# Ontario EBT Hub to Hub Protocol

## Version 3.0

Published by:

Ontario EBT Working Group

January 10, 2005

# NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The information provided is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

While the information contained herein has been prepared from sources deemed to be reliable, The EBT Standards Working Group ("EBT WG"), operating under the auspices of the Ontario Energy Board ("OEB") or its successor organization reserves the right to revise the information without notice, but has no obligation to do so. Use of the information is at your discretion and THE OEB EBT WG MAKES NO REPRESENTATION OR WARRANTY THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION AND MAKES NO REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. IN NO EVENT SHALL THE OEB EBT WG OR ITS SUCCESSOR ORGANIZATION BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ANY AND ALL USE OF OR RELIANCE UPON SUCH INFORMATION, INCLUDING ANY SELECTION OF PRODUCTS OR VENDORS IS SOLELY YOUR RESPONSIBILITY AND YOU ASSUME ALL RISKS AND LIABILITIES, IF ANY, WITH RESPECT THERETO.

## Contents

## ~~1.~~6. Executive Summary

This document defines the Internet Data Transport protocol and rules for EBT transactions for the specific case where a hub communicates with a second hub as defined by the Ontario Energy Board's EBT Work Group for the deregulated Electric marketplace in Ontario, Canada.

## ~~2.~~6. Revision History

| Author | Version | Date | Description |
|---|---|---|---|
| J. Stewart | 0.9 | March 21, 2001 | Initial draft version |
| J. Cartwright | 0.91 | March 28, 2001 | Proposed revisions |
| J. Stewart | 0.92 | April 9, 2001 | Revisions per initial discussions |
| J. Stewart | 0.93 | April 18, 2001 | Revisions per April 17 meeting |
| J. Stewart | 0.94 | April 30, 2001 | Revisions per April 23 meeting |
| J. Stewart | 0.95 | May 8, 2001 | Revisions per May 4 meeting. Added appendix on certification testing. |
| J. Stewart | 0.96 | May 14, 2001 | Revisions per May 11 meeting. Added figure 1. |
| J. Stewart | 2.0 | August 3, 2001 | Reformat dates for 2.0 release |
| J. Stewart | 2.1 | December 12, 2001 | Updates for issue #595 |
| T. Stark | 2.2 Patch 1 | October 25, 2004 | Released as Version 2.2 Patch 1 with no changes |
| T. Stark | 3.0 | January 10, 2005 | Add Disclaimer Statement |

# 3. Introduction

This document defines the necessary protocol for data transport of Electronic Business Transactions (EBT) between EBT hubs.

This document assumes the reader is familiar with the Ontario EBT Specifications, the Ontario Transport Level Protocol, public key encryption and HTTP.

## ~~3.1~~4.0 *Scope*

**Formatted:** Bullets and Numbering

The EBT Hub to Hub Protocol defines the technical and functional standard for EBT messaging between hubs in the Ontario deregulated electric market. This includes Hub to Hub messages and the responsibilities of hubs in a multi-hub environment.

This document does not cover the messaging between a hub and its subscriber, or point-to-point connections directly between trading partners. This document does not cover the contents or format of PIPE Documents carrying consumer information.

The EBT Hub to Hub Protocol consists of the following parts:

- Transport Level protocol and connections;
- The delivery of Functional Acknowledgements;
- Time synchronisation and time stamping of transactions;
- Routing of subscriber messages;
- XML Parsers; and
- Hub Certification.

## ~~3.2~~5.0 *Definitions*

**Formatted:** Bullets and Numbering

This document uses the following definitions:

| | |
|---|---|
| **EBT Message** | A transport-protocol object that includes HTTP information and encapsulates one PIPE Document. |
| **EBT Document** | One XML instance document consisting of a PIPE Document, which in turn is made up of one or more EBT transactions. |
| **EBT Hub** | <To be defined> |
| **Hosting Hub** | The hub that directly connects to the originating Market Participant. |
| **Link** | A connection between one hub and another hub or between a hub and a Market Participant. |
| **PIPE** | Partner Interface Protocol for Energy. |

**Routing Hub** A hub that does not directly connect to the sending Market Participant, but is used by a Hosting Hub to direct an EBT Message to the target Market Participant. The target Market Participant connects directly to the Routing Hub.

