User Guide for the preparation and encryption of files for transmission through the CTS v2.0

(Revised Version – March 2024)

I. Introduction

1. The explanations in this user guide are provided using a fictitious ABC schema as an example for demonstration purposes, but the same principles will apply for all the message types (CRS, CbC, ETR, exchange on request, TRACE, MDR, etc.), using the CTS for transmissions (please see the complete list of message types on page 4).

2. For example, in the context of the CRS schema:

– The term “ABC schema” would refer to the CRS schema

– The term “ABC message” or “ABC XML file” would refer to a CRS message (the CRS XML file which has been produced using the CRS XML schema)

– The term “ABC Status Message” would refer to the “CRS Status Message”. This will be the CRS Status Message XML file which has been produced using the CRS Status Message XML schema. For most Status messages, except the CRS, CbC and ETR Schemas, the Generic Status Message will be used. For more information, please consult the Generic Status Message user guide.

Terminology

Term	Definition
Status Message	The ABC Status Message allows reporting file errors and record errors found on the previously transmitted ABC Message.
XML validation	XML validation allows validating the ABC XML data file against the ABC XML Schema.
Additional validation	Additional validation allows providing additional checks that are not performed by the XML validation. Additional validations include both file validations and record validations.
File validation	File validation verifies if the XML file can be opened, read and validated. When file validation is successful, the record validation can be performed. Examples of file validation: Failed download, decrypt, decompress, check signature, found viruses or threats , failed XML Validation, etc.
Record validation	Record validation provides additional validation of the data (which are not already validated by the XML Schema itself). Examples of record validation: An invalid Account Number, a missing field, a missing DocRefID (for corrections).
File error	A file error report allows reporting that an ABC XML file has failed the file validation.
Record error	A record error report allows reporting that an XML file has failed the record validation.
Record	The term record refers to the correctable records (ex: Account Report and Reporting FI for the CRS XML Schema). The correctable records contain a DocSpec (and a DocRefID), thus allowing for future corrections.
CTS	The Common Transmission System developed under the auspices of the Forum on Tax Administration and operated within the framework the Global Forum.

II. Step-by-step guide on file preparation for the CTS

Introduction

3. The explanations in the step-by-step guide are provided using the fictitious ABC schema as an example for demonstration purposes, but the same principles apply for all the message types to be sent through the CTS. Wherever ABC appears in the example file naming conventions or CTS metadata content in this guide, the respective relevant message type code should be used. The message types code are defined in the Section “Message types in the Metadata schema v2.0”. It is also highly recommended to rely on the file preparation rules set out in this document for transmissions through channels other than the CTS.

4. This section describes how to prepare a CTS data file. For the preparation of a file for transmission through the CTS, it is mandatory to have a valid EVSSL certificate from a CTS-approved certificate authority[1]. The updated list of authorised Certificate Authorities and products can be accessed at http://community.oecd.org/docs/DOC-117999https://community.oecd.org/docs/DOC-126787.

5. The following certificate authorities are authorized for use for CTS transmission encryption:

Certificate Authority	Type of Certificate
DigiCert	Extended Validation (not code signing)
Entrust	Extended Validation (not code signing)
Thawte	Extended Validation (not code signing)
GlobalSign	Extended Validation (not code signing)
Sectigo	Extended Validation (not code signing)
Network Solutions	Extended Validation (not code signing)
SecureTrust	Extended Validation (not code signing)
QuoVadis	Extended Validation (not code signing)
Actalis	Extended Validation (not code signing)

6. The narrative description of the file preparation process in this section reflects the approach applied in the CTS File Preparation code sample. This code sample can be accessed through: CTS 2.0 FilePrep Application

Message types in the Metadata schema v2.0

7. The below list sets out the Message Types included in the Metadata schema v2.0. Only the codes listed below can be used for:

– the file naming convention (see below)

– the Metadata.CTSCommunicationTypeCd element

– the CommunicationType specified in the SenderFileID format

Description	**Code**
CRS	CRS
CbC	CBC
ETR	ETR
DTC AEOI	DTCAEOI
MDR	MDR
FHTP NoNom exchanges	NTJ
CRS Data Quality	CDQ
DPI Model Rules	DPI
EOIR free format – Direct Tax	EOIRFreeDT
EOIR free format – Indirect Tax	EOIRFreeIT
EOIR free format – Tax collection and recovery	EOIRFreeTCR
EOIR structured format (e-forms) – Direct Tax	EOIRStructDT
EOIR structured format (e-forms) – Indirect Tax	EOIRStructIT
EOIR structured format (e-forms) – Tax collection and recovery	EOIRStructTCR
Spontaneous exchanges free format – Direct Tax	SponFreeDT
Spontaneous exchanges free format – Indirect Tax	SponFreeIT

[1] It should be noted that, in the process of obtaining a PKI certificate (such as an EVSSL certificate) from a certificate authority, the private key must be generated by the certificate requester and kept securely. When requesting a certificate from a certificate authority, only the public key is shared in the CSR (Certificate Signing Request).

Spontaneous exchanges free format – Tax collection and recovery	SponFreeTCR
Spontaneous exchanges structured format (e-forms) – Direct Tax	SponStructDT
Spontaneous exchanges structured format (e-forms) – Indirect Tax	SponStructIT
Spontaneous exchanges structured format (e-forms) – Tax collection and recovery	SponStructTCR
Joint Audits	JointAudits
JITSIC	JITSIC
MAP	MAP
TRACE	TRACE
Other exchanges under international tax agreements	Other
CRS Status message	CRSStatus
CbC Status message	CBCStatus
ETR Status message	ETRStatus
DTC AEOI Status message	DTCAEOIStatus
MDR Status message	MDRStatus
FHTP NoNom exchanges Status message	NTJStatus
CRS Data Quality Status message	CDQStatus
DPI economy Status message	DPIStatus
EOIR free format – Direct Tax Status message	EOIRFreeDTStatus
EOIR free format – Indirect Tax Status message	EOIRFreeITStatus
EOIR free format – Tax collection and recovery Status message	EOIRFreeTCRStatus
EOIR structured format (e-forms) – Direct Tax Status message	EOIRStructDTStatus
EOIR structured format (e-forms) – Indirect Tax Status message	EOIRStructITStatus
EOIR structured format (e-forms) – Tax collection and recovery Status message	EOIRStructTCRStatus
Spontaneous exchanges free format – Direct Tax Status message	SponFreeDTStatus
Spontaneous exchanges free format – Indirect Tax Status message	SponFreeITStatus
Spontaneous exchanges free format – Tax collection and recovery Status message	SponFreeTCRStatus
Spontaneous exchanges structured format (e-forms) – Direct Tax Status message	SponStructDTStatus
Spontaneous exchanges structured format (e-forms) – Indirect Tax Status message	SponStructITStatus
Spontaneous exchanges structured format (e-forms) – Tax collection and recovery Status message	SponStructTCRStatus
Joint Audits Status message	JointAuditsStatus
JITSIC Status message	JITSICStatus
MAP Status message	MAPStatus
TRACE Status message	TRACEStatus
Other exchanges under international tax agreements Status message	OtherStatus

Prerequisites for the file preparation process

File Naming Convention

8. CTS file names will use the Country Code to identify the Sending Competent Authority and the Message type code (see the list of allowed codes in the Section "Message types in the Metadata schema v2.0") to identify the type of information exchange.

