



Interconnectivity Framework for Certificates of Origin

This report provides the results work carried out by the Informal Working Group (IWG) of the WCO Technical Committee on Rules of Origin (TCRO) in the context of the Feasibility Study on the Interconnectivity Framework for Certificates of Origin.

September 2025

Table of Contents

- 1. INTRODUCTION 6**
 - 1.1 Purpose of this document..... 6
 - 1.2 Utility block executive summary..... 6
- 2. CONTEXT AND PURPOSE 11**
 - 2.1 Advantages 12
 - 2.1.1 Advantages to government..... 12
 - 2.1.2 Advantages to Customs..... 12
 - 2.1.3 Advantages to business..... 13
 - 2.2 Legal framework and compliance 13
 - 2.2.1 Legal framework..... 13
 - 2.2.2 Compliance..... 17
- 3. BUSINESS PROCESS MODEL (BPM) 20**
 - 3.1 Data exchange model..... 20
 - 3.2 Entities..... 20
 - 3.3 Business process flow..... 22
 - 3.4 Data exchange sequence..... 24
 - 3.5 Triggers..... 25
 - 3.6 Data cluster 25
 - 3.7 Business rules 25
- 4. TECHNOLOGICAL REQUIREMENTS AND SPECIFICATIONS 26**
 - 4.1 System integration architecture..... 26
 - 4.2 Interface 28
 - 4.2.1 Service Interface Protocol 29
 - 4.2.2 Service patterns..... 29
 - 4.2.3 Service operation 30
 - 4.2.4 Message format..... 30
 - 4.3 Network communication..... 31
 - 4.3.1 Network communication infrastructure 31
 - 4.3.2 Network and security 32
 - 4.3.3 Service levels 32
 - 4.4 System security..... 33
 - 4.4.1 General security requirements..... 33

4.4.2 Security policy	33
4.4.3 Security implementation stack.....	34
ANNEX I: Business Process Description	37
I. Introduction.....	37
II. Phases and Actions.....	37
IIA. Entity Registration Phase (P.1/RP)	37
II.B Commodity Registration Phase (P.2/GP)	39
II.C. CO Issuance Phase (P.3/RP).....	40
II.D. CO Amendment Phase (Cancellation and Re-Issuance) (P.4/GP)	42
II.E. Origin-Based Treatment Claim Phase (P.5/RP).....	44
ANNEX II: Data Elements to be Exchanged	47
ANNEX III: Semi-Automated Pull Model for Certificate of Origin	55
I. Introduction.....	55
II. Entities	56
III. Business Process for CO Issuance/Amendment	56
IV. Origin Treatment Claim.....	57
ANNEX IV: Push Model for Self-Declaration of Origin.....	59
I. Introduction.....	59
II. Entities	60
III. Phases and Actions	60
III.A Registration Phase (P.1)	60
III.B. “Completing the Declaration of Origin” Phase (P.2).....	62
III.C. Origin-based Treatment Claim (P.3).....	63
ANNEX V: Comparative Information on Technological Specifications for Interconnectivity for Certificates of Origin	65
I. Introduction.....	65
II. Comparison of technical specifications	65
II.A. Service interface protocols	65
II.B. Message formats.....	66
II.C. Network infrastructure	66
II.D. Middleware solutions	67
II.E. System security.....	68
III. Recommendations	69

1. INTRODUCTION

1.1 Purpose of this document

This document provides the first version of the Globally Networked Customs (GNC) Utility Block (UB) for the Certificate of Origin (CO) data exchange. This UB is built on the UB structure endorsed by the WCO and established based on the current bilateral projects of CO data exchange and Customs interconnectivity under several specific Free Trade Agreements (FTAs). It may also be used in the context of bilateral exchanges of CO data between Free Trade Agreement (FTA) Member States and multilateral exchanges.

This UB is primarily intended to specify the process of CO information exchange between countries. Its overall purpose is to share information on the origin of exported goods and to enhance cooperation and transparency between countries regarding the movement of goods throughout the end-to-end supply chain. More specifically, it enables importing countries to access CO information in order to improve the efficiency of Customs clearance, conduct their risk analysis and take the necessary organizational measures accordingly. Being able to carry out an early risk analysis using available export information also helps to reduce the level of fraud and safeguard the end-to-end supply chain between countries.

The underlying principle of this UB is that any decision on what information to share, how to share it and for what business purpose is left to the countries entering into an agreement to use this UB.

1.2 Utility block executive summary

Purpose	<p>There is increased interest from different stakeholders in managing origin-related procedures of international trade through digitalization. Taking into account the needs relating to digitalization of the Certificate of Origin (CO), Customs administrations are strengthening both operational and organizational capacities to improve efficiencies within the cross-border trading environment.</p> <p>One of the key components of the digitalization of the CO is to support system interconnectivity. This will ensure that systems are interconnected in order to enhance cooperation for automated data exchange between the exporting authorities and importing Customs administrations, enabling the simplification and harmonization of border procedures, streamlining the entire process, and saving time and effort for the businesses and government agencies involved.</p> <p>Two types of proof of origin have been assessed: the CO, and the Declaration of Origin (DO). The Feasibility Study on Interconnectivity of CO and the Study Report on CO Digitalization indicated that most of the existing practices on proof of origin interconnectivity were centred on exchanging CO data, with only a few exchanging DO data. With this in mind, CO interconnectivity is included in the main body of this document, while DO interconnectivity will be included as additional information, attached as Annex IV to this document.</p>
----------------	--

	<p>The purpose is to specify the process that regulates information interaction between partners in the exchange of structured CO data between the exporting and importing countries¹ in order to provide partners with:</p> <ul style="list-style-type: none"> - a reference (this CO Interconnectivity Framework) for enabling exchange of CO data under bilateral or multilateral FTA; and - a guide for the development of a technological solution for CO Interconnectivity between parties. <p>The Interconnectivity Framework was developed based on the experience on preferential CO. However, the framework, in particular aspects on business process models and technological specifications (Chapter III and IV), could be referenced for either non-preferential or preferential CO. Members may decide the type of the CO to be exchanged based on the framework at the implementation level.</p>
Advantages to government	<p>Advantages to government of implementing this CO Interconnectivity Framework include:</p> <p>Establishing sustainable trade practices by replacing paper-based CO with the electronic document;</p> <p>Permitting the electronic data transfer of CO information between exporting and importing countries, allowing real-time information sharing, streamlining and expediting of the origin-based treatment claim process and enhancing trade facilitation;</p> <p>Enabling the transmitting of CO data at the commencement of a Customs procedure in the Country of Export/Exit, and analysis of data using pre-defined risk criteria;</p> <p>Expedited goods movement processing and better resource planning as a result of access to CO information provided by the Country of Export/Exit, leading to reduced fraud and, as a result of a better risk analysis, to better enforcement; and</p> <p>Providing a basis for improving rules of origin by monitoring the utilization of free trade agreements.</p>
Advantages to business	<p>Advantages to business of implementing this CO Interconnectivity Framework include:</p> <p>Promoting harmonized processing of regional goods declarations;</p> <p>Promoting cross-border reuse of data to expedite Customs declarations; and</p> <p>In conjunction with other measures (sharing of advance information, pre-arrival processing, One Stop Border Post), reducing processing times at border posts from days to hours.</p>
Legal framework and compliance	<p>The GNC Legal Toolbox provides the context for Customs to Customs data exchange as follows:</p>

¹ For the purpose of this document, country means Customs territory or Customs Union.

	<p>Article 1 Automatic exchange of information for risk management purposes.</p> <p>Article 2 Utility Blocks.</p> <p>Article 3 Use of information.</p> <p>Article 4 Confidentiality and protection of information.</p> <p>Legal Framework – Contracting Parties should ensure:</p> <p>Domestic legislation that is administered by/applicable to each Contracting Party’s Customs administration, and which suitably enables the intended e-CO data exchange.</p> <p>FTA which is/are in force between Parties, and which suitably enable/s intended e-CO data exchange.</p> <p>Implementation arrangement(s) between Partners' Customs Administrations that give effect to the intended e-CO data exchange in terms of relevant, enabling legislation and FTA.</p> <p>Compliance – Partners should ensure:</p> <p>Data disclosure, exchange, handling, use, storage, and protection by their Customs administrations in accordance with their own and each other’s domestic legislation, relevant FTA and agreed implementation instrument;</p> <p>Consistency, security, protection and availability of their own and each other’s data in and across their respective systems; and</p> <p>Synchronization of any code lists or tables required for the validation and/or authentication of exchanged data across respective IT systems.</p>
<p>Entities layer</p>	<p>The following entities play roles in the origin interconnectivity:</p> <p>Parties involved in FTA</p> <p>Applicant</p> <p>Issuing authorities</p> <p>Outbound data authorities (e.g. Single Window)</p> <p>Inbound data authorities (e.g. Single Window)</p> <p>Customs of the import country</p> <p>Declarant</p> <p>With regard to the data exchange interaction, each entity may play a role as the “sending entity” and “receiving entity”.</p>
<p>Business rules layer</p>	<p>To ensure consistent application of CO interconnectivity, a set of business rules has been defined as follows:</p> <p>Establishment of contact points between partner countries (BR.1)</p> <p>Export countries should establish automated CO issuance systems (BR.2)</p>
<p>Trigger layer</p>	<p>The UB features the following sequences for choreographing interactions between the partners. Events which initiate electronic data flow:</p> <p>CO issued: when upon the request of the applicant, the issuing authority of the export country completes the CO issuance process.</p> <p>CO amendment requested: Export/Exit or Transit Country transmits Export/Transit Message to Transit Country or Import/Entry Country.</p>

	<p>CO claimed: When a decision on origin-based treatment is made, the importing Customs will transmit the feedback on origin-based treatment.</p>
<p>Data cluster layer</p>	<p>Within the CO interconnectivity system, involved parties transmit the following information:</p> <ul style="list-style-type: none"> CO data Acknowledgement CO cancellation notification CO cancellation decline/acceptance Feedback on the origin-based treatment status <p>All data is transmitted using the WCO DM-compliant electronic message.</p>
<p>Integration layer</p>	<p>CO interconnectivity interconnects Customs automated clearance systems of the participating countries through messaging gateways. All participating gateways are configured following a distributed systems integration architecture.</p> <p>The distributed system integration architecture aligns with the core GNC-UB core principles where Customs to Customs interconnectivity systems are to be established at bilateral/plurilateral level in accordance with available international standards.</p>
<p>Interface layer</p>	<p>The interface segment defines how participating gateways interconnect one to another. The segment outlines standards, requirements and specifications for the service protocol, service patterns, service operation names, and electronic message format.</p> <p>The service interface protocol within the systems could operate using two primary protocols for data exchange: JSON API and XML. The use of either can be considered to further expand interoperability and data exchange capabilities.</p>
<p>Communication layer</p>	<p>The CO electronic messages are transported over a network communication infrastructure. The CO interconnectivity Framework does not prescribe one particular type of network communication infrastructure. Participating countries may decide the type of the network communication at the bilateral level.</p> <p>Some network communication infrastructure types that could be considered include the dedicated (leased) line, public internet, Transport Layer Security (TLS) or Virtual Private Network (VPN).</p>

1.3 Intended readership

This document is addressed to:

- The WCO function/entity responsible for the deployment of GNC to review and comment on the structure and content of the UB;
- The WCO Technical Committee on Rules of Origin (TCRO), Permanent Technical Committee (PTC) and any other WCO groups deemed necessary to review and comment on the structure and content of the UB;
- Any person involved in the establishment of an international arrangement/agreement on IT connectivity and data exchange on Certificates of Origin, to provide recommendations regarding the improvement of the material provided; and
- Any person responsible for the implementation of information exchange between countries, to provide inspiration for setting up such exchange between non-participating countries.

1.4 Acronyms and abbreviations

Abbreviation or Acronym	Description
BPM	Business Process Model
CO	Certificate of Origin
DO	Declaration of Origin
FTA	Free Trade Agreement
GNC	Globally Networked Customs
UB	Utility Block
UML	Unified Modelling Language
WCO	World Customs Organization
WCO DM v.4	WCO Data Model Version 4.0.0

1.5 Reference documents

Ref.	Title	Publisher	Version
1	Specific Annex K of the Revised Kyoto Convention	WCO	
2	WCO GNC Feasibility Study	WCO	
3	WCO Origin Compendium	WCO	
4	WCO Data Model	WCO	4.0.0

1.6 Implementation history

FTA reference	Parties	Status at date of publishing
<i>Korea - Indonesia FTA</i>	<i>Korea - Indonesia</i>	<i>Testing and piloting</i>
<i>The implementation history entry above was added only as an example</i>		

2. CONTEXT AND PURPOSE

The CO is a specific form, in which the authority or body of the exporting country empowered to issue it certifies expressly that the goods to which the certificate relates originate in a specific country. This CO also includes a declaration by the manufacturer, producer, supplier, exporter or other competent person. In general, a claim for preferential tariff treatment is required to be supported by a proof of origin, which must be presented to the Customs authority of the importing country upon request.

Traditionally, origin certification processes are manual, paper-based, slow and cumbersome. Exporters have to submit a request for a CO to the competent issuing authority and, after the information is verified by the competent authority, the CO can be printed on paper with a manual signature and stamp to validate its authenticity. The hard-copy CO is then handed over to the exporter, and afterwards submitted to the importing Customs for the Customs declaration. Manual origin certification processes are prohibitive to trade and not in line with trade facilitation objectives. In addition, paper-based origin certification is prone to origin fraud.

There is increased interest from different stakeholders in managing origin-related procedures of international trade through digitalization. Taking into account the needs relating to digitalization of the CO, Customs administrations are strengthening both operational and organizational capacities to improve efficiencies within the cross-border trading environment. One of the key components of the digitalization of the CO is to support system interconnectivity. This will ensure that systems are interconnected in order to enhance cooperation for automated data exchange between the exporting authorities and importing Customs administrations, enabling the simplification and harmonization of border procedures, streamlining the entire process, and saving time and effort for the businesses and government agencies involved.

In line with the World Customs Organization (WCO) Strategic Plan 2022-2025 to enhance digitalization and Customs cooperation (FA1. Technology and innovation), as well as reinforcement of Customs cooperation and cooperation with key stakeholders (SP2), and taking into account the need to facilitate the establishment of smooth and efficient exchange of information related to CO, in 2022-2023 the WCO conducted, with the support of Members, a survey on the digitalization of the CO. The Study on the Digitalization of the CO was developed by the WCO Secretariat, based on 84 responses received. The survey indicated that 22 Members (26.2% of the Members responding) had implemented a data exchange system on Certificates of Origin. Furthermore, 9 Members responded that they were in the process of developing or constructing a data exchange system on Certificates of Origin. In addition, data exchange on CO is practised in multiple regions, including Asia and the Pacific, Africa, North America, South America, and Europe.

As for the challenges in establishing an electronic data exchange programme: the alignment of technical standards and specifications with other contracting parties was reported as a common challenge. Other common challenges were mutually agreeing on the data element standards, message implementation guidelines and business process specifications.

The Interconnectivity Framework for CO aims to provide partners with a reference (this CO Interconnectivity Framework) for enabling exchange of CO data under bilateral or multilateral FTA; and Guide the development of a technological solution for CO Interconnectivity between parties; The Interconnectivity Framework helps to develop interconnectivity systems in a cost-effective and faster way. It enables the parties involved to reuse their established interconnectivity system for origin certification, verification and Customs clearance processes, by ensuring that the CO interconnection developed with new partners in accordance with the Framework is fully compatible with the existing system.

The scope of the Interconnectivity Framework referred to in this document is broadly understood as the transmission of electronic data on the CO between two or more governments through the interconnection of computerized systems administered by Customs or any other government agencies.

Under the Interconnectivity Framework for Certificates of Origin, two types of proof of origin have been assessed: the CO involving a specific form issued by the competent authority, and the Self-Declaration of Origin.

The Feasibility Study results on the Interconnectivity Framework for CO and the Study Report on the Digitalization of CO indicated that most of the existing practices on proof of origin interconnectivity were centred on exchanging CO data, with only a few exchanging Self-Declarations of Origin. With this in mind, CO interconnectivity is included in the main body of the Study, while Self-Declaration of Origin (DO) interconnectivity will be included as additional information, attached as Annex IV to this document.

The Interconnectivity Framework was developed based on the experience on preferential CO. However, the framework, in particular aspects on business process models and technological specifications (Chapter III and IV), could be referenced for either non-preferential or preferential CO. Members may decide the type of the CO to be exchanged based on the framework at the implementation level.

2.1 Advantages

2.1.1 Advantages to government

The following advantages are envisaged for the governments of the countries involved:

- Permitting the electronic data transfer of CO information between exporting and importing countries, allowing real-time information sharing, streamlining and expediting of the origin-based treatment claim process and enhancing trade facilitation;
- risk assessment prior to arrival of goods;
- data-matching; and
- Confirmation of origin-based treatment.
- Expedited goods movement processing and better resource planning as a result of access to CO information provided by the Country of Export/Exit, leading to reduced fraud and, as a result of a better risk analysis, to better enforcement; and
- Monitoring the utilization of the FTA, either with regard to specific Certificates of Origin, or to specific industries or products, and utilizing it as a reference tool to evaluate the extent to which businesses are taking advantage of reduced or eliminated tariffs.

2.1.2 Advantages to Customs

The following advantages are envisaged for Customs administrations:

- Use of harmonized data which has been validated by the country's Customs administrations, ultimately leading to expedited processing of import of goods and increased data quality between countries;
- Better enforcement and alignment of risk assessment criteria;
- Better information for origin-based risk analysis purposes since approved CO data is available;
- Cost reductions due to broader cooperation among exporting and importing authorities and use of synergies, leading to less fraud;
- Better information sharing between countries;
- Low costs to establish the technical annex (using this CO Interconnectivity Framework as the template) and a consequent reduction in IT implementation, faster implementation and an increased time span of use;
- Quick(er) implementation of CO data exchange under international Free Trade Agreements and shorter discussions between the parties of the FTAs for establishment of CO data exchange arrangements; and
- Enhanced quality and integrity of data for audit and risk management, etc.

2.1.3 Advantages to business

The following advantages are envisaged for business/stakeholders:

- Cost reduction due to harmonized data, processes and statutes;
- Reduction in processing time at the border;
- Acceleration of Customs procedures and facilitation of legitimate trade;
- Cost reductions due to the automated processing of issuance of Certificates of Origin and Customs clearance. This reduces the need for manual intervention, streamlining the entire process and avoiding redundant efforts; and
- Enhanced transparency and predictability concerning the CO and treatment from Customs authorities, provided by harmonization of processes and data and enhanced cooperation among Customs administrations.
- Economic and societal protection
 - Reduction in origin-related smuggling and boost in the fight against origin-related organized crime;
 - Reduction in origin fraud – contributing to the proper collection of Customs duties;
 - Reduction in corruption;
 - Improvement of “Risk analysis” and “Risk Profiling” on the CO data; and
 - Improvement of overall organizational capacity of partner administrations.
- Global integration
 - Promote/improve cross-border communication and cooperation;
 - Encourage government agencies to work together; and
 - Provide sustainability in administrative cooperation.

