# Test Criteria: 170.315.h.2 – Direct Project, Edge Protocol, XDR/XDM

|  |  |
| --- | --- |
| **Testing Result** |  |
| Participant and Product-with-version |  |
| Setting (Ambulatory or Inpatient) |  |
| Test Proctor |  |
| Test Date |  |
| Test Result | Pass:  Fail:  No Attempt: |
| Error Description (if applicable) |  |
| Modifications to Product Under Test |  |
| Additional Software Used |  |
| Additional Proctor Notes |  |

### Overview

In this document you will find:

* [Test Data and Test Tools](#_Test_Data_and)
* [Standards Support](#_Demonstrate_Standards_Support)
* [Drummond Test Report (Instructions, Expected Results, Points to Remember)](#_170.315(h)(2)(i)(A)_Applicability_S)
* [Test Procedures](#_Test_Procedures)
* [Appendix A: Testing Guide](#_Appendix_A:_Testing)
* [Appendix B: ONC Criteria](#_Appendix_B:_ONC)
* [Appendix C: Attestation Template](#_Appendix_C:_170.315(h)(2))

### Version of ONC Test Method

1.5

### Scope of Proctoring Sheet

The ONC test method associated with this criterion is the only approved test method for technology Meaningful Use certification. This Proctoring Sheet is not a replacement test method but a test procedure document for performing the ONC test method and recording the results. Proctoring Sheet describe test data, test criteria and expected results. It is assumed the Health IT developer or Participant under Test is familiar with the associated ONC test method.

# Robustness and Reliability Requirement

To satisfy the module criteria, it is expected that the Product-Under-Test is able to complete the testing requirements reliably, including repeat testing with the same result without error, and with a satisfactory level of robustness. This includes unexpected error messages produced through normal operation, multiple unintended restarts of the application or any other “buggy” facets of the product displayed while testing. These errors are record in the Additional Proctor Notes of the proctor sheet. Lack of reliability and robustness of design will result in failure of the module.

# Test Data and Tools

|  |  |
| --- | --- |
| **Test Data Source:** | ONC-Supplied  DG-Supplied:  Developer-Supplied: |
| **Pre-Test Data Setup:**  Health IT developer downloads:   * DCDT Discovery Test Trust Anchor and configures in their Direct instance * ETT Direct Testing ETT Trust Anchor and configures in their Direct system trust store * ETT Direct Testing ETT Public Cert and configures in their Direct system trust store   Health IT developer provides:   * Attestation letter to Test Proctor prior to test event (see [Appendix C](#_Appendix_C:_170.315(h)(2):) for template). * Endpoints to be used for sending/receiving with the Edge Test Tool (ETT). | |
| **Test Data:**  ONC-Supplied test data supplied in test tools or health IT developer may opt to use own C-CDA for use in the “Send” test. If supplying own data, notify Test Proctor before test event. | |
| **Test Tools:**   * [2015 Edition Direct Certificate Discovery Tool (DCDT)](https://ttpedge.sitenv.org/ttp/#/direct/certdiscovery/dcdt2) * [Edge Testing Tool (ETT)](https://ttpedge.sitenv.org/ttp/#/home) | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Implement standards to demonstrate compliance to the Direct Project, Edge Protocol, and XDR-XDM. | |

|  |  |  |
| --- | --- | --- |
|  | **Standard** |  |
|  | §170.202(a)(2) | [Applicability Statement for Secure Health Transport, Version 1.2, August 2015](http://wiki.directproject.org/file/view/Applicability+Statement+for+Secure+Health+Transport+v1.2.pdf) |
|  | §170.202(b) | [ONC XDR and XDM for Direct Messaging Specification](http://healthit.gov/policy-researchers-implementers/direct-project) |
|  | §170.202(d) | [ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014](http://www.healthit.gov/sites/default/files/implementationguidefordirectedgeprotocolsv1_1.pdf) |
|  | §170.202(e)(1**)** | [Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012](http://wiki.directproject.org/file/view/Implementation+Guide+for+Delivery+Notification+in+Direct+v1.0.pdf) |

# 170.315(h)(2)(i)(A) Applicability Statement for Secure Health Transport (Direct) - Send

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**  Health IT developer:   * Downloads the DCDT Discovery test Trust Anchor and configures in their Direct instance. * Sends Direct message per instructions of each DCDT test case (refer to DCDT test tool) to show that the HIT module can properly discover hosted certificates. * Sends a CCDA payload via a Direct “wrapped” message to the appropriate ETT Direct Testing tool email address. | |
| **Expected Test Result:**   * Using the DCDT, Test Proctor inspects the validation report results received via email and system logs to verify that all test cases for discovery of certificates hosted in DNS and LDAP were successful. * Health IT module Direct email address can be registered in the ETT Direct Testing tool. * After properly setting up ETT Direct Testing registration, Test Proctor verifies ETT can successfully decrypt and validate received Direct message from the HIT module. * Health IT module successfully sends encrypted and signed health information to three partner HISPs using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport. The verification includes:   + Indication through documentation that the HIT module sent “Wrapped” RFC-5751 messages   + Indication through documentation that the HIT module receiving processed Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated upon receiving the Direct message from the HIT module. | |
| **Points to Remember:**   * For this criterion, it is required to send messages in only “wrapped” format even though the specification allows use of “unwrapped” messages. * (h.2) attestation template provided in [Appendix C](#_Appendix_C:_170.315(h)(2):). | |

### Test Procedures

### 1.1 Discover Certificates: Positive Test Cases [(h)(2)(i)(A) – Send 1-2]

DCDT: <https://ttpedge.sitenv.org/ttp/#/direct/certdiscovery/dcdt2>

|  |  |
| --- | --- |
|  | User downloads the DCDT Trust Anchor and upload into the HIT module’s Direct trust store. |
|  | Using the DCDT, Proctor register the Health IT developer’s Direct email address and map it to Proctor’s non-direct email address.  **Direct From email address**: <type here> |
|  | DCDT positive test cases: Health IT developer uses the HIT module functionality to send a direct message to each test case Direct To email address. Record results below. |

