

CMS Issuer Technical Workgroup



✓ ***Housekeeping***

- Webinar Schedule Through July 15th
- CMSzONE Updates
(Updated Data Baseline Specs)
- Updated Help Desk PII Procedures

✓ ***Onboarding for Plan Year 2014***

- EDI Registration Form
(Refresher & Changes)
- EFT Connectivity &
Direct Enrollment Connectivity
- Data Center Migration Activities
This Summer

June 17, 2014

Housekeeping: Enrollment Webinar Schedule through Mid-July

- **Welcome New FFM Issuers!**

- Moving forward we'll differentiate between agenda meetings that affect all 2015 FFM issuers (such as today's focus on onboarding) vs. only existing 2014 FFM issuers

- **Upcoming Sessions**

- Monday, June 23rd Noon E.T.

- Continued update on Enrollment Baseline Initiative and Issues for Existing 2014 FFM Issuers (Register via www.RegTap.info)

- Tuesday, July 1st 3:00 p.m. E.T.

- Brief Highlight of 834 Enrollment Companion Guide for all issuers
- Further details on Data Center Migration activities this summer (Will post updated dial-in on CMSzONE)

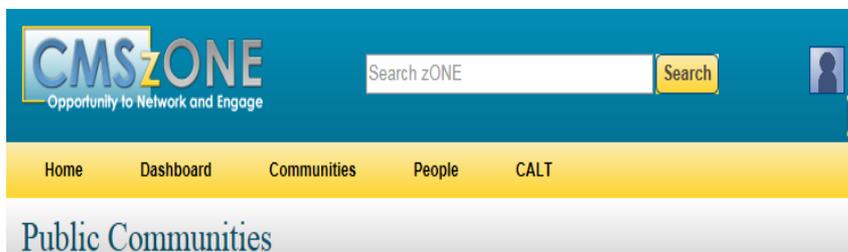
- Monday, July 7th Noon E.T.

- Continued update on Enrollment Baseline Initiative and Issues for Existing 2014 FFM Issuers ((Register via www.RegTap.info)

- Tuesday, July 15th 3:00 p.m. E.T.

- Deep-Dive Walk-Through of 834 Enrollment Companion Guide for all issuers (Will post updated dial-in on CMSzONE)

Issuers New to FFM: CMSzONE Registration Process



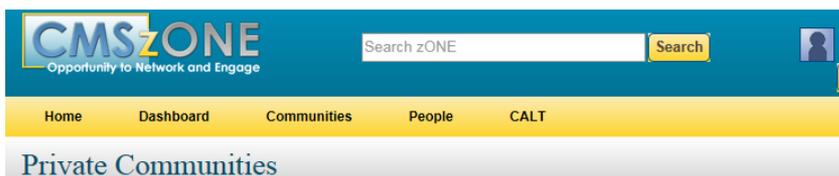
[Browse Private Communities](#)



Filters

Title

| Title | State or Territory | Since |
|-------------|--------------------|--------|
| CMSzONE 101 | Federal | 1 year |



[Browse Public Communities](#)

Filters

Title

Tags

State or Territory

- Any -

Apply

| Title | State or Territory |
|--|--------------------|
| Issuer Community - Private | Federal |
| Web Broker Community | Federal |
| SBM Media Resource Library | Federal |
| Alpha Test Community | Federal |
| DE Agent/Broker Pilot Community | Federal |
| zONE Features and Content Test Community | Federal |
| Sprint 32 Private Hidden for UAT | |

- For CMSzONE Access, e-mail request to CMS_FEPS@cms.hhs.gov and fill out CALT form
- After being granted initial access, log into zONE and click on the Communities tab
- Click Browse Private Communities
- Click on Issuer Community – Private
- Click Join Community
- **Provide explanation for why you need access to this community.**
 - Include name and contact information, issuer POC contacts, and specific work for issuer (i.e. fill out QHP templates, processing 834's, etc.)

CMSzONE Update: Updated Enrollment Data Baselining Specs

The screenshot displays the CMSzONE web application interface. At the top, there is a navigation bar with the CMSzONE logo, a search bar, and a user profile for Daniel Miller_FED_CMS. Below the navigation bar, the page title is "Issuer Community - Private". A secondary navigation bar includes options like View, Edit, Manage, Revisions, Documents, Events, and Wiki. The main content area is divided into several sections:

- Community Information:** Features the CMS logo and an "Unjoin" button. It lists the creation date (Mon, 05/20/2013), the manager (Elaine Stefanou_FC), and the visibility (Private - Accessible only to group members).
- Add Content:** A sidebar menu with options for Documents, Event, and Wiki.
- Members:** Lists members such as Christi Dennhardt_IC and Amanda Walters_FC.
- Description:** Contains the main text of the update, including dates and links to related documents.
- Calendar:** Shows a calendar for June 2014 with a highlighted date (June 17) and a list of events for the month.

- Updated both “Issuer to FFM Inbound Data Baseline IDBL0” and “FFM to Issuer Outbound Data Baseline ODBL0” to Version 5
- Provide courtesy copy of kickoff used with Beta testers

Housekeeping Reminder: To Add (or Remove) Yourself from the CMS Issuer Communication Distribution List

- CMS Issuer Communications distribution list sends courtesy alerts on:
 - Daily IMP1A testing environment status message (~9:30 a.m. E.T.)
 - Alerts on IMP1A outages/reboots (standard testing window is 9:30 a.m. – 8 p.m. ET, except Wednesdays/tomorrow 9:30 – 5:00 p.m.)
 - Deliveries for Enrollment Pre-Audit files, Enrollment Data base lining initiative and other alerts
- To add yourself to the CMS Issuer Communications distribution list:
 - Send an e-mail to CMS_Issuer_Communications@cms.hhs.gov with the exact subject line:
“Add POC to Testing Distribution List”
(Please do not use any other subject line)
 - To remove yourself send an e-mail with the subject line
“Remove POC from Testing Distribution List”
- To add yourself to the Operations Distribution List (separate from the List above):
 - Please provide CMS with one or two email addresses to notify when there are planned system maintenance windows or unexpected outages of the FFM system in production. Please send this information to the Issuer_Registration@cms.hhs.gov mailbox with “Systems notification POC for [company name]” on the subject line.

