (YYYY-MM-DDThh:mm:ss.sss+/-hh:mm), milliseconds included, as defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" (https://www.w3.org/TR/xmlschema-2/) which is aligned with ISO 8601.

4.1.3.3 Response body

Element	Type	Condition	Description
partyNameMatch	Party Name Match Code	{Or	Future ISO code expected [AT-R001] Matching result can be Match, No Match, Close Match with the Name of the Payment Counterparty, Verification Not Possible
partyIdMatch	Party Identification Match Code	Or}	Future ISO code expected [AT-R011] Matching result can be Match, No Match, , Verification Not Possible
matchedName	Max140Text	Conditional	Name of the Payment Counterparty as reported by Responding PSP in the relevant character set. It is up to the Requesting PSP to decide how to display it to the PSU. [AT-R010] This information must be provided if and only if the result of partyNameMatch is “Close Match”

More information about the business and operation rules of the VOP Scheme can be found in the Chapter 3 of the Verification Of Payee Scheme Rulebook [1]

4.2 VOP API Data Model

Note : When an attribute contains sub-elements, these are indented to the right and noted with a plus sign (+) per level.

4.2.1 Party Type

Attribute	Type	Condition	Description
+ name	Max140Text	{Or	The name of the Payment Counterparty [AT-E001] Mandatory for Natural Person (*)
+ identification		Or}	
++ organisationId			
+++ lei	LEI	{Or	Legal entity identification as an alternate identification for a party. LEI is a code allocated to a party as described in ISO 17442 "Financial Services - Legal Entity Identifier (LEI)". [AT-E005]
+++ anyBIC	BIC	Or	Business identification code of the organisation.
+++ others	Array of Generic Organisation Identification	Or }	Usage Rule : the following attributes will be assigned in this array : AT-E005 and AT-E013 Usage Rule : Only one entry to be used

(*) Two combinations are supported as VOP requests (A) Name + IBAN and (B) Identifier Code + IBAN. These two combinations can be supplemented by the optional additional information concerning the Payment Account Number of the Payment Counterparty sent by the Requester (see Chapter 3.2 VOP Scheme Rulebook [1]).

In case of Natural Person, only combination (A) is possible.

4.2.2 Account Type

Attribute	Type	Condition	Description
+ iban	IBAN	Mandatory	The Payment Account Number of the Payment Counterparty [AT-C001]

4.2.3 Agent Type

Attribute	Type	Condition	Description
+ financialInstitutionId			
++ bicfi	BICFI	Mandatory	BIC of the Agent

4.2.4 Generic Organisation Identification

Attribute	Type	Condition	Description
+ identification	Max256Text	Mandatory	The identification code of the Payment Counterparty [AT-E005]
+ schemeNameCode	Organisation Identification Code	{Or-optional	The type of the identification code of the Payment Counterparty (E005) External ISO Code List [AT-E013] Name of the identification scheme, in a coded form as published in an external list (ExternalOrganisationIdentification1Code). (*)
+ schemeNameProprietary	Max35Text	Or-optional}	Name of the identification scheme, in a free text form. (*)
+ issuer	Max35Text	Optional	Entity that assigns the identification

(*) Usage Rule : As an exception to ISO 20022 standards and in accordance with the Verification Of Payee Scheme Rulebook [1], the use of either 'schemeNameCode' or 'schemeNameProprietary' is mandatory when the 'identification code' is used.

4.2.5 Party Name Match Code

Code	Description
MTCH	Match
NMTC	No Match
CMTC	Close Match The provided "payee" name closely resemble the account holder name
NOAP	Verification Check Not Possible Validation Check is not applicable

4.2.6 Party Identification Match Code

Code	Description
MTCH	Match

NMTC	No Match
NOAP	Identification code not supported/known by the Responding Verification Check Not Possible Validation Check is not applicable

Note :

(i) the status code 'NOAP' has to be used with an HTTP 200 response when the identification code is supported at EDS level but is not available for the payee concerned.

(ii) if the identification code is not supported at EDS level, then a http 400 error (bad request) code response should be used.

4.2.7 Other ISO-related basic Types

The following codes and definitions are used from ISO 20022

BICFI :	BICFIIdentifier
Iban :	IBAN2007Identifier Pattern: [A-Z]{2}[0-9]{2}[A-Z0-9]{1,30}
LEI :	LEIIdentifier as defined in ISO 17442 "Financial Services - Legal Entity Identifier (LEI)".