<INSERT SCREEN SHOTS or LOG FILE – Direct Certificate Discovery Tool discovery of EHR certificates>

* D1 – Valid address-bound certificate discovery in DNS
* D2 – Valid domain-bound certificate discovery in DNS
* D3 – Valid address-bound certificate discovery in LDAP
* D4 – Valid domain-bound certificate discovery in LDAP
* D9 – Select valid address-bound certificates over invalid certificate in DNS
* D10 – Certificate discovery in LDAP with one unavailable LDAP server
* D14 – Discovery of certificate large than 512 bytes in DNS
* D15 – Certificate discovery in LDAP based on SRV priority value
* D16 – Certificate discovery in LDAP based on SRV weight value
* D17 – CRL-based revocation checking for address-bound cert discovery in DNS
* D18 – AIA-based intermediate issuer cert retrieval for address-bound cert discovery in DNS

### 1.2 Discover Certificates: Negative Test Cases [(h)(2)(i)(A) – Send 1-2]

DCDT: <https://ttpedge.sitenv.org/ttp/#/direct/certdiscovery/dcdt2>

|  |  |
| --- | --- |
|  | DCDT negative test cases: Health IT developer uses the HIT module functionality to send a direct message to each test case Direct To email address. Record results below. |
|  | Proctor verifies HIT module does NOT send email because a certificate in Direct Certificate Discovery Tool discovery test was correctly not found. |

<INSERT SCREEN SHOTS or LOG FILE – Direct Certificate Discovery Tool discovery of EHR certificates>

* D5 – Invalid address-bound certificate discovery in DNS
* D6 – Invalid domain-bound certificate discovery in DNS
* D7 – Invalid address-bound certificate discovery in LDAP
* D8 – Invalid domain-bound certificate discovery in LDAP
* D11– No certificates discovered in DNS CERT records and no SRV records
* D12 – No certificates found in DNS CERT records and no available LDAP servers
* D13 – No certificates discovered in DNS CERT records or LDAP servers

### 1.3 Register Direct Address [(h)(2)(i)(A) – Send 2]

ETT – DIRECT <https://ttpedge.sitenv.org/ttp/#/direct/register>

### 1.4 Send Health Information Using Direct [(h)(2)(i)(A) – Send 3-5]

ETT – DIRECT [https://ttpedge.sitenv.org/ttp/#/direct](https://ttpedge.sitenv.org/ttp/#/direct/register)

|  |  |
| --- | --- |
|  | Using the ETT Register Direct functionality, Proctor register the Health IT developer’s Direct From email address and map it to a non-direct email address.    **Direct From email address:** <type here> |

<INSERT SCREEN SHOTS>

|  |  |
| --- | --- |
|  | Health IT developer uses HIT Module functionality to send an encrypted and signed Direct “wrapped” message payload to the ETT Direct To email address.  Example test case  [r2\_170.315\_b1\_toc\_amb\_sample1\_v9.pdf@ttpedge.sitenv.org](mailto:r2_170.315_b1_toc_amb_sample1_v9.pdf@ttpedge.sitenv.org) |
|  | Proctor using the ETT validation report verifies message payload:   * Encrypted using the ETT’s Public Key * Transmitted via Direct “wrapped” message format * Message successfully decrypted |

<INSERT SCREEN SHOT – HIT Module sending message>

<INSERT SCREEN SHOT OR LINK TO FILE – ETT Validation Report>

### 1.5 Send Using Direct – Three HISP Partners [(h)(2)(i)(A) – Send – Required Enhanced Testing]

|  |  |
| --- | --- |
|  | Health IT developer provides documentation as evidence of successful send of Direct v1.2 “wrapped” messages to three partner HISPs:   * **Partner 1: <type here>** * **Partner 2: <type here>** * **Partner 3: <type here>**   Developer should include a signed attestation that health IT module supports “message wrapping” as a sender as this is not easily discernible in data captures/logs. |
|  | Health IT developer provides documentation as evidence of successfully processed MDNs received from the three partner HISPs identified above upon sending the Direct messages. |

<INSERT SCREEN SHOT OR LINK TO FILE – HISP Partner Supporting Documents>

<INSERT SCREEN SHOT OR LINK TO FILE – HISP MDN Processing>

# 170.315(h)(2)(i)(A) Applicability Statement for Secure Health Transport (Direct) - Receive

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Health IT developer identifies the HIT module’s Public Key for encryption of messages to be sent by ETT to the HIT module. * Demonstrate DCDT Hosting test case based on 1) either address-bound or domain-bound, and 2) either DNS or LDAP. * Health IT module receives (4) CCDA payloads via a Direct “wrapped” message from the Edge Test Tool (ETT). * Health IT module rejects health information not in accordance with the standard specified at §170.202(a)(2) based on the “negative test cases” within the ETT. * Health IT developer provides documentation and demonstrates receiving “wrapped” direct messages from three partner HISPs. | |
| **Expected Test Result:**   * Able to receive health information in accordance with the standards specified in §170.202(a)(2), including formatted only as a “wrapped” message. * Health IT module rejects health information not in accordance with the standard specified at §170.202(a)(2). * Health IT module demonstrates hosted certificates are discoverable based on error-free validation from the DCDT. * Health IT module successfully receives four “wrapped” Direct message payloads from the ETT. * Health IT module generates and sends valid MDN notifications for all received Direct messages. * Health IT module successfully receives encrypted and signed health information to 3 partner HISPs using Direct v1.2 in accordance with the standard specified at §170.202(a)(2). The verification includes:   + Documentation that the health IT module received “Wrapped” RFC-5751 messages from three partner HISPs; and   + Documentation the health IT module sent MDNs to each of the three partner HISPs generated upon receiving the Direct message from the HIT module. | |
| **Points to Remember:**   * For this criterion, it is required to receive messages in only “wrapped” format even though the specification allows use of “unwrapped” messages. * (h.2) attestation template provided in [Appendix C](#_Appendix_C:_170.315(h)(2):). | |