2.2 Legal framework and compliance

2.2.1 Legal framework

E-CO data exchange must be based on a rigorous but realistic domestic and international legal framework that gives Contracting Parties confidence in reciprocal data exchanges. This confidence must extend to important areas such as electronic transactions, data protection, privacy, authentication, and the integrity of the process. The legal framework must not only allow for the exchange of GNC information, but it must also consider the following enabling aspects:

- Ensuring automatic exchange of information for trade facilitation and risk management purposes.
- Making use of Utility Blocks
- Managing the use of information received; and
- Ensuring the confidentiality and protection of information

When examining the legal framework governing e-CO data exchange, it is essential to recognize the distinctive aspects of its distribution. In the context of a trade agreement, the issuing authority of the exporting party issues a CO, which is then submitted to the Customs administration of the importing party. This submission is a critical step for claiming the benefit of origin-based treatment.

E-CO exchange would benefit from the incorporation of relevant enabling provisions in legislation and in existing or new FTA. It is important to note that in this context, Customs matters should be regarded as covering the broadest possible area of laws and regulations on the cross-border traffic of goods to ensure proper application of Customs laws, the security of the international trade supply chain, trade facilitation, and the prevention, investigation and combating of Customs offences.

A. Domestic legislation

Domestic legislation is essential for e-CO exchange since it governs the sharing, handling and protection of Customs information between Contracting Parties' administrations. Ensuring a proper, sustainable and consistent domestic legal basis across all Contracting Parties, aligned with common international standards and obligations, should be a key objective. At a minimum, areas to provide for include:

- Sharing information, including personal information, with another Customs administration on an automatic basis, in advance and in a structured and systematic manner;
- Protecting, using, handling, storing, or discarding Customs information that is being disclosed and received; and
- Implementing relevant arrangements or similar appropriate instruments with other Customs administrations to implement such sharing.

Example

Legal provision on use of the electronic version of the CO

Example from China

- To facilitate the implementation of the China-Republic of Korea Free Trade Agreement (hereinafter referred to as the 'China-Korea FTA') Electronic Origin Data Exchange and simplify the submission process for Certificate of Origin, the following announcement is hereby issued:
For goods declared under the China-Korea FTA preferential tariff, Customs will no longer require the importer or their agent to submit the original Certificate of Origin at the time of import declaration. However, Customs reserves the right to request supplementary submission of the relevant original certificate of origin when deemed necessary.

Example from Uruguay

- General Resolution No. 24/2022: Control procedure for the reception and declaration of the Certificate of Origin in accordance with the Economic Complementation Agreement No. 60 with the United Mexican States.
General Resolution No. 37/2021: Control procedure for the reception and declaration of the Certificate of Origin in accordance with the Economic Complementation Agreements Numbers 35 and 73 with the Republic of Chile.

Legal provision enabling automated CO data transfer

Example from Korea

- Act on Special Cases of the Customs Act for the Implementation of Free Trade Agreements
 - Article 9 (Requests for Ex Post Facto Application of Conventional Tariffs) (3): When filing a request referred to in paragraph (1) or (2), an importer shall submit a document evidencing origin. Nevertheless, of the origin-evidencing document, submission of Certificate of Origin may be omitted for the goods imported from the Contracting State, where the electronic origin data exchange system referred to in

Article 33 Paragraph 2 Subparagraph 4 is in place and in operation and the information from the Certificate of Origin was electronically exchanged through the system.

- Article 33 (Reciprocal Cooperation) (2) The Commission of the Korea Customs Service may cooperate with the customs authority of any Contracting State, as prescribed by the relevant agreement for uniform and efficient implementation of the agreement as follows:

4. the establishment and operation of the system enabling electronic exchange of the Certificate of Origin information with the customs authority of the Contracting Party, which is filed and issued in accordance with Article 11 Paragraph 1 Subparagraph 1.

Example from Uruguay

- General Resolution No. 24/2022: Control procedure for the reception and declaration of the Certificate of Origin in accordance with the Economic Complementation Agreement No. 60 with the United Mexican States.
General Resolution No. 37/2021: Control procedure for the reception and declaration of the Certificate of Origin in accordance with the Economic Complementation Agreements Numbers 35 and 73 with the Republic of Chile.

Legal provision on personal data protection

Example from Uruguay

Personal Data Protection Law No. 18.331

“Article 23: Data transferred internationally – The transfer of personal data of any kind to countries or international organizations that do not provide adequate levels of protection in accordance with the standards of international or regional law on the matter is prohibited.

The prohibition will not apply when *it concerns*:

- 1) International judicial cooperation, in accordance with the respective international instrument, whether treaty or convention, taking into account the circumstances of the case.
- (2) Exchange of medical data, where required by the treatment of the affected party for reasons of public health or hygiene.
- (3) Bank or stock transfers, in relation to the respective transactions and in accordance with the legislation that is applicable to them.
- (4) Agreements within the framework of international treaties to which the Eastern Republic of Uruguay is a party.
- (5) International cooperation between intelligence agencies for the fight against organized crime, terrorism and drug trafficking.”

B. International treaties

E-CO exchange also requires complementing domestic legislation with a suitable FTA as the enabling international legal basis.

It is recommended that the FTA include important elements that:

- Enable the Contracting Parties to share origin-related information with each other on an automatic and advanced basis by mutual arrangement; and
- Provide for any obligations or conditions for such exchange and for the protection, use, handling, storing, or discarding of shared information, including personal information.

Example

RCEP Chapter 3, Article 3.29: Electronic System for Origin Information Exchange

- The Parties may develop an electronic system for origin information exchange to ensure the effective and efficient implementation of this Chapter in a manner jointly determined by the relevant Parties.

RCEP Chapter 3, Article 3.16: Proof of Origin

- 5. A Proof of Origin shall: (a) be in writing, or any other medium, including electronic format as notified by an importing Party ...

Agreement: Korea-Indonesia CEPA, Article 3.16 (Certificate of Origin)

2. For purposes of this Agreement, a Certificate of Origin is any of: (a) a certificate of origin in paper format; or (b) an electronic certificate of origin.

FTA México-Uruguay Decision No. 03/2020:

1. The certificate of origin in digital format and the documents linked to it shall have the same legal validity as the certificate of origin in paper format with a handwritten or facsimile signature and a stamp in ink or image, provided that they are issued and digitally signed in accordance with the respective laws of the Parties, by duly authorized entities and officials, in accordance with the procedures and technical specifications of the Digital Certification of Origin established in Resolution 386 of the ALADI Committee of Representatives, as well as its amendments and/or supplements.

2. Certificates of origin in digital format shall be exchanged through the Single Window for Foreign Trade (VUCE) of each Party by means of an interoperability platform, in accordance with electronic version number 4.0 of the XML Schema (XSD) of the DCO or a higher version.

FTA 35 Chile-MERCOSUR 63° Additional Protocol, Annex 13, Article 11/ (FTA 73 Chile-Uruguay), Chapter 2, Section A, Article 2.8:

“The Certificate of Origin mentioned in the previous paragraph in its digital format, and the documents linked to it, will have the same legal validity as the Certificate of Origin in paper format and handwritten signature, provided that they are issued and digitally signed in accordance with the respective legislation of the Signatory Parties, by duly authorized entities and officials, in accordance with the procedures and technical specifications of the Digital Certification of Origin established in Resolution 386 of the ALADI Committee of Representatives, its amendments and/or supplements.”

C. Implementing instruments at administration level

Contracting Parties that have an enabling domestic and international legal basis in place and seek to implement e-CO exchange with each other should put administrative instruments in place between their Customs administrations to provide for such implementation, such as an Arrangement for Automatic Data Exchange, Memorandum of Implementation, Memorandum of Understanding (MOU), etc. Such administrative instruments can be done on a bilateral or regional Customs-to-Customs basis and would set out the agreed implementation of data exchange, taking into account respective mandates and the enabling legal, operational and systems frameworks. The instruments would only apply to the participating administrations and would not bind the respective governments as a whole. They would also not be used as a substitute for required domestic legislation or treaties or used to in any way amend, supplement, or detract from existing legal frameworks.

Contracting Parties are further encouraged to use the CO Interconnectivity Framework as the template for any technical annex to such an implementation instrument, if deemed necessary. Among other things, a technical annex would define the process regulating the exchange of information between the Contracting Parties, which underpins the CO Interconnectivity Framework. Furthermore, the CO Interconnectivity Framework defines the responsibilities of the Contracting Parties, the data to be exchanged, its structure, and the general methods of the exchange. In addition, it sets the terms for mutual assistance, mutual recognition, and mutual cooperation.

2.2.2 Compliance

For the exchange of information under this CO Interconnectivity Framework, each Contracting Party must ensure that their Customs administrations comply with relevant domestic legislation and FTA obligations regarding the disclosure, exchange, handling, use, and protection of their own and each other's information. Measures for secure data transfer, data consistency and data availability and/or unavailability must also be specified and followed. The elements below are considered to be key requirements.

Electronic Data Interchange (C.1)

Data exchange under this CO Interconnectivity Framework is "Electronic Data Interchange", which Partners should consider defining along the following lines in legislation.

Automatic Exchange of Information (C.2)

Data exchange under this CO Interconnectivity Framework will be triggered automatically and according to mutually agreed processing rules by Contracting Parties' automated CO systems, and should normally not require human intervention. Partners should enable this in domestic legislation and the applicable FTA, while providing for it in the relevant implementing instrument.

If Contracting Parties believe their FTA basis to be weak, they can include enabling FTA provisions such as:

"The Customs administrations may, by mutual arrangement in accordance with Article [x], exchange any information covered by this Agreement on an automatic basis." (Article 6, WCO Model Bilateral Agreement)

The relevant implementing instrument should provide the agreed-upon information or data cluster that will be exchanged on an automatic basis.

Advanced Exchange of Information (C.3)

Data exchange under this CO Interconnectivity Framework will be triggered by the issuance of an CO in the "sending" Contracting Party's CO issuance systems, with the e-CO data being provided to the "receiving" Contracting Party.

If Contracting Parties believe the FTA basis to be weak, they can include enabling FTA provisions such as:

“The Customs administrations may, by mutual arrangement in accordance with Article [x], exchange specific information in advance of the arrival of consignments in the territory of the other Contracting Party.” (Article 7, WCO Model Bilateral Agreement)

The relevant implementing instrument should provide the agreed-upon information or data cluster that will be exchanged in advance.

Coverage (C.4)

Data exchange under this CO Interconnectivity Framework will cover all CO for movements where goods physically cross from one Contracting Party to another Contracting Party, or cross multiple Contracting Parties, and are considered movements under the “International Trade Supply Chain”. Contracting Parties should consider defining “International Trade Supply Chain” as follows in the relevant legislation, FTA basis and/or implementing instrument, if such definition is deemed necessary:

“International Trade Supply Chain” shall mean all processes involved in the cross-border movement of goods from the place of origin to the place of final destination.” (Article 1 (g), WCO Model Bilateral Agreement)

Technical Assistance to implement the CO Interconnectivity Framework (C.5)

The commitment between Contracting Parties’ Customs administrations to assist each other in implementing the information exchange under this CO Interconnectivity Framework should be clearly provided for in the relevant implementing instrument.

Use of Information Exchanged under this CO Interconnectivity Framework (C.6)

Information exchanged under this CO Interconnectivity Framework is subject to conditions of use as defined in the relevant domestic legislation and FTA basis, and the use of shared information should be clarified by the Contracting Parties’ Customs administrations and stipulated in the relevant implementing instrument.

If Contracting Parties believe the FTA basis to be weak, they can include enabling FTA provisions such as:

“Any information received under this Agreement shall be used only by the Customs administrations of the Contracting Parties and solely for the purpose of administrative assistance under the terms set out in this Agreement.” (Article 24 (1), WCO Model Bilateral Agreement)

“On request, the Contracting Party that supplied the information may, notwithstanding paragraph 1 of this Article, authorize its use by other authorities or for other purposes, subject to any terms and conditions it may specify. Such use shall be in accordance with the legal and administrative provisions of the Contracting Party which seeks to use the information. The use of information for other purposes includes its use in criminal investigations, prosecutions or proceedings.” (Article 24 (2), WCO Model Bilateral Agreement)

Confidentiality of Information (C.7)

Information exchanged under this CO Interconnectivity Framework is subject to conditions and requirements of confidentiality as defined in the relevant domestic legislation and FTA basis, which should be clarified by the Contracting Parties’ Customs administrations and stipulated in the implementing instrument.

If Contracting Parties believe the FTA basis to be weak, they can include enabling FTA provisions such as:

“Any information received under this Agreement shall be treated as confidential and shall, at least, be subject to the same confidentiality and protection as the same kind of information is subject to under the legal and administrative provisions of the Contracting Party where it is received.” (Article 25 (1), WCO Model Bilateral Agreement)

Personal Data Protection (C.8)

Information exchanged under this CO Interconnectivity Framework may be subject to conditions and requirements of Personal Data Protection as defined in the relevant domestic legislation and FTA basis, which should be clarified by the Contracting Parties and stipulated in the implementing instrument.

If Contracting Parties believe the FTA basis to be weak, they can include enabling FTA provisions such as:

“Personal data exchange under this Agreement shall not begin until the Customs administrations have, by mutual arrangement in accordance with Article 28, decided that such data will be afforded, in the territory of the Contracting Party where it is received, a level of protection that satisfies the requirements of the national law of the supplying Customs administration.” (Article 25 (2), WCO Model Bilateral Agreement)

“In the absence of a mutual arrangement as referred to in paragraph 2 of this Article, personal data may only be supplied when the supplying Customs administration is satisfied that such personal data will be protected in the territory of the Contracting Party where it is received, in accordance with paragraphs 4 to 10 of this Article.” (Article 25 (3), WCO Model Bilateral Agreement)

“On request, the Customs administration receiving personal data shall inform the Customs administration which supplied that data of the use made of it and the results achieved.” (Article 25 (4), WCO Model Bilateral Agreement)

“Personal data supplied under this Agreement shall be kept only for the time necessary to achieve the purpose for which it was supplied.” (Article 25 (5), WCO Model Bilateral Agreement)

“The Customs administration supplying personal data shall, to the extent possible, ensure that this data has been collected fairly and lawfully and that it is accurate and up to date and not excessive in relation to the purposes for which it is supplied.” (Article 25 (6), WCO Model Bilateral Agreement)

“If personal data supplied is found to be incorrect or should not have been exchanged, this shall be notified immediately. The Customs administration that has received such data shall amend or delete it.” (Article 25 (7), WCO Model Bilateral Agreement)

“The Customs administrations shall record the supply or receipt of personal data exchanged under this Agreement.” (Article 25 (8), WCO Model Bilateral Agreement)

“The Customs administrations shall take the necessary security measures to protect personal data exchanged under this Agreement from unauthorized access, amendment or Dissemination.” (Article 25 (9), WCO Model Bilateral Agreement)

“Either Contracting Party shall be liable, in accordance with its legal and administrative provisions, for damage caused to a person through its use of personal data exchanged under this Agreement. This shall also be the case where the damage was caused by a Contracting Party supplying inaccurate data or supplying data that is contrary to this Agreement.” (Article 25 (10), WCO Model Bilateral Agreement)

Mutual Arrangement (C.9)

Data exchange between the administrations of two or more Contracting Parties shall not begin until they have confirmed and agreed, by mutual arrangement, that such data will be afforded, in the territory of the ‘receiving’ Contracting Party, a level of protection that satisfies the domestic law requirements of the ‘supplying’ Contracting Party. Relevant provisions in domestic legislation and the applicable FTA basis should be clarified between the Contracting Parties and the mutual commitment in this regard should be stipulated in the implementing instrument.

3. BUSINESS PROCESS MODEL (BPM)

The BPM describes how data exchange on the interconnectivity system take places in the context of relevant Customs procedures, such as export, transit and import and the broader supply chain processes. The BPM includes additional processes that take place surrounding the data exchange as additional context to provide comprehensive understanding of the data exchange process. The BPM provides an overview of several GNC segments, namely, the Entities, Business Rules, Triggers, and Data Cluster.

