ICC international computing centre

Service Requirements Specifications

IPPC ePhyto HUB

v2.2

Confidential - IPPC/FAO

31/03/2017

Table of Contents

Document Profile

Author:	ICC
Owner:	ICC
Client:	FAO/IPPC
Document Number:	

Document Location

This document is only valid on the day it was printed.

The source of the document is the IPPC Project Site (https://project.unicc.org).

Revision History

Date of next revision: N/A

Version:	Who:	What:	When:
Draft_v1	ICC	No changes. Release to IPPC	9-September -2016
2.0	ICC	Release to IPPC after PTC, Argentina meeting	14-Dec-2016
2.1	ICC	Updates after feedback	26-Jan-2017
2.2	ICC	Updates after PTC meeting in Geneva	22-Mar-2017
2.2	ICC	Document approved	31-Mar-17

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version
IPPC	SRS-ePhyto HUB_Draft_v1	8-September-2016	Draft v1
IPPC	SRS-ePhyto HUB_v2.0	14-Dec-16	v2.0
IPPC	SRS-ePhyto_HUB_v2.1	26-Jan-17	v2.1
IPPC	SRS-ePhyto_HUB_v2.2	31-Mar-17	v2.2

1. Introduction

1.1 Purpose

The purpose of this document is to formally specify the requirements for the development of the ePhyto HUB- a transfer service that will facilitate the communication and exchanges of ePhyto certificates between countries. The document will describe all the technical components of the HUB without going into the details of the applied ePhyto standards, agreements between countries, release and implementation details.

The HUB itself will be agnostic to the status and type of ePhyto sent through it. Countries can bi-laterally agree to exchange ePhyto certificates with status 'Approved' or 'Rejected'; if their national IT systems support processing of ePhyto with these statuses.

Further details of the ePhyto and the HUB can be found on the ePhyto Steering Group's website; located at https://www.ippc.int/en/ephyto/ephyto-steering-group/

1.2 Intended Audience and Reading Suggestions

This document will serve as an unambiguous and common understanding of the requirements for the ePhyto HUB, between the Project Technical Committee and the ICC; but also available for:

- Stakeholders
- System Business Analyst
- System Architect
- Quality Assurance Team
- Software Developers

It is strongly suggested to read documentation published under the FAO/IPPC ePhyto site https://www.ippc.int/en/ephyto/ see more on the reference section of this document.

1.3 References

A Global ePhyto Feasibility Study

ePhyto Hub - Frequently Asked Questions

Global ePhyto Solution

Codes And Schemas

ePhyto Certificates ISPM 12

2. Overall Description

2.1 Service Operation Requirements

ICC will build and operate the IPPC ePhyto HUB. This section lists some key operational requirements of the HUB; and the remainder of this document describes the technical requirements for building the service.

The ICC services for the ePhyto HUB should include:

a) 24/7 (round-the-clock) Service Desk to provide assistance in technical matters only. Specifics of how to access the Service Desk will be established during the project implementation.

b) NPPO On-boarding process: Upon request of the IPPC Secretariat, ICC will 'on-board' a NPPO to use the HUB. A detailed procedure will be established during project implementation. ICC will liaise with the NPPO nominated technical focal point for this process. Whilst ICC will not act as an 'Certificate Authority' to issue Transport Layer Security (TLS) certificates; it can assist NPPOs in obtaining such certificates from other Certificate Authorities (CA); as described in section 4.1, 4.2 and 5.5 below.

   During the on-boarding, NPPO will also choose between the PUSH or PULL methods for receiving the envelopes from the HUB.

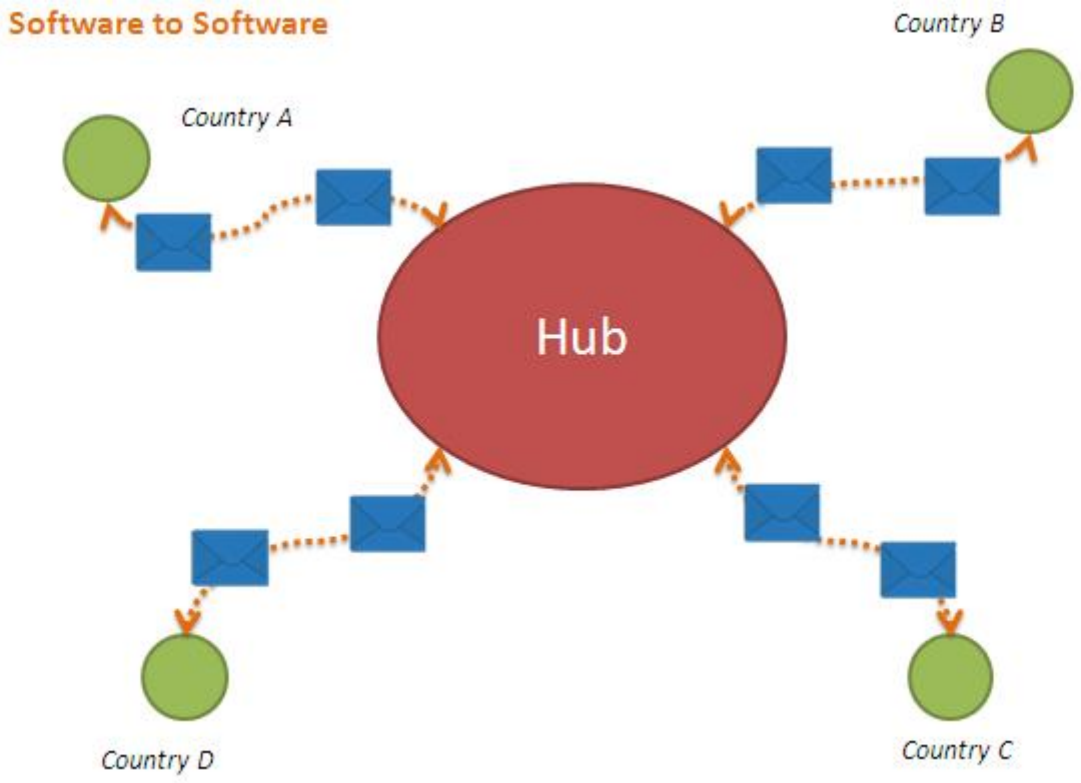
c) Service Level Agreements (SLAs): ICC will ensure that the HUB operates on agreed Service Levels and intervene as and when necessary to uphold these Service Levels. Some key SLAs have been identified in this document as 'Non-functional requirements'.

