

CESOP

Data Submission Specifications Document

Date: 29/01/2024

Version: 1

Table of Contents

DOCUMENT CONTROL INFORMATION	ERROR! BOOKMARK NOT DEFINED.
TABLE OF CONTENTS	ii
01. INTRODUCTION	3
01.1 PROJECT BACKGROUND	3
01.2 SCOPE OF PROJECT	3
01.3 TERMINOLOGY	3
02. DESIGN CONSIDERATIONS	5
02.1 ASSUMPTIONS AND DEPENDENCIES	5
02.2 CONSTRAINTS	5
02.3 OPERATING ENVIRONMENT	5
DESIGN	6
02.4 AUTHENTICATION	6
02.5 WEBSERVICE	6
02.6 DATA DICTIONARY	7
APPENDIX A – SWAGGER – WEBSERVICE SPECIFICATIONS	8
APPENDIX B – HOW TO GET TOKEN FOR TESTS	11
APPENDIX C – CORRECTION MECHANISMS	12
02.1 TS - CORRELATION AND CORRECTION MECHANISM	12
02.1.1 Correlation and correction mechanism	12
02.1.1.1 Correlation between a Payment Data message and a Validation Result message	12
02.1.1.2 Correlation between two Payment Data messages	14
02.1.2 Precision about the MessageTypeIndic and DocTypeIndic elements	17
APPENDIX D – HIGH LEVEL SCHEMA	19

01. Introduction

01.1 Project Background

On 18 February 2020, the Council adopted a legislative package to request payment service providers to transmit information on cross-border payments originating from Member States and on the beneficiary (“the payee”) of these cross-border payments. Under this package, payment service providers offering payment services in the EU will have to monitor the payees of cross-border payments and transmit information on those who receive more than 25 cross-border payments per quarter to the administrations of the Member States.

This information will then be centralised in a European database, the Central Electronic System of Payment information (CESOP) where it will be stored, aggregated and cross-checked with other European databases. All information in CESOP will then be made available to anti-fraud experts of Member States via a network called Eurofisc.

The objective of this new measure is to give tax authorities of the Member States the right instruments to detect possible e-commerce VAT fraud carried out by sellers established in another Member State or in a non-EU country.

01.2 Scope of Project

Operators will be integrating through a web service to be able to send and amend CESOP reports. This project will focus on the system-to-system interface and the relevant technical specifications to aid PSP technical teams develop the required IT infrastructure to integrate with this service.

01.3 Terminology

The technical and business terms used in this document shall be interpreted in line with the definitions set out within Subsidiary Legislation 406.22 Value Added Tax (Reporting Obligations For Payment Service Providers) Regulations, and the following:

Term	Definition
Submit/submission	The expression submit/submission is used for information exchange between the PSPs and MS TAX administrations. As this exchange relates to external/national domain, this document does not define the means of this information exchange.
Transmit/transmission	The expression transmit/transmission is used for information exchange between the MS TAX administrations and the CESOP system. This transmission may imply different means of transport, like physical upload of file to CESOP system or system-to-system exchange of information.
XSD (XML Schema Definition)	XSD (XML Schema Definition) is a World Wide Web Consortium (W3C) recommendation that specifies how to formally describe the elements in an Extensible Markup Language (XML) document. This description can be used

Term	Definition
	to verify that each item of content in a document adheres to the description of the element in which the content is to be placed.

02. Design Considerations

02.1 Assumptions and Dependencies

It is assumed that the Payment Service provider systems are already in place to be able to generate the required data to be passed to the CESOP - S2S web service in the correct format (XML).

It is assumed that this web service will not provide a front-end interface, integrating system will have to provide their own front-end interface.

02.2 Constraints

The S2S web service will be limited to the functionality required by CESOP reporting exchange.

CESOP file size should be limited to a size of 1GB

02.3 Operating Environment

The web services provided are built using a Rest webservice architecture with XML as the accepted data formats.

Design

02.4 Authentication

For testing purposes all interested PSPs will be required to send an email to cesop.mtca@gov.mt requesting specifications on Authentication/Authorization mechanisms.

