



**Centers for Medicare & Medicaid Services**  
**CMS eXpedited Life Cycle (XLC)**

## **Electronic Submission of Medical Documentation / esMD**

### **HH Onboarding/ Offboarding Manual**

---

**Version 1.1**  
**9/09/2014**

## Table of Contents

<b>1. Introduction .....</b>	<b>4</b>
<b>2. Overview .....</b>	<b>4</b>
2.1 Cautions & Warnings .....	4
<b>3. Getting Started .....</b>	<b>4</b>
3.1 Health Level 7 (HL7) Object Identifiers (OIDs) .....	4
3.1.1 HL7 OID Registration .....	4
3.2 Internet Protocol (IP) Addresses .....	5
3.3 Transport Layer Security (TLS) Certificates .....	5
3.3.1 Generating a Certificate Signing Request (CSR) .....	7
3.4 Set-up Considerations .....	7
3.5 Windows 64-bit Environment Issues and Resolution .....	7
3.5.1 Issue A .....	7
3.5.2 Issue B .....	8
3.6 Gateway Software .....	8
3.6.1 CONNECT Specific Installation .....	9
3.6.2 Federal Information Processing Standards (FIPS) Mode Configuration .....	9
3.7 HIH Applications .....	11
3.8 VAL Testing Preparations .....	11
3.8.1 esMD Specific Configurations for Connectivity Validation Testing .....	11
3.8.2 Domain.xml .....	12
3.8.3 HIH Gateway internalConnectionInfo.xml Changes .....	12
3.8.4 SOAP UI Tool .....	13
<b>4. Validation Integration Testing .....</b>	<b>13</b>
4.1 Telnet testing in Validation .....	13
4.2 Connectivity Testing in Validation .....	14
4.2.1 Testing with SOAP UI Tool for Connectivity Testing .....	14
4.3 Functionality Testing .....	14
4.4 Validation End-to-End Testing .....	15
4.5 Status and Notification Messages .....	16
<b>5. HIH Gateway Configuration .....</b>	<b>17</b>
<b>6. Production Testing .....</b>	<b>18</b>
6.1 Telnet Testing in Production .....	18
6.2 Connectivity Testing in Production .....	18
6.2.1 esMD Specific Configurations for Connectivity Production Testing .....	18
6.3 Production End-to-End Testing .....	18
6.4 Special Considerations .....	19
6.5 Support .....	19

**7. Offboarding Process ..... 20**  
    7.1 Offboarding Procedure ..... 20  
**Acronyms..... 21**  
**Referenced Documents ..... 23**  
**Record of Changes ..... 24**  
**Approvals..... 25**

### List of Figures

Figure 1: Status and Notification Messages ..... 16

### List of Tables

Table 1: Test Claim and Case IDs for Validation Testing ..... 15  
Table 2: Test Claim and Case IDs for Production Testing..... 19  
Table 3: Support Points of Contact ..... 19  
Table 4: Acronyms ..... 21  
Table 5: Referenced Documents..... 23

## 1. Introduction

---

This Onboarding Manual provides the information necessary for Health Information Handlers (HIHs) to effectively construct a gateway in order to submit medical documentation to review contractors via the use of the Centers for Medicare & Medicaid Services' (CMS) Electronic Submission of Medical Documentation (esMD) system.

## 2. Overview

---

This guide outlines the testing phases and additional instructions HIHs will follow in order to onboard to esMD.

### 2.1 Cautions & Warnings

Please be advised that QSSI will provide limited support to HIHs. It is the HIH's responsibility to provide the necessary resources in order to complete tasks. Some details in this guide are geared toward users of CONNECT 3.1, which Quality Software Services; Inc. (QSSI) has successfully tested against the CMS esMD Gateway. HIHs may use a CONNECT –compatible software or other versions of CONNECT.

**Commented [A1]:** This needs to be changed as we now use CONNECT version 4.2. With the new release this version will change again.

## 3. Getting Started

---

In order to begin the HIHs must return a completed HIH Onboarding Request Form. Upon receipt of the completed form, QSSI will process the information and confirm acceptance to the onboarding process.

**Commented [A2]:** Where will the HIH find this form.

The following subsections provide helpful information to HIHs at the pre-onboarding stage and assist them in completing the HIH Onboarding Request Form.

### 3.1 Health Level 7 (HL7) Object Identifiers (OIDs)

CMS esMD requires HIHs to use Health Level 7 (HL7) registered Object Identifiers (OIDs). HIHs only need to obtain one OID. The same HIH OID will be used for validation and production environments by adding .2 (for validation) or .1 (for production) as a suffix to the original OID. This helps esMD to identify from which HIH gateway environment the request is submitted to the CMS esMD Gateway.