d) Operational Procedures: As part of the project implementation, ICC will work with the IPPC to establish operational procedures for change management, monitoring & reporting as well as incident & problem handling in line with industry best-practices conforming to ISO 20000 (commonly known as ITIL). Monthly reporting to IPPC on various service parameters will be part of these procedures.

e) Service Security: ICC will ensure security of the service during operations; more specifically on protecting the sensitive data contained within the transactional envelopes carrying the ePhyto Certificates.

2.2 Product Perspective

The product is a new messaging software component based on SOAP web services protocols that should provide delivery of ePhyto certificates across the globe, providing NPPOs the means to avoid establishing point-to-point communication and agreements with the associated technical issues that this could cause.



2.3 Product Functions

The following is a list of main modules and related functionalities needed by the HUB; these are further elaborated in Section 4: System Features.

Component	Use Case/Functionality	Description
TLS Certificate Services		Transport Layer Security (commonly referred to as SSL) provides functionalities for Authenticating and maintaining confidentiality of information exchanged with NPPOs.
	Client Authentication	The web service authenticates NPPO clients based on a TLS certificate
	Server Authentication	When a NPPO is configured as a 'PUSH' service, this authenticates the NPPO server based on a TLS certificate
	Error Handling	Invalid or expired certificates: Error message sent back to the *client* NPPO. In case of 'server authentication' failure, the connection is dropped. Log event in Audit Logs
HUB Web Service		SOAP Web service
	Receive Envelope(s)	Web Service Operation(s) to receive envelopes from exporting NPPO.

	Validate Envelope	Validation of envelope attributes including sender and receiver two letter country codes. Send Error message to exporting NPPOs in case of invalid envelopes.
	Store Envelope	Functional process to store validated messages pending delivery. Send Acknowledge messages to exporting NPPOs.
	Pull Envelope(s)	Web Service operation to receive a request from the importing NPPO for pulling envelopes
	Received Acknowledge	Web Service operation and related process to remove the pending envelope from the HUB on successful PUSH delivery.
	Error Handling	Attempt to PULL envelopes already under delivery: Respond back with error to importing NPPO client application, attempting a PULL operation. Any other error messages
	Delivery Failure	Queue Expiry Period: If delivery of envelopes is unsuccessful after a configured **number of days** (default:5 days); remove envelopes from the HUB and send email notification to both NPPOs. The threshold for delete on delivery failure should be configurable per NPPO
	Get Envelope Tracking Info	Web service operation that can be used by the client application of the exporting NPPO to verify the tracking info of a given envelope. The service will respond back with one of the following four messages: (1) PendingDelivery (2) Delivered (3) FailedDelivery (4) EnvelopeNotExists
HUB Delivery PUSH Orchestrator		Application component that sends envelopes pending delivery
	Process Pending delivery envelopes	The process that gathers envelopes ready to be sent to the importing NPPO
	Send Envelope	Connect to remote web service (authenticate the server) and send the envelope
	Received Acknowledge	Web Service operation and related process to remove the pending envelope from the HUB after a successful PUSH delivery

