UN/CEFACT

Implementation Guide, SPS-part

E-Certification

April 2021

Inhoudsopgave

1 Introduction

UN/CEFACT delivered the Electronic SPS Certificate (e-CERT) several years ago. Many countries have implemented this and are successfully exchanging e-Certificates.

In 2018 IPPC introduced a tailor-made e-Cert platform called e-Phyto hub. Two operational instruments have been implemented; a hub and a generic web-based national system. The e-Phyto hub offers a standardized method for exchanging these certificates. The situation to date is that for phytosanitary certificates both direct (country to country,) and interactions via the Hub exist.

This Implementation Guide describes and gives guidance to implementation which is on the one hand HUB compliant and on the other hand still facilitates direct communications

The aim is to facilitate a standardized implementation in countries which wish to implement e-Certification for SPS certificates.

Using the Implementation Guide, governments should be able to implement the UN/CEFACT standard: Electronic SPS Certificate (e-CERT) .

e-Cert can be used in all WTO-SPS-domains: Phytosanitary (IPPC), Food (Codex Alimentarius) en Veterinary (OIE)

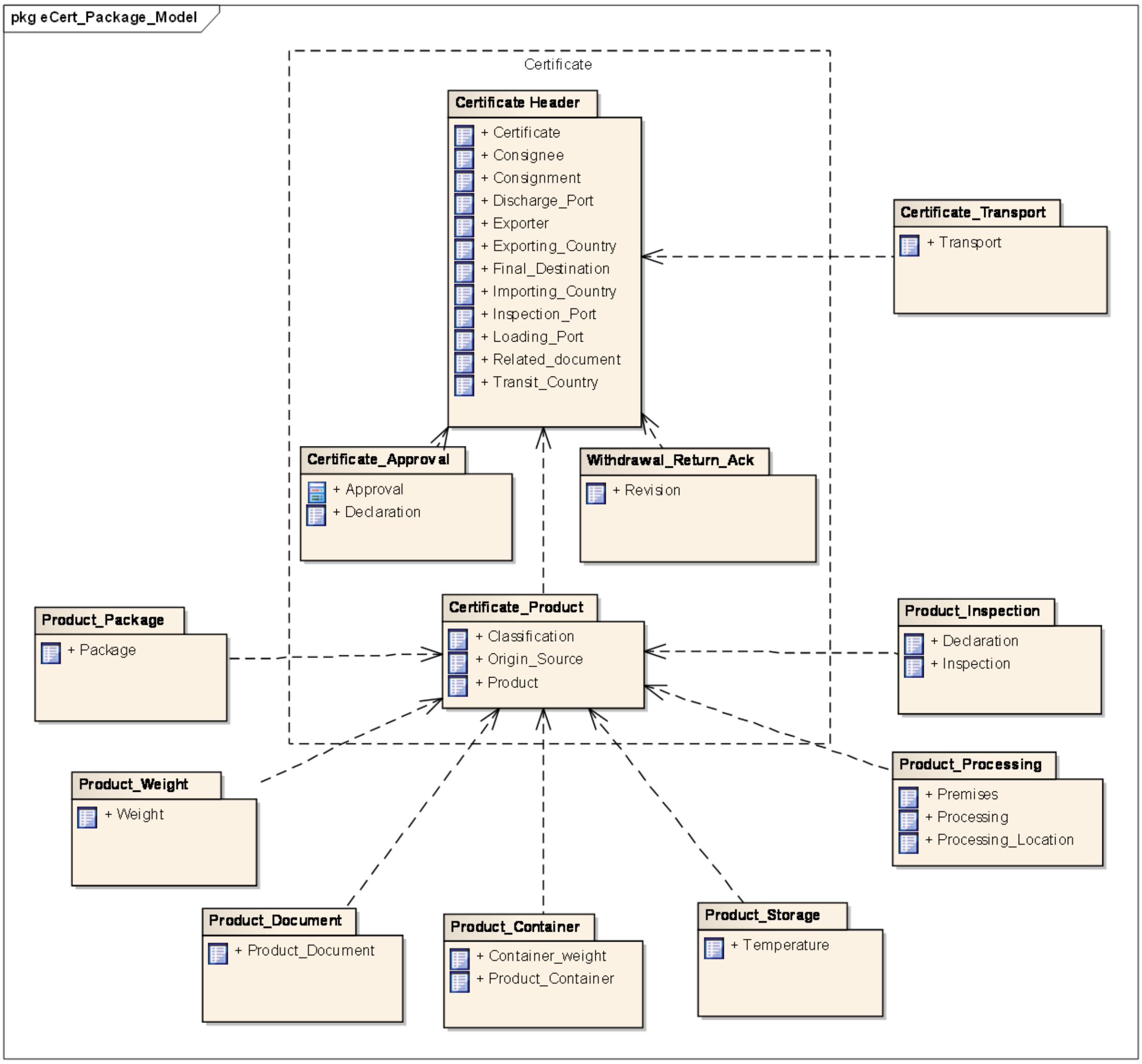
The Implementation Guide is based on existing implementations using Webservices Description Language (WSDL), a free, open standard.

2 Abbreviations

CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CODEX Alimentarius Commission	The Codex Alimentarius Commission was created in 1963 by FAO and WHO to develop food standards, guidelines and related texts such as codes of practice under the Joint FAO/WHO Food Standards Programme. The main purposes of this Programme are protecting health of the consumers and ensuring fair trade practices in the food trade, and promoting coordination of all food standards work
CPM	Commission on Phytosanitary Measures is the governing body of the IPPC
ePhyto	Electronic Phytosanitary Certificate for fresh products of plant origin
G2G	Government tot Government
IPPC	International Plant Protection Convention
NPPO	National Plant Protection Organization
OIE	World Organisation for Animal Health
SPS	Sanitary and Phytosanitary
UNECE	UN Nations Economic Commission for Europe
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UNCITRAL	United Nations Commission on International Trade Law
WCO	World Customs Organization
WHO	World Health Organization
WSDL	Web Service Definition Language
WTO	World Trade Organization
XML	Extensible Markup Language http://www.w3.org/XML/

3 The Concept of E-Cert

The e-Cert conceptual data model below describes the structure of e-Cert components that are required to verify compliance with agreed requirements.



Certificate Header

The Certificate Header comprises base information relating to the whole consignment. The certificate header section is primarily used for identification, traceability and authentication. It describes the following attributes:

Document specific

- The type of document issued
- Title and subtitle of the export certificate
- Indication whether the document is a copy of an issued original export certificate
- The issuing competent authority
- Official or commercial remarks

- References to documents that support the export certificate

Export specific

- Name, address, and/or registration of the party exporting the consignment
- The country from which the consignment is sent
- Location at which the consignment is loaded for export

Import specific

- Name, address, identifier, and representative of the party receiving the consignment
- The country and region to which the consignment is being sent for import
- Location of final destination to which the consignment is being sent
- Location where the consignment is to be inspected for border clearance purposes

A separate certificate is issued for each consignment and these attributes are unique to each certificate. Multiple authorising, supporting or corresponding documents may be referenced to facilitate border clearance.

Certificate Transport

The Certificate Transport details identify the main carriage for this consignment, including routing details:

- Country/s through which the consignment transits
- Border crossing points through which the consignment transits
- Locations at which the consignment may be stored while in transit
- Name and address of customs agent
- References to the voyage, journey, or conveyance, including the mode of transport
- The carrier on the main carriage
- Identifiers of the used transport equipment, such as shipping containers, seals applied by the competent authority, and controlled transport temperature settings, where applicable
- Indication whether the commodities are used as Ship Stores

Certificate Product

The Certificate Product details identify individual agricultural commodity items included in this consignment. This information will determine the type of certificate provided. It may also state the handling processes that were applied to the product, such as sterilization or packaging. It may be used by the border control authority to determine the level of inspection required at the point of entry. It describes the following attributes:

- Descriptions, including common and scientific names for the agricultural commodities
- Commodity codes governed by various national and international classification systems
- The intended use of the agricultural commodities
- Expiry dates
- The country or region of origin
- Manufacturing batch identifier and marks of the agricultural commodity as shown on the package
- Commodity item specific official or commercial remarks

- Product Package: Number and type of packages, nested if applicable
- Product Weight: Gross and net weight (or volume) of the agricultural commodity items
- Product Container: The identifiers of containers and seals product is shipped in
- Product Processing: Processing or handling details pertaining to the agricultural commodities include:
    - The type of processing or handling
    - Name, address, and registration identifier of the relevant operator
    - Process dates or periods
    - Countries and regions of origin
    - Process characteristics such as sterilization or treatment conditions
- Product Storage: Identifies the appropriate storage temperatures for the product during transit to the exporting country
- Product Inspection: The verification of treatments applied to the products within a consignment and the type of inspection the goods have been subjected to. These activities may vary depending on a number of factors such as origin country, type of product etc.
- Product Documentation: The use of supporting documentation to further verify product eligibility for the purpose of import clearance

Certificate Approval

The Certificate Approval comprises base information relating to the whole consignment. It describes the following attributes:

- Certifying declarations in multiple languages of the exporting, importing, and transit countries
- Authentication of the certificate, implying approval, and including details of the certifying officer

Withdrawal/ Return/ Acknowledgement Document

The Acknowledgement Document comprises base information relating to the whole consignment. It describes the following attributes:

- References to the received export certificate
- Revised status of the certificate, including a revision date and reason information

4 The UN/CEFACT standard Electronic SPS Certificate (e-CERT)

The structure of an electronic SPS certificate has been published by UN/CEFACT as a global international standard under the name e-CERT.

The standard includes:

- A Business Requirement Specification (BRS) or Business Process Model, which explains the business processes that are supported by the e-CERT standard;
- A Data Requirement Specification (RSM), which is a data model of the message and explains the data fields used in the message;
- A set of XML Schemas, which specify the structure of the messages for electronic exchange of the certificates.

Information about the e-CERT standard is available on the UN/CEFACT website.

The model provides an XML based message structure and associated data components suitable for use by developers in the building of e-CERT compatible systems.

