



**Centers for Medicare & Medicaid Services (CMS)**  
**7500 Security Boulevard**  
**Baltimore, MD 21244-1850**

---

**HIPAA Eligibility Transaction System (HETS)**  
**Submitter SOAP/MIME Connectivity Instructions**

---

**Version: 8.0**  
**Last Modified: May 2025**

**Document Number: SYS-9005**

## Table of Contents

1. Introduction .....	1
2. Authentication and Authorization Handling .....	3
2.1 X.509 Digital Certificates .....	3
2.1.1 DigiCert.....	4
2.1.2 Entrust .....	4
2.1.3 IdenTrust .....	4
2.2 Overall HETS Web Services Security Policy .....	5
3. SOAP .....	6
3.1 SOAP Data Requirements.....	6
3.1.1 SOAP Digital Signature.....	7
3.2 SOAP Examples .....	8
4. MIME .....	14
4.1 MIME Data Requirements .....	14
4.2 MIME Examples .....	15
5. Common Error Processing for SOAP and MIME .....	19
5.1 HTTP Status and Error Codes .....	19
5.2 CORE Envelope Processing Status and Error Codes .....	19
5.3 SOAP Specific Processing Errors .....	19
5.4 SOAP and MIME Transaction (X12) Error Processing .....	19
6. General Onboarding Checklist.....	20
Appendix A: HETS Web Services Security Policy.....	21
Appendix B: Frequently Asked Questions.....	25
Appendix C: References.....	28
Appendix D: Acronyms.....	29
Appendix E: Glossary of Terms .....	31
Appendix F: Revision History.....	33

**List of Figures**

Figure 1. HETS 270/271 Communication Process .....2

**List of Tables**

Table 1. Required Body Elements for 270 Requests Using SOAP .....7  
 Table 2. Required Body Elements for X12 Responses Using SOAP .....7  
 Table 3. SOAP Request Message Structure ..... 8  
 Table 4. SOAP Response Message Structure ..... 11  
 Table 5. Required Body Elements for 270 Requests Using MIME..... 14  
 Table 6. Required Body Elements for X12 Responses Using MIME..... 15  
 Table 7. MIME Request Message Structure ..... 16  
 Table 8. MIME Response Message Structure..... 17  
 Table 9. Envelope Process Status and Errors..... 19  
 Table 10. SOAP Specific Processing Errors ..... 19  
 Table 11. General Onboarding Checklist .....20  
 Table 12. Frequently Asked Question.....25  
 Table 13. References ..... 28  
 Table 14. Acronyms .....29  
 Table 15. Glossary of Terms .....31  
 Table 16. Revision History.....33

## 1. Introduction

---

This document provides information on how to connect to the Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) 270/271 application using support of Simple Object Access Protocol + Web Services Description Language envelope standards (SOAP+WSDL) and support of Hypertext Transfer Protocol/Multipurpose Internet Mail Extensions (HTTP/MIME) Multi-part envelope standards. The SOAP and MIME protocols are offered in addition to the Centers for Medicare & Medicaid Services (CMS) Extranet connection. HETS Trading Partners will have the option of using any of the available connection methods to submit and receive eligibility data. The HETS 270/271 application will continue to only accept real-time transactions.

The Department of Health and Human Services (HHS) has named the Council for Affordable Quality Healthcare/Committee on Operating Rules for Information Exchange (CAQH/CORE) the authoring entity of the Operating Rules mandated under the Patient Protection and Affordable Care Act (ACA). The HETS 270/271 follows the federally mandated Phase I CORE 153: Eligibility and Benefits Connectivity Rule and the Phase II CORE 270: Connectivity Rule. For a copy of these federally mandated Operating Rules, please refer to <https://www.caqh.org/core/operating-rules>

Specifically, HETS 270/271:

- Supports SOAP/MIME protocol and associated errors
- Requires Trading Partners transmitting with SOAP or MIME to obtain a digital certificate and send the transaction to the HETS 270/271 application via a secure internet connection
- Requires Trading Partners to maintain annual renewal requirements of the Trading Partner Agreements (TPA) and SOAP or MIME digital certificate

It is important to note that this document is intended for use by a technical professional who has experience implementing secure, web-based connectivity.

The HETS 270/271 application authenticates the Trading Partner via a unique HETS 270/271 Submitter ID and ensures that the Trading Partner is associated with valid National Provider IDs (NPIs) in the HETS database. If the Trading Partner is not authorized, or is not associated with valid NPIs, then the appropriate X12 error response is returned. Please refer to the HETS Companion Guide found in the 'Downloads' section on the HETS Help website (<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index.html>) for the errors returned in the above situations.

Before submitting a 270 request to the HETS 270/271 application, the Submitter must ensure that all valid Submitter ID (SID) Number and NPI (SID/NPI) relationships have been added under their new Web Submitter ID in the HETS Desktop (HDT). A Web Submitter ID indicates the Submitter has been set up to submit 270 requests to the HETS 270/271 application using SOAP or MIME. Existing Clearinghouse Submitters that have access to batch NPI Management can perform actions (query, add, and/or terminate) for multiple NPIs at one time through batch file functionality. They can use the same HDT user account, mailbox number, and file naming convention that they use for their non-Web Submitter IDs. Submitters should ensure that when submitting the HDT Batch file, they include their Web Submitter ID rather than their

non-Web Submitter ID. All other Submitters should set up their individual SID/NPI relationships via HDT. The user manual for the HDT application can be found at the following link:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index.html>

Figure 1 illustrates the high-level process for communicating with the HETS 270/271 application. The lock icons represent system checkpoints that must be passed before eligibility information is returned on the 271 response.