### Test Procedures

### 2.1 Hosting Certificates [(h)(2)(i)(A) – Receive 1]

DCDT: <https://ttpedge.sitenv.org/ttp/#/direct/certdiscovery/dcdt2>

|  |  |
| --- | --- |
|  | Health IT developer provides the Direct To email address to use for DCDT Hosting test  **Direct To email address**: <type here> |
|  | Proctor executes at least one of the following DCDT Hosting test case based on health IT module’s implementation:   * **H1 - Normal address-bound certificate search in DNS** * **H2- Normal domain-bound certificate search in DNS** * **H3 - Normal address-bound certificate search in LDAP** * **H4 - Normal domain-bound certificate search in LDAP** |
|  | Proctor verifies health IT module’s hosted certificates are discoverable based on DCDT test case validation. |

<INSERT SCREEN SHOTS – DCDT Hosting Test Result>

### 2.2 Receive Direct Message [(h)(2)(i)(A) – Receive 3]

ETT – DIRECT <https://ttpedge.sitenv.org/ttp/#/direct/send>

|  |  |
| --- | --- |
|  | If the certificate is not discoverable in DNS, Health IT developer provides the test with the HIT module’s public key to use for sending messages from the ETT Direct. |
|  | Using the ETT Send Direct Message functionality, Proctor selects and sends a “wrapped” message for one of these xml payloads and verifies receipt by the HIT module:   * **CCDA\_Ambulatory.xml** * **CCDA\_Inpatient.xml** |

<INSERT SCREEN SHOT – Message Received>

<INSERT SCREEN SHOT – MDN validation report>

### 2.3 Reject Direct Messages: Negative Test Cases [(h)(2)(i)(A) – Receive 4-8]

ETT – DIRECT <https://ttpedge.sitenv.org/ttp/#/direct/send>

|  |  |
| --- | --- |
|  | Proctor executes each of the “Negative” test cases below. This is done in the ETT Direct by selecting one of the payloads and then select one of the signing certs to send a “Wrapped” direct message:   * **Invalid Certificate** * **Expired Certificate** * **Different Trust Anchor** * **Bad AIA Extension** * **Invalid Message Digest** |
|  | Proctor verifies no MDNs were received for any of the negative test cases above. |

<INSERT SCREEN SHOTS>

### 2.4 Receive Using Direct – Three HISP Partners [(h)(2)(i)(B) – Required Enhanced Testing]

|  |  |
| --- | --- |
|  | Health IT developer provides documentation as evidence of successful receipt of Direct v1.2 “wrapped” messages from three partner HISPs:   * **Partner 1: <type here>** * **Partner 2: <type here>** * **Partner 3: <type here>**   Developer should include a signed attestation that health IT module supports “message wrapping” as a receiver as this is not easily discernible in data captures/logs. |
|  | Health IT developer provides documentation as evidence of successfully generated MDNs sent to the three partner HISPs identified above upon receipt of the Direct messages. |

<INSERT SCREEN SHOT OR LINK TO FILE – HISP Partner Supporting Documents>

<INSERT SCREEN SHOT OR LINK TO FILE – HISP MDN Processing>

# 170.315(h)(2)(i)(B) Send Using Direct + XDM

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Health IT developer sends a XDM payload via a Direct “wrapped” message to the appropriate ETT Direct testing tool email address. * Health IT developer provides documentation attesting to sending of “wrapped” Direct XDM message payloads to at least three partner HISPs (e.g., other Health IT developer HIT module HISPs) using Direct v1.2. | |
| **Expected Test Result:**   * Edge Test Tool (ETT) can successfully decrypt and validate received Direct XDM message from the health IT module. * Health IT module successfully sends encrypted and signed health information to three partner HISPs using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport. The verification includes:   + Documentation that the health IT module received “Wrapped” RFC-5751 messages from three partner HISPs; and   + Documentation the health IT module sent MDNs to each of the three partner HISPs generated upon receiving the Direct message from the HIT module. | |
| **Points to Remember:**   * (h.2) attestation template provided in [Appendix C](#_Appendix_C:_170.315(h)(2):). | |

### Test Procedures

### 3.1 Discover Certificates (Completed in section Send 1)

### 3.2 Register Direct Address (Completed in section Send 1.2)

### 3.3 Send Health Information Using Direct with XDR/XDM [(h)(2)(i)(B) – Send 3-6]

ETT – DIRECT <https://ttpedge.sitenv.org/ttp/#/direct>

|  |  |
| --- | --- |
|  | **Limited XDS Metadata:** Health IT developer uses HIT Module functionality to send an encrypted and signed Direct “wrapped” XDM message limited XDS metadata payload to the ETT Direct To email address.   * **Validation report received** * **Message successfully decrypted** |
|  | Proctor uploads the XDM payload received in the ETT validation report to the ETT’s Message Validator to verify the XDM package is valid. |

<INSERT SCREEN SHOT – HIT Module sending message>

<INSERT SCREEN SHOT OR LINK TO FILE – ETT Validation Report>

<INSERT SCREEN SHOT OR LINK TO FILE – ETT Message Validator>

|  |  |
| --- | --- |
|  | **Full XDS Metadata:** Health IT developer uses HIT Module functionality to send an encrypted and signed Direct “wrapped” XDM message full XDS metadata payload to the ETT Direct To email address.   * **Validation report received** * **Message successfully decrypted** |
|  | Proctor uploads the XDM payload received in the ETT validation report to the ETT’s Message Validator to verify the XDM package is valid. |

<INSERT SCREEN SHOT – HIT Module sending message>

<INSERT SCREEN SHOT OR LINK TO FILE – ETT Validation Report>

<INSERT SCREEN SHOT OR LINK TO FILE – ETT Message Validator>

### 3.4 Send Using Direct + XDM – Three HISP Partners

(Completed in section 1.5)