**Spoke** A subscriber to a hub that exchanges EBT Messages with other Market Participants by connecting to its Hosting Hub and sending its messages to that hub.

## ~~3.3~~6.0 *References*

**Formatted:** Bullets and Numbering

For additional information, please see the following documents:

- "Ontario EBT Data Transport Protocol", Ontario EBT Working Group;
- "Ontario Electronic Business Transactions (EBT) Standards Document" (Business Rules Document), Ontario EBT Working Group.

**Formatted:** Bullets and Numbering

## ~~4.~~7. Transport Level Protocol

This section defines the transport level issues for Hub to Hub connections.

### ~~4.1~~8.0 *Basic Transport Level Protocol*

Formatted: Bullets and Numbering

The communication from one hub (the Hosting Hub) to another hub (the Routing Hub) extends the protocol as is used in Hub to Subscriber communications and Point-to-Point communications. This is the Ontario EBT Transport Protocol for:

- Security protocol;
- Message protocol;
- Delivery protocol; and
- Hub processing.

Formatted: Indent: Left: 18 pt, Bulleted + Level: 1 + Aligned at: 0 pt + Tab after: 18 pt + Indent at: 18 pt, Tabs: 36 pt, List tab + Not at 18 pt

A hub must have a unique identifier (the equivalent of an OEB License Number within the EBT Message standard) and a user_id and password for each hub in the market.

Note that the basic Transport Level Protocol is not end to end and therefore the EBT Message will be encrypted using a different key for each link between an originating Market Participant and the destination Market Participant. For example, an EBT Message travelling from an LDC to Hub1 to Hub2 to a Retailer would be encrypted three times. Once for the LDC to Hub1 link, once for the Hub1 to Hub2 link and once for the Hub2 to Retailer link.

### ~~4.2~~9.0 *Push vs. Pull*

Formatted: Bullets and Numbering

Each hub connects to every other hub and reads (pulls) transactions from them. A hub cannot write (push) a transaction to another hub. Each hub must maintain a ‘mailbox’ for EBT messages destined for every other hub. A hub will not place messages targeted for another hub into a mailbox on that hub. Instead, the other hub will connect and retrieve messages that it should process.

### ~~4.3~~10.0 *Frequency of Hub to Hub Connections*

Formatted: Bullets and Numbering

In order to expedite delivery of transactions, a hub must connect to all other hubs at least once every 15 minutes, unless the hub is unavailable due to scheduled maintenance (see section 7.2 Availability Requirements).

### ~~4.4~~11.0 *Store and Forward Storage Requirements*

Formatted: Bullets and Numbering

- In order to have space available to hold messages before other hubs have retrieved them, a hub will maintain sufficient online storage to ensure proper continued operation and unrestricted message transmission.

Formatted: Indent: Left: 18 pt, Bulleted + Level: 1 + Aligned at: 0 pt + Tab after: 18 pt + Indent at: 18 pt, Tabs: 36 pt, List tab + Not at 18 pt

Formatted: Bullets and Numbering

# ~~5.~~12. Functional Acknowledgements

This section describes the requirements for Functional Acknowledgements between hubs. Functional Acknowledgements are used to acknowledge the delivery of PIPE Documents. They identify invalid XML formatting of PIPE Documents and good and bad formatting of PIP transactions. A more complete description of Functional Acknowledgements can be found in the "Ontario Electronic Business Transactions (EBT) Standards Document" (Business Rules Document).

## ~~5.1~~13.0 *Operation of Functional Acknowledgements*

**Formatted:** Bullets and Numbering

The Hosting Hub will XML-validate each EBT Message that it receives from its subscribers. After checking for errors, the Hosting Hub will send a Functional Acknowledgement back to its subscriber as described in the "Ontario Electronic Business Transactions (EBT) Standards Document" (Business Rules Document).

Since it is assumed that the Hosting Hub has already XML-validated an EBT Message, the Routing Hub may, but is not required to, XML-validate these EBT Messages. In all cases the Routing Hub must however return a PIPEFunctionalAcknowledgement to the Hosting Hub to acknowledge receipt of the EBT Message. The Routing Hub may only send PartialFunctionalAcknowledgement if it has XML-validated the EBT Message.