3.1 Data exchange model

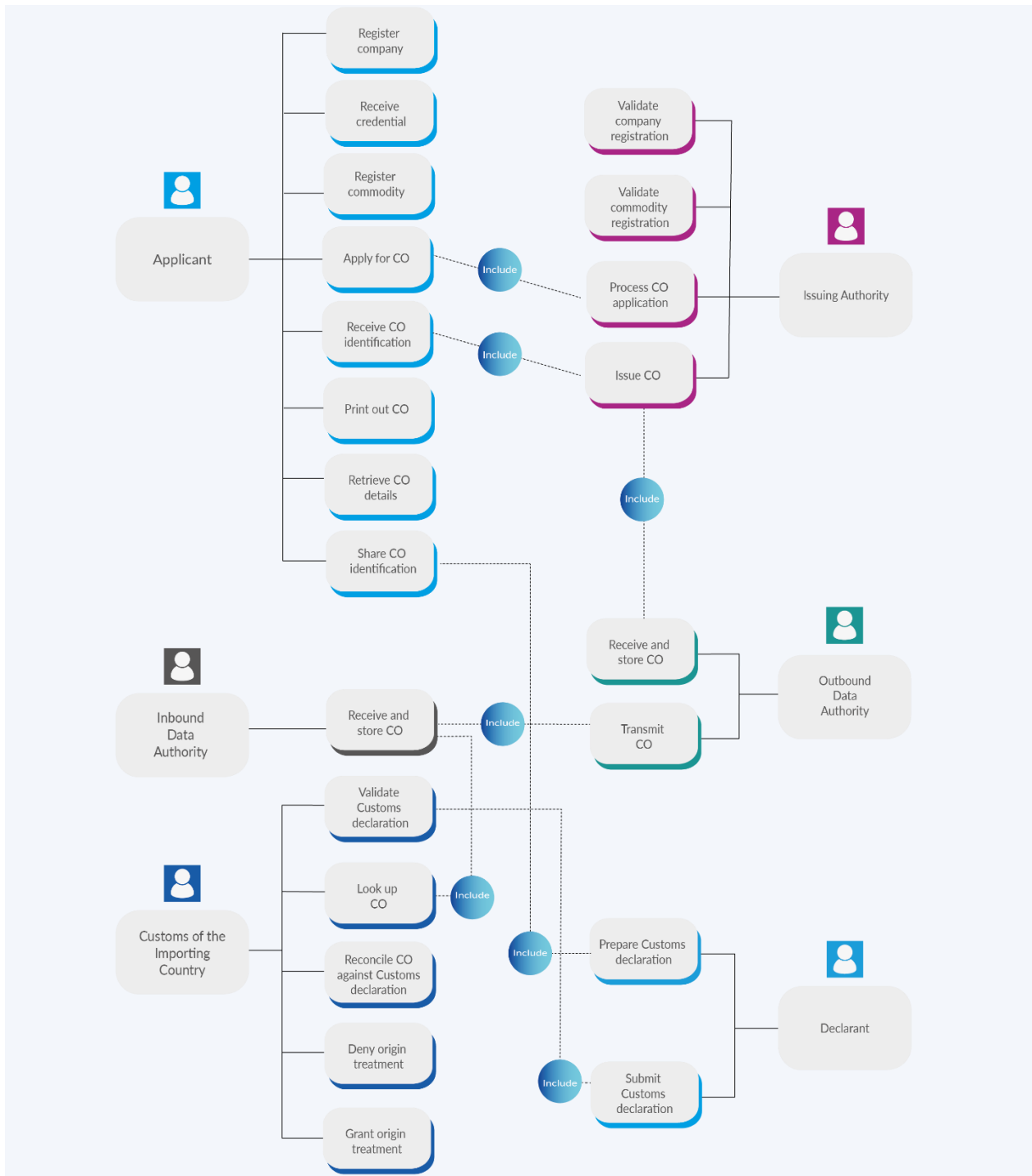
Two data exchange models for the CO were examined, namely, the Push Model and the Pull Model. In the Push Model, after the CO is issued, the exporting country's authority begins the CO data transfer to the importing country's authority. This allows the importing country to receive the CO data almost in real time and in advance of the claiming of the origin-based treatment process (i.e. import clearance). In contrast, the Pull Model requires that the importing country's authority initiate access to the CO data from the exporting country's outbound gateway, normally during the claiming of the origin-based treatment.

Several key points related to both Models include the following:

- Currently, most data exchanges for the CO practised by several WCO Members in different regions are implemented using the Push Model. The Push Model offers real-time data exchange, where the CO can be transmitted by the export country to the import country soon after it is issued.
- However, no fully automated Pull Model practice implemented by WCO Members was observed.
- The practices on Pull Models take place only in a semi-automated way, where the authority of the importing country can get access to the outbound gateway of the exporting country to look up the details of the CO, but is not able to process the data in an automated way.
- In this regard, the Push Model is proposed as the optimal model for the Interconnectivity Framework for the CO, and the Semi-Automated Pull Model will be included as additional information, attached as Annex III to this document.

3.2 Entities

The stakeholders involved in the Push Model are described by the Unified Modelling Language (UML) Use Case Diagram below.



Note: "Include" indicates that the base use case cannot function properly without the included one. The included use case is a necessary subset of the base use case's behaviour. For example, the applicant's action 'Apply for CO' cannot function properly without the issuing authority's action 'Process CO application.'

Figure 1 – UML Use Case Diagram

Entity	Definition	National Practices
Applicant	The entity which applies for CO	Producer, Consignor, Exporter, Seller
Issuing authority	The authority of the exporting country which is responsible for issuing CO	Customs, Ministry of Trade, and authorized issuing body such as Chamber of Commerce,
Outbound data authority	The authority of the exporting country which is responsible for transmitting CO data to the importing country	Single Window, Customs, other authorized data exchange entity
Inbound data authority	The authority of the importing country which is responsible for receiving CO data from the exporting country.	Single Window, Customs, other authorized data exchange entity
Customs of the importing country	The Government Service which is responsible for the administration of Customs law and the collection of duties and taxes, and which also has the responsibility for the application of other laws and regulations relating to the importation, exportation, movement or storage of goods.	Customs
Declarant	The entity which makes a declaration to Customs or – where legally permitted – in whose name, or on whose behalf, a declaration to Customs is made.	Importer, Agent, Consignee, Forwarder

3.3 Business process flow

The Push Process Model of the CO data exchange is described by the UML Activity Diagram below.

The diagram organizes the process flow into several phases (Entity Registration, Commodity Registration and CO Issuance). Each phase is identified with Phase identification number (P.n). Each phase contains actions identified with Action identification number (A.n). The numeric identification does not determine the order/sequence of the action in the process flow. Their order only represents the time when the actions were introduced in the framework. A detailed process description of the process flow is attached as **Annex I** to this document.

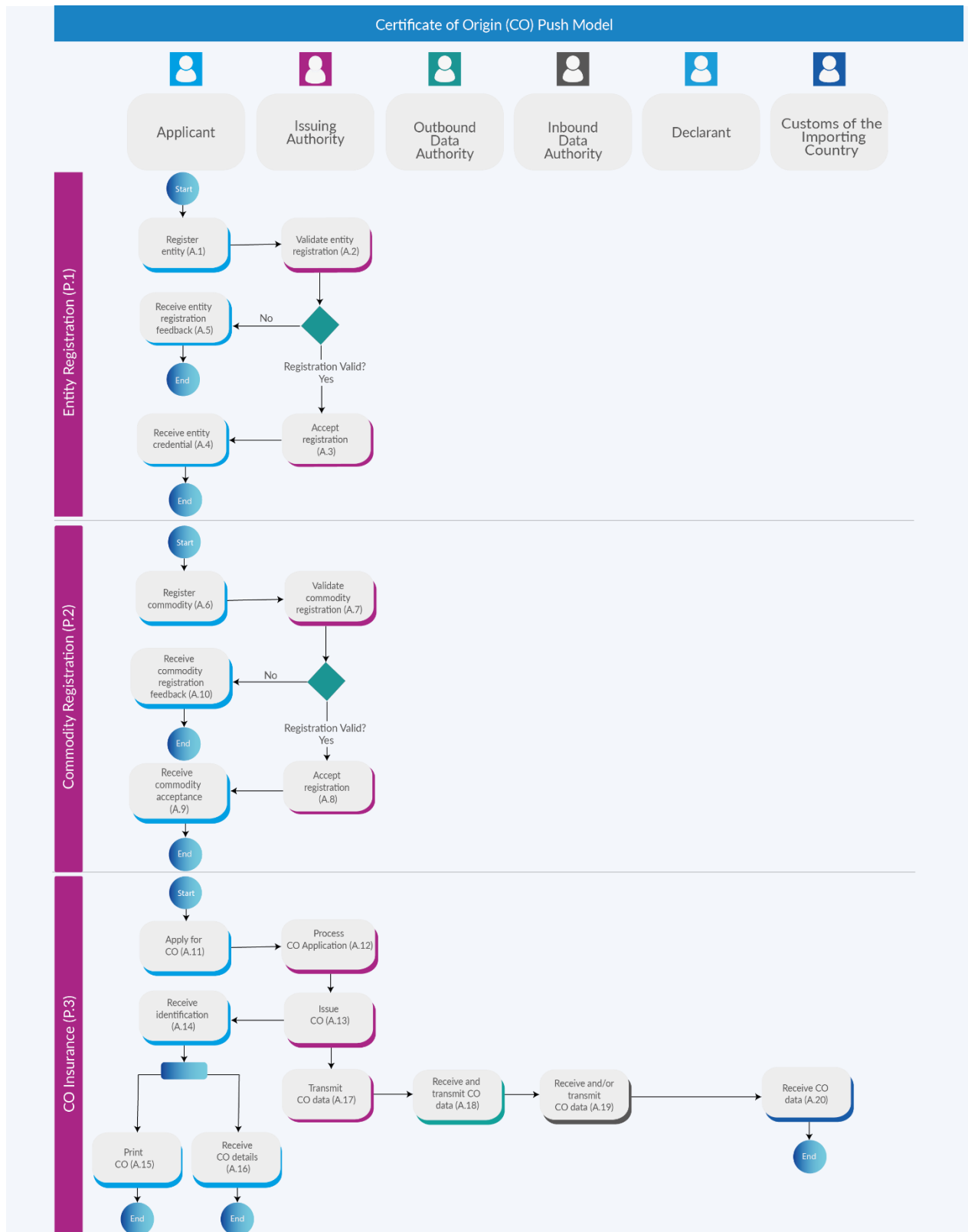


Figure 2 – UML Activity Diagram

3.4 Data exchange sequence

The data exchange sequence outlines the interaction (i.e. send/receive or request/response) between two entities. The sequence is based on the Push Model, where the entity which intends to send data initiates the data exchange. The receiving entity is required to provide the applicable acknowledgement or error response for each data push.

The data exchange interaction is illustrated by the UML Sequence Diagram below.

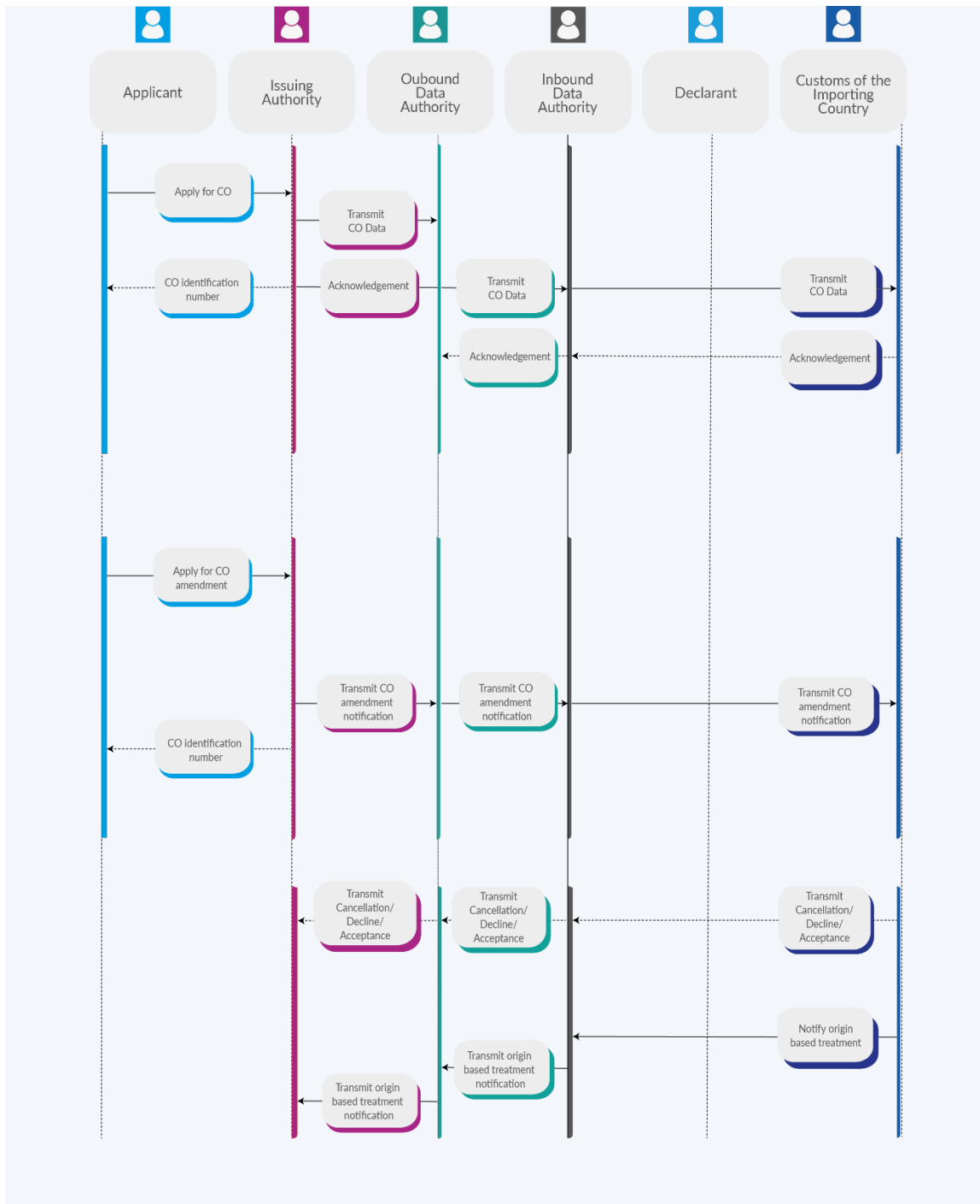


Figure 3 - UML Sequence Diagram

3.5 Triggers

The Trigger segment outlines the events and the timing of when data exchange takes place, including:

- **CO issued (T1):** When upon the request of the applicant, the issuing authority of the export country completes the CO issuance process. Following this trigger, the export Contracting Party will transmit the issued CO data to the import country.
- **CO amendment requested (T2):** When upon the request of the applicant, the issuing authority of the export country requires confirmation from the importing country that the CO amendment can be made. Following this trigger, the export country will transmit notification of CO cancellation.
- **CO claimed (T3):** When a decision on origin-based treatment is made, the importing Customs will transmit the feedback on origin-based treatment (e.g. granting or rejection of the preferential tariff treatment) to the exporting country.

3.6 Data cluster

All data is transmitted using the WCO Data Model (WCO DM)-compliant electronic message.

The WCO DM is an international standard that provides a globally standardized set of data definitions and electronic messages essential for Customs and other regulatory agencies. It outlines clearly defined data elements, data structures, and messaging guidelines that support digital Customs procedures, enabling interoperability between diverse Customs and other regulatory agencies systems worldwide. Developed collaboratively by WCO Members, it aligns with other international standards, facilitating easier, faster, and more reliable data exchange.

The implementation of the WCO DM is particularly important for CO interconnectivity systems. It enables consistent interpretation of origin-related data exchanged between exporting and importing countries, ensuring smooth processing and verification of certificates. The structured approach provided by the WCO DM helps Customs and other regulatory agencies conduct accurate risk assessments, prevent fraud, and enhance trade facilitation by streamlining the authentication and validation of origin claims.

Within the CO interconnectivity system, parties involved transmit the information below.

- **CO data:** CO data issued by the issuing authorities of the export country.
- **CO cancellation notification:** Notification of the cancellation of a CO in conjunction with a request to amend the CO made by the applicant. The notification is required if confirmation of the CO cancellation by the export country is required before proceeding with the amendment process.
- **CO cancellation decline/acceptance:** Confirmation of the decline/acceptance of a CO cancellation provided by the import country as a response to the prior CO cancellation notification.
- **Origin-based treatment status:** Status of the origin-based treatment (e.g. granting/rejecting of preferential tariff treatment) of the CO provided by the import country to the export country.

3.7 Business rules

To ensure consistent application of CO interconnectivity, a set of business rules has been defined as follows:

Establishment of contact points between Contracting Party countries (BR.1)

- Each Contracting Party should establish national contact points dealing with information exchanged under this CO Interconnectivity Framework.
- Each Contracting Party should notify contact details of contact points and any change thereto.

Partner countries to implement automated customs systems (BR.2)

- Member States have each implemented an automated Customs system.
- Such Customs system shall include capability for Bilateral/Multi-lateral CO Data exchange between Member States.

Exchanged data to conform to Standards (BR.3)

- Traders are following the Single Administrative Document layout key document while preparing CO as outlined in the Data Cluster segment.
- The latest version of the WCO DM shall be the standard for exchanged data elements, data structures and electronic message format as outlined in the Interface segment.
- It is recommended that Member States develop WCO My Information Package (MyIP) for Customs Declarations to ensure that the declaration (B2G) data from which the exchanged data came are standardized.

Push data transmission model (BR.4)

- Exchanged Data should be pushed. Data will be transmitted using the PUSH method.

Acknowledge each UB messages (BR.5)

- The recipient of the electronic message will validate the message and respond to the acknowledge or error message.

4. TECHNOLOGICAL REQUIREMENTS AND SPECIFICATIONS

Technological requirements and specifications standardize approaches to building technical solutions for CO interconnectivity by providing necessary standard references for technology implementation. The CO Interconnectivity technological requirements and specifications are described by three GNC-UB segments: system integration architecture, interface and network communication.

To capture Members' practices regarding technological specifications and requirements, a survey was conducted within the Informal Working Group (IWG). Five (5) Members – namely China, Indonesia, Japan, Korea and Uruguay – shared updates as part of the survey. The practices referenced below are based on the survey findings.

4.1 System integration architecture

CO interconnectivity interconnects Customs automated clearance systems of the participating countries through messaging gateways. All participating gateways are configured following a distributed systems integration architecture. The distributed system integration architecture aligns with the GNC-UB core principles where Customs-to-Customs interconnectivity systems are to be established at bilateral and/or plurilateral level in accordance with available international standards.

The distributed integration architecture model aims at enabling Customs to reuse the same system to interconnect with other Customs administrations in other countries, minimizing the need to build different systems, simplifying system implementation and making interconnectivity implementation cost-effective.

The integration architecture eliminates the need for a centralized platform and/or hub to enable interconnectivity. A centralized platform increases the risk of system failure because all connected systems rely on its resilience (single point of failure, etc.). In addition, unlike distributed systems, which require each country to finance its own systems, it may require a complex funding scheme.

In order to establish CO interconnectivity, a Customs administration needs to implement all standards, requirements and specifications set out in this interconnectivity Framework as much as possible to build a messaging gateway that will connect its Customs systems with the CO ecosystem. Deviation from the Framework’s standards, requirements and specifications will lead to increased complexity, as well as implementation and operational costs.