Help Desk PII Procedures Starting Tomorrow (June 18th) for Existing FFM Issuers

- **Acceptable Data in Help Desk Tickets:**
 - Issuers can send Application ID or Exchange-Assigned Policy ID in the body of an e-mail to CMS_FEPS@cms.hhs.gov so long as it does not include any other PII (such as consumer's name, etc.) Otherwise, please follow the below procedures:
- **Procedures for Issuers Sending PII via Standard E-mail:**
 - Embed the PII in an encrypted attachment requiring a password
 - Input the subject line “Encrypted File – [MMdd/hhmm]”
 - Follow-up with a second e-mail containing password, using the same subject line. Examples:
 - This morning, at 11:07 a.m. Jane Doe sends first e-mail to FEPS with subject line “Encrypted File – 0617-1107” with encrypted file and follows-up with a second e-mail containing the pw, using the same subject line
 - Later this afternoon, around 3:10 p.m. Jane sends second e-mail to FEPS with subject line “Encrypted File – 0617-1510” with encrypted file and follows-up with a second e-mail containing the pw, using the same subject line
 - Issuers must not write “password” or “pw” in the subject line of the e-mail containing the password (i.e. simply repeat the subject line of the initial e-mail)
- **Note on Secure E-mail:** If your organization requires you to send e-mails via Secure, third-party e-mail service that already requires a password for the recipient to access, you do not need to add a separate encrypted attachment. (Otherwise please use the same procedures above for sending passwords via separate e-mail.)
 - If your Secure Email Provider does not allow sending an email using your individual email address, please make sure to include your individual email address along with your other identifying information (e.g. phone number, HIOS Issuer ID, company name, State) within the email.
 - If our teams encounter problems obtaining the required password to open your secure e-mail, we may need to work with you to obtain the information by other means (such as by having a Tier 2 entity contact you directly.)
- **Request on Sending Separate E-mails for Separate Issues:** Please do not combine separate, unrelated issues into the same Help Desk e-mail/ticket; doing so will slow down the response times as different issues are typically routed to different teams for proper troubleshooting and tracked separately.

Trading Partner Form End Dates: Extended to 12/31/2014

- EDI Form contains QHP/QDP End Dates that are starting to expire in early June for some of the issuers and their partners for 2014 QHP IDs.
- CMS is currently updating all the transaction Plan Year 2014 end dates for any forms that were marked to end prior to 12/31/2014 (updating the end date to equal 12/31/2014 in those instances).
- Moving forward, please make sure that any EDI Registration form(s) that your organization updates and submits for the current 2014 plan year has an end date that is equal to 12/31/2014. F
- For Plan Year 2015 product information, the Start Date should be no sooner than 01/01/2015 and End Date information should reflect the 12/31/2015.

Electronic Data Interchange (EDI) Trading Partner



Agenda

- CMS Marketplace EDI Registration Form
 - Review the Technical Data Collection
 - Schedule for Systematic Collection
 - Discussion of Electronic Data Exchange Agreement Section

Question and Answer Review

1. Is EDI 834 Effectuation Test to be in response to an inbound 834 received from CMS?

For Enrollment Integration Phase, yes it will be. Sample files will be used for Connectivity Testing.

2. When do onboarding forms need to be completed?

No, this is the first date CMS will accept the forms; this will be an on-going process.

3. Will there be any instances of Group Enrollment File testing for SHOP?

Yes, SHOP 2014 details are currently being executed at this point but 2015 Group Enrollment File exchanges will be part 2015 SHOP testing.

4. Will CMS provide a central POC for specific detailed questions during the testing process?

Yes, CMS will leverage the Help Desk to triage questions and find the right resource to provide a response. CMS is also looking for trade associations to provide support to their members.

Onboarding Form

Examples of Partner Types can be:
 Issuer,
 State based Exchange,
 Clearinghouse,
 Clearinghouse Vendor Services
 Third Party Administrator

Centers for Medicare and Medicaid Services Marketplace EDI Registration Form

Most Form Types for Issuers
 are either New or Change

SUBMIT

Partner Type* Confirmation Number Form Type* New Change Remove

1) General Information. Do Not Write in Shaded Areas of this Form. Refer to Instructions for Form Completion. This Section Has to be Filled for All Scenarios Including New Registration, Change Registration and Removing a Partner.

| | | | | |
|--|-----------------------|----------------------------------|----------------------|----------------------|
| Legal Business Name of Partner Submitting this Form* | Partner Name* | Tax Payer Identification Number* | | |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | | |
| Street Address Line 1* | Street Address Line 2 | City* | State* | Zip* |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| E-Mail Address* | Phone Number* | | Extension | |
| <input type="text"/> | <input type="text"/> | | <input type="text"/> | |
| Fax Number | Trading Partner ID* | Payee Group Number | Clearinghouse Name | Clearinghouse TPID |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

The trading Partner ID is one of the following configurations:

1. HIOS ID (5 numeric characters only)
2. HIOS ID plus 1 Alphabetic Character (A-Z)
3. Tax ID (9 numeric characters only)
4. Tax ID plus 1 Alphabetic Character (A-Z)
5. Health Plan ID or Other Entity ID (As stated in the Health Plan Identifier Rule 10 Numeric characters)

The Payee Group Number is the preferred grouping related to payment organization to support the Financial Management Aspects of an organization

The Clearinghouse information which links the Issuer to its Business Associate/Contractual partner for the purposes of routing Electronic Data Interchange (EDI) and other payloads

Onboarding Form

Contact Points for:

Security Officer, EDI Administration, Technical Officer, Web Services, Testing, and Production Support.

The **Clearinghouse Contact** information is used only when an organization contracted with a Clearinghouse to route electronic traffic on behalf of the Issuer(s).

2) Contact Information. Refer to Instructions for Form Completion.

| Contact Type | Last Name* | First Name* | Title | E-Mail Address* | Primary Phone* | Secondary Phone | Fax Number |
|-----------------------|------------|-------------|-------|-----------------|----------------|-----------------|------------|
| Security Officer | | | | | | | |
| EDI Admin | | | | | | | |
| Technical Officer | | | | | | | |
| Web Service Contact | | | | | | | |
| Testing Support | | | | | | | |
| Production Support | | | | | | | |
| ClearingHouse Contact | | | | | | | |

3) EDI Transactions List for the Organization. Refer to instructions for Form completion. If the transactions have to be routed / received from other entities than the Partner described in Section 1 (i.e., The Partners will indirectly communicate with CMS through the entities, the Clearing House / Third Party Administrator. The values for these entities needs to be filled).

| EDI Transaction or Service | Version | Reason for Request A/C/D | Start Date | End Date |
|---|--------------|--------------------------|------------|----------|
| 834 – Benefit Enrollment | 005010X220A1 | | | |
| 820 – Remittance Advice | 005010X306 | | | |
| 999 – Functional Acknowledgement | 005010X231A1 | | | |
| 824 – Application Reporting for Insurance (Reserved for Future Use) | | | | |
| Application Error Reporting (XML) | AER | | | |
| Direct Enrollment (Applicant Enrollment Web Services) | AEWS | | | |
| Employer Group Enrollment (SHOP Only) | EGRP | | | |

Onboarding Form

4) List, as appropriate, the Qualified Health Plan Identifier and relationship to the FEIN/OEID.

| Request Type | QHP ID (10 Characters) | Optional Clearinghouse Relationship (FEIN or OEID) |
|----------------------|------------------------|--|
| <input type="text"/> | | |

Add Item

* INCOMPLETE APPLICATIONS WILL BE RETURNED.*

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is [000-000]. The time required to complete this information collection is estimated to average (0) (45) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850.