02.5 Webservice

The web service will provide the following methods:

The web service can be accessed through the following endpoint URI:

Test - PGS: <https://cesopsubmission-dwe-app.azurewebsites.net/swagger/index.html>

Test Token:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJpbmtpbmUgSldUIEJ1aWxkZXIiLCJpYXQiOiJlMjUyNDkwNzgsImV4cCI6MTczNzE4NTA4MCwiYXVkIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NTg5NDUiLCJzdWIiOiJ0ZXN0QHRlc3QuY29tIiwicnBvSWQiOiIxMjMiLCJ0YXhSZWYiOiIxMjMifQ.LC2W9x04UvjXS7BTJrwfT5i5I2-2NUucjHa0IOJGAz8
```

Name	/File/PaymentDataMsg
Method	POST
Description	This endpoint is used to upload a NEW/Update/Delete file. It requires the 'year' query parameter, and the file as part of the request body.
Request parameters	year: The year to which this data pertains. It is of type integer and required.
Request body	file: The file to upload, in xml format.
Response	201: File created successfully. Returns the ID of the newly created file.

Name	/File/NoPaymentDataMsg
Method	POST
Description	This endpoint is used to upload an empty file. It requires the 'year' query parameter, and the file as part of the request body.
Request parameters	year: The year to which this data pertains. It is of type integer and required.
Request body	file: The file to upload, in xml format.
Response	201: File created successfully. Returns the ID of the newly created file.

Name	/File/StatusMsg/{id}
Method	GET
Description	This endpoint retrieves the status of a file by its ID.
Request parameters	id: The ID of the file to retrieve. It is of type string (format: UUID) and required.
Request body	N/A
Response	200: Success. Returns the status of the file.

02.6 Data Dictionary

A data dictionary will be distributed as a separate file with this document to serve as a supporting document - CESOP - XSD User Guide-v4.61.docx.