#### 3.1.1 HL7 OID Registration

To obtain and register for an HL7 OID, follow these steps:

1. Visit <http://www.hl7.org/oid/index.cfm?ref=common>;
2. Click the "Obtain/Register an OID" link located on the right-hand side of the screen;

3. As a submitter, complete the following fields: first name, last name, email address;
4. To enter contact information, use the same information for the following fields: name (first, last), phone number, email address;
5. To enter information for the responsible body, use your company information to complete the required fields:
  - a. Name (company name);
  - b. Phone (company or submitter phone number)
  - c. Email (company email address)
  - d. Address (company address)
  - e. Type (choose "vendor")
  - f. Uniform Resource Locator (URL) - (not required/can use company URL)
  - g. If your organization already has an OID, enter the OID in the responsible body OID field.
6. For internal/external OIDs:
  - a. Choose the internal OID option if you are registering a new OID
  - b. If you already have an OID that you need to register, you will choose "external" and enter the OID in the field provided.
7. OID information:
  - a. OID Type is 3-Root to be a Registration Authority;
  - b. Desired symbolic name: enter your company's name or acronym as lowercase with no spaces;
  - c. Full name of object: enter your company's official name;
  - d. Description of object: describe for what purpose your company will use this OID.
8. Click the "continue" button. Your OID will be issued and a confirmation email will be sent to the submitter's email address.

## 3.2 Internet Protocol (IP) Addresses

A public-facing Internet Protocol (IP) address is the address that identifies the HIH network and allows the CMS esMD Gateway to connect to the HIH network from the internet. The HIH will hide their internal private esMD Gateway (or server) IP address with Network Address Translation (NAT) to the public-facing IP address. The HIH technical team will contact their network team to assign or assign a public-facing IP address to their internal private IP. If an HIH is using multiple esMD servers, then the HIH will only submit one IP address for both inbound and outbound. QSSI suggests the HIH use load balancing and NAT to convert/submit the request from multiple servers to one IP address.

## 3.3 Transport Layer Security (TLS) Certificates

HIHs acquire a Transport Layer Security (TLS) server certificate from a certificate authority (CA) which conforms to the esMD security standards for the on-boarding process. Currently, CMS mutual authentication security hardware has successfully tested only with Entrust and Thawte CA Certificates. It is up to the HIH to take the risk in procuring the certificate from a well-established and perfectly tested CA Certificate.

CMS does not enforce the procurement of any particular CA Certificate and only suggests based on testing results.

TLS certificates that have been tested successfully with the CMS esMD Gateway are as follows:

1. Entrust
  - a. Suggested Type: Entrust Advantage SSL Certificate
  - b. URL: <http://www.entrust.net/ssl-certificates/advantage.htm>
  - c. \$239/yr. as of 9/17/2013
2. Thawte
  - a. Suggested Type: SSL Web Server Certificates
  - b. URL: <http://www.thawte.com/ssl/index.html>
  - c. \$199/yr. as of 9/17/2013

All CAs used to generate certificates for use in the esMD must adhere to the following guidelines:

1. Level 2 Identity Proofing as described in section 7 of this National Institute of Standards and Technology (NIST) publication:  
[http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf).  
(Specifically, see Table 1 on pages 22 through 24.)
2. 2048 bit RSA (algorithm) keys
3. Advance Encryption Standard (AES) 128 bit encryption
4. Secure Hash Algorithm-1 (SHA-1) certificate signing algorithm
5. Server Level and server-to-server communication certificate. (Note: No wild card (\*.\*) or domain level certificate are accepted).
6. All cryptographic modules used by HIH eHealth Exchange instances (typically CONNECT) must adhere to Federal Information Processing Standards (FIPS) 140-2 Compliance criteria and utilize TLS.
  - a. CMS security policies require HIHs to procure certificate renewals on a yearly basis. HIHs should only procure a certificate that expires after one year.
  - b. HIHs should note the expiration date of their certificates and plan accordingly to renew and submit certificate renewals to the CMS esMD Help Desk ([CMSesMDHelpdesk@gssinc.com](mailto:CMSesMDHelpdesk@gssinc.com)) three weeks in advance of the expiration date.

For reference, use the following links:

- [http://www.cms.gov/informationsecurity/downloads/ARS\\_App\\_B\\_CMSR\\_Moderate.pdf](http://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf) (See section Appendix B, SC13-1)

### 3.3.1 Generating a Certificate Signing Request (CSR)

Generate the Certificate Signing Request (CSR) and submit it to the CA Certificate authority (e.g., Entrust or Thawte) in order to procure the signed TLS certificate.

The Certificate Authority will process your submitted TLS Certificate Signing Request and will send an email to you (the HIH) with the download links. Download the server, intermediate, and root certificates and load the certificates from the CA website. Submit the server, intermediate, and root certificates to the esMD Coordinator using the HIH Onboarding Request Form.

