Annex 3

Common Reporting Standard User Guide

Version 2.0

Introduction

The OECD working with G20 countries has developed a common standard on reporting, due diligence and exchange of financial account information. Under this common standard, jurisdictions obtain from reporting financial institutions and automatically exchange with exchange partners, as appropriate, on an annual basis financial information with respect to all reportable accounts, identified by financial institutions on the basis of common reporting and due diligence rules.

Part of the technical solution to support this common standard is a schema and related instructions.

A schema is a data structure for holding and transmitting information electronically and in bulk. XML "extensible markup language" is commonly used for this purpose. Examples are the OECD's Standard Transmission Format "STF" or the Fisc 153 format used for information exchange for the European Savings Directive.

This User Guide explains the information required to be included in each CRS data element to be reported in the CRS XML Schema v. 1.0. It also contains guidance on how to make corrections of data items within a file that can be processed automatically.

How the CRS User Guide links to the CRS Schema

This 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 CRS Schema Information sections are

I Message Header with the sender, recipient, message type, reporting period

II Controlling Person or Account Holder details if an individual

III Account Holder if an entity

IV CRS Body; Reporting FI and Reporting Group and Account details

The numbers of the sections are reflected in the numbering of the diagrams in Appendix A.

The CRS XML Schema is designed to be used for the automatic exchange of financial account information between Competent Authorities ("CAs"). In addition the CRS could also be used for domestic reporting by Financial Institutions ("FIs") to domestic tax authorities under the CRS. Items relevant for domestic reporting only are shown in [*brackets*].

The CRS schema is re-using the FATCA schema and elements of STF, so there are some elements in the CRS schema that are not required for purposes of reporting and exchange under the CRS (e.g. Pool Report and Nationality). These elements are shown in the User Guide as optional, followed by "*non-CRS*".

The comment "*non-CRS*" is also shown on the Appendix A diagrams where relevant.

The CRS XML Schema and its User Guide provide for elements that are unique to CRS e.g. undocumented and closed accounts.

The requirement field for each data element and its attribute indicates whether the element is validation or optional in the schema. Every element is one or the other in the 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 and if they are not, correct the file. The Receiver may also do so and if incorrect, may reject the file. Where there is a choice between 2 validation elements under a validation parent and only one is needed, this is shown as "Validation (choice)". If the elements are under an optional parent, they are shown as optional.

There may be different business rules for elements that are optional in the schema:

- Some optional fields are shown as "(Optional) Mandatory" – an optional element that is required for CRS reporting as specified in CRS reporting requirements depending on availability of information or legal factors. Mandatory elements may be present in most (but not all) circumstances, so there cannot be a simple IT validation process to check these. (E.g. the CRS provides that a reporting FI is required to report the TIN of an Account Holder only if issued by his jurisdiction of residence / place of birth only if otherwise required to retain and report and is held in electronically searchable records).
- Optional elements may represent a choice between one type or another, where one of them must be used (e.g. choice between address fix or address free). Shown as "Optional" requirement.
- The element may not be required for either schema validation or CRS. It should not be reported in a CRS only file as indicated by "Optional (non CRS)".

Appendix A to the CRS User Guide shows a diagrammatic representation of the CRS XML Schema with all its elements. The numbers next to the headings are the corresponding section numbers in the User Guide text. The comment boxes include both explanations, and changes from the previous version of the CRS schema which will be removed when the draft is agreed.

Appendix B to the CRS User Guide contains a Glossary of namespaces for the CRS XML Schema.

Common Reporting Standard Schema Information

I. Message Header

Information in the message header identifies the tax administration that is sending the message. It specifies when the message was created, what period (normally a year) the report is for, and the nature of the report (original, corrected, supplemental, etc.).

Element	Attribute	Size	Input Type	Requirement
SendingCompanyIN		Unlimited	xsd:string	Optional

[*Although not used for exchange between Competent Authorities under CRS, for domestic reporting the Sending Company Identification Number element would be Mandatory and would identify the Financial Institution reporting to the Sending tax authority by domestic TIN (or IN).*]

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

This data element identifies the jurisdiction where the reported financial account is maintained or where the reported payment is made by the reporting FI. If the sender is a tax administration, the transmitting country is the jurisdiction of the tax administration. This data element uses the 2-character alphabetic country code and country name list[1] based on the ISO 3166-1 Alpha 2 standard.

[*For domestic reporting this element would be the domestic Country Code.*]

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

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

[*For domestic reporting this element would be the domestic Country Code.*]

Element	Attribute	Size	Input Type	Requirement
MessageType			crs:MessageType_EnumType	Validation

This data element specifies the type of message being sent. The only allowable entry in this field for CRS AEOI is "CRS".

Element	Attribute	Size	Input Type	Requirement
Warning			xsd:string	Optional

This data element is a free text field allowing input of specific cautionary instructions about use of the CRS message content, for example terms of the Instrument or Convention under which the data is exchanged. If the reported

1. The following disclaimer refers to all uses of the ISO country code list in the CRS 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.*

data is for a period other than for a full reporting year this information can be given here as narrative e.g. “ten month period”.

Element	Attribute	Size	Input Type	Requirement
Contact			xsd:string	Optional

This data element is a free text field allowing input of specific contact information for the sender of the message. [*May give FI or third party contact for domestic reporting only.*]

Element	Attribute	Size	Input Type	Requirement
MessageRefID			xsd:string	Validation

This data element is a free text field capturing the sender’s unique identifying number (created by the sender) that identifies the particular message being sent. The identifier allows both the sender and receiver to identify the specific message later if questions or corrections arise. For exchanges between Competent Authorities, the first part should be the country code of the sending jurisdiction, the second part the year to which the data relates and the third part the receiving country code, before a unique identifier created by the sending jurisdiction (the “national part”).

[*If the CRS schema is used for domestic reporting, the FI could include an FI Identification Number in the MessageRefID at the start of the unique identifier created by the FI which is recommended as good practice.*]

Element	Attribute	Size	Input Type	Requirement
MessageTypeIndic			crs:CrsMessageTypeIndic_EnumType	Optional

This data element allows the sender to define the type of message sent. This is an optional element as the DocTypeIndic also identifies whether data is new or corrected (see Guidance on the Correction Process below). Messages must contain all new or all corrected data, [*or advise domestically that there is no data to report*].

[*The MessageTypeIndic can be used domestically to indicate that the Financial Institution has carried out the appropriate checks of its client data but there is no data to report (a “nil return” in effect). In this instance only, Account Report IVc need not be completed.*]

The possible values are:

CRS701= The message contains new information

CRS702= The message contains corrections for previously sent information

CRS703= *The message advises there is no data to report*

Element	Attribute	Size	Input Type	Requirement
CorrMessageRefID			xsd:string	Optional

This data element is a free text field capturing the unique identifying number (as determined by the sender) that identifies a corrected message being sent. This data element MUST reference the original Message Reference ID created for the original message. Guidance on the Correction Process is given below, to explain that this is only used in CRS to cancel a previous message.

Element	Attribute	Size	Input Type	Requirement
ReportingPeriod			xsd:date	Validation

This data element identifies the last day of the reporting period (normally a tax year) to which the message relates in YYYY-MM-DD format. For example, if reporting information for the accounts or payments made in calendar year 2014, the field would read, "2014-12-31". If exceptionally the reporting period is not a year then show the length of the reporting period in Warning.

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. Fractions of seconds are not used. Example: 2015-03-15T09:45:30.

II. PersonParty_Type

The data elements in this section are used for Individual Account Holders or Controlling Persons of Passive NFEs. This complex type is comprised of the following data elements:

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

Element	Attribute	Size	Input Type	Requirement
TIN			cfc:TIN_Type	(Optional) Mandatory

Element	Attribute	Size	Input Type	Requirement
Name			crs:NamePerson_Type	Validation

Element	Attribute	Size	Input Type	Requirement
Address			cfc:Address_Type	Validation

Element	Attribute	Size	Input Type	Requirement
Nationality			iso:CountryCode_Type	Optional (Non CRS)

Element	Attribute	Size	Input Type	Requirement
BirthInfo				(Optional) Mandatory

IIa. ResCountryCode

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

This data element describes the tax residence country code(s) for the individual being reported upon and must be present in all data records for CRS AEOI between Competent Authorities.

A separate report for each residence jurisdiction of the Reportable Person including Controlling Persons who are Reportable Persons is required, along with details of the Entity, if there is more than one jurisdiction of residence.

[*For domestic reporting, if the individual is certified or treated as tax resident in more than one jurisdiction then this element may be repeated and the data should be sent to the tax authority. It would also be advisable to mandate the use of the domestic country code for undocumented accounts, which will not be exchanged between Competent Authorities.*]

The complete information including all residence country codes that have been identified as applicable to the Reportable Person may be sent to every Competent Authority of a jurisdiction of residence so that there is an awareness of the possible need to resolve dual residence status or other issues attached to multiple reporting. It is recommended that the Competent Authority send a data record to each of the residence jurisdictions showing all reportable residence jurisdictions.

Alternatively, in certain circumstances the sending jurisdiction may choose to send data with only the residence country code of the receiving jurisdiction to each and may use a different method to exchange information relevant to multiple residence jurisdictions in accordance with the applicable legal instrument(s) if and when required.

IIb. TIN Type

Element	Attribute	Size	Input Type	Requirement
TIN		Min 1 char	cfc:TIN_Type	(Optional) Mandatory

This data element identifies the Tax Identification Number (TIN) used by the receiving tax administration to identify the Individual Account Holder. The TIN (if available) should be supplied as specified in the CRS.

Element	Attribute	Size	Input Type	Requirement
TIN	issuedBy	2-character	iso:CountryCode_Type	(Optional) Mandatory

This attribute identifies the jurisdiction that issued the TIN. If the issuing jurisdiction is not known then this may be left blank.

IIc. NamePerson_Type

Element	Attribute	Size	Input Type	Requirement
NamePerson_Type	nameType		stf:OECDNameType_EnumType	Optional

This data element allows the FI to report both the name at birth and the name after marriage.

OECDNameType_EnumType

It is possible for a CRS individual or entity to have several names. This is a qualifier to indicate the type of a particular name. Such types include nicknames (“nick”), names under which a party does business (“dba” a short name for the entity, or a name that is used for public acquaintance instead of the official business name) etc.

The possible values are:

- OECD201= SMFAliasOrOther (not used for CRS)
- OECD202= indiv
- OECD203= alias
- OECD204= nick
- OECD205= aka
- OECD206= dba
- OECD207= legal
- OECD208= atbirth

Element	Attribute	Size	Input Type	Requirement
PrecedingTitle			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
Title			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
FirstName			xsd:string	Validation

This data element is required for CRS reporting. If the reporting FI or tax administration transmitting the message does not have a complete first name for an Individual Account Holder or Controlling Person an initial or NFN ("No First Name") may be used here.

Element	Attribute	Size	Input Type	Requirement
FirstName	xnlNameType		xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
MiddleName			xsd:string	Optional

This data element allows for the Individual's Middle Name. The data is optional for CRS reporting; if the Reporting FI holds a Middle Name or initial it may be included here.

Element	Attribute	Size	Input Type	Requirement
MiddleName	xnlNameType		xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
NamePrefix			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
NamePrefix	xnlNameType		xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
LastName			xsd:string	Validation

This data element is required for CRS reporting. The reporting FI or tax administration transmitting the message must provide the Individual Account Holder's last name. This field can include any prefix or suffix legally used by the Account Holder.

As the element is a string it is possible to use this for a free format name or two last names although wherever possible the structured first name and last name should be used.

Element	Attribute	Size	Input Type	Requirement
LastName	xnlNameType		xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
GenerationIdentifier			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
Suffix			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
GeneralSuffix			xsd:string	Optional

IId. Address_Type

There are two options for Address type in the schema – AddressFix and AddressFree. AddressFix should be used for all CRS reporting unless the reporting FI or tax administration transmitting the message cannot define the various parts of the account holder's address.

This data element is the permanent residence address e.g. of the individual account holder. If the reporting FI or tax administration does not have a permanent residence address on file for the individual, then the address is the mailing address used by the financial institution to contact the individual account holder when the report is compiled.

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

This data element provides the country code associated with the account holder's address. [*For undocumented accounts the domestic country code will be used as no address is available. As the address requires another data item to be completed then "undocumented" could be used instead of an actual address.*]

Element	Attribute	Size	Input Type	Requirement
AddressFree			xsd:string	Optional*

This data element allows input of address information in free text. If the user chooses the option to enter the data required in a less structured way in

"AddressFree" all available address details shall be presented as one string of bytes, blank or "/" (slash) or carriage return-line feed used as a delimiter between parts of the address. *This option should only be used if the data cannot be presented in the AddressFix format.

NOTE: If the reporting FI or tax administration transmitting the message selects AddressFix, it will have the option of inputting the full street address of the account holder in the AddressFree element rather than using the related fixed elements. In this case, the city, subentity, and postal code information should still be entered in the appropriate fixed elements.

Element	Attribute	Size	Input Type	Requirement
AddressType	legalAddressType		stf:OECDLegalAddressType_EnumType	Optional

OECDLegalAddressType_EnumType

This is a datatype for an attribute to an address. It serves to indicate the legal character of that address (residential, business etc.)

The possible values are:

- OECD301= residentialOrBusiness
- OECD302= residential
- OECD303= business
- OECD304= registeredOffice
- OECD305= unspecified

Element	Attribute	Size	Input Type	Requirement
Street			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
BuildingIdentifier			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
SuiteIdentifier			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
FloorIdentifier			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
DistrictName			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
POB			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
PostCode			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
City			xsd:string	Validation

Element	Attribute	Size	Input Type	Requirement
CountrySubentity			xsd:string	Optional

The above data elements comprise the AddressFix type. The "City" data element is required for schema validation. The PostCode should always be included where it exists. Information pertaining to the account holder's street address may be entered here or in the AddressFree data element.

IIe. Nationality

Element	Attribute	Size	Input Type	Requirement
Nationality		2-character	iso:CountryCode_Type	Optional (non-CRS)

This data element is not required for CRS and should not be completed.

IIf. BirthInfo

Element	Attribute	Size	Input Type	Requirement
BirthDate			xsd:date	(Optional) Mandatory

This data element identifies the date of birth of the Individual Account Holder. The date of birth may be left empty when it is not required to be reported under the CRS (this may occur for Pre-existing Accounts if the date of birth is not available in the records of the Reporting Financial Institution and is not otherwise required to be collected by such Reporting Financial Institution under domestic law).

The data format is YYYY-MM-DD.

The three data elements below apply specifically to the place of birth and may be provided in accordance with CRS guidance where the financial institution is required to obtain and report the information under domestic law, and it is available in its electronically searchable records.

Element	Attribute	Size	Input Type	Requirement
City			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
CitySubentity			xsd:string	Optional

Element	Attribute	Size	Input Type	Requirement
CountryInfo				Optional

This data element gives a choice between a current jurisdiction (identified by 2-character country code) or a former jurisdiction (identified by name). One or other should be supplied if place of birth is reported, together with City or City and CitySubentity.

Element	Attribute	Size	Input Type	Requirement
CountryCode		2-character	iso:CountryCode_Type	Optional

Element	Attribute	Size	Input Type	Requirement
FormerCountryName			xsd:string	Optional

III. OrganisationParty_Type

This complex type identifies the name of an Account Holder that is an Entity as opposed to an Individual.

It is comprised of the following four data elements:

Element	Attribute	Size	Input Type	Requirement
ResCountryCode		2-character	iso:CountryCode_Type	(Optional) Mandatory

Element	Attribute	Size	Input Type	Requirement
IN		Min 1 char	crs: OrganisationIN_Type	(Optional) Mandatory

Element	Attribute	Size	Input Type	Requirement
Name			cfc:NameOrganisation_Type	Validation

Element	Attribute	Size	Input Type	Requirement
Address			cfc:Address_Type	Validation

IIIa. ResCountryCode

Element	Attribute	Size	Input Type	Requirement
ResCountryCode		2-character	iso:CountryCode_Type	(Optional) Mandatory

This data element describes the tax residence country code for the organisation reporting or being reported upon.

IIIb. Entity IN (OrganisationIN_Type)

Element	Attribute	Size	Input Type	Requirement
IN		Min 1 char	crs: OrganisationIN_Type	(Optional) Mandatory

This data element provides the identification number (IN) used by the sending and/or receiving tax administration to identify the Entity Account Holder. For CRS this may be the US GIIN, a TIN, company registration number, Global Entity Identification Number (EIN) or other similar identifying number specified by the tax administration.

This data element can be repeated if a second IN is present.

Element	Attribute	Size	Input Type	Requirement
IN	issuedBy	2-character	iso:CountryCode_Type	Optional

This attribute describes the jurisdiction that issued the IN. If the issuing jurisdiction is not known then this may be left blank.

Element	Attribute	Size	Input Type	Requirement
IN	INType		xsd:string	Optional

This Attribute defines the type of identification number being sent (e.g. US GIIN, EIN, TIN). Possible values should normally be agreed between Competent Authorities.

IIIc. Organisation Name

Element	Attribute	Size	Input Type	Requirement
Name			cfc:NameOrganisation_Type	Validation

Legal name of the entity that is reporting or being reported on.

Element	Attribute	Size	Input Type	Requirement
Name	nameType		stf:OECDNameType_EnumType	Optional

IV. CRS Body

The CRS body comprises the Reporting FI and Reporting Group elements.

IVa. Reporting FI

Identifies the financial institution that maintains the reported financial account or that makes the reported payment.

Reporting FI or tax administration uses the OrganisationParty_Type to provide identifying information

Element	Attribute	Size	Input Type	Requirement
ReportingFI			crs:CorrectableOrganisationParty_Type	Validation

Element	Attribute	Size	Input Type	Requirement
DocSpec			stf:DocSpec_Type	Validation

DocSpec identifies the particular report within the CRS message being transmitted. It allows for identification of reports requiring correction (see also guidance on Corrections below).

IVb. ReportingGroup

This data element provides specific details about the CRS report being sent by the reporting FI or tax administration transmitting the message.

Although in the schema this element is repeatable, for CRS only one ReportingGroup for each CRSBody is to be provided. The AccountReport should be repeated as required.

Element	Attribute	Size	Input Type	Requirement
ReportingGroup			crs:CorrectableOrganisationParty_Type	Validation

The following four data elements comprise the Reporting Group:

Element	Attribute	Size	Input Type	Requirement
Sponsor			crs:CorrectableOrganisationParty_Type	Optional (non-CRS)

Where a Financial Institution uses a third party to submit information on their behalf for CRS this element is not used but contact details can be given in Element "Contact".

Element	Attribute	Size	Input Type	Requirement
Intermediary			crs:CorrectableOrganisationParty_Type	Optional (non-CRS)

IVc. Account Report

Element	Attribute	Size	Input Type	Requirement
AccountReport			crs:CorrectableOrganisationParty_Type	(Optional) Mandatory

AccountReport is mandatory under CRS *(except where the MessageTypeIndic CRS703 is used domestically to indicate that there is no data to report).* In all other instances AccountReport must be completed. AccountReport includes the following data elements under CorrectableAccoutReport_Type:

Element	Attribute	Size	Input Type	Requirement
DocSpec			stf:DocSpec_Type	Validation

DocSpec identifies the particular report within the CRS message being transmitted. It allows for identification of reports requiring correction. See guidance on Corrections and a description of DocSpec Type.

IVd. Account Number

Element	Attribute	Size	Input Type	Requirement
AccountNumber			crs:FIAccountNumber_Type	Validation

Provide the account number used by the financial institution to identify the account. If the financial institution does not have an account number then provide the functional equivalent unique identifier used by the financial institution to identify the account.

Mandatory for financial institutions that have an account number (including alpha numeric identifiers).

For example: The account number may be the account number of a Custodial Account or Depository Account; ii) the code (ISIN or other) related to a Debt or Equity Interest (if not held in a custody account); or iii) the identification code of a Cash Value Insurance Contract or Annuity Contract.

If exceptionally there is no account numbering system use NANUM for no account number as this is a Validation element.

This format for account number is the same as FATCA and can be used for structured account numbers as well as free format; a non-standard account identifier or an insurance contract number could be included here.

Element	Attribute	Size	Input Type	Requirement
AccountNumber	AcctNumberType		cfc:AcctNumberType_EnumType	Optional

There is an option to include information about the account number type as an enumeration. The possible values are:

- OECD601= IBAN International Bank Account Number (follows a known structure)
- OECD602= OBAN Other Bank Account Number
- OECD603= ISIN International Securities Information Number (follows a known structure)
- OECD604= OSIN Other Securities Information Number
- OECD605= Other Any other type of account number e.g. insurance contract

Where an IBAN or ISIN is available, it should be provided and the appropriate information about the account number type supplied.

Element	Attribute	Size	Input Type	Requirement
AccountNumber	UndocumentedAccount		xsd:boolean	(Optional) Mandatory

[*This attribute is for use in CRS domestic reporting to indicate that the account is undocumented.*]

Element	Attribute	Size	Input Type	Requirement
AccountNumber	ClosedAccount		xsd:boolean	(Optional) Mandatory

This attribute is for use in CRS reporting to indicate that the account is closed.