The data structures of the e-CERT are based on the UN/CEFACT Core Component Library (CCL), which means that the data structures are compatible with other CEFACT messages.

The e-CERT data model describes the structure of e-CERT components that are required to verify compliance with agreed requirements.

5 Electronic SPS Certificate (e-CERT): Exchange of e-Cert certificates with the exporting/importing country

Electronic SPS Certificate (e-CERT) can be represented in the following model:

In order to exchange e-Cert certificates electronically between trading countries, firstly, in case that the inspection- en distribution- process is based on paper, the certificate data needs to be converted into an electronic form.
When there is an electronic certificate available, it can be exchanged. The technical basis of the electronic exchange is the standard of UN/CEFACT (UN/CEFACT, 2008) Electronic SPS Certificate (e-CERT);

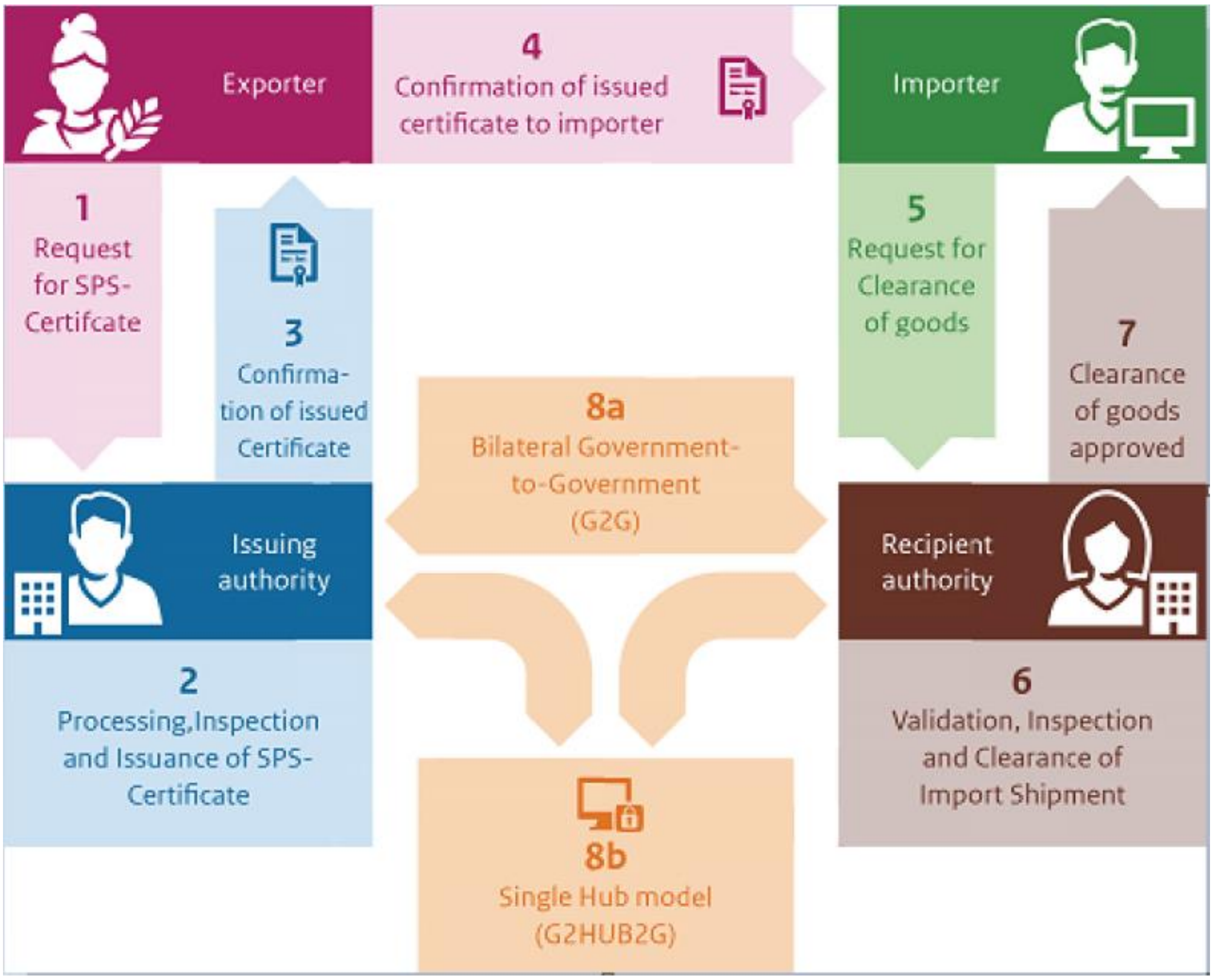
SPS certificates can be exchanged in the following way:

Bilateral Government-to-Government: e-CERT SPS-Certificates are exchanged directly from government bodies to government bodies via their electronic SPS certificate management systems, National Single Windows. This approach has been used for example by New Zealand, Australia and the Netherlands with their trading partners.

Single Hub Model: This model is currently available for phytosanitary certificates in the context of the ePhyto exchange HUB.
An exporting NPPO can send an ePhyto certificate via a secured system to the importing country's mailbox, upon which the hub notifies the importing country that it has an ePhyto certificate in its box, and the importing country can then retrieve the ePhyto certificate. This option eliminates the need for multiple bilateral access agreements and enables all countries (NPPOs) that adopt the hub protocols to exchange data with one another

6 Proces in general

The process-steps for exchange of the certificates can be illustrated as follows:


Exporter
4
Confirmation of issued certificate to importer
Importer
1
Request for SPS-Certifcate
3
Confirma-tion of issued Certificate
5
Request for Clearance of goods
7
Clearance of goods approved
8a
Bilateral Government-to-Government (G2G)
Issuing authority
Recipient authority
2
Processing,Inspection and Issuance of SPS-Certificate
6
Validation, Inspection and Clearance of Import Shipment
8b
Single Hub model (G2HUB2G)

Step 1 is a request for an electronic certificate from the Exporter to the Competent Authority of the issuing country

Step 2 is potentially carry out an inspection, and processing /issuing an electronic certificate

Step 3 is a conformation of the issuing authority to the Exporter that an electronic certificate has been issued

Step 4 is a message from the Exporter to the Importer that an electronic Certificate has been issued

Step 5 is a request from the Importer for Clearance of the Goods to the Recipient Authority

Step 6 is a Validation, Inspection and Clearance of the Import Shipment

Step 7 is the Clearance of the approved Goods

A main step in this total process is the exchange of the electronic certificate between the issuing and recipient authority

This exchange can be done either Government to Government (step 8a) or with the use of the IPPC-HUB (step 8b)

7 The Process Actors of e-Certification

Introduction

The main stakeholders are:

IMPORTS

- Ministry of Agriculture/Ministry of trade for the SPS agreements
- Competent authority of the exporting country
- [Border Control authorities of the exporting country][1]
- Border Control authorities of the importing country
- [Exporters]
- Importers

EXPORTS

- Ministry of Agriculture/Ministry of trade for the SPS agreements
- Competent authority
- [Border Control authorities of the exporting country]
- Exporters
- [Border Control authorities of the importing country]
- [Competent authority of the importing country]
- [Importers]

e-CERT can be used by the exchange of e-certificates between the competent authorities of the importing and exporting countries.

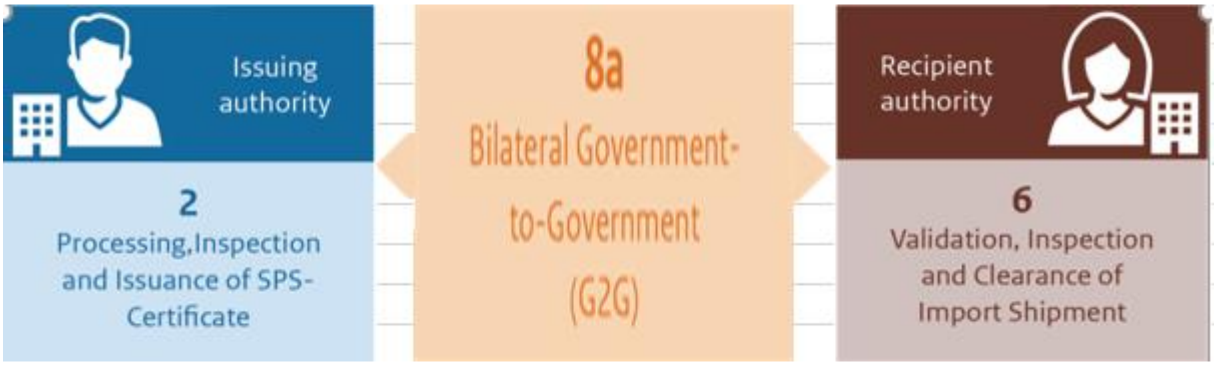
For exporting countries, the exchange of electronic SPS certificates with other nations requires the Ministry of Agriculture/Trade for the bilateral agreements and Border Control officials and/or the Competent Authority of the importing country for an agreement of the message transport methodology and its details. Only the competent authority and the exporters are stakeholders.

For importing countries, the actors and processes are different and independent of the export process. The main differences are that contact needs to be established with the exporting countries for agreement on the message transport methodology and the collaboration between importers and their competent authorities.