The CO interconnectivity technical standards, requirements and specifications establish an abstraction for a virtual-centralized interconnectivity infrastructure to the actual distributed, peer-to-peer ecosystem. In other words, although they are connected bilaterally, the CO interconnectivity framework appears to connect each participant to a centralized infrastructure. The CO system integration architecture is outlined in the diagram below:

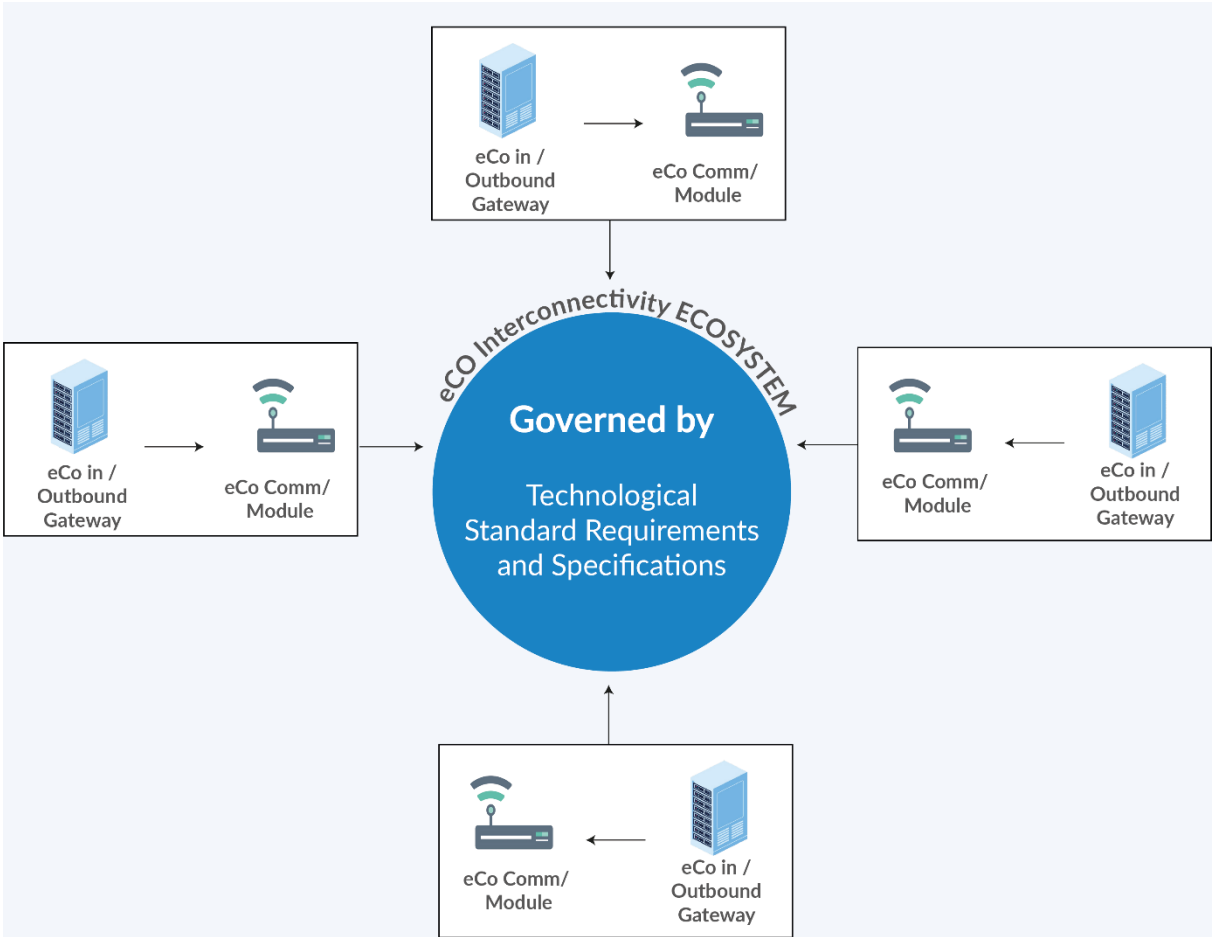


Figure 4 – Integration Architecture

CO interconnectivity uses a service protocol, such as web service or web Application Programming Interface (API). Within the interconnectivity ecosystem, each gateway can function as both a service client and a service provider.

In accordance with Business Rule BR.5, outlining the Push Model, data transmission is initiated by the sending entity by using its gateway as a service client to invoke a specific service hosted by the receiving entity, which is using its gateway as a service provider. Because data can be sent and received both ways, each gateway must be capable of functioning as both a service client and a service provider.

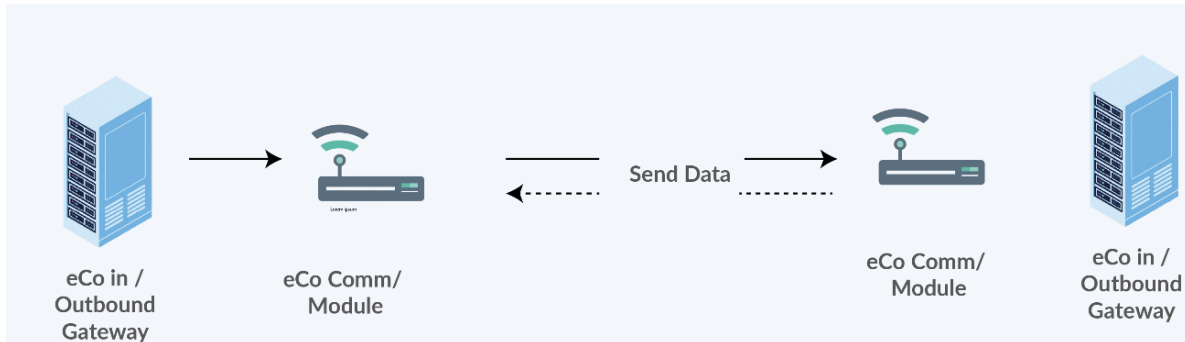


Figure 5 – Gateway Service Roles

The gate service describes the technical process that takes place when sending data. The above-mentioned roles include:

- The gateway of the sending entity transforms data in the Customs clearance system's database into an electronic message in accordance with the format specified in the interface segment of this document.
- The gateway of the sending entity encrypts the electronic message.
- The gateway of the sending entity invokes a service hosted by the gateway of the receiving entity.
- The gateway of the receiving entity decrypts the electronic message.
- The gateway of the receiving entity transforms the electronic message and processes and/or stores it in the Customs clearance system.
- The gateway of the receiving entity prepares a response (acknowledgement, etc.) back to the gateway of the sending entity.

4.2 Interface

The interface segment illustrates how participating gateways can interconnect with one another. It provides examples of standards, requirements and specifications that Member administrations may consider when developing their own service protocols, service patterns, service operation names and electronic message formats.

These examples are not prescriptive but are intended to showcase possible approaches that align with the CO Interconnectivity Framework's objectives. Member administrations retain the flexibility to adopt, adapt or extend these examples according to their unique operational requirements and technological capabilities.

4.2.1 Service Interface Protocol

The service interface protocol within the systems can exchange data using either JSON API or XML, which helps improve interoperability and data exchange capabilities.

CO interconnectivity can use the JSON API protocol. The protocol uses the Java Script Object Notation (JSON) format for sending and/or requesting data through the Rest API. The Rest API is an Application Programming Interface (API) that meets the constraints of the Representational State Transfer (REST) architectural style.

In addition, the eXtensible Markup Language (XML) protocol could be used. XML offers a standardized format for representing structured data, facilitating seamless integration and communication between diverse systems. This protocol follows a Service-Oriented Architecture (SOA), providing a robust framework for transmitting and receiving information across various platforms and applications.

Countries within relevant FTA will engage in bilateral discussions and mutual agreements to determine the preferred protocol for exchanging information. This bilateral approach empowers each country to select the most suitable protocol, either JSON API or XML, that aligns with their specific technological infrastructure, operational requirements, and preferences.

IWG Members' practices

Regarding the service interface protocol, a SOAP web service is being implemented by all five (5) Members who responded to the survey questionnaire.

Additionally, three (3) Members are implementing Restful Web API as well.

None of the responding Members is implementing EDI.

As for the preference regarding the number of service protocols required to connect with different Contracting Parties, all responding Members are open to using different service protocols.

4.2.2 Service patterns

For the purposes of promoting consistent interaction between gateways, this section provides examples of how service patterns can be implemented. The service pattern outlined below is provided as an example using JSON API, showcasing one possible approach to designing interconnectivity solutions.

https://{environment}.coconnect.{domain}/{service_operation}

Variable	Definition	Example/possible value
Environment	The server environment	<ul style="list-style-type: none"> • dev (Development) • test (Testing) • prod (Production)
		<ul style="list-style-type: none"> • customs.go.kr, • beacukai.go.id,

Domain	The domain name of the API	<ul style="list-style-type: none"> • aduana.gub.uy
Service operation	The service operation as defined in the Service Operation section, lower cased and kebab cased (all spaces are replaced with dash character)	send-CO

Example: “https://prod.coconnect.customs.go.kr/send-co” demonstrates a production environment (prod) using the domain name customs.go.kr for the Customs API, with the operation send-co referring to the “send certificate of origin” service.

4.2.3 Service operation

Name	Definition	Service Client	Service Provider	REST Provider
Send CO	Send CO data	Outbound gateway	Inbound gateway	POST
Send cancellation status	Send cancellation status	Inbound gateway	Outbound gateway	POST
Send feedback	Send origin treatment feedback	Inbound gateway	Outbound gateway	POST

4.2.4 Message format

CO interconnectivity exchanges messages using the JSON format. The JSON data structure is determined based on the WCO DM’s CO Information Package published on the WCO DM App

(<https://datamodel.wcoomd.org/#/infopack/scope/national/bceed8417e>).

IWG Members’ practices

Regarding the message format, all five (5) Members who responded to the survey questionnaire use XML. Of these, three (3) Members use JSON as well. None of the responding Members uses EDIFACT.

Additionally, some Members mentioned that they are flexible about using other formats for different payload messages using the same envelope (gateway).

As for the preference on the number of message formats for exchanging e-COs with different Contracting Parties, two (2) Members prefer the single message format, while the other three (3) Members are open to using a different message format.

4.3 Network communication

4.3.1 Network communication infrastructure

The CO electronic messages are transferred over a network communication infrastructure. The CO interconnectivity Framework does not prescribe any particular type of network communication infrastructure. Participating countries may decide on the type of network communication at the bilateral level.

Examples of network communication infrastructure types to consider include:

- Dedicated (leased) line: A network infrastructure established to serve a single purpose and which is disconnected and isolated from the public internet. A dedicated line is relatively more secure compared to other types of network infrastructure.
- Public internet: The internet is an open ecosystem and serves multiple communication purposes. A plain internet-based connection does not provide any security measures. Internet-based network communication is widely available and reasonably inexpensive. The use of public internet without an additional layer of security is not suited for CO interconnectivity purposes.
- Transport Layer Security (TLS): A cryptographic protocol established to provide communications security over the public internet. Hypertext Transfer Protocol Secure (HTTPS) is one example of TLS implementation that could be applied in addition to the public internet. HTTPS makes the public internet suitable for CO interconnectivity.
- Virtual Private Network (VPN): A mechanism to establish a secure connection in addition to an insecure network such as the internet by creating a virtual point-to-point connection by using a tunnelling protocol. Even though implemented on top of the public internet, VPN virtually isolates the communication tunnel from the public internet and provides a higher level of security. VPN provides similar benefits to those of a dedicated line in addition to the more affordable public internet.

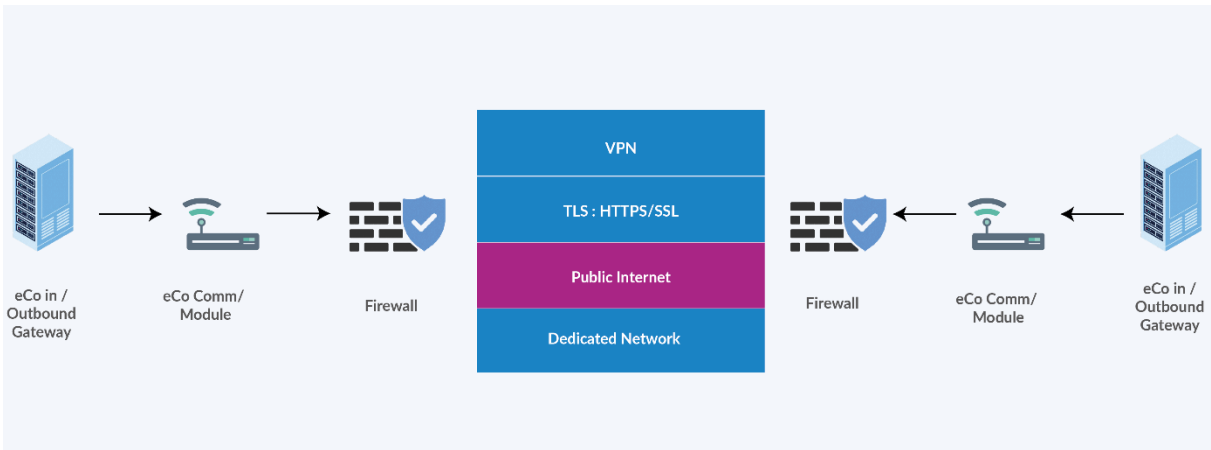


Figure 6 – CO Network Infrastructure

IWG Members' practices

Regarding the network infrastructure type, Transport Layer Security is being used by all responding Members.

A dedicated line is used by two (2) Members; a Virtual Private Network is also used by two (2) Members.

IWG Members' practices

The purpose of an electronic signature is to provide authentication, integrity and non-repudiation for digital documents and transactions. It ensures that the sender of a message is who they claim to be, that the message has not been altered in transit and that the sender cannot deny sending the message.

Currently, all responding Members use an electronic signature for CO data exchange.

For some Members' practices, in a payload that uses an electronic signature, the sender includes an electronic signature in the payload sent to the recipient. The receiving party verifies the electronic signature using a digital certificate previously agreed by both parties.

IWG Members' practices

All responding Members operate the system in the mode of 24 hours a day, 365 days a year, excluding planned outages and other maintenance downtime, in order to ensure the system's availability.

4.3.2 Network and security

A username and password will be included in the HTTP message header. These credentials will be validated, and if validation fails, an immediate rejection message will be returned to the web service consumer. If the validation is successful, the payload will be processed accordingly.

IP addresses will be configured on a firewall to only allow IP addresses of the counterparts. Basic authentication will be used in the communication headers for the REST API.

4.3.3 Service levels

A Service-Level Agreement (SLA) is established to ensure CO reliability and business continuity and to mitigate interruption risk.

- All participating systems will be in operation around the clock and all year round.

- National contact points shall notify planned and unplanned downtime to other Member States.
- For planned downtime, a Member State should aim to provide at least 24 hours' notice to other Member States.
- All Member States will aim to initiate transmission of the export and/or transit messages within one (1) hour of their clearance acceptance.
- The receiving Member State shall send an acknowledgement as a response via the web service.
- In the event of technical and protocol errors, the sending entity is expected to retry every 10 minutes for one hour and alert the support team of the failure to investigate and contact the receiver if required. If the error persists after the initial one-hour retry cycle, the system may undergo subsequent rechecks according to an escalated protocol. The system could retry after the 2-hour mark, 4-hour mark and 8-hour mark, and carry out a final retry at the 16-hour mark. If the error still persists, manual intervention would be necessary to rectify the issue. In this case, the receiving entity should safeguard its systems from storing multiple instances of the same message, particularly if some of the retries are received by its system.
- An alert must be triggered for any rejected messages.

However, these service levels are merely examples that Member administrations may consider when defining their own SLAs. For instance, the retry process described above, in the event of technical and protocol errors, could be replaced with real-time monitoring and the resending of messages in batches once the system stabilizes. This approach helps prevent the risk of overloading the transmission system.

4.4 System security

4.4.1 General security requirements

General security requirements can be summarized as follows:

- Identification and authentication of the communicating parties.
- Authorization: Information and services access policy based on the communicating party's roles and the permissions that come with them.
- Transparent transactions supported by the security audit.
- Reliable and secure transmission.
- Confidentiality and integrity of data during transmitting or archiving.
- Non-repudiation, ensuring that the sender an/or receiver of the message cannot deny sending and/or receiving it.

4.4.2 Security policy

Contacting Parties have to provide and guarantee the security of their gateway and internal systems. The following security policies shall be taken into account:

- The resources and assets must be protected from unauthorized access. (SP1)
- Precautions must be taken to ensure that confidential information is erased from applications and tools as soon as it is no longer required. (SP2)
- Controls should be implemented to ensure that the information supplied to the application systems and tools is accurate and consistent with other information stored elsewhere. (SP3)
- Data that is passed between systems does so without alteration, loss or addition. (SP4)
- The interconnectivity architecture must be designed and managed in order to ensure continuity of service. (SP5)
- Controls must exist to limit the impact of a denial-of-service (DoS) attack mounted against any interconnectivity system's resources. (SP6)
- Data defined under this interconnectivity framework should be exchanged only between entities that have been mutually authenticated. (SP7)

- Information exchanged should be protected from unauthorized disclosure, loss or alteration. (SP8)

All users and communicating parties must be uniquely identifiable.

Precautions must be taken to ensure that an adversary could not use the authentication information to masquerade as a user or communicating party.

4.4.3 Security implementation stack

Security shall be implemented at different levels:

Network level

Network-level protection is important for keeping unauthorized users from reading, changing or deleting information, from the intranet of Contracting Parties.

IWG Members' practices

Currently, IDS, IPS, send data, IP control, SSL, whitelisting and physical security with its own fibre channel (reduy) authentication via certificate are being used by responding Members based on their needs to ensure network-level security.

Transmission level

Transmission-level security is implemented using PKI and Secure Socket Layer (SSL) technologies. These technologies were chosen with the aim of protecting the messages in the transport channel. In addition, they offer authentication, data integrity and data confidentiality.

The internet infrastructure is used for information exchange. Since information in the e-CO data exchanges is considered sensitive, it must be protected from unauthorized access to ensure its confidentiality and integrity. The authentication of the senders and receivers of information must also be ensured. Except for simple acknowledgements, all messages must be encrypted.

IWG Members' practices

Currently, dedicated lines, VPNs, HTTPS and encrypted communication using TLS, digital and SSL certificates are being used by responding Members based on their needs to ensure transmission-level security.

Message level

Message-level security provides end-to-end security by protecting the content of the messages. Using this approach, the actual content will only be available to the desired recipient, regardless of the number of hops.

The use of XML provides the opportunity to apply different security models of varying granularity. These techniques can be applied within the document and refer to signing and encrypting portions of XML messages. The main relevant developments that specify the above-mentioned XML security issues are XML encryption and the related XML Signature.

XML Signatures were incorporated to reinforce the authority of the sender and XML encryption to provide element-wise encryption in combination with traditional transport-level security.

To guarantee the confidentiality, a secure connection SSL (HTTPS) shall be used. Also, all XML messages shall be encrypted and digitally signed. To encrypt and sign messages, digital certificates issued by the WCO Certificate Authority should be used. Another advantage of using digital signatures is that they ensure the integrity of XML datasets.

In addition, non-repudiation has to be guaranteed, which should confirm the user's action beyond doubt using a series of metadata such as user identity, date and time.

IWG Members' practices

Currently, data encryption/decryption, electronic signatures and signature keys are being used by responding Members based on their needs to ensure message-level security.

Business level

Security issues at the business level are mainly related to access control and document state control. The mechanism used to guarantee the access control (either related to a service or a document) has been modelled by authorizations assigned to each communicating party. The correct sequence of the permitted statuses in a lifecycle of documents is governed by the business rules.