9. For an ABC message, the file names are as follows:

File Name	Description
CountryCodeSender_ABC_Payload	Encrypted payload using a randomly generated one-time use key
CountryCodeReceiver_ABC_Key	Key encrypted using the public key of the Receiving Competent Authority
CountryCodeSender_ABC_Metadata.xml	CTS Metadata to ensure that the Receiving Competent Authority properly processes the XML reports. The Metadata

	file is not encrypted.
CountryCodeSender_ABC_UTC.zip	Complete transmission file to be sent to the CTS. This Zip file will contain the 3 files listed above, i.e.: – CountryCodeSender_ABC_Payload – CountryCodeReceiver_ABC_Key – CountryCodeSender_ABC_Metadata.xml

10. The CountryCodeSender is the Country code of the Sending Competent Authority sending the file, and CountryCodeReceiver is the Country code of the Receiving Competent Authority. The Country codes used must be same as the respective Country Codes in CTS Metadata Schema, which uses the 2-character alphabetic country code and country name list based on the ISO 3166-1 Alpha 2 standard.

– The country codes enumerated in version 1.0.1 of the CTS metadata isoctstypes xsd include, in addition to country codes, ten codes dedicated for testing purposes: QM, QN, QO, QP, QQ, QR, QS, QT, QU, QV (and their unique CTS metadata .00 counterparts, see the relevant clause below). These are codes dedicated in the ISO 3166-1 Alpha 2 standard for user-assigned functions. In the CTS Conformance testing environment, it is possible for interested Competent Authorities to temporarily enrol as one of these country codes, in addition to the Competent Authority's own country code, by contacting the OECD CTS Secretariat, for the purpose of testing transmissions exchanges end-to-end (i.e.: controlling both the sending Competent Authority and the receiving Competent Authority at the same time). In the context of this particular type of testing, it is possible to send transmissions on the CTS to and from these dedicated country codes. To note, these special codes are only to be used for the CTS Metadata Schema and the file naming, but not in the substantive XML Schema.

– Countries using the regional hub for CTS transmissions may want to also be able to receive and/or send files directly. In these instances, the Country Code may need to be followed by a dot and two zeros (.00) for transmissions that do not follow the country's chosen default transmission path. The .00 is only to be used for the CTS Metadata Schema and the file naming, but not in the substantive XML Schema.

Transmission prerequisites

11. Prior to starting the file preparation process, the following prerequisites must be in place:

– Obtain a digital certificate from an approved Certificate Authority (see above).

– Complete a valid enrollment in the CTS.

– Ensure the file does not contain any file validation errors (XML validation, virus, threats, etc.). A list of file validation errors is set out in Annex I.

– Ensure the file does not contain any record validation errors. The record validation errors can be found in the relevant Status Message User Guides (Generic, CRS, CbC and ETR, respectively).

– Ensure that, whenever possible, in the case of bulk information (e.g. CRS, CbC), the data is sorted and aggregated by receiving jurisdiction.

– Ensure that the following best practices are followed regarding the namespaces declaration and prefixes:

– Ensure that the payload and metadata file have the correct namespace declaration.

– Ensure that the xml namespace is declared only at the root element of the unsigned payload file and the metadata file.

– Ensure that all XML elements have prefixes and do not use default namespaces.

– The different namespaces and prefixes can be found in the different user guides found on the CTS ONE Community.

– XSD location is optional, as jurisdictions will have different locations for the different XSD files.

– Ensure the file meets the agreed file size limitations. The CTS allows files of up to 250 MB compressed (ZIP package containing the compressed and encrypted payload, the encrypted key, and the metadata file). However, as a business rule, it is agreed that Competent Authorities will limit the file size for the XML payload to 100 MB (uncompressed), unless they bilaterally agree on a different payload size limitation, within the CTS transmission limit of 250 MB.

XML Schema Best Practices

12. All XML files to be transmitted through the CTS should conform to the following best practices for XML schemas. Certain characters are prohibited and, if included, will cause the file to be rejected for transmission.

Entity Reference

13. If an XML file contains one or more of these characters, these should be replaced by the following predefined entity references to conform to XML schema best practices.

Character	Description	Entity Reference
&	Ampersand	&amp;
<	Less Than	&lt;

Optional Entity Reference

14. If an XML file contains one or more of these characters, their presence will not cause a file error. The characters should, however, be replaced by the following predefined entity references to conform to XML schema best practices.

Character	Description	Entity Reference
>	Greater Than	&gt;
'	Apostrophe	&apos;
"	Quotation Mark	&quot;

SQL Injection Validation

15. If an XML document contains one of these combinations of characters, the data packet will be rejected and a failed threat detection (error) notification will be generated. These combinations of characters are not allowed. To prevent file errors, please do not include any of these combinations of characters in the payload or the signature of the packet.

Character	Description	Entity Reference
--	Double Dash	N/A
/*	Slash Asterisk	N/A
&#	Ampersand Hash	N/A

The steps for preparing a file for CTS transmission

Steps	Process	File Naming Convention
---	Obtain a digital certificate from an approved Certificate Authority (CA).	Not applicable
1	Create the XML file	Not applicable
2	Digitally sign the payload file	CountryCodeSender_ABC_Payload.xml
3	Compress the ABC XML file with compatible zip utility	CountryCodeSender_ABC_Payload.zip
4	Encrypt the ABC XML file with AES-256 key. Please note that the file does not have a file extension.	CountryCodeSender_ABC_Payload
5	Encrypt AES key and IV with the public key of the recipient	CountryCodeReceiver_ABC_Key
6	Create Sending Competent Authority metadata	CountryCodeSender_ABC_Metadata.xml
7	Create the transmission file	CountryCodeSender_ABC_UTC.zip
8	Transmit the data packet to CTS and receive delivery confirmation	Not applicable

Step 1 – Create the XML File

16. As a first step, the Sending Competent Authority should create the relevant XML file for transmission. Where a structured XML schema is available, for example for CRS, CbC, ETR, MDR or TRACE transmissions, the file should be created by using the relevant XML schema.

17. In the case of bulk information (e.g. CRS, CbC), the information should, whenever possible, be sorted and aggregated by jurisdiction. For example, information should, whenever possible, not be sent separately with respect to each Reporting Financial Institution (for the CRS) or each Reporting Entity (for CbC). Corrections of previously sent data are expected to be transmitted periodically, for example every six months, and should be sorted and aggregated by jurisdiction as well.

18. For the exchange of non-XML files (including PDF-files, TXT-files and JPG-images), for instance as part of the documentation provided for an exchange of information request the CTS Wrapper can be used. The purpose of the CTS Wrapper is to package the non-XML files in an XML format, so that they can be exchanged through the CTS. The User Guide for the CTS Wrapper is included in Annex III to this Guide.

Step 2 – Digitally sign the XML File

19. Digital signatures are used to assure data integrity, which means that the messages are not altered in transmission through the CTS. The Receiving Competent Authority can verify that the received message is identical to the sent message. A Sending Competent Authority uses its private key to digitally sign the message.

20. The Sending Competent Authorities will ensure that the file was not corrupted during compression or encryption, and Receiving Competent Authorities will ensure that the file was not corrupted during decryption or altered during transmission through the CTS.

Step: **2 - Sign the XML File**

File Naming Convention: **CountryCodeSender_ABC_Payload.xml**

Step description:

Prepare the data using XML element prefixes. Do not use the default namespaces.