Or can be accessed through EU commission site: https://taxation-customs.ec.europa.eu/taxation-1/central-electronic-system-payment-information-cesop_en

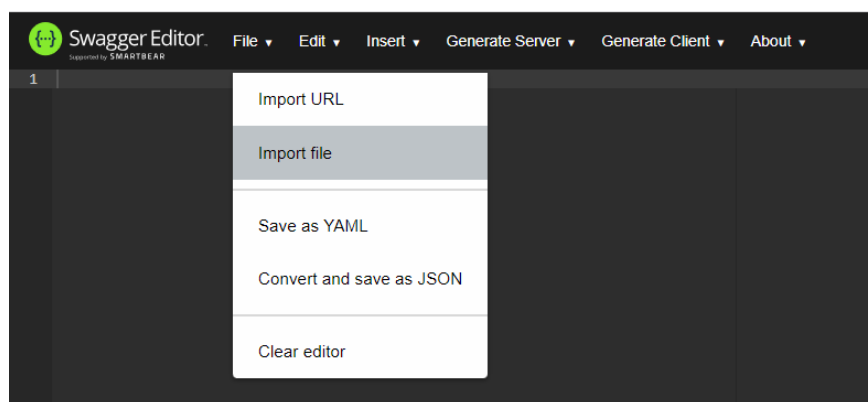
For more information on CESOP: https://taxation-customs.ec.europa.eu/taxation-1/central-electronic-system-payment-information-cesop_en

Introduction

In this document, we will walk through how to use the Swagger UI to interact with the "AEOI – CESOP Data Exchange API".

Accessing Swagger UI

CESOP StoS specifications and try me feature can be accessed through Swagger Editor which can be accessed from: <https://editor.swagger.io/>



From the File – Import File, search for CESOP Yaml file (YAML file is going to be made available through CFR portal) or through the PGS URI (Listed above). Once loaded Swagger will provide all the methods of the service:

You should be presented with a webpage that resembles this:

Navigating the Swagger UI

On the Swagger UI page, you'll notice a section containing the API endpoints. In the CESOP StoS we have the following - `Example` and `File` endpoints. These are collapsible sections and once clicked the section is expand and more detailed documentation is made available.

File

POST	/File/PaymentDataMsg Uploads a file	🔒	▼
POST	/File/NoPaymentDataMsg Uploads a empty file	🔒	▼
GET	/File/StatusMsg/{id} Get the status of a file by id	🔒	▼

In each section, you will see several rows, each representing a different API endpoint. An API endpoint is a specific URL where your API can access the resources it needs. Each endpoint in Swagger UI is described in a few parts:

HTTP method:	This is the type of HTTP request. There are four methods in our Swagger.json: GET, POST, PUT, and DELETE.
Endpoint path:	This is the last segment of the URL for a specific resource.