The following lists the rules for a Routing Hub to send Functional Acknowledgements:

- If the Market Participant Recipient in the EBT document is a subscriber of the hub then the FunctionalAcknowledgement should be of type Accept.
- If the Recipient is not a subscriber then the FunctionalAcknowledgement should be of type DocReject.
- If the Routing Hub is sending a FunctionalAcknowledgement of type PartialAccept, it will only send along good transactions to the destination subscriber. The PartialAccept Functional Acknowledgement being returned will list which transactions were accepted, and forwarded, and which transactions were rejected.
- The Routing Hub may send a DocReject Functional Acknowledgement if it detects other errors within the EBT document.

The following lists the responsibilities of a Routing Hub when it sends Functional Acknowledgements:

- If Routing Hub returns a PIPEFunctionalAcknowledgement of type Accept to a Hosting Hub then the Routing Hub takes responsibility for delivery of the EBT Message to the destination Mailbox of the end subscriber.
- If the Routing Hub is unable to process the EBT Message by loading it into the destination Mailbox of the end subscriber, then it must report the problem back to the Hosting Hub. Since all hubs are validating based on public schemas at the OEB web site, this should only due to network failures. This reporting is to be done offline and not via the EBT system.

The following lists the responsibilities of the Hosting Hub when it receives Functional Acknowledgements:

- When the Hosting Hub receives a DocumentReject or PartialAccept Functional Acknowledgement, within four hours it will notify the Routing Hub and trigger a process to resolve the issue. This notification will be made via an automatically generated e-mail message. Best efforts should be made to resolve the issue within the four hours. This mechanism is identical to the situation where a subscriber reports a PartialAccept Functional Acknowledgement to the Hosting Hub.

**Formatted:** Bullets and Numbering

### ~~5.2~~14.0 *Availability Requirements*

For the purposes of dispute resolution, each hub must archive all EBT Messages it forwards and their corresponding Functional Acknowledgements to the same criteria specified in the Hub to Subscriber protocol.

**Formatted:** Bullets and Numbering

### ~~5.3~~15.0 *XML Parsers*

This section describes a hub’s requirements for XML Parsers.

In the strictest sense the issue of XML parsers is not really a Hub to Hub issue, but is beyond the scope of this document. However because hubs will do the majority of the XML validation and multiple hubs performing validation can create some issues, it does make sense to touch briefly on this issue.

Each party is free to select and use their own XML validating parser. If two parties disagree on the XML validity of a PIPE Document, final resolution will be determined by examination of the XML according to the schemas as published on the OEB web site. Validity will be determined using the current active specification of the XML Schema Definition Language as listed on the World Wide Web Consortium (W3C) web site.

**Formatted:** Bullets and Numbering

### ~~5.4~~16.0 *Detection of Other Errors*

Where the error reporting tools and mechanisms of the protocol (i.e., HTTPS responses and Functional Acknowledgements) do not provide a mechanism for communicating the type of error back to the sender, an e-mail message containing the error information will be automatically sent to the originator of the failing message. If there is no e-mail response, the issue is escalated via a telephone call to the operations staff of the originator of the transaction.

Such errors include:

- Decryption errors;
- Signature errors;
- Receipt of a Partial Functional Acknowledgement or Document Reject Functional Acknowledgement from a routing hub; and
- Lack of a Functional Acknowledgement from the recipient within the required four hours.

# ~~6.~~17. Time Synchronisation and Time Stamping

This section describes the hub requirements for time synchronisation and the time stamping of transactions. In a networked environment such as the EBT marketplace and since the arrival times for transactions are used for dispute resolution an accurate consistent time stamp is imperative.

**Formatted:** Bullets and Numbering

## ~~6.1~~18.0 *Time Synchronisation*

Each hub will maintain an accurate and consistent time by connecting through the NTP protocol to a service with an accuracy of at least that provided by a stratum-2 server[1]. There are various stratum-2 timeserver sources available, including free servers, subscription servers and potentially the IMO time-servers if they become accessible.

Since implementing the NTP protocol in a system requires only a piece of client software which is readily available for all major platforms, it will be possible for subscribers to hubs to synchronize in the same way, although this is not mandatory.