Element	Attribute	Size	Input Type	Requirement
AccountNumber	DormantAccount		xsd:boolean	Optional

This attribute may be used in CRS reporting to indicate that the account is dormant.

IVe. Account Holder

Element	Attribute	Size	Input Type	Requirement
AccountHolder			crs:AccountHolder_Type	Validation

For CRS this data element may identify an entity account holder who is

- a passive NFE with one or more controlling person that is a Reportable Person
- a CRS Reportable Person

As there is a choice of entering an individual, or an organisation plus AcctHolderType, (but one or other must be entered as the account holder), these are shown as Validation (choice) below.

Element	Attribute	Size	Input Type	Requirement
Individual			crs:PersonParty_Type	Validation (choice)

If the Account Holder reported is a natural person, report his/her identifying information here.

Element	Attribute	Size	Input Type	Requirement
Organisation			crs:OrganisationParty_Type	Validation (choice)

If the Account Holder reported is not a natural person, report the entity's identifying information here.

Element	Attribute	Size	Input Type	Requirement
AcctHolderType			crs:CrsAcctHolderType_EnumType	Validation (choice)

This data element identifies an entity account holder that is

- a passive NFE with one or more controlling person that is a Reportable Person
- a CRS Reportable Person
- a passive NFE that is a CRS Reportable Person

Complete only if the reported financial account is held by an entity or the reported payment is made to an entity described-above. Allowable entries for CRS:

- CRS101= Passive Non-Financial Entity with – one or more controlling person that is a Reportable Person
- CRS102= CRS Reportable Person
- CRS103= Passive Non-Financial Entity that is a CRS Reportable Person

IVf. Controlling Person

Element	Attribute	Size	Input Type	Requirement
ControllingPerson			crs:ControllingPerson_Type	(Optional) Mandatory

Provide the name of any Controlling Person of a Passive NFE that is a Reportable Person. Mandatory only if the entity Account Holder is a Passive NFE with one or more Controlling Persons who is are Reportable Persons. If the Passive NFE has more than one Controlling Person that is a Reportable Person, then the name of all such Reportable Persons must be reported.

A separate report should be created with respect to each Reportable Jurisdiction that has been identified as a jurisdiction of residence of the Controlling Persons who are Reportable Persons. However, only information of the Reportable Persons of each Reportable Jurisdiction (including information of the Passive NFE and other associated data) should be included in the report.

Where an Entity Account Holder is a Reportable Person and is also a Passive NFE with one or more Controlling Persons that is a Reportable Person, and both the Entity and any of such Controlling Persons are resident in the same Reportable Jurisdiction, the information with respect to the account may be reported *(i)* as an account of an Entity that is a Passive NFE with a Controlling Person that is a Reportable Person, or *(ii)* as such and as an account of an Entity that is a Reportable Person (i.e. as if were information with respect to two accounts).

Where none of such Controlling Persons is resident in the same Reportable Jurisdiction as the Entity, the information with respect to the account must nevertheless be reported as an account of an Entity that is a Reportable Person.

Element	Attribute	Size	Input Type	Requirement
Individual			crs:PersonParty_Type	Validation

Defines a Controlling Person with its Name, Address, Country of Residence.

Element	Attribute	Size	Input Type	Requirement
CtrlgPersonType			crs:CrsCtrlgPersonType_EnumType	(Optional) Mandatory

This data element allows the identification of the type of each Controlling Person ("CP") when available, by use of the attribute "ControllingPersonType" with the following options:

a) CP of legal person – ownership

b) CP of legal person – other means

c) CP of legal person – senior managing official

d) CP of legal arrangement – trust – settlor

e) CP of legal arrangement – trust – trustee

f) CP of legal arrangement – trust – protector

g) CP of legal arrangement – trust – beneficiary

h) CP of legal arrangement – trust – other

i) CP of legal arrangement – other – settlor-equivalent

j) CP of legal arrangement – other – trustee-equivalent

k) CP of legal arrangement – other – protector-equivalent

l) CP of legal arrangement – other – beneficiary-equivalent

m) CP of legal arrangement – other – other-equivalent

Allowable entries for CRS:

- CRS801= CP of legal person – ownership
- CRS802= CP of legal person – other means
- CRS803= CP of legal person – senior managing official
- CRS804= CP of legal arrangement – trust – settlor
- CRS805= CP of legal arrangement – trust – trustee
- CRS806= CP of legal arrangement – trust – protector
- CRS807= CP of legal arrangement – trust – beneficiary
- CRS808= CP of legal arrangement – trust – other
- CRS809= CP of legal arrangement – other – settlor-equivalent
- CRS810= CP of legal arrangement – other – trustee-equivalent
- CRS811= CP of legal arrangement – other – protector-equivalent
- CRS812= CP of legal arrangement – other – beneficiary-equivalent
- CRS813= CP of legal arrangement – other – other-equivalent

IVg. Account Balance

Element	Attribute	Size	Input Type	Requirement
AccountBalance			cfc:MonAmnt_Type	Validation

Provide the account balance or value of the reported financial account.

- Depository and custodial accounts. The account balance or value shall be in accordance with CRS guidance.
- Cash value and annuity contracts. The cash value insurance or annuity contract is the balance or value of the account.
- Debt or equity accounts. The account balance is the value of the debt or equity interest that the account holder has in the financial institution.
- Enter Zero if account has been closed, in combination with account closed attribute.
- Numeric characters (digits). Account balance is entered with 2-digit fractional amounts of the currency in question. For example, USD 1 000 would be entered as 1000.00.

Element	Attribute	Size	Input Type	Requirement
AccountBalance	currCode	3 characters	iso:currCode_Type	Validation

All amounts must be accompanied by the appropriate 3 character currency code[2] based on the ISO 4217 Alpha 3 standard.

IVh. Payment

Element	Attribute	Size	Input Type	Requirement
Payment			crs:Payment_Type	Optional

Provide information on payment made to the reported financial account during the reporting period.

2. The following disclaimer refers to all uses of the ISO currency code list in the CRS schema: *For practical reasons, the list is based on the ISO 4217 Alpha 3 currency 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.*

Payment information is a repeating element, if more than one payment type needs to be reported.

For example payment types may include the following:

Depository accounts:

- The aggregate gross amount of interest paid or credited to the account during the calendar year.

Custodial accounts:

- The aggregate gross amount of dividends paid or credited to the account during the calendar year (or relevant reporting period);
- The aggregate gross amount of interest paid or credited to the account during the calendar year (or relevant reporting period);
- The gross proceeds from the sale or redemption of property paid or credited to the account during the calendar year (or relevant reporting period) with respect to which the FFI acted as a custodian, broker, nominee, or otherwise as an agent for the account holder and;
- The aggregate gross amount of all other income paid or credited to the account during the calendar year (or relevant reporting period).

Debt or equity accounts:

- The aggregate gross amount of payments paid or credited to the account during the calendar year (or relevant reporting period), including redemption payments.

Cash value insurance and annuity contract accounts:

- The aggregate gross amount of payments paid or credited to the account during the calendar year (or relevant reporting period), including redemption payments.

Element	Attribute	Size	Input Type	Requirement
Type			crs:CrsPaymentType_EnumType	Validation

Select the proper code to identify the payment type. Specific payment types listed are:

- CRS501= Dividends
- CRS502= Interest
- CRS503= Gross Proceeds/Redemptions
- CRS504= Other – CRS. (Example: other income generated with respect to the assets held in the account)

Element	Attribute	Size	Input Type	Requirement
PaymentAmnt			cfc:MonAmnt_Type	Validation

Payment Amounts are entered with 2-digit fractional amounts of the currency in question. For example, USD 1 000 would be entered as 1000.00.

Element	Attribute	Size	Input Type	Requirement
PaymentAmnt	currCode	3 characters	iso:currCode_Type	Validation

All payment amounts must be accompanied by the appropriate 3 character currency code based on the ISO 4217 Alpha 3 standard.

IVi. Pool Report

Element	Attribute	Size	Input Type	Requirement
PoolReport			ftc:CorrectablePoolReport_Type	Optional (Non-CRS)

Pool reporting is not applicable to CRS.

Transliteration

Where transliteration is required because sending and receiving jurisdictions do not use a common alphabet, Competent Authorities may agree how they will undertake such transliteration. If there is no such agreement, then the sending jurisdiction should, if so requested, transliterate from its domestic alphabet or literation to a Latin alphabet aligned with international standards for transliteration (for example as specified in ISO 8859). The sending jurisdiction may send designatory data (e.g. name or address) in both domestic alphabet or literation and separately in Latin alphabet within each account record if they so choose. The receiving jurisdiction should also be prepared to transliterate between Latin and its own domestic alphabet or literation.

Guidance on the correction process for Common Reporting Standard

In the course of AEOI, the sending jurisdiction may need to correct some elements of data previously sent. The section below describes how to make automatic corrections by sending a file of corrected data that can be processed in the same systems as the original data that was received. Reference to corrections also includes deletion of data elements in the following section.

If the whole of a data file is to be completely replaced, there can be a cancellation of the first message, then a new message with a file of completely new data can be sent, with no link to the previous records apart from in the message header – "cancel and replace" not "correct".

(The Competent Authority may keep the original file to investigate reasons for the errors in the data that led to cancellation and issue of the replacement file.)

Technical Guidance

In order to identify the elements to correct, the top-level elements Reporting FI or Account Report include an element of type DocSpec_Type, which provides necessary information for corrections.

DocSpec Type

Element	Attribute	Size	Input Type	Requirement
DocSpec			stf:DocSpec_Type	Validation

DocSpec identifies the particular record within the CRS message being transmitted. It allows for identification of records that require correction. DocSpec_Type is comprised of the following elements:

Element	Attribute	Size	Input Type	Requirement
DocTypeIndic			stf:OECDDocTypeIndic_EnumType	Validation

This element specifies the type of data being submitted. Allowable entries are:

- OECD0= Resent Data (only to be used for resending the Reporting FI element)
- OECD1= New Data
- OECD2= Corrected Data
- OECD3= Deletion of Data
- OECD10= Resent Test Data (only to be used for resending the Reporting FI element)
- OECD11= New Test Data
- OECD12= Corrected Test Data
- OECD13= Deletion of Test Data

A message can contain either new records (OECD1) or corrections/deletions (OECD2 and OECD3), but should not contain a mixture of both. OECD10 – OECD13 should only be used during previously agreed-upon testing periods or after a bilateral discussion where both parties agree to testing. This is to help eliminate the possibility that test data could be co-mingled with "live" data.

Element	Attribute	Size	Input Type	Requirement
DocRefID		Minimum 1 character	xsd:string	Validation

A unique identifier for this document (i.e. one record and all its children data elements).

A correction (or deletion) must have a new unique DocRefID for future reference.

Element	Attribute	Size	Input Type	Requirement
CorrDocRefID		Minimum 1 character	xsd:string	Optional

The CorrDocRefID references the DocRefID of the element to be corrected/deleted. It must always refer to the latest reference of this Account-report (DocRefID) that was sent.

In this way, a series of corrections or amendments can be handled as each correction completely replaces the previous version. The CRS Correction examples below show how this works in practice.

Element	Attribute	Size	Input Type	Requirement
CorrMessageRefID		Minimum 1 character	xsd:string	Optional (Non-CRS)

Since the DocRefID is unique in space and time, this element is not used for CRS at the DocSpec level.

Uniqueness of MessageRefID and DocRefID

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

The identifier can contain whatever information the sender uses to allow identification of the particular report but should start with the sending country code as the first element for Competent Authority to Competent Authority transmission, then the year to which the data relates, then the receiving country code before a unique identifier.

e.g. FR2013CA123456789

The unique identifier in the DocRefID could be the reference used by the FI to report nationally, or a different unique reference created by the sending tax administration, but should in all cases start with the country code of the sending jurisdiction

e.g. FRFI286abc123xyz

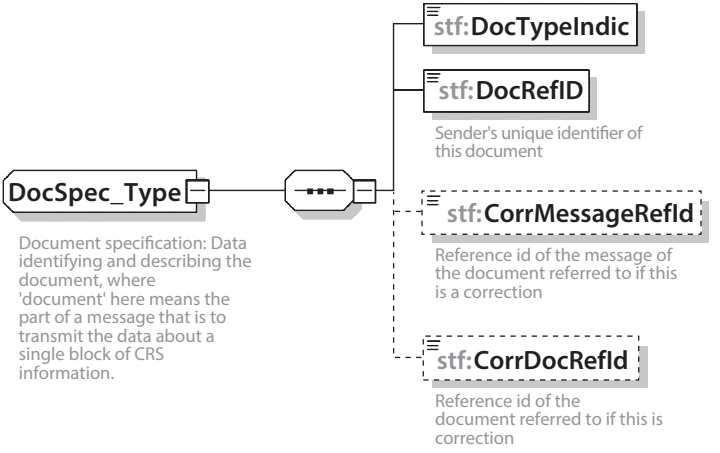
or FRabc123xyz

[*If the CRS schema is used for domestic reporting, the FI may similarly include an FI Identification Number in both MessageRefID and DocRefID which is recommended as good practice to ensure uniqueness in time and space and helps to link queries to source data.*]

MessageSpec and Corrections

Correction messages must have their own unique MessageRefID so they can also be corrected in the future. There is no equivalent for the DocSpecIndic when it comes to messages as a whole.

To cancel a complete message, the MessageSpec.CorrMessageRefID is not to be used. Instead, a correction message should be sent deleting all records of the erroneous message in these instances.



Correctable elements

In the CRS XML Schema, there are two correctable elements, the Reporting FI and the Account Report. Only these two elements are correctable in the CRS XML Schema. These two correctable elements must be considered separately for the correction process. The correction of one of the two correctable elements must not impact the other related correctable element.

If a correction targets a previously sent child element of a correctable element, the whole correctable element (the correctable element and all its children) must be resubmitted. This is applicable for both the Reporting FI and Account Report elements.

In order to be able to identify the elements to correct, the definition of these correctable elements includes an element of type DocSpec_Type, which includes the elements named DocTypeIndic, DocRefID and CorrDocRefID.

For a correction message, the following combinations of DocTypeIndic are permissible for the correctable elements, taking into account that the Account Report element is not mandatory:

		w/o Account Report	Account Report			
			OECD1	OECD2	OECD3	OECD0
Reporting FI	OECD1					
	OECD2	OK		OK	OK	
	OECD3	OK			OK	
	OECD0			OK	OK	

Combinations of DocTypeIndic for the correctable elements within a correction message

When a correction targets only the Account Report element and there is no modification of the related Reporting FI element, the DocTypeIndic "OECD0-Resend Data" is used for the Reporting FI element. This type is only allowed for Reporting FI element.

If the receiving Competent Authority encounters other combinations than those presented above, the receiving Competent Authority rejects the received file and returns a status message with the relevant error code (see CRS Status Message User Guide).

Structure of a correction message

A correction message has essentially the same structure as an initial message (with new data), as it follows the same schema. There is only a minor difference in the Message Header: the optional MessageTypeIndic can be set to CRS702 (CRS702= The message contains corrections for previously sent information).

As for the initial messages, all correction messages must have their own unique MessageRefID, while the Reporting FI element can have a DocTypeIndic value of OECD0, in case it has not been modified.

A corrected element will have a DocTypeIndic value of OECD2 or OECD3 (OECD1 for initial messages). Its CorrDocRefID references the DocRefID of the element to correct (this element is not specified in initial messages). Since the DocRefID is unique in time and space, the correcting records must have different DocRefIDs than those of the records being corrected.

A correction message can contain either corrections (OECD2) or deletions (OECD3) or both, as well as a resent Reporting FI element (OECD0), but may not contain new data (OECD1).

Relationship between messages

The following section describes how messages exchanged through the correction mechanism described above interact with one another. Since messages specify the reporting period to which they relate, a correction message may correct records originating from any previous initial or correction messages for the same reporting period.

Correction of an initial message

The correction of an initial message is the most common situation. The correction is used to correct the elements that were not correct (from a technical point or business point of view), or to delete elements from the initial message.

A new DocRefID is created for each correctable element and should follow the format described previously.

The CorrDocRefID must reference the DocRefID of the elements to be corrected/deleted from the initial message.

Correction of a correction message

Corrections of corrections are legitimate. In that case, the CorrDocRefID of the second correction of the message must reference the DocRefID of the first correction.

This is required in order to uniquely determine the order in which the receiving Competent Authority must handle the corrections. Otherwise, in case two corrections reference the same message and, for technical reasons (e.g. infrastructure or architecture constraints), arrive out of order, the receiving Competent Authority would first integrate the second correction, then the first one, effectively dismissing the second (and most recent) correction.

If the receiving Competent Authority receives messages that it considers as probably being out of order, it should – as a best practice – wait for some time before discarding the message, in case the previous messages arrive late. If the relevant message does not arrive, the receiving Competent Authority should contact the sending Competent Authority.

Common Reporting Standard Correction examples

The following sections provide examples of concrete correction scenarios, and highlight correction rules applicable to each of them.

Each example includes one or more figures to illustrate the situation. These figures omit most of the data, and only highlight the main areas of interest.

In the examples below, the following convention has been used to highlight the elements that need to be corrected or resent:

- The dark grey colour is used when the Reporting FI element has to be resent, even if no modifications are required. In this situation, the element is identified with the same DocRefID as the immediately preceding version of the Reporting FI element and the code OECD0 is used;
- The black colour is used to identify the elements that require being corrected (initial message) or are corrected (correction message).

First example: Two successive corrections of the same account

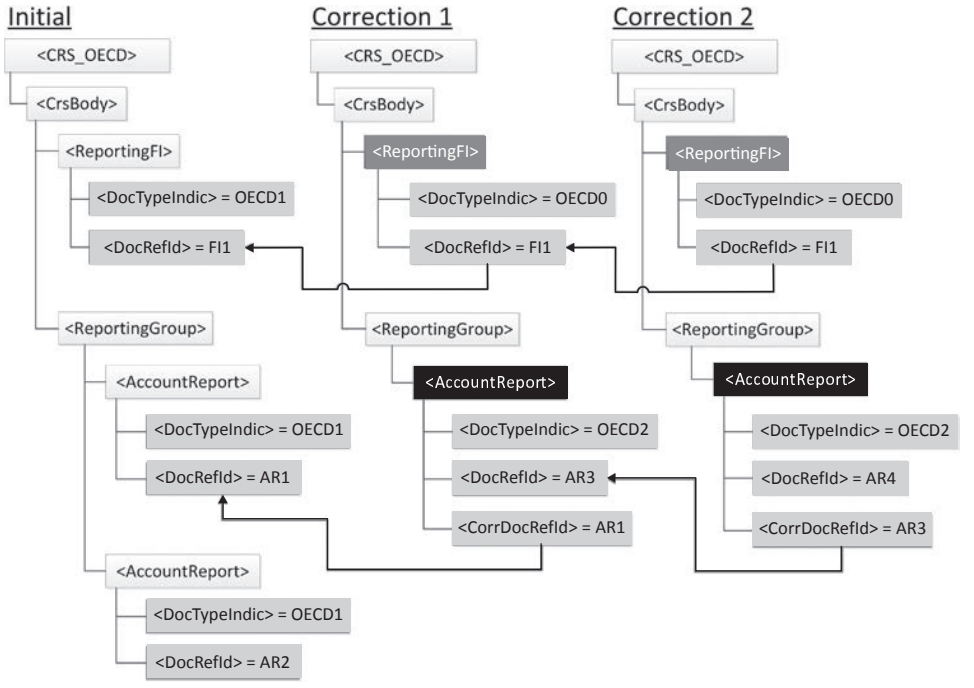
This example covers the following scenario:

- The sending Competent Authority sends an initial message with one Reporting FI and two Account Reports;
- It then sends a first correction message correcting the Payment Amount of the first Account Report;
- It finally sends a second correction message, correcting the Account Balance, yet again for the first Account Report.

There are four areas of interest here highlighted by the figure below:

- The CorrDocRefID of the Account Report refers to the immediately preceding message, not to any preceding one (in particular, not systematically to the first one);
- The DocTypeIndic of the Account Report is set to OECD1 within an initial message and to OECD2 within a correction message;
- The sending Competent Authority must always resend the Reporting FI associated to the Account Report being corrected, even though it did not require modifications. The DocTypeIndic is set to OECD0 and the DocRefID is the same as the immediately preceding message;
- The sending Competent Authority must only resend the corrected Account Report. The second one, which does not require corrections, is not part of the correction message.

Please note that the DocRefIDs provided in the figure examples have been simplified to make the figures easier to read.