Summary:	A short description of what the endpoint does.
Tags:	These are general labels that help to organize the endpoints.
Responses:	Possible responses that the endpoint will return.

Using an Endpoint

After expanding a section, you can try out any endpoint by clicking the "Try it out" button on the right, changing any relevant parameters, and then clicking "Execute".

File

POST	/File/PaymentDataMsg Uploads a file	🔒	^
Parameters		Try it out	
Name	Description		
year	Year		
integer(\$int32)	year		
<i>(query)</i>			
Request body		multipart/form-data ▼	

To demonstrate this, we will use the POST endpoint under the `File` section.

1. Expand the `File` section by clicking on it.
2. Click on the POST method row. You will see detailed information about this endpoint, such as its parameters and responses.
3. Click the "Try it out" button on the right. This allows you to fill in any parameters that the endpoint requires.
4. In the "requestBody" section, click "Browse" to select a file from your computer to upload.
5. After filling in all the necessary parameters, click the "Execute" button. This sends a request to the API.

Viewing the Server Response

After clicking "Execute", the server response will appear in the "Responses" section of the endpoint documentation.

Here, you can see the HTTP response code, headers, and body. A successful file upload would have a response code of 200 or 201 and return the ID of the newly created file.

For further help on Swagger please refer to the official Swagger UI documentation:

<https://swagger.io/tools/swagger-ui/>

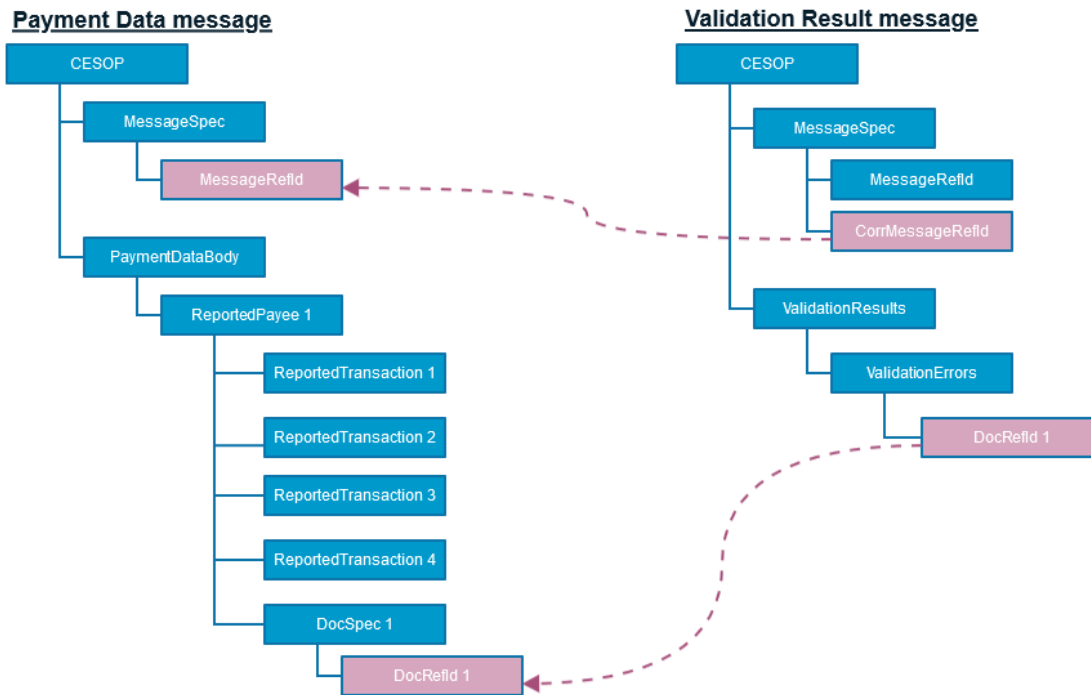
Appendix B – How to get token for tests

Test Tokens are going to be provided by MTCA to interested platform operators to be used with the test StoS service.