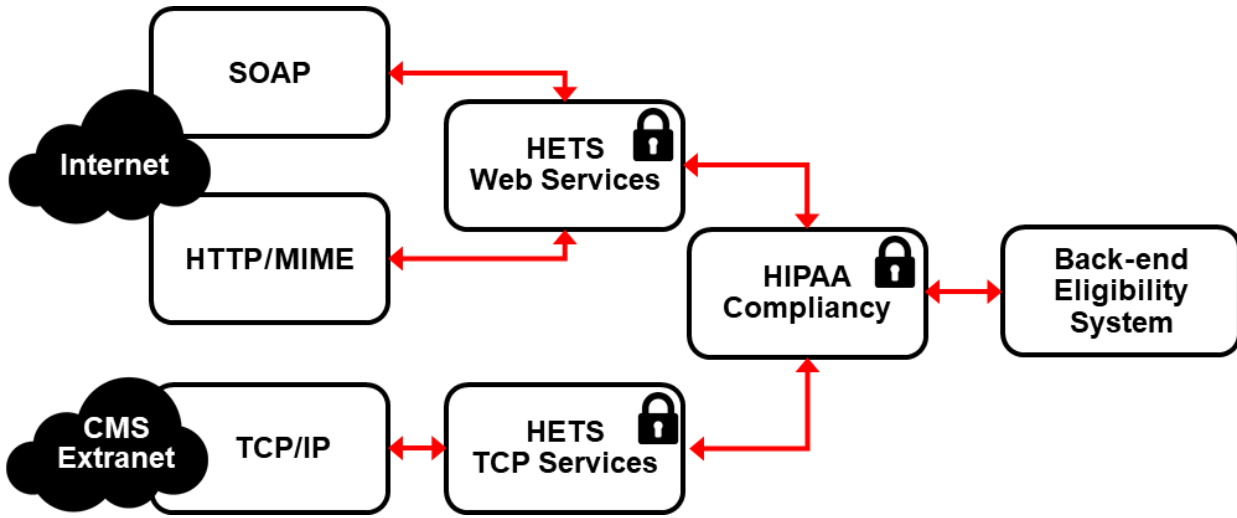


Figure 1. HETS 270/271 Communication Process

## **2. Authentication and Authorization Handling**

---

To connect to the HETS 270/271 application via SOAP or MIME, Trading Partners shall authenticate with an X.509 Digital Certificate using the Transport Layer Security (TLS) 1.2 open standard for client certificate-based authentication. TLS 1.2 is required for compliance per the federally mandated National Institute of Standards and Technology (NIST) Special Publication NIST SP 800-52 Rev.2 <https://csrc.nist.gov/pubs/sp/800/52/r2/final>

The Trading Partner's originating IP address will be verified by CMS prior to allowing the 270 inquiry through to the HETS 270/271 application. Note that the Trading Partner's originating IP address must be an address from the organization's Production (not Testing) environment. Also note that the supplied Trading Partner originating IP address must be a public address and listed on the Trading Partner's Trading Partner Agreement (TPA).

### **2.1 X.509 Digital Certificates**

The information provided in the following steps should allow the Trading Partners to locate proper digital certificates for HETS connectivity. Trading Partners will need to generate a Certificate Signing Request (CSR) to obtain the digital certificate for their organization. The CSR generation process is platform specific. Please review the CSR generation process for your Certificate Authority (CA) carefully, as shown in the links found in the following three subsections and contact the CAs directly in order to obtain the digital certificate. CMS requires that all Trading Partners using SOAP or MIME use a SHA2-256 digital certificate.

The Trading Partners will need to procure a digital certificate from one of the following CAs detailed in sections 2.1.1 through 2.1.3 to allow their infrastructure to connect to the HETS servers. Information on certificate procurement and platform-specific CSR generation processes can be found on each CA's webpage. Links to their home pages are provided in sections 2.1.1 - 2.1.3.

The digital certificate obtained by the Trading Partner must be provided to CMS in advance by contacting the Medicare Customer Assistance Regarding Eligibility (MCARE) Help Desk during the onboarding process.

#### **MCARE Contact Information:**

Monday to Friday 7:00 am to 7:00 pm ET

1-866-324-7315

[MCARE@cms.hhs.gov](mailto:MCARE@cms.hhs.gov)

MCARE will verify the digital certificate as well as the HETS Trading Partner Agreement and initiate the process to properly configure Trading Partner access to the HETS system. The same digital certificate is also required for digitally signing the SOAP message timestamp and payload fields as specified in Section 3.1.1. The SOAP response will also be digitally signed by CMS for authenticity of the message.

Trading Partners that acquire a new Digital Certificate for HETS 270/271 SOAP or MIME MUST provide a copy of the new Digital Certificate to CMS by contacting MCARE. The Trading Partner will also be required to complete an updated [HETS Trading Partner Agreement](#) that includes the new Digital Certificate details. In order to ensure an uninterrupted transition, CMS requires that

Trading Partners begin this process at least 30 days prior to the expiration of the existing Digital Certificate.

### 2.1.1 DigiCert

Information on digital certificates provided by DigiCert can be found using the following link: <http://www.digicert.com>

Digital certificates issued by the following DigiCert Intermediate certificates are accepted:

- DigiCert SHA2 Assured ID CA
- DigiCert SHA2 Secure Server CA
- DigiCert EV RSA CA G2<sup>1</sup>
- DigiCert SHA2 High Assurance Server CA
- DigiCert Assured ID CA G2
- DigiCert Global CA G2

### 2.1.2 Entrust

Information on digital certificates provided by Entrust can be found using the following link: <https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificates>

Digital certificates issued by the following Entrust Intermediate certificates are accepted:

- Entrust Certification Authority – L1K
- Entrust Certification Authority – L1M

### 2.1.3 IdenTrust

Information on digital certificates provided by IdenTrust can be found using the following link: <https://www.identrust.com/digital-certificates/tlsssl-website-security>

Trading Partners should ensure that they obtain an Organization Validated (OV) digital certificate from IdenTrust.

Digital certificates issued by the following IdenTrust Intermediate certificates are accepted:

- Root CA: IdenTrust Commercial Root CA 1
- Intermediate CA: TrustID Server CA O1

---

<sup>1</sup> DigiCert replaced their DigiCert SHA2 Extended Validation Server CA certificate with the DigiCert EV RSA CA G2 certificate on March 8, 2023. Previously issued DigiCert SHA2 Extended Validation Server CA certificates will continue to be accepted through that certificate's valid dates.