Two successive corrections of the same account

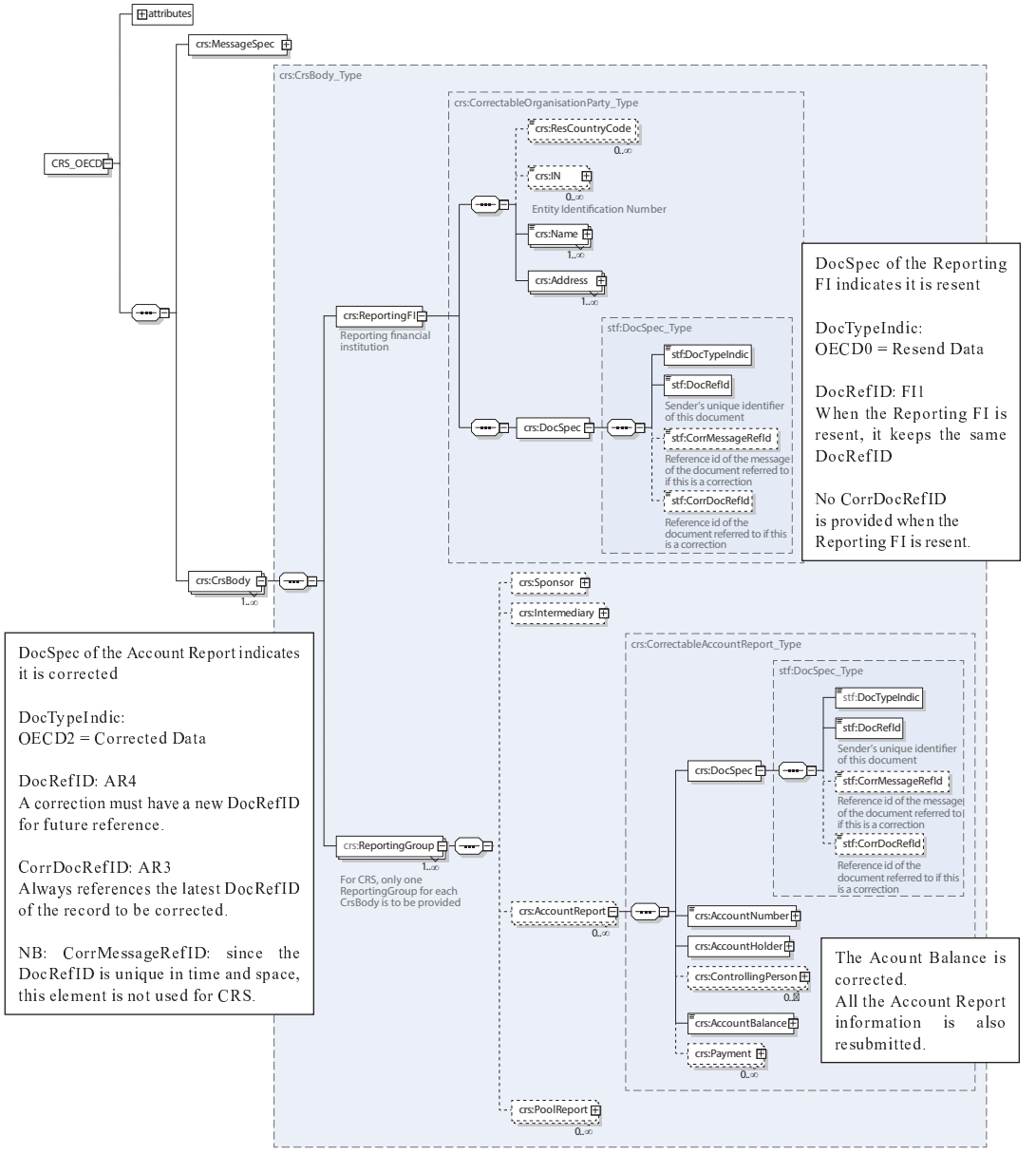
The DocRefID should follow the DocRefID format defined previously:

- It should start with the country code of the sending jurisdiction;
- It must be unique in time and space.

e.g. FR2013-11111 or or FRabc123xyz

Please note that these examples show exchanges between Competent Authorities, but the same correction process would apply if the CRS schema is used domestically.

The diagram below shows the message “Correction 2” within the CRS schema diagram (for the first example shown above).



Showing the "Correction 2" message within the CRS schema

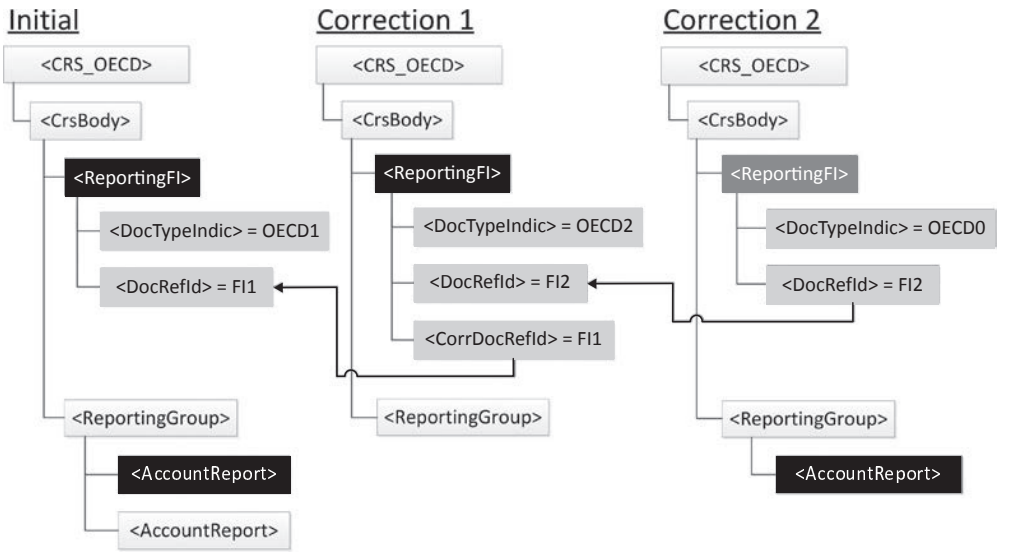
Second example: Two successive corrections of data from the same message

This example covers the following scenario:

- The sending Competent Authority sends an initial message with one Reporting FI and two Account Reports;
- It then sends a first correction message correcting the address of the Reporting FI;
- It finally sends a second correction message, correcting the first Account Report (new Account Payment).

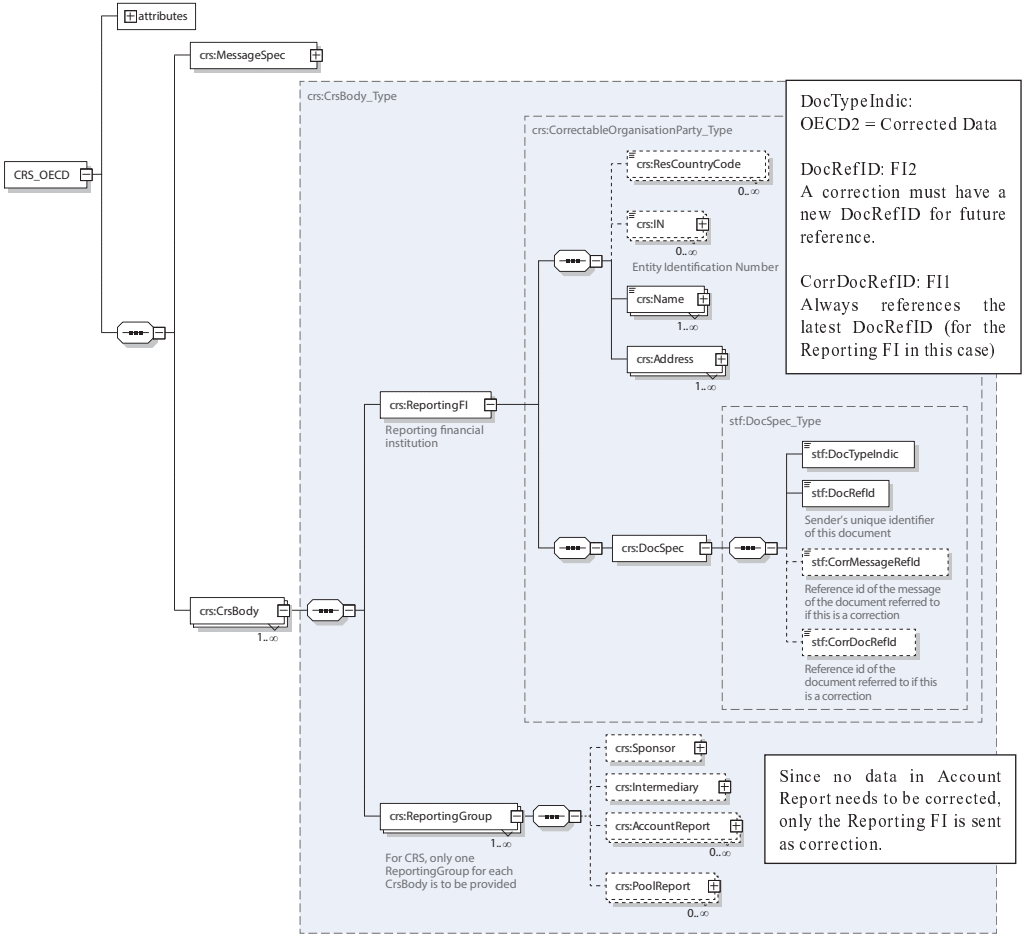
The figure below highlights the three areas of interest:

- The sending Competent Authority must always resend the Reporting FI associated to the Account Report being corrected, even though it did not require modifications. The DocTypeIndic is set to OECD0 and the DocRefID is the same as the immediately preceding message;
- The sending Competent Authority must only resubmit the corrected Account Report. The other Account Report, which does not require corrections, is not part of the correction message;
- The sending Competent Authority can send the corrected Reporting FI without the Account Reports if they do not require corrections.



Two successive corrections of data from the same message

The diagram below shows the message "Correction 1" within the CRS schema diagram (for the second example shown above).



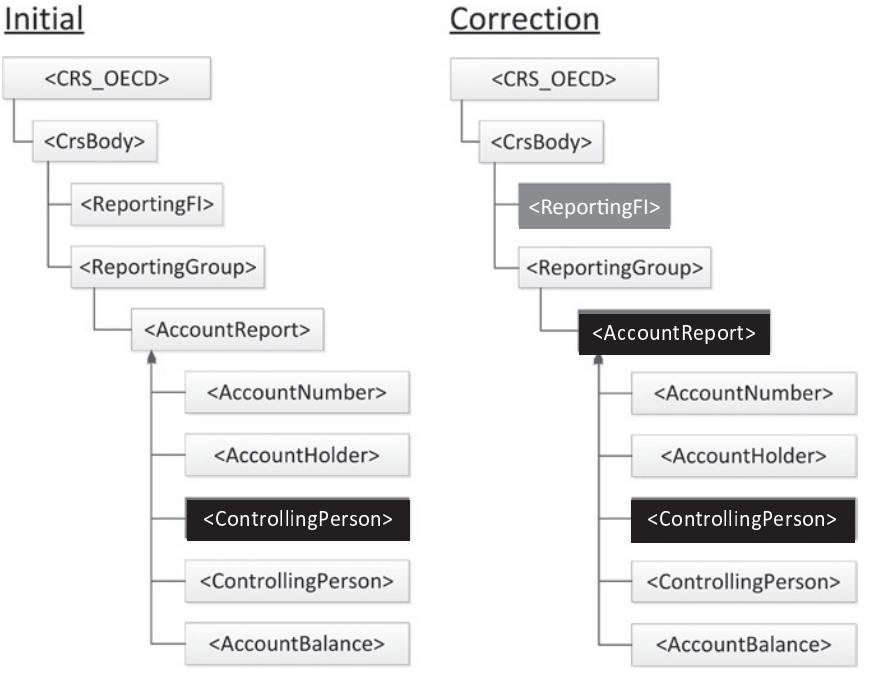
Showing the message "Correction 1" within the CRS schema

Third example: Correction of a child element of the Account Report

This example covers the following scenario:

- The sending Competent Authority sends an initial message with a Reporting FI, and an Account Report, composed of an Account Number, an Account Holder, two Controlling Persons (residing in the same jurisdiction) and an Account Balance element;
- It then wants to correct the Address of the first Controlling Person.

In this case, the sending Competent Authority must correct the Account Report from the initial message, and send it back with the corrected Controlling Person data. It must also include the Reporting FI since this element is mandatory, as well as the second Controlling Person, the Account Number, the Account Holder and the Account Balance; even though these elements did not require modifications. The figure below highlights this.



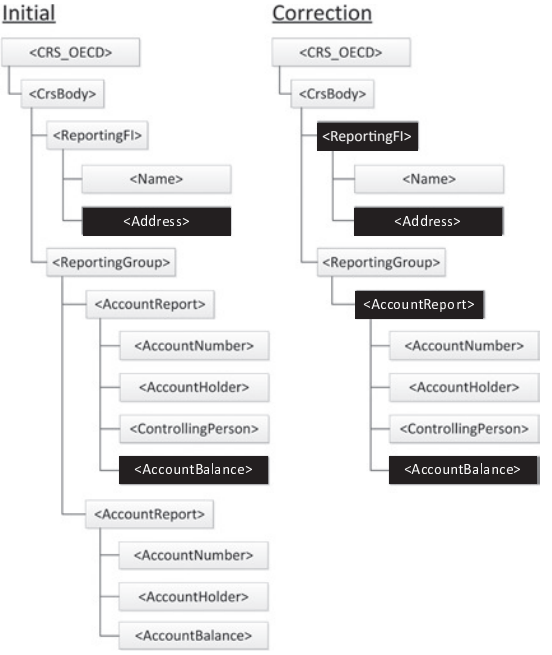
Correction of a child element of the Account Report

Fourth example: Correction of both correctable elements within the same message

This example covers the following scenario:

- The sending Competent Authority sends an initial message containing two Account Reports and the associated Reporting FI. The first Account Report is composed of an Account Number, an Account Holder, a Controlling Person and an Account Balance element. The second Account Report is composed of an Account Number, an Account Holder and an Account Balance element. The Reporting FI is composed of a Name and an Address element;
- It then wants to correct the Address of the Reporting FI and the Account Balance of the first Account Report.

In this case, the sending Competent Authority must correct the Reporting FI and the first Account Report from the initial message. The Reporting FI must contain the corrected Address as well as the Name. The first Account Report must contain the corrected Account Balance, as well as the Account Number, the Account Holder and the Controlling Person elements. The second Account Report is not resubmitted. The figure below highlights this.



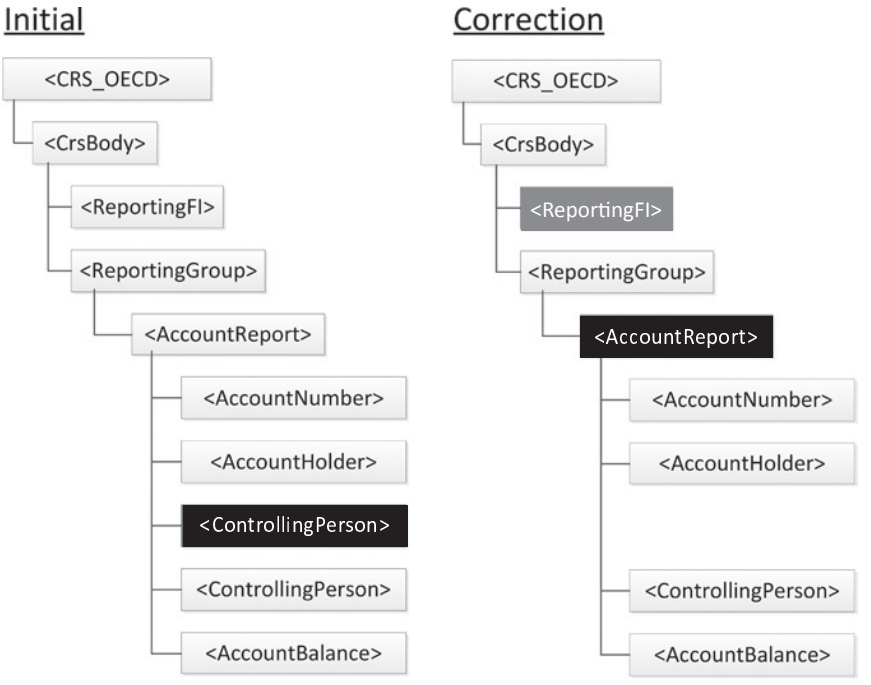
Correction of both correctable elements within the same message

Fifth example: Removal of a child element of the Account Report

This example covers the following scenario:

- The sending Competent Authority sends an initial message with a Reporting FI, and an Account Report composed of an Account Number, an Account Holder, two Controlling Person and an Account Balance element;
- It then wants to remove the first Controlling Person element.

In this case, the sending Competent Authority must correct the Account Report from the initial message, and send it back without the deleted Controlling Person element, but with the other Controlling Person, the Account Number, the Account Holder, the Account Balance elements, as well as the Reporting FI element, as this element is mandatory. The figure below highlights this.



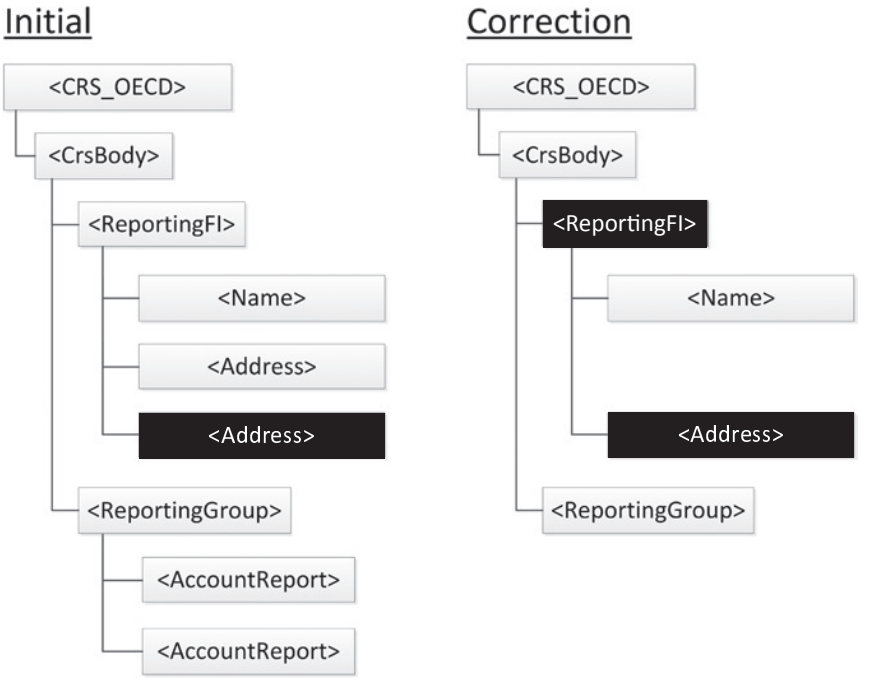
Removal of a child element of the Account Report

Sixth example: Removal of a child element of the Reporting FI

This example covers the following scenario:

- The sending Competent Authority sends an initial message with two Account Reports and the associated Reporting FI having a Name and two Addresses;
- It then wants to remove the second Address of the Reporting FI.

In this case, the sending Competent Authority must correct the Reporting FI from the initial message, and send it back without the deleted Address but with the other Address, and the Name. The Account Reports are not resubmitted. The figure below highlights this.



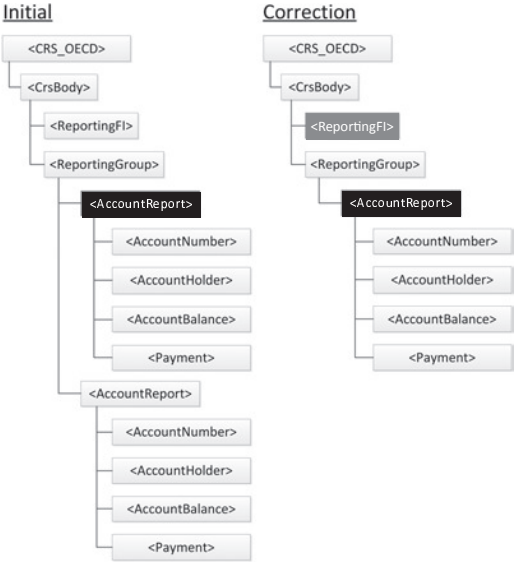
Removal of a child element of the Reporting FI

Seventh example: Removal of an Account Report

This example covers the following scenario:

- The sending Competent Authority sends an initial message with two Account Reports and the associated Reporting FI. Each Account Report is composed of an Account Number, an Account Holder and an Account Balance element;
- It then wants to remove the first Account Report.

In this case, the sending Competent Authority must correct the first Account Report indicating that it must be deleted (DocTypeIndic is set to OECD3), omit the second Account Report since it does not require corrections, and send it back with the child elements of the corrected Account Report as well as the Reporting FI since this element is mandatory. The figure below highlights this.