Use the following commands to generate CSR using the java keytool:

1. **Generate java keystore (JKS) file:** `keytool -genkey -keyalg RSA -keysize 2048 -keystore <FilenameG1.jks> -keypass <Password> -storepass <password> -validity 365 -alias <alias name> -dname "cn=<common name>, OU=<Organization unit>, O=<Organization>, L=<Location>, S=<State>, C=<Country>"`
2. **List the JKS details:** `keytool -list -keystore <FilenameG1.jks> -storepass <password> -v`
3. **Export the certificate from the keystore we just created:** `keytool -export -rfc -alias < alias name> -file <FilenameG2.cer> -keystore <FilenameG1.jks> -keypass <password> -storepass <password>`
4. **List the certificate created and verify the certificate:** `keytool -printcert -file <FilenameG2.cer> -v`
5. **Create a CSR:** `keytool -certreq -alias < alias name> -file <FilenameG3.csr> -keystore <FilenameG1.jks> -storepass <password>`

## 3.4 Set-up Considerations

HIHs are able to use any server platform. The following platforms are successfully tested against esMD by certified HIHs:

1. Windows 2008, 64bit
2. Linux, 64bit
3. Ubuntu 8.04, 64bit

## 3.5 Windows 64-bit Environment Issues and Resolution

### 3.5.1 Issue A

eHealth Exchange CONNECT Gateway Binary installation / Source installation doesn't work on Windows 64-bit using 64-bit version of Java.

### 3.5.1.1 Solution

1. Go to the path C:\Java\jdk1.6.0\_16\jre\lib\ext;
2. Take a backup of file: sunpkcs11.jar;
3. Uninstall 32-bit version of Java;
4. Download and install 64-bit version of Java specific to the CONNECT 3.1 (i.e., 1.6.0\_16);
5. Install 64-bit version of Java;
6. Copy sunpkcs11.jar file from backup folder to new version of java in the same path **C:\Java\jdk1.6.0\_16\jre\lib\ext**;
7. Create a folder in your Windows machine **C:\Projects\NHINC\3.1**;
8. Check out CONNECT 3.1 source code from svn: <https://github.com/CONNECT-Solution/CONNECT/tree/3.1> to 3.1 folder created;
9. Follow the steps from: <https://developer.connectopensource.org/display/NHINR31/Source+Code+Install+%28Windows%29>;
10. Do a source installation;
11. Run validation tests; and
12. You should see all green.

### 3.5.2 Issue B

eHealth Exchange CONNECT Gateway Binary FIPS installation / Source FIPS installation doesn't work on Windows 64-bit using 64-bit version of Java.

#### 3.5.2.1 Solution

1. This is a known issue to all major vendors' communities using FIPS. The reason is the Mozilla development team has not focused much on Windows 64-bit version of binaries.
2. There is a bug available, and the CONNECT team claims it is now fixed: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=227049](https://bugzilla.mozilla.org/show_bug.cgi?id=227049).
3. However, the binaries are not available yet for the public.
4. The best solution is to setup a build environment for Mozilla FIPS development and perform a build to generate libraries. Required software licenses are applicable: [https://developer.mozilla.org/en/Windows\\_Build\\_Prerequisites](https://developer.mozilla.org/en/Windows_Build_Prerequisites).

## 3.6 Gateway Software

HIHs may use CONNECT or a CONNECT-compatible software. The CMS esMD Gateway uses CONNECT version 4.2. QSSI has not yet tested an HIH gateway using CONNECT-compatible software against the CMS esMD Gateway. HIHs should use and run any self-tests associated with the software they choose to use to ensure

installation is successful. It is the responsibility of the HIH to ensure proper software installation and perform any associated troubleshooting. The CMS esMD Onboarding Process does not include CONNECT or CONNECT-compatible software installation or troubleshooting support.

### 3.6.1 CONNECT Specific Installation

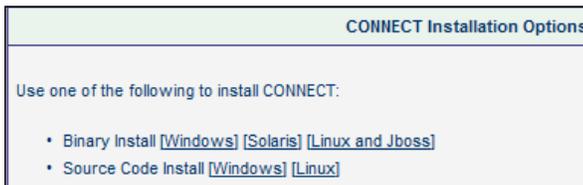
This section provides installation information for HIHs using CONNECT 3.1 software. If using CONNECT-compatible software, please check its associated installation instructions and minimum hardware requirements

HIHs can locate the CONNECT software version 3.1 download at this link:

<https://developer.connectopensource.org/display/NHINR31/Release+3.1+Home;jsessionid=BDF2C623193D85D78EBCC346D45F2BFE>.

The following is a list of suggested environments for installation:

1. Workstation environment – Source Code Install
2. Development environment – Binary Install
3. Validation environment – Binary Install
4. Production environment – Binary Install



The following are minimum hardware requirements for CONNECT Installation are the following (Please, refer to the environment specific CONNECT Installation instructions):

1. Processor: Minimum dual 2GHz
2. RAM: Minimum of 4GB
3. Hard Disk Size: The application is dependent on the deployment configuration. For sizing purposes, assume 100K per record, 1K per audit log record (The testing environment allocated = 20GB)
4. Hard Disk Speed: Minimum of 7200 RPM and 10K RPM preferred.
5. Network Interface: 100MB Ethernet acceptable. 1GB Ethernet desirable.