# 170.315(h)(2)(i)(B) Receive Using Direct + XDM

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Demonstrate hosted certificates are discoverable. * Health IT developer receives a XDM payload via a Direct “wrapped” message sent from the ETT. * Health IT developer provides documentation attesting to receiving “wrapped” Direct XDM message payloads to at least three partner HISPs (e.g., other Health IT developer HIT module HISPs) using Direct v1.2. * Health IT module rejects health information not in accordance with the standard specified at §170.202(a)(2) based on the “negative test cases” within the ETT. | |
| **Expected Test Result:**   * Able to receive health information in accordance with the standard specified in §170.202(b), including support for both limited and full XDS metadata profiles. * Health IT module’s hosted certificates are discoverable for the DCDT test cases executed. * Edge Test Tool (ETT) successfully receives and validates MDN from the health IT module. * Health IT module successfully receives encrypted and signed health information to three partner HISPs using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport. The verification includes:   + Documentation that the health IT module received “Wrapped” RFC-5751 messages from three partner HISPs; and   + Documentation the health IT module sent MDNs to each of the three partner HISPs generated upon receiving the Direct message from the HIT module. | |
| **Points to Remember:**   * (h.2) attestation template provided in [Appendix C](#_Appendix_C:_170.315(h)(2):). | |

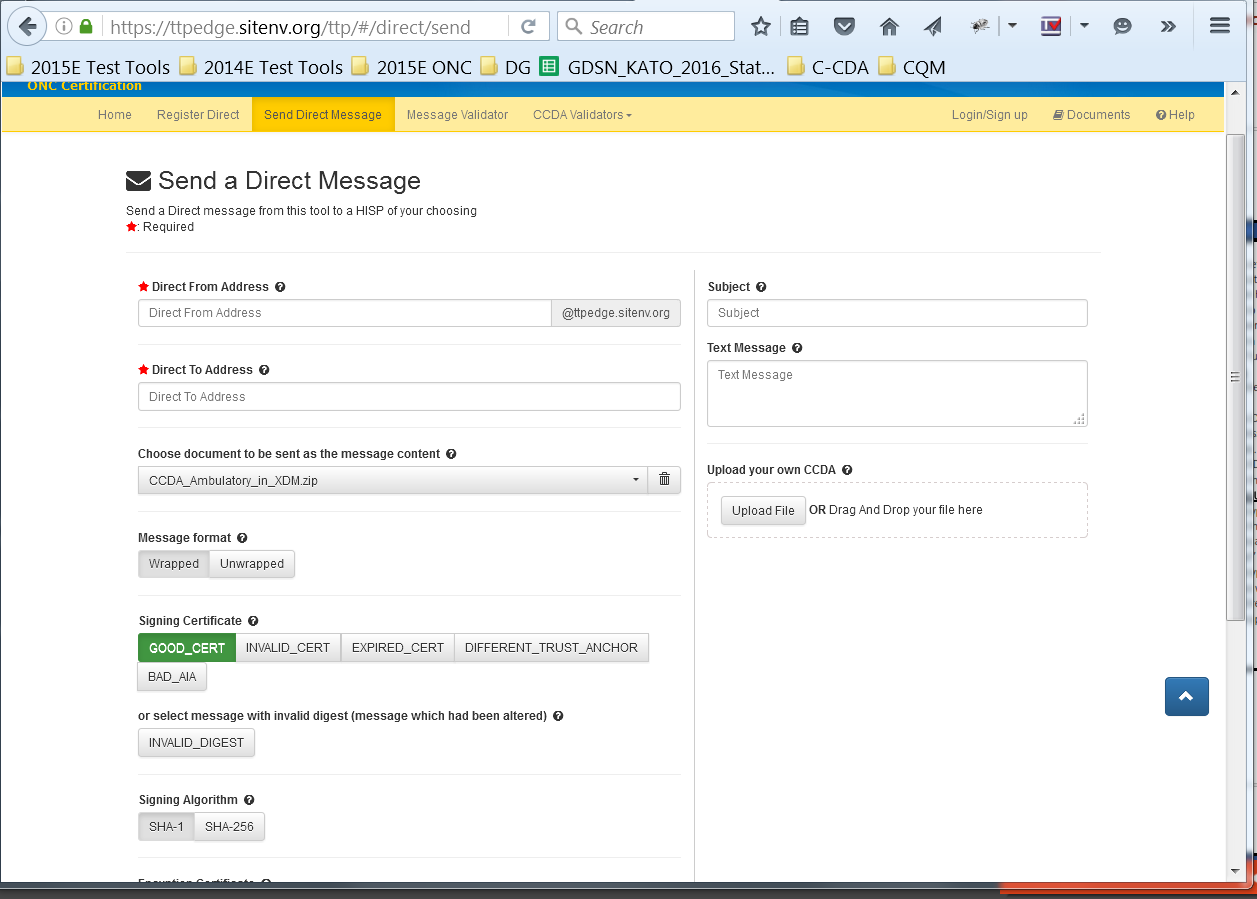
### Test Procedures

### 4.1 Hosting Certificates

(Completed in section 2.1)

### 4.2 Receive Direct Message [(h)(2)(i)(B) – Receive 3 - 5]

<https://ttpedge.sitenv.org/ttp/#/direct/send>



|  |  |
| --- | --- |
|  | If the certificate is not discoverable in DNS, Health IT developer provides the test with the HIT module’s public key to use for sending messages from the ETT Direct. |
|  | Using the ETT Send Direct Message functionality, Proctor selects and sends a “wrapped” message for one of these XDM payloads and verifies receipt by the HIT module:   * **CCDA\_Ambulatory\_in\_XDM.zip** * **CCDA\_Inpatient\_in\_XDM.zip** |

<INSERT SCREEN SHOT – Message Received>

<INSERT SCREEN SHOT – MDN validation report from ETT>

### 4.3 Reject Direct Messages: Negative Test Cases

(Completed in section Receive 2.3)

### 4.4 Receive Using Direct + XDM – Three HISP Partners

(Completed in section Receive 2.4)