Point-to-Point

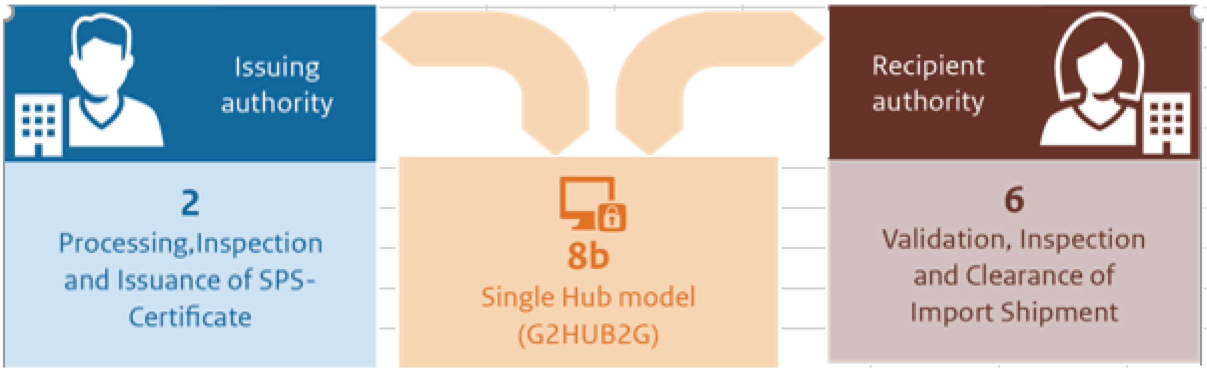
eCERT messages in this (Government-to-Government)model are exchanged directly from government bodies to government bodies via their National Single Windows, or more frequently their electronic SPS certificate management systems. This approach has been used for example by New Zealand, Australia and the Netherlands with their trading partners.

[1] Square brackets indicate parties that do not necessarily play a role in the process.


Issuing authority
2
Processing,Inspection and Issuance of SPS-Certificate
8a
Bilateral Government-to-Government (G2G)
Recipient authority
6
Validation, Inspection and Clearance of Import Shipment

Using the HUB

Single point (HUB) exchange allows exchanges between all of the countries connected to the HUB. Any new country connecting to the HUB will be able to exchange certificates with all of the other connected countries


Issuing authority
2
Processing,Inspection and Issuance of SPS-Certificate
8b
Single Hub model (G2HUB2G)
Recipient authority
6
Validation, Inspection and Clearance of Import Shipment

8 The Processes

Using the HUB

1. The Issuing Authority prepares the Certificate Data
2. The Issuing Authority authorizes the issuance of the XML Certificate Data Set
3. The Issuing Authority asks (once) for a Credential at the Administrator of the HUB
4. The Issuing Authority inserts the XML Message and the Credential into an Envelope. The envelope contains data to facilitate the delivery envelope (Credential, Message itself, Sender ID, Receiver ID, Message Date, Message ID)
5. The Issuing Authority Envelope containing the XML Message and the Credential is delivered to the HUB.
6. The HUB verifies the Envelope Data
7. The Envelope is saved in the HUB until sent to the Recipient Authority. The security of the Envelope at this stage is responsibility of the HUB
8. When the Envelope is to be sent to the Recipient Authority, the HUB searches the HUB storage folders, retrieves the Envelope and sends this to the Recipient Authority.
9. In order to the Recipient Authority could be sure of the HUB Identity, the HUB needs to ask for a Credential (once) to the Issuing Authority
10. All the Envelopes are introduced in a new Envelope that also contains the HUB Credential
11. The Delivery of the new envelope to the Recipient Authority is also a secure transmission (HTTPS)
12. The Recipient Authority opens the Envelope, obtains the Messages (Original Envelopes) and depending of the type of each Message, the Recipient Authority decides what to do.

Point-to-Point

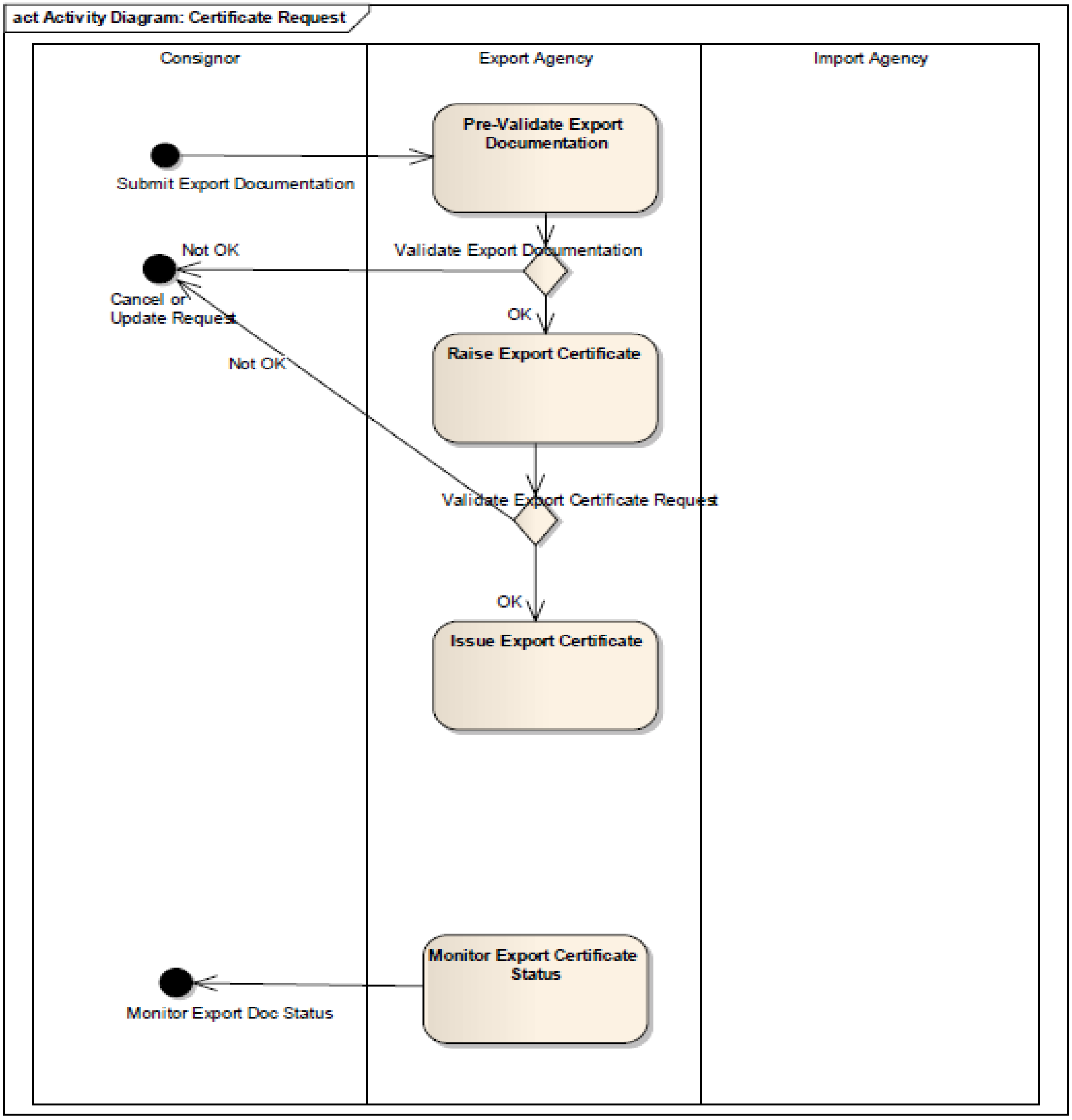
The bi-lateral management of Export Certification information flows includes a number of activities carried out by a number of parties and roles. In the normal course of events, the flow is:

Consignor (Exporter) -> Export Agency -> Import Agency (Border Inspector) -> Consignee (Importer)

Some of the information flows described within this section are not necessarily a direct flow of information; they act as a monitor of the current status of an export certificate request.

Certificate Request

The activity diagram below illustrates the activities of the consignor and export agency:


act Activity Diagram: Certificate Request
Consignor
Export Agency
Import Agency
Pre-Validate Export Documentation
Submit Export Documentation
Not OK
Validate Export Documentation
Cancel or Update Request
OK
Raise Export Certificate
Not OK
Validate Export Certificate Request
OK
Issue Export Certificate
Monitor Export Certificate Status
Monitor Export Doc Status

The certificate request process involves:

1. The export agency receiving export documentation from the consignor.

2. The export agency checking the validity of the export documentation against the business rules and MoU (if relevant) for export.

3. The consignor raising an export certificate request from the provided export documentation or requesting that the consignor update the export documentation provided or cancel the export request.

4. The export agency checking the validity of the export certificate request.

5. The export agency approving (issuing) the export certificate or requesting that the consignor update their export certificate request or cancel the export request.

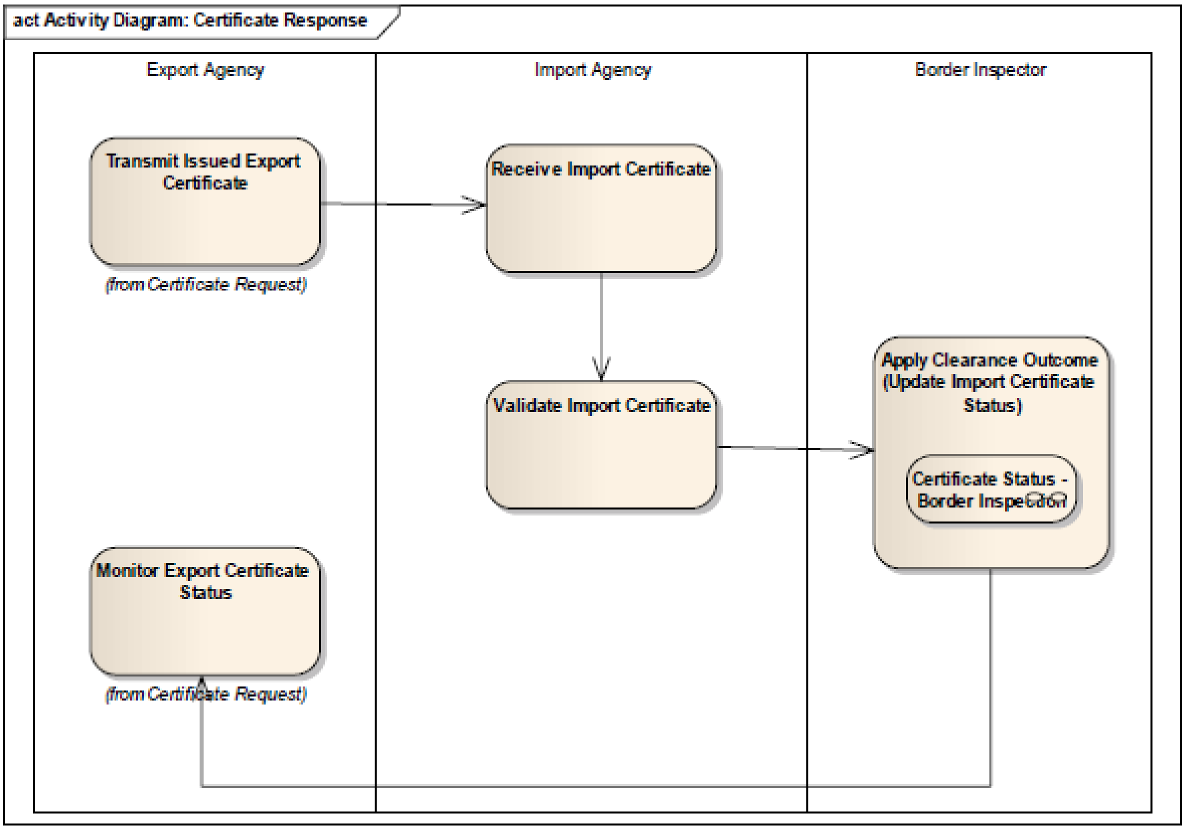
6. The export agency and the consignor monitoring the certificate progress (status) throughout the certificate request process.