IWG Members' practices

Responding Members reported that access control is implemented by using ID/password authentication, single sign-on (SSO) or electronic signature verification.

According to some Members' responses, application-level security requires several steps, e.g. authentication, authorization, log recording, application security testing, ethical hacking and transmission of encrypted information.

Additionally, the system needs to comply with the development guidelines published by the government to ensure that there are no software security weaknesses in the development and operation of information systems, and to check and take measures against web vulnerabilities published by OWASP and others.



ANNEX I: Business Process Description

I. Introduction

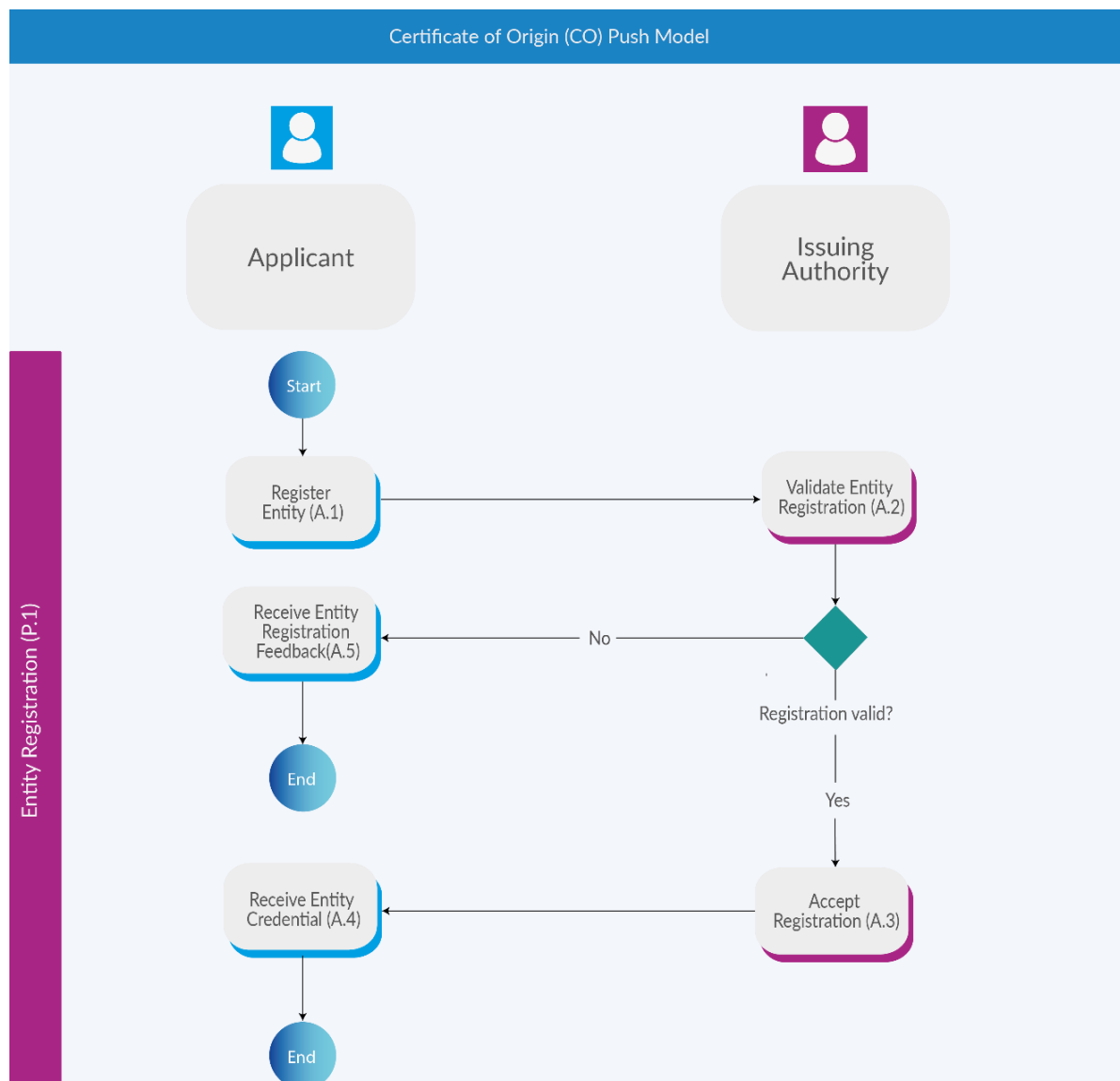
Each Phase/Action is marked with the following status:

Recommended practice (RP): Phase/Action recommended by the Interconnectivity Framework and essential to ensure harmonized implementation of the Framework, aiming at enabling system development and operation to be conducted in an efficient manner.

Good practice (GP): Phase/Action that could be omitted from the implementation of the Interconnectivity Framework without impacting the system, but whose implementation will bring additional benefits for the overall data exchange process.

II. Phases and Actions

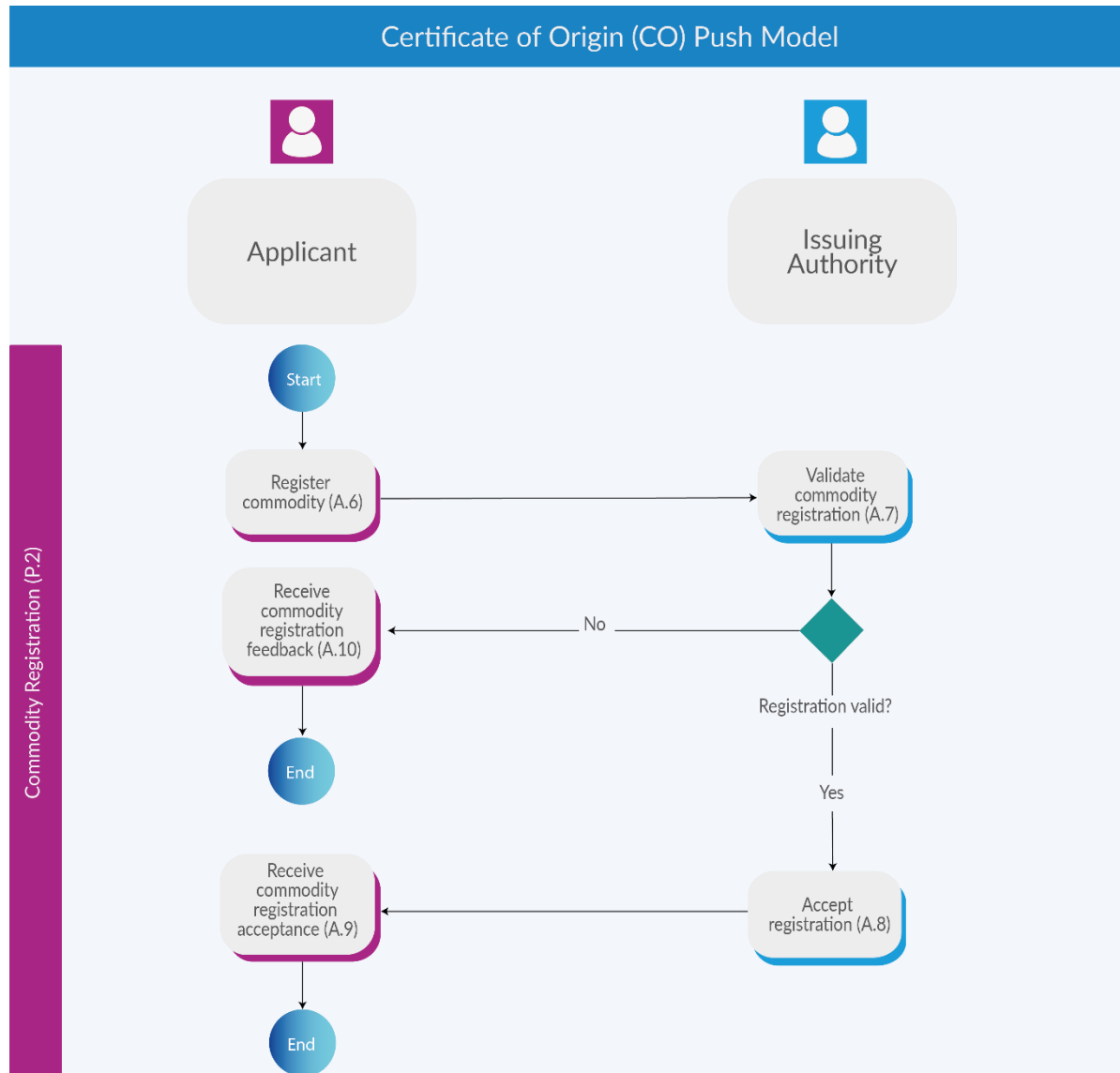
IIA. Entity Registration Phase (P.1/RP)



The applicant is required to register with the issuing authority. The Entity Registration Phase consists of the following actions:

Action Code	Action Name	Status
	Action Description	
A.1	Register Entity	RP
	The applicant (companies or individuals) intending to apply for CO are required to register with the issuing authority.	
A.2	Validate Entity Registration	RP
	The applicant (companies or individuals) intending to apply for CO are required to register with the issuing authority.	
A.3	Accept Registration	RP
	The issuing authority accepts the applicant's registration and creates credentials for the applicant to enable the applicant to access information related to its entities, including CO data that belongs to the applicant.	
A.4	Receive Entity Credential	RP
	The applicant receives the credential given by the issuing authority.	
A.5	Receive Entity Registration Feedback	RP
	The applicant receives feedback from the issuing authority regarding the entity registration.	

II.B Commodity Registration Phase (P.2/GP)

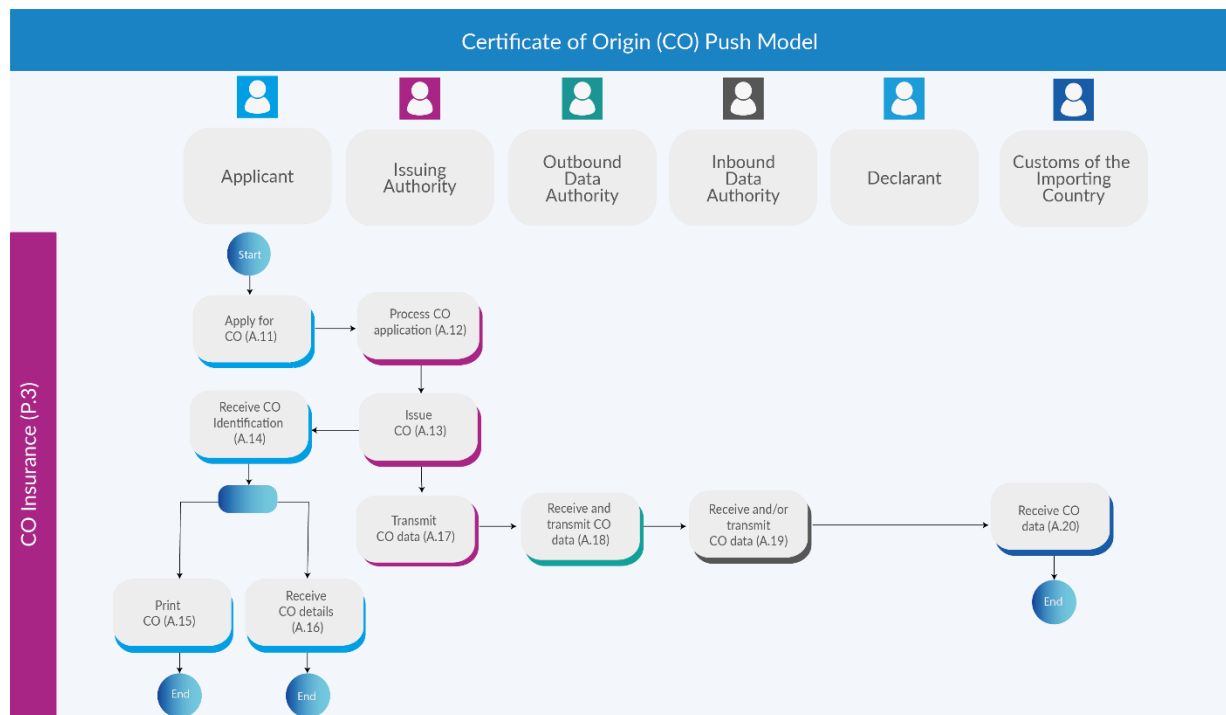


Applicants register the commodity with the issuing authority, when required. When commodity registration is required, applicants can only apply for CO of registered commodities. The Commodity Registration Phase consists of the following actions:

Action Code	Action Name	Status
	Action Description	
A.6	Register Commodity	GP
	The applicant registers the commodity with the issuing authority.	
A.7	Validate Commodity Registration	GP
	The issuing authority validates the applicant's commodity registration.	

A.8	Accept Registration	GP
	The issuing authority accepts the applicant's commodity registration.	
A.9	Receive Commodity Registration Acceptance	GP
	The applicant receives the commodity registration given by the issuing authority.	
A.10	Receive Commodity Registration Feedback	GP
	If the commodity registration is not accepted by the issuing authority, the applicant receives feedback from the issuing authority regarding the commodity registration.	

II.C. CO Issuance Phase (P.3/RP)

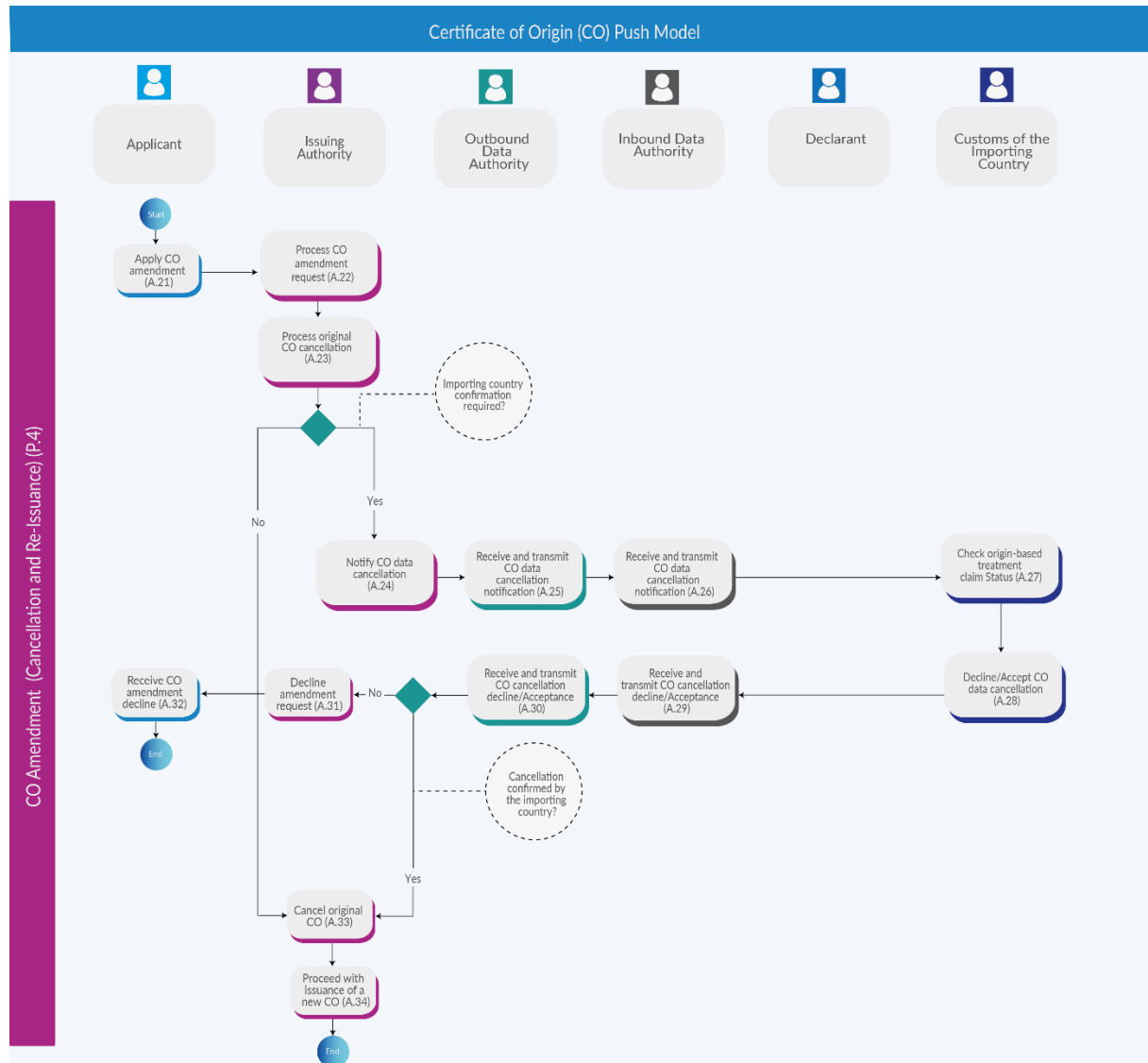


The applicant is required to submit the application for the issuance of the CO to the issuing authority. The CO Issuance Phase consists of the following actions:

Action Code	Action Name	Status
	Action Description	
A.11	Apply for CO	RP
	The applicant applies for the CO to the issuing authority through the CO issuance system or Single Window, by providing other supporting documents/information as required (China, Japan, Korea, Colombia and Mexico).	

A.12	Process CO Application	RP
	The issuing authority examines the application and the supporting documents/information.	
A.13	Issue CO	RP
	The issuing authority issues the CO if all CO application requirements are met.	
A.14	Receive CO Identification	RP
	The applicant receives notification of the issuance of the CO, which includes the CO identification number (China, Japan, Korea, Colombia and Mexico).	
A.15	Print Certificate	RP
	<p>When applicable, the applicant can print the CO themselves. The self-printed CO requires a digital stamp and/or signature to be in place.</p> <p>Three practices related to the validity of the printed CO are observed: the first is that the printed CO is regarded as the validated CO, which can be used as a hard-copy version as an origin document; the second practice is that the printed CO has a watermark indicating it is NOT a validated CO and is for information ONLY; and the third practice is that the printing of CO is not available once the data is transmitted.</p>	
A.16	Retrieve CO Details	RP
	The applicant is able to retrieve the details of the CO, identified by the available CO identification number.	
A.17	Transmit CO Data	RP
	The issuing authority transmits the CO data to the outbound data authority, e.g. Single Window.	
A.18	Receive and Transmit CO Data	RP
	The outbound data authority receives the CO data from the issuing authority and transmits the CO data to the inbound data authority of the importing country.	
A.19	Receive and Transmit CO Data	RP
	The inbound data authority receives the CO data from the outbound data authority of the exporting country and transmits the CO data to Customs of the importing country.	
A.20	Receive CO Data	RP
	The Customs of the importing country receives the CO data from the inbound gateway.	