Production Tokens are to be generated by the PSP through the MTCA portal following a valid registration.

Appendix C – Correction Mechanisms

02.1 TS - Correlation and correction mechanism



02.1.1 Correlation and correction mechanism

02.1.1.1 Correlation between a Payment Data message and a Validation Result message

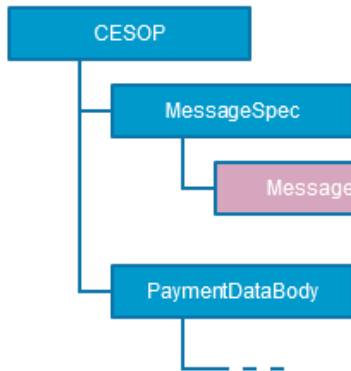
Main principles:

- **MessageRefId** must be unique and different for each and every message.
- **CorrMessageRefId** of the Validation Result message always equals to the **MessageRefId** of the related Payment Data message, whatever is the validation result (positive or negative).

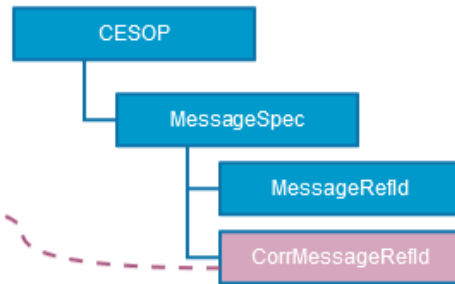
02.1.1.1.1 Correlation rules in case of error at message or reporting PSP level

- In case of error at message level or at reporting PSP level, the underlying Reported Payees and related transactions will not be evaluated.

Payment Data message



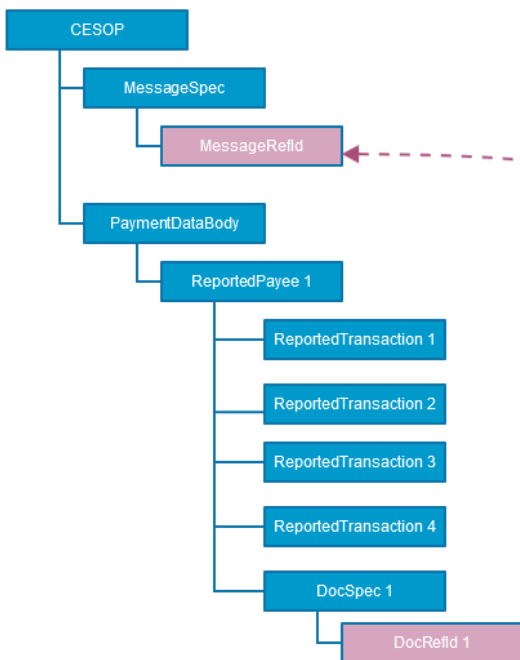
Validation Result message



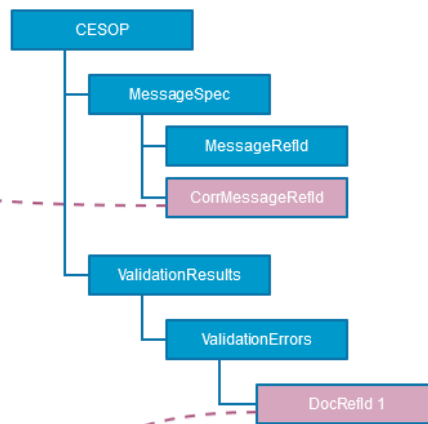
02.1.1.1.2 Correlation rules in case of error at Reported Payee level

- In case of error at Reported Payee level, the whole Reported Payee will be rejected. The underlying transactions will not be evaluated;
- DocRefId of the Validation Result message equals DocRefId of the related Reported Payee in the correlated Payment Data message.

Payment Data message



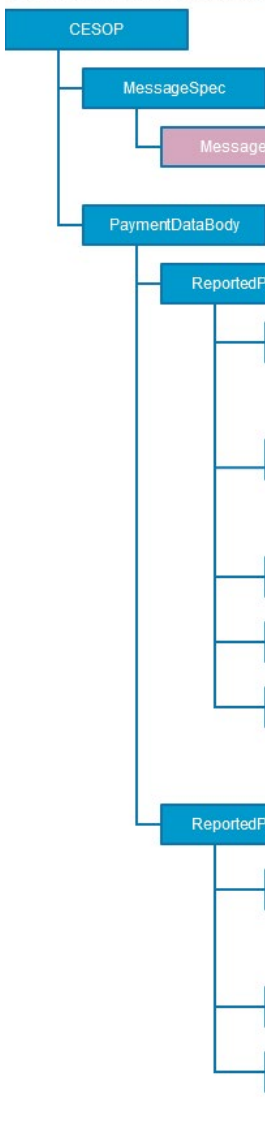
Validation Result message



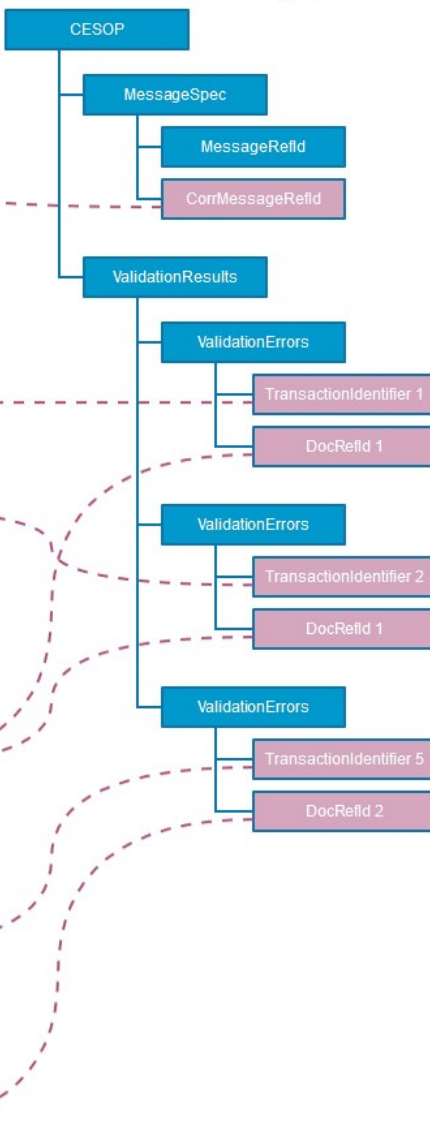
02.1.1.1.3 Correlation rules in case of error at Reported Transaction level

- In case of error at Transaction level, DocRefId of the Validation Result message equals DocRefId of the related Payee in the Payment Data message;
- TransactionIdentifier of the Validation Result message equals TransactionIdentifier of the related transaction in the Payment Data message.