## 2.2 Overall HETS Web Services Security Policy

HETS Web Services Security Policy assertions use both transport level and message level security bindings. The information provided for Transport Level Security applies to SOAP and MIME requests. The information provided for Message Level Security applies only to SOAP.

### Transport Level Security (Transport Binding) – SOAP and MIME

- Create an SSL connection using an RSA 2048-bit certificate
- CMS requires TLSv1.2 and supports the following cipher suites:
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
  - TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

### Message Level Security (Asymmetric Binding) – SOAP ONLY

- Digitally sign the timestamp and payload using an RSA-SHA256 signature algorithm.
- Include a Binary Security Token inside the Web Services Security Header
- Include a TimeStamp node in the Web Services Security Header

## 3. SOAP

---

The HETS 270/271 application supports transactions formatted according to SOAP Version 1.2, conforming to standards set forth by WSDL for Extensible Markup Language (XML) envelope formatting, submission, and retrieval. The X12 payload data MUST be embedded using the inline method (Character Data (CDATA) element), the XML schema, and WSDL definitions formatted according to the Phase II CORE 270: Connectivity Rule. The following key resources should be used as reference:

- SOAP XML Schema
- WSDL Schema
- Phase II CORE 270: Connectivity Rule

These resources are available for download via the following website:

[CAQH CORE – Committee on Operating Rules for Information Exchange](#)

HETS 270/271 Submitters connecting via SOAP will need to use a specific URL to access HETS. Please contact the MCARE Help Desk to obtain the URL.

### 3.1 SOAP Data Requirements

Submitters should specify appropriate SOAP headers. SOAP specifications are precise and require that the headers and body are constructed perfectly. Any incorrectly constructed SOAP headers will fail and result in an error.

#### SOAP Header

The SOAP Header must include the timestamp element which must be digitally signed. The Web Services Security Binary Security Token must be added to the SOAP Header which is used for verification of the signature. The CORE Connectivity Rule referenced in [Section 3](#) should be used as a reference when constructing the SOAP Header.

#### SOAP Body

The following link should be used as a reference when constructing the SOAP Body:  
<http://www.w3.org/TR/soap12-part1>

Only those characters referenced in the Basic and Extended Character Sets noted in the Appendix of the ASCX12 270/271 version 005010X279A1 TR3 including the 005010X279E1 Errata are acceptable within a HETS 270 inquiry.

**Table 1** and **Table 2** describe the required HETS-specific body elements for 270 requests and X12 responses using SOAP.

**Table 1. Required Body Elements for 270 Requests Using SOAP**

Element Name	Description
PayloadType	X12_270_Request_005010X279A1
ProcessingMode	RealTime
PayloadID	Refer to Section 4.4.2 of Phase II CORE 270: Connectivity Rule for structural guidelines for CORE envelope metadata.
TimeStamp	Format is YYYY-MM-DDTHH:MMSSZ. Refer to <a href="http://www.w3.org/TR/xmlschema11-2/">http://www.w3.org/TR/xmlschema11-2/</a> for more information. SenderID
SenderID	This is a Submitter defined alphanumeric field. The value must be 10 characters in length. Recommended value is your HETS 270/271 SOAP Submitter ID plus trailing zeros for a total of 10 characters.
ReceiverID	CMS
CORERuleVersion	2.2.0
Payload	X12 request. This element must be digitally signed, and the entire payload should be enclosed within a CDATA tag.

**Table 2. Required Body Elements for X12 Responses Using SOAP**

Element Name	Description
PayloadType	X12_271_Response_005010X279A1, X12_TA1_Response_00501X231A1, X12_999_Response_005010X231A1
ProcessingMode	RealTime
PayloadID	Refer to Section 4.4.2 of Phase II CORE 270: Connectivity Rule for structural guidelines for CORE envelope metadata.
TimeStamp	Format is YYYY-MM-DDTHH:MMSSZ. Refer to <a href="http://www.w3.org/TR/xmlschema11-2/">http://www.w3.org/TR/xmlschema11-2/</a> for more information.
SenderID	CMS
ReceiverID	This field must have 10 characters in length, the same as the 270 Sender ID.
CORERuleVersion	2.2.0
Payload	X12 response

### 3.1.1 SOAP Digital Signature

The SOAP communication protocol requires Trading Partners to embed their certificate within the eligibility request and digitally sign the SOAP Body Payload and SOAP Header Timestamp using their private key. CMS will embed their certificate in the 271 response, enabling the

Trading Partner to verify that it came from CMS. Trading Partners can obtain a copy of CMS' Certificate in advance by contacting the MCARE Help Desk.

Trading Partners sending via SOAP must utilize a canonicalization method algorithm for signature that is Exclusive Without Comments: <http://www.w3.org/2001/10/xml-exc-c14n#> . Signatures using algorithms that are Exclusive With Comments, Inclusive With Comments or Inclusive Without Comments will not be accepted.

Refer to the following link for details related to digital signatures as they relate to SOAP: <http://www.w3.org/TR/SOAP-dsig/>

## 3.2 SOAP Examples

Examples of a real time SOAP request and response can be found in Sections 4.2.2.3 and 4.2.2.4 of the CORE Phase II Connectivity Rule (link to that Rule available in [Section 3](#) of this document).

**Table 3** provides an example of a 270 request using SOAP. Carriage returns should NOT be used in the SOAP Body Payload field. They appear in the example information in the HETS Companion Guide for readability purposes only. Also, it is important that the Content-Type line of the HTTP Header and the namespace declaration in the Envelope begin tag contain values associated with SOAP 1.2 as shown below. Using values for SOAP 1.1 or different values may cause the SOAP message to be rejected by HETS. Note: The below example is for illustrative purposes only. All of the variable data will be unique per transaction and should not be copied verbatim and sent to HETS. Lastly, it is highly recommended that the encoding Style attribute for the Envelope begin tag not be specified.