To generate the digital signature[2], the XML file is processed by a "one-way hashing" algorithm to generate a fixed length message digest.

Depending on the tool used to perform the digital signature, a different type of canonicalization method may be required. The following methods are acceptable:

- <Canonicalization Method Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
- <Canonicalization Method Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

It is required that the payload file be signed by first creating a SHA2-256[3] hash. The Sending Competent Authority will then create an RSA digital signature using the 4096-bit (or 2048-bit until 31 May 2018) private key that corresponds to the public key found in the Sending Competent Authority's digital certificate on the CTS Portal (www.cts-eoi.com/MemberInfo) or on test https://oecddataexchange.org/MemberInfo).

The transforms element should be present if any transformation is completed.

After validating the schema, digitally sign the XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition)[4] "enveloping" signature.

Use the digital signature "enveloping" type. The "enveloped and detached" types will cause failure at the destination. The file name is "CountryCodeSender_ABC_Payload.xml". The file name and extension are case sensitive and any variation in file name or format will cause failure at the destination.

Step 3 - Compress the XML File

21. The XML file "CountryCodeSender_ABC_Payload.xml" should be compressed using the deflate compression algorithm.

***Step:* 2 - Compress the XML File**

***File Naming Convention:* CountryCodeSender_ABC_Payload.zip**

Step description:

- Ensure "zip" is the file extension used by the compression tool or library.
- Ensure the file is compressed using the deflate compression algorithm.

Summary:

The file name is "CountryCodeSender_ABC_Payload.zip". The file is case sensitive and any variation in file name or format will cause the transmission to fail.

Note: The current supported compression is ZIP compression using the standard Deflate compression method.

[2] Digital Signature Standard (DSS) (FIPS 186-4), July 2013, nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[3] Secure Hash Standard (SHS) (FIPS 180-4), March 2012, csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[4] XML Signature Syntax and Processing (Second Edition), June 2008, http://www.w3.org/TR/xmldsig-core/

Step 4 - Encrypt the XML File with AES 256 Key

22. AES is one of the most secure encryption algorithms and the required encryption standard for all transmissions through the CTS. The file is encrypted to protect sensitive information.

***Step:* 4 - Encrypt the XML File with AES 256 Key**

***File Naming Convention:* CountryCodeSender_ABC_Payload**

Step description:

After compression, encrypt the file “CountryCodeSender_ABC_Payload.zip” using the AES-256 cipher with a randomly generated “one-time use” AES key.

There are several steps necessary to perform AES encryption. The following agreed settings should be used to maintain compatibility:

- Cipher Mode: CBC (Cipher Block Chaining)
- Salt: No salt value
- Initialization Vector (IV): 16 byte IV. The IV must, for the Competent Authority performing the encryption, be random and unique for every encryption.
- Key Size: 256 bits / 32 bytes – the key size should be verified. Moving the key across operating systems can affect the key size.
- Encoding: None. There can be no special encoding. The file will contain only the raw encrypted bytes.
- Padding: PKCS#7 version 1.5

The AES encrypted file name is “CountryCodeSender_ABC_Payload”. The file is case sensitive and any variation in file name or format will cause the transmission through the CTS to fail.

Additional information regarding the AES-256 encryption algorithm and keys can be found in:

- NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revision 5)
- Advanced Encryption Standard (FIPS 197), November 2001

Step 5 - Encrypt the AES Key and IV with Public Key of Receiving Competent Authority

23. The next step is to encrypt the AES key with the public key of the Receiving Competent Authority. The file is encrypted to protect the AES key.

24. All Competent Authorities enrolled in the CTS must validate X.509 Digital Certificate with an approved Certificate Authority. An X.509 Digital Certificate contains the public key for each Competent Authority and is retrieved from the CTS Portal https://www.cts-eoi.com/MemberInfo (or on test https://oecddataexchange.org/MemberInfo). While data preparation occurs outside the scope of CTS, the operators of a regional hub must, similar to the restrictions to the operators of the CTS, never have access to the private keys that allow encryption/decryption of payloads containing tax treaty information.

Process: **Validate Certificate**

Step: 5a - Encrypt the AES Key and IV with Public Key of Recipient

File Naming Convention: **N/A**

Step description:

To validate the certificate:

- Verify the certificate chain;
- Check the revocation status of the certificate chain. There are two methods:
  - Retrieve a Certificate Revocation List (CRL) or
  - Send an Online Certificate Status Protocol (OCSP) query to a Certificate Authority designated responder

Process: **Encrypt the AES Key**

Step: **5b - Encrypt the AES Key and IV with Public Key of the Receiving Competent Authority**

File Naming Convention: **CountryCodeReceiver_ABC_Key**

Step description:

After validating the certificate, use the public key from the Receiving Competent Authority's certificate to encrypt the 32 byte AES 256 key concatenated with the 16 byte IV. The encrypted value must be 48 bytes in length.

The public key encryption uses the standard RSA algorithm. There are several steps necessary to perform AES encryption. The following agreed settings should be used to maintain compatibility:

- Padding: PKCS#1 version 1.5
- Key Size: 4096 bits (or 2048 bits until 31 May 2018)

The encrypted file name is "CountryCodeReceiver_ABC_Key".

Summary:

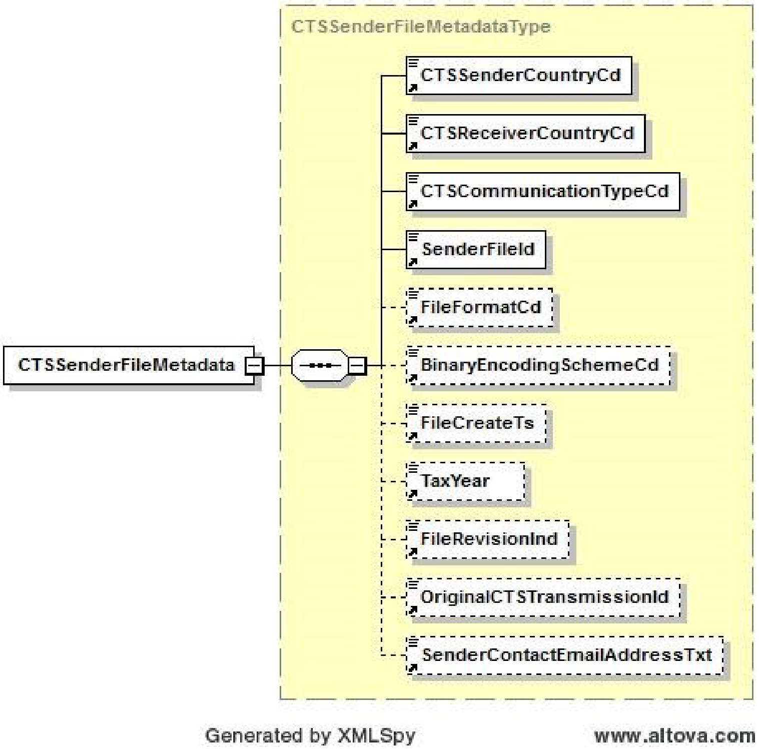
There will be two encrypted files. The files are case sensitive and any variation in file name or format will cause the transmission to fail:

- Symmetric encryption - the AES 256 encrypted XML file name is "CountryCodeSender_ABC_Payload"
- Asymmetric encryption - the public key encrypted AES 256 key file name is "CountryCodeReceiver_ABC_Key"

Step 6 - Create Sender Metadata File

25. In order to ensure that the CTS can correctly route a file from the Sending Competent Authority to the Receiving Competent Authority, each file transmission needs, in addition to the encrypted file containing the tax information, to include an unencrypted Metadata File. The Metadata File is never encrypted as it is used to verify and route transmissions through the CTS to the correct Receiving Competent Authority. The Sending Competent Authority generates the CTS Metadata XML file by using the CTS Metadata XML Schema. The correct file name is "CountryCodeSender_ABC_Metadata.xml."