### 3.6.2 Federal Information Processing Standards (FIPS) Mode Configuration

The HIH turns on the Federal Information Processing Standards (FIPS) 140-2 (for cryptographic modules). The FIPS 140-2 is a government standard that provides a benchmark for how to implement cryptographic software

(<http://technet.microsoft.com/en-us/library/cc180745.aspx>). For the CONNECT Solution, this standard is being met to ensure that the CONNECT/CONNECT -

**Commented [A3]:** Update connect version. We are using version 4.2 now

**Commented [A4]:** Link did not work for me

compatible gateway is FIPS 140-2 compliant. Any HIH that needs to communicate with the esMD Gateway needs to have the FIPS mode enabled. The esMD Onboarding Process does not include support for FIPS mode configuration. The following CONNECT instructions may be used as a reference on how to configure CONNECT to be FIPS 140-2 compliant:

<https://developer.connectopensource.org/display/CONNECTWIKI/Instructions+to+set+up+CONNECT+in+FIPS+mode+on+Windows+Glassfish+environment>

Commented [A5]: Link does not work

### 3.6.2.1 FIPS Configuration Instructions

This section provides the steps to FIPS configuration if the HIH is using CONNECT software:

1. Load the certificates into the FIPS Database. You can find the FIPS NSS Database (DB) files in the application server under the following path:
  - a. If using Linux or Solaris - <http://opt/SUNWappserver/domains/nssdomain/config>
  - b. If using Windows - C:\Sun\AppServer\domains\domain1\config\nhin

Commented [A6]: Link does not work

#### FIPS - NSS Database (DB) Files:

- a. key3.db
  - b. Cert8.db
  - c. secmod.db
2. Extract the private key from the JKS keystore and append into the CA Signed Certificate Privacy Enhanced Email (PEM) file:
    - a. `java -cp keyexport.jar com.sun.xml.wss.tools.KeyExport -outform PEM -storepass <password> -keypass <password> -keyfile <FilenameG3_key.PEM> -alias < alias name> -keystore <FilenameG1.jks>`
    - b. Download the CA signed certificate from CA website in the java application format:
    - c. Assume the file name downloaded as CAfilename1.cer
    - d. Append the private key PEM FilenameG3\_key.PEM to certificate PEM file CAfilename1.cer.
  3. Convert the PEM to Public Key Cryptography Standards (PKCS) #12 and upload to NSS DB:
    - a. `openssl pkcs12 -export -in < CAfilename1.cer > -out < CAfilename.cer2.p12> -name < "alias name">`
    - b. `/nhin/nss-3.12.4/bin/pk12util -i < CAfilename.cer2.p12> -n < alias name> -d $AS_HOME/domains/nssdomain/config`
  4. List the NSS DB certificate nickname and trust attribute values:

```
certutil -d $AS_HOME/domains/nssdomain/config -L
```

```
certutil -d $AS_HOME/domains/nssdomain/config -K
```

5. Remove the gateway certificate added to the NSS DB and reload the same with the preferred attributes:

```
certutil -d $AS_HOME/domains/nssdomain/config -D -n <alias name>
```

```
certutil -d $AS_HOME/domains/nssdomain/config -A -t "T,c,c" -i <CAfilename1.cer> -n <yourgatewayaliasname>
```

6. List the certificate nickname and trust attribute values:

Confirm attributes comply with "Tu,cu,cu".

7. Load the other gateway certificates using the following command:

```
certutil -d $AS_HOME/domains/nssdomain/config -A -t "T,c,c" -i <certtobeimported> -n <gatewayname>
```

### 3.7 HIH Applications

HIHs should build an HIH application interface as a mechanism to move PDFs to their gateway for transport via esMD. The CMS esMD Onboarding Process does not include HIH application support. HIHs may use the SOAP UI tool or their application to perform testing; however, any HIH application issues must be resolved by the HIH or their IT vendor.

### 3.8 VAL Testing Preparations

Before HIHs can begin esMD onboarding, they need to complete the tasks covered in this section in preparation for validation integration testing.

#### 3.8.1 esMD Specific Configurations for Connectivity Validation Testing

The specifications mentioned below only apply to those that have opted to use CONNECT 3.1. If another version of CONNECT or CONNECT - compatible software is used, the HIH will need to make adjustments accordingly.

1. Stop the GlassFish server
2. Change the following in HIH gateway.properties and adapter.properties files:
  - A. **gateway.properties:**
    - a. Enable the External Data Representation (XDR) request/response:
      - i. serviceDocumentSubmissionDeferredReq=true
      - ii. serviceDocumentSubmissionDeferredResp=true
    - b. Enable the pass-through SOAP UI:
      - i. documentSubmissionDeferredRespPassthrough=true
      - ii. documentSubmissionDeferredReqPassthrough=true
      - iii. documentSubmissionPassthrough=true

- c. Update the HIH OID (use your HL7 OID). HIHs will need to add .2 suffix to their OID (i.e., 2.16.840.1.113883.XX.XX.XXXX.2)
  - i. localHomeCommunityId= **HIH OID**
  - ii. localDeviceId= **HIH OID**