II.D. CO Amendment Phase (Cancellation and Re-Issuance) (P.4/GP)



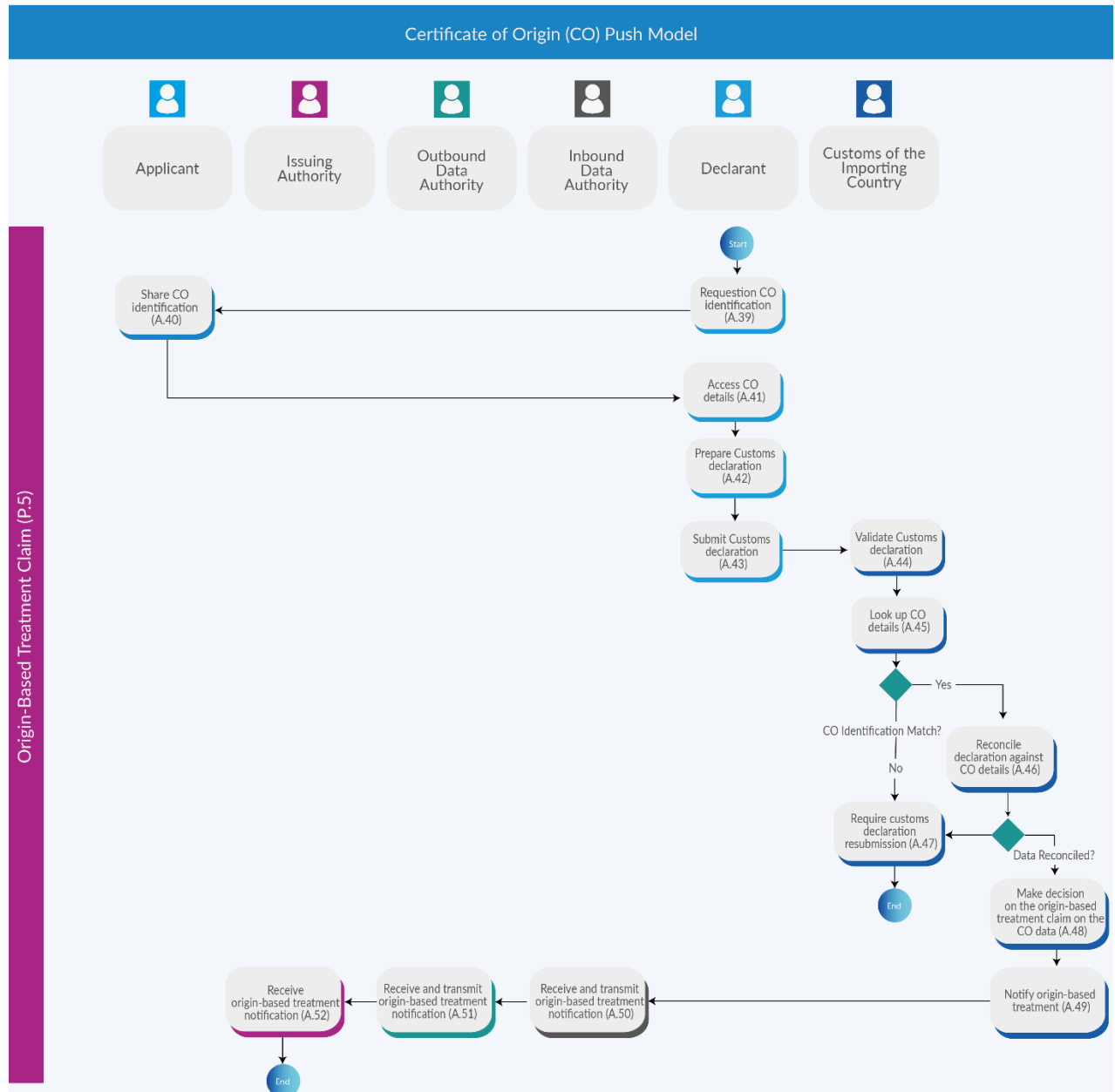
The applicant is allowed to submit the application for amendment of the CO to the issuing authority. The CO Amendment Phase consists of two steps, namely, cancellation of the previous CO and re-issue of the amended CO, which consists of the following actions:

Action Code	Action Name	Status
	Action Description	
A.21	Apply CO Amendment	RP
	The applicant applies for the CO amendment to the issuing authority through the declaration system or Single Window, with other supporting documents as required.	

A.22	Process CO Amendment Request The issuing authority examines the application for amendment and the supporting documents. If all relevant requirements are fulfilled, the CO can be amended, if not, the issuing authority will reject the amendment of the CO and return the application to the applicant.	RP
A.23	Process Original CO Cancellation The issuing authority makes a cancellation of the original CO.	RP
A.24	Notify CO Data Cancellation The issuing authority notifies Customs of the importing country of the CO data amendment through outbound and inbound data authorities.	RP
A.25	Receive and Transmit CO Data Cancellation Notification The outbound data authority receives the CO data cancellation notification from the issuing authority and transmits the CO data cancellation notification to the inbound data authority of importing countries.	RP
A.26	Receive and Transmit CO Data Cancellation Notification The inbound data authority receives the CO data cancellation notification from the outbound data authority and transmits the CO data cancellation notification to Customs of the importing country.	RP
A.27	Check Origin-based Treatment Claim Status The Customs of the importing country checks if a decision on the origin-based treatment for the original CO has been made.	GP
A.28	Decline/Accept CO Data Cancellation The Customs of the importing country makes a decision to decline or accept the CO data cancellation based on the origin-based treatment claim status and responds to the notification provided by the issuing authority through inbound and outbound data authorities.	GP
A.29	Receive and Transmit CO Cancellation Decline/Acceptance The inbound data authority receives the decision of the Customs of the importing country on the decline or acceptance of the CO amendment and subsequently transmits the decision to the outbound data authority.	GP
A.30	Receive and Transmit CO Cancellation Decline/Acceptance The outbound data authority receives the decision on the decline or acceptance of the CO amendment and subsequently transmits the decision to the issuing authority.	GP
A.31	Decline Amendment Request The issuing authority declines the application for the CO amendment based on the decision of the Customs of the importing country transmitted by the inbound and outbound data authorities.	GP
A.32	Receive CO Amendment Decline The applicant receives a CO amendment decline notification from the issuing authority.	GP
A.33	Cancel Original CO	

	The applicant receives a CO amendment decline notification from the issuing authority.	GP
A.34	Proceed with Issuance of a New CO	RP
	The issuing authority proceeds with issuing a new CO.	

II.E. Origin-Based Treatment Claim Phase (P.5/RP)



The declarant claims for the origin treatment for the shipment as part of the Customs clearance of the importing country. The Origin Treatment Claim Phase consists of the following actions:

Action Code	Action Name	Status
	Action Description	
A.39	Request CO Identification Number	RP
	The declarant requests the CO identification number(s) relevant for the shipment from the applicant.	
A.40	Share CO Identification Number	RP
	The issuing authority examines the application for amendment and the supporting documents. If all relevant requirements are fulfilled, the CO can be amended, if not, the issuing authority will reject the amendment of the CO and return the application to the applicant.	
A.41	Access CO Details	RP
	<p>The declarant accesses the CO details with the CO identification number.</p> <p>Different practices related to accessing CO details are observed. The platform to access the CO details varies from country to country, e.g. National Single Window, Customs Systems.</p> <p>The identification method to get access to the CO details is either to use the CO identification number as the primary key, or a combination of the CO identification number and invoice number/company number/tax identification as the primary keys for looking up the correct CO data.</p>	
A.42	Prepare Customs Declaration	RP
	The declarant prepares the Customs declaration and includes the CO identification number in the Customs declaration.	
A.43	Submit Customs Declaration	RP
	The declarant submits the Customs declaration to the Customs of the importing country.	
A.44	Validate Customs Declaration	RP
	The Customs of the importing country validates the Customs declaration.	
A.45	Look Up CO Details	RP
	The Customs of the importing country looks up the CO details based on the CO identification number included in the Customs declaration.	
A.46	Reconcile Declaration against CO Details	RP
	The Customs of the importing country examines the CO Details against the Customs declaration.	
A.47	Require Customs Declaration Resubmission	RP
	The Customs of the importing country requires the declarant to resubmit the Customs declaration.	
A.48	Make Decision on the Origin-Based Treatment Based on the CO Data	RP
	The Customs of the importing country, based on the CO data, makes a decision on the origin-based treatment.	

A.49	Notify Origin-Based Treatment	GP
	The Customs of the importing country send notification to the outbound data authority on the origin-based treatment	
A.50	Receive and transmit origin-based treatment notification	GP
	The inbound data authority of the exporting country receives origin-based treatment notification and afterward transmit the notification to outbound data authority.	
A.51	Receive and transmit origin-based treatment notification	GP
	The outbound data authority of the importing country receives origin-based treatment notification and afterward transmit the notification to Issuing authority.	
A.52	Receive origin-based treatment notification	GP
	The issuing authority of the exporting country receive the origin-based treatment notification	

ANNEX II: Data Elements to be Exchanged

Information package: <https://datamodel.wcoomd.org/#/infopack/scope/national/bceed8417e>

Dataset: <https://datamodel.wcoomd.org/#/mydataset/code/mapping/e448a5c010>

WCO ID	Name	Definition	IWG USE	NEW	Path
D011	Document issuing date/time	Date and time the document was issued and, when appropriate, signed or otherwise authenticated.	X		LPCO/D011
D013	Document name code	Code specifying the name of a document.	X		LPCO/D013
61B	Authentication	Details related to the authentication of a document.	X		LPCO/Authentication
104	Authentication statement	Statement providing proof that the document has been authenticated.	X		LPCO/Authentication/104
539	Document authentication location name	Name of a location where a document was signed or otherwise authenticated.	X		LPCO/Authentication/539
12A	Authenticator	Details related to an authenticating party.	X		LPCO/Authentication/Authenticator
R007	Authenticator name	Name of the party which certifies that a document is authentic.	X		LPCO/Authentication/Authenticator/R007
03A	Additional Information	Details related to the special request from declarant to government to take or not to take action.	X		LPCO/AdditionalInformation
369	Additional statement type code	Code specifying the subject of the additional statement.	X		LPCO/AdditionalInformation/369
28A	Consignment	Details related to the transport between a consignor and a consignee as specified in the transport contract document.	X		
15A	Border Transport Means	Details related to the means of transport crossing the border of the Customs territory.	X		

T005	Crossing the border transport means name	Name to identify the means of transport used for the carriage of the goods in crossing the border.	X		LPCO/Consignment/BorderTransport Means/T005
T006	Transport means crossing the border identifier	Identification of the means of transport used in crossing the border.	X		LPCO/Consignment /BorderTransportMeans/T006
T010	Type of means of transport crossing the border code	Code specifying type of means of transport used for the carriage of the goods in crossing the border.	X		LPCO/Consignment /BorderTransportMeans/T010
149	Conveyance identifier	Identification of the journey of a means of transport, for example, voyage number, flight number, trip number.	X		LPCO/Consignment /BorderTransportMeans/149
27A	Consignee	Details related to the party to which goods are consigned.	X		
R014	Consignee name	Name of the party to which goods are consigned.	X		LPCO/Consignment /Consignee/R014
R015	Consignee identifier	Identification of a party to which goods are consigned.	X		LPCO/Consignment /Consignee/R015
R005	Role code	Code specifying the role of a party.	X		LPCO/Consignment /Consignee/R005
04A	Address	Details related to an address.	X		
410	Address type code	Code specifying the type of address.	X		LPCO/Consignment /Consignee/Addresses/410
241	City name	Name of a city.	X		LPCO/Consignment /Consignee/Addresses/241
242	Country code	Code specifying the name of the country or other geographical entity as specified in ISO 3166 and UN/ECE Rec 3.	X		LPCO/Consignment /Consignee/Addresses/242
412	Country name	Name of the country or other geographical entity.	X		LPCO/Consignment /Consignee/Addresses/412
244	Country sub-entity identification code	Code specifying the name of a country subdivision.	X		LPCO/Consignment /Consignee/Addresses/244
243	Country sub-entity name	Name of a country subdivision.	X		LPCO/Consignment /Consignee/Addresses/243
239	Street and number/P.O. Box	Specification of the postal delivery point such as street and number or post office box.	X		LPCO/Consignment /Consignee/Addresses/239

245	Postcode identifier	Identification of the postal zone or address.	X		LPCO/Consignment /Consignee/Addresses/245
29A	Consignment Item	Details related to an item in a consignment.	X		
006	Sequence number	Number indicating the position in a sequence.	X		LPCO/Consignment /ConsignmentItem/006
03A	Additional Information	Details related to the special request from declarant to government to take or not to take action.	X		
23A	Commodity	Details related to the properties of the goods.	X		LPCO/Consignment /ConsignmentItem/Commodity
137	Goods description	Description of the nature of a goods item sufficient to identify it for cross-border regulatory purposes such as Customs, phytosanitary, statistical or transport.	X		LPCO/Consignment /ConsignmentItem/Commodity/137
65A	Goods Measure	Details related to goods weight, quantities, and amounts.	X		LPCO/Consignment /ConsignmentItem/GoodsMeasure
131	Gross weight	Weight of goods including packing but excluding carrier's equipment.	X		LPCO/Consignment /ConsignmentItem/GoodsMeasure/131
128	Net weight	Weight of the goods themselves without any packing.	X		LPCO/Consignment /ConsignmentItem/GoodsMeasure/128
92A	Origin	Details related to the origin of the goods.	X		LPCO/Consignment /ConsignmentItem/Origin
063	Country of origin code	Code specifying the country in which the goods have been produced or manufactured, according to criteria laid down for the application of the Customs tariff or quantitative restrictions, or any measure related to trade.	X		LPCO/Consignment /ConsignmentItem/Origin/063
93A	Packaging	Details related to packaging.	X		LPCO/Consignment /ConsignmentItem/Packaging
142	Shipping marks	Marks and/or numbers on a transport unit or package.	X		LPCO/Consignment /ConsignmentItem/Packaging/142

144	Number of packages	Quantity specifying the number of individual items packaged in such a way that they cannot be divided without first undoing the packing.	X		LPCO/Consignment /ConsignmentItem/ Packaging/144
141	Type of packages identification code	Code specifying the type of package of an item.	X		LPCO/Consignment /ConsignmentItem/ Packaging/141
30A	Consignor	Details related to the party which, by contract with a carrier, consigns or sends goods with the carrier, or has them conveyed by him.	X		
R020	Consignor name	Name of the party consigning goods as stipulated in the transport contract by the party ordering transport.	X		LPCO/Consignment /Consignor/R020
R021	Consignor identifier	Identification of the party consigning goods as stipulated in the transport contract by the party ordering the transport.	X		LPCO/Consignment /Consignor/R021
R005	Role code	Code specifying the role of a party.	X		LPCO/Consignment /Consignor/R005
04A	Address	Details related to an address.	X		
410	Address type code	Code specifying the type of address.	X		LPCO/Consignment /Consignor/Addresses/410
241	City name	Name of a city.	X		LPCO/Consignment /Consignor/Addresses/241
242	Country code	Code specifying the name of the country or other geographical entity as specified in ISO 3166 and UN/ECE Rec 3.	X		LPCO/Consignment /Consignor/Addresses/242
412	Country name	Name of the country or other geographical entity.	X		LPCO/Consignment /Consignor/Addresses/412
244	Country sub-entity identification code	Code specifying the name of a country subdivision.	X		LPCO/Consignment /Consignor/Addresses/244
243	Country sub-entity name	Name of a country subdivision.	X		LPCO/Consignment /Consignor/Addresses/243
239	Street and number/P.O. Box	Specification of the postal delivery point such as street and number or post office box.	X		LPCO/Consignment /Consignor/Addresses/239

245	Postcode identifier	Identification of the postal zone or address.	X		LPCO/Consignment /Consignor/Addresses/245
83A	Loading Location	Details related to the location at which the goods (i.e. consignments) are loaded onto the active means of transport.	X		
L009	Loading location name	Name of a seaport, airport, freight terminal, rail station or other location at which goods are loaded onto the means of transport being used for their carriage.	X		LPCO/Consignment /LoadingLocation/L009
L010	Loading location identifier	Identification of a seaport, airport, freight terminal, rail station or other location at which goods are loaded onto the means of transport being used for their carriage.	X		LPCO/Consignment /LoadingLocation/L010
31B	Transport Equipment	Details related to transport equipment used for the consignment.	X		
152	Equipment size and type code	Code specifying the characteristics (e.g. size and type of a piece of transport equipment).	X		LPCO/Consignment /TransportEquipment/152
44B	Seal	Details related to the seal affixed to a piece of transport equipment, used to secure an object and protect from unauthorized entry or tampering.	X		
006	Sequence number	Number indicating the position in a sequence.	X		
165	Seal identifier	Identification of a seal affixed to a piece of transport equipment by number.	X		LPCO/Consignment /TransportEquipment/Seal/165
38B	Unloading Location	Details related to the location at which the goods (i.e. consignment) are unloaded from the active means of transport having been used for their carriage.	X		
L012	Unloading location name	Name of the unloading location, seaport, airport, freight terminal, rail station or other location at which the cargo is to be unloaded from the means of transport having been used for their carriage.	X		LPCO/Consignment /UnloadingLocation /L012

L013	Unloading location identifier	Identification of a seaport, airport, freight terminal, rail station or other location at which goods are unloaded from the means of transport having been used for their carriage.	X		LPCO/Consignment/UnloadingLocation/L013
451	Actual Authentication Date	Actual date and optional time when this authentication was signed or otherwise authenticated.	X	X	LPCO/Authentication/451
L098	Actual Authentication Location, coded	Identifier of a location where a document was signed or otherwise authenticated.	X	X	LPCO/Authentication/544
D017	Place of authentication of document	Name of a location where a document was signed or otherwise authenticated.	X	X	LPCO/Authentication/539
R005	Role code	Code giving specific meaning to a party.	X	X	
105	Free text	Free text field available to the message sender for information.	X	X	
21A	Classification	Details about the non-commercial categorization of a commodity by a standard-setting organization.	X	X	
145	Commodity Classification	The non-commercial categorization of a commodity by a standard-setting organization.	X	X	LPCO/Consignment/ConsignmentItem/Commodity/Classification/145
337	Commodity Classification Type	A qualifier to describe the commodity classification, e.g. Harmonized Tariff Schedule (HTS), Export Control Classification Code (ECCC), UNDG Code list, International Code of Zoological Nomenclature (ICZN).	X	X	LPCO/Consignment/ConsignmentItem/Commodity/Classification/337
130	Tariff quantity/Supplementary quantity	Quantity of the goods in the unit as required by Customs for tariff, statistical or fiscal purposes or as indicated in Type.	X	X	LPCO/Consignment/ConsignmentItem/GoodsMeasure/130
78A	Invoice	Information of a commercial invoice.	X	X	
D016	Invoice number	Reference number to identify an invoice.	X	X	LPCO/Consignment/ConsignmentItem/Invoice/D016
D015	Invoice date	Date of issue of an invoice.	X	X	LPCO/Consignment/ConsignmentItem/Invoice/D015