Further basic ISO data types:

- **ISODateTime**: A particular point in the progression of time defined by a mandatory date and a mandatory time component, expressed in either UTC time format (YYYY-MM-DDThh:mm:ss.sssZ) or local time with UTC offset format (YYYY-MM-DDThh:mm:ss.sss+/-hh:mm),. These representations are defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" which is aligned with ISO 8601.

- **ISODate**: A particular point in the progression of time in a calendar year expressed in the YYYY-MM-DD format.

4.3 Business Use Case and result

The "Confirmation Of Payee TF" has identified different Business use cases.

4.3.1 Matching results scenarios

A successful process may return a positive or a negative response. In this case, the HTTP response code will be 'HTTP Code 200 - OK' and will be accompanied by a reason code. In accordance with the Rulebook definition, if the response is positive, the reason code will state Match, No Match or Close Match (+Name). In the event of a negative return, the reason code will be 'Verification Check Not Possible' in all cases.

This validation check applies either to the combination Name-Account Number and Identification Code-Account Number.

Combination Payment Account Number-Name of the Payment Counterparty	Combination Payment Account Number-identification code	HTTP Code
• Match • No Match • Close Match with the Name of the Payment Counterparty • Verification check not possible	• Match • No Match • Verification check not possible	• 200

Table 1: Matching result scenarios [1]

4.3.2 Name + IBAN

Case ID	Case description	partyNameMatch codes
1.1	Name Verification done – Match	MTCH
1.2	Name Verification done – No Match	NMTC
1.3	Name Verification done – Close Match	CMTC + Name of the Payment Counterparty
1.4	Matching not possible for the responding application for any reason	NOAP

4.3.3 Identification code (LEI or VAT number...) + IBAN

Case ID	Case description	partyIdMatch Code
2.1	Id Verification done – Match	MTCH
2.2	Id Verification done – No Match	NMTC
2.3	Id matching not possible for the responding application for any reason	NOAP

4.4 Error Handling

This section introduces the error handling in the VOP API.

If detailed error information is provided by the server in addition to a negative HTTP status code, then the related response must comply with the recommendations of the **RFC7807- Problem**

Details for HTTP APIs standard for HTTP statuses, while adding a dedicated message code attribute. This specification defines a structured method for returning machine-readable error details, typically in JSON format, in addition to standard HTTP status codes.

Detailed error responses will be provided with an appropriate HTTP status code, a properly defined Content-Type header, and a response body structured in JSON for easy interpretation by clients.

4.4.1 Error Response Parameters in case or detailed Error Information

4.4.1.1 Header of the Response in case of Error

Attribute	Type	Condition	Description
Content-type	String	Mandatory	The string application/json is used
X-Request-ID	UUID	Mandatory	The Requesting PSP's reference number of the VOP Request
X-Response-Timestamp	ISODateTime	Mandatory	Time Stamp of the VOP Response [AT-T061]

Note : The X-Response-Timestamp header must contain a valid ISO 8601 timestamp string, expressed in either UTC time format (YYYY-MM-DDThh:mm:ss.sssZ) or local time with UTC offset format (YYYY-MM-DDThh:mm:ss.sss+/-hh:mm), milliseconds included, as defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" (https://www.w3.org/TR/xmlschema-2/) which is aligned with ISO 8601.

4.4.1.2 Body of the Response in case of Error

Attribute	Type	Condition	Description
type	Max70Text	Mandatory	A URI reference [RFC3986] that identifies the problem type
code	Error Message Code	Mandatory	Message code to explain the nature of the underlying error
title	Max70Text	Optional	Short human readable description of error type. Could be in local language. To be provided by PSPs.
status	Integer	Optional	HTTP response code generated by the Server. If contained, this is more relevant as the actual http response code in the actual response, because it is introduced by the Application Server.
detail	Max500Text	Optional	Detailed human readable text specific to this instance of the error.
instance	Max256Text	Optional	This attribute is containing a JSON pointer (as defined in RFC6901) or XPath expression to indicate the path to an issue generating the error in the related request.

4.4.1.3 Error Message Code

Code	Description
FORMAT_ERROR	Incorrect data format has been provided, not compliant with the expected specifications (e.g., invalid JSON format, missing or incorrectly formatted fields).
CLIENT_INVALID	The client is not recognized or is invalid (,an attempt to access resources by an unauthorized client).
CLIENT_INCONSISTENT	The client information provided in the certificate and/or in the request message body is not consistent with related directory information.
TIMESTAMP_INVALID	The timestamp provided in the request is invalid (incorrect format, value in the future, or if it exceeds the allowed validity period by the system).

4.4.2 Error cases

The table below shows some error cases identified and provides the corresponding error code.