Removal of an Account Report

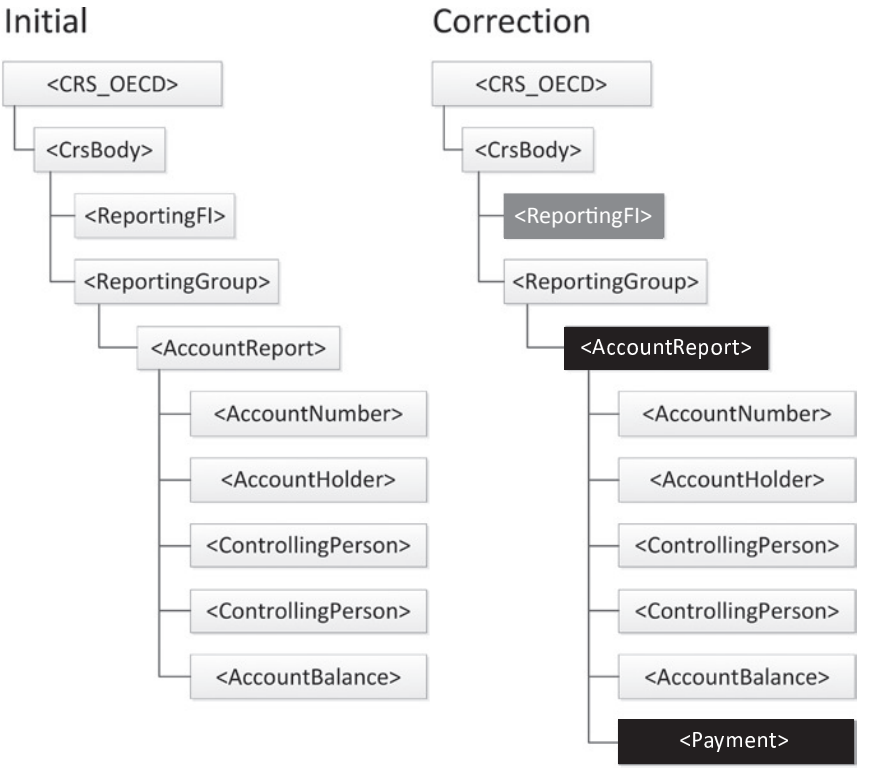
An exception can occur if the correction message removes only the Reporting FI, without the associated Account Reports. In this case, the deletion of the Reporting FI must be rejected, as a Reporting FI must always be associated to an Account Report. The removal of a Reporting FI element is allowed only if all the associated Account Reports have been already removed (either in same message or in previous messages).

Eighth example: Creation of a child element

This example covers the following scenario:

- The sending Competent Authority sends an initial message containing an Account Report and the associated Reporting FI. The Account Report is composed of an Account Number, an Account Holder, two Controlling Persons, and an Account Balance element;
- It then wants to add a Payment element to the Account Report.

In this case, the sending Competent Authority must correct the Account Report from the initial message, specifying a new Payment element and send it back with the Account Number, the Account Holder, two Controlling Persons, and the Account Balance elements, as well as the Reporting FI element, since this element is mandatory. The figure below highlights this.



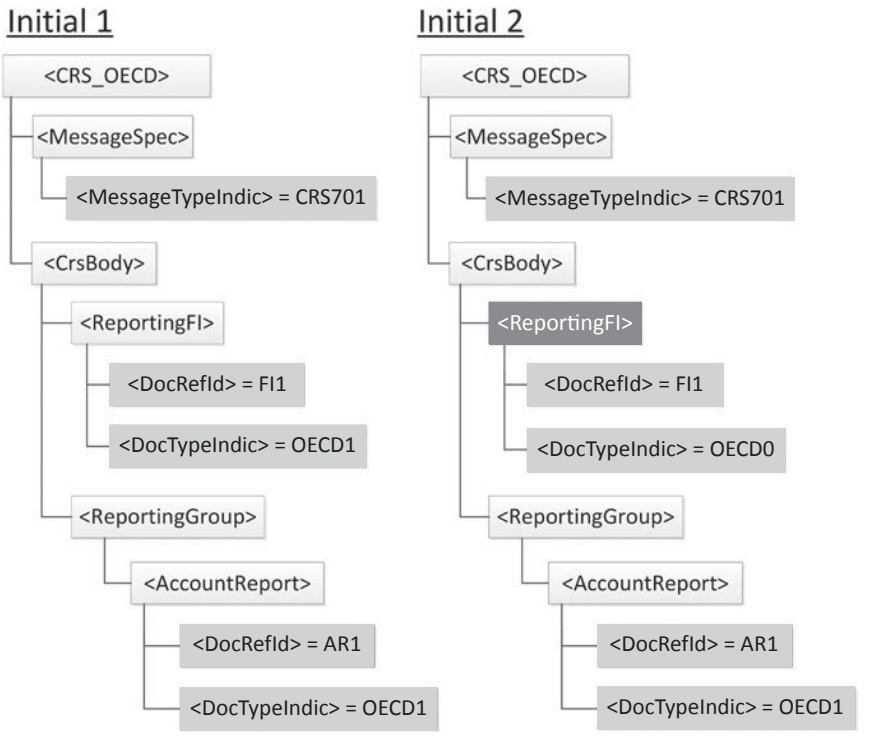
Creation of a child element

Ninth example: Adding an Account Report for an existing Reporting FI

This example covers the following scenario:

- The sending Competent Authority sends an initial message with one Account Report and the associated Reporting FI;
- It then wants to send another Account Report.

In this case, the sending Competent Authority creates a new initial message, with only the new Account Report and the already sent Reporting FI. The figure below highlights this.



Adding an Account Report for an existing Reporting FI

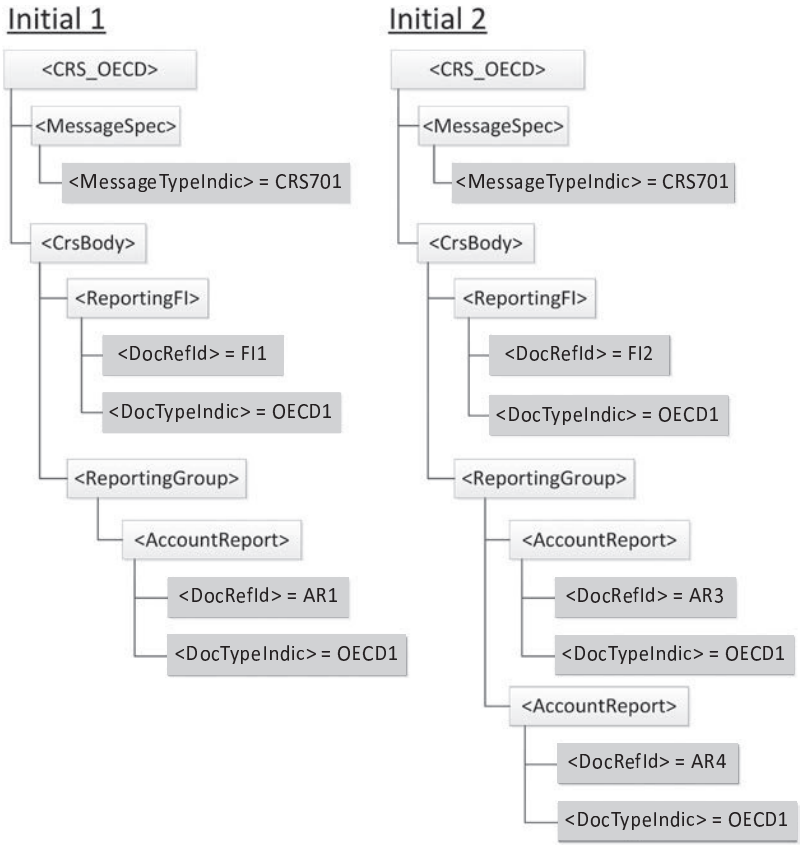
This scenario occurs only in specific circumstances, such as late reporting or in case of split messages.

Tenth example: Adding a new Reporting FI with its Account Reports

This example covers the following scenario:

- The sending Competent Authority sends an initial message with one Account Report and the associated Reporting FI;
- It then wants to send another Reporting FI with two Account Reports.

In this case, the sending Competent Authority creates a new initial message, with only the new Reporting FI and the two Account Reports. The figure below highlights this.

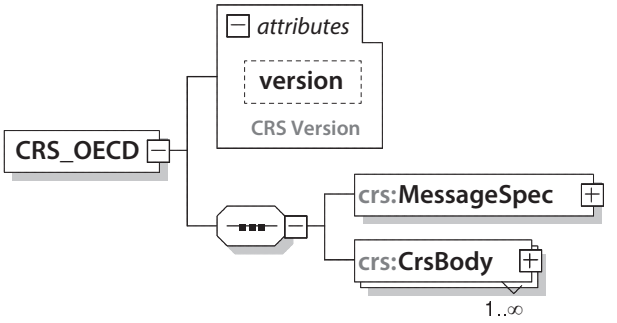


Adding a new Reporting FI with its Account Reports

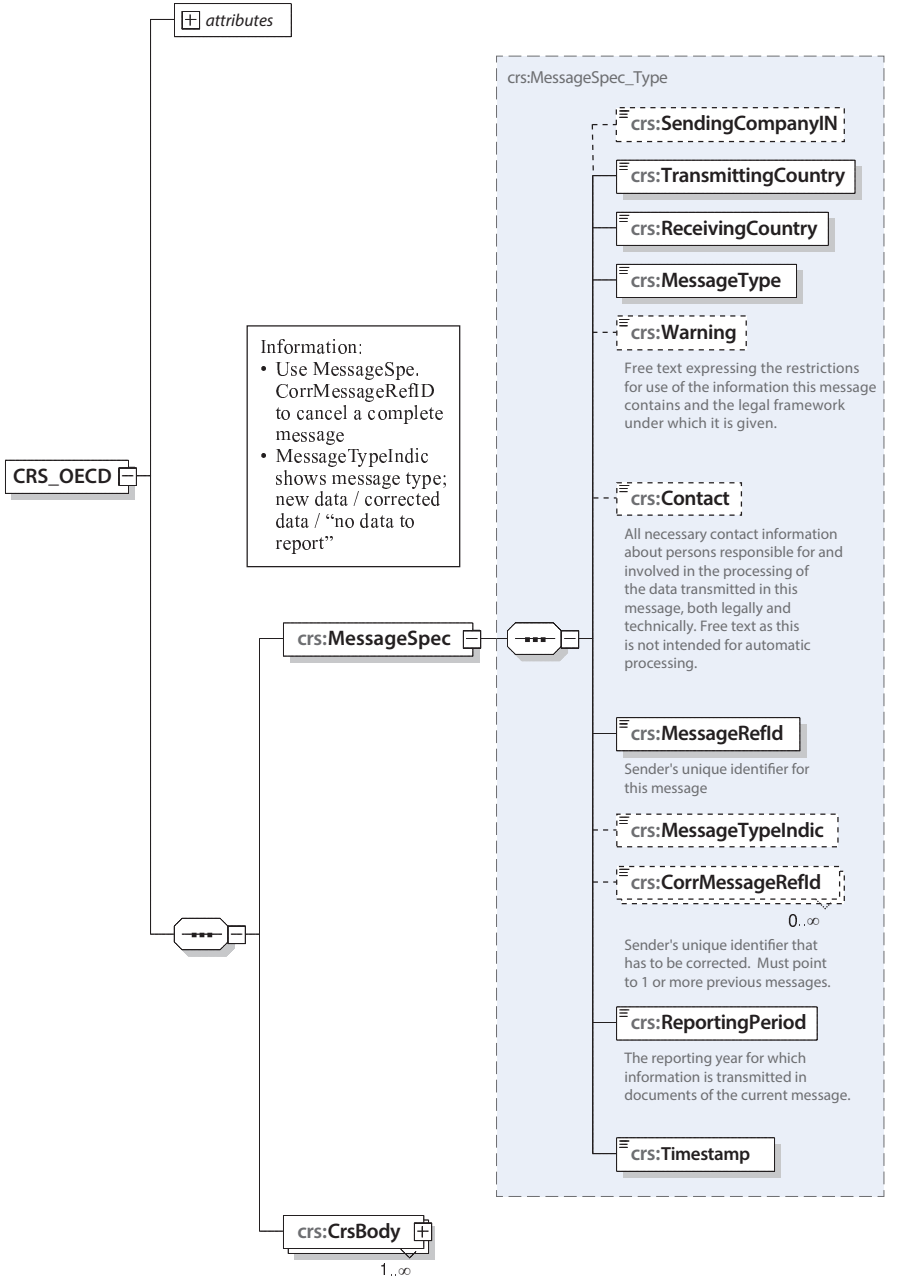
As in the previous example, this scenario occurs only in specific circumstances, such as late reporting or in case of split messages.

Appendix A

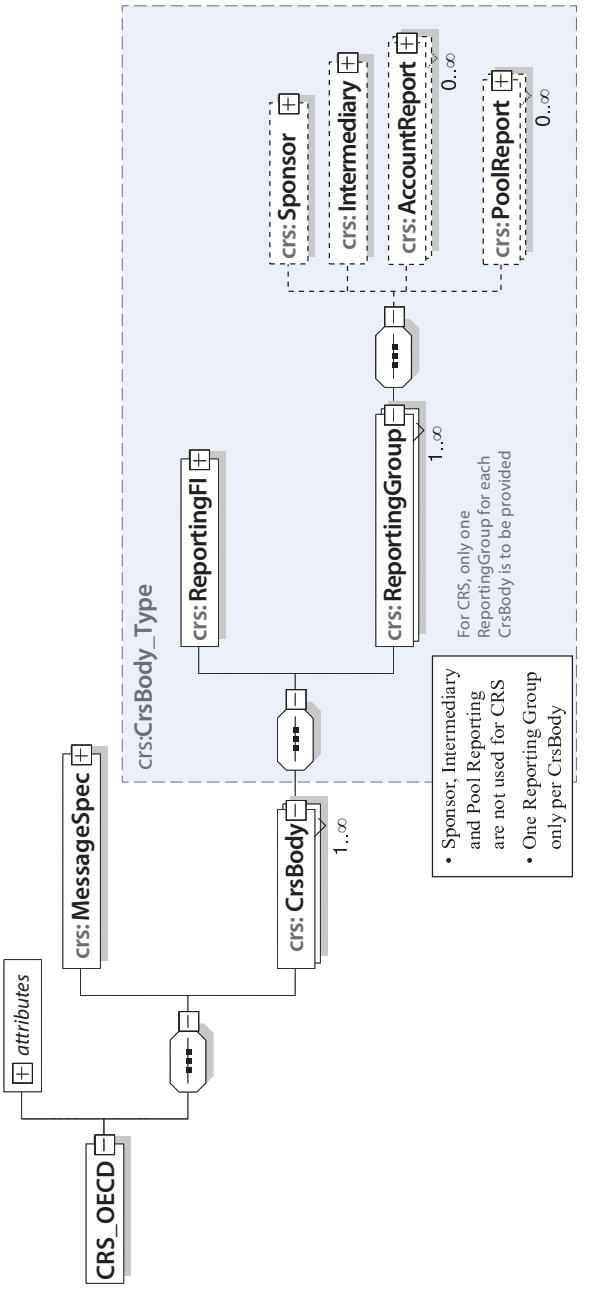
CRS XML Schema v. 1.0 Diagrams



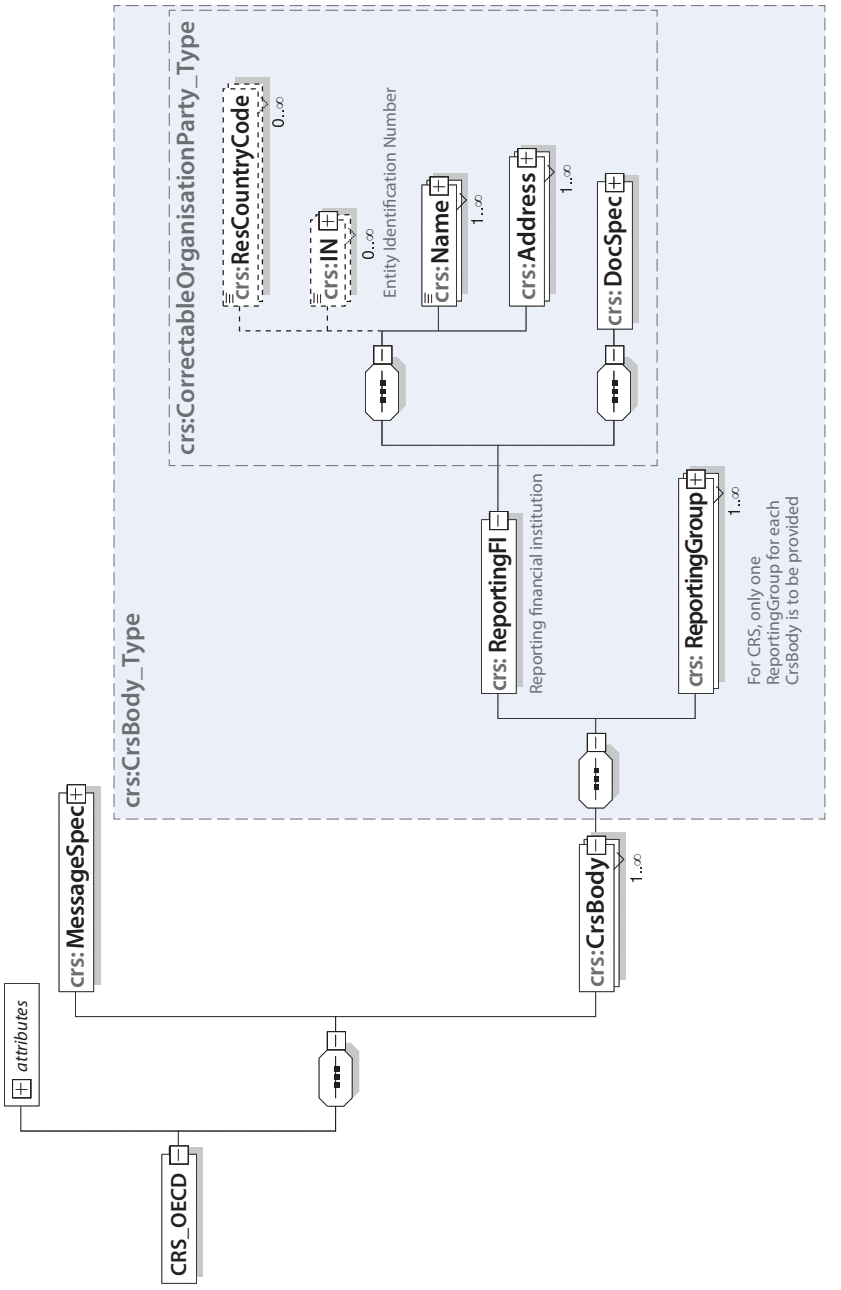
Message Header (Section I)



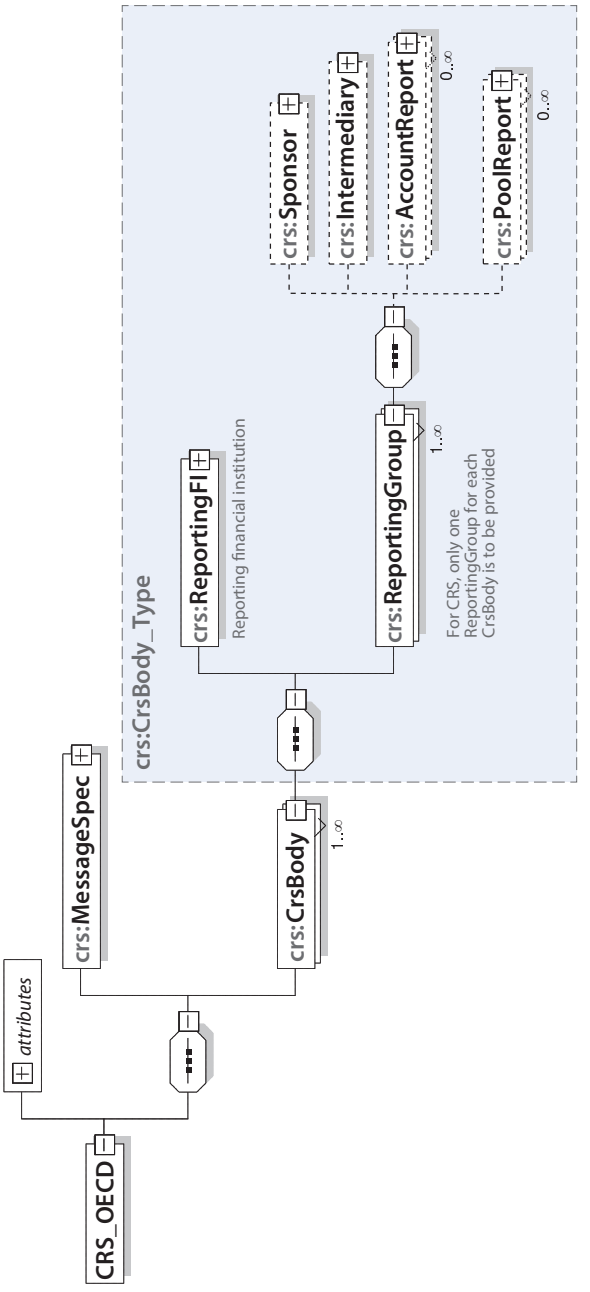
CRS Body (Section IV)