436	Rule of origin, coded	Code specifying the criterion of determination as to whether a good qualifies as an originating good in accordance with the rules.	X	X	LPCO/Consignment /ConsignmentItem/ Origin/436
306	Value of goods	FOB value - Monetary amount that has to be or has been paid as calculated under the applicable trade delivery.	X	X	LPCO/Consignment /ConsignmentItem/ Commodity/306
K9	Third country invoice country	The country of the company issuing the invoice in cases where the invoice is issued by a third country.	X	X	
K10	Third country invoice company	The name of the company issuing the invoice in cases where the invoice is issued by a third country.	X	X	
K11	Third country invoice address	The address of the company issuing the invoice in cases where the invoice is issued by a third country.	X	X	
K12	Exhibition name	The name of the exhibition in cases where goods are sent from the territory of the exporting Party for exhibition in another country and sold during or after the exhibition for importation into the territory of a Party.	X	X	
K13	Exhibition address	The address of the exhibition in cases where goods are sent from the territory of the exporting Party for exhibition in another country and sold during or after the exhibition for importation into the territory of a Party.	X	X	
K14	Issued retroactively	Yes in the case that CO is issued retroactively.	X	X	
K15	Back-to-back CO	Yes in the case of back-to-back CO.	X	X	
K16	Document type code	To indicate under which trade agreement (or any other preferential/non-preferential trade scheme) the CO is issued.	X	X	
K17	Operation mode	Operation mode code to command whether to issue or delete CO message.	X	X	
D014	Document reference number	Reference number identifying a specific document.	X	X	LPCO/D014

D031	Document category, coded	Code specifying the category of a document.	X	X	
D012	Document issuing place, coded	Place at which a document was issued and, when appropriate, signed or otherwise authenticated.	X	X	LPCO/D012
D034	Document issuing place	Place at which a document was issued and, when appropriate, signed or otherwise authenticated.	X	X	LPCO/D034
019	Document/message status, coded	Code specifying the status of a document.	X	X	
501	Origin type, coded	Code to differentiate between different types of origin, e.g. preferential and non-preferential Country of Origin codes.	X	X	
413	Country of origin name	The name of the country in which the goods have been produced or manufactured, according to criteria laid down for the application of the Customs tariff or quantitative restrictions, or any measure related to trade.	X	X	LPCO/Consignment/ConsignmentItem/Origin/413
066	Region of origin, coded	Region in which the goods have been produced or manufactured, according to criteria laid down for the purposes of application of the Customs tariff, or quantitative restrictions, or of any other measure related to trade.	X	X	LPCO/Consignment/ConsignmentItem/Origin/066
436	Rule of origin, coded	Code specifying the criterion of determination as to whether a good qualifies as an originating good in accordance with the rules.	X	X	
01B	Producer	Details related to the producer of the product.	X	X	
R034	Producer name	Name of the party or person who has produced the product.	X	X	LPCO/Consignment/ConsignmentItem/Commodity/Producer/R034
04A	Address	Details related to an address.	X	X	
324	Tariff quantity amount	Amount reported in 1 st , 2 nd or 3 rd tariff quantity.	X	X	
156	Departure date/time	Date and time of departure of the means of transport.	X	X	

ANNEX III: Semi-Automated Pull Model for Certificate of Origin

I. Introduction

In addition to CO Interconnectivity through the Push Model, Korea Customs Service (KCS) has implemented a Semi-Automated Pull Model with the Customs authority of one of its FTA partner countries.

CO Interconnectivity through the Semi-Automated Pull Model is characterized by an electronic verification system, an official website/platform operated by the issuing authorities for the authentication of the CO, and an agreement between the exporting and importing Customs authorities to replace the original paper-based CO with the electronic copies when importers claim preferential tariff treatment.

In this Model, the Customs authority in the importing country, in accordance with the agreement with the exporting Customs authority, verifies the CO in the electronic verification system using the electronic copy of the CO, instead of receiving the paper CO submitted by the importer.

For the purposes of claiming preferential tariff treatment, an exporter does not need to send an original paper CO to the importer. Instead, he sends an electronic copy of the CO to the importer, who uses the information received to make a claim to the Customs authority for preferential tariff treatment.

In terms of application, the Push Model of CO Interconnectivity is a much more efficient option as it allows the automatic and simultaneous exchange of CO data between exporting and importing countries. However, considerable resources and expertise are required to set up a secure communication platform for the cross-border exchange of sensitive data. In addition, the participating authorities need to address legal issues, data protection issues and the risk of system failure.

In this sense, the Semi-Automated Pull Model can offer a more practical and affordable solution, especially if an electronic verification system is already in place. However, making a query in respect of each CO can be time-consuming, and for this reason the Semi-Automated Pull Model is recommended for countries with moderate to low trade volumes.

In the initial negotiation phase, KCS and the partner Customs authority agreed to establish CO interconnectivity through the Push Model. However, at a later stage both authorities decided that it would be preferable to switch to a Semi-Automated Pull Model, taking into account the frequency of CO issuance and the volume of trade between the two countries.

Korean issuing authorities operate their own electronic verification systems, where users can make queries on COs by entering a unique CO Reference Number and a Reference Code – see KCS (<https://customs.go.kr/co.html>) and Korea Chamber of Commerce and Industry (KCCI) (<http://cert.korcham.net/search/index.htm>). In particular, the KCS system allows users to verify COs issued by KCCI, as KCS supervises the issuance of preferential COs.

II. Entities

The Stakeholders involved in the Semi-Automated Pull Model are described in the following table.

Entity	Definition	Korean Practice
Applicant	The entity that applies for a CO	Producer, exporter or its authorized representative
Issuing Authority	The authority in the exporting country which is responsible for issuing the CO and operating the electronic verification system for the authentication of CO	Korea Customs Service (KCS), Korea Chamber of Commerce and Industry (KCCI)
CO Verification Portal Authority	The authority in the exporting country responsible for the management/operation of online CO verification systems. This authority may be the same as or different from the issuing authority. The Single Window authority is well placed to take on this role.	Korea Customs Service (KCS), Korea Chamber of Commerce and Industry (KCCI) * The electronic verification system of the KCS is able to verify CO issued by both the KCS and the KCCI
Customs of importing country	The Government Service which is responsible for the administration of the Customs law and the collection of duties and taxes, and which also has responsibility for the application of other laws and regulations relating to the importation, exportation, movement and storage of goods	
Declarant	The entity that makes a declaration to Customs or - where legally permitted - in whose name, or on whose behalf, a declaration is made to Customs	Owner of goods, licensed Customs broker

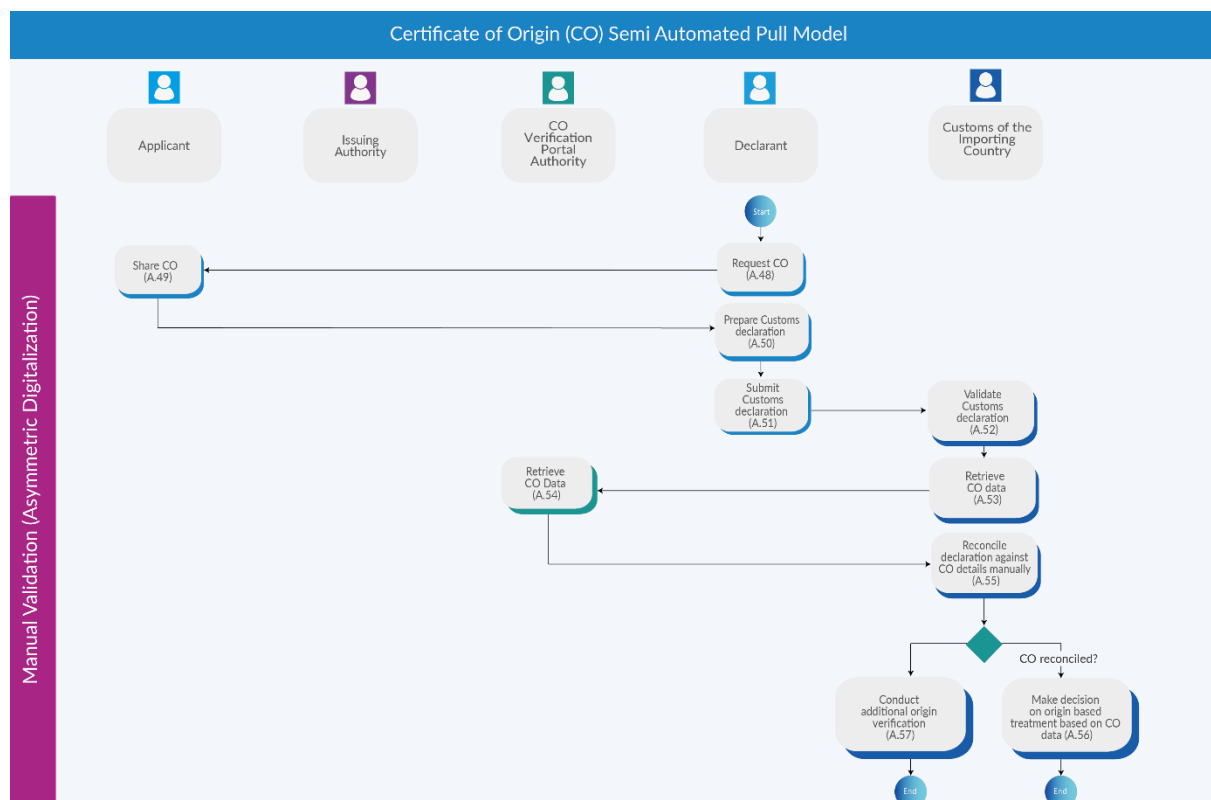
III. Business Process for CO Issuance/Amendment

Diagrams showing the phases from Entity Registration (Phase 1) to CO Amendment (Phase 4) have been omitted, as they are identical or similar to those of the Push Model.

Entity Registration (Phase 1) and Commodity Registration (Phase 2) are the same as in the Push Model.

With regard to CO Issuance (Phase 3) and CO Amendment (Phase 4), the action flow ends when the CO or amended CO is issued and the data is transmitted to the Outbound Gateway, enabling a query to the electronic verification system. In the Semi-Automated Pull Model, the Inbound Gateway and Customs in the importing country do not receive the data – this is the main difference between this Model and the Push Model.

The Origin Treatment Claim (Phase 5) in the Semi-Automated Pull Model consists of several phases, which are shown in the UML Activity Diagram set out below.



IV. Origin Treatment Claim

The Origin Treatment Claim phase (Phase 5) covers the process by which the declarant clears the shipment and claims preferential tariff treatment for it through Customs in the importing country. This phase consists of the following actions:

Action Code	Action Name
	Action Description
A.48	Request CO The declarant requests the CO details or softcopy from the applicant, in order to claim preferential tariff treatment for the shipment.
A.49	Share CO The applicant shares the CO of the shipment with the declarant.
A.50	Prepare Customs Declaration The declarant prepares the Customs declaration using the CO received from the applicant, and other supporting documents.
A.51	Submit Customs Declaration The declarant submits the Customs declaration to Customs in the importing country.
A.52	Validate Customs Declaration

	Customs in the importing country validates the Customs declaration.
A.53	<p>Retrieve CO Data</p> <p>Customs in the importing country retrieves the CO details from the Customs declaration and makes a query to the Outbound Gateway regarding the authenticity of the CO.</p>
A.54	<p>Display CO Data</p> <p>The Outbound Gateway displays the CO data.</p>
A.55	<p>Reconcile Declaration against CO Details Manually</p> <p>Customs in the importing country verifies the authenticity by manually examining the Customs declaration against the CO details.</p>
A.56	<p>Make decision on the Origin-based Treatment based on the CO data</p> <p>If the CO is valid, Customs in the importing country makes a decision regarding preferential tariff treatment.</p>
A.57	<p>Conduct Additional Origin Verification</p> <p>If the CO is not valid, Customs in the importing country conducts additional origin verification.</p>

ANNEX IV: Push Model for Self-Declaration of Origin

I. Introduction

In addition to CO Interconnectivity through the Push Model, China Customs has implemented a Push Model for self-declaration of origin with the Customs authorities of its FTA partners.

Since 2022, China Customs has implemented a unified Approved Exporters Scheme across all the eligible FTAs. The management of the Approved Exporters Scheme is operated via an IT system, which is one of the modules of China Customs' Rules of Origin Management Platform. The main functions of the system consist of:

- a. The application and approval of the approved exporter,
- b. The issuance of Declarations of Origin (DO),
- c. The management of DO data and approved exporters list.

To apply for approved exporter status, an enterprise must submit the required information on its operations and commodities to the IT system, for Customs to review. Once it has been granted approved exporter status, the enterprise will be able to issue DOs in the system.

The approved exporter can issue two kinds of DO via the IT system.

A. Formatted DO (e.g. DO of RCEP).

The system provides a user-friendly interface for approved exporter to submit the information of the DO with the autofill function for the information that already stored in the system. After the submission, the system will generate the DO in compliance with the requirements of different FTA with a unique serial number.

B. DO based on commercial documents (e.g. DO of China-Switzerland FTA).

The approved exporter uploads the scan copy of its commercial documents, and based on the information provided by approved exporter, the system will generate the DO in PDF format with a unique serial number, attaching the standardized statement of origin and the commercial documents.

This IT system provides a convenient and error-free way for the approved exporters to issue their DO, while enables China Customs to monitor the statistic of DO, as well as gathers all the necessary data for carrying out DO data exchange with its FTA partners. Currently, China Customs is exchanging DO with Switzerland and New Zealand and sharing the approved exporter list with multiple trading partners. As China Customs is technically ready to carry out DO data exchange, it is actively working with its trading partners to explore the possibility of establishing such cooperation.

The following diagrams and tables explain the business model of China Customs' DO data exchange.

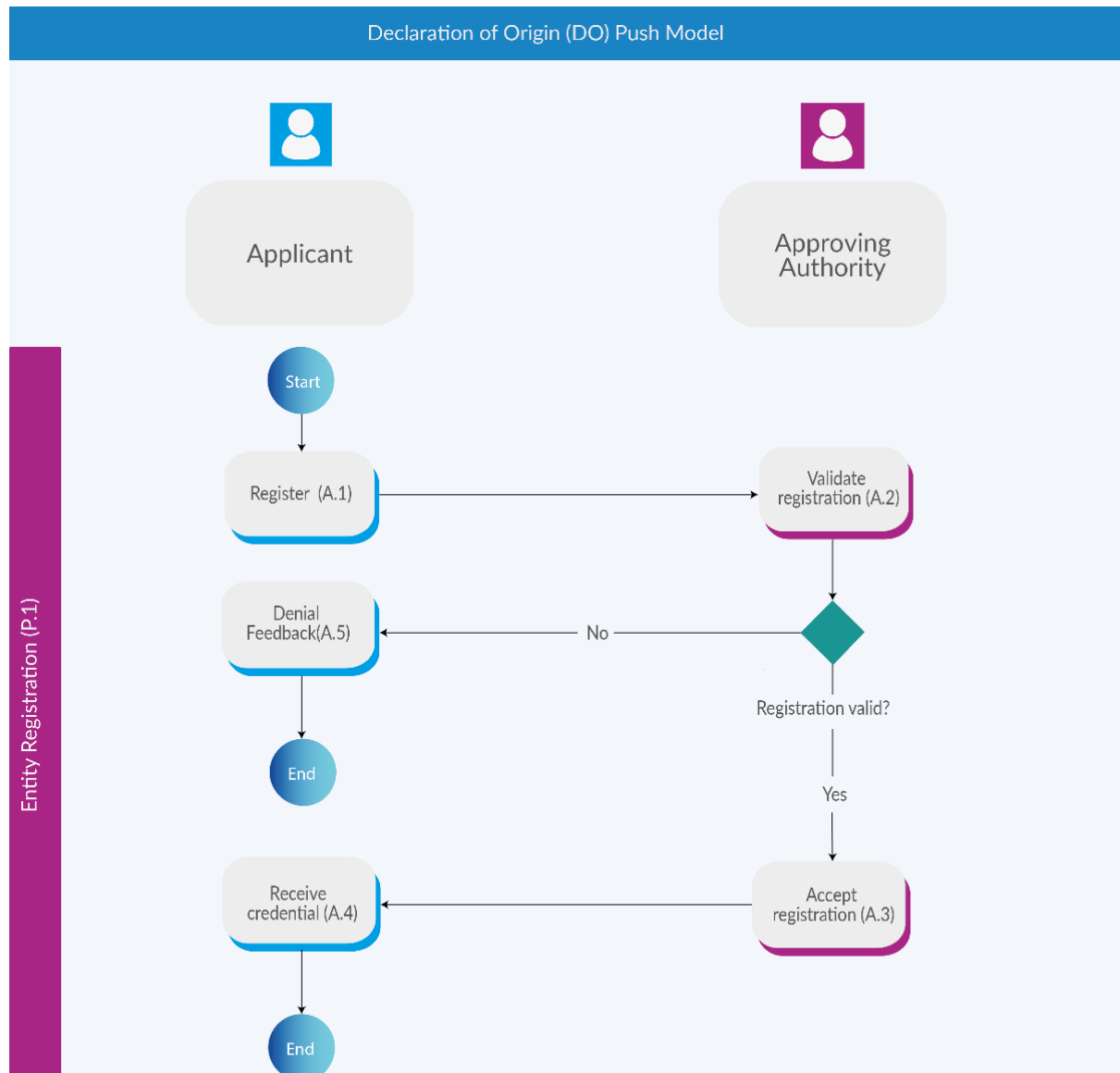
II. Entities

The Stakeholders involved in the DO Push Model are described in the following table.