**B. adapter.properties:**

- a. Update HIH OID (use your HL7 OID). HIHs need to add .2 suffix to their OID (i.e., 2.16.840.1.113883.XX.XX.XXXX.2)
  - i. assigningAuthorityId= **HIH OID**
  - ii. XDSbHomeCommunityId=**HIH OID**
- b. Start the GlassFish server

### 3.8.2 Domain.xml

The domain.xml (under SUNWappserver/domains/nssdomain/config/domain.xml) should contain the following HTTP Listener and JVM settings to allow the receipt of the esMD notifications from the CMS esMD Gateway at port 8191 and the TLS cipher exchange for authentication between the CMS esMD Gateway and the HIH gateway.

**1. Http Listener for 8191 port in domain.xml:**

```
<http-listener acceptor-threads="1" address="0.0.0.0" blocking-enabled="false" default-virtual-server="server" enabled="true" family="inet" id="http-listener-2" port="8191" security-enabled="true" server-name="" xpowered-by="true">
<ssl cert-nickname="v2031esmdGateway" client-auth-enabled="true" ssl2-enabled="false" ssl3-enabled="false" ssl3-tls-ciphers="+TLS_RSA_WITH_AES_128_CBC_SHA,+TLS_DHE_DSS_WITH_AES_128_CBC_SHA,+TLS_DHE_RSA_WITH_AES_128_CBC_SHA,+SSL_RSA_WITH_3DES_EDE_CBC_SHA" tls-enabled="true" tls-rollback-enabled="true"/>
</http-listener>
```

**2. JVM Cipher suite configuration in domain.xml:**

```
<jvm-options>
Dhttps.cipherSuites=TLS_DHE_RSA_WITH_AES_128_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA</jvm-options>
```

### 3.8.3 HIH Gateway internalConnectionInfo.xml Changes

This section covers the changes HIHs need to make to the internalConnectionInfo.xml.

#### 3.8.3.1 CMS esMD Gateway Request End-Point

The CMS esMD Gateway - XDR Document Submission Deferred Request Endpoint is required to submit the request to the CMS esMD Gateway: These configuration details are provided in the esMD Validation Configuration Document. QSSI issues this document is issued to HIHs following configuration of HIH IP addresses, OID, and TLS certificates at the CMS esMD Gateway.

### 3.8.3.2 HIH esMD Gateway Response End-Point

The XDR Deferred Document Submission Response Endpoint is required for HIHs to receive Notifications from the CMS esMD Gateway to the HIH esMD Gateway Response End-Point. This Endpoint Configuration should be added to the CONNECT InternalConfigurationInfo.xml under the HIH Production OID.

### 3.8.3.3 HIH Gateway Configuration

After the HIH validation configuration (e.g., IP address, SSL/TLS certificates, OID) is configured at the CMS esMD Gateway, QSSI will send the HIH the esMD Validation Configuration Document. The HIH will have one week to complete the necessary configurations on their end before validation integration testing begins.

## 3.8.4 SOAP UI Tool

The SOAP UI tool is used by HIHs during validation (and sometimes production) integration testing. HIHs should download and install a SOAP UI tool prior to beginning validation integration testing.

### 3.8.4.1 Sample SOAP UI Message

The HIH needs to run the sample SOAP message prior to testing.

The following attachments include the sample SOAP message and a sample SOAP UI setup.

**Commented [A7]:** Where the attachment? Or will you be providing this to the HIHs?

## 4. Validation Integration Testing

This section outlines the steps to validation integration testing. HIHs have 8 weeks to complete validation integration testing. HIHs that require additional time for troubleshooting are placed back into the prospective HIH pool and have 6 months to re-enter the onboarding process. Any expired certificates must be replaced and configured before testing can resume.

### 4.1 Telnet testing in Validation

HIH will need to telnet (inbound to CMS) or ping to the CMS IP address (example: XX.XXX.XXX.X @ 443) as noted in the [Validation Configuration Document](#) and forward a screenshot to QSSI ([esMDCoordinators@qssinc.com](mailto:esMDCoordinators@qssinc.com)) for verification.

After confirmation of a successful inbound telnet from QSSI, HIHs need to ensure their port is open at port 8191, and QSSI will have CMS telnet (outbound) to the HIH IP address.

Upon successful inbound and outbound telnet tests, the HIH may proceed on to

**Commented [A8]:** Where do HIHs get this form? Perhaps there should be mention that this document will be provided

connectivity testing.

## 4.2 Connectivity Testing in Validation

Tests in this phase are to establish connectivity in the validation environment between the CMS Gateway and HIH gateway. In order to perform connectivity testing, the following is required:

1. The HIH needs to complete the configuration according to the esMD Validation Configuration Document;
2. QSSI has confirmed HIH IP address and TLS certificates are configured at the CMS esMD VAL Gateway;
3. The HIH needs to install the SOAP UI Tool; and
4. The HIH needs to run the sample SOAP message (provided by QSSI prior to testing).