Payment Data message



Validation Result message



02.1.1.2 Correlation between two Payment Data messages

The correction mechanism is applicable only at message level or Reported Payee level.

- In case of error at message level, the whole Payment Data message will be rejected by CESOP. Technically, this means the whole Payment Data message must be resubmitted, including all transactions of all payees.
- In case of error at Payee or Transaction level, only the erroneous Payee(s) will be rejected by CESOP. The other one(s) will be ingested. Technically, this means the correction message will only contain the Payee(s) to be corrected.

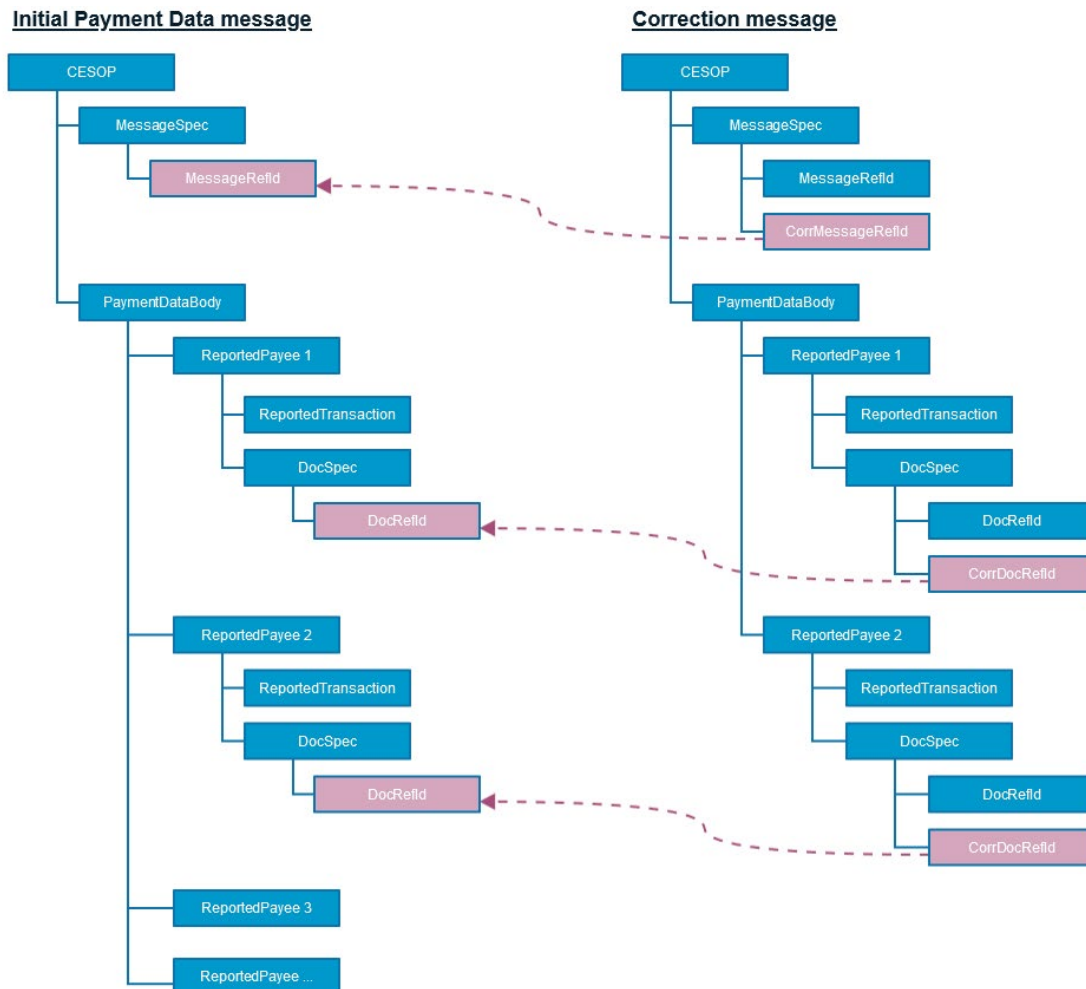
The way to populate CorrMessageRefId and CorrDocRefId can be synthesized as following :

- CorrMessageRefId must always refer to MessageRefId of the last Payment Data message which was not fully rejected (meaning in which at least one Payee has been positively validated and recorded in the CESOP data store);
- CorrDocRefId must always refer to the DocRefId of the rejected Payee, in the correlated Payment Data message.

02.1.1.2.1 First correction of a Payment Data message

In this case the correlation rule is simple:

- The CorrMessageRefId of the correction refers to the MessageRefId of the initial Payment Data message
- The CorrDocRefId's of the corrected Payees refer to the DocRefId's of the related Payees in the initial Payment Data message



02.1.1.2.2 Two successive corrections at Payee level

It is supposed here that the Initial Payment Data message is not fully rejected, meaning that at least one Reported Payee is valid.

Here two different cases could occur:

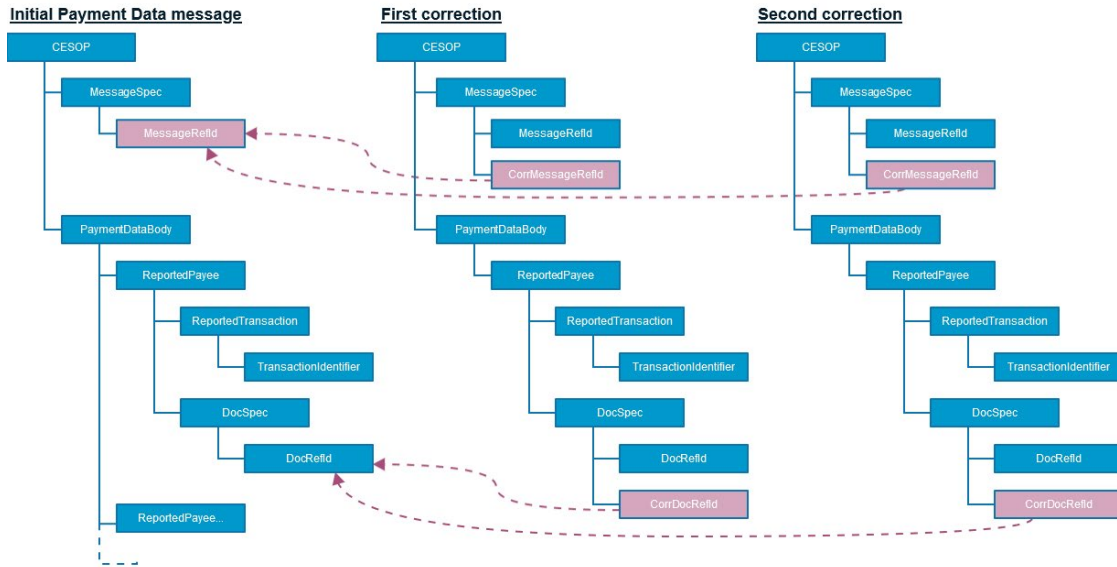
1. The first correction is fully rejected (new error at message level, or at PSP level, or all corrected Payees are still erroneous);