	Delivery Failure	Queue Expiry Period: If delivery of envelopes is unsuccessful after a configured **number of days** (default:5 days); remove envelopes from the HUB and send email notification to both NPPOs. The threshold (number of days) for delete on delivery failure should be configurable per exporting NPPO
HUB Internal Database		Store audit log entries to track and facilitate troubleshooting of the overall message delivery process
	Insert envelope pending delivery	Used by the Store Envelope process to store the message
	Get pending delivery envelope	Used by the HUB to retrieve messages to be delivered
	Lock the envelope	The envelope has been queued for delivery and waiting acknowledgement. The lock is a timestamp and will expire based on exporting NPPO expressed configuration or a default value.
	Delete envelope	Remove the stored envelope after confirmation of delivery or upon failure to deliver (end of lock period).
	Insert new log entry	Insert new log entry (internal troubleshooting)
	Insert new Transaction Log entry	Insert new transaction log entry (external with transaction details). This may be extended to support reporting and charging
	List transaction log entries	List transaction log entries based on a variety of parameters/filter
HUB Admin Interface		Application to manage the HUB configuration and operations. Only ICC operational personnel will have access to this interface. IPPC will be given ‘read-only’ access to view this.
	Configure new NPPO	This will allow administrators to configure the NPPOs, add the certificate enter the PUSH information and different thresholds (for the exporting NPPO); as well as administrative information such as NPPO contact information.
	View Audit Log	This will show administrators the audit log and search for events related to any NPPO and/or Certificate Number events. It will expose the capabilities to view logs across the entire system and not only limited a single NPPO.

HUB NPPO Interface		Application to view help & log information by NPPO.
	Help / client samples	Online help for the NPPOs containing technical information as well as sample code on creating ‘clients’ for connection.
	View and export transactional & audit logs	Each NPPO will be able to view (and export as CSV) logs for envelopes originating from or destined to their country. This will be a single account per NPPO without any hierarchy of users. The NPPO will be provided a username/password to access the service during the on-board process.

2.4 Design and Implementation Constraints

The following is the list of constraints

Description	**Rationale**
Each envelope will contain only one ePhyto certificate.	This will ease the technical operations of the HUB and NPPO client applications. It will also provide IPPC clear visibility into the volume of transactions.
Each envelope can only have one destination. In the scenario where the exporting NPPO has to send the same ePhyto to two or more countries (one final destination of consignment and others as in-transit countries); the exporting NPPO will put the same ePhyto in multiple envelopes and post each envelope separately to the HUB	This will ease the technical operations and prevent the HUB from parsing the ePhyto certificate itself.
Data sent to the HUB by any NPPO for transmission is very sensitive and must be adequately protected.	The data relates to trade between countries and is thus highly confidential for each country. The service should be built in a manner that it is completely transparent and highly secure to provide assurance to countries about correct handling of their data.
The reception of the message by the HUB and the delivery of the message to the destination is not synchronous	To make this synchronous the sender and the receiver must be permanently online and available posing limitations to the usage of the system.
The HUB must use TLS client certificates to authenticate NPPO clients & servers	This would be a secure choice for authenticating systems, looking at a single option of authentication.

Ensure sender and receiver identity.	For every interaction between the HUB and NPPO (send envelopes, PUSH or PULL envelopes), each entity must authenticate the other party with their TLS certificates. This will ensure that 3rd parties cannot impersonate either the sender or receiver.
The HUB service must record the incoming messages and transactions preventing any data loss	Once the ePhyto is received by the HUB, the message is stored on HUB database until it is received by the destination. Failures of the database should be recovered up to the last committed transaction.
The HUB functionalities must be implemented as a single SOAP web service	The data exchange communication protocol is standardized, though there is no limitation in the number of operations that can be implemented
The HUB web services must communicate in a secure manner.	The communication between the HUB and the connected client is encrypted. TLS provides confidentiality and integrity of the information exchanged.
The HUB service must be available as per the Availability Requirements defined later.	HUB Clients will connect at any time to send information, the HUB should be able to receive envelopes (and process other operations) without interruption.
The system should be implemented operating system that is : Trusted, Maintainable, Patched and Supported by the Vendor	The underlying platform, on top of which the HUB resides, should prevent security threats, ensure maintainability and support issues.
The HUB service should be implemented using a Messaging platform that can provide fundamental messaging processing functionalities	This will limit the implementation risks and provide out of the box options for enhancements.

2.5 User Documentation

The HUB service should be embraced and implemented by countries and their own software development agencies. Manuals of the HUB should be technically completed and up to date, with 100% coverage of all the usage scenario and possible alternative flows and issues.

The following products should be released:

- Manuals on implementing the client connector to the HUB and the testing environment details – available online as well as copies for download.
- Prototype of the client connector developed in C#, Java and Python. If the need arises, ICC will make efforts to provide client implementations in other languages.
- On-line help with knowledge base and FAQ in multiple languages. The Pilot implementation should be done in English; whilst the system should support multiple languages. As the documentation is translated into other languages; these should be uploaded into the HUB user support area.
- Detailed information on how to contact the ICC Service Desk for support.

2.6 Assumptions and Dependencies

No specific assumptions/dependencies are identified that are not covered by the above Design and Implementation constraints section.

3. External Interface Requirements

3.1 User Interfaces

User interfaces of the HUB system are only covering the administrative and user support areas, with the following functionalities:

- Administrative Area:
    - View to query the audit log of the system, identify errors in the communication and internal state changes
    - View to list all the configured NPPO, edit the configuration details
    - Window Form to configure NPPO with the below details
        - URL for push notification
        - Timeout/Counts of the PUSH delivery failures
        - NPPO Client Certificate
        - PUSH Server Certificate
        - Administrative details such as technical contact person name, phone number, email address.
- IPPC should have read-only access to the administrative interface; with the ability to export logs in CSV format.
- NPPO Area
    - All information from section 2.5: User Documentation
    - View for the NPPO to list and search for audit log history and export as CSV
    - View for the NPPO to list the transactions history with tracking info and export as CSV

The User interface should support multiple languages; giving the end-user an option to choose the language. The initial pilot implementation will be in English only; with other languages being added subsequently. IPPC will provide ICC with the translated copies of the documentation, user-interface menu options etc. The software should be designed so that these can be easily ingested.