The specific processes are:

Process	**Brief Description**
Pre-validate Export Documentation	The export regulator (agency) assesses and approves product eligibility for the intended market.
Validation Export Documentation	Based on the export agencies validation decision the submitted documentation may need to be updated (by the consignor), an export certificate request may be raised, or the export documentation may be cancelled.
Raise Export Certificate Request	When the export documentation provided has been fully validated (as correct) by the export agency the consignor can request an export certificate.
Validate Export Certificate Request	The export agency receives the export certificate request, assesses the information for compliance (against importing country requirements including any relevant MoU).
Cancel Export Certificate Request	Where the export certificate request fails to comply with importing country requirements that export request is cancelled.
Issue Export Certificate	The export regulator approves the export certificate request and issues a certificate confirming the import regulator's requirements have been met.
Monitor Export Certificate Status	A message is sent within the system and/or between systems whenever the status of an export certificate request or issued export certificate changes.

Certificate Response
The activity diagram illustrates the activities of the export agency and the import agency.

The certificate response process details the actions taken by the export agency to transmit the issued export certificate to the importing country and for the import agency to review the export certificate, apply internal rules (as required) and advise the clearance outcome of the import request.

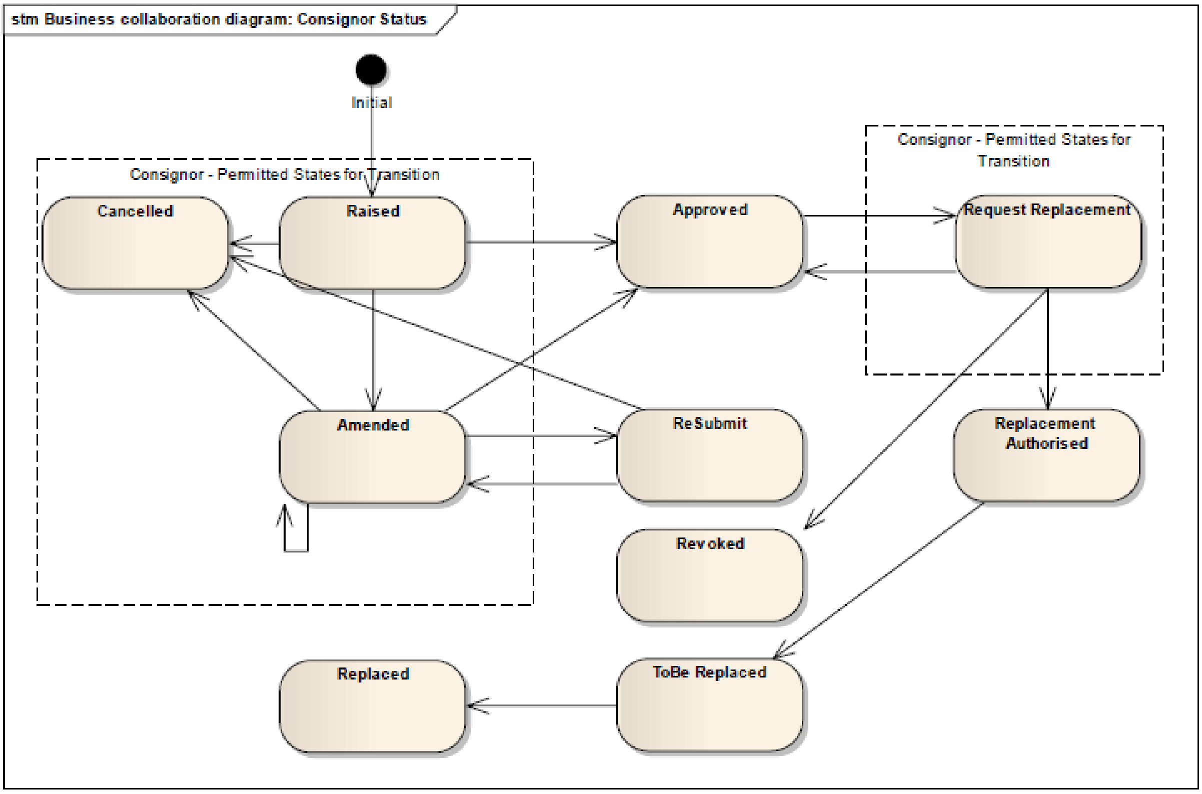

act Activity Diagram: Certificate Response
Export Agency
Import Agency
Border Inspector
Transmit Issued Export Certificate
(from Certificate Request)
Receive Import Certificate
Validate Import Certificate
Apply Clearance Outcome (Update Import Certificate Status)
Certificate Status - Border Inspector
Monitor Export Certificate Status
(from Certificate Request)

The specific processes are:

Process	Brief Description
Transmit Export Certificate	Upon issuing the export certificate the printed certificate accompanies the certificate and/or an XML (representation of the issued certificate) is exchanged.
Receive Export Certificate	The import agency receives the export certificate.
Validate Export Certificate	The import agency assesses the information for compliance (against importing country requirements including any relevant MoU).
Apply Clearance Outcome	The border inspector (of the import agency) acknowledges receipt of the export certificate and in due course notifies the outcome of the validation undertaken.
Monitor Certificate Progress	A message is sent within the system and/or between systems whenever the status of an export certificate request or issued export certificate changes.

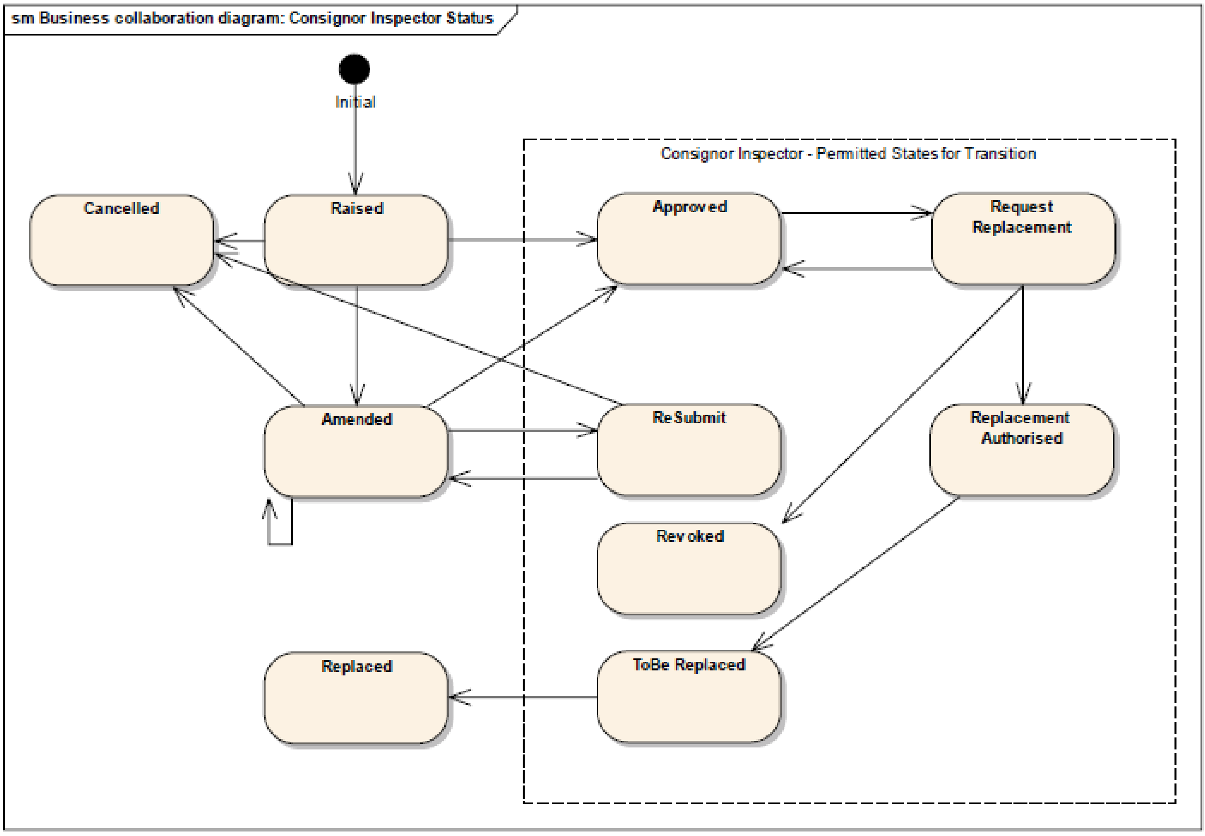
Certificate Statuses

The permitted export certificate states and transitions available to the **consignor (exporter)** are:


stm Business collaboration diagram: Consignor Status
Initial
Consignor - Permitted States for Transition
Cancelled
Raised
Amended
Approved
ReSubmit
Revoked
Consignor - Permitted States for Transition
Request Replacement
Replacement Authorised
Replaced
ToBe Replaced