**Table 3. SOAP Request Message Structure**

SOAP Structure Element	Content
HTTP Header	POST https://soap.hetsp-haa.cms.gov HTTP/1.1 Accept-Encoding: gzip,deflate Content-Type: application/soap+xml;charset="UTF-8";action="RealTimeTransaction" Content-Length: 4808 Host: soap.hetsp-haa.cms.gov Connection: Keep-Alive User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
SOAP Envelope Begin	<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
SOAP Header Begin	<soap:Header>
SOAP Header Web Services Security	<wsse:Security soap:mustUnderstand="true" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

SOAP Structure Element	Content
SOAP Header TIMESTAMP	<pre>&lt;wsu:Timestamp wsu:Id="id-155"&gt; &lt;wsu:Created&gt; yyyy-MM-dd'T'hh:mm:ss'Z'&lt;/wsu:Created&gt; &lt;wsu:Expires&gt; yyyy-MM-dd'T'hh:mm:ss'Z'&lt;/wsu:Expires&gt; &lt;/wsu:Timestamp&gt;</pre>
SOAP Header Binary Security Token	<pre>&lt;wsse:BinarySecurityToken EncodingType="http://docs.oasis- open.org/wss/2004/01/oasis-200401-wss-soap-message-security- 1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis- 200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="X509- 0E4E74F95B0421C31C135515946875040"&gt;{{{BASE-64 Encoded Certificate}}}</pre>
SOAP Header Signature	<pre>&lt;ds:Signature Id="SIG-44" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"&gt; &lt;ds:SignedInfo&gt; &lt;ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc- c14n#" /&gt; &lt;ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa- sha256" /&gt; &lt;ds:Reference URI="#id-43"&gt; &lt;ds:Transforms&gt; &lt;ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"&gt; &lt;InclusiveNamespaces PrefixList="ns1 soap" xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" /&gt; &lt;/ds:Transform&gt; &lt;/ds:Transforms&gt; &lt;ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /&gt; &lt;ds:DigestValue&gt;cktVDws5KS70zUTfNB90jcz/F5K/GwliDF09aEV2fMA=&lt;/ds:Di- gestValue&gt; &lt;/ds:Reference&gt; &lt;ds:Reference URI="#id-155"&gt; &lt;ds:Transforms&gt; &lt;ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"&gt; &lt;InclusiveNamespaces PrefixList="ns1 soap" xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" /&gt; &lt;/ds:Transform&gt; &lt;/ds:Transforms&gt; &lt;ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /&gt; &lt;ds:DigestValue&gt;tu65ngGe0d2f2f3iwN/phQBDEXEPFVw2u6/1ZKmX/A=&lt;/ds:Di- gestValue&gt; &lt;/ds:Reference&gt; &lt;/ds:SignedInfo&gt;</pre>

SOAP Structure Element	Content
SOAP Header Signature Value	<ds:SignatureValue>{{{Encoded Signature Value}}} </ds:SignatureValue> Note: The digest value of timestamp + payload is the final string that should be digitally signed to arrive at the final signature.
SOAP Header KeyInfo	<ds:KeyInfo Id="KI-0E4E74F95B0421C31C135515946875041"> <wsse:SecurityTokenReference wsu:Id="STR0E4E74F95B0421C31C135515946875042"> <wsse:Reference URI="#X509-0E4E74F95B0421C31C135515946875040" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509- token-profile-1.0#X509v3"/> </wsse:SecurityTokenReference> </ds:KeyInfo>
SOAP Header End	</ds:Signature> </wsse:Security> </soap:Header>
SOAP Body Begin	<soap:Body> <ns1:COREEnvelopeRealTimeRequest xmlns:ns1=" <a href="http://www.cagq.org/SOAP/WSDL/CORERule2.2.0.xsd">http://www.cagq.org/SOAP/WSDL/CORERule2.2.0.xsd</a> ">
SOAP Body PayloadType	<PayloadType>X12_270_Request_005010X279A1</PayloadType>
SOAP Body ProcessingMode	<ProcessingMode>RealTime</ProcessingMode>
SOAP Body PayloadID	<PayloadID> d5cf23d4-240d-1d9e-b7d5-ab0f8185296b</PayloadID>
SOAP Body TimeStamp	<TimeStamp> yyyy-MM-ddThh:mm:ssZ</TimeStamp>
SOAP Body SenderID	<SenderID>ABCDEFGHIJ</SenderID>
SOAP Body ReceiverID	<ReceiverID>CMS</ReceiverID>
SOAP Body CORERuleVersion	<CORERuleVersion>2.2.0</CORERuleVersion>
SOAP Body Payload	<Payload wsu:Id="id-43"xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><![CDATA[The 270 request will appear here beginning with the ISA segment and ending with the IEA segment as shown in the example from Appendix A of the HETS Companion Guide located on the HETSHelp site - <a href="https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html">https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html</a> ]]></Payload>
SOAP Body End	</ns1:COREEnvelopeRealTimeRequest> </soap:Body>

SOAP Structure Element	Content
SOAP Envelope End	</soap:Envelope>

**Table 4** provides an example of a 271 response using SOAP. Carriage returns should NOT be used in the SOAP Body Payload field. They appear in the example information in the HETS Companion Guide for readability purposes only.

**Table 4. SOAP Response Message Structure**

SOAP Structure Element	Content
HTTP Header	HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Length: 4430 Content-Type: application/soap+xml Date: Mon, 27 Jan 2020 15:45:25 GMT Content-Type: application/soap+xml
SOAP Envelope Begin	<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
SOAP Header Begin	<soap:Header>
SOAP Header Web Services Security	<wsse:Security soap:mustUnderstand="true" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
SOAP Header TIMESTAMP	<wsu:Timestamp wsu:Id="id-155"> <wsu:Created>2020-01-27T15:45:25Z</wsu:Created> <wsu:Expires>2020-01-27T15:46:25Z</wsu:Expires></wsu:Timestamp>
SOAP Header Binary Security Token	<wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="X509-0E4E74F95B0421C31C135515946875040">{{{BASE-64 Encoded Certificate}}} </wsse:BinarySecurityToken>