3.2 Hardware Interfaces

No Hardware requirements are specified; the implementation of the HUB shall be free from hardware specification.

3.3 Software Interfaces

The HUB system should be implemented using platform operating systems that is: trusted, maintainable and vendor supported. This is to ensure that the underlying platform can secured against malicious attacks; and any issues can be resolved by the platform provider.

3.4 Communications Interfaces

The HUB will communicate using HTTPS/TLS and SOAP protocols, using client and server X.509 certificates to authenticate over secure channels.

This also applies to the importing NPPO exposing the PUSH web service to receive the ePhyto messages directly at their premises.

4. System Features

Note: System features listed in this document are given a unique identifier (example PIRQ-5 below in section 4.1.3). These identifiers correspond to entries in a separate ICC internal document: ‘Traceability Matrix’. ICC will use the Traceability Matrix to track service development during the project. The identifiers have been left in this document for linking the Requirements document to this Matrix. Please refer to

Appendix A: Glossary and Naming Convention for further details.

4.1 HUB Portal – NPPO Configuration & Admin Area

4.1.2 Description and Priority

The HUB will offer an administration console, used to configure NPPO connections by creating and modifying the configuration of:

- Client Certificates
- Optional PUSH URL end points and operations (this will exclude the PULL operation option)
- PUSH & PULL failures threshold
- Time between PUSH runs (default to every 2 hours)
- List of PUSH orchestration idle periods (the PUSH operation will not run during the defined windows, by default the PUSH will be idle out of defined working hours of the NPPO capital city office)
- NPPO email addresses to receive notifications and usage logs
- NPPO credentials for accessing the NPPO admin page

Assumption: The NPPO will obtain a Client Certificate from a recognized Certificate Authority of its choice and provide ICC the 'distinguished and common name' of the certificate.

NPPO will also receive a set of credentials, validated through a provided email, for NPPO administrators in order to access the Portal and download documents (e.g.: Client Samples, PUSH WSDL, notifications, testing instructions, etc.)

4.1.2 Stimulus/Response Sequences

The HUB administrators (ICC support team) will have access to the administration console over the web. The console will provide the administrators a view of the NPPO configuration. The administrator can view the list of configured NPPOs, create a new one or modify an existing record. The interface will not provide an audit of the changes; audit will be implemented natively on the selected storage (HUB DB).

The NPPO console will be securely accessible through the web but also to NPPO administrators, providing them information pertaining to their country only, as follows:

- Audit logs of accesses (also sent monthly via e-mail)
- Audit logs of NPPO related HUB activities
- NPPO export/import messages related transaction logs (also sent daily via email)
- NPPO export tracking info

4.1.3 Requirements

PDRQ-5: Maintenance Users and Service Technicians (UNICC) should be able to respond to users and customers reported incident or request for services without entering and manipulating the system.

PIRQ-6: The project should release a sample client in the most common programming languages (.net, java and python) to give practical examples to developers.

PIRQ-7: The project should release an administration tool that can be provided to 1st and 2nd support tiers in order to facilitate full-filling of services requests and troubleshooting.

NFRQ-49: The HUB Portal must be released with the option to be translated.

PCRQ-50: The HUB portal will be initially released in English.

4.2 TLS Services - Authentication

4.2.1 Description and Priority

Authentication between the NPPO Clients and the HUB is performed using X.509 based TLS Client and Server certificates. This is critical for the overall functioning of the System and has usages in the authentication of parties exchanging data as well as ensuring integrity of incoming messages. The TLS certificates will use 'strong ciphers' only (*current TLS v1.2*[1] at the time of writing this document).In response to evolving attack vectors, ICC will work with NPPOs to update the cryptographic algorithms used in TLS over the life of the service. **It is assumed that the national legal and regulatory framework of the NPPO interacting with the HUB allows the use of such ciphers.**

4.2.2 Stimulus/Response Sequences

The NPPO will connect to the HUB using TLS protocol and present its TLS client certificate, before any HUB operation can commence. The TLS client certificate has to be issued by any public Certification Authority (refer to security requirements for more details). Such a client certificate represents the identity of the NPPO that will be then authorized accordingly by the HUB.

In case of invalid, expired or revoked certificates, the NPPO will receive an error message on the 'application server' layer.

If the NPPO is configured to receive envelops via PUSH service, the HUB will authenticate the NPPO service using their server certificate. It is strongly advised that the NPPO also authenticates the HUB via the HUB's client certificate. In case of an invalid or expired NPPO server certificate, the application will record the event in the audit logs.