This Section of the form performs a dynamic add of information to the form on the next slide several QHP/QDP ID linkages are created

Onboarding Form

3) EDI Transactions List for the Organization. Refer to instructions for Form completion. If the transactions have to be routed / received from other entities than the Partner described in Section 1 (i.e., The Partners will indirectly communicate with CMS through the entities, the Clearing House / Third Party Administrator. The values for these entities needs to be filled).

| EDI Transaction or Service | Version | Reason for Request A/C/D | Start Date | End Date |
|---|--------------|---|------------|------------|
| 834 – Benefit Enrollment | 005010X220A1 | Addition <input type="button" value="v"/> | 06/17/2014 | 06/17/2015 |
| 820 – Remittance Advice | 005010X306 | <input type="button" value="v"/> | | |
| 999 – Functional Acknowledgement | 005010X231A1 | Addition <input type="button" value="v"/> | 06/16/2014 | 06/16/2015 |
| 824 – Application Reporting for Insurance (Reserved for Future Use) | | | | |
| Application Error Reporting (XML) | AER | <input type="button" value="v"/> | | |
| Direct Enrollment (Applicant Enrollment Web Services) | AEWS | <input type="button" value="v"/> | | |
| Employer Group Enrollment (SHOP Only) | EGRP | <input type="button" value="v"/> | | |

4) List, as appropriate, the Qualified Health Plan Identifier and relationship to the FEIN/OEID.

| Request Type | QHP ID (10 Characters) | Optional Clearinghouse Relationship (FEIN or OEID) | |
|---|------------------------|--|---|
| Addition <input type="button" value="v"/> | 12345XX001 | | - |
| Addition <input type="button" value="v"/> | 12345XX002 | | - |
| Addition <input type="button" value="v"/> | 12345XX003 | | - |
| <input type="button" value="v"/> | | | - |

Add Item

Addition, Change or Delete of the QHPID to TPID linkages Dropdown

These are only the first ten (10) characters of the Qualified Health/Dental Plan.

DSH On Boarding Summary for Issuers



*Test Environment Access
and Service Details*

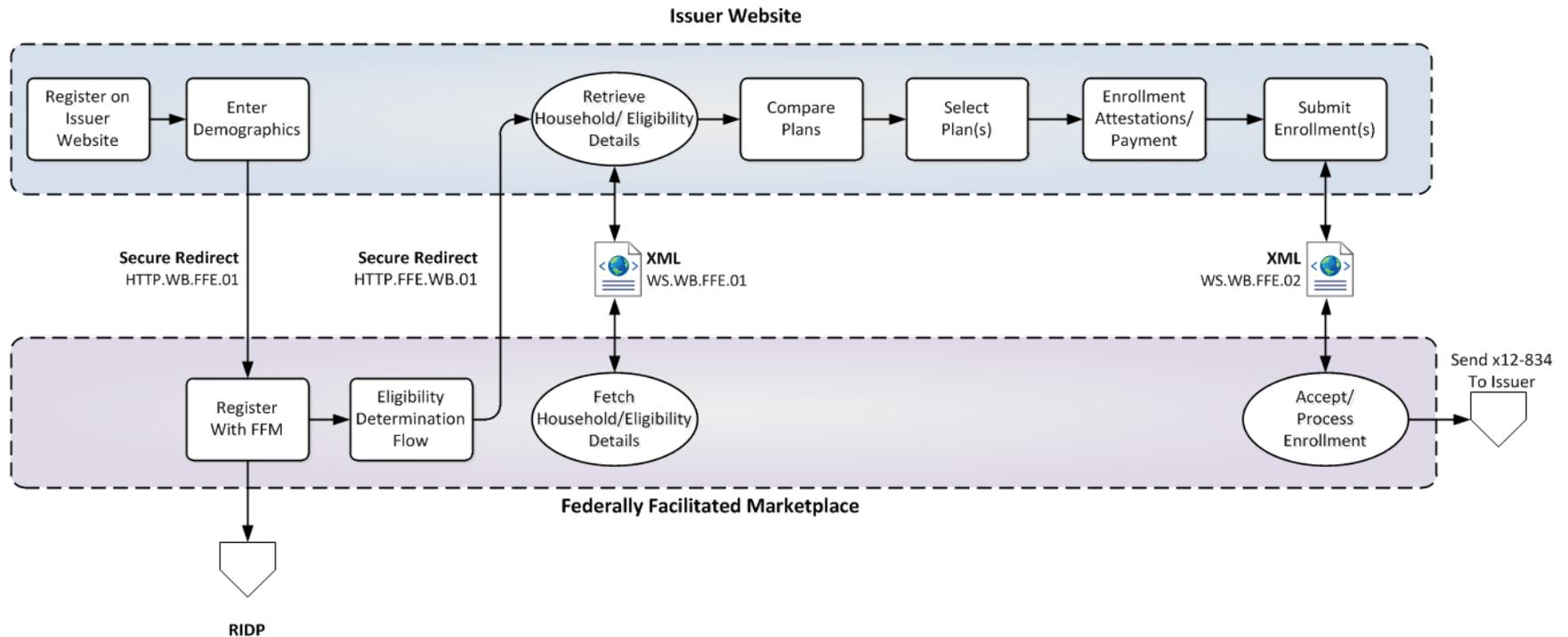
Issuer Overview

- Service Overview
- Steps for Direct Enrollment Web Service Connectivity
- How to obtain a DSH Partner ID

Service Overview

- Secure Redirect
 - Process of a user securely transferred from an issuer website to FFM for eligibility determination purposes and once they complete this function they are securely redirected back to the issuer website for enrollment
- SAML
 - See API spec Section 6.3
- Fetch Eligibility
- Submit Enrollment

Consumer Direct Enrollment Workflow



Current Status of Direct Enrollment

- Direct enrollment is currently on hiatus and cannot process enrollments outside of the annual open enrollment period.
 - Direct enrollment currently cannot process changes in circumstance (CiC) or special enrollment period (SEP) transactions.
- Common questions:
 - When will direct enrollment be available again?
 - Direct enrollment will be able to process enrollments in production on 11/15/14.
 - When will I be able to test direct enrollment?
 - Issuers can currently test both the redirect and fetch eligibility components.
 - We are currently working on the timeframe for issuers to test DE in the Fall in advance of OE 2015; will share ETA in this forum as we progress.
 - Can I still use fetch eligibility in IMP1A?
 - Issuers can use fetch eligibility in IMP1A, although the SEP effective dates are not accurate or reliable.

Steps for Direct Enrollment Web Service Connectivity

- CMS will contact the “Web Services Contact” asking for a SSL Certificate and POC info.
- Issuer and CMS will exchange SSL Certificates and Issuer will obtain a Partner ID.
- CMS will work with the Issuer team to establish connectivity in the Test Environment.
- The Issuer will use the provided soapUI test cases and connectivity instructions to establish initial Federal DSH Test Environment connectivity.
- After soapUI connectivity is established in the Test Environment, Issuers establish connectivity from their application to the Test Environment.