**Formatted:** Bullets and Numbering

## ~~6.2~~19.0 *Time Stamping of Transactions*

Each hub will date and time-stamp each EBT Document when it receives it. If the PIPE Document has been downloaded from another hub, the local hub will overwrite the previous HTTP time-stamp.

The hub should use Eastern Standard Time with no Daylight Savings Time change as specified in the “Ontario Electronic Business Transactions (EBT) Standards Document”

**Formatted:** Bullets and Numbering

[1] Stratum-1 servers connect to GPS or atomic clocks. Stratum-2 servers obtain their reference from stratum-1 servers. Startum-2 does not define an accuracy of the clock, but instead defines the number of hops to a source time-base. The resulting accuracy is dependent on the Internet and the number of routers between the various timeservers. By connecting to a stratum-2 timeserver, the hub becomes stratum-3. Stratum-3 timeservers are expected to have a short-term drift of less than 3.7 x $10^{-7}$ in 24 hours.

# ~~7.~~20. Routing of Subscriber Messages

This section describes a Hosting Hub's requirements for the routing of EBT messages to a Routing Hub. This occurs when a hub receives an EBT document from its subscriber, which is intended for a subscriber to a different hub. The lack of a centralised directory service forces the use of peer-to-peer communication of routing information. This includes the management of routing information and how to route EBT messages between hubs.

Hubs will not alter the structure of EBT Messages from subscribers (except to remove bad transactions from the message during the processing of PartialAccept Functional Acknowledgement transactions) by either:

- Combining EBT Message into a single message; or by
- Splitting EBT Messages into more than one message.

**Formatted:** Bullets and Numbering

## *~~7.1~~21.0 Connection Requirements*

The EBT System must operate as a single unit and it is not necessary for a Market Participant to be required to subscribe to more than one hub in order to do business in the Ontario market.

Because of this requirement, as soon as the market supports more than a single hub, all hubs are required to connect to every other hub. By doing this, a regular Market Participant, subscribing to a hub, need only connect to a single hub in order to send a message to any other Market Participant subscribed to a hub.

Each hub operator must provide adequate security access to all other hubs in the market through the use of a user_id and password as specified in the protocol for Hub to Subscriber communications.

**Formatted:** Bullets and Numbering

## *~~7.2~~22.0 Availability Requirements*

Because the routing of EBT messages by hubs is critical to the success of the marketplace and other hubs will be calling to retrieve messages, hubs must commit to remain online connected to the Internet with no more than 15 minutes of downtime per day.

A suggested maintenance window exists between midnight Saturdays (EST) and noon Sundays (EST) when hub servers can be shut down for longer periods.

**Formatted:** Bullets and Numbering

## *~~7.3~~23.0 Routing Information*

In order to route an EBT message to the correct hub, each hub must maintain routing information within their systems.

When a hub reads an EBT Document, it looks into the Market Participant directory within the EBT Document and routes the EBT message accordingly using routing information stored within its system. See the EBT Schema for more details on the Market Participant directory.

The routing information consists of the following information for each Market Participant in the Ontario retail electricity marketplace:

- OEBLicenseNumber: The OEB licence number for the Market Participant
- Hub: The hub identifier for the hub to which a Market Participant belongs (i.e., the identifier for the Hosting Hub for the subscriber).
- Status: The status of the participant indicating whether, or not, a Market Participant is in good standing and can receive EBT Messages.

**Formatted:** Bullets and Numbering

### ~~7.~~424.0 *Routing Information Messages*

In order to stay as close as possible to the Spoke to Hub protocol, routing information will be handled by extending that protocol to include an HTTP Request Type specifically for hub to hub communication. A subscriber never submits this request.

Section 6.2.4 of the Spoke to Hub protocol will be used with the addition of type ‘RouteInfo’ as shown below in section 7.4.1. The extended schema for this transaction is listed in Appendix C – “Hub Response XML Schema”.

**Formatted:** Bullets and Numbering

#### ~~7.4.1~~25.0.0 request_type

```
Content-Disposition: form-data; name=”request_type”
Request
```

Where request is a string and may only be:

- Upload
- Download
- Directory
- RouteInfo

A hub will respond similarly to the directory request defined in the Spoke to Hub Protocol, with a message body consisting of XML presenting the Routing Information based on the response schema – “response.xsd”. (This is the same schema as used in spoke to hub communications. The version to be used must be equal to, or better than, version v2.0.)

