

API description of iXBRL reception service

Technical document for software suppliers
Version 0.4 (9 September 2026)

Version history

Date	Author	Description
17 December 2024	Riina-Alisa Huotari, Solita	Official published version 0.1 of API version v3
6 March 2025	Riina-Alisa Huotari, Solita	Corrections of translations of error messages, one additional error response (invalid query parameter <i>submissionID</i>), specification of <i>submission ID</i> length, update of the description of service <i>Supported company forms and taxonomies</i>
18 March 2025	Riina-Alisa Huotari, Solita	Update of supported taxonomies (removal of old taxonomies for consolidated financial statements)
9 September 2026	Riina-Alisa Huotari, Solita	General specifications Update of certificate approval chains Update of the Taxonomies section References to foundations have been removed Less repetition in the description of service responses

Table of contents

1	General description of the API.....	4
2	For users.....	4
3	System description.....	4
3.1	Top-level description of the architecture	5
3.2	Authentication.....	5
3.3	XBRL API.....	6
3.4	API contact addresses	6
3.4.1	In the test environment	6
3.4.2	In the production environment	6
3.5	Certificates	7
3.5.1	Approval chain in the test environment	7
3.5.2	Approval chain in the production environment	7
4	Technical description	7
4.1	Authentication.....	7
4.1.1	Responses returned by the service	8
4.2	Submitting reports for validation.....	9
4.2.1	Responses returned by the service	12
4.3	Validation status service	16
4.3.1	Responses returned by the service	17
4.4	Forwarding reports	19
4.4.1	Responses returned by the service	20
4.5	Service for supported company forms and taxonomies	21
4.5.1	Responses returned by the service	22
4.6	Error responses common to all services	22
5	Taxonomies	24
6	Appendices	24

This document describes the REST API version 3.0, which is intended for submitting reports in iXBRL format to the Finnish Trade Register. With this overview, customers can familiarise themselves with the technical and functional content of the API.

A general description of the API is given in Chapter 1. The API services are described in detail from Chapter 2 onwards.

1 General description of the API

The **XBRL reception service** is an API in which the customer (company, accounting firm or a third party acting on their behalf) can submit reports (incl. metadata) in iXBRL format to the Finnish Trade Register.

As a rule, the API connection is open 24 hours a day.

- Maintenance services and user support are available during office hours.

2 For users

The PRH does not provide the customers with ready-made software for using the API. This means that customers must develop adequate functionalities for their own systems that they use to submit the reports to the PRH.

The customers should take the following technical features into account when planning the introduction of the API:

- The PRH provides a test server for testing the API.
- Both the production and test servers only permit a TLS 1.2 secure connection.
- UTF-8 character encoding must be used in the messages and reports sent to the API.
- Connections to the test server are permitted for IP addresses (space) on a case-by-case basis. Customers must notify the PRH contact person of the required IP addresses well in advance.
 - Connections to the production server are open to everyone.
- Client systems use customer-specific technical user IDs and passwords for identification via a separate authentication server before sending a service call. The OpenID Connect protocol is used in authentication. This means that each service call must contain an access token retrieved from the authentication service. The token is valid for a limited period. Customers must request the required user ID and password from the PRH contact person well in advance.
- New versions of the API may be published in the future and thus different versions of the service featuring different requirements and functionalities may be available at the same time. Customers should therefore use the same API version for all services (for example, only API v3 services).

3 System description

The API is based on the REST principle, which is explained in the RAML description language in the technical API description appended to this document (see [Appendices](#)).

The customer calls the XBRL reception service via a front-end server, identifying itself with an access token. The access token is retrieved from a separate authentication server using the **OpenID Connect**¹ protocol and the **Client Credentials Grant Flow**.

- The XBRL reception service has been implemented as a REST API.
- The HTTPS protocol (port 443) is used in the call.
- The service returns a response stating whether the call succeeded or failed.
- The service guarantees the sending of the company's reports to the back-end systems in the correct order of reception (the reports of a company already received are always processed before its reports received later).
- The time when the reports are received in the service is considered the time when they are submitted. This information is stored with the other submission metadata and forwarded to the PRH's back-end systems.