Partner ID Process – Step 1

- **DSH Support will contact “Web Services” Contact requesting additional info once the EDI Form is Approved**
- **Provide the following information in an email:**
 - Organization Name (e.g., ABCD Corp)
 - Web Site URL
 - POC Name
 - POC Email address
 - POC Phone number
 - SSL Certificate file for each environment

Note: The QSSI email server does not accept attachments with the .cer extension. Copy your alias.cer file to alias.txt and attach the alias.txt file. If your organization has trusted CA issued certificate, copy your trusted .cer file to alias.txt and attach the alias.txt file.

Partner ID Process – Step 2

- **Generate SSL Certificates for Application Servers consuming DSH Services**
 - ✓ CA Secured Certificates may be used, but not required for Testing Environment – local certificates are accepted
 - ✓ Production environment required a CA Signed Certificate
- **Respond back to DSH Support with requested info and certificates**

Partner ID Process – Step 3

- **Issuers will receive a response from the DSH Support group with the following details:**
 - Partner HUB ID to be used in the WSSE header
 - End points
 - An attached zip file, which will include the following:
 - Primary and Secondary VeriSign certificates for both of the following
 - DSH Web Service Requests
 - FFM SAML Redirects
 - The public key for the DSH and FFM Gateways
 - A second email will follow with the password.
 - Use the User ID, Password, and Certificate to configure the Transport Layer Security

If you encounter problems with the security certificate steps, please contact QSSI at dsh.support@gssinc.com

Required Skill Sets for FDSH Access

Issuer companies should have the following skills and experience to connect to the Federal Data Services Hub (FDSH):

- System integration experience in consuming Simple Object Access Protocol (SOAP)-based services, including the following:
- Familiarity with Web Services Description Language (WSDL) and Extensible Markup Language (XML) Schema Definitions (XSDs)
- Experience with Web Services Security (WS-Security) Headers
- Experience with Transport Layer Security (TLS)
- Familiarity with X.509
- Business Analyst (BA)/Interface Analyst skills
- Network Security Administration skills

Direct Enrollment Documentation Available in CMS zONE

- Direct Enrollment API Specification Document
- System Concept Document
- Approved Direct Enrollment Changes Doc (XSL Change doc)
- Direct Enrollment Application Eligibility Mapping
- Direct Enrollment Application Enrollment Mapping
- Enrollment ICD for Direct Enrollment
- Direct Enrollment Application IEPD. This includes: Applicant Enrollment request and response XMLs, Extensions, Schema and WSDLs.
- Agent Broker and DE Testing Guide
- APTC ppt
- Error Code

Data Center Migration Overview



Data Center Migration Overview This Summer

CMS data center will migrate from Terremark (TM) data center to Hewlett Packard (HP) data center. This migration will take place on the following date; formal testing environment 8/1 and production environment 8/18.

Summer change due to lower traffic periods and to provide time to test in order to be ready for Open Enrollment 2015

Requirements

- Issuer Requirements
 - Issuers shall test the following hosted services with CMS / Regional Technical Support:
 - Fetch Eligibility (H67)
 - Direct Enrollment (H68)
 - Hub Connectivity Service (H74 – TBD)
 - Implementation of new IP address (IP address will be used till cutover date)
 - Testing of new connection
 - Cut over to new environments
- Formal environment
 - Issuers shall be connected to the HP environment by 8/1/14.
- Production environment
 - Issuers shall be connected to the to the HP environment by 8/18/14.
- No IV&V requirements

Timelines

- Current timeline for the following FDSH environments to migrate from TM to HP
 - Formal (8/1)
 - Informal (8/10) (*Tentative*)
 - Production (8/18)
- Testing Timelines
 - Formal (7/1-7/31)
 - Informal (7/15-8/9) (*Tentative*)
 - Production (8/1-8/17)
- Requirements
 - Implementation of new IP address (IP address will be used till cutover date)
 - Testing of new connection
 - Cut over to new environments

Testing with Regional Technical Support – Issuer Connections to DSH

- Issuer testing with DSH Support
 - All IP addresses require to be updated due to the data center migration
 - Issuers will test new connections with Regional Technical Support
 - Regional Technical Support will track testing and provide feed back to CMS
- Issuers shall do the following testing to validate the connection to the new data center environments
 - IMP1A Test connections
 - Prior to IMP1a cutover, test connection using IP address (rather than URL) to access service endpoint (e.g – instead of invoking <https://impl.hub.cms.gov/Imp1/>, Issuers would invoke https://<ip address>/Imp1/to confirm connectivity to HP Environment (actual IP address to follow)
 - Test would invoke a full end-to-end test
 - May use updated DSH IMP1A Certificate (Issuers will be provided a temporary cert for testing good till 8/1)
 - Issuers will likely need to update firewall settings to support HP IMP1A Connection
 - After IMP1A cutover, issuers would test connection to current end points to confirm HP connectivity (e.g. <https://impl.hub.cms.gov/Imp1/>)
 - Prod Connections
 - Prior to Production Cutover, test connection to HP production environment by using the DSH Hub Connectivity Service using the IP address (https://<ip address>/HubConnectivityService – actual IP address to follow)
 - May use updated DSH Production Certificate (Issuers will be provided a temporary cert for testing good till 8/18)
 - After Production cutover, issuers will call existing endpoints to confirm HP Connectivity (<https://hub.cms.gov/HubConnectivityService>)

Production Activities

- CMS will update the DNS address with new IP address for the current URLs the date of the migration
- HP will provide a new certificate for `hub.cms.gov` to be effective on the cutover date (targeted for 8/18)
- The temporary cert used for testing the new production HP environment will become invalid on the cutover date

For additional onboarding questions we don't answer in the remaining time today...