The Routing Information Response XML includes the following information:

- The Name and ID of the hub sending the response
- The License number and Status information for each subscriber to the given hub.

The following rules apply to the RouteInfo request:

- A hub must request Routing Information from every other hub at least once every 24 hours.
- A hub must update its internal routing information within eight hours of receiving notice of a change from one of its own subscribers.

- When a hub retrieves the routing information it will match the Market Participants in its system routing information with those of the incoming routing information and update the local system routing information where applicable.

For the format of a Routing Information HTTP Request, see Appendix A—"HTTP Request". For the format of a Routing Information successful HTTP Response see Appendix B—"HTTP Response".

**Formatted:** Bullets and Numbering

## ~~8.~~26. Hub Certification

This section defines the requirements for certification of new hubs. More details are provided in Appendix C—Hub Certification Testing.

The OEB will maintain a list of hub names for hubs that have been certified.

In order to become certified a new hub must pass a connectivity and protocol adherence test with each hub. The hubs will define a certification test to exercise the Hub to Hub and Transport Level Protocols. A new hub has been certified when it has passed the connectivity and protocol tests with each other certified hub.

When a hub is certified to participate in the market it will need to publish access information available to every other hub. A at minimum, access information will include the URL for the hub, the name of the hub and the identifier for the hub. The hub identifier is being used as the equivalent to the OEB licence number for the purposes of the protocol. Each hub will need to store this information within their system and to issue a user_id and password for the new hub to access their mailbox.

Since certification of a hub implies that the hub follows and promotes the EBT Standard, Hub Certification Testing will also include some aspects of the subscriber to hub standard as well. To perform these tests, the certifying hub will connect to the hub being certified and act in a fashion similar to a subscriber.

# Appendix A -- HTTP Request

The following is an example of a Hub to Hub HTTP Request:

```
POST /RecipientServer/mailbox HTTP/1.1
Date: Tue, 20 Dec 2000 08:12:31 GMT
Connection: Keep-Alive
Host: www.ontarioRecipientServer.com
Content-Language: en, fr
Content-Type: multipart/form-data; boundary=EBTpart;
Content-Length: 3222

--EBTpart
Content-Disposition: form-data; name=”sender”
12345678

--EBTpart
Content-Disposition: form-data; name=”user_id”
aUser

--EBTpart
Content-Disposition: form-data; name=”user_password”
aPassword

--EBTpart
Content-Disposition: form-data; name=”request_type”
RouteInfo
--EBTpart--
```

## Appendix B -- HTTP Response

The following is an example of a Hub to Hub HTTP Response:

```
HTTP/1.1 200 OK
Date: Tue, 20 Dec 2000 08:12:31 GMT
Host: www.ontarioRecipientServer.com
Content-Type: text/XML
Content Length: 1234

<?xml version="1.0" encoding="UTF-8"?>
<RESPONSE xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="
http://www.ontariohub.com/Response.xsd ">
  <HTTP_RESPONSE>
         <STATUS_CODE>200</STATUS_CODE>
         <REASON_PHRASE>OK</REASON_PHRASE>
         <REQUEST_TYPE>RouteInfo</REQUEST_TYPE>
         <TIMESTAMP>Tue, 10 Apr 2001 08:12:31 GMT</TIMESTAMP>
  </HTTP_RESPONSE>
  <ROUTEINFO>
         <HUB name="OntarioHub" identifier="HubONT"/>
         <SUBSCRIBER oeblicense="12345678" status="good"/>
         <SUBSCRIBER oeblicense="87654321" status="suspended"/>
  </ROUTEINFO>
</RESPONSE>
```

# Appendix C – Hub Certification Testing

This appendix describes the details of a single Hub Certification test made by one hub (the certifying hub) to test another hub (the hub under test).

## Background

Before being certified for operation in the Ontario electricity EBT marketplace, a potential Hub must successfully complete a Certification Test executed by each of the existing hubs. The OEB will notify the existing certified hubs when all certified hubs have tested the new hub. At this point the new hub will be deemed 'certified'.