CTS Metadata XML Schema



26. Sending Competent Authorities must provide the values for the required elements in the Metadata File (please ensure the CTS Metadata XML file is valid against the CTS Metadata XML Schema). Please note that the Metadata file is validated by the CTS system and if required information is missing, the upload will fail.

27. The content to be provided in the different elements of the CTS Metadata Schema is as follows:

- The CTSSenderCountryCd element identifies the jurisdiction of the Sending Competent Authority.
- The CTSReceiverCountryCd element indicates the jurisdiction of the Receiving Competent Authority.
- The CTSCommunicationTypeCd element specifies the type of message transmitted. Only the agreed Message type codes (defined in the Section "Message types in the Metadata schema v2.0") are allowed.
- The SenderFileID element is a free text field to capture the ID created by the Sending Competent Authority. The element helps both the Sending and Receiving Competent Authority to track and monitor a specific message. The agreed format is:
- CountryCdSender_CountryCdReceiver_CommunicationType_MessageRefID5
- The FileFormatCd element specifies the file format of message transmitted. When sending an XML file, the value must be XML. When using the CTS Wrapper (for non-XML files), the

[5] While the MessageRefID length is unlimited in some schemas (ex: CRS v1.0), it is important to take into account that MessageRefID will be contained in the SenderFileID field which is limited to a maximum of 200 characters. Therefore, the MessageRefID must not exceed 170 characters to ensure the proper functioning of the CTS Metadata Schema. The Generic Status Message user guide indicates that for the Status Message type codes starting with "EOIR" or "SPON", the MessageRefID is limited to 160 characters.

Metadata.FileFormatCd can be omitted, since it will be specified for each file in the CTS Wrapper. For more information, please consult the CTS Wrapper User Guide in Annex III.

- The BinaryEncodingSchemeCd element identifies the type of encoding scheme for the transmission payload. If sending an XML file, the value must be "NONE". When using the CTS Wrapper (for non-XML files), the Metadata. BinaryEncodingSchemeCd can be omitted, since it will be specified for each file in the CTS Wrapper.
- The FileCreateTs element identifies the timestamp for the transmission payload created by the Sending Competent Authority.
- The Tax Year element is optional and allows specifying the tax year to which the file relates.
- The FileRevisionInd element is a Boolean field to indicate if the file is a revised message. The only allowable values are "true" or "false". If a file was rejected by the receiving Competent Authority, the FileRevisionInd can be set to true when correcting a file. If the FileRevisionInd element is set to "true", the element OriginalCTSTransmissionId must be included.
- The OriginalCTSTransmissionId element is a free text field to reference the unique original CTS transmission ID. The identifier helps both the Sending and Receiving Competent Authority to track and monitor messages. The OriginalCTSTransmissionId, should be left blank when sending a correction message. When retransmitting an ABC message, this field references the OriginalCTSTransmissionId associated with the previously failed or rejected transmission. If a Status Message is sent, this field references the OriginalCTSTransmissionId associated with the original ABC message.
- The SenderContactEmailAddressTxt element is a free text field to identify the email address of the Sending Competent Authority.

Step 7 - Create the transmission file (data packet)

28. A file that is transmitted through the CTS is known as the CTS data packet. The CTS data packet is an archive in .ZIP file format, and it should be created using the deflate compression algorithm (see Step 3 - Compress the XML File, above).

29. The CTS only supports data packets in a .ZIP file format with a .zip file extension. The files are case sensitive and any variation in the file name or format will cause the transmission through the CTS to fail.

30. The three files to be contained in a CTS data packet are:

File Name	Description
CountryCodeSender_ABC_Payload	Encrypted payload using a randomly generated one-time use key
CountryCodeReceiver_ABC_Key	Key encrypted using the Receiving Competent Authority's public key
CountryCodeSender_ABC_Metadata.xml	CTS Metadata Schema to ensure that the CTS that the CTS can correctly route the file from the Sending Competent Authority to the Receiving Competent Authority and the Receiving Competent Authority can properly process the XML reports. The Metadata File is not encrypted.

31. The CTS data packet will be named:

File Name	Description
CountryCodeSender_ABC_UTC.zip	Transmission file to be sent through the CTS.

32. Each CTS data packet must start by Country Code of Sending Competent Authority, followed by the communication type (see the list of the agreed message type codes on page 4) and followed by a Coordinated Universal Time (UTC) timestamp. The timestamp format of the UTC is YYYYMMDDTHHMMSSmsZ where:

- YYYY = 4-digit year
- MM = 2-digit month
- DD = 2-digit day
- HH = 24-hour
- MM = 2-digit minutes
- SS = 2-digit seconds
- ms = 3-digit milliseconds

33. For example, if Canada transmits a CRS data packet on January 15, 2017 at 16:30:45, the CTS data packet will be named as: CA_CRS_20170115T163045123Z.zip

Step 8 - Transmit the CTS Data Packet

34. After the CTS data packet is uploaded and transmitted, the CTS sends an alert to the Sending Competent Authority via email. More detailed explanations about the transmission alerts generated by the CTS is available at https://community.oecd.org/docs/DOC-223688.

35. The message provides status information about the file upload. If the upload and CTS file checks are successful, CTS assigns a unique "CTS Transmission ID" in the email. If there is an error, the CTS alert provides an appropriate error code in the email message.

Example for the sequence of exchanges through the Common Transmission System

36. This section contains an example of CRS and CRS Status Message exchanges through the Common Transmission System. The same approach is applicable for the other message types[6], unless certain file/record error(s) does not apply to this message type[7].

37. Please note that file preparation will need to be performed for all exchanges through the Common Transmission System, independent of message type being exchanged.