- Please e-mail CMS_Issuer_Communications@cms.hhs.gov with the specific subject line “Onboarding Question”
- While we will not respond by e-mail individually, we will collect these and provide FAQ's to common questions in upcoming sessions (such as July 1st)

Questions



Appendix: DSH Web Services Testing Connectivity



*Test Environment Access
and Service Details*

Accessing Web Services

- WS Security Standards for performing testing of DSH Web services
- Assumptions and Recommendations for effective testing
- Generating Certificate and Keystore for Connectivity
- Initial setup of SoapUI configurations to successfully test DSH Services

Important URLs

| Production URL Info | |
|---|-------------------------|
| Web Service Endpoint | |
| https://hub.cms.gov/ApplicantEnrollmentService | (Applicant Enrollment) |
| https://hub.cms.gov/ApplicantEligibilityService | (Applicant Eligibility) |
| Secure Redirect URL | |
| https://www.healthcare.gov/marketplace/brokerService | |
| IMP1A Testing URL Info | |
| Web Service Endpoint | |
| https://impl.hub.cms.gov/Imp1/ApplicantEnrollmentService | (Applicant Enrollment) |
| https://impl.hub.cms.gov/Imp1/ApplicantEligibilityService | (Applicant Eligibility) |
| Secure Redirect URL | |
| https://imp1a.healthcare.gov/marketplace/brokerService | |
| Akamai Cookie URL | |
| https://imp1a.healthcare.gov/?ACA=9Ym7jwMU5DkLp | (sets English cookie) |
| https://imp1a.cuidadodesalud.gov/?ACA=26vzLHbgNnkD | (sets Spanish cookie) |
| <p>Note you may encounter “Access Denied” when redirecting, but this can be fixed by first opening the Akamai cookie URL, to load the cookie into your browser session, then proceeding to the Secure Redirect URL. Additionally you may get an “Access Denied” error message upon logging out of IMP1A. However, this does not affect your testing and you can simply log in. (Error is unique to IMP1A; please do not report to the Help Desk.) Please alert your respective testing teams.</p> | |

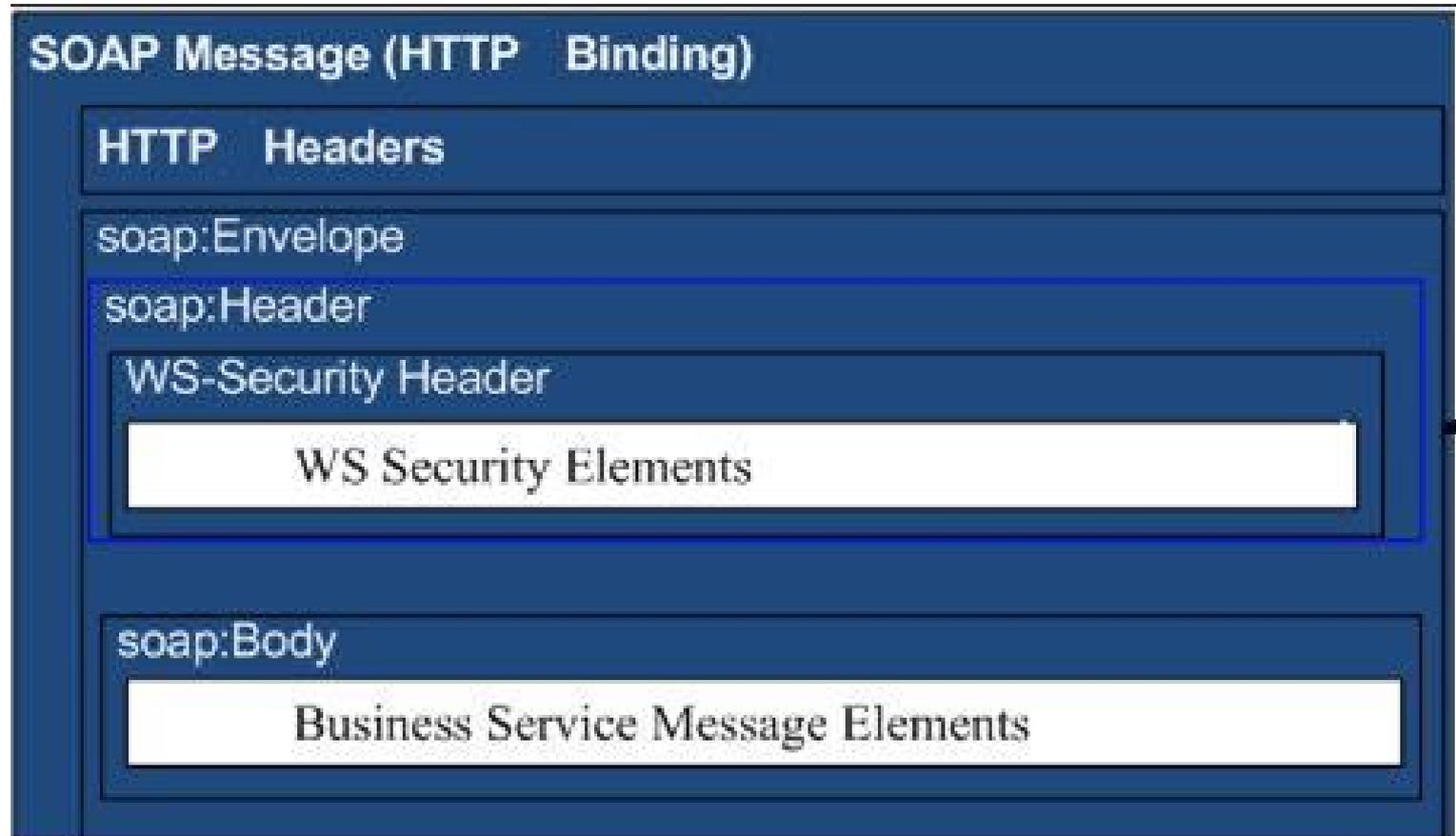
**SoapUI Project on zONE:
IMP1A**
<https://zone.cms.gov/document/imp1a-issuer-soapui-projects>

WS Security Standards

Required security standards to perform testing of the DSH Secure Web service are as follows:

- Web Services Security (WS-Security) v1.1
- WS Security UserNameToken Profile 1.1
- Password Hashing Algorithm: Base64 encoded, SHA-1
- SOAP Version 1.2
- TLS v1.2 (HTTP)
- Each request must have a WS-Security header that has a
 - Username (HUB Partner ID)
 - Password (Password Digest Type)
 - Timestamp (5 min recommended)
- The Hub services' client authentication is password-based.
- The Hub and FFM use Unicode Transformation Format (UTF)-8 for character encoding of all messages.
- When there is no data to return, the FFM omits the element in its response for optional XML elements.

WS Security Standards



Certificates and Keystore

- DSH Support sent your POC two sets of Certificates for each environment (Prod/IMP1A)
 - “hub.cms.gov” & “impl.hub.cms.gov” are the HUB Web Services Public Certs
 - “app.prod.healthcare.gov” & “app1a.imp.healthcare.gov” are for the SAML Redirect
- Keystore can be .jks/.p12/.pfx format and contain
 - Private Key (matches the public cert sent to DSH Support)
 - HUB Public Cert matching the environment (This cert is not needed in the keystore if you have it loaded to your system TrustStore)

Assumptions

Assumptions for configuring soapUI DSH Web services for security testing are as follows:

- Experience in using soapUI or soapUI PRO.
- soapUI project is already present in the tester's workspace.
- soapUI project downloaded from zONE
- Windows XP or higher as the operating system.
- JDK 1.6 installed on the tester's machine.
- JDK 1.6 and Java binaries are set in the PATH variable.
- Familiarity using WSSE elements in the SOAP header message within soapUI.