Error (+ Message Code if applicable)	Detailed Error	HTTP Code	Example
Format Error (Message Code = FORMAT_ERROR)	This applies to headers and body entries	400	Malformed JSON Request Body could not be parsed
	Missing mandatory field	400	Requesting PSP's BIC is missing
	Presence of two fields that are mutually exclusive	400	Name and identification code
	Unknown field	400	Malformed field's name
	Invalid field's value	400	Malformed IBAN
Timestamp Invalid (Message Code = TIMESTAMP_INVALID)	Timestamp not in accepted Time Period	400	The timestamp refers to a previous day
Client Invalid (Message Code = CLIENT_INVALID)	The API Client has a valid certificate but is not contained in the addressed scheme directory	401	The Requesting's PSP is not adherent to the Scheme
Certificate items	Certificate is invalid, revoked …	401	The API Client's certificate is not a valid PSD2 QWAC.
Authorisation Issue (Message Code = CLIENT_INCONSISTENT)		401	Certificate's NAN and request BIC do not match
Internal Server Error		500	An exception occurs during code execution and the request cannot be further processed

4.5 Definition of the HTTP Codes

The VOP API supports the following HTTP response codes.

Code	Name	Description
200	OK	The request has succeeded.
400	Bad Request	Validation error occurred. The request could not be understood by the server due to malformed syntax in request or incorrect data in payload. The client SHOULD NOT repeat the request without modifications.
401	Unauthorized	The Requesting's PSP is not correctly authorized to perform the request. Retry the request with correct authentication information.
500	Internal Server Error	The server encountered an unexpected condition which prevented it from fulfilling the request.

5 Example of API uses

5.1 Example of a VOP Request for a Natural/Legal Person (Name + IBAN)

<table>
<tr><th>Request</th><th>Response</th></tr>
<tr><td>

```
POST /api/vop/v1/payee-verifications
Host: api.example.com
Content-Type: application/json
Accept: application/json
User-Agent: MyApp/1.0
Content-Length: 312
Date: Mon, 12 Aug 2024 15:19:21 GMT
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Request-Timestamp: 2024-08-12T15:19:21.123Z

{
   "party": {
      "name": "Dupont Jean"
   },
   "partyAccount": {
      "iban": "BE12345678901234"
   },

   "partyAgent": {
      "financialInstitutionId": {
         "bicfi": "ABCDBEBBXXX "
      }
   },
   "requestingAgent": {
      "financialInstitutionId": {
         "bicfi": "ABCDBEB0XXX"
      }
   }
}
```

</td><td>

Result Match

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyNameMatch": "MTCH"
}
```

Result No Match

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyNameMatch": "NMTC"
}
```

Close Match with the Name of the Payment Counterparty

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 72

{
    "partyNameMatch": "CMTC",
    “matchedName”: "Dupond Jean"
}
```

Verification Check not possible

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyNameMatch": "NOAP"
}
```

</td></tr>
</table>

5.2 Example of a VOP Request for a Legal Person (Id + IBAN)

Request

```
POST /api/v1/payee-verification
Host: api.example.com
Content-Type: application/json
Accept: application/json
User-Agent: MyApp/1.0
Date: Mon, 12 Aug 2024 15:19:21 GMT
Content-Length: 481
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Request-Timestamp: 2024-08-12T15:19:21.123Z

{
  "party": {
    "identification": {
      "organisationId": {
          "others": [
             {
               "identification": "ABC1234",
               "schemeNameCode": "XXXX"
             }
          ]
      }
    }
  },
  "partyAccount": {
    "iban": "BE12345678901234"
  },
  "partyAgent": {
    "financialInstitutionId": {
      "bicfi": "ABCDBEBBXXX "
    }
  },
  "requestingAgent": {
    "financialInstitutionId": {
      "bicfi": "ABCDBEB0XXX"
    }
  }
}
```

Response

Result Match

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyIdMatch": "MTCH"
}
```

Result No Match

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyIdMatch": "NMTC"
}
```

Identification code not supported/known by the Responding

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyIdMatch": "NOAP"
}
```

Verification Check not possible

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-ID: 123e4567-e89b-12d3-a456-426614174000
X-Response-Timestamp: 2024-08-12T15:19:22.678Z
Content-Length: 37

{
    "partyIdMatch": "NOAP"
}
```

In the case of a request based on “ID+IBAN”, the API cannot return “Close Match”.