2. The first correction is partially positively validated (at least one Payee has been well corrected, but not all of them).

02.1.1.2.2.1 First correction is fully rejected

In the following example, the considered Payee is erroneous in the Initial Payment Data message, and still not correct in the first correction.

By consequence, the first correction will be fully rejected (no Payee being validated).

In this case, the second correction must refer to the last message where at least one Payee has been validated, so here the initial submission.

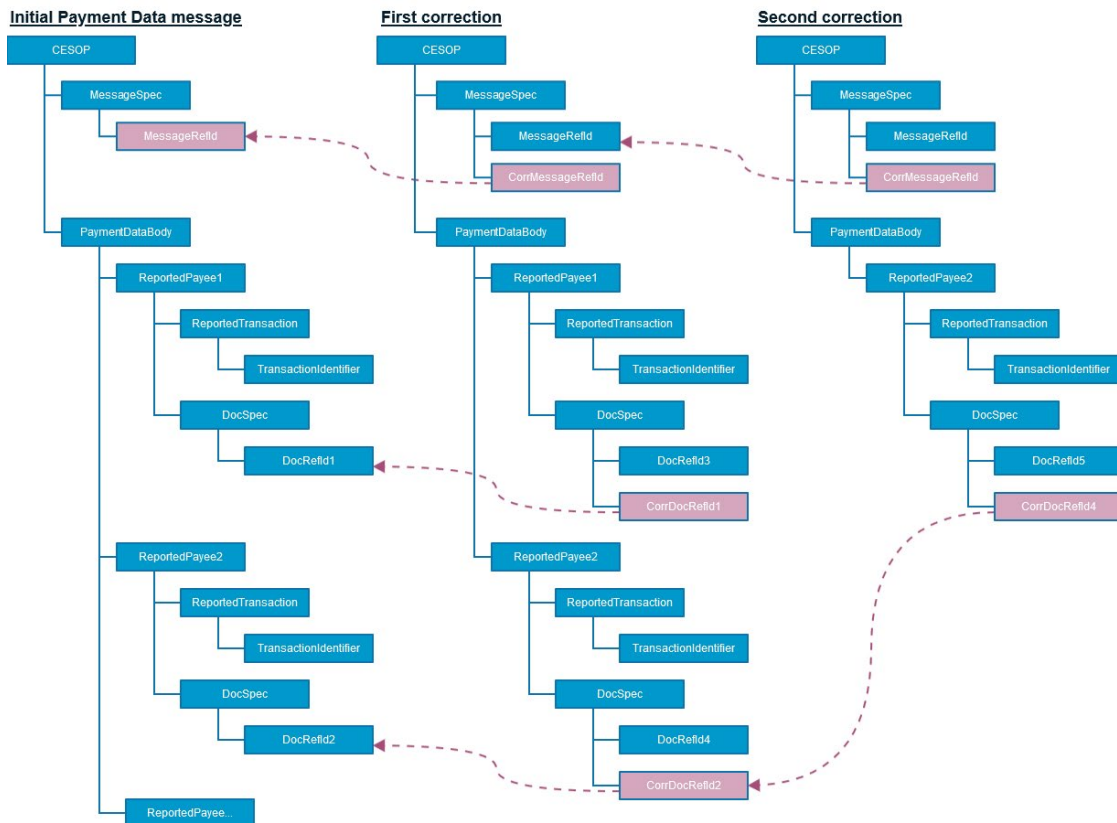


02.1.1.2.2.2 First correction is partially validated

In the following example, two Payees are erroneous (called here after respectively "ReportedPayee1" and "ReportedPayee2").

In the first correction, only one of them will be positively validated ("ReportedPayee1"), the second one ("ReportedPayee2") being rejected.

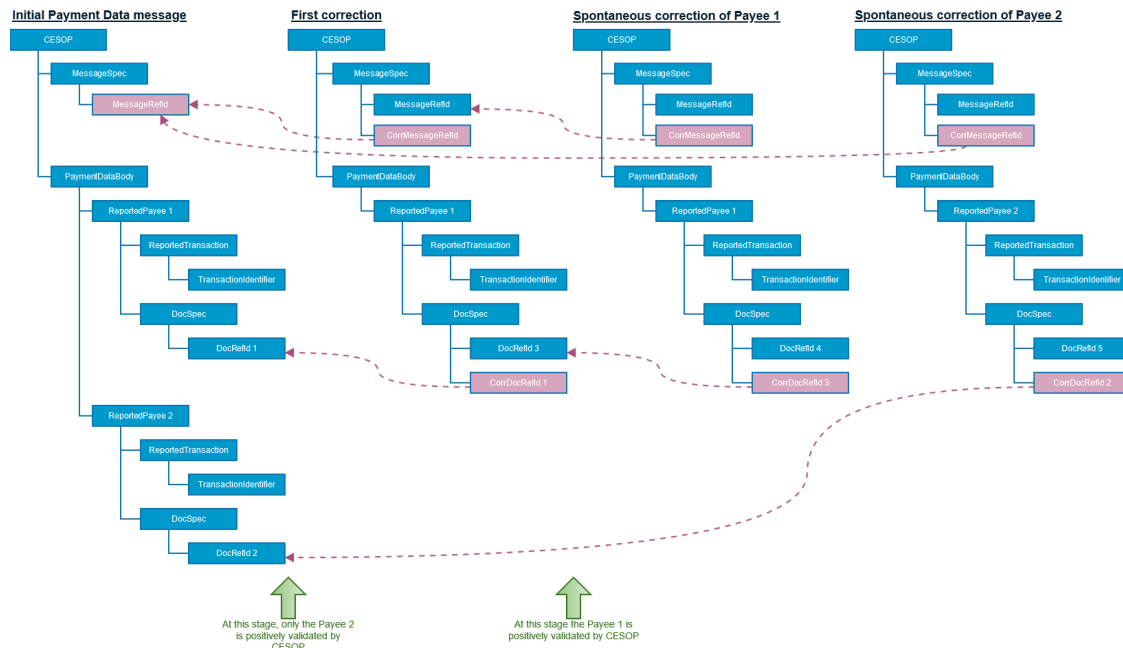
As the first correction is not fully rejected, the second one shall refer to the first correction.



02.1.1.2.3 Spontaneous correction of a previously validated Payee

Based on the previous examples, the following schema depicts two spontaneous corrections:

- One related to a Payee (ReportedPayee 1) that has already been corrected.
 - In that case, the spontaneous correction must refer to the message in which the Payee has been validated, so the 'first correction'
- One related to a Payee (ReportedPayee 2) that has been positively validated by CESOP at the initial submission of the Payment Data message;
 - In that case, the spontaneous correction must refer to the initial submission



02.1.2 Precision about the MessageTypeIndic and DocTypeIndic elements