38. As an example, for an exchange of CRS information between Canada and France, the following events occur:

1. Canada sends a CRS message with new data to France

– France is not able to decrypt the file and sends a CRS Status Message

2. Canada corrects the file with proper encryption

– France found XML validation errors and send a CRS Status Message

3. Canada corrects the XML validation issues and resubmits the file

– France found no file error, but ten (minor) record errors. France accepts the file

4. Canada corrects the ten records errors (the file contains the ten corrected records)

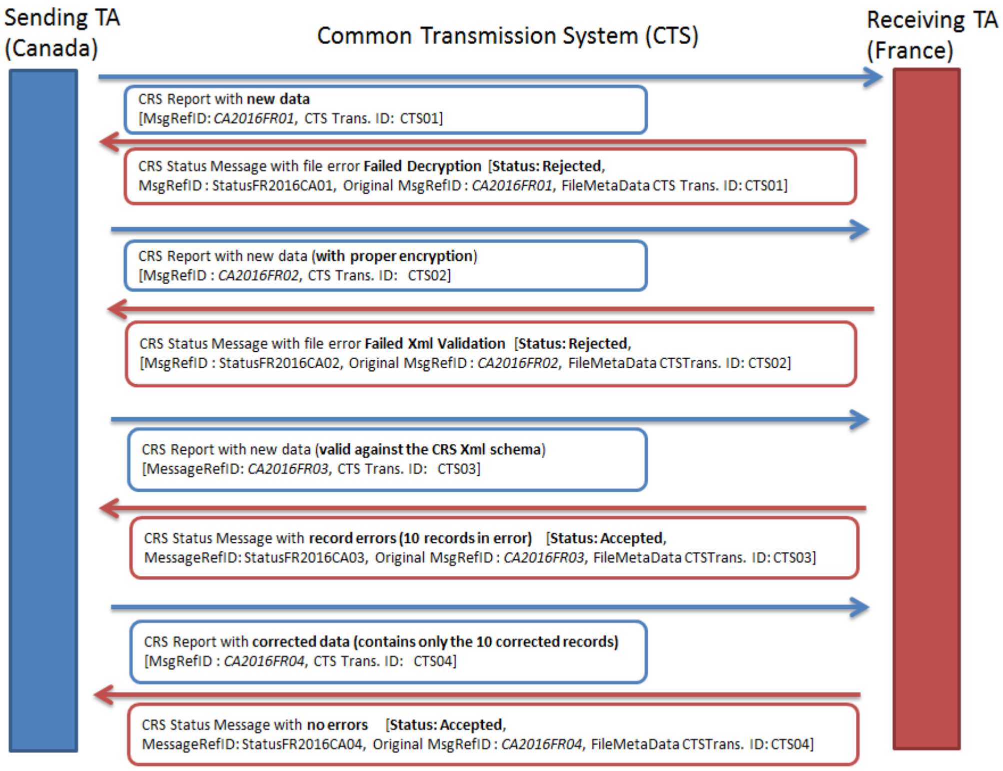
– France found no further errors. France accepts the file.

[6] Please see the list of agreed message type codes in the Section « Message types in the Metadata schema v2.0 ».

[7] Please consult the relevant (Generic, CRS, CbC or ERTR) Status Message user guide to know which record error applies for the message.

Example of exchanges between two competent authorities

39. As shown in the diagram above, file preparation is required for all files sent, i.e. for CRS XML Schema files and for CRS Status Message files.



CRS Report with **new data**
[MsgRefID: *CA2016FR01*, CTS Trans. ID: CTS01]

CRS Status Message with file error **Failed Decryption** [**Status: Rejected**,
MsgRefID : StatusFR2016CA01, Original MsgRefID : *CA2016FR01*, FileMetaData CTS Trans. ID: CTS01]

CRS Report with new data (**with proper encryption**)
[MsgRefID : *CA2016FR02*, CTS Trans. ID: CTS02]

CRS Status Message with file error **Failed Xml Validation** [**Status: Rejected**,
[MsgRefID : StatusFR2016CA02, Original MsgRefID : *CA2016FR02*, FileMetaData CTSTrans. ID: CTS02]

CRS Report with new data (**valid against the CRS Xml schema**)
[MessageRefID: *CA2016FR03*, CTS Trans. ID: CTS03]

CRS Status Message with **record errors (10 records in error)** [**Status: Accepted**,
MessageRefID: StatusFR2016CA03, Original MsgRefID : *CA2016FR03*, FileMetaData CTSTrans. ID: CTS03]

CRS Report with **corrected data (contains only the 10 corrected records)**
[MsgRefID : *CA2016FR04*, CTS Trans. ID: CTS04]

CRS Status Message with **no errors** [**Status: Accepted**,
MessageRefID: StatusFR2016CA04, Original MsgRefID : *CA2016FR04*, FileMetaData CTSTrans. ID: CTS04]

Annex I

File Validation Errors

File Validations (50 000 – 59 999)

Please do not submit a request to correct or delete any of the records in this file until you receive a Status Message that this file has been received as valid (Status is Accepted). In case a file error is detected, the file should be resubmitted by the sender, using a new, unique MessageRefID.

Failed Download (50001)

File error code: 50001

Failed Download

File error description:

The receiving Competent Authority could not download the referenced file.

Action Requested:

Please resubmit the file, with a new unique MessageRefID.

Failed Decryption (50002)

File error code: 50002

Failed Decryption

File error description:

The receiving Competent Authority could not decrypt the referenced file.

Action Requested:

Please re-encrypt the file with a valid key and resubmit the file.

Failed Decompression (50003)

File error code: 50003

Failed Decompression

File error description:

The receiving Competent Authority could not decompress the referenced file.

Action Requested:

Please compress the file (before encrypting) and resubmit the file with a new unique MessageRefID.

Failed Signature Check (50004)

File error code: 50004

Failed Signature Check

File error description:

The receiving Competent Authority could not validate the digital signature on the referenced file.

Action Requested:

Please re-sign the file with the owner's private key using procedures as defined in the context of the CTS.

Failed Threat Scan (50005)

File error code: 50005

Failed Threat Scan

File error description:

The receiving Competent Authority detected one or more potential security threats within the decrypted version of the referenced file. Such threats include but are not limited to hyperlinks, Java script, and executable files. URLs (internet addresses) provided as plain text and not in hyperlink form should be allowed, although each Competent Authority is responsible for maintaining its own list of potential security threats.

Action Requested:

Please scan the file for known threats and viruses, remove all detected threats and viruses prior to encryption and re-encrypt and resubmit the file.

Failed Virus Scan (50006)

File error code: 50006

Failed Virus Scan

File error description:

The receiving Competent Authority detected one or more known viruses within the decrypted version of the referenced file.

Action Requested:

Please scan the file for known threats and viruses, remove all detected threats and viruses prior to encryption, and re-encrypt and resubmit the file.

Failed Schema Validation (50007)

File error code: 50007

Failed Schema Validation

File error description:

The referenced file failed validation against the relevant XML Schema.

When the Metadata.FileFormatCd is different than XML (e.g. PDF or JPEG), the file will be sent with the CTS Wrapper (for non-XML files). In such a case the file error 50007 will indicate that the XML file failed the validation against the CTS Wrapper.

Action Requested:

Please re-validate the file against the relevant XML Schema, resolve any validation errors, and re- encrypt and resubmit the file.

Invalid MessageRefID format (50008)

File error code: 50008

Invalid MessageRefID format

File error description:

The structure of the MessageRefID is not in the correct format, as set out in the relevant User Guide.

Action Requested:

Please ensure the MessageRefID follows structure defined in the relevant User guide, and resubmit the file.

MessageRefID has already been used (50009)

File error code: 50009

MessageRefID has already been used

File error description:

The referenced file has a duplicate MessageRefID value that was received on a previous file.

Action Requested:

Please replace the MessageRefID field value with a new unique value (not containing all blanks), and resubmit the file.

File Contains Test Data for Production Environment (50010)

File error code: 50010

File Contains Test Data for Production Environment

File error description:

The referenced file contains one or more records with a DocTypeIndic value in the range OECD10-OECD13, indicating test data. As a result, the receiving Competent Authority cannot accept this file as a valid file submission.

For more information on the DocTypeIndic data element, please consult the relevant User Guide.