4.2.3 Requirements

NFRQ-28: Authentication of the client must be performed using client TLS Certificates

NFRQ-52: The authentication of client certificates must support a Certificate Revocation List[2]

4.3 HUB Web Service – Receive Envelope(s)

4.3.1 Description and Priority

Web service operation that receives an envelope from an exporter NPPO containing the envelope header with the following attributes; as well as **one ePhyto certificate (as per the IPPC ISPM 12 Schema)**:

- From (verified with the sender TLS certificate): ISO 3166-1 Alpha-2 Code of the exporting NPPO.[3]
- To: ISO 3166-1 Alpha-2 Code of the importing NPPO[4]
- Certificate Type: Number representing the Type of the ePhyto

Type Number	Type Value
851	Phyto
657	Re-Export Phyto

- Certificate Status: The Number representing the status of the ePhyto[5]-

[1] https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.2

[2] https://en.wikipedia.org/wiki/Revocation_list

[3] The compliance check to these rules will be done in the HUB application code and not in the HUB XML Schema. This will give the flexibility to extend the sender/receiver details.

[4] The compliance check to these rules will be done in the HUB application code and not in the HUB XML Schema. This will give the flexibility to extend the sender/receiver details.

Status Number	Status Value
70	Issued
39	Approved
40	Withdrawn
41	Rejected

- NPPO certificate Number: A mandatory text field for the exporting NPPO to insert the certificate number; limited to 60 characters.

- Content (ePhyto XML): One certificate per Envelope limited to 104 MB

4.3.2 Stimulus/Response Sequences

The exporting NPPO client application will connect, provide authenticate credentials (the TLS certificate) and send the envelope (header + content) to the HUB. The message can originate from any number of business events – e.g. Send ePhyto to importing country, withdraw or re-issue ePhyto. The HUB will not read the envelope content (ePhyto).

The HUB will authenticate the exporting NPPO client application and validate the header of the envelope; write the actions and errors in the audit log. It will assign a HUB Tracking Number and store the envelope for deliver to the importing NPPO. Finally, it will respond to the exporting NPPO with the HUB Tracking Number and enter the transactions log for the request of delivery.

If the envelops are invalid, the HUB will reject the message and respond to the importing NPPO with error details.

4.3.3 Requirements

NFRQ-13: The HUB functionalities must be implemented as single SOAP web service

PCRQ-18: The HUB service must record the incoming messages and transactions preventing any data loss

FCRQ-19: Communications between Client and HUB shall be atomic. Acknowledge of the receipt of a message is sent only when the message is correctly recorded

FCRQ-24: The HUB will log transactions and exchanges of messages to allow for any audit of the service by the connected parties

FCRQ-37: The HUB will not process the envelope content. The importing NPPO client application must be responsible of handling the ePhyto certificate.

FCRQ-38: The HUB must validate the envelope header and ensure compliance to business rules.

NFRQ-46: Each envelope will contain only one certificate

NFRQ-47: The envelope will contain only one destination country (single importing NPPO)

4.4 HUB Web Service – Pull Envelope(s)

4.4.1 Description and Priority

Web service operation that provides importing NPPO client application envelopes that are pending delivery:

- Destination NPPO (extracted from the client certificate): thus, will only deliver message that meet the client certificate NPPO.
- Filter Structure (optional – suggested functionality; not for first release of HUB):
    - From Date
    - To Date

[5] The certificate status in the header it is used only for reporting capability of the HUB, the status of the certificate is defined within the certificate contents, following the ISPM 12 and the related schema. The HUB does not read or retain that information as per security and data retention requirements as well as does not limit the usage of the field to above list

- Results Limit
- Sender NPPO

4.4.2 Stimulus/Response Sequences

The importing NPPO application will connect, authenticate and request envelops from the HUB.

The HUB will validate the request parameters and write the actions and errors in the audit log. Then the envelopes will be locked in the delivery queue until the importing NPPO acknowledges successful receipt. The HUB will send with all (zero or more) envelopes for the connecting NPPO. The HUB will send up to 50 envelopes per connection – to ensure delivery over slow connections. The number of envelopes that are sent in one session will be a configurable parameter and can be brought down to 1. This will allow the HUB transmission to be adjusted on a per NPPO basis.

Subsequent enhancement (future versions of HUB), this response can be a list of envelops (based on the filter structure), that the connecting NPPO can then selectively pull.

The importing NPPO client confirms the receipt of the envelopes by sending back (to a dedicated web service operation), the HUB Tracking number of each of the envelope received.

The HUB will delete the acknowledged envelope and insert transaction and audit log records.

If the connecting NPPO initiates a new PULL operation, while one PULL connection is ongoing, the HUB will send an error message indicating locked envelopes for transfer.

If 'new' envelopes have arrived in the interim (after the first PULL was initiated); the second PULL operation will initiate the delivery of 'new' envelopes.

In the event of a failed PULL, and when an envelope reaches the queue expiry time, the HUB will delete the envelope from the queue and update the logs. It will send an email to both the NPPOs involved about the failure. It will also update the status, which can be 'pulled' by the web service operation in section 4.5.