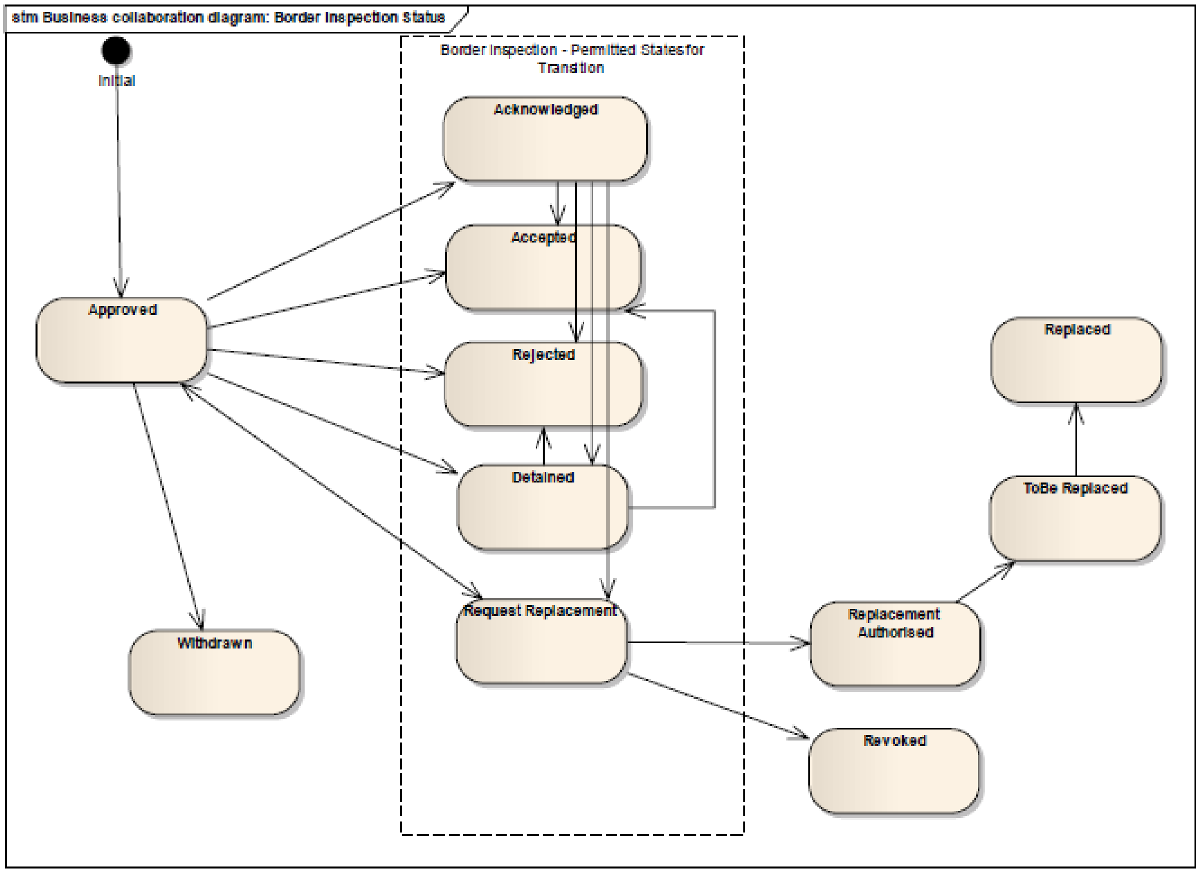
Status	Brief Description
Raised	The initial application for the Certificate is submitted by the consignor
Cancelled	The Certificate request is cancelled by the consignor.
Amended	The Certificate request is amended by the consignor before the goods are presented for validation by the Export Agency (regulator)
Request Replacement	When an 'Approved' Certificate is to be replaced at the request of the consignor.

The permitted export certificate states and transitions available to the **export agency (regulator / consignor inspector**) are:


sm Business collaboration diagram: Consignor Inspector Status
Initial
Consignor Inspector - Permitted States for Transition
Cancelled
Raised
Approved
Request Replacement
Amended
ReSubmit
Replacement Authorised
Revoked
Replaced
ToBe Replaced

Status	Brief Description
Resubmit	Export Agency (consignor inspector) requires amendments to be applied to the request for a Certificate.
Approved	The Certificate is approved by the Export Agency (consignor inspector).
Request Replacement	When an 'Approved' Certificate is to be replaced at the request of the Export Agency (consignor inspector).
Replacement Authorised	Request to replace an approved Certificate has been authorised by the Export Agency (regulator). This triggers the state "To be Replaced".
To be Replaced	Exporter Agency (regulator) agrees to replace the Certificate. Certificate remains in this state until the replacement certificate is approved.
Revoked	The certificate is revoked by the Export Agency (regulator).
Replaced	The Certificate is replaced as a resultof the export agency (consignment inspector) approving the replacement certificate.

The permitted export certificate states and transitions available to the **import agency (border inspector)** are:



Status	Brief Description
Acknowledged	The Certificate is acknowledged as having been received by the Import Agency (border inspection).
Accepted	The Certificate is accepted by the Import Agency (border inspection). This does not mean the acceptance of the actual consignment; rather it is the acceptance of the certificate data.
Detained	The Certificate is detained whilst the Import Agency applies its inspection regime.
Rejected	The goods are refused entry by the Import Agency and the certificate is rejected.
Request Replacement	When an 'Approved' Certificate is to be replaced at the request of the Import Agency.
Withdrawn	When an 'Approved' Certificate is withdrawn by the Export Agency
Replaced	When an 'Approved' Certificate has been replaced at the request of the Import Agency.
Revoked	When a replacement request is denied, the certificate is revoked or returned to the status of approved by the Export Agency

9 Business Requirement Specification (BRS)

In the BRS relevant actors, processes, information flows, and data element are presented in a business-friendly way

In the BRS the BIEs (business information entities), ABIEs (aggregate business information entities) and ASBIEs (associated business information entities) are defined by the Business

For typing the Business Entities, the Core Datatypes of the Core Component Library (UNCCL) can be used.

The E-cert Package Model, as described in chapter 2, indicates the structure of the export certificate.

The export certificate has two fundamental levels - the Certificate and Product.

Within each of these levels are a number of related subject areas and classes.

Certificate Header	Contains Information relating to the whole consignment for recording ownership and transport aspects
Certificate Transport	Contains Transport Details relating to the consignment
Certificate Product	Contains the details of the product that makes up the consignment being certified
Product Package	Contains the packaging associated with the products within the consignment
Product Weight	Contains the actual weight of the product being certified
Product Document	Contains the use of supporting documentation to further verify product eligibility for the purpose of import clearance
Product Container	Contains container-information that the consignment is shipped in for traceability purposes
Product Storage	Identifies the appropriate storage temperatures for the product during transit to the exporting country
Product Processing	Processing plays a significant part of determining the product compliance to the regulator's requirements. Both the export and import regulator may approve particularly premises for preparation of the goods.
Product Inspection	Contains the verification of treatments applied to the products within a consignment and the type of inspection the goods have been subjected to. These activities may vary depending on a number of factors such as origin country, type of product etc.
Certificate Approval	Is critical to the acceptance of this certificate as it verifies the authenticity and confirms the integrity of the export certificate.
Withdrawal, Return, Acknowledgement	This package describes the flow of clearance decisions for the certificate between the export and import regulator that reflects the overall outcome of the consignment being exported. It allows the regulators to replace certificates where necessary and to determine the final clearance outcome of the certificate issued.

More Information can be found in the UNECE BRS Document , chapter 5.4, **Information Model Definition (Class Diagrams & Components)**
https://www.unece.org/fileadmin/DAM/cefact/brs/BRS_ExportCertificate__eCert__v5.1.0.pdf

10 Requirements Specification Mapping (RSM)

In de RSM business objects which are defined as BIEs, ABIEs and ASBIEs in business-language mapped on generic objects from the UNCCL.

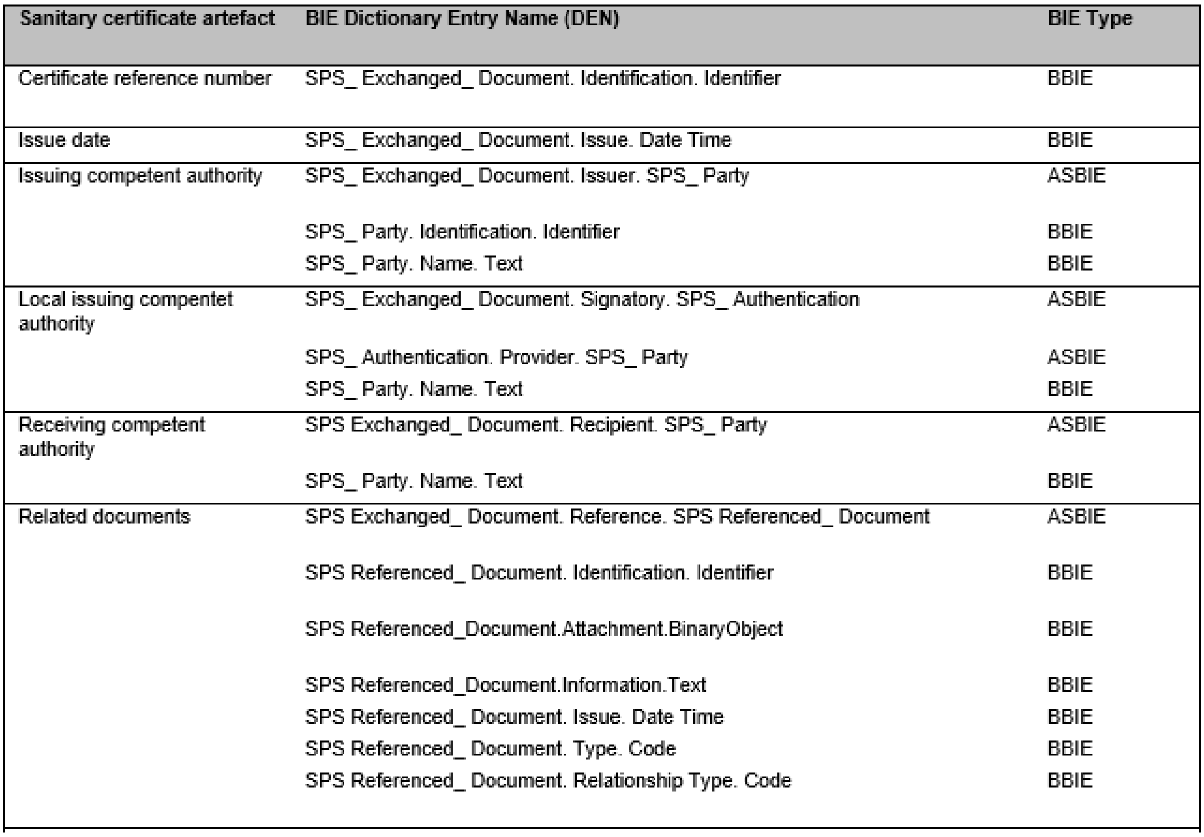
Each BIE is related to an existing or new Core Component element (CC):