# 170.315(h)(2)(i)(C) Send Using Edge Protocol for IHE XDR profile for Limited Metadata

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT – HISP System, XDR Test Cases as Sender functionality, the Proctor executes the required test cases * Using the ETT – HISP System, XDR Test Cases as Receiver functionality, the Proctor executes the required test cases (Message Tracking). | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with both edge protocol methods specified by the standard in §170.202(d). * All test cases pass without error. | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 5.1 SUT Connection Tests [(h)(2)(i)(C) – Send 1-2]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Sender)

|  |  |
| --- | --- |
|  | XDR Test 16 – Mutual TLS Session established. |
|  | XDR Test 17 – HISP disconnects when server provided certificate is invalid. |
|  | Secure Network (Alternative if not using TLS) – Developer demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at 170.202(d) Implementation Guide for Direct Edge Protocols v1.1. |

<INSERT SCREEN SHOTS>

### 5.2 Send Payload Tests [(h)(2)(i)(B) – Send using SOAP + XDR 1 - 3 / (h)(2)(i)(C) – Send 3]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Sender)

|  |  |
| --- | --- |
|  | XDR Test 10 – Direct to send to Edge as an XDR message |
|  | XDR Test 11 – Direct + XDM, Limited Metadata: HISP creates an XDR message per specification and forwards to the Edge. |
|  | XDR Test 12 – Direct + XDM, Full Metadata: HISP creates an XDR message per specification and forwards to the Edge. |

<INSERT SCREEN SHOTS>

### 5.3 Message Tracking Using Processed MDNs Tests [(h)(2)(i)(C) – Send 4-8]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Receiver)

|  |  |
| --- | --- |
|  | XDR MT Test 13 – Appropriately responds to a delivery to a non-existent address |
|  | XDR MT Test 14 – Appropriately responds to a delivery to untrusted HISP |
|  | XDR MT Test 15 – Appropriately responds to a delivery to HISP whose certificate is unpublished |
|  | XDR MT Test 16 – Appropriately responds to MDN delivery timeout failure |

<INSERT SCREEN SHOTS>

# 170.315(h)(2)(i)(C) Receive Using Edge Protocol for IHE XDR profile for Limited Metadata

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT – HISP System, XDR Test Cases as Receiver functionality, the Proctor executes the required test cases | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with both edge protocol methods specified by the standard in §170.202(d). * All test cases pass without error | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 6.1 SUT Connection Tests [(h)(2)(i)(C) – Receive 1-2]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Receiver)

|  |  |
| --- | --- |
|  | XDR Test 18 – Mutual TLS Session established |
|  | XDR Test 19 – HISP disconnects when Edge provided certificate is invalid |
|  | Secure Network (Alternative if not using TLS) – Developer demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at 170.202(d) Implementation Guide for Direct Edge Protocols v1.1. |

<INSERT SCREEN SHOTS>

### 6.2 Receive Payload Tests [(h)(2)(i)(B) – Receive SOAP + XDR 1-2 / (h)(2)(i)(C) – Receive 3-4]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Receiver)

|  |  |
| --- | --- |
|  | XDR Test 13 – HISP can receive a properly formatted XDR, limited metadata message and translate to Direct |
|  | XDR Test 14 – HISP can receive a properly formatted XDR, full metadata message and translate to Direct |

<INSERT SCREEN SHOTS>

### 6.3 Incorrect XDR Message Receive [(h)(2)(i)(C) – Receive 5-6]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Receiver)

|  |  |
| --- | --- |
|  | XDR Test 15a – Tester verifies that SUT rejects invalid messages. |
|  | XDR Test 15b – Tester verifies that the SUT rejects bad messages. |

<INSERT SCREEN SHOTS>

# 170.315(h)(2)(i)(C) Send Using Edge Protocol for SMTP

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT – HISP System, SMTP Test Cases as Sender functionality, the Proctor executes the required test cases. | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with both edge protocol methods specified by the standard in §170.202(d). * All test cases pass without error. * Provide documentation attesting to health IT module’s ability to reject the connection for a TLS session initiated with an Edge due to an invalid certificate and to authenticate using DIGEST-MD5 SASL (see [Appendix C](#_Appendix_C:_170.315(h)(2):) for template). | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 7.1 SUT Connection Tests [(h)(2)(i)(C) – Send 1-4]

<https://ttpedge.sitenv.org/ttp/#/hisp/smtp> (as Sender)

|  |  |
| --- | --- |
|  | SMTP Tests 8 and 14: Health IT developer sends a message to the ETT email address identified in the test case. Proctor verifies:   * TLS Session is established; and * Authenticated using PLAIN SASL |
|  | Health IT developer supplied documentation:   * Ability to reject a TLS session connection with an Edge due to an invalid certificate; and * Ability to authenticate using DIGEST-MD5 SASL. |
|  | Secure Network (Alternative if not using TLS) – Developer demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at 170.202(d) Implementation Guide for Direct Edge Protocols v1.1. |

<INSERT SCREEN SHOTS>

<INSERT SCREEN SHOTS or links to Health IT developer documents>

### 7.2 Message Tracking Using Processed MDNs Tests [(h)(2)(i)(C) – Send 5-9]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | Delivery Failure: **Message to Bad Address** (IMAP and POP are optional):  SMTP MT Test1  SMTP/IMAP MT Test 5  SMTP/POP MT Test 9 |
|  | Delivery Failure: **Receiving HISP Not Trusted** (IMAP and POP are optional):  SMTP MT Test2  SMTP/IMAP MT Test 6  SMTP/POP MT Test 10 |
|  | Delivery Failure: **Recipient’s Certificate Not Published** (IMAP and POP are optional):  SMTP MT Test3  SMTP/IMAP MT Test 7  SMTP/POP MT Test 11 |
|  | Delivery Failure: **No Processed MDN** (IMAP and POP are optional):  SMTP MT Test4  SMTP/IMAP MT Test 8  SMTP/POP MT Test 12 |