### 4.2.1 Testing with SOAP UI Tool for Connectivity Testing

Connectivity testing involves the use of the SOAP UI tool and sample SOAP message.

**Commented [A9]:** Where is the sample soap message?

Before each test is fired, the unique ID and message ID (or select “Randomly generate messageID”) need to be changed.

When the HIH has successfully passed connectivity using the SOAP message, they contact QSSI ([esMDCoordinators@qssinc.com](mailto:esMDCoordinators@qssinc.com)). QSSI will verify connectivity and inform the HIH of a successful status to move forward.

## 4.3 Functionality Testing

Tests in this phase are performed to confirm that the HIH application will send proper metadata and payload (PDFs) to the CMS esMD Gateway using their esMD application and esMD HIH Gateway. The esMD Gateway validates and processes the metadata and will deliver payload to the Enterprise Content Management (ECM) repository.

Functionality testing is completed and validated by the HIH. HIHs are not given extra time during the validation integration testing timeline to complete this testing. Once connectivity testing is complete, QSSI expects HIHs to complete end-to-end testing.

The purpose of this is to test different functionality case scenarios to ensure the HIH Gateway is receiving the proper acknowledgements, notifications, and error messages, if any, back from the CMS esMD Gateway. Please reference the Appendix C of the esMD Implementation Guide for the functional test cases and verify the results against the listed “expected results”.

**Commented [A10]:** Where can the HIH locate the Implementation Guide?

This step of testing requires no verification from QSSI and is the responsibility of the HIH to ensure functionality of their gateway.

### 4.4 Validation End-to-End Testing

Tests in this phase are performed to ensure the HIH’s submitted metadata is validated and delivered to the ECM and, ultimately, delivered on to the review contractor. In addition, this testing will ensure that once the review contractor picks up the submitted documents, the notification will be sent back to the HIH regarding the pickup status.

**Commented [A11]:** Update. ECM is no longer used.

As mentioned previously, this test should be performed using the HIH application but can be performed using the SOAP UI tool. HIHs are requested to use the recipient OID and sample test claim ID and case ID when submitting a test submission. The recipient OID is listed in Table 1.

Please refer to Section 5.3.8 of the esMD Implementation Guide for numeric length for claim and case IDs. When submitting tests, HIHs must use the numeric digits “8378” prefix to any claim and case ID. If using the sample format in the Table 1, do not exceed 23 characters for claim ID or 32 characters for case ID.

TEST Claim and TEST Case IDs for End-to-End Testing in esMD Validation			
Review Contractor (RC)	OID	Claim ID	Case ID
TEST RC 1	2.16.840.1.113883.13.34.110.1.999.1	8378CLAIMID<HIH>1	8378CASEID<HIH>1
TEST RC 1	2.16.840.1.113883.13.34.110.1.999.1	8378CLAIMID<HIH>2	8378CASEID<HIH>2

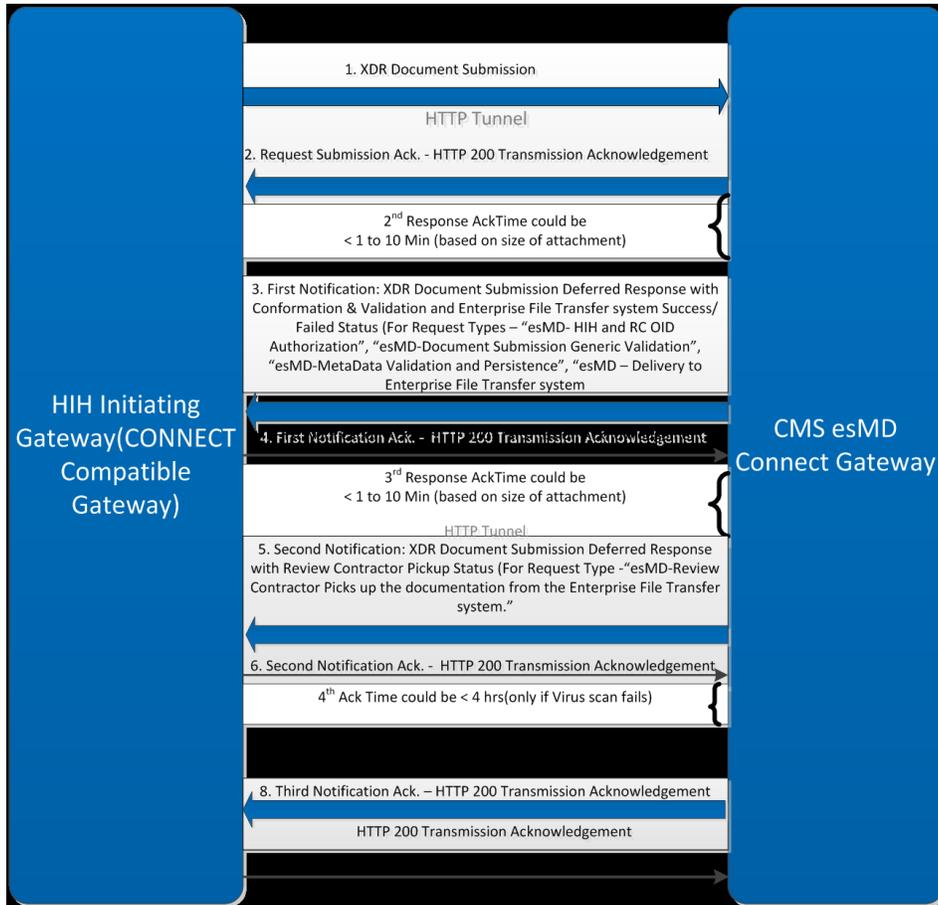
**Table 1: Test Claim and Case IDs for Validation Testing**