Entity	Definition	National Practices
Applicant	Entity applying for approved exporter authorization and eligibility to complete DOs	Exporter
Approving authority	Authority of the exporting party responsible for authorizing approved exporters and allowing them to complete DOs	China Customs
Outbound data authority	Authority of the exporting party responsible for transmitting data of DOs to the importing party	China International Trade Single Window, China Customs
Inbound data authority	Authority of the importing party responsible for receiving data of DOs from the exporting party	Single Window, Customs of the importing party
Declarant of the importing party	The entity that makes a declaration to Customs or - where legally permitted - in whose name, or on whose behalf, a declaration is made to Customs	Importer/ licensed customs broker/ Consignee / Forwarder
Declarant of the exporting party	The entity that received the authorization of approved exporter and being eligible to complete DOs.	Approved exporter

III. Phases and Actions

III.A Registration Phase (P.1)

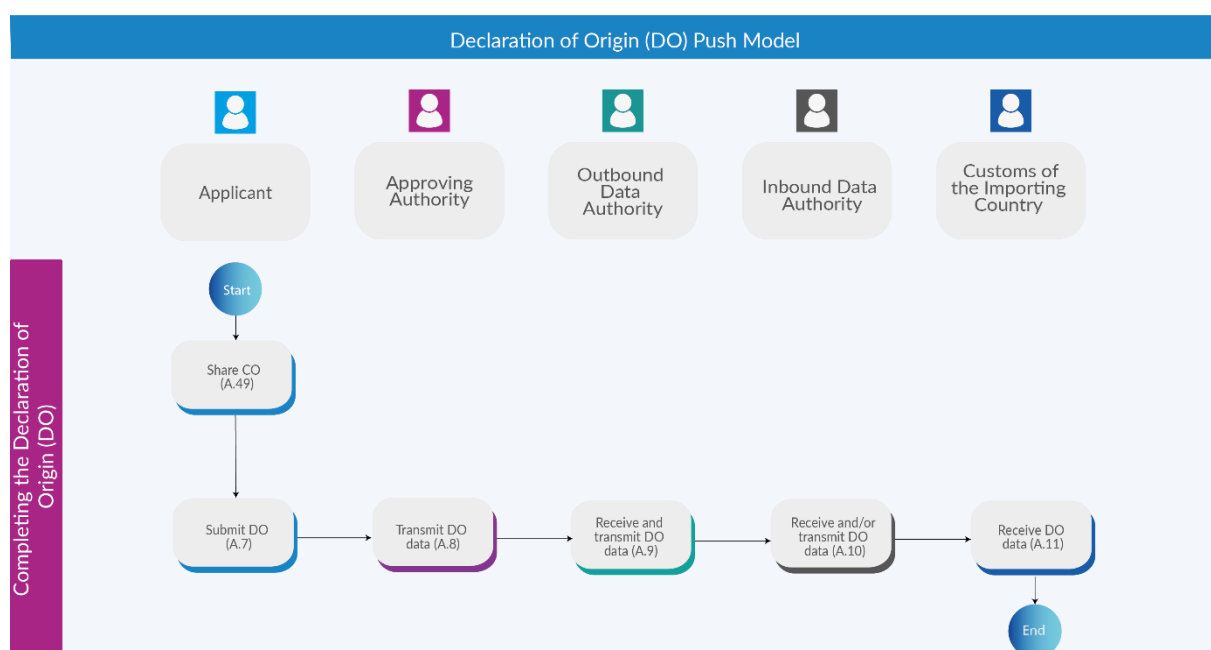


Before they can complete Declarations of Origin, applicants must apply to Customs for authorization as approved exporters. The Registration phase consists of the following actions :

Action Code	Action Name
	Action Description
A.1	Register
	Exporter applies for the authorization of approved exporter at Customs.
A.2	Validate Registration
	Customs receives and reviews application for authorization.
A.3	Accept Registration
	Customs authorizes applicant who meets the requirements for approved exporter status.

A.4	Receive Credential
	Applicant receives feedback from Customs on the application and will be granted an authorization code.
A.5	Denial Feedback
	Where the application that does not meet the requirement will receive the denial feedback from Customs..

III.B. “Completing the Declaration of Origin” Phase (P.2)

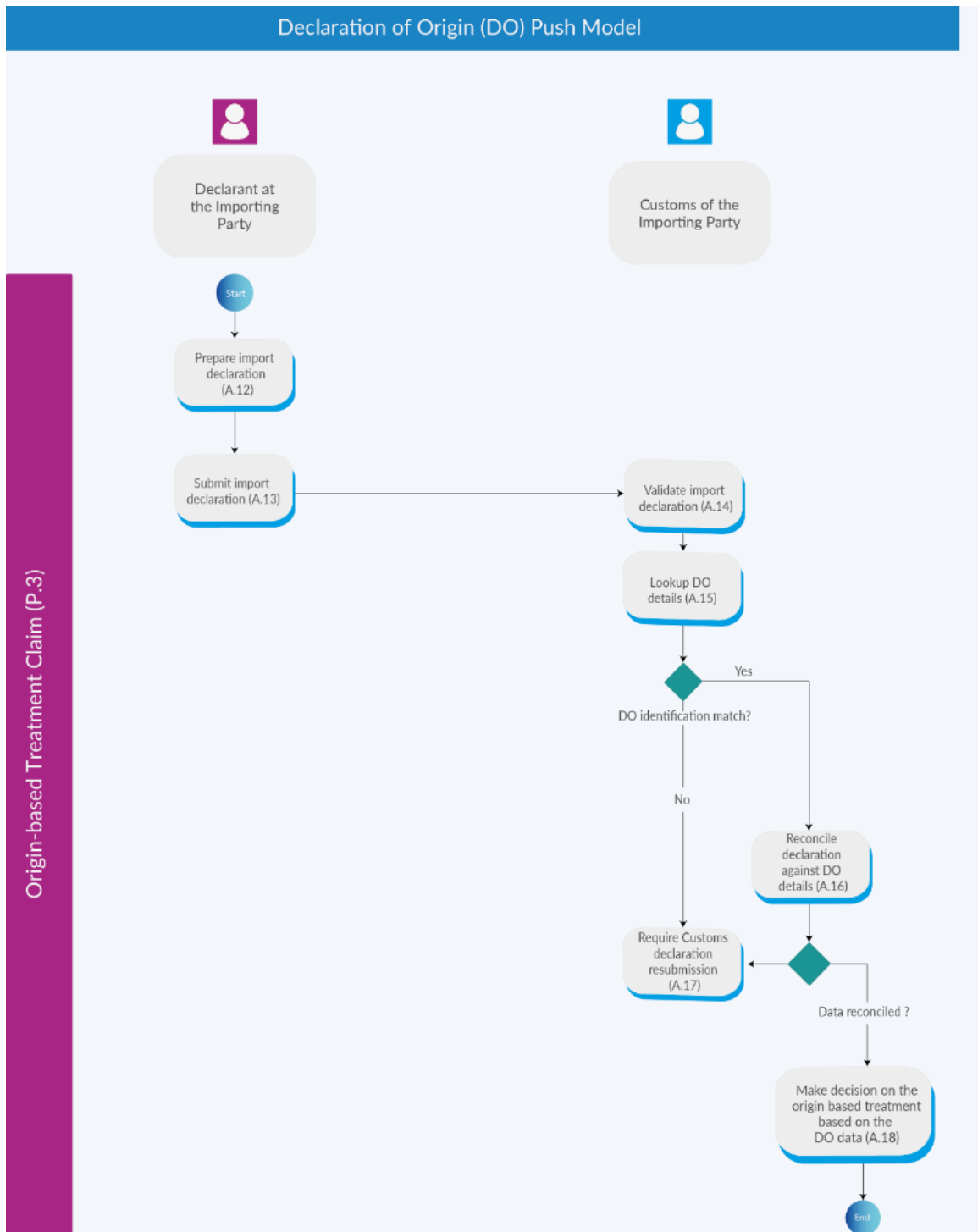


The approved exporter completes DOs for its commodity via IT system. The “Completing the Declaration of Origin” phase consists of the following actions:

Action Code	Action Name
	Action Description
A.6	Prepare DO
	Applicant prepares the necessary information for completing the DO.
A.7	Submit DO
	Applicant completes and submits the DO via the Single Window, and supplies Customs with the DO data.
A.8	Transmit DO Data
	Customs receives the DO data from the applicant and transmits the data to the Outbound data authority.
A.9	Receive and Transmit DO Data
	The Outbound data authority receives the DO data from Customs and transmits the data to the Inbound data authority of the importing party.

A.10	Receive and/or Transmit DO Data The Inbound data authority of the importing party receives the DO data and transmits the data to Customs in the importing party.
A.11	Receive DO Data Customs in the importing party receives the DO data.

III.C. Origin-based Treatment Claim (P.3)



The declarant claims Origin treatment for the shipment as part of Customs clearance in the importing party. The Origin Treatment Claim phase consists of the following actions:

Action Code	Action Name
	Action Description
A.12	Prepare Import Declaration
	The declarant prepares the Customs declaration and includes the DO identification number in the Customs declaration. The declarant requests from the applicant the relevant DO identification number(s) for the shipment.
A.13	Submit Import Declaration
	The declarant of the imported goods submits the Customs declaration to Customs of the importing party.
A.14	Validate Import Declaration
	Customs of the importing party validates the import declaration.
A.15	Look up DO details
	Customs of the importing party looks up the DO details with reference to the DO identification number included in the Customs declaration.
A.16	Reconcile Declaration against DO details
	Customs of the importing party checks the DO details against the Customs declaration.
A.17	Require Customs Declaration Resubmission
	In cases where the DO data does not match the information about the goods which is contained in the import declaration, or the DO data cannot be found, Customs of the importing party will conduct further verifications regarding the origin of the goods.
A.18	Make decision on the Origin-based treatment based on the DO data
	If the DO details match the Customs clearance data, Customs of the importing party will grant the corresponding Origin-based treatment to the goods.

ANNEX V: Comparative Information on Technological Specifications for Interconnectivity for Certificates of Origin

I. Introduction

This annex provides a detailed comparison of technological solutions for cross-border Certificate of Origin (CO) data exchange. It covers service interface protocols, message formats, network infrastructure, middleware solutions and system security, highlighting their strengths and weaknesses in the context of the current practices of the Members concerned, with the aim of providing a frame of reference and facilitating decision-making on the most suitable approach for CO interconnectivity.

II. Comparison of technical specifications

II.A. Service interface protocols

Service interface protocols define the methods and rules that systems use to communicate. They ensure consistent and reliable exchanges of data between exporting and importing countries. The choice of protocol significantly impacts interoperability, scalability and ease of integration with other systems.

Protocol	Description	Strengths	Weaknesses
SOAP	Strict protocol-based solution with WSDL (Web Services Description Language) for highly structured exchanges	<ul style="list-style-type: none"> – Ensures interoperability through strict schemas – Robust error handling and WS-Security – Ideal for complex, standards-compliant systems 	<ul style="list-style-type: none"> – XML verbosity increases payload size – Complex setup and maintenance – Requires skilled resources
RESTful APIs	Lightweight architectural style using HTTP methods for data exchange	<ul style="list-style-type: none"> – Simpler and faster than SOAP – Flexible and cost-effective for real-time exchanges – Scalable for cloud environments 	<ul style="list-style-type: none"> – Limited built-in security – Not ideal for batch processing or complex workflows
EDI	Legacy solution for structured business document exchange (e.g. EDIFACT, X12)	<ul style="list-style-type: none"> – Proven reliability for large-scale data exchanges – Built-in integrity and non-repudiation – Strong standardization for compliance 	<ul style="list-style-type: none"> – Costly and inflexible legacy systems – Initial implementation complexity – Requires middleware for integration

II.B. Message formats

Message formats specify the structure and encoding of data exchanged between systems. Selecting the right format affects data size, parsing efficiency and compatibility with the chosen protocols and infrastructure.

Format	Description	Strengths	Weaknesses
XML	Highly structured format used in SOAP and some RESTful APIs	<ul style="list-style-type: none"> – Ensures robust validation with schemas – Ideal for complex nested structures such as COs listing multiple goods with differing HS codes and origin criteria 	<ul style="list-style-type: none"> – Verbose, leading to larger payloads and slower transmission – Parsing overhead for systems
JSON	Lightweight format primarily used in RESTful APIs	<ul style="list-style-type: none"> – Faster and more efficient than XML. – Easier to parse and process for modern systems 	<ul style="list-style-type: none"> – Less rigid validation compared to XML – Not ideal for highly structured compliance documents
EDIFACT	A standard for EDI, designed for structured trade documents	<ul style="list-style-type: none"> – Tailored to global trade requirements, ensuring high compatibility – Proven reliability in Customs settings 	<ul style="list-style-type: none"> – Limited flexibility for customization – Requires middleware for modern integration

II.C. Network infrastructure

Network infrastructure refers to the underlying systems and technologies that enable secure and efficient communication. It encompasses the physical and virtual methods used to transmit data across borders, ensuring reliability and compliance with security standards.

Type	Description	Strengths	Weaknesses
Dedicated lines	A private physical connection between two parties	<ul style="list-style-type: none"> – High level of security and reliability – Minimal latency and downtime, ideal for high-volume exchanges 	<ul style="list-style-type: none"> – Expensive to install and maintain. – Limited scalability; not suitable for dynamic systems
TLS (Transport Layer Security)	Cryptographic protocol securing data in transit, commonly used in HTTPS	<ul style="list-style-type: none"> – Widely adopted, cost-effective and easy to implement – Compatible with public internet and cloud-based systems 	<ul style="list-style-type: none"> – Does not address security needs beyond data transit – Dependent on proper implementation to avoid vulnerabilities

Type	Description	Strengths	Weaknesses
VPN (Virtual Private Network)	Creates a private and encrypted connection over public internet infrastructure	<ul style="list-style-type: none"> – Cost-effective compared to dedicated lines – Scalable and flexible for dynamic environments 	<ul style="list-style-type: none"> – Dependent on public internet reliability – May require regular updates to ensure robust encryption

II.D. Middleware solutions

Middleware solutions act as intermediaries, enabling seamless, reliable and secure communication between diverse systems in cross-border CO data exchange. These tools simplify the development and management of systems by decoupling service interface protocols, message formats and network infrastructure.

For example:

- Middleware can translate between protocols like SOAP, REST or EDI, ensuring systems with different interfaces can still communicate seamlessly.
- It can convert message formats, such as transforming XML messages into JSON or EDIFACT, to enable compatibility between modern and legacy systems.
- Middleware also provides an abstraction layer over network infrastructure like VPNs, TLS or cloud services, simplifying network management and allowing developers to focus on business logic rather than technical connectivity.

However, these solutions should be recommended restrictively, to be used only for complex system integration or workflows demanding a high level of reliability. While middleware simplifies integration, it often incurs significant costs, including licensing, maintenance and reliance on solution providers for support.

Type	Description	Examples	Strengths	Weaknesses
Message-oriented middleware (MOM)	Facilitates reliable, asynchronous messaging between systems, ensuring guaranteed delivery and order	IBM MQ, RabbitMQ	<ul style="list-style-type: none"> – Ideal for workflows with high reliability requirements – Supports multiple protocols like SOAP or REST 	<ul style="list-style-type: none"> – Requires specialized setup and maintenance – Adds complexity to simpler systems
Managed file transfer (MFT)	Provides secure, monitored and auditable file exchanges between systems	Axway, GoAnywhere	<ul style="list-style-type: none"> – Ensures compliance with regulatory requirements – Handles large file transfers securely 	<ul style="list-style-type: none"> – Typically focused on batch processes; less suited for real-time exchanges

Type	Description	Examples	Strengths	Weaknesses
API management platforms	Tools that enable API creation, security and analytics for seamless integration between applications	Apigee, MuleSoft, WSO2	<ul style="list-style-type: none"> – Simplifies API deployment and monitoring – Supports scalability in modern cloud-based systems 	– Can increase upfront costs and complexity for small-scale implementations

II.E. System security

System security ensures the confidentiality, integrity and availability of data exchanged across Customs administrations. Given that the system is designed for the cross-border exchange of Certificate of Origin (CO) data, which is regulatory and sensitive in nature, ensuring robust security is paramount. Strong system security safeguards against unauthorized access, data tampering and breaches, while also ensuring compliance with international data protection regulations. Implementing robust security mechanisms is critical to protecting sensitive information and meeting international data protection regulations.

Type	Description	Examples
Network-level security	Protects the communication channel from interception or tampering by securing the pipeline between endpoints	VPNs, TLS protocols
Transmission-level security	Ensures the confidentiality and integrity of data during transit by encrypting it, regardless of the communication channel	TLS, IPsec
Message-level security	Provides end-to-end protection of the message content, ensuring authenticity, integrity and non-repudiation independently of the transport method	Electronic signatures, digital certificates
Application-level security	Secures the internal processes of applications, including input validation, secure data storage and protection against application vulnerabilities	Single sign-on (SSO), secure coding practices, role-based access control
Authentication mechanisms	Verifies the identity of users or systems accessing the system, ensuring that only authorized entities can interact with the system	Passwords, multi-factor authentication (MFA), OAuth
Audit and logging	Tracks and records system activities to provide accountability, traceability for monitoring and compliance monitoring	Activity logs, audit trails, ethical hacking

To ensure the comprehensive protection of the CO exchange system, a layered approach to system security is recommended. Each security measure addresses a specific vulnerability, and, when combined, they provide a robust defence-in-depth strategy.

By implementing multiple layers of security, Customs administrations can mitigate risks, comply with international regulations and build trust in the cross-border exchange of sensitive regulatory data.

III. Recommendations

Choosing the right protocol is critical to ensuring interoperability and meeting technical and legislative requirements.

- SOAP: Suited for Customs administrations with strict legislative and technical requirements that demand high reliability, security and adherence to standards.
- RESTful APIs: Suited for administrations with modern IT infrastructure, limited budgets or a focus on real-time data exchange. They work well for scalable, cloud-based systems.
- EDI: Suited for administrations with legacy systems or where established trade standards like EDIFACT are mandated by law.

Aligning infrastructure to administrative needs ensures secure and efficient cross-border data exchange.

- Dedicated lines: For administrations with high-security requirements and adequate budgets to ensure reliable, private connections.
- VPNs and TLS: Cost-effective solutions for smaller or budget-conscious administrations that still require strong data protection.

Ensuring legislative compliance and data protection safeguards sensitive information and maintains trust. By combining multi-layered security measures, administrations can ensure the secure exchange and protection of the CO data throughout its lifecycle – during transmission, storage and processing.

Optimizing middleware for system integration simplifies complex workflows and enhances connectivity. Middleware solutions often have recurring costs, which should be carefully weighed against their benefits in specific contexts.

Allocating budget and resources effectively ensures long-term sustainability and scalability of systems by considering the total cost of ownership (TCO), including initial setup, maintenance and training, when selecting technologies.

Future-proofing the system ensures adaptability to emerging technologies and evolving trade needs. Additionally, promoting international interoperability by aligning systems with WCO standards ensures seamless collaboration and long-term sustainability.





Contact us:

ori@wcoomd.org

Visit our website:

www.wcoomd.org