4.4.3 Requirements

FCRQ-19: Communications between Client and HUB shall be atomic. Acknowledge of the receipt of a message is sent only when the message is correctly recorded

FCRQ-24: The HUB will log transactions and exchanges of messages to allow for any audit of the service by the connected parties

FCRQ-31: NPPO client must be able to PULL incoming ePhytos from the HUB

FCRQ-33: The HUB will re-send envelopes with a PUSH or PULL process only if not already under delivery

FCRQ-37: The HUB will not process the envelope content. The importing NPPO client application must be responsible of handling the ePhyto certificate.

FCRQ-38: The HUB must validate the envelope header and ensure compliance to business rules.

FCRQ-42: The HUB will delete messages upon confirmation of receipt of the importing NPPO Client

4.5 HUB Web Service – Get Envelope Tracking status and Under Delivery Envelops

4.5.1 Description and Priority

<u>HUB Tracking Info Service</u>: This web service feature will provide the status of an envelope to the exporting NPPO. The NPPO provides an envelope tracking number. The HUB verifies that the tracking number belongs to the connecting NPPO. On successful check, the HUB responds back with the status to the enquiring NPPO. The status can by any one of the four:

(1) PendingDelivery: implies that the envelope is still held within the HUB and has not been delivered. Also, the queue expiry period is **<u>not</u>** over; thus, the HUB still has the envelope.

(2) Delivered: The envelope was successfully delivered by the HUB and has been deleted after delivery

(3) FailedDelivery: The HUB has not been able to deliver the envelope and the Queue expiry period set by the exporting NPPO was reached. Thus, the envelope was deleted from the HUB queue.

(4) EnvelopeNotExists: For the given Tracking Number, the HUB does not have any information. This may imply one of the two:

a) the tracking number supplied by the NPPO is incorrect

b) A major IT failure/disaster; where the HUB service was severely impacted- has led to data corruption. Thus, the HUB has does not have the envelope and the exporting NPPO has to resend/resubmit it. Please refer to the Availability requirements for the HUB in the non-functional section.

HUB Under Delivery Service: This web service will provide the exporting NPPO a list of all envelops with the PendingDelivery status.

4.5.2 Stimulus/Response Sequences

Envelope Tracking: The exporting NPPO's client application will connect and authenticate with the HUB and send a HUB Tracking Number request

The HUB will validate the client certificate and ensure that the Tracking Number belongs to the connecting NPPO; write the actions and errors in the audit log and reply with the related tracking info.

UnderDelivery: The exporting NPPO's application will connect and authenticate with the HUB and initiate the request to get under delivery envelops.

The HUB will validate the client certificate and ensure check the message queue for all envelopes from the exporting NPPO with the status 'PendingDelivery'. It will then respond back with the list of all envelops pending delivery.

4.5.3 Requirements

FCRQ-24: The HUB will log transactions and exchanges of messages to allow for any audit of the service by the connected parties

FCRQ-45: The exporting NPPO client application must be able to query the HUB to understand the state of envelopes

4.6 HUB Orchestrator – Push Envelope(s)

4.6.1 Description and Priority

For the importing NPPO, that opts to receive messages through PUSH service, the HUB will connect to a web service end point of the importing NPPO, following the configured PUSH schedule.

In order to receive messages in PUSH model from the HUB, the importing NPPO's web service should implement the provided WSDL, specifically the "Receive Envelope" operation.

In cases where the importing NPPO implements a web-service of their choice (i.e. not based on the HUB's standard WSDL); ICC will work along with IPPC to analyze the cost of custom implementation. IPPC may choose to pass the cost of this custom development to the NPPO.

4.6.2 Stimulus/Response Sequences

The HUB Orchestrator will check the configuration for each importing NPPO and try to send messages on the provided web service end point.

The Orchestrator will connect and authenticate the importing NPPO web service.

The HUB will try to send the messages. If the importing NPPO web service is not responding, the HUB will discard the PUSH action and log the failure.

The importing NPPO client confirms the receipt of the envelopes by sending back (to a dedicated web service operation) the HUB Tracking number of each envelope it has successfully received.

The HUB will delete the acknowledged envelope content and insert transaction and audit log records.

In the event of a delivery failure and when an envelope reaches the queue expiry time, the HUB will delete the envelope from the queue and update the logs. It will send an email to both the NPPOs involved about the failure. It will also update the status, which can be 'pulled' by the web service operation in section 4.5

4.6.3 Requirements

FCRQ-24: The HUB will log transactions and exchanges of messages to allow for any audit of the service by the connected parties

FCRQ-29: The HUB must be able to receive one e-Phyto in a single SOAP PUSH message

FCRQ-30: Importing NPPO client application must be able to receive ePhytos from the HUB on a dedicated service end point hosted in the NPPO infrastructure

FCRQ-33: The HUB will re-send envelopes with a PUSH or PULL process only if not already under delivery

FCRQ-34: The HUB PUSH tentative threshold must be configurable for each NPPO client

FCRQ-35: the HUB should report to HUB support operators any messages that have been waiting for delivery for a long time

FCRQ-37: The HUB will not process the envelope content. The importing NPPO client application must be responsible for handling the ePhyto certificate.