3.1 Top-level description of the architecture

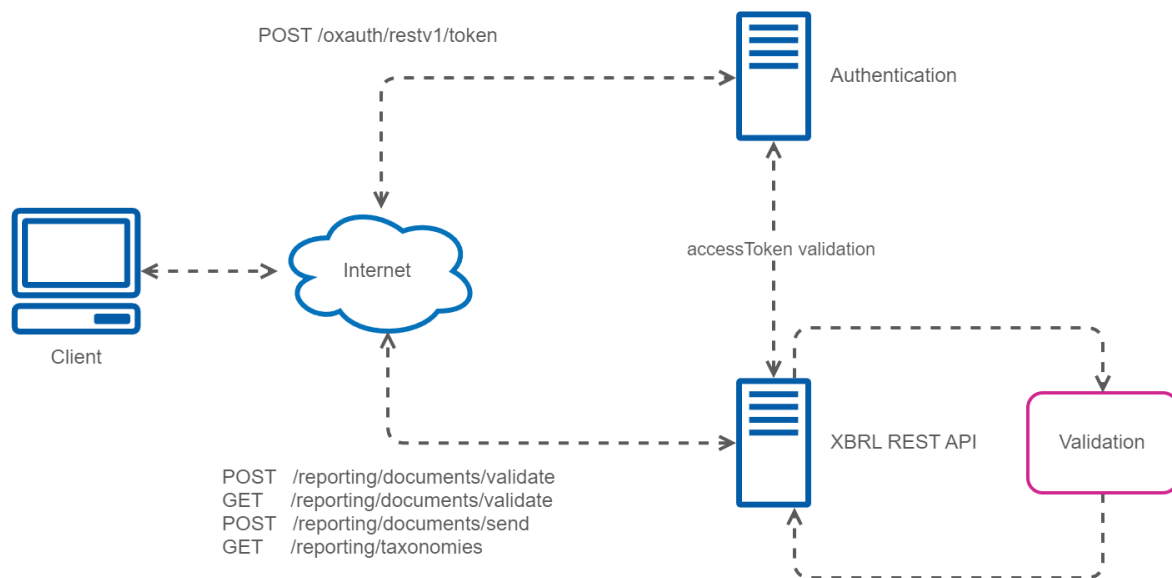


Figure 1 Top-level description of the service architecture

3.2 Authentication

The customer certificate is retrieved from a separate authentication server using the **OpenID Connect** protocol and the **Client Credentials Grant Flow**.

The customer must authenticate itself via the PRH's centralised access management. As a response to the authentication, the customer receives an access token, which is valid for a limited period and which is used for identification in the service calls.

The API uses the access token to validate the customer's right to call the API.

¹ <https://openid.net/connect/>

The access token is valid for the time specified in the response message until it expires. After the access token has expired, the customer must authenticate itself again so that new service calls can be made.

3.3 XBRL API

The service provides the API user with the opportunity to validate and send reports in iXBRL format to the PRH's back-end systems.

The service calls offered by the API are as follows:

1. POST reporting/documents/validate
 - Receives the reports in iXBRL format and the metadata message (JSON) submitted for validation
 - The API makes the necessary checks on the call and then forwards the reports to a separate validator application for validation
2. GET reporting/documents/validate
 - Based on the *submissionID*, returns the validation status of the reports and the validation result if the validation has been completed
3. POST reporting/documents/send
 - Receives the *submissionID* and forwards the reports already submitted for validation with the *submissionID* if they have been successfully validated
4. GET reporting/taxonomies
 - Returns the taxonomy schemas supported by the API and their versions by company form.

The sending of the reports always starts with the submission of the reports for validation (first service call). Only after the reports have been successfully validated (second service call), the reports can be sent (third service call). The taxonomies service (fourth service call) is an auxiliary service, which can be called if the customer needs to check the taxonomy versions and company forms supported by the API.

3.4 API contact addresses

3.4.1 In the test environment

Service request	Type	Contact address in the test environment
AccessToken	POST	https://auth.qa.prh.fi/oxauth/restv1/token
Validate	GET, POST	https://xbml-qa.prh.fi/api/v3/reporting/documents/validate
Send	POST	https://xbml-qa.prh.fi/api/v3/reporting/documents/send
Taxonomies	GET	https://xbml-qa.prh.fi/api/v3/reporting/taxonomies

3.4.2 In the production environment

Service request	Type	Contact address in the production environment
-----------------	------	---

AccessToken	POST	https://auth.prh.fi/oxauth/restv1/token
Validate	GET, POST	https://xbml.prh.fi/api/v3/reporting/documents/validate
Send	POST	https://xbml.prh.fi/api/v3/reporting/documents/send
Taxonomies	GET	https://xbml.prh.fi/api/v3/reporting/taxonomies

3.5 Certificates

Test and production environments use SSL certificates issued by SSL.com. The SSL.com root certificates required at the client end can be found at <https://www.ssl.com/repository/>

- Test and production environment root certificate:
 - USERTrust RSA Certification Authority

Certificate approval chains are described in the sections below.