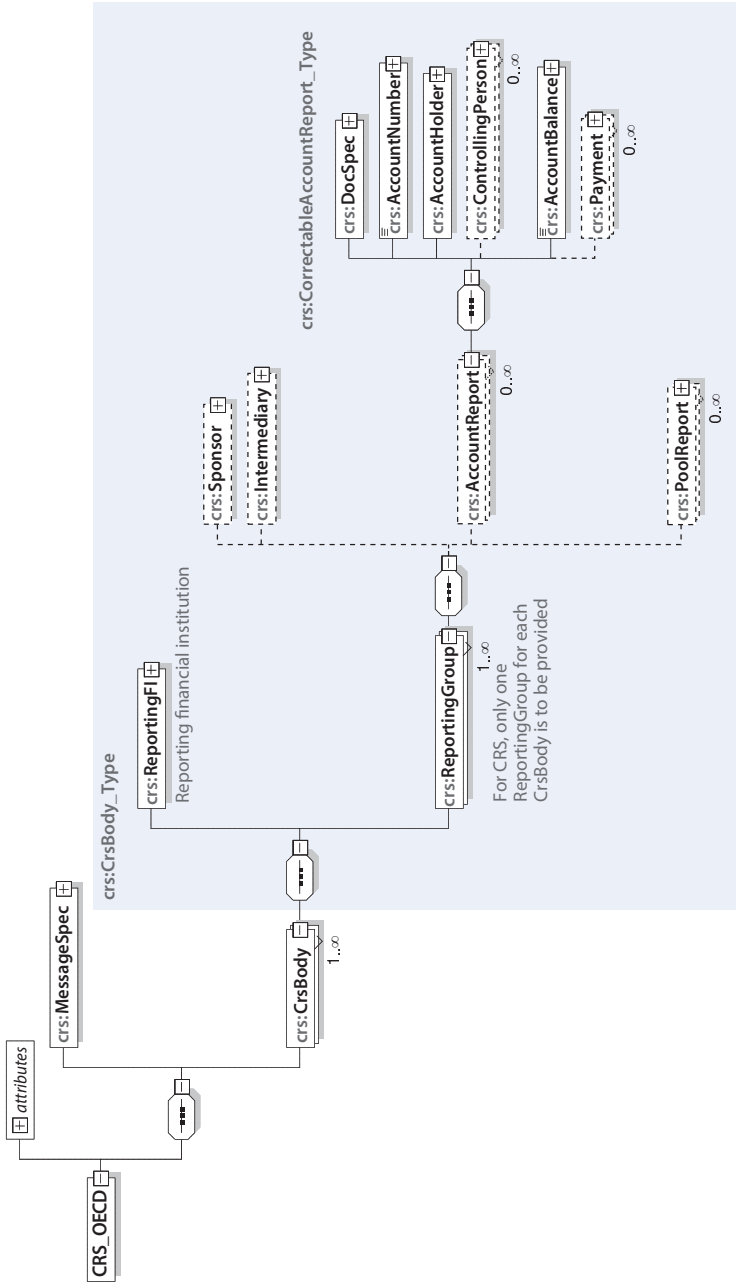
Reporting FI (Section IVa)



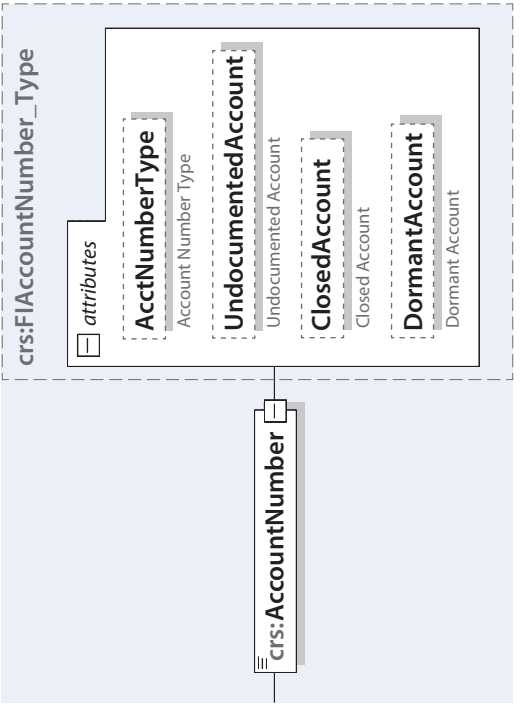
Reporting Group (Section IVb)



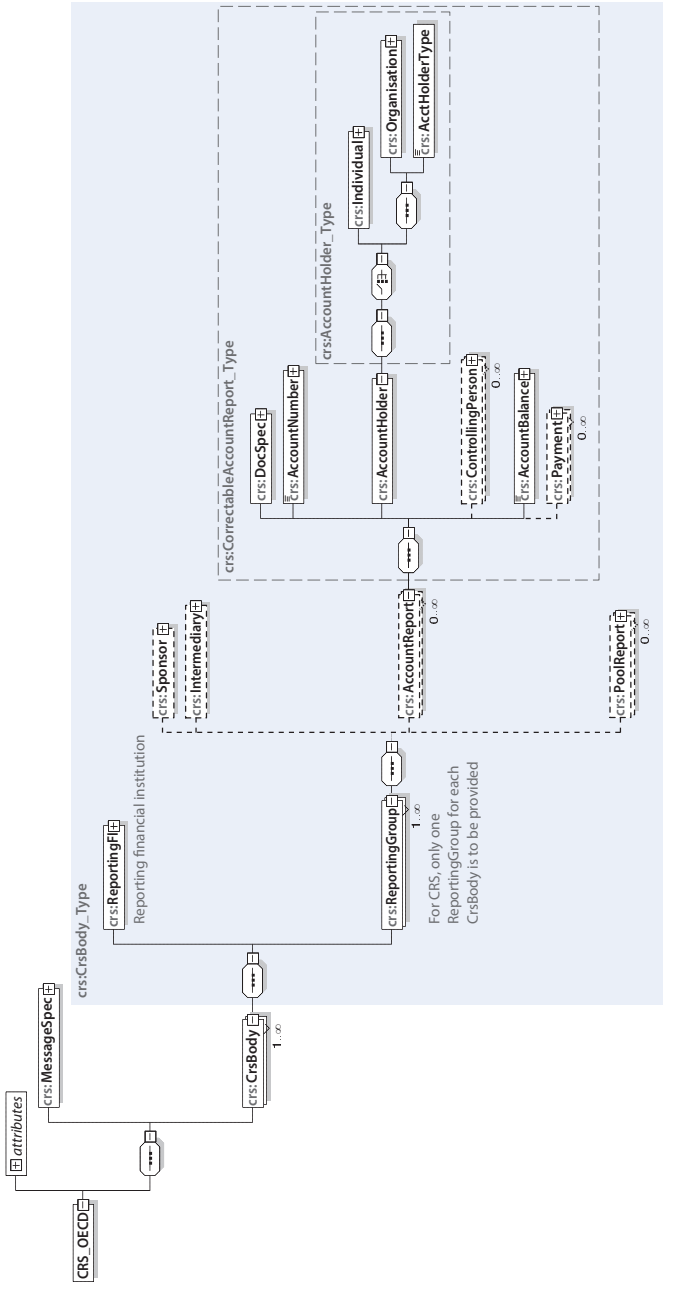
Account Report (Section IVc)



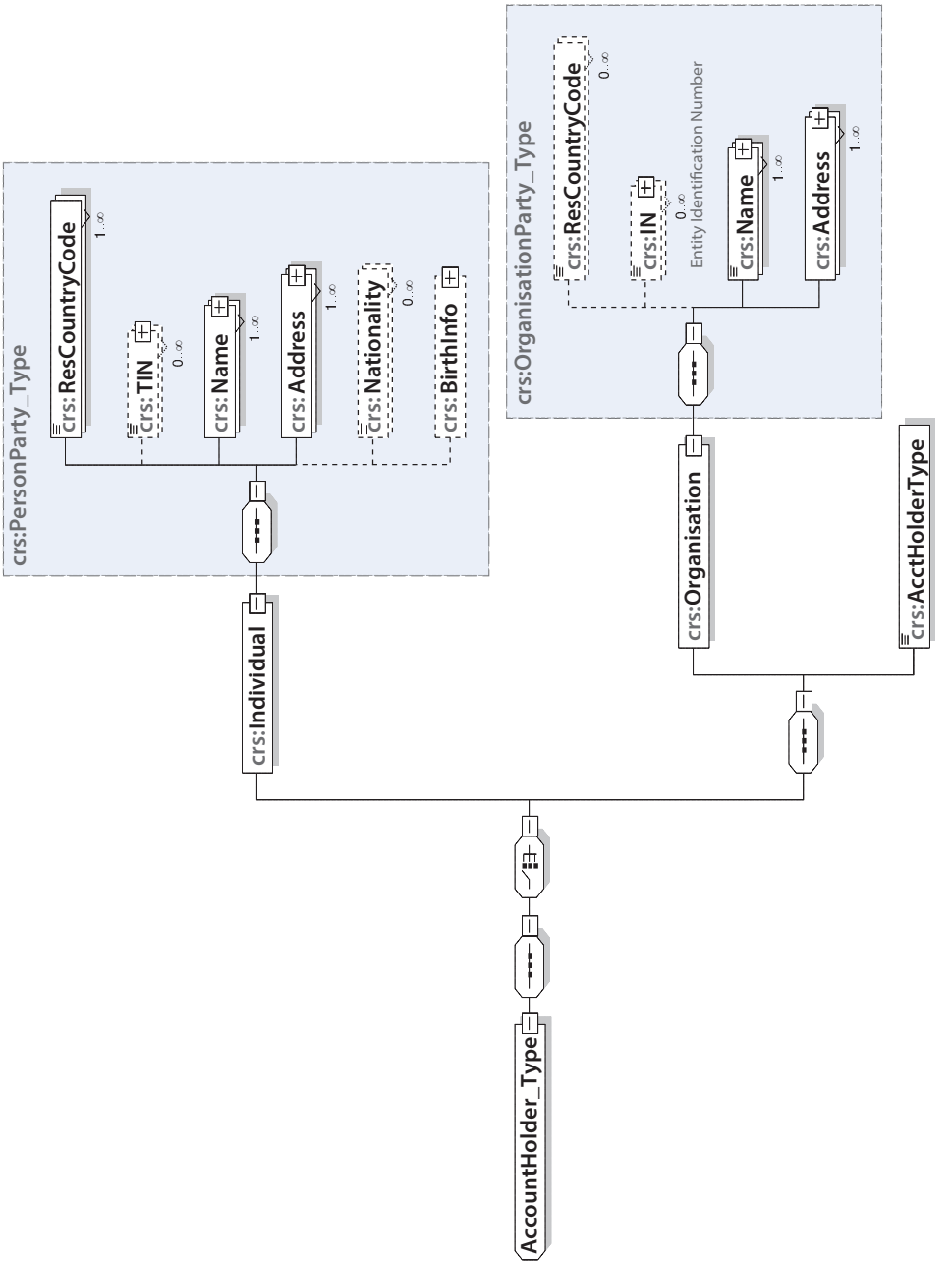
Account Number Type (Section IVd)



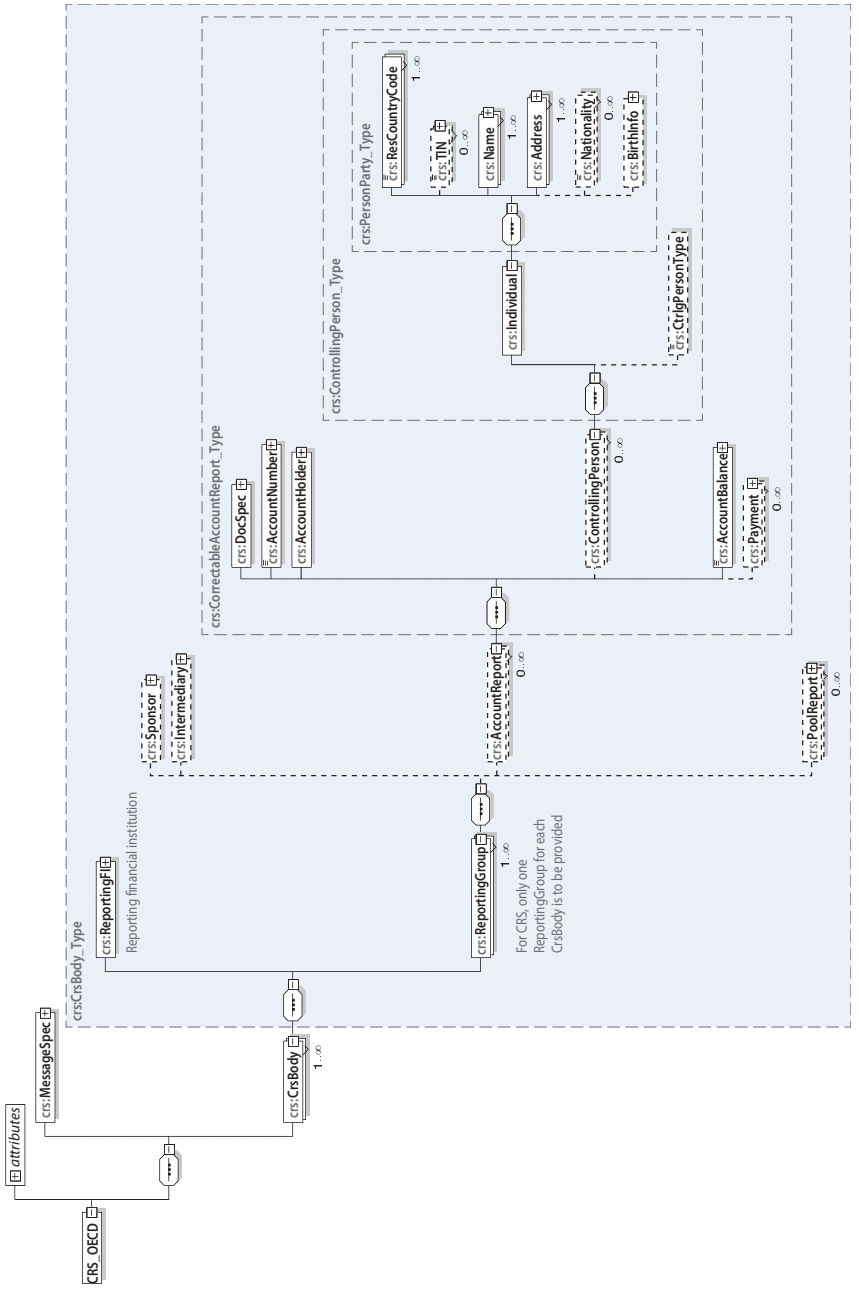
Account Holder (Section IVe)



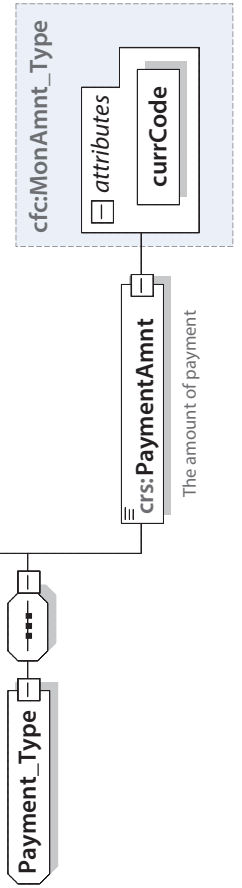
Individual/Organisation Account Holders (Section IVe)



Controlling Person (Section IVf)

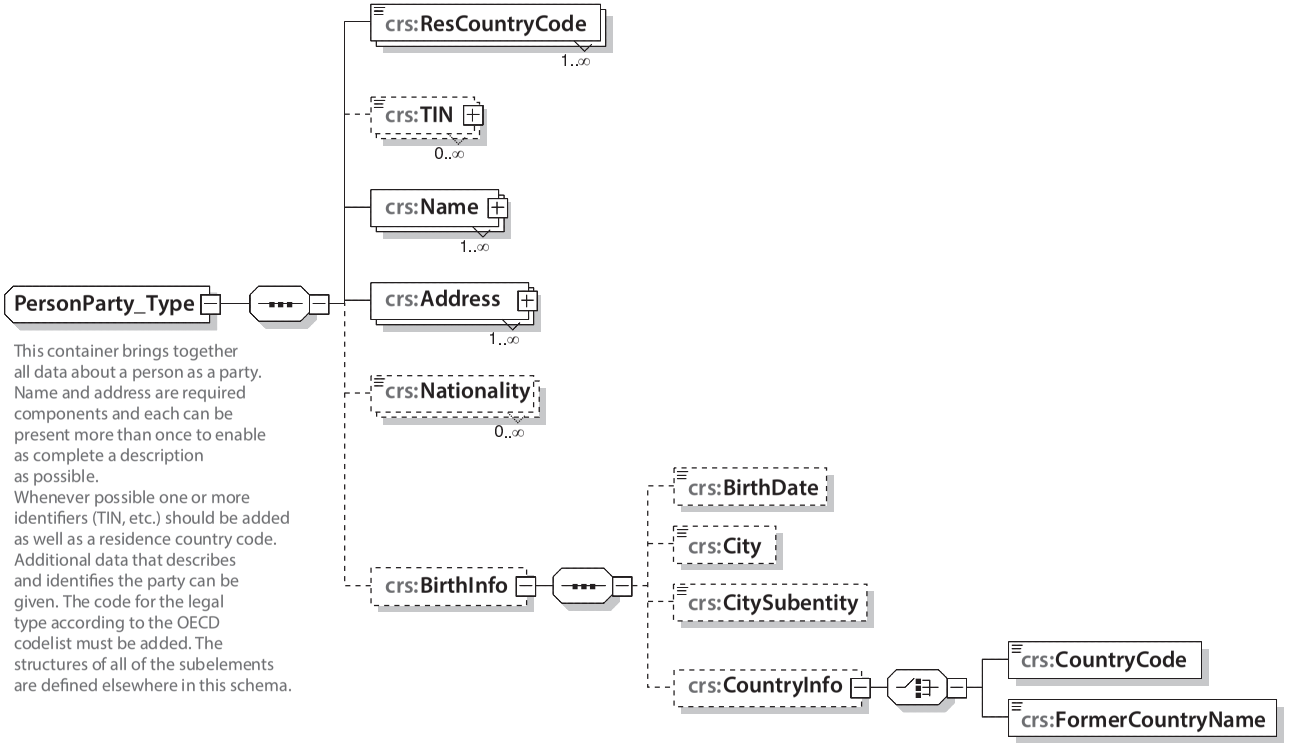


Payment type (Section IVh)



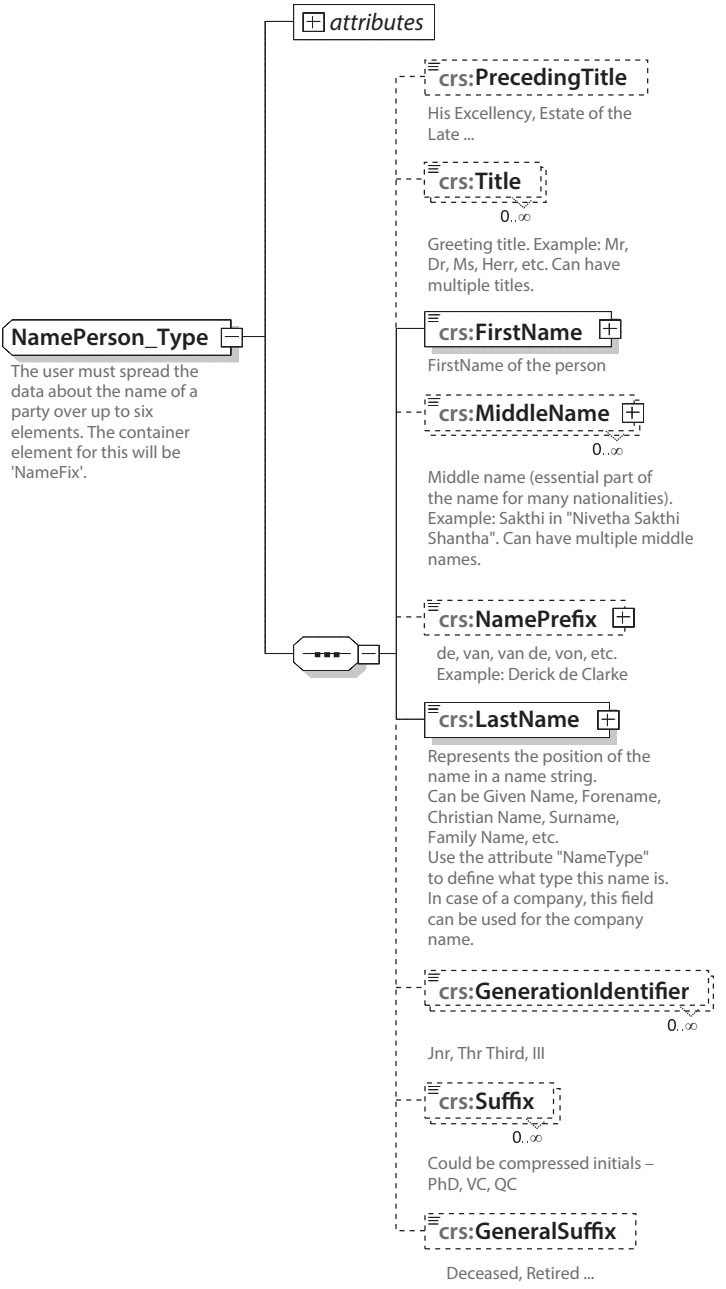
For practical reasons, the CurrencyCode list is based on the ISO 4217 currency code list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status 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.