- SoapUI Projects on zONE:
 - IMP1A
 - <https://zone.cms.gov/document/imp1a-issuer-soapui-projects>

Recommendations

The list of recommendations before running the DSH Secure Web service tests is as follows:

- Issuers/Brokers should make an effort to resolve the setup issues by contacting experts within the organization prior to contacting the DSH Support group.
- Use the same current working directory for all command prompt items.
- An effective technique to work through application connectivity issues is for Partners to create mock services on their application environment. The general flow for this approach is:
 - Partners establish successful soapUI connectivity with the FDSH service, using the FDSH provided test scenarios.
 - If the state experiences issues connecting their application to the FSDH service, they create a mock service that simulates the service's request payload.
 - Partners may then compare the payload sent from their application with the successful payload used in the soapUI tests, isolate the payload differences, and make appropriate changes in their application and middleware connectivity.

Generate Local Certificate for IMP1A Testing (OPTIONAL)

You can generate a Local Certificate or provide a CA Signed Certificate for IMP1A Testing

The steps to generate the local certificate are as follows:

1. Type `keytool -genkeypair -alias alias -keyalg RSA -validity 365 -keystore keystore.jks` in the command prompt window.
2. When prompted, select a password for your certificate. Be sure to avoid personal passwords.
3. In the **First and Last name** field, enter the *Organization*
4. Enter the *name of your organization unit*
5. Enter the *city, state, and country*.
6. Enter "yes" to import certificate into keystore
7. Press *ENTER*.

The steps to export your Public Cert to send to DSH Support:

1. `keytool -export -keystore keystore.jks -alias alias -rfc -file PublicCert.txt`

The steps to import the HUB Public certificate to your keystore are as follows:

1. Type `keytool -import -alias aliasname -file CertName.cer -keystore keystore.jks`
2. When prompted, enter a password.

Note :

- Ensure your current working directory has the three unzipped certificates.
- For ease of maintenance, use the same password created for the local certificate.
- The keystore will be stored in the current working directory. Be sure to make a note of the location.

Sharing the Security Certificate within the Organization

- Share the following items within your organization:
 - Keystore file. Keystore can be either pfx, p12 or jks, but it must include the Private Key that matches the Public Cert sent to DSH Support to load to the Gateway. The HUB and FFM Public certs that were sent back to you should be loaded to your Gateway.
 - The password created for the keystore file.
 - The user id and password received from the DSH Support group.
 - The endpoint received from the DSH Support group.

Configure soapUI for Outgoing Security

The steps to configure soapUI for the outgoing security are as follows:

1. Double-click the root node of a soapUI project (i.e. Applicant Eligibility).
2. Click *WS-Security Configuration* and select the *Outgoing WS-Security Configuration* tab.
3. Click the “+” sign under the Outgoing WS-Security Configuration tab to add Outgoing Configuration.
4. Enter a name for configuration (e.g., Outgoing).

The steps to configure the username and WSS entry are as follows:

1. Click the “+” sign on the bottom right tab to add the WSS entry.
2. Select the user name from the drop-down and click *OK*.
3. Enter the Partner ID and Password received from the DSH Support.

Note: Select *PasswordDigest* for the Password Type.

The steps to configure Timestamp WSS entry are as follows:

1. Click the “+” sign on the bottom right tab to add another WSS entry.
2. Select *Timestamp* from the drop-down and click *OK*.
3. Enter *60* in the Time to Live box.

Note: The soapUI tool should be configured to include the outgoing elements in the WS Header.

Configure soapUI for Outgoing Security (cont.)

The figure below shows the tabs and areas used in configuring soapUI for the Outgoing Security.

The screenshot shows the soapUI interface for configuring outgoing security. The 'WS-Security Configurations' tab is selected. Within this tab, the 'Outgoing WS-Security Configurations' sub-tab is active. A table lists configurations, with 'imp1a' selected. The configuration details for 'imp1a' are shown below the table, including fields for Username, Password, and options for adding nonces and timestamps.

| Name | Default Username/Alias | Default Password | Actor | Must Understand |
|-------|------------------------|------------------|-------|--------------------------|
| imp1a | | | | <input type="checkbox"/> |

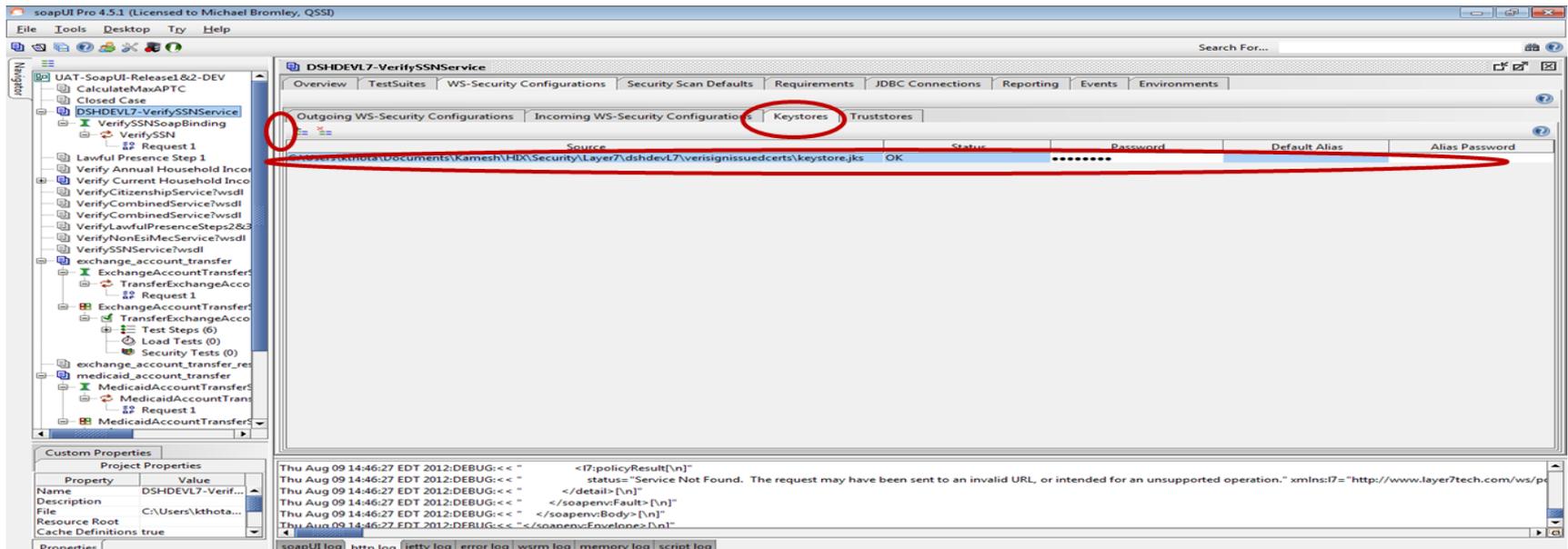
| | | |
|-----------|----------------|--|
| Username | Username: | <input type="text"/> |
| Timestamp | Password: | <input type="password"/> |
| | Add Nonce: | <input checked="" type="checkbox"/> Adds a nonce |
| | Add Created: | <input checked="" type="checkbox"/> Adds a created |
| | Password Type: | PasswordDigest |

Configure soapUI for Keystores/Certificates

The steps to configure soapUI for keystore/certificates are as follows:

1. Click on the *Keystores/Certificates* tab.
2. Click the “+” sign under the Outgoing WS-Security Configuration tab.
3. Navigate to the folder with the keystore file, and select *keystore.jks*.
4. When prompted, enter the password created while generating the keystore.jks file.