3.5.1 Approval chain in the test environment

USERTrust RSA Certification Authority
 → Sectigo Public Server Authentication Root R46
 → Entrust OV TLS Issuing RSA CA 2
 → xbrl-qa.prh.fi

3.5.2 Approval chain in the production environment

USERTrust RSA Certification Authority
 → Sectigo Public Server Authentication Root R46
 → Entrust OV TLS Issuing RSA CA 2
 → xbrl.prh.fi

4 Technical description

This document only presents the basic operating principles of the API. The complete technical API description can be found in the RAML API description appended to this document.

4.1 Authentication

Method: POST
URL: <https://<palvelin>.prh.fi/oxauth/restv1/token>

Headers:

Header	Value	Mandatory	Description
Host	<palvelin>.prh.fi	Yes	Server name of the authentication server
Accept	application/json	Yes	Specified acceptable content type

Authorization	Basic <Base64[client_id:client_secret]>	Yes	Client_id and client_secret issued by the PRH to the entity to be authenticated as Base64 encoded version. Note: the colon between client_id and client_secret is significant
Content-Type	application/x-www-form-urlencoded	Yes	Specified content type

Body:

- MIME-type: application/x-www-form-urlencoded

Parameter	Value	Mandatory	Description
grant_type	password	Yes	Issuing method specified for the entity to be authenticated
username	<käyttäjätunnus>	Yes	User ID issued by the PRH to the entity to be authenticated
password	<salasana>	Yes	Password issued by the PRH to the entity to be authenticated
scope	openid profile email group_membership	Yes	Attributes required for authentication

4.1.1 Responses returned by the service

4.1.1.1 Successful call

HTTP/1.1 200 OK Content-Type: application/json
<pre>{ "access_token": "a1111111-b222-c333-d44444444444", "scope": "group_membership openid profile email", "token_type": "bearer", "expires_in": 5999 }</pre>

- Authentication was successful
- Access token can be retrieved from the field *access_token*
- The access token expiration time (in seconds) is given in the field *expires_in*

4.1.1.2 Error responses

HTTP/1.1 400 Bad Request Content-Type: application/json
<pre>{</pre>

```
"error_description":  
"The request is missing a required parameter, includes an unsupported parameter or parameter value, repeats a parameter, includes multiple credentials, utilizes more than one mechanism for authenticating the client, or is otherwise malformed.",  
"error": "invalid_request"  
}
```

- Authentication failed
- The call is invalid; for example, the mandatory parameter is not given in the call or the body is of a wrong type

HTTP/1.1 401 Unauthorized
Content-Type: application/json

```
{  
  "error_description":  
    "Client authentication failed (e.g. unknown client, no client authentication included, or unsupported authentication method). The authorization server MAY return an HTTP 401 (Unauthorized) status code to indicate which HTTP authentication schemes are supported. If the client attempted to authenticate via the Authorization request header field, the authorization server MUST respond with an HTTP 401 (Unauthorized) status code, and include the WWW-Authenticate response header field matching the authentication scheme used by the client.",  
  "error": "invalid_client"  
}
```

- Authentication failed
- Invalid or missing Authorization-header, client_id, or client_secret
- Login details (ID or password) are missing, invalid or expired, or login is denied

HTTP/1.1 403 Forbidden
Content-Type: application/json

- Authentication failed
- Access from the customer application to the authentication API has been blocked

HTTP/1.1 500 Server Error

- Authentication failed
- Other technical error

4.2 Submitting reports for validation

Method: POST
URL: <https://<palvelin>.prh.fi/api/v3/reporting/documents/validate>

This service is called when the customer wants to start sending the reports. When this service is called both the reports and the required metadata must be submitted.

The API receives the call, checks its contents and forwards the reports to a separate validator application for validation.