FCRQ-41: The HUB orchestrator will try to push messages with a configurable schedule for each NPPO, that can be changed based on operational needs

FCRQ-42: The HUB will delete messages upon confirmation of the receipt of the importing NPPO Client

NFRQ-43: A pre-defined WSDL should be followed by NPPO Clients implementing the receiving web service for PUSH operations. Customization of such sending operations may be done but with additional costs

4.7 HUB Portal – Troubleshooting console

4.7.1 Description and Priority

The HUB will offer an administration console used to search and view audit events for troubleshooting purposes.

The HUB administrator only will be able to enter the console and search the log to understand the state of a given messages or activity related to NPPO clients and period.

The console will offer two sets of logs:

Transaction logs: These log entries will record the following information:

(A) Sender NPPO

(B) Recipient NPPO

(C) HUB Tracking Status

(D) Certificate Type

(E) Certificate Status

(F) Exporting NPPO Certificate Number

(G) Timestamp for each entry

Audit Logs: These will cover all other information

(A) Events – example: NPPO user log-on, NPPO National system connection, envelope stored, envelope deleted.

(B) Errors- example: failed login attempts, invalid envelope

The troubleshooting console will not display details of the ePhyto certificate.

4.7.2 Stimulus/Response Sequences

An Administration console will be accessible through the web to HUB administrators and provide visualization of the information **without details of messages** that may be available but not delivered yet.

4.7.3 Requirements

PIRQ-7: The project should release an administration tool that can be provided to 1st and 2nd support tiers in order to facilitate full-filling of services requests and troubleshooting

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The HUB system will not have a direct impact on user operations (NPPO systems) as communication mechanisms are completely asynchronous. The HUB may be slower in processing when there might be a sudden increase of traffic, resulting in a slower delivery of messages to the destination NPPO. This will not result in any data loss.

Expected number of transactions: These numbers are indicative to design a system that can scale (both horizontally and vertically in ICT parlance). Depending on the adoption of the HUB, the necessary servers will be added by the ICC to scale up the service.

Pilot	Up to 10,000 ePhyto Certificates per month
From Go-live (BaU) to next 1 year	Up to 20,000 ePhyto Certificates per month
Next 2 years (Go-live+3 years)	Up to 150,000 ePhyto Certificates per month

The system shall be designed with scaling capabilities in order to reduce the effects of a high load on internal operations. Client's usage of the service may also have an impact on the system. As a target performance metric, not more than 2% of the overall traffic in a month should receive 'connection timeout' errors.

5.2 Availability Requirements

Recovery Time Objective (RTO)[6]: After a service disruption, maximum amount of time before the normal service operation is restored.

Recovery Point Objective (RPO)[7]: It is the point in time (before service outage) to which data sent to the HUB will be restored after a disruptive incident occurs. Any data sent after this point has the **potential** of being corrupted or lost. NPPOs will have to re-transmit ePhytos for this period (HUB's Tracking operation – status EnvelopeNotExists will give information on envelopes corrupted due to service disruption).

Target availabilities for unscheduled outages are:

Pilot	99%	*Max. 72 hours of downtime (in total) during one calendar year but no more than 12 hours of downtime (RTO) in one single instance of outage with 4 hours RPO*
From Go-live (BaU)	99.5%	*Max. 44 hours of downtime (in total) during one calendar year but no more than 6 hours (RTO) in one single instance of outage with 1 hour RPO*
Target: improvement over the life of service	99.99%	*Max 1 hour of downtime in one calendar year with zero RPO*

Monthly availability calculations:

(Hours in month – unscheduled hours unavailable) / (total hours in a month)

[6] https://en.wikipedia.org/wiki/Recovery_time_objective

[7] https://en.wikipedia.org/wiki/Recovery_point_objective

IPPC and ICC will work towards improving this metrics as part of regular service optimization.

Zero RPO is a reasonable target due to the functional design of the overall delivery process. Exporting NPPO client applications will have the option to check the delivery state of messages and re-send them in case the HUB was not able to restore the incoming message after the unavailability period.

5.3 Data Life-cycle Requirements

Data	On-line Store	Off-line Archive
Envelopes with ePhyto Certificates	Deleted upon delivery to importing NPPO. In event of non-delivery; deleted after default 'expiry time' or as set per NPPO.	Not Applicable.
Transaction Logs	Online (accessible to HUB administrators and NPPO): 1 year	Off-line (archive): 7 years
Audit Logs	Online (accessible to HUB administrators and NPPO): 1 year	Off-line (archive): 7 years

System Back-ups: For the purpose of meeting Service Availability metrics, ICC will maintain back-up copies of the live system and its data. This implies that all 'current' envelops residing in the system will get backed up. All backup shall be kept in ICC datacenters (under UN jurisdiction) and encrypted.

The backups will be kept for the duration listed below:

Backup schedule	Backup retention
Daily backups	1 week
Weekly backups	4 weeks

After the specified period, the envelope data will be deleted from the backup systems.

All backups will be stored encrypted and will follow the operational security requirements.

5.4 Safety Requirements

No safety requirements are identified that are not covered in the Security Requirements here below.

5.5 Security Requirements

The primary security constrain is that all NPPO data (ephyto certificates, information on destination country etc.) should be secure. To this end, the system will not keep any information longer than necessary (as described in the Data Lifecycle section of this document).