6 Defined Terms in the Verification of Payee API Specifications

Term	Definition
API	Application Programming Interface
BIC	Bank Identification Code An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution in financial transactions
Close Match with the Name of the Payment Counterparty	*For the definition of the "Close Match" result, please refer to the "Proposed EPC Recommendations for the Matching Processes under the VOP Scheme Rulebook" [6]*
Endpoint	an *endpoint* refers to a specific URL where an API request is sent to access a particular resource or service. It defines the exact location on the server for performing operations.
EPC	European Payments Council
EPC Directory Service (EDS)	The EDS stores and maintains all required operational data about Participants to facilitate the interoperability between Scheme-based services offered by Participants, RVMs and any other relevant entities. The managed data concern among others Scheme adherence, identification, URLs and endpoints about Participants. Participants shall ensure that their reachability path and relevant data are included in the EDS. Refer to EDS specifications [10]
IBAN	International Bank Account Number (IBAN): uniquely identifies an individual account at a specific financial institution in a particular country (ISO 13616) ([2]).
IPR	Instant Payment Regulation
LEI	Legal Entity Identifier, means a global unique alphanumeric reference code based on the ISO 17442 standard assigned to a legal entity and maintained by GLEIF. The LEI and its reference data shall be updated regularly to conform with Regulatory Oversight Committee (ROC) Policies. More information is available on the webpage https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei
Match	*For the definition of the "Match" result, please refer to the "Proposed EPC Recommendations for the Matching Processes under the VOP Scheme Rulebook" [6]*
Name of the Payment Counterparty	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
NAN	National Authorization Number
NCA	National Competent Authority

Term	Definition
No Match	For the definition of the "*No Match*" result, please refer to the "Proposed EPC Recommendations for the Matching Processes under the VOP Scheme Rulebook" [6]
Payment Account	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Payment Account Number of the Payment Counterparty	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Payment Services Directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD).
Proxy	A "proxy" acts as a message gateway which remains transparent from a scheme perspective; also see definitions of RTSP and RVM below
PSD	Payment Services Directive.
PSP	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
PSU	Payment Service User.
QWAC	A 'Qualified Web Authentication Certificate' (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.
Requester	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Requesting PSP	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Responding PSP	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Rulebook	The Verification Of Payee Scheme Rulebook [1], as amended from time to time.
RVM	Routing and/or Verification Mechanisms
Scheme	The VOP Scheme, as described in the Rulebook. *See definition found in the Verification Of Payee Scheme Rulebook [1].*
Scheme Management	*See definition found in the Verification Of Payee Scheme Rulebook [1].*

Term	Definition
SEPA	The Single Euro Payments Area (SEPA) is the area where citizens, companies and other economic actors can make and receive payments in euro, within Europe, whether within or across national boundaries under the same basic conditions, rights and obligations, regardless of their location. SEPA is driven by the European Commission and the European Central Bank, amongst others, as a key component of the EU Internal Market. SEPA shall be deemed to encompass the countries and territories which are part of the geographical scope of the SEPA Schemes, as listed in the EPC List of SEPA Scheme Countries (see Reference [4]), as amended from time to time.
SEPA Regulation	Regulation (EU) 260/2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 (the 'SEPA Regulation').
SEPA Scheme	Is a common set of business rules, practices and standards for the provision and operation of a SEPA payment or SEPA payment-related instrument agreed at inter-PSP level in a competitive environment.
Supporting Documentation	A legal opinion in the form set out on the website of the EPC, duly executed by the undertaking's internal or external counsel in accordance with the Internal Rules.
Terms and Conditions	The general Terms and Conditions that a PSP has with its Payment Service Users and which may contain dispositions about their rights and obligations related to VOP. These dispositions may also be included in a specific agreement, at the Participant's choice.
Time Stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
TLS EV	Transport Layer Security Extended Validation
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VAT number	Value Added Tax number.
Verification Of Payee Request	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Verification Of Payee Response	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
Verification Of Payee Scheme Management Rules	*See definition found in the Verification Of Payee Scheme Rulebook [1].*
VOP	Verification Of Payee.
YAML	YAML (YAML Ain't Markup Language) is a data-oriented language structure used as the input format for diverse software applications

Annexe A : Errata List

Version	Amendments
1.0.1	• **Section 2.3.3:** Added in bold for the text: "In case of IBAN + Identification code: Match (MTCH), No Match (NMTC), **Not Applicable (NOAP)**.". • **Section 4.1.3.3**: Rephrased as follows: "This information is required only when the result of partyNameMatch is "Close Match". • **Section 4.2.4**: Correction for code 200222 - updated text: "As an exception to **ISO 20022**…". • **Section 4.4.1.1:** Add clarification regarding the header for the Response in cases of Error: adding the X-Request-ID and X-Response-Timestamp and the note (as described in the YAML file). • **Section 5.2:** Corrected the positioning of a closing bracket for the "party" element in the Request example.