Because initially no hubs exist, the certification process requires a step to launch the process and get it started. Whenever there are no hubs that are certified, the first two hubs to report to the OEB that they are ready for certification testing, and have submitted any required documentation to the OEB, will be deemed logically certified for testing purposes only. These two hubs can perform certification tests only and cannot call themselves completely certified until they have finished certification testing in the same manner as any potential hub.

If there are more than two hubs ready to do the initial certification, the hubs will perform the certification testing by initiating their testing in pairs. For example if three hubs are ready at the same time hub number one would test with hub number two and hub number one would also test with hub three. After the completion of the first round of testing, hub number two would test with hub number three.

In the unlikely event that only one hub is ready for certification testing, and no other hubs are ready, for a period of more than three months, a hub can be self-certified by successfully demonstrating that it has completing subscriber certification tests with at least two of its subscribers. New hubs must then perform certification testing with the self-certified hub in the normal manner.

## Certification Test

While each hub will develop its own complete set of tests, these tests will follow a standard structure and format. With the exception of reasonable improvements to catch problems found though experience or required for special configurations, a hub will use a consistent set of tests for all hubs that it certifies. In this context, consistent is with respect to number of scenarios, number of steps in the scenarios and objectives for the tests. The order of the scenarios and the details within the steps can be altered to introduce randomness to the test. The intent is that no one hub can be constrained from being certified by an inordinately long or difficult test. At the same time, the process must provide a high standard of quality and allow continuous improvement of the test to incorporate lessons learned during operation.

Hub certification tests will be based on the most current EBT standards. This includes the EBT Standards Document (Business Rules), the EBT schema and Implementation Guides, the Hub to Spoke Transport Protocol and the Hub-to-Hub Transport Protocol.

The certification test must include the testing of all documents that are defined in the EBT transaction set. This includes both accept and reject transactions. In order to ensure repeatability, accuracy and to simulate reasonable volumes, the transactions must not be manually generated. The hub performing the test will have timelines associated with when it expects the corresponding responses.

The Hub certification process will be monitored and assessed by an independent third party. Since each certifying hub is responsible for performing the tests and examining the results, this monitoring is more of a process to ensure that all documentation is collected and completed correctly. This includes any applications documents made by the hub under test and any results submissions made by the certifying hub.

In order to assist with the co-ordination of testing schedules between hubs, a run of certification testing will only begin on the first business day of a month.

Since the hub certification process will be a time consuming process, hubs should reach a mutually agreeable set of hours of operation. For example, if a response is required within four hours, perhaps the hours of operation should be set as between 8:00am and 8:00pm so as not to overburden the hubs with round the clock coverage during the tests.

Additionally, it is not the responsibility of the certifying hub to assist the hub under test in 'debugging' their code. At the same time, a reasonable amount of result data must be presented to the hub under test. When a test fails, the certifying hub may oblige the hub under test by continuing the test. Alternatively, the certifying hub may elect to deem the test as concluded and re-schedule the test at a later date after the hub under test has done more testing on its own.

The certification test is not deemed as a pass until the hub under test completes the entire suite of tests without incident on the same version of software.

### Certification Test Process

Each certification test has a certifying hub and a hub to be certified. (Initially before any hubs are certified, each hub will have to play both roles—one set of tests to certify itself and one set of tests to certify the hub it connects to.)

Hub Certification testing consists of the following steps:

1. The hub to be certified submits the documents to apply for a certification test (see figures 1 and 2) to both the OEB and the hub that will perform the certification. The Application for Certification document consists of the necessary due diligence to demonstrate that the potential hub meets all configuration and planning requirements as set out in the definition of a hub. This application will include items such as backup site and redundant system documentation, primary contact phone number, Help Desk phone number, name and phone number for the

certification test contact, etc. This document will be publicly available for all parties, including the certifying hub, subscribers and potential subscribers.

~~2.~~0.The hub under test will schedule test time with the certifying hub and respond with its contact information. (See figure 3 for a

~~3.~~0.The hub under test and the certifying hub will exchange configuration information including keys and URLs.

~~4.~~0.A transport level test will be performed for loading and unloading the mailboxes. This is a group of standard mailbox commands, each of which is expected to produce normal working results without causing transport level errors. For a description of the minimal set of these tests, see table 1. A hub may add to this set of tests to increase test coverage.