The file error 50010 will only apply if the ABC schema contains a correctable record. A correctable record contains a DocSpec (and a DocTypeIndic), thus allowing for future corrections. For example, the CDQ schema does not contain correctable records, so the file error 50010 cannot be used in the context of the CDQ schema. Similarly, if the ABC message is using the CTS Wrapper for non-XML files (e.g. an EOIR PDF file), then file error 50010 cannot be used.

Action Requested:

If this file was intended to be submitted as a valid file, please resubmit with DocTypeIndic values in the range OECD0-OECD3 (see relevant User guide). [If this file was intended as a test file, please submit to the CTS test environment during an agreed test window.]

File Contains Production Data for Test Environment (50011)

File error code: 50011

File Contains Production Data for Test Environment

File error description:

The referenced file was received in a test environment with one or more records having a DocTypeIndic value in the range OECD0-OECD3. These DocTypeIndic values indicate data in this file may have been intended as a valid file submission. Messages received in test environments are not accepted by the receiving Competent Authority as a valid file submission. Submissions to the test environment should only include records with DocTypeIndic in the range OECD10-OECD13, indicating test files.

The file error 50011 will only apply if the ABC schema contains a correctable record. A correctable record contains a DocSpec (and a DocTypeIndic), thus allowing for future corrections. For example, the CDQ schema does not contain correctable records, so the file error 50011 cannot be used in the context of the CDQ schema. Similarly, if the ABC message is using the CTS Wrapper for non-XML files (e.g. an EOIR PDF file), then file error 50011 cannot be used.

Action Requested:

If this file was intended to be submitted as a valid file, please resubmit with DocTypeIndic values in the range OECD0-OECD3. [If this file was intended as a test file, please correct the DocTypeIndic for all records and resubmit to the CTS test link.]

The received message is not meant to be received by the indicated jurisdiction (50012)

File error code: 50012

The received message is not meant to be received by the indicated jurisdiction

File error description:

The records contained in the payload file are not meant for the receiving Competent Authority, but should have been provided to another jurisdiction.

Action Requested:

The file is to be immediately deleted by the initial, erroneous receiver and that receiving Competent Authority will promptly notify the sending Competent Authority about the erroneous transmission through the relevant Status Message XML Schema.

An incorrect AES key size was detected by the receiving jurisdiction (50013)

File error code: 50013

The AES key size has been detected as incorrect by the receiving jurisdiction

File error description:

The recipient has detected one or more of the following errors:

- Data packet transmitted with ECB cipher mode (or any cipher mode other than CBC)
- Data packet does not include IV in Key File
- Combined (IV and AES) data packet key size is not 48 bytes
- Data packet does not contain the concatenated key and IV.

Action Requested:

The sending Competent Authority should resend the file (newly encrypted, with a new unique MessageRefID and with the correct AES key size).

The Message Type in the Generic Status Message does not match with the Message Type in the Metadata (50014)

File error code: 50014

The Message Type in the Generic Status Message does not match with the Message Type in the Metadata

File error description:

The message type specified in the Generic Status Message (MessageSpec.MesageType) does not match the message type specified in the Metadata (Metadata.CTSCommunicationTypeCd).

Action Requested:

The sending Competent Authority should resend the file and make sure the Message Type in the Generic Status Message does match with the Message Type in the Metadata.

Annex II
Documentation and Tools available

CTS File Preparation Tool (Sample Codes)

https://one-communities.oecd.org/community/cts/SitePages/uploaded-document-181858

CTS documentation

https://one-communities.oecd.org/community/cts

List of all User Guides and Schemas

https://one-communities.oecd.org/community/cts/SitePages/document-118640

Annex III
User Guide for the CTS Wrapper

Version 1.2 - March 2024
(Schema v2.0)

General instructions for scanning documents to be sent

Paper documents shall be scanned in a way that preserves their image in its exact physical view. The paper copies should be retained by the sending competent authority in accordance with its current procedures.

The documents must be in a platform-independent format such as PDF (Portable Document Format) or JPG (Joint Photographic Group).

Scanning and file format guidelines:

- Black & white – 200-300 DPI (dots per inch)
- Colour or grey – 150-200 DPI

CTS Wrapper XML Schema User Guide

Introduction

The User Guide contains further guidance on the use of the CTS File Wrapper XML Schema . The User Guide is divided into logical sections based on the schema and provides information on specific data elements and any attributes that describe that data element.

The CTS File Wrapper XML Schema Information sections are:

I. Message Header with the sender, recipient(s), message type and the timestamp

II. The body of the CTS File Wrapper XML Schema, containing the Files to be transmitted (see the element FileAttach).

The requirement field for each data element and its attribute indicates whether the element is validation or optional in the CTS File Wrapper XML Schema.

“Validation” elements MUST be present for ALL data records in a file and an automated validation check can be undertaken. The sender should do a technical check of the data file content using XML tools to make sure all validation elements are present.

"Optional" elements are, while recommended, not required to be provided and may in certain instances represent a choice between one type or another, where one of them must be used.

Appendix A to the CTS File Wrapper User Guide shows a diagrammatic representation of the CTS File Wrapper XML Schema with all its elements. The numbers next to the headings are the corresponding section numbers in the User Guide text, which provides further guidance on the information to be provided in each element.

Appendix B to the CTS File Wrapper User Guide contains a Glossary of namespaces for the CTS File Wrapper XML Schema.

I. Message Header

Information in the message header identifies the Competent Authority that is sending the message, as well as the Competent Authorities receiving the message. It specifies when the message was created and the nature of the report.

Element	Attribute	Size	Input Type	Requirement
TransmittingCountry		2-character	iso:CountryCode_Type	Validation

This data element identifies the jurisdiction of the Competent Authority transmitting the message. It uses the 2-character alphabetic country code and country name list[8] based on the ISO 3166-1 Alpha 2 standard.

Element	Attribute	Size	Input Type	Requirement
ReceivingCountry		2-character	iso:CountryCode_Type	Validation

This data element identifies the jurisdiction of the Competent Authority receiving the message. This data element identifies the jurisdiction of the Competent Authority that is the intended recipient of the message. It uses the 2-character alphabetic country code based on the ISO 3166-1 Alpha 2 standard.

Element	Attribute	Size	Input Type	Requirement
MessageType			cfw:MessageType_EnumType	Validation

This data element specifies the type of message being sent. The only allowable values are the codes indicated below.

Description	Code
DTC AEOI	DTCAEOI
EOIR free format – Direct Tax	EOIRFreeDT
EOIR free format – Indirect Tax	EOIRFreeIT
EOIR free format – Tax collection and recovery	EOIRFreeTCR
EOIR structured format (e-forms) – Direct Tax	EOIRStructDT
EOIR structured format (e-forms) – Indirect Tax	EOIRStructIT
EOIR structured format (e-forms) – Tax collection and recovery	EOIRStructTCR
Spontaneous exchanges free format – Direct Tax	SponFreeDT
Spontaneous exchanges free format – Indirect Tax	SponFreeIT
Spontaneous exchanges free format – Tax collection and recovery	SponFreeTCR
Spontaneous exchanges structured format (e-forms) – Direct Tax	SponStructDT

[8] The following disclaimer refers to all uses of the ISO country code list in the CTS File Wrapper User Guide XML Schema: For practical reasons, the list is based on the ISO 3166-1 country list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status of the territories listed. Its content is without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Spontaneous exchanges structured format (e-forms) – Indirect Tax	SponStructIT
Spontaneous exchanges structured format (e-forms) – Tax collection and recovery	SponStructTCR
Joint Audits	JointAudits
JITSIC	JITSIC
MAP	MAP
Other exchanges under international tax agreements	Other

Element	Attribute	Size	Input Type	Requirement
Warning		1 to Max 4'000 characters	cfw:StringMin1Max4000_Type	Optional

This data element is a free text field allowing input of specific cautionary instructions about use of the CTS File Wrapper Message.