Upon successful completion of the interoperability and integration testing (i.e., transmission of 100% correctly formed payload and receipt of the two asynchronous responses back from the esMD Gateway) between the HIH and the Validation region esMD Gateway, the HIH will officially receive an email confirmation of successful testing results from QSSI. The HIH can then start production testing preparations.

## 4.5 Status and Notification Messages

Please note the status in red is not yet active within esMD. For additional information on status notifications, please refer to Section 8 of the esMD Implementation Guide.

**Figure 1: Status and Notification Messages**



## 5. HIH Gateway Configuration

After the HIH production configuration (e.g., IP address, TLS certificates, and OID) is complete at the CMS esMD Gateway, QSSI will send the HIH the esMD Production Configuration Document. The HIH will have one week to complete the necessary configurations on their end before production integration testing begins.

## 6. Production Testing

This section outlines the steps to production integration testing. HIHs have 6 weeks to complete production integration testing. HIHs that require additional time for troubleshooting are placed back into the prospective HIH pool and have 5 months to re-enter the onboarding process. Any expired certificates must be replaced and configured before testing can resume.

### 6.1 Telnet Testing in Production

The HIH will need to telnet (inbound to CMS) or ping to the CMS IP address (example: XX.XXX.XXX.X @ 443) as noted in the esMD Production Configuration Document and forward a screenshot to QSSI ([esMDCoordinators@gssinc.com](mailto:esMDCoordinators@gssinc.com)) for verification.

After confirmation of a successful inbound telnet from QSSI, HIHs need to ensure that their port is open at 8291, and QSSI will have CMS telnet (outbound) to the HIH IP address.

Upon successful inbound and outbound telnet tests, the HIH may proceed on to connectivity testing.

### 6.2 Connectivity Testing in Production

Tests in this phase are to establish connectivity in the Production environment between the CMS Gateway and HIH Gateway. The SOAP UI tool is no longer required, but may be used. In order to perform connectivity testing, the following is required:

1. The HIH needs to complete the configuration according to the esMD Production Configuration Document; and
2. QSSI has confirmed HIH IP address and TLS certificates are configured at the CMS esMD PROD Gateway.

#### 6.2.1 esMD Specific Configurations for Connectivity Production Testing

The esMD specifications for Production are as follows

1. HIHs will add a .1 as a suffix to their existing OID to indicate the production environment.
2. The HIH will configure its gateway with the esMD Gateway Production region OID.

Once configurations are complete, the HIH can then fire a test using the test claim and case ID noted in section 6.3, Table 2, of this manual.

### 6.3 Production End-to-End Testing

Tests in this final phase are performed to ensure the HIH's submitted metadata is validated and delivered to the ECM and, ultimately, delivered on to the review contractor. In addition, this testing will ensure that once the review contractor picks up

Commented [A12]: Update

the submitted documents, the notification will be sent back to the HIH regarding the pickup status.

As mentioned previously, this test should be performed using the HIHs application. HIH are requested to use the recipient OID and sample test claim ID and case ID when submitting a test submission.

Please refer to Section 5.3.8 of the esMD Implementation Guide for numeric length for claim and case IDs. When submitting tests, HIHs must use the following numeric digits “8378” to indicate this is a test submission test “as prefix to any claim and case ID. If using the sample format in the Table 1, do not exceed 23 characters for claim ID or 32 characters for case ID.

TEST Claim and TEST Case IDs for End to End Testing in esMD Production			
Review Contractor (RC)	OID	Claim ID	Case ID
TEST RC 1	2.16.840.1.113883.13.34.110.1.999.1	8378CLAIMID<HIH>1	8378CASEID<HIH>1
TEST RC 1	2.16.840.1.113883.13.34.110.1.999.1	8978CLAIMID<HIH>2	8378CASEID<HIH>2

**Table 2: Test Claim and Case IDs for Production Testing**

Upon successful completion of the interoperability and integration testing (i.e., transmission of 100% correctly formed payload and receipt of the two asynchronous responses back from the esMD Gateway) between the HIH and the Production region esMD Gateway, the HIH will officially receive an email notification from QSSI informing them that they are now able to offer esMD services.

### 6.4 Special Considerations

For troubleshooting CONNECT, please visit: [www.connectopensource.org](http://www.connectopensource.org).