~~5.~~0.A transaction format test for transaction type will be performed to ensure each specific transaction type is working correctly. This is a group of working transactions, approximately three transactions of each type each of which is expected to produce normal results (i.e., all transactions are well formed) without causing Functional Acknowledge level errors.

~~6.~~0.An error generating set of transport level tests will be performed. This set will test the robustness of the transport level of the hub under test. The certifying hub will generate errors on purpose with the explicit intent of testing the recovery process of the hub under test.

~~7.~~0.An error generating set of transaction format test for each transaction type will be performed. This set of tests will stress the XML parser by generating formatting errors on purpose. For a sample of these tests, see table 2.

~~8.~~0.An analysis by the certifying hub to ensure that the hub under test is meeting performance standards, such as accessing the certifying hub's mailbox at least once every 15 minutes.

~~9.~~0.A subscriber simulation test where the certifying hub acts as a subscriber where it uploads and downloads and downloads documents as would a subscriber. This test is to ensure that all hubs communicate with their subscribers according to the same standard.

~~10.~~0. The hub performing the test submits the results to both the hub-under-test and the OEB.

The transport level tests include:

- Basic connection tests;
- PKI tests;
- HTTPS tests;
- Mailbox command tests; and
- Routing Table tests.

Transaction level tests include:

- Transaction requests;
- Transaction accepts;
- Transaction rejects; and
- XML formatting errors.

The test is made of sets of scenarios. Each scenario will roughly follow these steps:

~~1.~~0. The hub to be certified will set its configuration to a known state as specified by the certifying hub.

~~2.~~0. The certifying hub will load its mailbox with transactions for the hub to be certified.

~~3.~~0. The hub to be certified will connect to the certifying hub and pick up the transactions. (This tests the ability of the hub to be certified to retrieve transactions.)

~~4.~~0. The hub to-be-certified will XML validate the transactions that it retrieved. (This tests the XML parser on the hub to be certified.)

~~5.~~0. The hub to be certified will generate appropriate Functional Acknowledgements for the transactions it XML validated. (This tests the ability of the hub to be certified to create Functional Acknowledgements.)

~~6.~~0. The hub to be certified will deposit the Functional Acknowledgements that it created in its mailbox for pick-up by the certifying hub.

~~7.~~0. The certifying hub will retrieve the Functional Acknowledgements. (This tests the ability of the hub under test to manage the server side of the mailbox.)

~~8.~~0. The certifying hub will compare the Functional Acknowledgements it retrieved against what it expected. (This tests the complete message path through the hub under test.)

The certifying hub will make available a set of timelines for the above steps to allow the test to be tracked, to allow time out errors to be detected and to arrange for appropriate staff to be available.

### Test Configuration

In order to facilitate testing the following standard configuration will be set up:

- Each hub will define, and configure, a standard test retailer and a standard test distributor. Any transactions sent to these market participants will be discarded after Functional Acknowledgement processing has taken place. This configuration includes both mailboxes and routing table entries.
- Prior to being certified, each hub to be certified will use its production environment for hub certification testing. After certification, a functionally equivalent environment will be used for hub certification testing of new hubs.