- ABIEs -> ACCs (aggregate core component, entity types)

- BBIEs -> BCCs (basic core component, attributes)

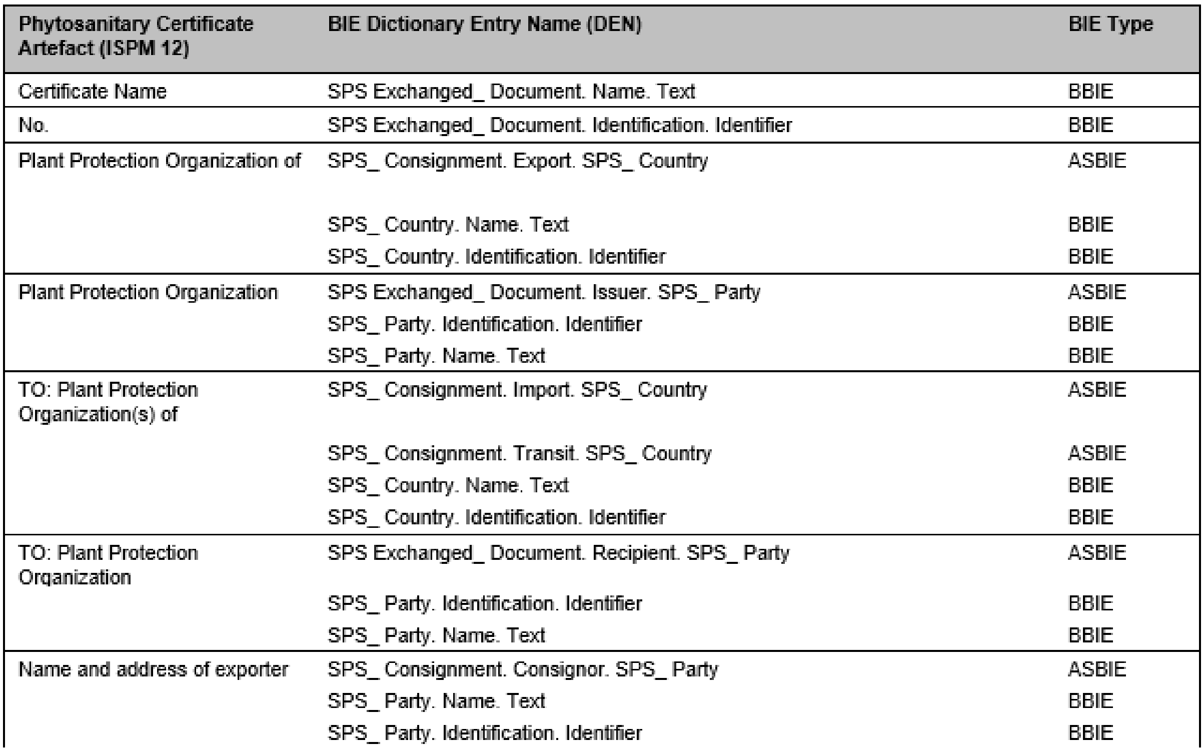
- ASBIEs -> ASCCs (association core component, relations)

The following table illustrates the implementation of **Sanitary** Certificate data against the Business Information Entities. Part of the table is represented.



Sanitary certificate artefact	BIE Dictionary Entry Name (DEN)	BIE Type
Certificate reference number	SPS_ Exchanged_ Document. Identification. Identifier	BBIE
Issue date	SPS_ Exchanged_ Document. Issue. Date Time	BBIE
Issuing competent authority	SPS_ Exchanged_ Document. Issuer. SPS_ Party	ASBIE
	SPS_ Party. Identification. Identifier	BBIE
	SPS_ Party. Name. Text	BBIE
Local issuing compentet authority	SPS_ Exchanged_ Document. Signatory. SPS_ Authentication	ASBIE
	SPS_ Authentication. Provider. SPS_ Party	ASBIE
	SPS_ Party. Name. Text	BBIE
Receiving competent authority	SPS Exchanged_ Document. Recipient. SPS_ Party	ASBIE
	SPS_ Party. Name. Text	BBIE
Related documents	SPS Exchanged_ Document. Reference. SPS Referenced_ Document	ASBIE
	SPS Referenced_ Document. Identification. Identifier	BBIE
	SPS Referenced_Document.Attachment.BinaryObject	BBIE
	SPS Referenced_Document.Information.Text	BBIE
	SPS Referenced_ Document. Issue. Date Time	BBIE
	SPS Referenced_ Document. Type. Code	BBIE
	SPS Referenced_ Document. Relationship Type. Code	BBIE

The following table illustrates the implementation of **Phytosanitary** Certificate data against the Business Information Entities. Part of the table is represented.



Phytosanitary Certificate Artefact (ISPM 12)	BIE Dictionary Entry Name (DEN)	BIE Type
Certificate Name	SPS Exchanged_ Document. Name. Text	BBIE
No.	SPS Exchanged_ Document. Identification. Identifier	BBIE
Plant Protection Organization of	SPS_ Consignment. Export. SPS_ Country	ASBIE
	SPS_ Country. Name. Text	BBIE
	SPS_ Country. Identification. Identifier	BBIE
Plant Protection Organization	SPS Exchanged_ Document. Issuer. SPS_ Party	ASBIE
	SPS_ Party. Identification. Identifier	BBIE
	SPS_ Party. Name. Text	BBIE
TO: Plant Protection Organization(s) of	SPS_ Consignment. Import. SPS_ Country	ASBIE
	SPS_ Consignment. Transit. SPS_ Country	ASBIE
	SPS_ Country. Name. Text	BBIE
	SPS_ Country. Identification. Identifier	BBIE
TO: Plant Protection Organization	SPS Exchanged_ Document. Recipient. SPS_ Party	ASBIE
	SPS_ Party. Identification. Identifier	BBIE
	SPS_ Party. Name. Text	BBIE
Name and address of exporter	SPS_ Consignment. Consignor. SPS_ Party	ASBIE
	SPS_ Party. Name. Text	BBIE
	SPS_ Party. Identification. Identifier	BBIE

More information can be found in the UNECE RSM Document,
chapter 6.3 Implementation of the e-Certmodel
https://www.unece.org/fileadmin/DAM/cefact/rsm/RSM_eCert_v1.4.1.zip

11 XML Scheme Definitions (XSD)

A UN/CEFACT standard Message is an electronic Message that meets the requirements set by UN/CEFACT, which is made up of UNCEFACT core components and is composed on the basis of an XSD published by UNCEFACT.

An Overview and Offer of the available UNCEFACT XML schemas is presented on the UN/CEFACT site:

http://www.unece.org/cefact/xml_schemas/index.html.

XML is the acronym for eXtensibleMarkup Language. It is an internationally recognized computer language. Its format is machine readable but can be easily converted to a more user friendly format such as a PDF file. It is standardized to allow communication through the Internet between different computer systems. It is one of the most widely used computer languages for sharing structured information.

To facilitate the exchange of ePhyto-certificates between various NPPOs, a harmonized schema, codes and lists are needed to ensure that the receiving NPPO can read the sending NPPO message.

CPM-9(2014) adopted the Appendix 1 Electronic phytosanitary-certificates, information on standard XML schemas and exchange mechanisms (2014)to ISPM 12.