When the service returns a successful response, it means that the reports have been received and forwarded to the validator application for processing. **In other words, the reports have not yet been forwarded to the PRH's back-end systems.**

Headers:

Header	Value	Mandatory	Description
Authorization	Bearer <access token>	Yes	OpenID Connect access token retrieved from the authentication server

Body:

- MIME-type: multipart/form-data

Type	Name	File name	Mandatory	Value
File	financialStatement	<vapaa teksti>	Yes	Financial statements as xhtml file or zip package
Text	requestMetadata		Yes	Call and attachment metadata as a string (see a more detailed description below)

```
POST /api/v3/reporting/documents/validate HTTP/1.1
Host: <server-name>.prh.fi
Authorization: Bearer a1111111-b222-c333-d44444444444
Content-type: multipart/form-data, boundary=AaB03x

--AaB03x
Content-Disposition: form-data; name="requestMetadata"
Content-Type: application/json

{ "submissionID": ... }

==binarydata==

--AaB03x
Content-Disposition: form-data; name="financialStatement";
filename="financialstatement.xhtml"
Content-Type: text/html

<!DOCTYPE html><title>Financial statement content<title>

--AaB03x--
```

A call must contain the following attachments presented in the table above: *requestMetadata* and *financialStatement*. The attachments are identified by name (*Content-Disposition > name*). The attachment name (*Content-Disposition > filename*), which is a free text field, is also retrieved from the attachment *financialStatement*. **However, the file name may have a maximum length of 200 characters and xhtml, html or zip must be used as file name extension.**

requestMetadata (JSON):

Structure of the attachment *requestMetadata* is described below, and one example of the attachment is given:

Field ID	Type	Explanation
submissionID	string	<i>submissionID</i> The value can be freely selected by the client software and it can be a running number (note: type string) or UUID. Length 1–200 characters.
establishmentID	string	The <i>Business ID</i> of the entity using its technical IDs (such as an accounting firm or a similar operator) that/whose software has compiled the reports to be submitted.
entityID	string	The <i>Business ID</i> of the company whose reports are being submitted.
reportType	string	<i>reportType</i> to be submitted. Permitted values: [AFR, CFR] - AFR: financial statements of a company - CFR: financial statements of a group company
periodStart	string	<i>periodStart</i> to be reported in the form yyyy-mm-dd.
periodEnd	string	<i>periodEnd</i> to be reported in the form yyyy-mm-dd.
documentName	string	Name of the attachment (same as the name of the body attachment). Permitted values: [financialStatement]
attachmentType	string	Attachment type. IXBRL is used for SBR taxonomy. ESEF is used for ESEF taxonomy. IFRS is used for IFRS taxonomy. For instructions for situations with more than one taxonomy, see 'Submission has been in accordance with two taxonomies' Permitted values: [IXBRL, ESEF, IFRS]
schemaVersion	string	Identifier of the taxonomy schema used in the attachment. The permitted values can be checked from the Taxonomies service.

```
{
  "submissionID": "12345",
  "establishmentID": "8765432-1",
  "entityID": "1234567-8",
  "reportType": "AFR",
  "periodStart": "2026-01-01",
  "periodEnd": "2026-12-31",
  "documents": [
    {
      "documentName": "financialStatement",
      "attachmentType": "IXBRL",
      "schemaVersion": "oytp_gaap_ind_2025-10-16"
    }
  ]
}
```

Values of the fields *reportType*, *attachmentType* and *schemaVersion* vary depending on the company form and the taxonomy of the financial statements being submitted and they must match each other. Field values in different situations are described below:

The submission has been made in accordance with one taxonomy

Case description	reportType	attachmentType	schemaVersion
Financial statements of a company, SBR taxonomy	AFR	IXBRL	*_ind_*
Financial statements of a group company, SBR taxonomy	CFR	IXBRL	*_con_*
Financial statements of a company, IFRS taxonomy	AFR	IFRS	IFRS-*
Financial statements of a public group company, IFRS taxonomy	CFR	IFRS	IFRS-*

The submission has been made in accordance with two taxonomies

Case description	reportType	attachmentType	schemaVersion
Financial statements of a group company, ESEF taxonomy. Financial statements of a company, SBR taxonomy.	CFR	ESEF	ESEF-*
Financial statements of a group company, IFRS taxonomy. Financial statements of a company, SBR taxonomy.	CFR	IFRS	IFRS-*
Financial statements of a group company, ESEF taxonomy. Financial statements of a company, IFRS taxonomy.	CFR	ESEF	ESEF-*