<INSERT SCREEN SHOTS>

# 

# 170.315(h)(2)(i)(C) Send Using Edge Protocol for IMAP (Optional)

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT – HISP System, IMAP Test Cases as Sender functionality, the Proctor executes the required test cases. | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with both edge protocol methods specified by the standard in §170.202(d). * All test cases pass without error. * Provide documentation (see [Appendix C](#_Appendix_C:_170.315(h)(2):) for template) attesting to health IT module’s ability to: * Accept a DIGEST-MD5 authentication mechanism and authenticates the edge; and * Process connection requests initiated using STARTTLS with cipher suites:   TLS\_RSA\_WITH\_RC4\_128\_MD5; and  TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA.   * Reject an authentication request from an Edge due to bad DIGEST-MD values. | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 8.1 Send IMAP Positive Tests [(h)(2)(i)(C) – Send 1-2]

<https://ttpedge.sitenv.org/ttp/#/hisp/imap> (as Sender)

|  |  |
| --- | --- |
|  | IMAP Test 1, 2, 3 –Verify command support:IMAP4 CAPABILITY, NOOP |
|  | IMAP Test 8,11,15 –Verify command support: AUTHENTICATE, STARTTLS, LOGIN, SELECT, FETCH |

<INSERT SCREEN SHOTS>

### 8.2 Send IMAP Negative Tests [(h)(2)(i)(C) – Send 3-4]

<https://ttpedge.sitenv.org/ttp/#/hisp/imap> (as Sender)

|  |  |
| --- | --- |
|  | IMAP Test 9 –Verify HISP reject bad command when command has bad syntax |
|  | IMAP Test 10 –Verify HISP reject commands with right syntax based on specific state of the connection |

<INSERT SCREEN SHOTS>

### 8.3 Send IMAP Message Processing [(h)(2)(i)(C) – Send 5-11]

<https://ttpedge.sitenv.org/ttp/#/hisp/imap> (as Sender)

|  |  |
| --- | --- |
|  | IMAP Test 12 – Using the ETT logs, the tester verifies the Health IT Module  generates unique identifiers for each message (UIDs). |
|  | HIT module supports h STARTTLS with TLS\_RSA\_WITH\_RC4\_128\_MD5 cipher suite |
|  | HIT module supports STARTTLS with TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite |
|  | HIT module supports DIGEST-MD5 authentication. |
|  | HIT Module rejects authentication from Edge due to bad DIGEST-MD5 values |
|  | IMAP Test 17 – Negative test: Verify HISP rejects incorrect username and password |
|  | IMAP Test 32 –Verify ability of the HISP to host attachments and make them available for fetching using IMAP |
|  | HIT Module rejects authentication from Edge due to bad DIGEST-MD5 values |

<INSERT SCREEN SHOTS>

# 170.315(h)(2)(i)(C) Send Using Edge Protocol for POP3 (Optional)

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT – HISP System, POP3 Test Cases as Sender functionality, the Proctor executes the required test cases. | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with both edge protocol methods specified by the standard in §170.202(d). * All test cases pass without error. * Provide documentation attesting to health IT module’s ability to process connection requests initiating STARTTLS with cipher suites: TLS\_RSA\_WITH\_RC4\_128\_MD5; and TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA (see [Appendix C](#_Appendix_C:_170.315(h)(2):) for template). | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 9.1 Send POP Positive Tests [(h)(2)(i)(C) – Send 1, 2]

<https://ttpedge.sitenv.org/ttp/#/hisp/pop> (as Sender)

|  |  |
| --- | --- |
|  | POP Test 1, 2 –Verify command support: POP3 CAPA, NOOP, QUIT |
|  | POP Test 5,11,15 –Verify command support: POP3 STAT, STARTTLS, RETR, LIST, RSET |

<INSERT SCREEN SHOTS>

### 9.2 Send POP Negative Tests [(h)(2)(i)(C) – Send 3-4]

<https://ttpedge.sitenv.org/ttp/#/hisp/pop> (as Sender)

|  |  |
| --- | --- |
|  | POP Test 9 –HISP rejects a command using bad syntax but in a bad state |
|  | POP Test 10 –HISP rejects a command using right syntax but in a bad state |

<INSERT SCREEN SHOTS>

### 9.3 Send POP - Message Processing [(h)(2)(i)(C) – Send 5-9]

|  |  |
| --- | --- |
|  | POP Test 12 – Verify ability of HISP to generate UID’s for each message when messages are added/deleted and synched multiple times after closing/re-opening connections |
|  | HIT module supports STARTTLS with TLS\_RSA\_WITH\_RC4\_128\_MD5 cipher suite with attestation document |
|  | HIT module supports STARTTLS with TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite with attestation document |
|  | POP Test 17 –HISP rejects authentication when a bad username and password is used |
|  | POP Test 32 –Verify ability of the HISP to host attachments and make them available for fetching using POP |

<INSERT SCREEN SHOTS>

# 170.315(h)(2)(i)(C) Receive Using Edge Protocol for SMTP

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT – HISP System, SMTP Test Cases as Receiver functionality, the Proctor executes the required test cases. | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with both edge protocol methods specified by the standard in §170.202(d). * All test cases pass without error. * Provide documentation attesting to health IT module’s ability to authenticate to an Edge using DIGEST-MD5 SASL as an SMTP server and reject authentication due to an invalid DIGEST-MD5 value (see [Appendix C](#_Appendix_C:_170.315(h)(2):) for template). | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 10.1 SUT Connection and Payload Tests [(h)(2)(i)(C) – Receive 1 –6]

<https://ttpedge.sitenv.org/ttp/#/hisp/smtp> (as Receiver)

|  |  |
| --- | --- |
|  | SMTP Test 9, 16, and 20 – Proctor verifies:   * STARTTLS Session is established * Authenticated using PLAIN SASL * Proctor uses ETT functionality to send a C-CCDA to the HIT module email address identified in the receiver profile (payload test) |
|  | SMTP Test 17 – Reject Invalid STARTTLS |
|  | HIT module supports ability to authenticate with the Edge using DIGEST-MD5 SASL |
|  | SMTP Test 22 – HISP rejects authentication due to bad DIGEST-MD5 value. |
|  | Secure Network (Alternative if not using TLS) – Developer demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at 170.202(d) Implementation Guide for Direct Edge Protocols v1.1. |