NPPO’s are encouraged to use standardized (harmonized) terms, codes and text for the data elements associated with the XML message for ePhyto-certificates

12 WSDL / Message Guide

Introduction

The Message Guide consists of a set of (web) services enabling Recipient Authorities to:

- Find certificates issued by the Issuing Authority
- Get (Download) certificates from the Issuing Authority
- Report the status of a downloaded certificate to the Issuing Authority
- Show the status of a certificate in the repository of the Issuing Authority
- Detect if the network and services at the Issuing are available (Hart beat)

The National Export Certification System NECS and the National Import Certification System (NICS) need to exchange information. In most cases this information needs to be transported over a public network like Internet. In order to prevent for

- Unauthorised access;
- Unauthorised changes;
- Eavesdropping (faking to be the NECS);

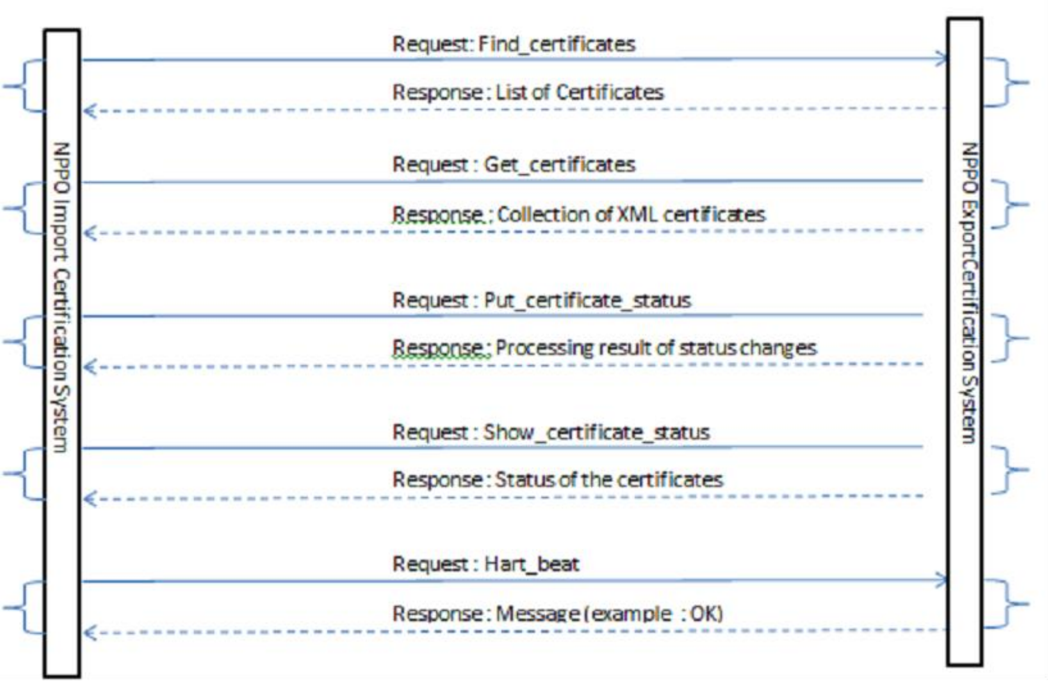
This exchange needs to be secured with an encryption protocol, including a identification and authentication of both the importing and exporting Competent Authority.

It was concluded that a Public Key Infrastructure and X509 certificate (digital fingerprint) , verified and (digitally) signed by a recognised Certificate Authority must be used for identification and authentication of the exporting Competent Authority since this a commonly accepted standard (using HTTPS and SSL) for Web services. At this moment, all implementations already use HTTPS/SSL, so this is already a widely accepted (defacto) standard.

Specification of Conversations

	Action	Service	Description
2.1	Find a list of certificates	Find_certificate	Put the request to the NECS to return all certificate numbers that meet the input criteria. Immediately after this Request the NECS returns the list of numbers
2.2	Download a list of certificates	get_certificate	Put the request to the NECS to return all certificates s that meet the input criteria. Immediately after this request the NECS returns all the certificates
2.3	Change the status of a certificate	Put_certificate_status	Put the request to the NECS to change the status of a list of certificates to the specified value. Immediately after this request the NECS returns the process result for every individual certificate (Succes or Failed with reason)

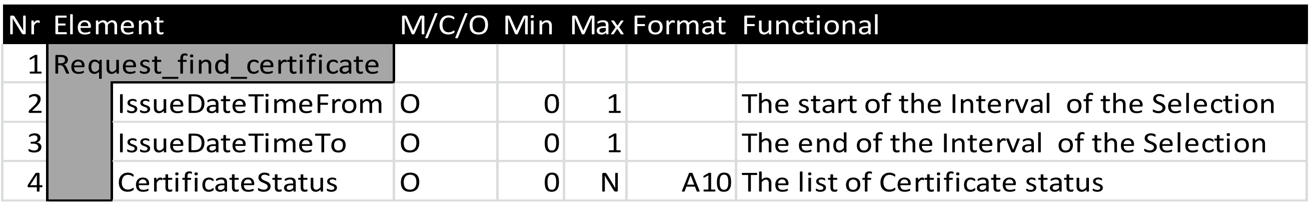
2.4	Show the status of a certificate	Show_certificate_status	Put the request to the NECS to show the status of a list of certificates. Immediately after this request the NECS returns the status for every individual certificate
2.5	Show status of the NECS	Hart_beat	Put the request to the NECS to confirm that the NECS and the network between the NECS and NICS are operational. Immediately after this Request the NECS returns the message OK


NPPO Import Certification System
NPPO ExportCertification System
Request: Find_certificates
Response: List of Certificates
Request : Get_certificates
Response : Collection of XML certificates
Request : Put_certificate_status
Response: Processing result of status changes
Request : Show_certificate_status
Response : Status of the certificates
Request : Hart_beat
Response : Message (example : OK)

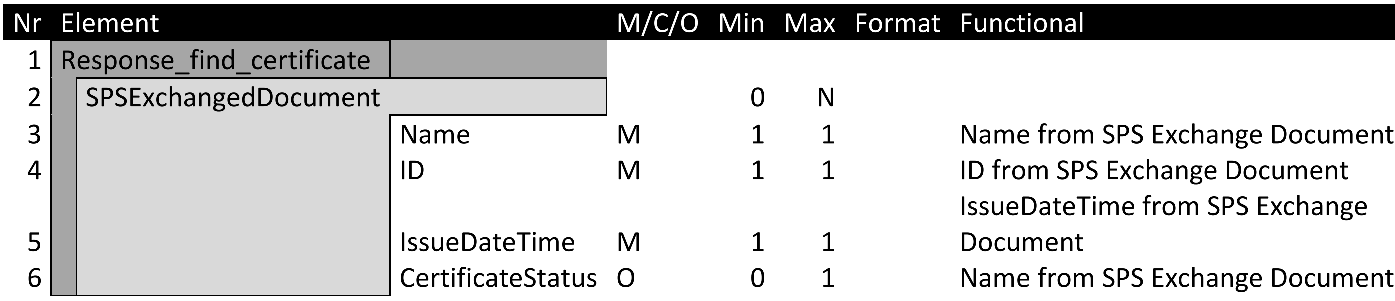
Message Guides

Constraints in the use of elements is specified in the column M/C/O (M= Mandatory, C = Condtional or O = Optional). This chapter shows the message guides (request/response) for each individual communication. Due to the simplicity of the response messages tis document does not specify Class Diagrams.

Message find_certificate



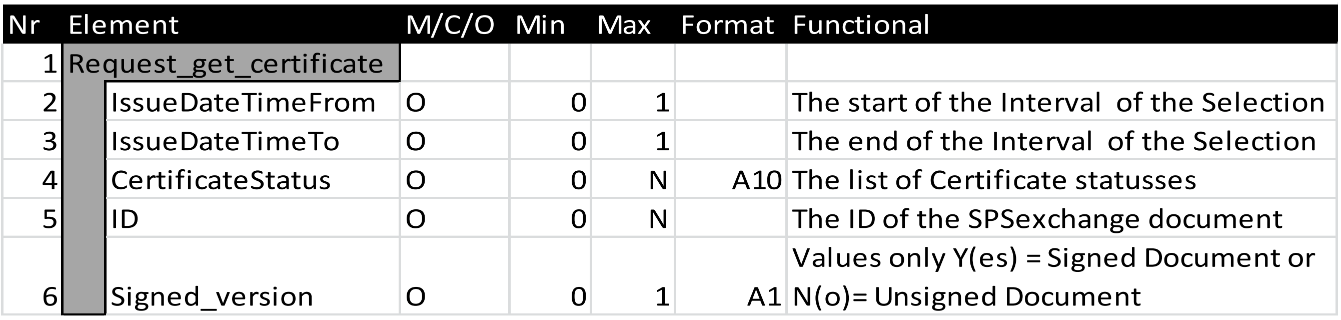
Nr	Element	M/C/O	Min	Max	Format	Functional
1	Request_find_certificate					
2	IssueDateTimeFrom	O	0	1		The start of the Interval of the Selection
3	IssueDateTimeTo	O	0	1		The end of the Interval of the Selection
4	CertificateStatus	O	0	N	A10	The list of Certificate status



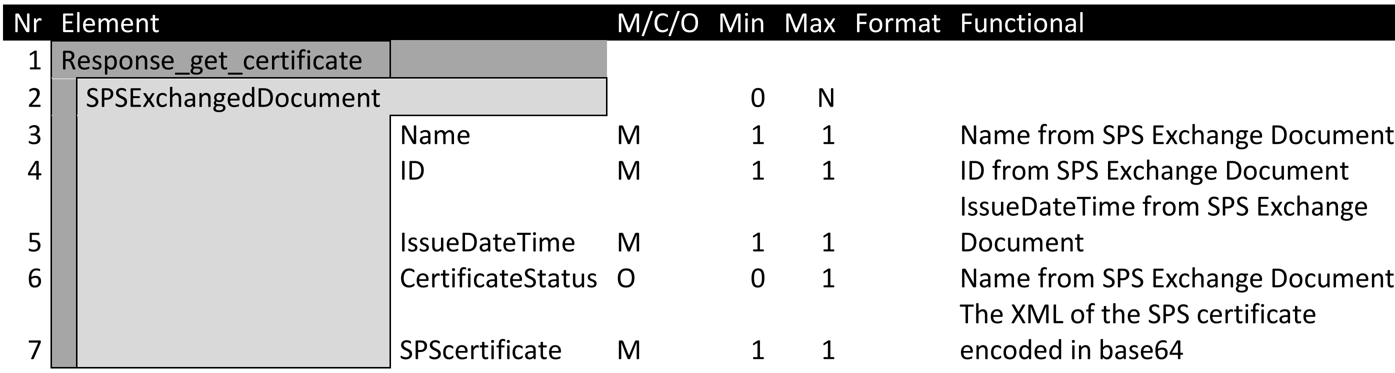
Nr	Element	M/C/O	Min	Max	Format	Functional
1	Response_find_certificate					
2	SPSExchangedDocument		0	N		
3	Name	M	1	1		Name from SPS Exchange Document
4	ID	M	1	1		ID from SPS Exchange Document
5	IssueDateTime	M	1	1		IssueDateTime from SPS Exchange Document
6	CertificateStatus	O	0	1		Name from SPS Exchange Document

If one of the optional elements in Request_find_certificate is absent or has a null value, the certificate is not tested to this value. If for example the element CertificateStatus is missing all the numbers of certificates (ID's) which are issued from and including IssueDateFimeFrom until and including IssueDateTo will be returned, regardless the value of their status.