SOAP Structure Element	Content
SOAP Header Signature	<pre> &lt;ds:Signature Id="SIG-44" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"&gt; &lt;ds:SignedInfo&gt; &lt;ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/&gt; &lt;ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/&gt; &lt;ds:Reference URI="#id-168"&gt; &lt;ds:Transforms&gt; &lt;ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"&gt; &lt;InclusiveNamespaces PrefixList="ns1 soap" xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" /&gt; &lt;/ds:Transform&gt; &lt;/ds:Transforms&gt; &lt;ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /&gt; &lt;ds:DigestValue&gt;ckKtVDws5KS70zUTfNB90jcz/F5K/GwliDF09aEV2fMA=&lt;/ds:DigestValue&gt; &lt;/ds:Reference&gt; &lt;ds:Reference URI="#id-155"&gt; &lt;ds:Transforms&gt; &lt;ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"&gt; &lt;InclusiveNamespaces PrefixList="ns1 soap" xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" /&gt; &lt;/ds:Transform&gt; &lt;/ds:Transforms&gt; &lt;ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /&gt; &lt;ds:DigestValue&gt;tu65ngGe0dl2f2f3iwN/phOQBDXEPFVw2u6/1ZKmX/A=&lt;/ds:DigestValue&gt; &lt;/ds:Reference&gt; &lt;/ds:SignedInfo&gt; </pre>
SOAP Header Signature Value	<pre> &lt;ds:SignatureValue&gt;{{{Encoded Signature Value }}} &lt;/ds:SignatureValue&gt; </pre>
SOAP Header KeyInfo	<pre> &lt;ds:KeyInfo Id="KI-0E4E74F95B0421C31C135515946875041"&gt; &lt;wsse:SecurityTokenReference wsu:Id="STR0E4E74F95B0421C31C135515946875042"&gt; &lt;wsse:Reference URI="#X509-0E4E74F95B0421C31C135515946875040" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/&gt; &lt;/wsse:SecurityTokenReference&gt; &lt;/ds:KeyInfo&gt; </pre>

SOAP Structure Element	Content
SOAP Header End	<pre>&lt;/ds:Signature&gt; &lt;/wsse:Security&gt; &lt;/soap:Header&gt;</pre>
SOAP Body Begin	<pre>&lt;soap:Body&gt; &lt;ns1: COREEnvelopeRealTimeResponse xmlns:ns1="<a href="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd</a>"&gt;</pre>
SOAP Body PayloadType	<pre>&lt;PayloadType&gt; X12_271_Response_005010X279A1&lt;/PayloadType&gt;</pre>
SOAP Body ProcessingMode	<pre>&lt;ProcessingMode&gt;RealTime&lt;/ProcessingMode&gt;</pre>
SOAP Body PayloadID	<pre>&lt;PayloadID&gt; d5cf23d4-240d-1d9e-b7d5-ab0f8185296b &lt;/PayloadID&gt;</pre>
SOAP Body TimeStamp	<pre>&lt;TimeStamp&gt; yyyy-MM-dd'T'hh:mm:ss'Z'&lt;/TimeStamp&gt;</pre>
SOAP Body SenderID	<pre>&lt;SenderID&gt;CMS&lt;/SenderID&gt;</pre>
SOAP Body ReceiverID	<pre>&lt;ReceiverID&gt;ABCDEFGHIJ&lt;/ReceiverID&gt;</pre>
SOAP Body CORERuleVersion	<pre>&lt;CORERuleVersion&gt;2.2.0&lt;/CORERuleVersion&gt;</pre>
SOAP Body Payload	<pre>&lt;Payload wsu:Id="id-168 " xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss- wssecurity-utility-1.0.xsd"&gt;"&gt;&lt;![CDATA[The 271 response will appear here beginning with the ISA segment and ending with the IEA segment as shown in the example from Appendix B of the HETS Companion Guide located on the HETSHelp site - <a href="https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index">https://www.cms.gov/Research-Statistics-Data-and- Systems/CMS-Information-Technology/HETSHelp/index</a> ]]&gt;&lt;/Payload&gt;</pre>
SOAP Body End	<pre>&lt;/ns1: COREEnvelopeRealTimeResponse&gt; &lt;ErrorCode&gt;Success&lt;/ErrorCode&gt; &lt;ErrorMessage/&gt; &lt;/soap:Body&gt;</pre>

## 4. MIME

HETS will support standard MIME messages. The MIME format used MUST be multipart/form-data.

Only those characters referenced in the Basic and Extended Character Sets noted in the Appendix of the ASCX12 270/271 version 005010X279A1 TR3 including the 005010X279E1 Errata are acceptable within a HETS 270 inquiry.

CORE does not specify the naming conventions as a mandate. HETS will implement the MIME body parts with the same field names as the SOAP element nodes. The response will be returned as MIME multipart/form-data, with the Payload body part containing the X12 response.

HETS 270/271 Submitters connecting via MIME will need to use a specific URL to access HETS. Please contact the MCARE Help Desk to obtain the URL.

### 4.1 MIME Data Requirements

Submitters must specify appropriate MIME headers. The MIME specification is very precise and requires that the headers and the body be constructed perfectly. Any incorrectly constructed MIME headers will fail and result in an error.

The HETS implementation of MIME allows for the use of the Basic and Extended Character Sets as noted in the Appendix of the ASCX12 270/271 version 005010X279A1 TR3 including the 005010X279E1 Errata only. Please refer to the Request for Comments (RFC) 2388 – returning values from Forms: multipart/form-data to review header and body specifications. RFC 2388 can be found at the following link:

<http://www.faqs.org/rfcs/rfc2388.html>

#### MIME Header

MIME Messages will have standard HTTP header data elements, such as POST, HOST, Content-Length and Content-Type. The supported Content-Type is MIME multipart/form-data.

#### MIME Body

Required HETS-specific body elements for 270 requests and X12 responses using MIME are defined in Table 5 and Table 6.

**Table 5. Required Body Elements for 270 Requests Using MIME**

Element Name	Description
PayloadType	X12_270_Request_005010X279A1
ProcessingMode	RealTime
PayloadID	Refer to Section 4.4.2 of Phase II CORE 270: Connectivity Rule for structural guidelines for CORE envelope metadata.