Person Party Type (Section II)

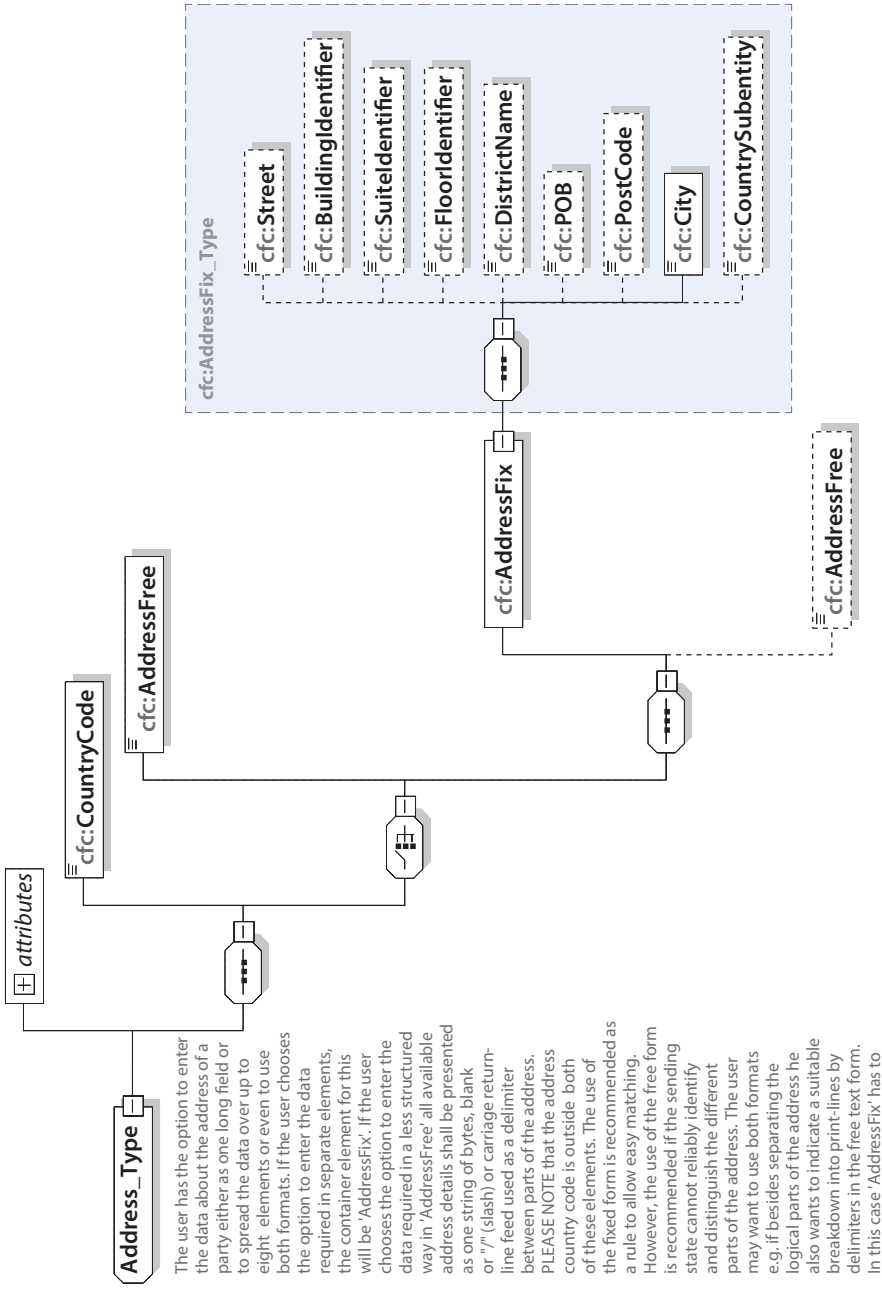


For practical reasons, the ResCountryCode list is based on the ISO 3166-1 country list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status 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.

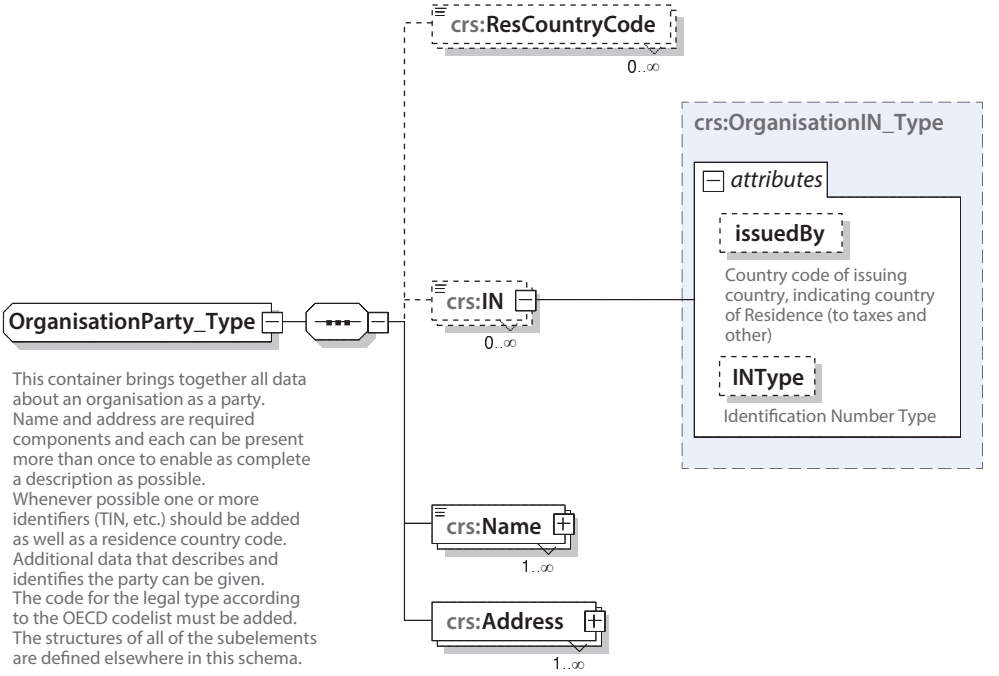
Person Name Type



Address Type

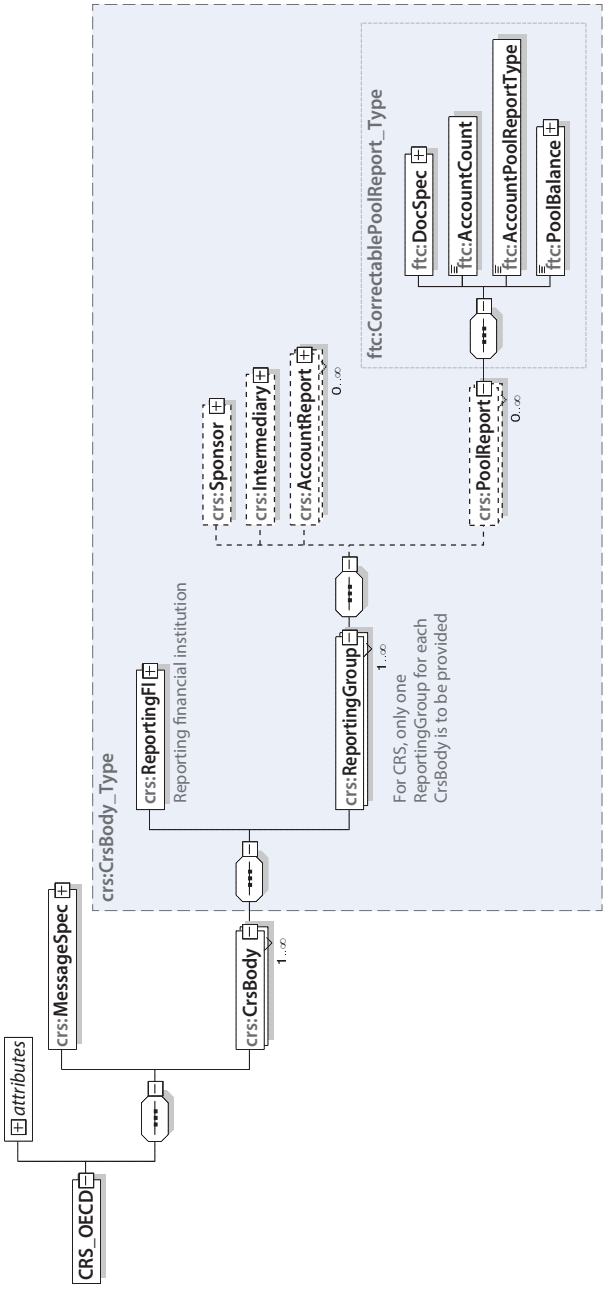


Organisation Party Type (Section III)

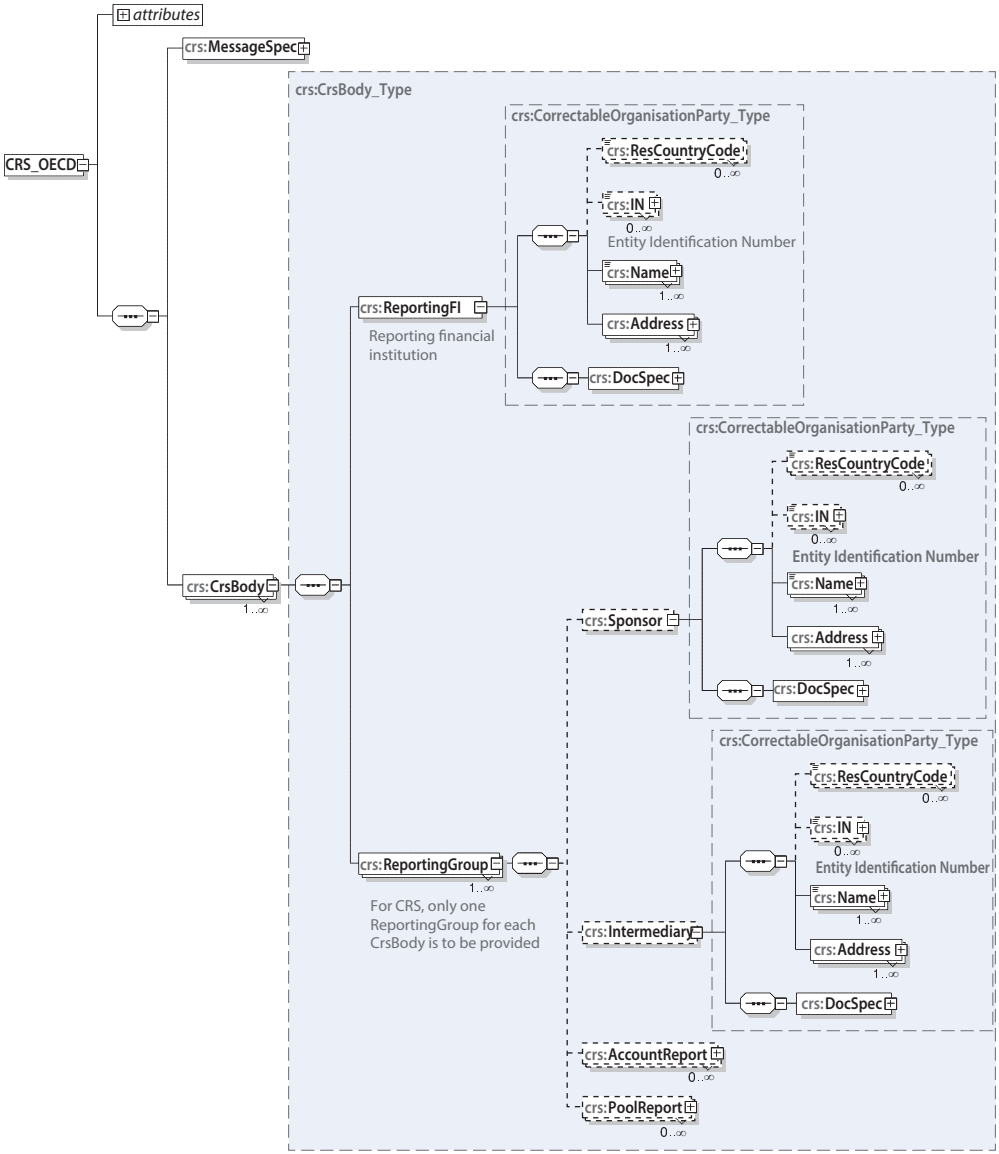


For practical reasons, the ResCountryCode list is based on the ISO 3166-1 country list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status 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.

Pool Report (Non-CRS) (Section IVi)



Sponsor & Intermediary (Non-CRS)



Appendix B

Glossary of Namespaces

CRS Schema Namespaces

Namespace	Description	Filename
crs	CRS specific types	CrsXML_v1.0.xsd
cfc	Common types for FATCA and CRS	CommonTypesFatcaCrs_v1.1.xsd
ftc	FATCA specific types	FatcaTypes_v1.1.xsd
stf	OECD Common Types	OECDTypes_v4.1.xsd
iso	ISO types (Country & Currency codes)	isocrstypes_v1.0.xsd

Annex 4

Example Questionnaire

1. Legal Framework

A legal framework must ensure the confidentiality of exchanged tax information and limit its use to appropriate purposes. The two basic components of such a framework are the terms of the applicable treaty, TIEA or other bilateral agreement for the exchange of information, and a jurisdiction's domestic legislation.

1.1. Tax Conventions, TIEAs & Other Exchange Agreements	
Primary Check-list Areas	• Provisions in tax treaties, TIEAs and international agreements requiring confidentiality of exchanged information and restricting use to intended purposes
How do the exchange of information provisions in your Tax Conventions, TIEAs, or other exchange agreements ensure confidentiality and restrict the use of both outgoing information to other Contracting States and incoming information received in response to a request?	

1.2. Domestic Legislation	
Primary Check-list Areas	• Domestic law must apply safeguards to taxpayer information exchanged pursuant to a treaty, TIEA or other international agreement, and treat those information exchange agreements as binding, restrict data access and use and impose penalties for violations.
How do your domestic laws and regulations safeguard and restrict the use of information exchanged for tax purposes under Tax Conventions, TIEAs, or other exchange instruments? How does the tax administration prevent the misuse of confidential data and prohibit the transfer of tax information from the tax administrative body to non-tax government bodies?	

2. Information Security Management

The information security management systems used by each jurisdiction's tax administration must adhere to standards that ensure the protection of confidential taxpayer data. For example, there must be a screening process for employees handling the information, limits on who can access the information, and systems to detect and trace unauthorised disclosures. The internationally accepted standards for information security are known as the "ISO/IEC 27000-series". As described more fully below, a tax administration should be able to document that it is compliant with the ISO/IEC 27000-series standards or that it has an equivalent information security framework and that taxpayer information obtained under an exchange agreement is protected under that framework.

2.1.1. Background Checks and Contracts	
Primary Check-list Areas	• Screenings and background investigations for employees and contractors • Hiring process and contracts • Responsible Points of Contact
What procedures govern your tax administration's background investigations for employees and contractors who may have access to, use, or are responsible for protecting data received through exchange of information? Is this information publicly available? If so, please provide the reference. If not, please provide a summary of the procedures.	

2.1.2. Training and Awareness	
Primary Check-list Areas	• Initial training and periodic security awareness training based on roles, security risks, and applicable laws
What training does your tax administration provide to employees and contractors regarding confidential information including data received from partners through the Exchange of Information? Does your tax administration maintain a public version of the requirements? If so, please provide the reference. If not, please provide a summary of the requirement.	

2.1.3. Departure Policies	
Primary Check-list Areas	• Departure policies to terminate access to confidential information
What procedures does your tax administration maintain for terminating access to confidential information for departing employees and consultants? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures.	

2.2.1. Physical Security: Access to Premises	
Primary Check-list Areas	• Security measures to restrict entry to premises: security guards, policies, entry access procedures
What procedures does your tax administration maintain to grant employees, consultants, and visitors access to premises where confidential information, paper or electronic, is stored? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures.	

2.2.2. Physical Security: Physical Document Storage	
Primary Check-list Areas	• Secure physical storage for confidential documents: policies and procedures
What procedures does your tax administration maintain for receiving, processing, archiving, retrieving and disposing of hard copies of confidential data received from taxpayers or exchange of information partners? Does your tax administration maintain procedures employees must follow when leaving their workspace at the end of the day? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. **Does your tax administration have a data classification policy? If so, please describe how your document storage procedures differ for data at all classification levels. Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.**	

2.3. Planning	
Primary Check-list Areas	• Planning documentation to develop, update, and implement security information systems
What procedures does your tax administration maintain to develop, document, update, and implement security for information systems used to receive, process, archive and retrieve confidential information? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. **What procedures does your tax administration maintain regarding periodic Information Security Plan updates to address changes to the information systems environment, and how are problems and risks identified during the implementation of Information Security Plans resolved? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.**	

2.4. Configuration Management	
Primary Check-list Areas	• Configuration management and security controls
What policies does your tax administration maintain to regulate system configuration and updates? Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary.	

2.5. Access Control	
Primary Check-list Areas	• Access Control Policies and procedures: authorised personnel and international exchange of information
What policies does your tax administration maintain to limit system access to authorised users and safeguard data during transmission when received and stored? Please describe how your tax administration's access authorisation and data transmission policies extend to data received from an exchange of information partner under a Treaty or TIEA or other exchange agreement. Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary.	

2.6. Identification and Authentication	
Primary Check-list Areas	• Authenticating the identifying users and devices that require access to information systems
What policies and procedures does your tax administration maintain for each information system connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary. **What policies and procedures govern the authentication of authorised tax administration users by systems connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary.**	

2.7. Audit and Accountability	
Primary Check-list Areas	• Traceable electronic actions within systems • System audit procedures: monitoring, analysing, investigating and reporting of unlawful/unauthorised use
What policies and procedures does your tax administration maintain to ensure system audits take place that will detect unauthorised access? Are the policies publicly available? If so, please provide a reference. If not, please provide a summary.	

2.8. Maintenance	
Primary Check-list Areas	• Periodic and timely maintenance of systems • Controls over: tools, procedures, and mechanisms for system maintenance and personnel use
What policies govern effective periodic system maintenance by your tax administration? Are these policies publicly available? If so, please provide a reference. If not, please provide a summary. **What procedures govern the resolution of system flaws identified by your tax administration? Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary.**	

2.9. System and Communications Protection	
Primary Check-list Areas	• Procedures to monitor, control, and protect communications to and from information systems
What policies and procedures does your tax administration maintain for the electronic transmission and receipt of confidential data. Please describe the security and encryption requirements addressed in these policies. Are these policies publicly available? If so, please provide a reference. If not, please provide a summary.	

2.10. System and Information Integrity	
Primary Check-list Areas	• Procedures to identify, report, and correct information system flaws in a timely manner • Protection against malicious code and monitoring system security alerts
What procedures does your tax administration maintain to identify, report, and correct information system flaws in a timely manner? Please describe how these procedures provide for the protection of systems against malicious codes causing harm to data integrity. Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary.	

2.11. Security Assessments	
Primary Check-list Areas	• Processes used to test, validate, and authorise the security controls for protecting data, correcting deficiencies, and reducing vulnerabilities
What policies does your tax administration maintain and regularly update for reviewing the processes used to test, validate, and authorise a security control plan? Is the policy publicly available? If so, please provide a reference. If not, please provide a summary.	

2.12. Contingency Planning	
Primary Check-list Areas	• Plans for emergency response, backup operations, and post-disaster recovery of information systems
What contingency plans and procedures does your tax administration maintain to reduce the impact of improper data disclosure or unrecoverable loss of data? Are the plans and procedures publicly available? If so, please provide a reference. If not, please provide a summary.	

2.13. Risk Assessment	
Primary Check-list Areas	• Potential risk of unauthorised access to taxpayer information • Risk and magnitude of harm from unauthorised use, disclosure, or disruption of the taxpayer information systems • Procedures to update risk assessment methodologies
Does your tax administration conduct risk assessments to identify risks and the potential impact of unauthorised access, use, and disclosure of information, or destruction of information systems? What procedures does your tax administration maintain to update risk assessment methodologies? Are these risk assessments and policies publicly available? If so, please provide a reference. If not, please provide a summary.	

2.14. Systems and Services Acquisition	
Primary Check-list Areas	• Methods and processes to ensure third-party providers of information systems process, store, and transmit confidential information in accordance with computer security requirements
What process does your tax administration maintain to ensure third-party providers are applying appropriate security controls that are consistent with computer security requirements for confidential information? Are the processes publicly available? If so, please provide a reference. If not, please provide a summary.	