4.2.1 Responses returned by the service

4.2.1.1 Successful call

HTTP/1.1 202 Accepted
Content-Type: application/json

```
{
  "validation": {
    "submissionID": "12345",
    "establishmentID": "8765432-1",
    "entityID": "1234567-8",
    "reportType": "AFR",
```

```

    "periodStart": "2026-01-01",
    "periodEnd": "2026-12-31",
    "documents": [
      {
        "documentName": "financialStatement",
        "attachmentType": "IXBRL",
        "schemaVersion": "oytp_gaap_ind_2025-10-16"
      }
    ],
    "receivedForValidationOn": "2027-01-01T12:00:00.123Z",
    "validationStatusEndpoint": "/reporting/documents/validate?submissionID=12345"
  }
}

```

- Reports successfully submitted for validation
- No resending

4.2.1.2 Error responses

The service can return several different error messages but they are all returned with HTTP status 400 Bad Request and the error response is always in the following format:

HTTP/1.1 400 Bad Request
Content-Type: application/json

```

{
  "detail": [
    {
      "loc": "<location of error>",
      "msgEn": "<error in English>",
      "msgFi": "<error in Finnish>",
      "msgSv": "<error in Swedish>",
      "type": "string"
    }
  ]
}

```

The cases in which a Bad Request error response is returned are described below:

Error description	Error location	Error message in Finnish	Resending
There was no attachment named <i>requestMetadata</i> among the attachments given in the call	requestMetadata	Metadata is missing from the call ('requestMetadata')	The missing attachment <i>requestMetadata</i> must be added to the call before resending
The <i>requestMetadata</i> (JSON) attached to the call is not valid	requestMetadata	Metadata is missing from the call ('requestMetadata')	The call attachment <i>requestMetadata</i> must be corrected to comply with the specified schema before resending
Details of the same file are given in the metadata more than once	requestMetadata	The file name ('documentName') is given in the metadata more than once	The attachment <i>requestMetadata</i> must be corrected to contain the

			data entered in the file only once before resending
An attachment with the same name is given in the call more than once	<liitteen nimi>	The attachment ' <liitteen nimi>' is given in the call more than once	The extra attachment must be removed from the call before resending
There was no attachment named <i>financialStatement</i> among the attachments given in the call	financialStatement	The call does not contain the attachment 'financialStatement'	The missing attachment <i>financialStatement</i> must be added to the call before resending
The attachments given in the call include an extra attachment	<liitteen nimi>	The call includes an unexpected attachment '<liitteen nimi>'	The extra attachment must be removed from the call before resending
The actual file name of the attachment <i>financialStatement</i> is too long (more than 200 characters)	financialStatement	The file name of the attachment 'financialStatement' is too long	The file name of the attachment <i>financialStatement</i> must be shortened before resending
The actual file name of the attachment <i>financialStatement</i> is not permitted (xhtml, html or zip are the permitted file formats)	financialStatement	The file format of the attachment 'financialStatement' is not permitted	The file given in the attachment <i>financialStatement</i> must be in a permitted format before resending
The actual file name of the attachment <i>financialStatement</i> could not be retrieved from the call	financialStatement	The file name of the attachment 'financialStatement' could not be retrieved	The call structure must be changed before resending so that the file name (field <i>filename</i> in the header Content-Disposition of the multipart call) is included in the attachment <i>financialStatement</i>
A submission has already been made with the same identifier	requestMetadata	A submission has already been made with the identifier '<submissionID>'	No resending
No company details matching the <i>Business ID</i> could be found	requestMetadata	Company information check failed: No company details matching the <i>Business ID</i> 1234567-8 could be found	No resending
Company details matching the <i>Business ID</i> were found but the company name was missing	requestMetadata	Company information check failed: company name for company 1234567-8 was not found	No resending

Company details matching the <i>Business ID</i> were found but the company form was missing	requestMetadata	Company information check failed: company form for company 1234567-8 was not found	No resending
Company details matching the <i>entityID</i> were found but the company form is invalid	requestMetadata	Company information check failed: company form of company 1234567-8 is not permitted	No resending
Company details matching the <i>entityID</i> were found but the registration status was missing	requestMetadata	Company information check failed: registration status for company 1234567-8 was not found	No resending
Company details matching the <i>entityID</i> were found but the company is not in the Finnish Trade Register	requestMetadata	Company information check failed: company 1234567-8 is not in the Finnish Trade Register"	No resending
The <i>periodStart</i> and/or <i>periodEnd</i> given is not valid (for example, '2027-02-30')	requestMetadata	The <i>periodStart</i> or <i>periodEnd</i> given is not valid	The attachment <i>requestMetadata</i> must be corrected to include the valid <i>periodStart</i> and/or <i>periodEnd</i> before resending
The <i>periodStart</i> given is not before <i>periodEnd</i>	requestMetadata	The accounting period given is invalid: <i>periodStart</i> must be before <i>periodEnd</i>	The attachment <i>requestMetadata</i> must be corrected to include the valid <i>periodStart</i> and <i>periodEnd</i> before resending
The <i>periodEnd</i> given is in the future	requestMetadata	The accounting period given is invalid: <i>periodEnd</i> cannot be in the future	The attachment <i>requestMetadata</i> must be corrected to include the valid <i>periodEnd</i> before resending
The gap between the <i>periodStart</i> and <i>periodEnd</i> given is more than 18 months	requestMetadata	The accounting period given is invalid: the period cannot exceed 18 months	The attachment <i>requestMetadata</i> must be corrected to include the valid <i>periodStart</i> and <i>periodEnd</i> before resending