Message get_certificate



Nr	Element		M/C/O	Min	Max	Format	Functional
1	Request_get_certificate						
2		IssueDateTimeFrom	O	0	1		The start of the Interval of the Selection
3		IssueDateTimeTo	O	0	1		The end of the Interval of the Selection
4		CertificateStatus	O	0	N	A10	The list of Certificate statusses
5		ID	O	0	N		The ID of the SPSexchange document
6		Signed_version	O	0	1	A1	Values only Y(es) = Signed Document or N(o)= Unsigned Document

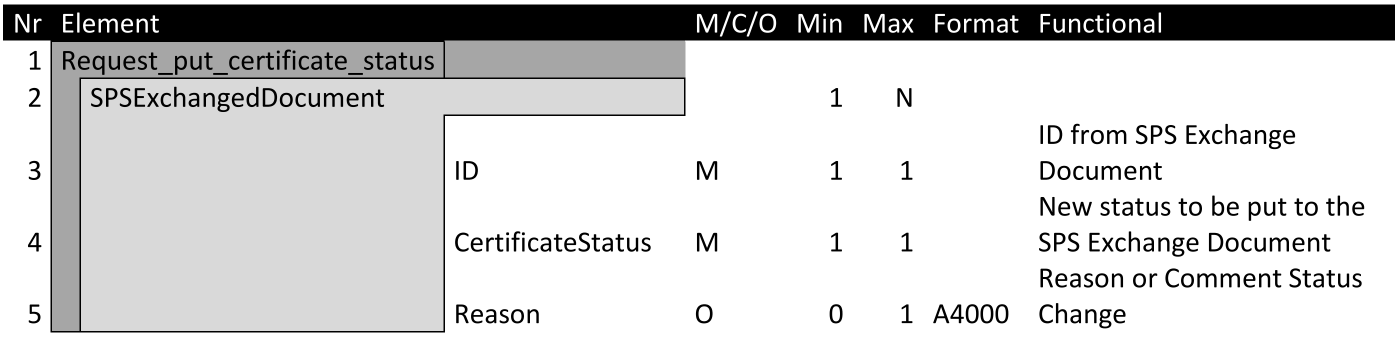


Nr	Element			M/C/O	Min	Max	Format	Functional
1	Response_get_certificate							
2		SPSExchangedDocument			0	N		
3			Name	M	1	1		Name from SPS Exchange Document
4			ID	M	1	1		ID from SPS Exchange Document
5			IssueDateTime	M	1	1		IssueDateTime from SPS Exchange Document
6			CertificateStatus	O	0	1		Name from SPS Exchange Document
7			SPScertificate	M	1	1		The XML of the SPS certificate encoded in base64

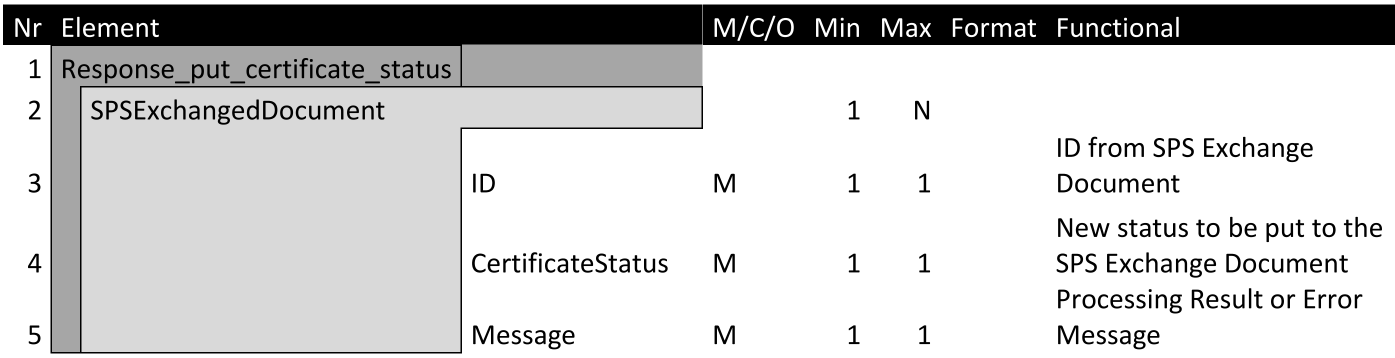
Is one of the optional elements in Request_get_certificate is absent or has a null value, the certificate is not tested to this value. If for example the element CertificateStatus is missing all the certificates (The Base64 version of the XML) which are issued from and including IssueDateTimeFrom until and including IssueDateTo will be returned, regardless the value of their status.

When the element Signed_version in Request_get_certificate is absent or has a null value the unsigned version of the XML will be returned.

Message put_certificate_status

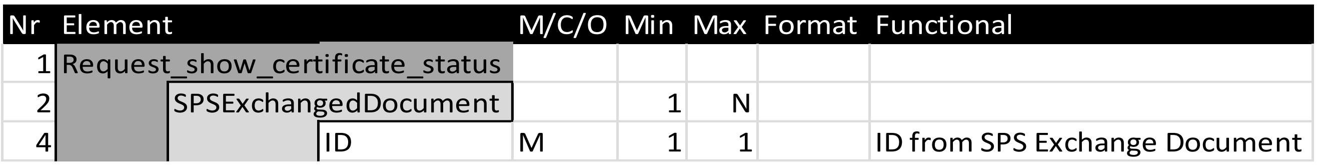


Nr	Element	M/C/O	Min	Max	Format	Functional
1	Request_put_certificate_status					
2	SPSExchangedDocument		1	N		
3	ID	M	1	1		ID from SPS Exchange Document
4	CertificateStatus	M	1	1		New status to be put to the SPS Exchange Document
5	Reason	O	0	1	A4000	Reason or Comment Status Change

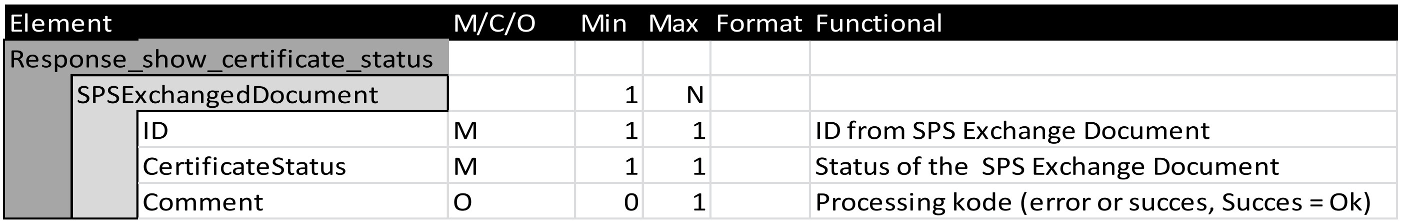


Nr	Element	M/C/O	Min	Max	Format	Functional
1	Response_put_certificate_status					
2	SPSExchangedDocument		1	N		
3	ID	M	1	1		ID from SPS Exchange Document
4	CertificateStatus	M	1	1		New status to be put to the SPS Exchange Document
5	Message	M	1	1		Processing Result or Error Message

Message Show_certificate_status



Nr	Element	M/C/O	Min	Max	Format	Functional
1	Request_show_certificate_status					
2	SPSExchangedDocument		1	N		
4	ID	M	1	1		ID from SPS Exchange Document



Element	M/C/O	Min	Max	Format	Functional
Response_show_certificate_status					
SPSExchangedDocument		1	N		
ID	M	1	1		ID from SPS Exchange Document
CertificateStatus	M	1	1		Status of the SPS Exchange Document
Comment	O	0	1		Processing kode (error or succes, Succes = Ok)

Message hart_beat

Nr	Element	M/C/O	Min	Max	Format	Functional
1	Request_Hart_beat					

Nr	Element	M/C/O	Min	Max	Format	Functional
1	Response_hart_beat					
2	Message		0	1	A10	Response message (OK/NOK)

Using the e-Phyto HUB

The HUB web service schema is composed by a large number of entities, some of them are part of the ePhyto definition, they will be described more in details in each web service operation. See below the list of the main elements:

1) Envelope Header

2) Envelope Content

3) ePhyto Envelope

The WSDL has several operations; mainly supported by the following entities:

a. Envelope Header

b. Envelope = header + content

c. ePhytoEnvelope = header + SPSCertificate

d. Array of Envelope Header

e. Array of Envelope

f. HUBTrackingInfo

g. NPPO

h. ValidationResult

More information can be found in HUB Web Service API IPPC ePhyto HUB v1.16

https://www.ephytoexchange.org/doc/HUB_Web_Service_API.pdf

13 SPS and CITES

Recently the Guideline for eCITES exchange is released.

The document provides a description and guidelines of the choreography that all Parties should follow when exchanging electronic permits with other Parties. It complements the data standard defined in the CITES ePermitting toolkit with a description of processes and a set of that Parties should follow when engaging in EPIX exchanges.

The SPS and CITES message are both fully compatible to the UN/CEFACT formats.

14 Used sources:

1. UNNext EBusiness Standard Handbook,
2. UN/CEFACT E-Cert presentation, Frans van Diepen, october 2015
3. Project Proposal Implementation Guide, september 2019
4. IPPC HUB Service API version 1.16 , Q3 release, oktober 2020
5. SPS E-Cert Background paper
6. Explanation of using the HUB and exchange between National Systems
7. UNECE BUSINESS REQUIREMENTS SPECIFICATION (BRS), Version: 5.1,Date of TBG approval: 2010/09/01
8. Streamlined presentation of UN/CEFACT standards (UNECE-site)
9. Handbook on Electronic Business Standards for Agricultural Trade Facilitation, V151030
10. UNECE Requirement Specification Mapping (RSM), version 1.4.1, September 2010
11. Guidelines for eCITES exchange, version 11, 21-07-2020
12. Draft WSDL Standard, author Lex Moret, 3 november 2015