2.15. Media Protection	
Primary Check-list Areas	• Processes to protect information in printed or digital form • Security measures used to limit media information access to authorised users only • Methods for sanitising or destroying digital media prior to disposal or reuse
What processes does your tax administration maintain to securely store and limit access to confidential information in printed or digital form upon receipt from any source? How does your tax administration securely destroy confidential media information prior to its disposal? Are the processes available publicly? If so, please provide a reference. If not, please provide a summary.	

2.16. Protection of Treaty-Exchanged data	
Primary Check-list Areas	• Procedures to ensure treaty-exchanged files are safeguarded and clearly labeled • Classification methods of treaty-exchanged files
What policies and processes does your tax administration maintain to store confidential information and clearly label it as treaty-exchanged after receipt from foreign Competent Authorities? Are these policies and processes publicly available? If so, please provide a reference. If not, please provide a summary.	

2.17. Information Disposal Policies	
Primary Check-list Areas	• Procedures for properly disposing paper and electronic files
What procedures does your tax administration maintain for the disposal of confidential information? Do these procedures extend to exchanged information from foreign Competent Authorities? Are the procedures publicly available? If so, please provide a reference. If not, please provide a summary.	

3. Monitoring and Enforcement

In addition to keeping treaty-exchanged information confidential, tax administrations must be able to ensure that its use will be limited to the purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect treaty-exchanged tax data. In addition, domestic law

must impose penalties or sanctions for improper disclosure or use of taxpayer information. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures.

3.1. Penalties and Sanctions	
Primary Check-list Areas	• Penalties imposed for unauthorised disclosures • Risk mitigation practices
Does your tax administration have the ability to impose penalties for unauthorised disclosures of confidential information? Do the penalties extend to unauthorised disclosure of confidential information exchanged with a treaty or TIEA partner? Are the penalties publicly available? If so, please provide a reference. If not, please provide a summary.	

3.2.1. Policing Unauthorised Access and Disclosure	
Primary Check-list Areas	• Monitoring to detect breaches • Reporting of breaches
What procedures does your tax administration have to monitor confidentiality breaches? What policies and procedures does your tax administration have that require employees and contractors to report actual or potential breaches of confidentiality? What reports does your tax administration prepare when a breach of confidentiality occurs? Are these policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary.	

3.2.2. Sanctions and Prior Experience	
Primary Check-list Areas	• Prior unauthorised disclosures • Policy/process modifications to prevent future breaches
Have there been any cases in your jurisdiction where confidential information has been improperly disclosed? Have there been any cases in your jurisdiction where confidential information received by the Competent Authority from an exchange of information partner has been disclosed other than in accordance with the terms of the instrument under which it was provided? Does your tax administration or Inspector General make available to the public descriptions of any breaches, any penalties/sanctions imposed, and changes put in place to mitigate risk and prevent future breaches? If so, please provide a reference. If not, please provide a summary.	

Annex 5

Wider Approach to the Common Reporting Standard

Introduction

1. The due diligence procedures in the CRS (in particular the indicia search procedures) are designed to identify Reportable Accounts understood as those of residents in a jurisdiction that is a Reportable Jurisdiction at the moment the due diligence procedures are performed. However, there are good reasons why jurisdictions may wish to go wider and, for instance, extend due diligence procedures to cover all non-residents or residents of jurisdictions with which they have an exchange of information instrument in place. Such an approach could significantly reduce costs for financial institutions because they would not need to perform additional due diligence each time a new jurisdiction joins.

2. This document contains an extract from the CRS which was amended to provide for such a wider approach. The main changes to the CRS are the following:

- Any language suggesting that the procedures are designed to identify accounts that are Reportable Accounts at the moment the due diligence procedures are performed is deleted or amended.
- Under the indicia search procedure the Reporting Financial Institution is now required to search for indicia indicating that the Account Holder is resident in a Foreign Jurisdiction and to treat the Account as held by an Account Holder that is resident of each Foreign Jurisdiction for which an indicium is found (unless the FI follows the "curing procedure"). A Foreign Jurisdiction would be defined as any Jurisdiction other than the Jurisdiction of the Reporting Financial Institution. The advantage of this approach is that, if a new jurisdiction joins the system, the Reporting Financial Institution can rely on the results of that indicia search to determine which of its Preexisting Accounts are held by residents of such jurisdiction.

3. The following examples illustrate the application of this wider approach:

- Example 1: Jurisdiction A decides to implement the Common Reporting Standard effective 1 January 2016, meaning that all accounts opened after that date are considered New Accounts.

  Mr. X is resident of Jurisdiction Z and opens an account with a financial institution in Jurisdiction A on 1 March 2016. At that moment, Jurisdiction Z is not a Reportable Jurisdiction. The financial institution will need to collect a self-certification from Mr. X, which will need to include his jurisdiction of residence for tax purposes but not his TIN or date of birth (as the account is not a Reportable Account at its opening). If Jurisdiction Z becomes a Reportable Jurisdiction in 2017, the financial institution can rely on the self-certification to establish that the account is a Reportable Account and will need to collect the TIN and date of birth from Mr. X by the end of 2019.

- Example 2: The same example, but the account is opened in 2014. If the financial institution has applied the indicia search with respect to Preexisting Accounts in 2016, it may rely on the information collected pursuant to such indicia search to determine the jurisdiction of residence of Mr. X and treat such account as a Reportable Account in 2017.

4. In the below extract, the Reporting Financial Institution would not be required to report the TIN and date of birth with respect to accounts that were not reportable at the moment it performed the due diligence procedures. However, it would be required to collect such TIN and date of birth by the end of the second calendar year following the year in which such accounts were identified as Reportable Accounts (similar to Preexisting Accounts). To the extent compatible with local data protection rules, jurisdictions may also consider requiring the collection of TIN and/or date of birth for all Account Holders that are identified as foreign upon account opening (and not just those that are identified as resident of a Reportable Jurisdiction). This may possibly further reduce the burden for Financial Institutions as it is easier to collect such information before rather than after account opening. In addition, requiring an Account Holder's TIN would also provide additional assurance of the veracity of its self-certification.

5. Although not required by the Common Reporting Standard, some jurisdictions may adopt an approach that goes beyond the approach contained in this Annex and, for example, extend the due diligence procedures to cover their own residents that are Controlling Persons of Passive NFEs. Thus, they would also receive information where one of their residents is a Controlling Person of a Passive NFE that holds an account with a Reporting Financial Institution. Such approach would require Reporting Financial Institutions

to report upon residents that, although not Account Holders themselves, are Controlling Persons of a Passive NFE that is an Account Holder. This may be done, e.g. by broadening the scope of the term "Reportable Person".

EXTRACT FROM THE CRS, AS AMENDED TO REQUIRE THE IDENTIFICATION OF THE STATUS OF ALL FOREIGN ACCOUNTS

Section I: General Reporting Requirements

A. Subject to paragraphs C through F, each Reporting Financial Institution must report the following information with respect to each Reportable Account of such Reporting Financial Institution:

1. the name, address, jurisdiction(s) of residence, TIN(s) and date and place of birth (in the case of an individual) of each Reportable Person that is an Account Holder of the account and, in the case of any Entity that is an Account Holder and that, after application of the due diligence procedures consistent with Sections V, VI and VII is identified as having one or more Controlling Persons that is a Reportable Person, the name, address, jurisdiction(s) of residence and TIN(s) of the Entity and the name, address, jurisdiction(s) of residence, TIN(s) and date and place of birth of each Reportable Person;
2. the account number (or functional equivalent in the absence of an account number);
3. the name and identifying number (if any) of the Reporting Financial Institution;
4. the account balance or value (including, in the case of a Cash Value Insurance Contract or Annuity Contract, the Cash Value or surrender value) as of the end of the relevant calendar year or other appropriate reporting period or, if the account was closed during such year or period, the closure of the account;
5. in the case of any Custodial Account:

   a) the total gross amount of interest, the total gross amount of dividends, and the total gross amount of other income generated with respect to the assets held in the account, in each case paid or credited to the account (or with respect to the account) during the calendar year or other appropriate reporting period; and

b) the total gross proceeds from the sale or redemption of Financial Assets paid or credited to the account during the calendar year or other appropriate reporting period with respect to which the Reporting Financial Institution acted as a custodian, broker, nominee, or otherwise as an agent for the Account Holder;

6. in the case of any Depository Account, the total gross amount of interest paid or credited to the account during the calendar year or other appropriate reporting period; and

7. in the case of any account not described in subparagraph A(5) or A(6), the total gross amount paid or credited to the Account Holder with respect to the account during the calendar year or other appropriate reporting period with respect to which the Reporting Financial Institution is the obligor or debtor, including the aggregate amount of any redemption payments made to the Account Holder during the calendar year or other appropriate reporting period.

B. The information reported must identify the currency in which each amount is denominated.

C. Notwithstanding subparagraph A(1), with respect to each Reportable Account that is a Preexisting Account or with respect to each Financial Account that is opened prior to becoming a Reportable Account, the TIN(s) or date of birth is not required to be reported if such TIN(s) or date of birth is not in the records of the Reporting Financial Institution and is not otherwise required to be collected by such Reporting Financial Institution under domestic law. However, a Reporting Financial Institution is required to use reasonable efforts to obtain the TIN(s) and date of birth with respect to Preexisting Accounts by the end of the second calendar year following the year in which such Accounts were identified as Reportable Accounts.

D. Notwithstanding subparagraph A(1), the TIN is not required to be reported if *(i)* a TIN is not issued by the relevant Reportable Jurisdiction or *(ii)* the domestic law of the relevant Reportable Jurisdiction does not require the collection of the TIN issued by such Reportable Jurisdiction.

E. Notwithstanding subparagraph A(1), the place of birth is not required to be reported unless the Reporting Financial Institution is otherwise required to obtain and report it under domestic law and it is available in the electronically searchable data maintained by the Reporting Financial Institution.

F. Notwithstanding paragraph A, the information to be reported with respect to [xxxx] is the information described in such paragraph, except for gross proceeds described in subparagraph A(5)(b).

Section II: General Due Diligence Requirements

A. An account is treated as a Reportable Account beginning as of the date it is identified as such pursuant to the due diligence procedures described in Sections II through VII and, unless otherwise provided, information with respect to a Reportable Account must be reported annually in the calendar year following the year to which the information relates.

B. A Reporting Financial Institution, which pursuant to the procedures described in Sections II through VII, identifies any account as a Foreign Account that is not a Reportable Account at the time the due diligence is performed, may rely on the outcome of such procedures to comply with future reporting obligations.

C. The balance or value of an account is determined as of the last day of the calendar year or other appropriate reporting period.

D. Where a balance or value threshold is to be determined as of the last day of a calendar year, the relevant balance or value must be determined as of the last day of the reporting period that ends with or within that calendar year.

E. Each Jurisdiction may allow Reporting Financial Institutions to use service providers to fulfil the reporting and due diligence obligations imposed on such Reporting Financial Institutions, as contemplated in domestic law, but these obligations shall remain the responsibility of the Reporting Financial Institutions.

F. Each Jurisdiction may allow Reporting Financial Institutions to apply the due diligence procedures for New Accounts to Preexisting Accounts, and the due diligence procedures for High value Accounts to Lower Value Accounts. Where a Jurisdiction allows New Account due diligence procedures to be used for Preexisting Accounts, the rules otherwise applicable to Preexisting Accounts continue to apply.

Section III: Due Diligence for Preexisting Individual Accounts

The following procedures apply with respect to Preexisting Individual Accounts.

A. **Accounts Not Required to be Reviewed, Identified, or Reported.** A Preexisting Individual Account that is a Cash Value Insurance Contract or an Annuity Contract is not required to be reviewed, identified or reported, provided the Reporting Financial Institution is effectively prevented by law from selling such Contract to residents of a Reportable Jurisdiction.

B. **Lower Value Accounts.** The following procedures apply with respect to Lower Value Accounts.

1. **Residence Address.** If the Reporting Financial Institution has in its records a current residence address for the individual Account Holder based on Documentary Evidence, the Reporting Financial Institution may treat the individual Account Holder as being a resident for tax purposes of the jurisdiction in which the address is located for purposes of determining whether such individual Account Holder is a Reportable Person.

2. **Electronic Record Search.** If the Reporting Financial Institution does not rely on a current residence address for the individual Account Holder based on Documentary Evidence as set forth in subparagraph B(1), the Reporting Financial Institution must review electronically searchable data maintained by the Reporting Financial Institution for any of the following indicia and apply subparagraphs B(3) through (6):

a) identification of the Account Holder as a resident of a Foreign Jurisdiction;

b) current mailing or residence address (including a post office box) in a Foreign Jurisdiction;

c) one or more telephone numbers in a Foreign Jurisdiction and no telephone number in the jurisdiction of the Reporting Financial Institution;

d) standing instructions (other than with respect to a Depository Account) to transfer funds to an account maintained in a Foreign Jurisdiction;

e) currently effective power of attorney or signatory authority granted to a person with an address in a Foreign Jurisdiction; or

f) a "hold mail" instruction or "in-care-of" address in a Foreign Jurisdiction if the Reporting Financial Institution does not have any other address on file for the Account Holder.

3. If none of the indicia listed in subparagraph B(2) are discovered in the electronic search, then no further action is required until there is a change in circumstances that results in one or more indicia being associated with the account, or the account becomes a High Value Account.

4. If any of the indicia listed in subparagraph B(2)(a) through (e) are discovered in the electronic search, or if there is a change in circumstances that results in one or more indicia being associated with the account, then the Reporting Financial Institution must treat the Account Holder as a resident for tax purposes of each Foreign Jurisdiction for which an indicium is identified, unless it elects to apply subparagraph B(6) and one of the exceptions in such subparagraph applies with respect to that account.

5. If a "hold mail" instruction or "in-care-of" address is discovered in the electronic search and no other address and none of the other indicia listed in subparagraph B(2)(a) through (e) are identified for the Account Holder, the Reporting Financial Institution must, in the order must appropriate to the circumstances, apply the paper record search described in subparagraph C(2), or seek to obtain from the Account Holder a self-certification or Documentary Evidence to establish the residence(s) for tax purposes of such Account Holder. If the paper search fails to establish an indicium and the attempt to obtain the self-certification or Documentary Evidence is not successful, the Reporting Financial Institution must report the account as an undocumented account.

6. Notwithstanding a finding of indicia under subparagraph B(2), a Reporting Financial Institution is not required to treat an Account Holder as a resident of a Foreign Jurisdiction if:

   a) the Account Holder information contains a current mailing or residence address in the Foreign Jurisdiction, one or more telephone numbers in the Foreign Jurisdiction (and no telephone number in the jurisdiction of the Reporting Financial Institution) or standing instructions (with respect to Financial Account other than Depository Accounts) to transfer funds to an account maintained in a Foreign Jurisdiction, the Reporting Financial Institution obtains, or has previously reviewed and maintains a record of:

      i) a self-certification from the Account Holder of the jurisdiction(s) of residence of such Account Holder that does not include such Foreign Jurisdiction; and

ii) Documentary Evidence establishing the Account Holder's residence for tax purposes other than such Foreign Jurisdiction.

b) the Account Holder information contains a currently effective power of attorney or signatory authority granted to a person with an address in a Foreign Jurisdiction, the Reporting Financial Institution obtains, or has previously reviewed and maintains a record of:

i) a self-certification from the Account Holder of the jurisdiction(s) of residence of such Account Holder that does not include such Foreign Jurisdiction; or

ii) Documentary Evidence establishing the Account Holder's residence for tax purposes other than Foreign Jurisdiction.

C. **Enhanced Review Procedures for High Value Accounts.** The following enhanced review procedures apply with respect to High Value Accounts.

1. **Electronic Record Search.** With respect to High Value Accounts, the Reporting Financial Institution must review electronically searchable data maintained by the Reporting Financial Institution for any of the indicia described in subparagraph B(2).

2. **Paper Record Search.** If the Reporting Financial Institution's electronically searchable databases include fields for, and capture all of the information described in, subparagraph C(3), then a further paper record search is no required. If the electronic databases do not capture all of this information, then with respect to a High Value Account, the Reporting Financial Institution must also review the current customer master file and, to the extent not contained in the current customer master file, the following documents associated with the account and obtained by the Reporting Financial Institution within the last five years for any of the indicia described in subparagraph B(2):

a) the most recent Documentary Evidence collected with respect to the account;

b) the most recent account opening contract or documentation;

c) the most recent documentation obtained by the Reporting Financial Institution pursuant to AML/KYC Procedures or for other regulatory purposes;

d) any power of attorney or signature authority forms currently in effect; and

e) any standing instructions (other than with respect to a Depository Account) to transfer funds currently in effect.

3. **Exception To The Extent Databases Contain Sufficient Information.** A Reporting Financial Institution is not required to perform the paper record search described in subparagraph C(2) to the extent the Reporting Financial Institution's electronically searchable information includes the following:

a) the Account Holder's residence status;

b) the Account Holder's residence address and mailing address currently on file with the Reporting Financial Institution;

c) the Account Holder's telephone number(s) currently on file, if any, with the Reporting Financial Institution;

d) in the case of Financial Accounts other than Depository Accounts, whether there are standing instructions to transfer funds in the account to another account (including an account at another branch of the Reporting Financial Institution or another Financial Institution);

e) whether there is a current "in-care-of" address or "hold mail" instruction for the Account Holder; and

f) whether there is any power of attorney or signatory authority for the account.

4. **Relationship Manager Inquiry for Actual Knowledge.** In addition to the electronic and paper record searches described above, the Reporting Financial Institution must treat as a Reportable Account any High Value Account assigned to a relationship manager (including any Financial Accounts aggregated with that High Value Account) if the relationship manager has actual knowledge that the Account Holder is a Reportable Person.

5. **Effect of Finding Indicia.**

a) If none of the indicia listed in subparagraph B(2) are discovered in the enhanced review of High Value Accounts described above, and the account is not identified as held by a resident for tax purposes in a Foreign Jurisdiction in subparagraph C(4), then further action is not required until there is a change in circumstances that results in one or more indicia being associated with the account.

b) If any of the indicia listed in subparagraph B(2)(a) through (e) are discovered in the enhanced review of High Value Accounts described above, or if there is a subsequent change in circumstances that results in one or more indicia being associated with the account, then the Reporting Financial Institution must treat the Account Holder as a resident for tax purposes of each Foreign Jurisdiction for which an indicium is identified unless it elects to apply subparagraph B(6) and one of the exceptions in such subparagraph applies with respect to that account.

c) If a "hold mail" instruction or "in-care-of" address is discovered in the enhanced review of High Value Account described above, and no other address and none of the other indicia listed in subparagraph B(2)(a) through (e) are identified for the Account Holder, the Reporting Financial Institution must obtain from such Account Holder a self-certification or Documentary Evidence to establish the residence(s) for tax purposes of the Account Holder. If the Reporting Financial Institution cannot obtain such self-certification or Documentary Evidence, it must report the account as an undocumented account.

6. If a Preexisting Individual Account is not a High Value Account as of 31 December [xxxx], but becomes a High Value Account as of the last day of a subsequent calendar year, the Reporting Financial Institution must complete the enhanced review procedures described in paragraph C with respect to such account within the calendar year following the year in which the account becomes a High Value Account. If based on this review such account is identified as a Reportable Account, the Reporting Financial Institution must report the required information about such account with respect to the year in which it is identified as a Reportable Account and subsequent years on an annual basis, unless the Account Holder ceases to be a Reportable Person.

7. Once a Reporting Financial Institution applies the enhanced review procedures described in paragraph C to a High Value Account, the Reporting Financial Institution is not required to re-apply such procedures, other than the relationship manager inquiry described in subparagraph C(4), to the same High Value Account in any subsequent year unless the account is undocumented where the Reporting Financial Institution should re-apply them annually until such account ceases to be undocumented.

8. If there is a change of circumstances with respect to a High Value Account that results in one or more indicia described in subparagraph B(2) being associated with the account, then the Reporting Financial Institution must treat the account as a Reportable Account with respect to each Foreign Jurisdiction for which an indicium is identified unless it elects to apply subparagraph B(6) and one of the exceptions in such subparagraph applies with respect to that account.

9. A Reporting Financial Institution must implement procedures to ensure that a relationship manager identifies any change in circumstances of an account. For example, if a relationship manager is notified that the Account Holder has a new mailing address in a Foreign Jurisdiction, the Reporting Financial Institution is required to treat the new address as a change in circumstances and, if it elects to apply subparagraph B(6), is required to obtain the appropriate documentation from the Account Holder.

D. Review of Preexisting Individual Accounts must be completed by [xx/xx/xxxx].

Section IV: Due Diligence for New Individual Accounts

The following procedures apply with respect to New Individual Accounts.