<sup>2</sup> Effective April 23, 2022. MIME Submitters should not utilize this URL prior to that date.

Element Name	Description
TimeStamp	Format is YYYY-MM-DDTHH:MMSSZ. Refer to <a href="http://www.w3.org/TR/xmlschema11-2/">http://www.w3.org/TR/xmlschema11-2/</a> for more information.
SenderID	This is a Submitter defined alphanumeric field. The value must be 10 characters in length. Recommended value is your HETS 270/271 MIME Submitter ID plus trailing zeros for a total of 10 characters.
ReceiverID	CMS
CORERuleVersion	2.2.0
Payload	X12 request. The X12 request must be submitted as part of the MIME request and not as an attachment. If an attachment is received, the transaction will be rejected. The request does not need to be enclosed within a CDATA tag. See Appendix A of the HETS Companion Guide located on the HETSHelp site for an example of the data that would appear here - <a href="https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html">https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html</a>

**Table 6. Required Body Elements for X12 Responses Using MIME**

Element Name	Description
PayloadType	X12_271_Response_005010X279A1, X12_TA1_Response_00501X231A1, X12_999_Response_005010X231A1
ProcessingMode	RealTime
PayloadID	Refer to Section 4.4.2 of Phase II CORE 270: Connectivity Rule for structural guidelines for CORE envelope metadata.
TimeStamp	Format is YYYY-MM-DDTHH:MMSSZ. Refer to <a href="http://www.w3.org/TR/xmlschema11-2/">http://www.w3.org/TR/xmlschema11-2/</a> for more information.
SenderID	CMS
ReceiverID	This field must be 10 characters in length. The same as the 270 Sender ID.
CORERuleVersion	2.2.0
Payload	X12 response

## 4.2 MIME Examples

Examples of a real time MIME request and response can be found in Sections 4.2.1.1 and 4.2.1.2 of the CORE Phase II Connectivity Rule (link to that Rule available in [Section 3](#) of this document).

### MIME Data Requirements for Header and Body:

<http://www.faqs.org/rfcs/rfc2388.html>

Refer to **Table 7** in this document for the HETS-specific body elements.

**MIME Request and Response Examples:**

**Table 7** and **Table 8** provide examples of a 270 request and 271 response using HTTP MIME Multipart. The below examples are for illustrative purposes only. The 270 request must be submitted as part of the MIME request and not as an attachment. If an attachment is received, the transaction will be rejected. The request does not need to be enclosed within a CDATA tag. All of the variable data will be unique per transaction and should not be copied verbatim and sent to HETS.

**Table 7. MIME Request Message Structure**

MIME Structure Element	Content
MIME Header	POST https://mime.hetsp-haa.cms.gov HTTP/1.1 Connection: keep-alive Content-Length: 1392 Content-Type: multipart/form-data; boundary=COSZiva9NdnYzPXUEGy-tLBO8n4-czud Host: mime.hetsp-haa.cms.gov User-Agent: Apache-HttpClient/4.2.1 (java 1.5)
MIME Body	--COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="PayloadType" X12_270_Request_005010X279A1 --COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="ProcessingMode" RealTime --COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="PayloadID" d5cf23d4-240d-1d9e-b7d5-ab0f8185296b --COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="TimeStamp" 2020-02-25T19:50:40.611Z --COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="SenderID" HETS00001 --COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="ReceiverID" CMS --COSZiva9NdnYzPXUEGy-tLBO8n4-czud Content-disposition: form-data; name="CORERuleVersion"

MIME Structure Element	Content
	<p>2.2.0</p> <p>--COSZiva9NdnYzPXUEGy-tLBO8n4-czud</p> <p>Content-disposition: form-data; name="Payload"</p> <p>***The 270 request will appear here beginning with the ISA segment and ending with the IEA segment as shown in the example from Appendix A of the HETS Companion Guide located on the HETSHelp site - <a href="https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index">https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index</a> ***</p> <p>--COSZiva9NdnYzPXUEGy-tLBO8n4-czud--</p>

**Table 8. MIME Response Message Structure**

MIME Structure Element	Content
MIME Header	<p>HTTP/1.1 200 OK</p> <p>Server: Apache-Coyote/1.1</p> <p>Content-Type: multipart/form-data; boundary=7aaeaf96-1e54-4567-a8d0-e93de77cd66a</p> <p>Content-Length: 1567</p> <p>Date: Mon, 27 Jan 2020 15:45:25 GMT</p>
MIME Body	<p>--7aaeaf96-1e54-4567-a8d0-e93de77cd66a</p> <p>Content-disposition: form-data; name="PayloadType"</p> <p>Content-type: text/plain</p> <p>X12_TA1_Response_005010X279A1</p> <p>--7aaeaf96-1e54-4567-a8d0-e93de77cd66a</p> <p>Content-disposition: form-data; name="ProcessingMode"</p> <p>Content-type: text/plain</p> <p>RealTime</p> <p>--7aaeaf96-1e54-4567-a8d0-e93de77cd66a</p> <p>Content-disposition: form-data; name="PayloadID"</p> <p>Content-type: text/plain</p> <p>d5cf23d4-240d-1d9e-b7d5-ab0f8185296b</p> <p>--7aaeaf96-1e54-4567-a8d0-e93de77cd66a</p> <p>Content-disposition: form-data; name="TimeStamp"</p> <p>Content-type: text/plain</p> <p>2020-02-25T19:50:40.611Z</p> <p>--7aaeaf96-1e54-4567-a8d0-e93de77cd66a</p> <p>Content-disposition: form-data; name="SenderID"</p> <p>Content-type: text/plain</p>