NPPO Data Security during processing: ICC will ensure that the HUB application, as part of processing the envelopes, handles all sensitive data to meet the primary security constrain; particularly the ePhyto certificate which is only held by the system for the purpose of delivery to destination NPPO and in accordance with the data lifecycle.

ICT operations access to the HUB: ICC will ensure that all access to the HUB system is adequately logged and monitored; including access at application developer/maintainer, Operating System, database and network levels. ICC will operate the service in compliance with internationally accepted security standard ISO 27001.

Trusted CA: The NPPO should get a client and/or server certificate from a trusted Certificate Authority. For the purpose of this project, any CA with its 'root certificate' in the 'root certificate store' of major browsers – Mozilla Firefox, Google Chrome, Microsoft or Apple Browsers[8] or desktop Operating Systems – MS Windows, Linux, Mac OSX; will be considered a Trusted CA. The system will also use Certificate Revocation List (CRL) provided by the different CAs in order to avoid using invalid certificates.

	Description	**Rationale**
NFRQ-14	The HUB web services must communicate using the HTTPS Protocol	The communication between the HUB and the connected client is encrypted. TLS provides privacy and integrity to the exchanged information
NFRQ-23	Information contained in the ePhyto is considered as restricted, only the destination NPPO can read the content	The HUB will only parse the envelope header. The HUB will not read the envelope content nor store it beyond the time necessary per data lifecycle.
NFRQ-28	Authentication of the client must be performed using client TLS Certificates	The certificate will be released by the HUB to the client, mutual TLS authentication can be used to secure the communication
NFRQ-45	The service should be given adequate security to protect it from being hacked or misused	Provide application level security: (*) Application code audit and use of application development best practices (prevent OWASP Top 10, SANS top 25 software errors) (*) Use of a Web Application firewall Provide Network level security: (*) Use of network level firewall and multi zone network. (*) Use of Intrusion detection system

[8] http://www.chromium.org/Home/chromium-security/root-ca-policy

		Provide server level security: (*) use of anti-malware tools on server (*) 'host hardening' of bastion servers Data Security: (*) Only very limited set of operational team will have capability to view data and applications. (*) Each access to system will be logged and an alert generated. The alert will be sent to the non-operational service manager.

5.6 Software Quality Attributes

	Description	Rationale
NFRQ-13	The HUB functionalities must be implemented as single SOAP web services	The data exchange communication protocol is standardized, though there is no limitation in the number of operations that can be implemented
NFRQ-15	The HUB service must be available as per the agreed availability requirements.	HUB Clients will connect at any time to send information, the HUB should be able to receive envelopes (and process other operations) without interruption.
NFRQ-19	Communications between Client and HUB shall be atomic. Acknowledgement of the receipt of a message is sent only when the message is correctly recorded	The overall delivery of the information is asynchronous and the HUB must take care of recording and keeping the information until it is delivered to the destination.
NFRQ-21	The HUB service must implement High Availability architecture	This will minimize the unavailability of the service for the connected clients

5.7 Business Rules

There are no business rules that are not covered in the Design & Implementation Constraints.

6. Other Requirements

	Description	Rationale
NFRQ-12	There must be a testing version of the system available to countries joining the HUB	Each country developing or adopting the HUB service will have a testing site and related configuration in order to design and test the changes
NFRQ-44	The project must release the WSDL that must be implemented at NPPO premises for the PUSH receiving web service end point	The HUB PUSH operation will be implemented using the provided WSDL and specifically implementing a receive operation that has the envelope schema matching the HUB incoming service.

Appendix A: Glossary and Naming Convention

WSDL: Web Service Definition Language
NPPO: National Plant Protection Organization

CA: Certificate Authority**-** An entity that issues digital certificates. This entity is itself trusted by both the NPPO and the ICC systems.

Code	Name	Description	Examples
FCRQ	Functional	The fundamental or essential subject matter of the product which are measured by concrete means like data values, decision-making logic and algorithms	The Scope of the Work The Scope of the Product Functional and Data Requirements
NFRQ	Non-Functional	Are the behavioral properties that the specified functions must have, such as performance, usability, etc. Non-functional requirements can be assigned a specific measurement.	Look and Feel Requirements Usability and Humanity Requirements Performance Requirements Operational Requirements Maintainability and Support Requirements Security Requirements Cultural and Political Requirements Legal Requirements
PCRQ	Project constraints	Identify how the eventual product must fit into the world. For example the product might have to interface with or use some existing hardware, software or business practice, or it might have to fit within a defined budget or be ready by a defined date	Mandated Constraints Naming Conventions and Definitions Relevant Facts and Assumptions
PDRQ	Project drivers	Are the business- related forces. For example the purpose of the project is a project driver, as are all of the stakeholders – each for different reasons	The Purpose of the Project Client, Customer and other Stakeholders Users of the Product
PIRQ	Project Issues	Define the conditions under which the project willbedone. Our reason for including these as part of the requirements is to present a coherent picture of all the factors that contribute to the success or failure of the project and to illustrate how managers can use requirements as input to managing a project	Open Issues Off-the-Shelf Solutions New Problems Tasks Cutover Risks Costs User Documentation and Training Waiting Room Ideas for Solutions