The specified taxonomy is not permitted for the company form	requestMetadata	Taxonomy 'oytp_gaap_ind_2025-10-16' is not permitted for company form 'SR'	No resending
The specified taxonomy does not match the attachment type given	requestMetadata	Taxonomy 'oytp_gaap_ind_2025-10-16' does not match attachment type 'ESEF'	The attachment <i>requestMetadata</i> must be corrected to include the valid attachment type before resending
The specified taxonomy does not match the report type given	requestMetadata	Taxonomy 'oytp_gaap_ind_2025-10-16' does not match report type 'CFR'	The attachment <i>requestMetadata</i> must be corrected to include the valid report type before resending

In addition to Bad Request responses, the service may also return error responses common to all services, see [Error responses common to all services](#).

4.3 Validation status service

Method: GET
URL: <https://<palvelin>.prh.fi/api/v3/reporting/documents/validate>
Example: <https://<palvelin>.prh.fi/api/v3/reporting/documents/validate?submissionID=12345>

This service is called after the reports have been submitted for validation using the service [Submitting reports for validation](#). The service returns a response stating whether the validation is incomplete, whether it has succeeded or failed, and the validation result if the validation has been completed.

This service is called at suitable intervals until the API returns a response stating that the validation has been completed.

- Duration of the validation depends on such matters as the size of the reports being validated and the load of the validator application
- Recommended interval for calling the service is 10–30 seconds

If the service returns a response stating that the validation has been successful, the reports can be forwarded to the back-end systems using the [Forwarding reports](#) service.

- Click [Responses returned by the service](#) to see how different responses differ from each other

Headers:

Header	Value	Mandatory	Description
--------	-------	-----------	-------------

Authorization	Bearer <access token>	Yes	OpenID Connect access token retrieved from the authentication server
---------------	-----------------------	-----	--

Query parameters:

Parameter	Type	Mandatory	Description
submissionID	string	Yes	<i>submissionID</i> The same <i>submissionID</i> that is given in the metadata when the reports are submitted for validation. Length 1–200 characters.

4.3.1 Responses returned by the service

4.3.1.1 Successful call

If the call is successful, the service returns the response in the following format:

HTTP/1.1 200 OK Content-Type: application/json
<pre>{ "submissionID": "12345", "documents": [{ "documentName": "financialStatement", "attachmentType": "IXBRL", "schemaVersion": "oytp_gaap_ind_2025-10-16", "validationStatus": "success", "validationResult": { "duration": "30000", "creationDate": "2027-01-01T12:00:00.123+0000", "completionDate": "2027-01-01T12:00:30.123+0000", "errorCount": 0, "memos": [] } }] }</pre>

However, the values and contents of the fields *validationStatus*, *errorCount* and *memos* vary depending on the validation status.

- **Note!** If the validation is still in progress, the value of the object *validationResult* is null, and the fields inside it (such as *errorCount* and *memos*) are not yet returned.

The values of the fields in different situations are described below:

Description of the situation	<i>validationStatus</i>	<i>errorCount</i>	<i>memos</i> (example)
Validation of reports is in progress	ongoing	<not returned>	<not returned>
The reports have been successfully validated and without comments	success	0	[]

The reports have been successfully validated but the validator returned comments	success	0	[“Warning: The financial statement is missing the information \"Financial statement is consolidated into the consolidated financial statements\".\", \"Warning: The value in the balance sheet item \"Assets\" does not match the sum of the items \"Non-current\" assets and \"Current assets\".\".]
Validation of the reports failed and the validator only returned errors	fail	1...n	[“Error: Any <i>entityID</i> did not match metadata, expected: 1234567-8. Document: financialstatement.xhtml”]
Validation of the reports failed and the validator returned both comments and errors	fail	1...n	[“Warning: Inline XBRL: Inconsistent duplicate fact definition detected for ...”, “Error: XBRL Validation Error: An instance must not have more than one fact having the same element name ...”]