MIME Structure Element	Content
MIME Body	<pre> CMS --7aaeaf96-1e54-4567-a8d0-e93de77cd66a Content-disposition: form-data; name="ReceiverID" Content-type: text/plain  HETS000001 --7aaeaf96-1e54-4567-a8d0-e93de77cd66a Content-disposition: form-data; name="CORERuleVersion" Content-type: text/plain  2.2.0 --7aaeaf96-1e54-4567-a8d0-e93de77cd66a Content-disposition: form-data; name="Payload" Content-type: text/plain  ***The 271 response will appear here beginning with the ISA segment and ending with the IEA segment as shown in the example from Appendix B of the HETS Companion Guide located on the HETSHelp site <a href="https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index">https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index</a> ***  --7aaeaf96-1e54-4567-a8d0-e93de77cd66a Content-disposition: form-data; name="ErrorCode" Content-type: text/plain  Success --7aaeaf96-1e54-4567-a8d0-e93de77cd66a Content-disposition: form-data; name="ErrorMessage" Content-type: text/plain  --7aaeaf96-1e54-4567-a8d0-e93de77cd66a— </pre>

## 5. Common Error Processing for SOAP and MIME

The HETS 270/271 application will process SOAP and MIME transactions and return errors as described in this section.

### 5.1 HTTP Status and Error Codes

The processing and error codes for the HTTP layer are defined as part of the HTTP specifications as noted at the following link:

<https://www.rfc-editor.org/rfc/rfc9110.html>

The intended use of these status and error codes in processing transactions is specified in Table 4.3.3.1 of the Phase II CORE 270: Connectivity Rule referenced in [Section 3](#).

### 5.2 CORE Envelope Processing Status and Error Codes

**Table 9** describes envelope processing status and error codes specific to the HETS 270/271 application for SOAP and MIME transactions.

**Table 9. Envelope Process Status and Errors**

Element Name	Description
<FieldName>Illegal	Illegal value provided for <FieldName>.
<FieldName>Required	The field <FieldName> is required but was not provided.
VersionMismatch	The CORERuleVersion sent is not acceptable to the Receiver.
Success	The envelope was processed successfully.

### 5.3 SOAP Specific Processing Errors

**Table 10** describes examples of SOAP processing errors.

**Table 10. SOAP Specific Processing Errors**

Element Name	Description
Unauthorized	The signature could not be verified.

### 5.4 SOAP and MIME Transaction (X12) Error Processing

Refer to the HETS Companion Guide for additional information on the transaction processing errors that will be returned as a SOAP message or MIME Multipart/form-data containing the related response.

The HETS Companion Guide can be found in the downloads section of the CMS HETS Help web site at the following link:

<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index.html>

## 6. General Onboarding Checklist

If the Trading Partner is a new HETS Submitter, they must first follow the traditional enrollment processes, which can be found at on the “How to Get Connected – HETS 270/271” page of the HETS Help website and includes the completion of the Trading Partner Agreement. It will take approximately two weeks to complete this process. The HETS Help website can be found at the following link:

<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index.html>

If the Trading Partner already has a HETS Submitter ID (SID), or if it has just completed the traditional enrollment process, the following steps can serve as a general guide to the onboarding process for SOAP/MIME submissions. It will take approximately two weeks to complete this process.

**Table 11. General Onboarding Checklist**

Checkbox	General Onboarding Checklist Items
<input type="checkbox"/>	<p>When the Trading Partner contacts MCARE to request access to use SOAP/MIME, they must have already purchased an X.509 Digital Certificate and be prepared to provide the following information:</p> <ul style="list-style-type: none"> <li>• Organizational Legal Business Name</li> <li>• Organization Submitter ID (SID) if previously assigned</li> <li>• Organization originating IP address(es) that will be linked to the certificate</li> <li>• X.509 Digital Certificate Issuer Name</li> <li>• X.509 Digital Certificate Type</li> <li>• X.509 Digital Certificate Serial Number</li> </ul>
<input type="checkbox"/>	<p>The Trading Partner should email the X.509 Digital Certificate to MCARE in (.PEM) format to MCARE at MCARE@cms.hhs.gov. The Trading Partner should NOT include the private key when sending the digital certificate.</p>
<input type="checkbox"/>	<p>MCARE will review the digital certificate. If there are issues or errors, MCARE will notify the Trading Partner and assist in the resolution.</p>
<input type="checkbox"/>	<p>Upon validation of the Digital Certificate, MCARE will work with the HETS team to provide access to the Trading Partner.</p>
<input type="checkbox"/>	<p>Once access has been provided, MCARE will inform the Trading Partner and work with them to verify transactions can be sent successfully.</p>
<input type="checkbox"/>	<p>After successfully implementing HETS via SOAP or MIME (i.e., sending a good 270 request and receiving a proper 271 response), the Trading Partner’s Submitter ID status will be moved from ‘Test’ to ‘Production’. The Trading Partner may then send regular Medicare eligibility traffic to HETS.</p>