<INSERT SCREEN SHOTS>

### 10.2 Receive Negative Tests [(h)(2)(i)(C) – Receive –7-9]

<https://ttpedge.sitenv.org/ttp/#/hisp/smtp> (as Receiver)

|  |  |
| --- | --- |
|  | SMTP Test 10 – Reject Invalid Data |
|  | SMTP Test 11 – Reject Bad Commands |
|  | SMTP Test 13 – Command Timeout |

<INSERT SCREEN SHOTS>

# 170.315(h)(2)(ii) Send Delivery Notification In Direct

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT’s “HISP Testing & Delivery Notification” functionality, Proctor selects “Message Tracking” and enters the Health IT developer’s “Sender” profile. * Proctor executes ETT test cases for HISP as sender. * Using the ETT’s “HISP Testing & Delivery Notification” functionality, Proctor selects “XDR Test Cases” and “Your System as: Receiver” * Proctor execute the required XDR test cases. | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with the standard specified in §170.202(e)(1). * All positive and negative test cases successfully pass as expected. | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 11.1 SMTP Tests: Disposition-Notification-Options Header [(h)(2)(ii) - Send 1]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | Disposition-Notification-Options Header. Execute a minimum of one test case:  **MT Test21(a)**  **IMAP Test21(b)**  **POP Test21(c)** |

<INSERT SCREEN SHOTS – Test Case Logs>

### 11.2 SMTP Tests: Delivery Failure [(h)(2)(ii) - Send 2-7]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | Delivery Failure: **Bad Destination Address**. Execute a minimum of one test case:  MT Test23(a)  IMAP Test23(b)  POP Test23(c) |
|  | Delivery Failure: **Untrusted Destination HISP**. Execute a minimum of one test case:  MT Test24(a)  IMAP Test24(b)  POP Test24(c) |
|  | Delivery Failure: **Unpublished Certificate for Destination HISP**. Execute a minimum of one test case:  MT Test25(a)  IMAP Test25(b)  POP Test25(c) |
|  | Delivery Failure: **Timeout for Processed MDN**. Execute a minimum of one test case:  MT Test26(a)  IMAP Test26(b)  POP Test26(c) |
|  | Delivery Failure: for **Dispatched MDN**. Execute a minimum of one test case:  MT Test27(a)  IMAP Test27(b)  POP Test27(c) |
|  | Delivery Failure: **Timeout for Dispatched MDN**. Execute a minimum of one test case:  MT Test28(a)  IMAP Test28(b)  POP Test28(c) |

<INSERT SCREEN SHOTS – Test Case Logs>

### 11.3 SMTP Tests: Positive Delivery [(h)(2)(ii) - Send 8]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | SMTP Positive Delivery Notification. Execute a minimum of one test case:  MT Test29(a)  IMAP Test29(b)  POP Test29(c) |

<INSERT SCREEN SHOTS – Test Case Logs>

### 11.4 XDR Tests: Requesting Delivery Notification for XDR Edge HISP [(h)(2)(ii) - Send 9-10]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | XDR MT Test 30 - Verify the ability of the receiving system to appropriately handle a valid delivery notifications request. |
|  | XDR MT Test 31 - Verify the ability of the receiving system to appropriately handle an invalid delivery notifications request. |

<INSERT SCREEN SHOTS – Test Case Logs>

### 11.5 XDR Tests: Delivery Failure [(h)(2)(ii) - Send 11-16]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | XDR MT Test 32 - Verify the ability of the receiving system to appropriately respond to a potential delivery to a non-existent address. |
|  | XDR MT Test 33 - Verify the ability of the receiving system to appropriately respond to a potential delivery to an untrusted HISP. |
|  | XDR MT Test 34 - Verify the ability of the receiving system to appropriately respond to a potential delivery to a HISP whose certificate is unpublished. |
|  | XDR MT Test 35 - Verify the ability of the receiving system to appropriately respond in the event of a lack of a Processed MDN. |
|  | XDR MT Test 36 - Verify the ability of the receiving system to appropriately respond in the event of a lack of a Dispatched MDN. |
|  | XDR MT Test 37 - Verify the ability of the receiving system to appropriately respond in the event of a message timeout failure. |

<INSERT SCREEN SHOTS – Test Case Logs>

### 11.6 XDR Tests: Positive Delivery Notification [(h)(2)(ii) - Send 17]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Sender)

|  |  |
| --- | --- |
|  | XDR MT Test 38 - Verify the ability of the receiving system to appropriately respond in the event of positive delivery notification |

<INSERT SCREEN SHOTS – Test Case Logs>

# 170.315(h)(2)(ii) Receive Delivery Notification In Direct

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:**   * Using the ETT’s “HISP Testing & Delivery Notification” functionality, Proctor selects “Message Tracking” and enters the Health IT developer’s “Receiver” profile. * Proctor executes ETT test cases for HISP as receiver. * Using the ETT’s “HISP Testing & Delivery Notification” functionality, Proctor selects “XDR Test Cases” and “Your System as: Receiver”. * Proctor executes the required XDR test cases. | |
| **Expected Test Result:**   * Able to send and receive health information in accordance with the standard specified in §170.202(e)(1). * All positive and negative test cases successfully pass as expected. | |
| **Points to Remember:**   * Not applicable. | |

### Test Procedures

### 12.1 SMTP Tests: Disposition-Notification-Options Header [(h)(2)(ii) - Receive 1-2]

<https://ttpedge.sitenv.org/ttp/#/hisp/mu2> (as Receiver)

|  |  |
| --- | --- |
|  | SMTP/IMAP MT Test 39 - Message with Good Header |
|  | SMTP/IMAP MT Test 40 - Message with Bad Header |

<INSERT SCREEN SHOTS – Test Case Logs>

### 12.2 XDR Tests: Failure Notifications [(h)(2)(ii) - Receive 3-4]

<https://ttpedge.sitenv.org/ttp/#/hisp/xdr> (as Receiver)

|  |  |
| --- | --- |
|  | XDR MT Test 43 - Verify the ability of the receiving system to appropriately provide a delivery failure message if it is unable to deliver the message to the destination |
|  | XDR MT Test 44 - Verify the ability of the receiving system to appropriately respond in the event of a message timeout failure. |

<INSERT SCREEN SHOTS – Test Case Logs>

# Appendix A: Testing Guide

*This appendix contains more details and background on the testing requirements, including explanation on underlying standards, notable issues and best practice suggestions.*

Rev 01-Mar-2016 Additions

* None.