The [MessageTypeIndic](#) element declares if the message contains new data, correction/deletion for previously sent data, or there is no data to report:

- **CESOP100:** The message contains new data.
 - This case is only applicable to the initial Payment Data message or to a spontaneous submission of omitted data;
- **CESOP101:** The message contains corrections or deletions of previously sent data.
 - This value can only be used in a correction message (spontaneous or not) or in a deletion message;
- **CESOP102:** The message indicates there is no data to report.

The correction mechanism uses the [DocSpec](#) element, as described above. Within this element, the [DocTypeIndic](#) element specifies the operation over the element to be corrected:

- **CESOP1:** New Data – the data was not submitted before.
 - This case is only applicable to the initial Payment Data message or to a spontaneous submission of omitted data;

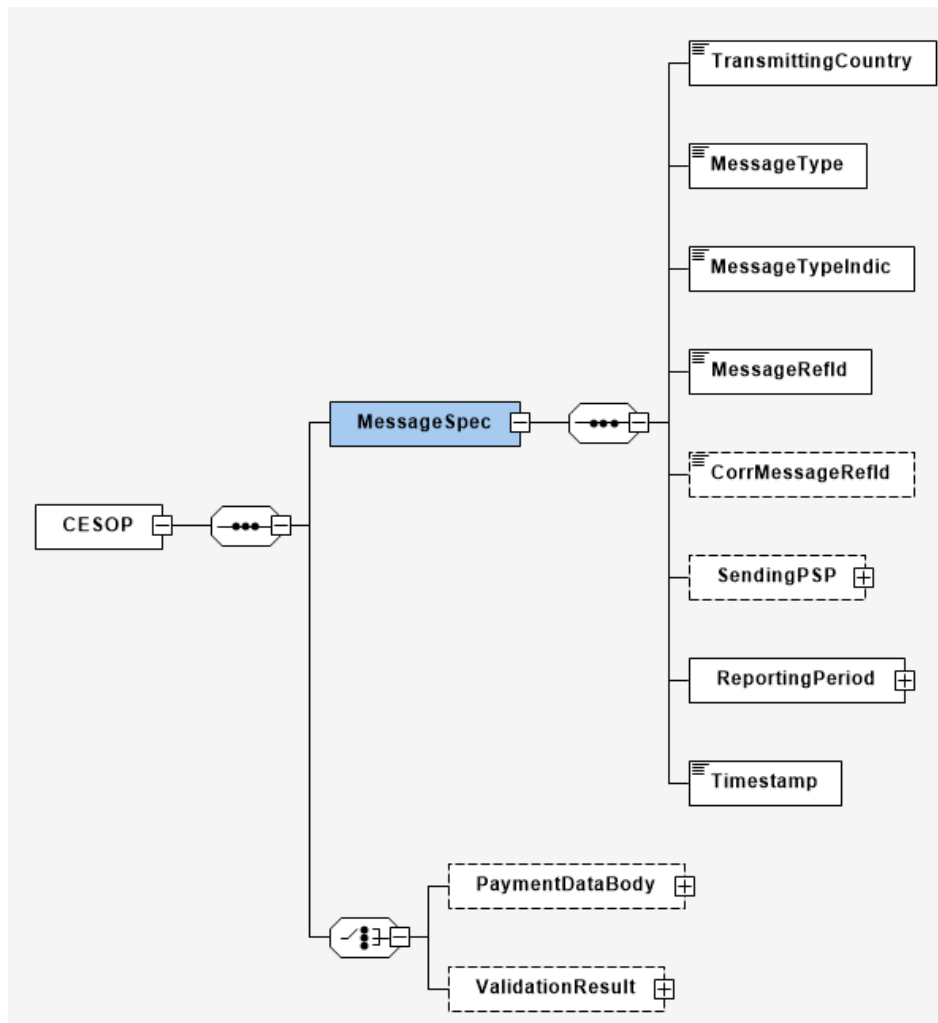
- **CESOP2:** Corrected Data – the element to be corrected must be replaced with the corrected data.
 - This value can only be used in a correction message (spontaneous or not);

- **CESOP3:** Deletion of Data – some data to be corrected, which was submitted before, was not correct and has to be deleted.
 - This is only applicable if the related Payee has been previously validated.

The possible combinations are the following:

<u>MessageTypeIndic</u>	<u>DocTypeIndic</u>
CESOP100	CESOP1
CESOP101	CESOP2 CESOP3
CESOP102	n/a

Appendix D – High level Schema



The XSD, can be referenced in the CFR portal with relevant Schema User Guide which provides a comprehensive description of the schema data elements and data dictionary.

XSD:

Description	Filename
Payment data	PaymentData.xsd
Common types	Commontypes.xsd
ISO types	Isotypes.xsd

Schema User guide:

CESOP - XSD User Guide-v4.61.docx