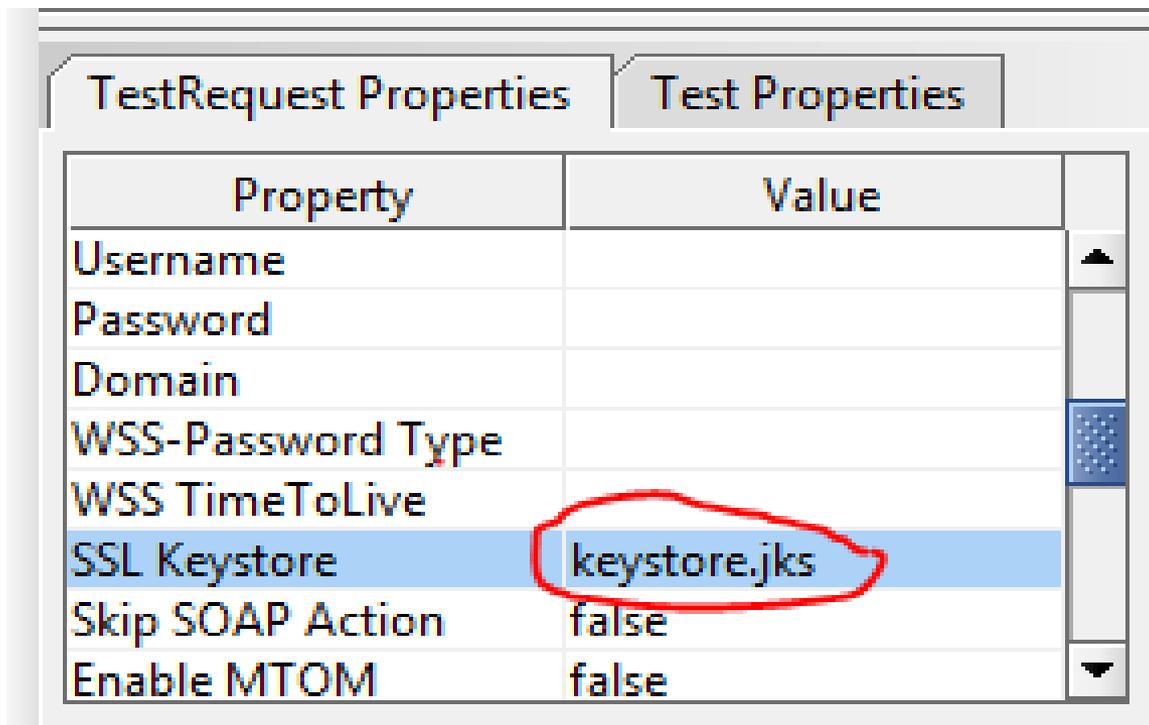
The figure below shows the tabs and areas used in configuring soapUI Keystores/Certificates.



Configure soapUI Test Request Properties

The steps to configure the soapUI test request properties are as follows:

1. Double-click the Test Step to open a Request/Response window on the right side.
2. Click the *TestRequest Properties* tab on the bottom right side.
3. Scroll down to select the *SSL Keystore* property and *keystore.jks* from the drop-down.



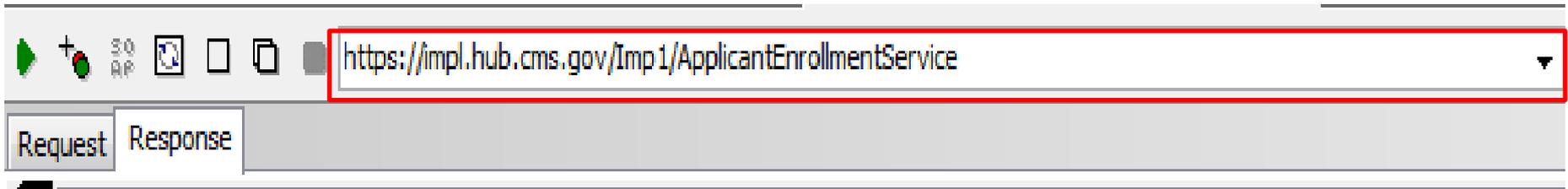
| Property | Value |
|-------------------|--------------|
| Username | |
| Password | |
| Domain | |
| WSS-Password Type | |
| WSS TimeToLive | |
| SSL Keystore | keystore.jks |
| Skip SOAP Action | false |
| Enable MTOM | false |

Configure soapUI Endpoint

The steps to configure the soapUI endpoint to use the DSH Gateway endpoint area are as follows:

1. Click the endpoint drop-down and select *Add New Endpoint*.
2. Enter the endpoint from the email, and click *OK*.

Note: You should have received the endpoint in an email from the DSH Support.