Table 1.) Hub to Hub protocol tests

| **Request Type** | **Description** | **HTTP Code** | **Response Body Contents** |
|---|---|---|---|
| Valid Directory request | Post a Directory request with all fields valid | 200 OK response | Response XML with Directory element. |
| Valid Download request | Post a Download request with all fields valid | 200 OK response | Valid document. |
| Valid Upload request | Post an Upload request with all fields valid | 200 OK response | Response XML with Upload element. |
| Valid RouteInfo request | Post a RouteInfo request with all fields valid | 200 OK response | Response XML with RouteInfo element. |
| Invalid Directory request – invalid sender | Post a Directory request with an unknown sender and all other fields valid | 403 Bad_Request | Response XML. |
| Invalid Directory request – invalid user_id | Post a Directory request with an incorrect sender and all other fields valid | 403 Bad_Request | Response XML. |
| Invalid Directory request – invalid password | Post a Directory request with an incorrect password and all other fields valid | 403 Bad_Request | Response XML. |
| Invalid Download request – invalid doc_id | Post a Download request with an unknown doc_id and all other fields valid | 400 Bad_Request | Response XML. |
| Invalid Upload request – unencrypted document | Post an Upload request to a plaintext document and all other fields valid | 400 Bad_Request | Response XML. |
| Invalid Upload request – invalid URI | Post an Upload request to an incorrect URI at a hub and all other fields valid | 404 Not_Found | Response XML. |
| Invalid request – invalid request_type | Post a request where the request_type is not Upload, Download, Directory or RouteInfo | 400 Bad_Request | Response XML. |
| Invalid request – invalid http method | Submit a request where the method is not a Post | 501 Method_Not_Implemented | Response XML. |
| Invalid request – invalid http version | Post a request where the HTTP header is not version 1.1 | 505 Version_Not_Supported | Response XML. |
| Invalid request – time out request | Establish a connection and allow the time-out period to expire before submitting a request | 408 Request_Time_Out | Response XML. |
| Invalid XML form – XML cannot be validated against Schema- | Post an HTTPS upload request containing an Enrolment request. The request is well formed, but cannot be XML validated. | 200 OK response | Response XML with Upload element. A DocReject FA is queued for delivery on the next download. |

| Request Type | Description | HTTP Code | Response Body Contents |
|---|---|---|---|
| Invalid XML data – XML contains an invalid recipient | Post an HTTPS upload request with a bad recipient in an Enrolment request | 200 OK response | Response XML with Upload element. A DocReject FA is queued for delivery on the next download. |
| Invalid XML data – XML contains an invalid sender | Post an HTTPS upload request with a bad sender in an Enrolment request. | 200 OK response | Response XML with Upload element. A DocReject FA is queued for delivery on the next download. |

Table 2.) Hub to Hub transaction format error tests

| Request Type | Description | Error Response | Response Body Contents |
|---|---|---|---|
| Invalid XML data – XML data is not well formed | Post an HTTPS upload request with badly formed data in an Enrolment request. | Email response to certifying hub administrator. | Response XML with Upload element. |
| Invalid Encryption – Digital Signature cannot be verified | Post an HTTP upload request with a bad digital signature attached to an Enrolment request. The method of generating the bad signature is not important, just that the signature cannot be verified. | Email response to certifying hub administrator. | Response XML with Upload element. |
| Invalid Encryption – Generic Unable to Decrypt | Post an HTTPS upload request with a corrupt or incorrectly encrypted file containing an Enrolment request. The method of generating the corrupted, encrypted data is not important, just that the data cannot be decrypted. | Email response to certifying hub administrator. | Response XML with Upload element. |

figure 1. General Information Form V0.1

| Item | Data |
|---|---|
| HUB ID  o/a | |
| OEB listed ID Number | |
| Hub Address (URL) | |
| Phone Number | |
| Mailing Address | |
| Contact email | |
| Testing Contact | |

figure 2. HUB to HUB - Request for Test V0.1

| **Test Definition** | | |
|---|---|---|
| Item | Description | Verified |
| Test ID | | |
| Test Explanation | | |
| Expected Result | | |

| **Requesting Hub** | | |
|---|---|---|
| Item | Description | Verified |
| HUB ID  o/a | | |
| Hub Address | | |
| Contact | | |

| **Security** | | |
|---|---|---|
| Item | Description | Verified |
| Security Considerations | | |
| Supplied Information. | | |
| Requested Information | | |

| **Schedule** | | |
|---|---|---|
| Item | Description | Verified |
| Requested Schedule | | |

figure 3. HUB to HUB – Response to Request for Test V0.1

| Test Identification | | |
|---|---|---|
| Item | Description | Verified |
| Test ID (From: Request for Test) | | |
| Requesting Hub ID o/a | | |
| Request Accept / Reject | | |
| Issues / Concerns | | |

| Responding Hub | | |
|---|---|---|
| Item | Description | Verified |
| HUB ID o/a | | |
| Hub Address | | |
| Contact | | |

| Security | | |
|---|---|---|
| Item | Description | Verified |
| Requested Information | | |

| Schedule | | |
|---|---|---|
| Item | Description | Verified |
| Response to Requested Schedule | | |