Element	Attribute	Size	Input Type	Requirement
Contact		1 to Max 4'000 characters	cfw:StringMin1Max4000_Type	Optional

This data element is a free text field allowing input of specific contact information for the sender of the message (i.e. the Competent Authority sending the CTS File Wrapper Message).

Element	Attribute	Size	Input Type	Requirement
MessageRefID		1 to 170 characters	cfw:StringMin1Max170_Type	Validation

This data element is a free text field capturing the sender's unique message identifier (created by the sender) that identifies the particular CTS File Wrapper Message being sent. The identifier allows both the sender and receiver to identify the specific message later if questions arise.

The MessageRefID identifier can contain whatever information the sender uses to allow identification of the particular Message but must start with the Message type code[9] followed by the sender country code, then the receiver country code before a unique identifier.

e.g. EOIRFreeDTFRCA123456789

This MessageRefID indicates that the Message type is "EOIR free format – Direct Tax", France is the country of the Competent Authority sending the Message, Canada is the country of the Competent Authority receiving the Message, and that the unique identifier is "123456789".

In order to ensure that a status message can be uniquely identified, the MessageRefID must be unique in space and time (i.e. there must be no other message in existence that has the same reference identifier).

Element	Attribute	Size	Input Type	Requirement
Timestamp			xsd:dateTime	Validation

This data element identifies the date and time when the message was compiled. It is anticipated this element will be automatically populated by the host system. The format for use is YYYY-MM-DD'T'hh:mm:ss.nnn. Fractions of seconds may be used (in such a case the milliseconds will be provided in 3 digits, see ".nnn" in the format above). Examples: **2018-02-15T14:37:40 or 2018-02-15T14:37:40.789 (with milliseconds).**

[9] The Message type code (specified in the MessageRefID) must be the same code as defined in the MessageSpec.MessageType element.

II. File Attach

The body of the Body of the CTS File Wrapper Message contains the file(s) being transmitted, as well as information to identify these files. For each file transmitted, the FileAttach element will be repeated.

Element	Attribute	Size	Input Type	Requirement
FileAttach			cfw:FileAttach_Type	Validation

The FileAttach element is composed of the four elements below.

Element	Attribute	Size	Input Type	Requirement
FileName		1 to 255 characters	cfw:StringMin1Max255_Type	Validation

This element will contain the name of the file being transmitted.

Element	Attribute	Size	Input Type	Requirement
FileFormatCd			cfw:FileFormat_EnumType	Validation

This element specifies the file name of the file being transmitted.The possible values are: PDF, JPG, RTF, TXT, DOC, DOCX, XLS, XLSX, and STF.

Element	Attribute	Size	Input Type	Requirement
BinaryEncoding SchemeCd			cfw:BinaryEncodingScheme_EnumType	Validation

This element specifies the type of encoding scheme used for the file. When sending a TXT file, the BinaryEncodingSchemeCd will be set to “NONE”, in all other cases it will be set to “BASE64”.

Element	Attribute	Size	Input Type	Requirement
FileWrapper			xsd:string	Validation

This element will contain the file being transmitted. Please follow the instructions below on how to proceed to incorporate the file into the FileWrapper element.

In order to convert a file with an extension of .PDF, .JPG, .RTF, .DOC, DOCX, .XLS, .XLSX, or .STF, you must use Base64 encoding scheme to convert the binary based content into text, and then apply <FileWrapper> element tag around the text. In such a case, the Metadata. BinaryEncodingSchemeCd will be set to “BASE64”.

In order to convert a file with a .TXT extension, you must convert the .TXT file by using the <FileWrapper> element tag directly around the text. In such a case, the Metadata. BinaryEncodingSchemeCd will be set to “NONE”.

In order to see an example of how to perform this conversion programmatically, please see the .Net version of the CTS File Preparation code sample for CTS v2.0.

III. Schema version

The version of the schema and the corresponding business rules have a unique version number assigned that usually consists of two numbers separated by a period sign: major and minor version (ex: 1.0). The version number could also contain a third number (ex: 1.0.1) which indicates that the schema was revised with very minor changes (ex: only new enumerations were added).

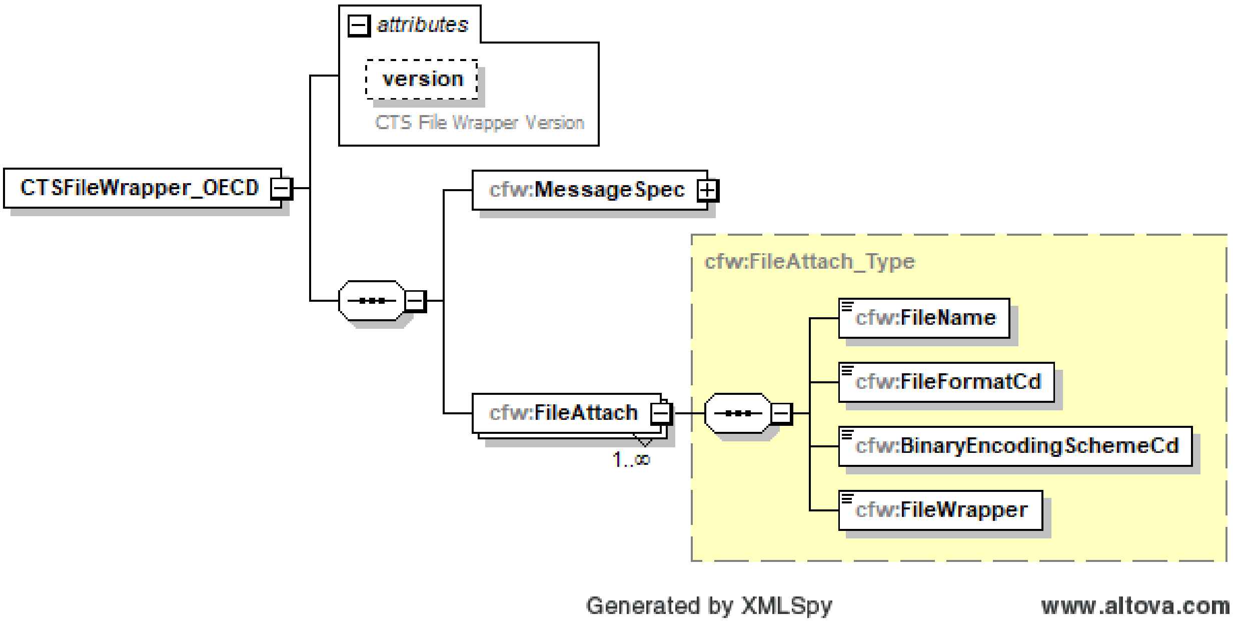
The version is identified by the version attribute on the schema element. The target namespace of the CTS File Wrapper schema contains only the major version.