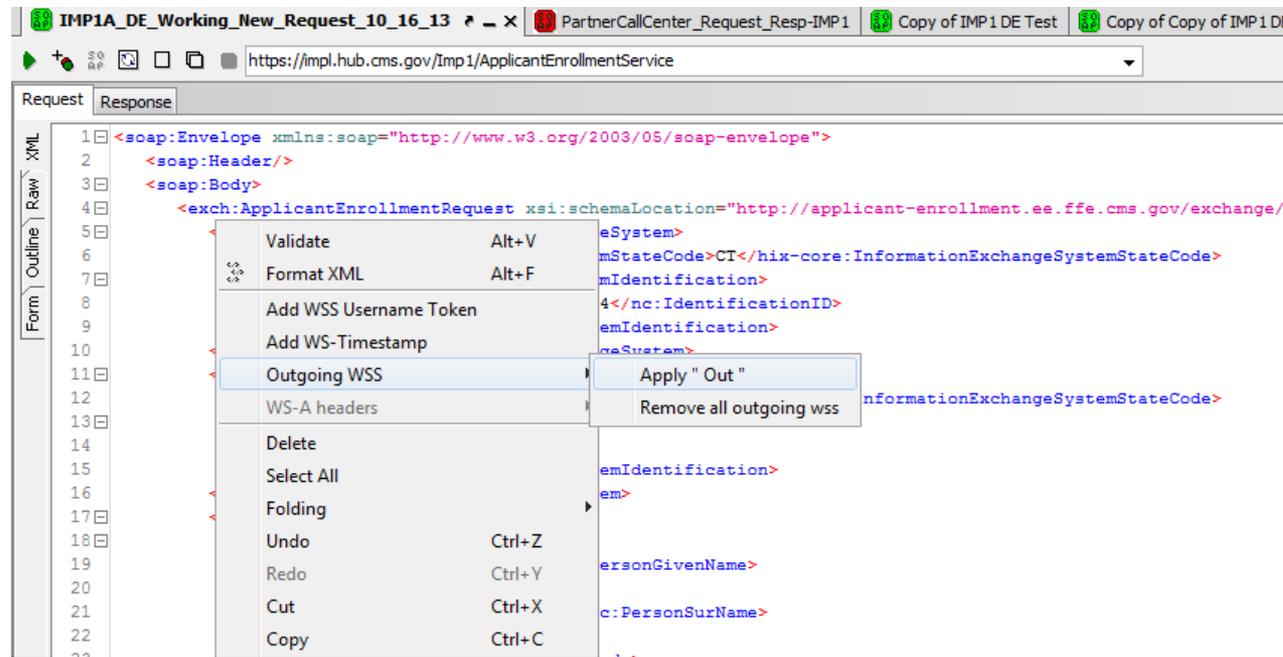


Configure soapUI to Add WS Security Header

The steps to configure soapUI to add WS security header are as follows:

1. Select the *Request* tab, right click, select *Outgoing WSS*, then select *Apply "Name of Outgoing WSS"*

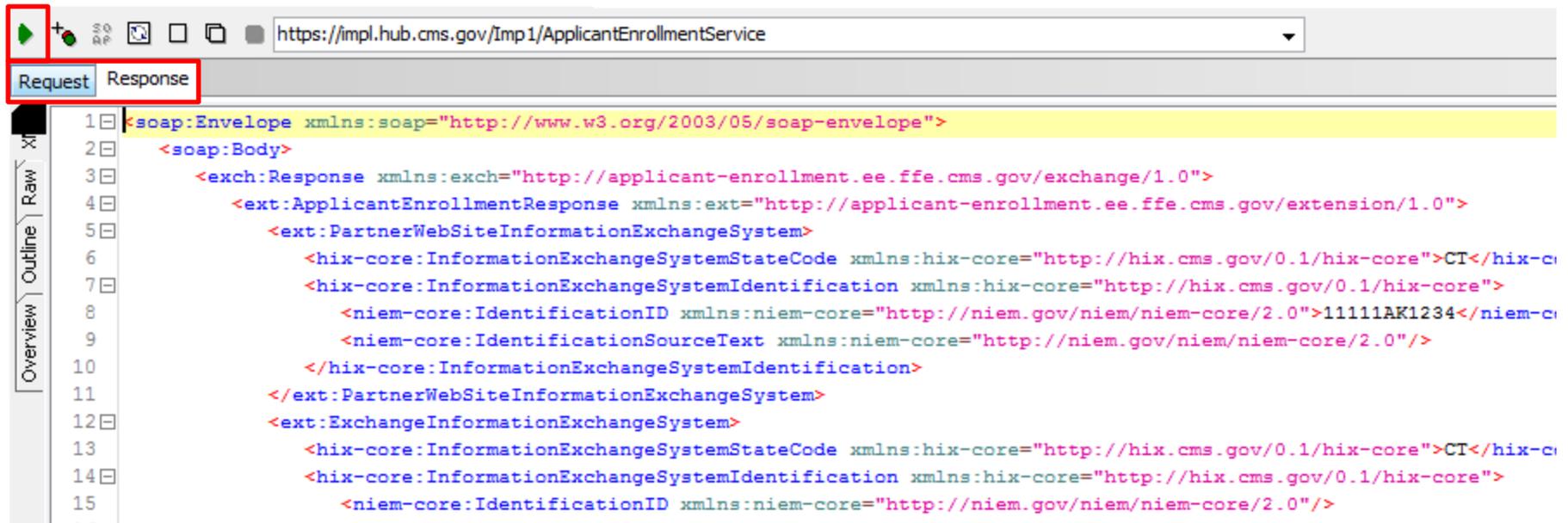
Note: This will insert the WSSE:Security tag in the SOAP header.



2. Press *Alt+F* to reformat the newly inserted information to make it readable.
3. Run the test.

soapUI Security Test

Submit the SoapUI Request Payload. You should receive a Response Payload from the Hub.



The screenshot shows the SoapUI interface with the URL `https://impl.hub.cms.gov/Imp1/ApplicantEnrollmentService` in the address bar. The 'Request' tab is selected, and the response payload is displayed in the main area. The payload is a SOAP envelope containing an exchange response with partner website information and exchange system details.

```
1 <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
2   <soap:Body>
3     <exch:Response xmlns:exch="http://applicant-enrollment.ee.ffe.cms.gov/exchange/1.0">
4       <ext:ApplicantEnrollmentResponse xmlns:ext="http://applicant-enrollment.ee.ffe.cms.gov/extension/1.0">
5         <ext:PartnerWebSiteInformationExchangeSystem>
6           <hix-core:InformationExchangeSystemStateCode xmlns:hix-core="http://hix.cms.gov/0.1/hix-core">CI</hix-c
7         <hix-core:InformationExchangeSystemIdentification xmlns:hix-core="http://hix.cms.gov/0.1/hix-core">
8           <niem-core:IdentificationID xmlns:niem-core="http://niem.gov/niem/niem-core/2.0">11111AK1234</niem-c
9           <niem-core:IdentificationSourceText xmlns:niem-core="http://niem.gov/niem/niem-core/2.0"/>
10          </hix-core:InformationExchangeSystemIdentification>
11        </ext:PartnerWebSiteInformationExchangeSystem>
12        <ext:ExchangeInformationExchangeSystem>
13          <hix-core:InformationExchangeSystemStateCode xmlns:hix-core="http://hix.cms.gov/0.1/hix-core">CI</hix-c
14          <hix-core:InformationExchangeSystemIdentification xmlns:hix-core="http://hix.cms.gov/0.1/hix-core">
15            <niem-core:IdentificationID xmlns:niem-core="http://niem.gov/niem/niem-core/2.0"/>
```

Retest

Points to remember before retesting are as follows:

1. The WS Security feature uses a timestamp that expires after the time you setup in WSS timestamp configuration. The HUB allows up to 5 minutes.
2. Refresh the WS Security information if you want to re-test the same service after 60 seconds.
3. Right-click *Request*, select *Outgoing WSS*, and select *Remove All Outgoing WSS*. This will remove all WS security information.
4. Right-click *Request*, select *Outgoing WSS*, and select *Apply Outgoing*. This will add WS security information.
5. Press *Alt+F* to auto format the newly inserted information.
6. Run the test.

Web Services Sample Requests

SAMPLE RAW Fetch Eligibility Request (PendingEffectuation Response)



Applicant Eligibility Request Sample IMP1A.txt

SAMPLE RAW Submit Enrollment Request (InvalidMember Response)



Applicant Enrollment Request Sample IMP1A.txt