4.3.1.2 Error responses

The service can return several different error messages but they are all returned with HTTP status 400 Bad Request and the error response is always in the following format:

HTTP/1.1 400 Bad Request Content-Type: application/json
<pre>{ "detail": [{ "loc": "<location of error>", "msgEn": "<error in English>", "msgFi": "<error in Finnish>", "msgSv": "<error in Swedish>", "type": "string" }] }</pre>

The cases in which a Bad Request error response is returned are described below:

Error description	Error location	Error message in Finnish	Resending
The mandatory query parameter <i>submissionID</i> is not given in the call	submissionID	The query parameter 'submissionID' is not given in the call	The missing query parameter <i>submissionID</i> must be added to the call before resending
The value given in the query parameter <i>submissionID</i> is not valid (the value is too short or too long)	submissionID	The value of the query parameter 'submissionID' is not valid.	The value of the query parameter must be corrected before resending

No submission has been made with the submissionID and user ID given	submissionID	Submission '<submissionID>' does not exist	No resending
---	--------------	--	--------------

In addition to Bad Request responses, the service may also return error responses common to all services, see [Error responses common to all services](#).

4.4 Forwarding reports

Method: POST

URL: <https://<palvelin>.prh.fi/api/v3/reporting/documents/send>

This service is called when you want to forward the reports to the back-end systems after validation. The reports must first be submitted for validation using the service [Submitting reports for validation](#) and the validation must be checked using the service [Validation status](#).

When calling this service, you do not need to resubmit the reports. Only the *submissionID* with which the reports have already been submitted for validation should be given with the call.

The API receives the call, checks its contents and forwards the reports to the back-end systems.

The reports can only be sent after they have been successfully validated. The reports must be

- sent within seven (7) days after the validation has been completed

Headers:

Header	Value	Mandatory	Description
Authorization	Bearer <access token>	Yes	OpenID Connect access token retrieved from the authentication server

Body:

- MIME-type: application/json

Field ID	Type	Explanation
submissionID	string	<i>submissionID</i> The same <i>submissionID</i> that is given in the metadata when the reports are submitted for validation. Length 1–200 characters.

```
POST /api/v3/reporting/documents/send HTTP/1.1
Host: <server-name>.prh.fi
Authorization: Bearer a1111111-b222-c333-d44444444444
Content-type: application/json
```

```
{
  "submissionID": "12345"
}
```

4.4.1 Responses returned by the service

4.4.1.1 Successful call

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "submissionID": "12345",
  "receivedOn": "2025-01-01T12: 31: 00.123Z",
}
```

- Reports were successfully forwarded
- No resending

4.4.1.2 Error responses

The service can return several different error messages but they are all returned with HTTP status 400 Bad Request and the error response is always in the following format:

```
HTTP/1.1 400 Bad Request
Content-Type: application/json

{
  "detail": [
    {
      "loc": "<location of error>",
      "msgEn": "<error in English>",
      "msgFi": "<error in Finnish>",
      "msgSv": "<error in Swedish>",
      "type": "string"
    }
  ]
}
```

The cases in which a Bad Request error response is returned are described below:

Error description	Error location	Error message in Finnish	Resending
The body (JSON) given in the call is not valid	body	Invalid call JSON. Errors: <virheet englanniksi>	Call body must be corrected to comply with the specified schema before resending

No submission has been made with the submissionID and user ID given	submissionID	Submission '<submissionID>' does not exist	No resending
The reports with the <i>submission ID</i> given have already been forwarded	submissionID	Submission '<submissionID>' has already been sent	No resending
The submission made with the <i>submissionID</i> given has expired (too much time has passed since the validation was completed), and the reports cannot thus be forwarded	submissionID	Submission '<submissionID>' has expired. Please make a new submission	No resending
Validation of the reports with the <i>submissionID</i> given failed and the reports cannot thus be forwarded	submissionID	Validation of one or more files failed. Submission '<submissionID>' cannot be sent	No resending
Validation of the reports with the <i>submissionID</i> given has not yet been completed and the reports cannot thus be forwarded yet	submissionID	Not all files have been validated yet. Submission '<submissionID>' cannot be sent	You can try to resend the reports after the validation has been successfully completed

In addition to Bad Request responses, the service may also return error responses common to all services, see [Error responses common to all services](#).

4.5 Service for supported company forms and taxonomies

Method: GET

URL: <https://<palvelin>.prh.fi/api/v3/reporting/taxonomies>

This service is called when you want to check which company forms and taxonomies the API is supporting.

In the response returned by the service, the values in the field *schemaVersion* are identifiers of the taxonomy schema.

- These values are the same as the values that the service [Submitting reports for validation](#) accepts for the field of the same name given in metadata.

In the response returned by the service, the values in the field *entryPointURI* are references to the XML schema file of the taxonomy in question.

- If there is no specific XML schema file for the taxonomy (such as ESEF taxonomy), the field returns *null* as value.

Headers:

Header	Value	Mandatory	Description
Authorization	Bearer <access token>	Yes	OpenID Connect access token retrieved from the authentication server

4.5.1 Responses returned by the service

4.5.1.1 Successful call

HTTP/1.1 200 OK Content-Type: application/json
<pre>[{ "companyForm": "OY", "schemaVersions": [{ "schemaVersion": "oytp_gaap_ind_2025-10-16", "entryPointURI": "http://www.valtiokonttori.fi/fi/fr/xbnl/crr/fws/oytp/kpl-2016-12/2025-10-16/mod/oytp_gaap_ind.xsd" }, { "schemaVersion": "oytp_gaap_con_2025-10-16", "entryPointURI": "http://www.valtiokonttori.fi/fi/fr/xbnl/crr/fws/oytp/kpl-2016-12/2025-10-16/mod/oytp_gaap_con.xsd" }] }, { "companyForm": "OYJ", "schemaVersions": [{ "schemaVersion": "ESEF-2025", "entryPointURI": "https://www.esma.europa.eu/taxonomy/2025-03-27/esef_cor.xsd" }] }]</pre>

- Query was successful
- **Note: this is only a simplified example response, not an up-to-date list of supported taxonomies.**

4.5.1.2 Error responses

The service only returns error responses that are common to all services, see [Error responses common to all services](#).

4.6 Error responses common to all services

There are error responses common to all API services (excluding [Authentication](#)) and these responses can be returned when any of the services is called.

There are error responses common to the services. These responses are returned with HTTP status 400 Bad Request and the error response is always in the following format:

HTTP/1.1 400 Bad Request Content-Type: application/json
<pre>{ "detail": [{ "loc": "<location of error>", "msgEn": "<error in English>", "msgFi": "<error in Finnish>", "msgSv": "<error in Swedish>", "type": "string" }] }</pre>

The Bad Request error responses common to the services are described below:

Error description	Error location	Error message in Finnish	Resending
No HTTP header <i>Authorization</i> is given in the call	headers	The header 'Authorization' is missing from the call	The missing HTTP header <i>Authorization</i> must be added to the call before resending
The value of the HTTP header <i>Authorization</i> given in the call is not in valid format	headers	Invalid value entered for 'Authorization'	The value of the HTTP header <i>Authorization</i> given in the call must be corrected before resending

The rest of the error responses common to the services are such that no specific error messages are returned to them, only the HTTP status describing the situation. These error responses common to the services are described below:

Error description	HTTP status	Resending
The access token given in the call is invalid or has expired	401 Unauthorized	Before resending, the customer must reauthenticate itself and replace the expired or invalid access token with a new one
The access token used does not have sufficient rights to call the service	403 Forbidden	Before resending, the user must be changed or the user's authorisations must be corrected
The client software has made too many calls to the service within a certain time window and for this reason, rate limiting is applied	429 Too Many Requests	Resending can be made in a few moments (for example, in a few seconds)

Other call processing error that is of unexpected nature	500 Internal Server Error	You may try to resend the reports
--	---------------------------	-----------------------------------

5 Taxonomies

An up-to-date list of the taxonomy versions and company forms supported by XBRL API v3 can be accessed by calling the service [Supported taxonomies and company forms](#) or by visiting the [PRH website](#).

6 Appendices

API description

xbrlapi_v3_20260909.html

- The API description is a file that has been translated from the RAML description to a visual HTML file. The API description describes the reception API services with easy-to-approach graphical presentation and examples and provides a quick overview of the way in which the API functions.

RAML description

xbrlapi_v3_raml-package_20260909.zip

- The RAML description contains detailed technical documentation of the API in the RAML description language. The description is distributed from this document as an external package to entities developing applications utilising the API.