### 6.5 Support

**Table 3: Support Points of Contact**

Contact	Organization	Email	Role
esMD Coordinator	QSSI	<a href="mailto:esMDCoordinators@qssinc.com">esMDCoordinators@qssinc.com</a>	Provide assistance to HIH and facilitates the processing of TLS certificate renewals for all HIHs.

Contact	Organization	Email	Role
esMD Helpdesk	QSSI	<a href="mailto:CMSesMDHelpdesk@qssinc.com">CMSesMDHelpdesk@qssinc.com</a>	Handles esMD transaction transport issues for certified HIHs.

## 7. Offboarding Process

This section outlines the steps to off board an HIH who has already completed the process of Onboarding the CMD esMD System. The same steps will apply to an HIH involved in the onboarding process whose Environment Details have already been configured within the CMS esMD Gateway.

### 7.1 Offboarding Procedure

The steps below outline the HIH Off boarding procedure:

1. The HIH will inform the HIH Coordinator of the decision to discontinue utilizing the CMS esMD system.
2. The HIHs Environment Detail configurations will be removed from both the CMS Validation and Production Environments to include the IP address, TLS certificates, and OID.
3. The HIH's organization will be made inactive in the CMS esMD Web Application.
4. The HIHs information and URL will be removed from the CMS Website, brochures, and presentations relating to the CMS esMD Program.

## Acronyms

Table 4: Acronyms

Acronym	Literal Translation
<b>AES</b>	Advance Encryption Standard
<b>CA</b>	Certificate Authority
<b>CMS</b>	Centers for Medicare & Medicaid Services
<b>CSR</b>	Certificate Signing Request
<b>DB</b>	Database
<b>ECM</b>	Enterprise Content Management
<b>esMD</b>	Electronic Submission of Medical Documentation
<b>FIPS</b>	Federal Information Processing Standards
<b>JKS</b>	Java Keystore
<b>HIH</b>	Health Information Handler
<b>HL7</b>	Health Level 7
<b>IP</b>	Internet Protocol
<b>NAT</b>	Network Address Translation
<b>NHIN</b>	Nationwide Health Information Network
<b>NIST</b>	National Institute of Standards and Technology
<b>OID</b>	Object Identifier
<b>PEM</b>	Privacy Enhanced Email (format)
<b>PKCS</b>	Public Key Cryptography Standards
<b>PROD</b>	Production
<b>QSSI</b>	Quality Software Services, Inc.
<b>RC</b>	Review Contractor
<b>XDR</b>	External Data Representation

<b>Acronym</b>	<b>Literal Translation</b>
<b>XML</b>	Extensible Markup Language
<b>SHA</b>	Secure Hash Algorithm
<b>SOAP</b>	Simple Object Access Protocol
<b>TLS</b>	Transport Layer Security
<b>URL</b>	Uniform Resource Locator
<b>VAL</b>	Validation

## Referenced Documents

Table 5: Referenced Documents

Document Name	Document Number and/or URL	Issuance Date
esMD Implementation Guide	<a href="http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Downloads/Release20_esMDImplementationGuide_v42.pdf">http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Downloads/Release20_esMDImplementationGuide_v42.pdf</a>	2013
esMD Implementation Guide	<a href="http://cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Downloads/R_3_0_HIImplementationGuide_V_5_3-508-clean.pdf">http://cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Downloads/R_3_0_HIImplementationGuide_V_5_3-508-clean.pdf</a>	2014

## Record of Changes

**Table 6: Record of Changes**

Version Number	Date	Author/Owner	Description of Change
0.1	8/28/2013	Theresa Howard	Initial Draft
0.2	8/29/2013	Laura Higdon	Updated content
0.3	8/30/2013	Laura Higdon	Correction to 3.8.5
0.4	9/11/2013	Laura Higdon	Addressed Comments
1.0	9/17/2013	Laura Higdon	Finalized
1.1	9/09/2014	Melony Stehlik	Change prefix for Test Claim and Case IDs from "test" to "8378"; provided new OID information for test OID in Validation; Added updated Status and Notifications message diagram in Figure 1; Updated Table 5, Table of Referenced Documents, with new URL for current CMS esMD HIH Implementation Guide; Updated Approval page with CMS' System Approval Authority.  Added HIH Off boarding details.

## Approvals

The undersigned acknowledge that they have reviewed the User Manual and agree with the information presented within this document. Changes to this User Manual will be coordinated with, and approved by, the undersigned, or their designated representatives.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Print Name: Lori Moser  
Title: QSSI – esMD Program Director  
Role: Submitting Organization’s Approving Authority

Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Print Name: LT Joyce Davis  
Title: Health Insurance Specialist  
Role: CMS’ Business Approving Authority

Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Print Name: Edward K. Klein  
Title: System Owner  
Role: CMS’ System Approving Authority

Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Print Name: Braeyon Terry-Connor  
Title: Contracting Officer’s Representative  
Role: CMS Approving Authority