A. With respect to New Individual Accounts, upon account opening, a Reporting Financial Institution must obtain a self-certification, which may be part of the account opening documentation, that allows the Reporting Financial Institution to determine the Account Holder's residence(s) for tax purposes and confirm the reasonableness of such self-certification based on the information obtained by the Reporting Financial Institution in connection with the opening of the account, including any documentation collected pursuant to AML/KYC Procedures.

B. If the self-certification establishes that the Account Holder is resident for tax purposes in a Reportable Jurisdiction, the Reporting Financial Institution must treat the account as a Reportable Account and the self-certification must also include the Account Holder's TIN with respect to such Reportable Jurisdiction (subject to paragraph D of Section I) and date of birth.

C. If there is a change of circumstances with respect to a New Individual Account that causes the Reporting Financial Institution to know, or have reason to know, that the original self-certification

is incorrect or unreliable, the Reporting Financial Institution cannot rely on the original self-certification and must obtain a valid self-certification that establishes the residence(s) for tax purposes of the Account Holder.

Section V: Due Diligence for Preexisting Entity Accounts

The following procedures apply with respect to Preexisting Entity Accounts.

A. **Entity Accounts Not Required to Be Reviewed, Identified or Reported.** Unless the Reporting Financial Institution elects otherwise, either with respect to all Preexisting Entity Accounts or, separately, with respect to any clearly identified group of such accounts, a Preexisting Entity Account with an aggregate account balance or value that does not exceed USD 250 000 as of 31 December [xxxx], is not required to be reviewed, identified, or reported as a Reportable Account until the aggregate account balance or value exceeds USD 250 000 as of the last day of any subsequent calendar year.

B. **Entity Accounts Subject to Review.** A Preexisting Entity Account that has an aggregate account balance or value that exceeds USD 250 000 as of 31 December [xxxx], and a Preexisting Entity Account that does not exceed USD 250 000 as of 31 December [xxxx] but the aggregate account balance or value of which exceeds USD 250 000 as of the last day of any subsequent calendar year, must be reviewed in accordance with the procedures set forth in paragraph D.

C. **Review Procedures for Identifying Entity Accounts With Respect to Which Reporting may be Required.** For Preexisting Entity Accounts described in paragraph B, a Reporting Financial Institution must apply the following review procedures:

1. **Determine the Residence of the Entity.**

a) Review information maintained for regulatory or customer relationship purposes (including information collected pursuant to AML/KYC Procedures) to determine the Account Holder's residence. For this purpose, information indicating the Account Holder's residence includes a place of incorporation or organisation, or an address in a Foreign Jurisdiction.

b) If the information indicates that the Account Holder is a Reportable Person, the Reporting Financial Institution must treat the account as a Reportable Account unless it obtains a self-certification from the Account Holder, or reasonably determines based on information in its possession or that is publicly available, that the Account Holder is not a Reportable Person.

2. **Determine the Residence of the Controlling Persons of a Passive NFE.** With respect to an Account Holder of a Preexisting Entity Account (including an Entity that is a Reportable Person), the Reporting Financial Institution must identify whether the Account Holder is a Passive NFE with one or more Controlling Persons and determine the residence of such Controlling Persons. If any of the Controlling Persons of a Passive NFE is a Reportable Person, then the account is treated as a Reportable Account. In making these determinations the Reporting Financial Institution must follow the guidance in subparagraphs C(2)(a) through (c) in the order most appropriate under the circumstances.

   a) **Determining whether the Account Holder is a Passive NFE.** For purposes of determining whether the Account Holder is a Passive NFE, the Reporting Financial Institution must obtain a self-certification from the Account Holder to establish its status, unless it has information in its possession or that is publicly available, based on which it can reasonably determine that the Account Holder is an Active NFE or a Financial Institution other than an Investment Entity described in subparagraph A(6)(b) of Section VIII that is not a Participating Jurisdiction Financial Institution.

   b) **Determining the Controlling Persons of an Account Holder.** For the purposes of determining the Controlling Persons of an Account Holder, a Reporting Financial Institution may rely on information collected and maintained pursuant to AML/KYC Procedures.

   c) **Determining the residence of a Controlling Person of a Passive NFE.** For the purposes of determining the residence of a Controlling Person of a Passive NFE, a Reporting Financial Institution may rely on:

      i) information collected and maintained pursuant to AML/KYC Procedures in the case of a Preexisting Entity Account held by one or more Passive NFEs with an

aggregate account balance or value that does not exceed USD 1 000 000; or

ii) a self-certification from the Account Holder or such Controlling Person of the jurisdiction(s) in which the Controlling Person is resident for tax purposes. If a self-certification is not provided, the Reporting Financial Institution will establish such residence(s) by applying the procedures described in paragraph C of Section III.

D. **Timing of Review and Additional Procedures Applicable to Preexisting Entity Accounts.**

1. Review of Preexisting Entity Accounts with an aggregate account balance or value that exceeds USD 250 000 as of 31 December [xxxx] must be completed by 31 December [xxxx].

2. Review of Preexisting Entity Accounts with an aggregate account balance or value that does not exceed USD 250 000 as of 31 December [xxxx], but exceeds USD 250 000 as of 31 December of a subsequent year, must be completed within the calendar year following the year in which the aggregate account balance or value exceeds USD 250 000.

3. If there is a change of circumstances with respect to a Preexisting Entity Account that causes the Reporting Financial Institution to know, or have reason to know, that the self-certification or other documentation associated with an account is incorrect or unreliable, the Reporting Financial Institution must re-determine the status of the account in accordance with the procedures set forth in paragraph C.

Section VI: Due Diligence for New Entity Accounts

The following procedures apply with respect to New Entity Accounts.

A. **Review Procedures for Identifying Entity Accounts With Respect to Which Reporting may be Required.** For New Entity Accounts, a Reporting Financial Institution must apply the following review procedures:

1. **Determine the Residence of the Entity.**

a) Obtain a self-certification, which may be part of the account opening documentation, that allows the Reporting Financial Institution to determine the Account Holder's residence(s) for tax purposes and confirm the reasonableness of such

self-certification based on the information obtained by the Reporting Financial Institution in connection with the opening of the account, including any documentation collected pursuant to AML/KYC Procedures. If the Entity certifies that it has no residence for tax purposes, the Reporting Financial Institution may rely on the address of the principal office of the Entity to determine the residence of the Account Holder.

b) If the self-certification indicates that the Account Holder is resident in a Reportable Jurisdiction, the Reporting Financial Institution must treat the account as a Reportable Account unless it reasonably determines based on information in its possession or that is publicly available, that the Account Holder is not a Reportable Person with respect to such Reportable Jurisdiction.

2. **Determine the Residence of the Controlling Persons of a Passive NFE.** With respect to an Account Holder of a New Entity Account (including an Entity that is a Reportable Person), the Reporting Financial Institution must identify whether the Account Holder is a Passive NFE with one or more Controlling Persons and determine the residence of such Reportable Persons. If any of the Controlling Persons of a Passive NFE is a Reportable Person, then the account must be treated as a Reportable Account. In making these determinations the Reporting Financial Institution must follow the guidance in subparagraphs A(2)(a) through (c) in the order most appropriate under the circumstances.

a) **Determining whether the Account Holder is a Passive NFE.** For purposes of determining whether the Account Holder is a Passive NFE, the Reporting Financial Institution must rely on a self-certification from the Account Holder to establish its status, unless it has information in its possession or that is publicly available, based on which it can reasonably determine that the Account Holder is an Active NFE or a Financial Institution other than an Investment Entity described in subparagraph A(6)(b) of Section VIII that is not a Participating Jurisdiction Financial Institution.

b) **Determining the Controlling Persons of an Account Holder.** For purposes of determining the Controlling Persons of an Account Holder, a Reporting Financial Institution may rely on information collected and maintained pursuant to AML/KYC Procedures.

c) **Determining the residence of a Controlling Person of a Passive NFE.** For purposes of determining the residence of a Controlling Person of a Passive NFE, a Reporting Financial Institution may rely on a self-certification from the Account Holder or such Controlling Person.

Section VII: Special Due Diligence Rules

The following additional rules apply in implementing the due diligence procedures described above.

A. **Reliance on Self-Certifications and Documentary Evidence.** A Reporting Financial Institution may not rely on a self-certification or Documentary Evidence if the Reporting Financial Institution knows or has reason to know that the self-certification or Documentary Evidence is incorrect or unreliable.

B. **Alternative Procedures for Financial Accounts Held by Individual Beneficiaries of a Cash Value Insurance Contract or an Annuity Contract.** A Reporting Financial Institution may presume that an individual beneficiary (other than the owner) of a Cash Value Insurance Contract or an Annuity Contract receiving a death benefit is not a Reportable Person and may treat such Financial Account as other than a Reportable Account unless the Reporting Financial Institution has actual knowledge, or reason to know, that the beneficiary is a Reportable Person. A Reporting Financial Institution has reason to know that a beneficiary of a Cash Value Insurance Contract or an Annuity Contract is a Reportable Person if the information collected by the Reporting Financial Institution and associated with the beneficiary contains indicia of residence in a Foreign Jurisdiction as described in paragraph B of Section III. If a Reporting Financial Institution has actual knowledge, or reason to know, that the beneficiary is a Reportable Person, the Reporting Financial Institution must follow the procedures in paragraph B of Section III.

C. **Account Balance Aggregation and Currency Rules.**

1. **Aggregation of Individual Accounts.** For purposes of determining the aggregate balance or value of Financial Accounts held by an individual, a Reporting Financial Institution is required to aggregate all Financial Accounts maintained by the Reporting Financial Institution, or by a Related Entity, but only to the extent that the Reporting Financial Institution's computerised systems link the Financial Accounts by reference to a data element such as client number or TIN, and allow

account balances or values to be aggregated. Each holder of a jointly held Financial Account shall be attributed the entire balance or value of the jointly held Financial Account for purposes of applying the aggregation requirements described in this subparagraph.

2. **Aggregation of Entity Accounts.** For purposes of determining the aggregate balance or value of Financial Accounts held by an Entity, a Reporting Financial Institution is required to take into account all Financial Accounts that are maintained by the Reporting Financial Institution, or by a Related Entity, but only to the extent that the Reporting Financial Institution's computerised systems link the Financial Accounts by reference to a data element such as client number or TIN, and allow account balances or values to be aggregated. Each holder of a jointly held Financial Account shall be attributed the entire balance or value of the jointly held Financial Account for purposes of applying the aggregation requirements described in this subparagraph.

3. **Special Aggregation Rule Applicable to Relationship Managers.** For purposes of determining the aggregate balance or value of Financial Accounts held by a person to determine whether a Financial Account is a High Value Account, a Reporting Financial Institution is also required, in the case of any Financial Accounts that a relationship manager knows, or has reason to know, are directly or indirectly owned, controlled, or established (other than in a fiduciary capacity) by the same person, to aggregate all such accounts.

4. **Amounts Read to Include Equivalent in Other Currencies.** All dollar amounts are in US dollars and shall be read to include equivalent amounts in other currencies, as determined by domestic law.

Annex 6

Declaration on Automatic Exchange of Information in Tax Matters

(Adopted on 6 May 2014)

WE, THE MINISTERS AND REPRESENTATIVES of Argentina, Australia, Austria, Belgium, Brazil, Canada, the People's Republic of China, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Saudi Arabia, Singapore, the Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States and the European Union;

WELCOMING the OECD *Standard for Automatic Exchange of Financial Account Information*, which provides the key elements for establishing a single, common global standard for the automatic exchange of financial account information (hereafter "the new single global standard") thereby affording tax administrations around the world with a very powerful new tool to tackle cross-border tax evasion and non-compliance;

NOTING WITH SATISFACTION its strong endorsement by the G20 Finance Ministers and Central Bank Governors and their commitment to implement it at their meeting on 22-23 February 2014;

CONSIDERING that tax fraud and tax evasion jeopardise citizens' trust in the fairness and integrity of the tax system as a whole, thereby undermining voluntary tax compliance by all taxpayers, which is essential to effective tax administration;

CONSIDERING that the fight against tax fraud and tax evasion will, in turn, increase revenues which will help enable growth-enhancing public

investment, restore the health of our public finances and provide the essential public services that our citizens demand;

MINDFUL that as the world becomes increasingly globalised it is becoming easier for all taxpayers to make, hold and manage investments through financial institutions outside of their country of residence, and that investments that are kept offshore by taxpayers may go untaxed to the extent that taxpayers fail to comply with their tax obligations to the detriment of those who pay their taxes;

CONSIDERING that cross-border tax fraud and tax evasion are serious problems for jurisdictions all over the world, small and large, developed and developing;

CONSCIOUS that co-operation between tax administrations is critical in the fight against tax fraud and tax evasion and in promoting international tax compliance, and that a key aspect of such co-operation is effective exchange of information on an automatic basis subject to appropriate safeguards;

RECOGNISING the tremendous progress achieved by the Global Forum on Transparency and Exchange of Information for Tax Purposes (hereafter "Global Forum") in ensuring that international standards of transparency and exchange of information on request are fully implemented around the globe;

NOTING that there is growing interest in many countries in the opportunities provided by reciprocal automatic exchange of information between tax authorities;

WELCOMING the commitments already made for early adoption of the new single global standard by a large number of countries and jurisdictions;

CONSCIOUS that the new single global standard should not impose undue business and administrative costs;

NOTING that although the new single global standard covers financial account information, it does not restrict the ability of countries to exchange financial information under different types of legal arrangements or to exchange other types or categories of information on an automatic basis;

ACKNOWLEDGING the important role that the multilateral Convention on Mutual Administrative Assistance in Tax Matters can play in facilitating rapid implementation of automatic exchange of information and WELCOMING the fact that over 60 countries have already signed the Convention, including almost all OECD countries, all G20 countries, and a growing number of financial centres and developing countries;

WELCOMING the recent establishment by the Global Forum of a Working Group on Automatic Exchange of Information, which will develop

a mechanism to monitor and review the implementation of the new single global standard for automatic exchange of information and also a framework to offer technical assistance to developing countries in meeting the standard.

****

1. DECLARE that we are determined to tackle cross-border tax fraud and tax evasion and to promote international tax compliance through mutual administrative assistance in tax matters and a level playing field;

2. CONFIRM that automatic exchange of financial account information will further these objectives particularly if the new single global standard, including full transparency on ownership interests, is implemented among all financial centres;

3. ACKNOWLEDGE that information exchanged on the basis of the new single global standard is subject to appropriate safeguards including certain confidentiality requirements and the requirement that information may be used only for the purposes foreseen by the legal instrument pursuant to which it is exchanged;

4. ARE DETERMINED to implement the new single global standard swiftly, on a reciprocal basis. We will translate the standard into domestic law, including to ensure that information on beneficial ownership of legal persons and arrangements is effectively collected and exchanged in accordance with the standard;

5. CALL on all financial centres to implement the new single global standard without delay;

6. UNDERLINE the need for assistance to be provided to developing countries so that they may be able to reap the benefits of this form of co-operation;

7. URGE the OECD Committee on Fiscal Affairs, working with G20 members, to proceed rapidly with the elaboration of a) a detailed commentary to help ensure the consistent application of the new single global standard and b) the remaining technical modalities and safeguards including information and guidance on the necessary technical solutions, a standard format for reporting and exchange, and minimum standards on confidentiality;

8. EXPECT that the remaining elements of the work referred to in paragraph 7 will be finalised and approved by mid-2014;

9. ENCOURAGE all countries that have not already done so to sign and ratify the multilateral Convention on Mutual Administrative Assistance in Tax Matters without further delay;

10. EXPECT the swift establishment by the Global Forum of a mechanism to monitor and review the implementation of the new single global standard;

11. INVITE the Secretary-General of the OECD to report on the Committee on Fiscal Affairs' progress in developing further guidance on the implementation of the new single global standard at the 2015 Meeting of the Council at Ministerial level and at other international fora as appropriate.

Annex 7

Recommendation of the Council on the Standard for Automatic Exchange of Financial Account Information in Tax Matters

(Adopted on 15 July 2014)

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

HAVING REGARD to the Recommendation of the Council on Tax Avoidance and Evasion [C(77)149/FINAL], the Recommendation of the Council on the Use of Tax Identification Numbers in an International Context [C(97)29/FINAL] and the Recommendation of the Council concerning the Model Tax Convention on Income and on Capital [C(97)195/FINAL];

HAVING REGARD to Article 26 of the Model Tax Convention on Income and on Capital;

HAVING REGARD to the Convention on Mutual Administrative Assistance in Tax Matters of 25 January 1988, as amended by the 2010 Protocol [C(2010)10/FINAL], which has a growing number of Parties and signatories, currently totalling over 60 countries;

HAVING REGARD to the significant progress achieved by the Global Forum on Transparency and Exchange of Information for Tax Purposes in ensuring that international standards of transparency and exchange of information on request are fully implemented around the globe;

HAVING REGARD to the Declaration on Automatic Exchange of Information in Tax Matters adopted on 6 May 2014 by 47 countries, including all Members, Argentina, Brazil, the People's Republic of China, Colombia, Costa Rica, India, Indonesia, Latvia, Lithuania, Malaysia, Saudi Arabia, Singapore, South Africa as well as the European Union [C/MIN(2014)5/FINAL];

CONSIDERING that international cooperation is critical in the fight against tax fraud and tax evasion and in ensuring tax compliance, and that a key aspect of such cooperation is effective exchange of information on an automatic basis subject to appropriate safeguards;

CONSIDERING that the adoption of a single standard for automatic exchange of financial account information in tax matters will avoid the proliferation of different standards which would increase complexity and costs for both governments and financial institutions;

CONSIDERING that implementation of a single standard by all financial centres will ensure a level playing field;

CONSIDERING the need to encourage consistent application and interpretation across countries of the single standard;

CONSIDERING the mandate of the Global Forum on Transparency and Exchange of Information for Tax Purposes and the rapid evolution of the standards of transparency and exchange of information for tax purposes;

WELCOMING the Standard for Automatic Exchange of Financial Account Information in Tax Matters which is composed of the Common Reporting Standard and the Model Competent Authority Agreement (hereafter the "Standard"), approved by the Committee on Fiscal Affairs;

TAKING NOTE of the Commentaries to the Common Reporting Standard and the Commentaries to the Model Competent Authority Agreement (hereafter the "Commentaries"), approved by the Committee on Fiscal Affairs [C(2014)81/ADD1];

On the proposal of the Committee on Fiscal Affairs:

I. RECOMMENDS that Members and non-Members adhering to this Recommendation (hereafter the "Adherents") swiftly implement on a reciprocal basis the Standard set out in the Annex to this Recommendation of which it forms an integral part.

To this effect, Adherents should:

(a) transpose the Standard into domestic law, including to ensure that information on beneficial ownership of legal persons and arrangements is effectively collected and exchanged in accordance with the Standard;

(b) take the necessary measures in compliance with their domestic law to implement any amendments to the Standard; and

(c) ensure that appropriate safeguards are in place to protect the confidentiality of information exchanged and to comply with

the requirement that information may be used only for the purposes foreseen by the legal instrument pursuant to which the information is exchanged;

II. RECOMMENDS that Adherents follow the Commentaries when applying and interpreting the relevant domestic law provisions;

III. INVITES Adherents and the Secretary-General to disseminate this Recommendation widely;

IV. INVITES non-Members to implement the Standard and to adhere to this Recommendation;

V. INVITES Adherents to support efforts for capacity building and assistance to developing countries so that they may be able to participate in and reap the benefits of this form of co-operation;

VI. INVITES all countries that have not already done so to sign and ratify the Convention on Mutual Administrative Assistance in Tax Matters as amended by the 2010 Protocol;

VII. INVITES the Global Forum on Transparency and Exchange of Information for Tax Purposes to monitor the implementation of the Standard;

VIII. INSTRUCTS the Committee on Fiscal Affairs to:

(i) monitor the application of the Recommendation and to report thereon to the Council no later than three years following its adoption and regularly thereafter;

(ii) stand ready to review the Standard and Commentaries in the light of experience gained by Adherents and in consultation with stakeholders;

(iii) adopt any required modifications to the Commentaries and make appropriate proposals to Council for modifications to the Standard.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(23 2016 53 1 P) ISBN 978-92-64-26798-5 – 2017

Standard for Automatic Exchange of Financial Account Information in Tax Matters

Second Edition

The Common Reporting Standard (CRS), developed in response to the G20 request and approved by the OECD Council on 15 July 2014, calls on jurisdictions to obtain information from their financial institutions and automatically exchange that information with other jurisdictions on an annual basis. It sets out the financial account information to be exchanged, the financial institutions required to report, the different types of accounts and taxpayers covered, as well as common due diligence procedures to be followed by financial institutions. This publication contains the following four parts: A model Competent Authority Agreement (CAA) for the automatic exchange of CRS information; the Common Reporting Standard; the Commentaries on the CAA and the CRS; and the CRS XML Schema User Guide.

This edition expands the last part on the CRS XML Schema User Guide. It contains additional technical guidance on the handling of corrections and cancellations within the CRS XML Schema, as well as a revised and expanded set of correction examples. The other parts remain unchanged relative to the first edition issued in 2014.

OECD*publishing*
www.oecd.org/publishing

ISBN 978-92-64-26798-5
23 2016 53 1 P