Element	Attribute	Size	Input Type	Requirement
CTSFileWrapper_ OECD	version	1 to 10 characters	cfw:StringMin1Max10_Type	Optional (Mandatory)

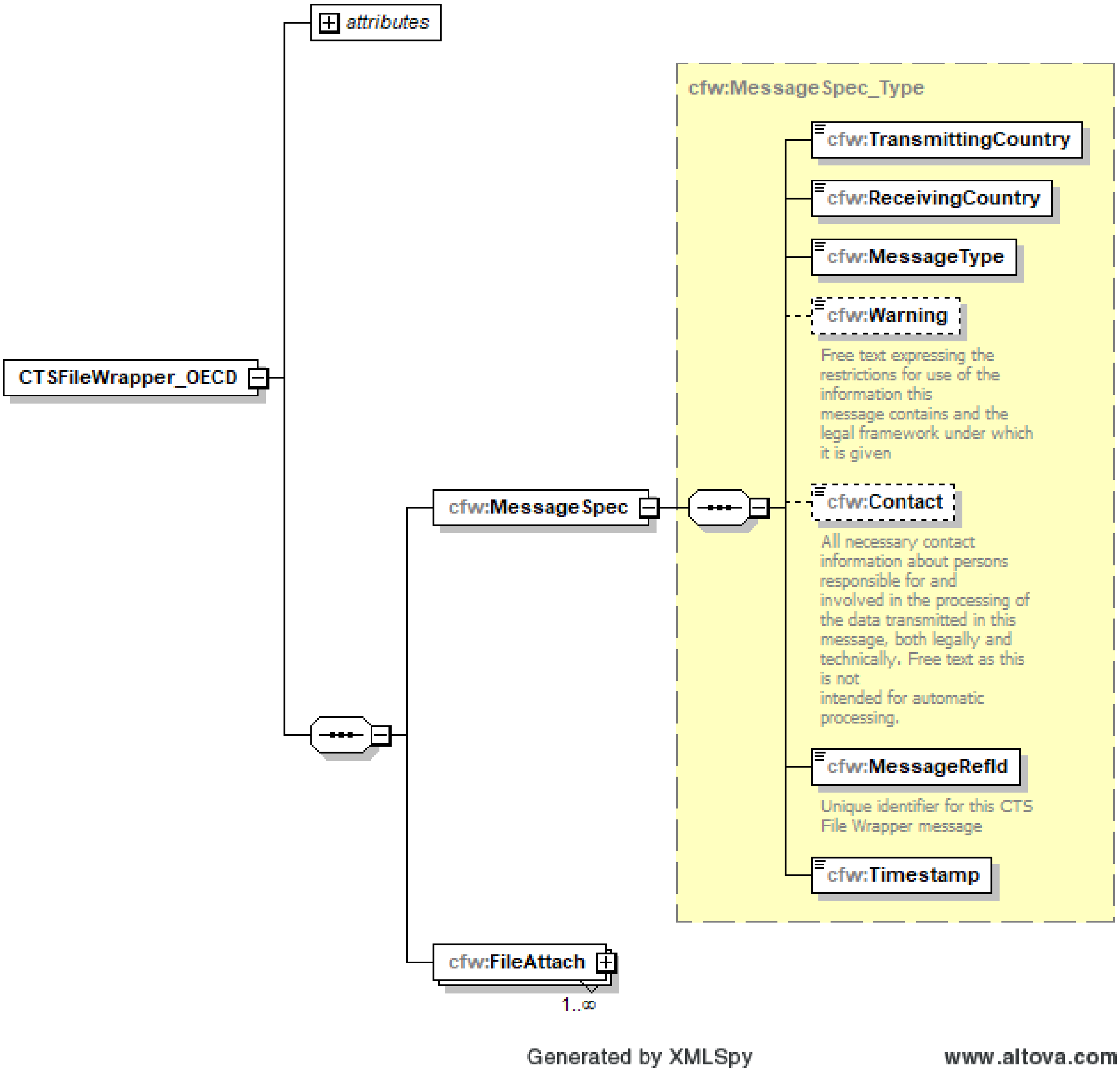
The root element CTSFileWrapper_OECDversion attribute in the XML report file must be set to the value of the schema version. This will identify the schema version that was used to create the report.

For the CTS File Wrapper schema version 2.0, the version attribute must be set to the value “2.0”.

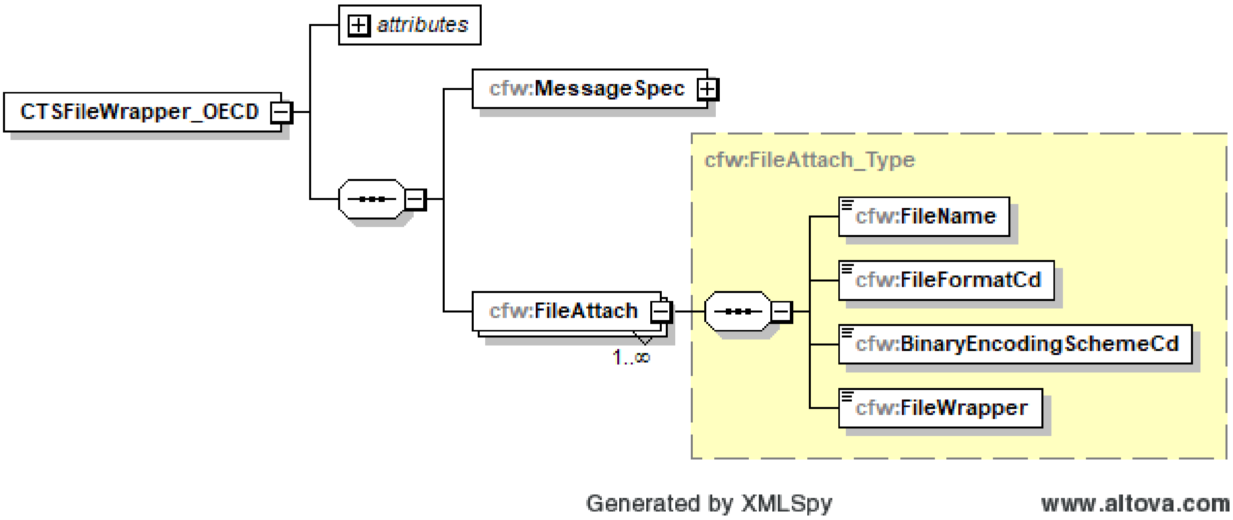
Appendix A: CTS File Wrapper XML schema diagrams



Message Header [Section I]


attributes
CTSFileWrapper_OECD
cfw:MessageSpec_Type
cfw:TransmittingCountry
cfw:ReceivingCountry
cfw:MessageType
cfw:Warning
Free text expressing the restrictions for use of the information this message contains and the legal framework under which it is given
cfw:MessageSpec
cfw:Contact
All necessary contact information about persons responsible for and involved in the processing of the data transmitted in this message, both legally and technically. Free text as this is not intended for automatic processing.
cfw:MessageRefId
Unique identifier for this CTS File Wrapper message
cfw:Timestamp
cfw:FileAttach
1..∞
Generated by XMLSpy
www.altova.com

File Attach [Section II]



Appendix B – CTS File Wrapper XML Schema Namespaces

Namespace	Description	Filename
cfw	CTS File Wrapper types	CTSFileWrapper_v2.0.xsd
iso	ISO types (Country codes)	isocfwtypes_v1.0.xsd