# Appendix B: ONC Criteria and Standards

*This appendix contains copy of the relevant ONC criteria and standards for this proctor sheet as a reference. In the event of a discrepancy with the ONC Final Rule, the ONC Final Rule takes precedence.*

**§** **170.315(h)(2) Direct Project, Edge Protocol, XDR/XDM.**

1. Able to send and receive health information in accordance with:

(A) The standard specified in § 170.202(a)(2), including formatted only as a “wrapped” message;

(B) The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and

(C) Both edge protocol methods specified by the standard in § 170.202(d).

1. Applicability Statement for Secure Health Transport and Delivery Notification in Direct. Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

**§** **170.202(a)(2)** [Applicability Statement for Secure Health Transport, Version 1.2, August 2015](http://wiki.directproject.org/file/view/Applicability+Statement+for+Secure+Health+Transport+v1.2.pdf)

**§ 170.202(b)** [ONC XDR and XDM for Direct Messaging Specification](http://healthit.gov/policy-researchers-implementers/direct-project)

XDS metadata profiles: IHE ITI: [IHE IT Infrastructure Technical Framework Volume 3 (ITI TF-3)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol3_FT_2010-08-10.pdf)

**§ 170.202(d)** [ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014](http://www.healthit.gov/sites/default/files/implementationguidefordirectedgeprotocolsv1_1.pdf)

**§ 170.202(e)(1)** [Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012](http://wiki.directproject.org/file/view/Implementation+Guide+for+Delivery+Notification+in+Direct+v1.0.pdf)

### Appendix C: 170.315(h)(2) Attestation Template

*This appendix contains a template for submitting the 170.315(h)(2) attestation requirements. The attestation letter should be returned on company letterhead addressing the required functionality.*

[Name of Authorized Senior Company Representative]

[Title of Company Representative]

[Company Contact Information]

[Company Name] attests that the System Under Test provides the functionality identified below for the associated ONC 2015 Edition criteria 170.315(h)(2) requirements:

* Rejects the connection for a TLS session initiated with an Edge due to an invalid certificate.
* Ability to authenticate using DIGEST-MD5 SASL.
* Initiate a STARTTLS connection using valid cipher suite: TLS\_RSA\_WITH\_RC4\_128\_MD5.
* Initiate a STARTTLS connection using valid cipher suite: TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA.
* Accept authentication requests using DIGEST-MD5 and reject authentication due to an invalid DIGEST-MD5 value.
* Authenticate to an Edge using DIGEST-MD5 SASL as an SMTP server and reject authentication due to an invalid DIGEST-MD5 value.
* Support full message wrapping for incoming and outgoing messages

**I hereby attest that all above statements are true, as an authorized signing authority on behalf of my organization.**

[Signature]

[Signature Block of Authorized Senior Company Representative]

[Date signed]

**Change Log**

|  |  |
| --- | --- |
| Revision | Change Description |
| 05-Jun-2017 | Removed Invalid Trust Anchor per ONC update. Added “Secure Network” Alternative for providing secure connection to sections 5.1, 6.1, 7.1, and 10.1. Update SMTP test cases (1-8, 14) to SMTP Test Cases (8 and 14) under section 7.1. Updated IMAP test case (4-8, 11, 15) to IMAP test case (8, 11, and 15) under section 8.1. Updated POP Test (3-5, 11, and 15) to POP Test (5,11, and 15) under section 9.1. |
| 03-Apr-2017 | Restructured sections (8.2 and 8.3) and (9.2 and 9.3). Updated test case SMTP 22. Corrected test case numbers throughout. |
| 10-Feb-2017 | Updated XDR Test Numbers In Section 5.2 & 6.2. Updated links to ETT. |
| 01-Dec-2016 | Replaced TTT references to ETT (Edge Test Tool). Added DCDT test cases 17 and 18. |
| 01-Nov-2016 | Removed deprecated tests. Consolidated tests into a single section where necessary (including sections 9.1 and 12.1). |
| 01-Oct-2016 | Added procedure mappings and hyperlinks for test tools. Added requirement for “message wrapping” attestation. Updated pretest activities under “Test Data and Tools” section. Updated hyperlinks for ONC-hosted ETT. |
| 01-May-2016 | Added documentation criteria under Expected Test Results and Appendix C attestation template. Added TLV step related MU Tracking Step 17. Removed negative test SMTP/IMAP/POP MT Test 22 from section 13.2. Removed SMTP/IMAP MT Test 41 (No Dispatched MDN) & SMTP/IMAP MT Test 42. |
| 01-Apr-2016 | Corrected instructions under “Receive using Direct + XDM” and “Send using SOAP + XDR” sections. |
| 01-Mar-2016 | Initial Release. |
|  |  |
|  |  |

**About Drummond Group LLC**

Drummond Group LLC is a global software test and certification lab that serves a wide range of vertical industries.  In healthcare, Drummond Group tests and certifies Controlled Substance Ordering Systems (CSOS), Electronic Prescription of Controlled Substances (EPCS) software and processes, and Electronic Health Records (EHRs) – designating the trusted test lab as the only third-party certifier of all three initiatives designed to move the industry toward a digital future. Founded in 1999, and accredited for the Office of the National Coordinator Health IT Certification Program as an Authorized Certification Body (ACB) and an Authorized Test Lab (ATL), Drummond Group continues to build upon its deep experience and expertise necessary to deliver reliable and cost-effective services. For more information, please visit <http://www.drummondgroup.com> or email [ehr@drummondgroup.com](mailto:ehr@drummondgroup.com)

END OF DOCUMENT