## Appendix A: HETS Web Services Security Policy

---

The following text is an example of the XML Schema.

```
<?xml version="1.0" encoding="utf-8"?>
<wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <wsp:ExactlyOne>
    <wsp:All>
      <wsp:Policy wsu:Id="transport-ssl-client-cert">
        <sp:TransportBinding>
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken>
                  <wsp:Policy>
                    <sp:RequireClientCertificate/>
                  </wsp:Policy>
                </sp:HttpsToken>
              <sp:HttpsToken RequestClientCertificate="true"/>
            </wsp:Policy>
          </sp:TransportToken>
        <sp:AlgorithmSuite>
          <wsp:Policy>
            <wsp:ExactlyOne>
              <sp:Basic256Sha256/>
            </wsp:ExactlyOne>
          </wsp:Policy>
        </sp:AlgorithmSuite>
      <sp:IncludeTimestamp/>
    </wsp:Policy>
  </sp:TransportBinding>
</wsp:Policy>
```

```
<sp:AsymmetricBinding>
  <wsp:Policy>
    <sp:RecipientSignatureToken>
      <wsp:Policy>
        <sp:X509Token
          sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToInitiator">
          <wsp:Policy>
            <sp:WssX509V3Token10/>
          </wsp:Policy>
        </sp:X509Token>
      </wsp:Policy>
    </sp:RecipientSignatureToken>
    <sp:InitiatorSignatureToken>
      <wsp:Policy>
        <sp:X509Token
          sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
          <wsp:Policy>
            <sp:WssX509V3Token10/>
          </wsp:Policy>
        </sp:X509Token>
      </wsp:Policy>
    </sp:InitiatorSignatureToken>
    <sp:AlgorithmSuite>
      <wsp:Policy>
        <sp:Basic256Sha256/>
      </wsp:Policy>
    </sp:AlgorithmSuite>
  </wsp:Policy>
</sp:AsymmetricBinding>
```

```

    <sp:IncludeTimestamp/>
  </wsp:Policy>
</sp:AsymmetricBinding>
<sp:EndorsingSupportingTokens
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
  <wsp:Policy>
    <sp:X509Token
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssX509V3Token10/>
      </wsp:Policy>
    </sp:X509Token>
  </wsp:Policy>
  <wsp:Policy>
    <sp:X509Token
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToInitiator">
      <wsp:Policy>
        <sp:WssX509V3Token10/>
      </wsp:Policy>
    </sp:X509Token>
  </wsp:Policy>
</sp:EndorsingSupportingTokens>
<wsp:Policy wsu:Id="request_parts">
  <sp:SignedElements>
<sp:XPath>*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and local-
name()='Envelope']/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and local-
name()='Header']/*[namespace-uri()='http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd' and local-name()='Security']/*[namespace-
uri()='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd' and
local-name()='Timestamp']</sp:XPath>
<sp:XPath>*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and local-
name()='Envelope']/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and local-
name()='Body']/*[namespace-uri()='http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd' and
local-name()='COREEnvelopeRealTimeRequest']/Payload</sp:XPath>
  </sp:SignedElements>

```

```
</wsp:Policy>
<wsp:Policy wsu:Id="response_parts">
  <wsp:ExactlyOne>
    <wsp:All>
<sp:SignedElements>
  <sp:XPath>/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and
local-name()='Envelope']/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and
local-name()='Header']/*[namespace-uri()='http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd' and local-name()='Security']/*[namespace-
uri()='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd' and
local-name()='Timestamp']</sp:XPath>
    <sp:XPath>/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and
local-name()='Envelope'] /*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and
local-name()='Body']/*[namespace-
uri()='http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd' and local-
name()='COREEnvelopeRealTimeResponse']/Payload</sp:XPath>
    </sp:SignedElements>
  </wsp:All>
<wsp:All>
  <sp:SignedElements>
<sp:XPath>/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and
local-name()='Envelope']/*[namespace-uri()='http://www.w3.org/2003/05/soap-envelope' and
local-name()='Header']/*[namespace-uri()='http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd' and local-name()='Security']/*[namespace-
uri()='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd' and
local-name()='Timestamp']</sp:XPath>
    </sp:SignedElements>
  </wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsaw:UsingAddressing xmlns:wsaw="http://www.w3.org/2005/08/addressing"/>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
```

## Appendix B: Frequently Asked Questions

Table 12. Frequently Asked Question

Question Number	Question	Answer
1	Do I need my own digital certificate for exchanging 270/271 via SOAP and MIME methods?	Yes. The User ID and Password authentication method are not supported by HETS. Instead, a Trading Partner must procure a digital certificate and configure their system to connect to HETS.
2	Are there specific Digital Certificates that can access HETS?	Sections 2.1.1 through 2.1.3 contain information regarding digital certificate issuance.
3	What specific connectivity configurations must I complete for a successful SOAP connection?	<p>Trading Partners using SOAP are encouraged to ensure the following:</p> <p>The SOAP communication protocol requires Trading Partners to send their certificate and digitally sign the payload and timestamp using their private key. This allows HETS to validate the contents of the received message and when it was sent.</p> <p>The “wsu:ID” attribute is contained in both the timestamp and payload nodes. They should both match the “&lt;Reference URI.”</p> <p>That their perimeter equipment IP range or subnet has been provided to MCARE for configuration within CMS firewall.</p> <p>Their application makes use of Public Key Infrastructure (PKI) and configures the Trading Partner keystore with the correct client certificate to sign the SOAP messages.</p> <p>The trust store is correctly configured with the CMS certificate.</p>
4	Do I need a Virtual Private Network (VPN) over internet for connection to HETS 270/271 Application?	A VPN connection to CMS is not required for connectivity to the HETS 270/271 Application.
5	What is the difference between SOAP and MIME transactions, specific to the HETS 270/271 Application?	From the Trading Partner’s perspective, the HETS 270/271 Application has two different URLs for sending these transactions. The processing for both MIME and SOAP is the same.
6	How do I go about developing my SOAP or MIME client?	HETS does not require any specific tool for client-side implementation. The Trading Partners are free to choose various Commercial-off-the-Shelf (COTS) products or custom code to create the SOAP & MIME requests.

Question Number	Question	Answer
7	How do I wrap a 270 transaction for submission?	For SOAP transactions, the Trading Partners must ensure that the 270 transaction is contained in the payload tag and the “CDATA” tag is present. For MIME transactions, the Trading Partners must ensure that the 270 transaction is contained in the payload MIME boundary. MIME does not use CDATA tags, and it should not be present.
8	Can I send more than one 270 in a single SOAP or MIME request?	No. Only one 270 should be submitted per SOAP or MIME request. The HETS 270/271 Application does not support batch.
9	Can I send my transactions as SOAP or MIME attachments?	No. The 270 transactions should be sent as part of payload tag in SOAP requests. For MIME requests they should be sent in-line, as part of the payload element.
10	Do I need to use a User ID / Password when establishing a connection to HETS to submit SOAP or MIME transactions?	No. The HETS 270/271 Application connection authentication requirements are based only on digital certificates.
11	Does the SID used in the SOAP message body need to match the X12 SID?	Trading Partners should ensure that the Submitter IDs match. However, the HETS 270/271 Application uses only the SID embedded in X12 270 transaction for authorization.
12	How can we ensure the digital certificate doesn't get activated until MCARE validates and authorizes the Submitter?	The certificate will be active the day it was issued to the Trading Partner. However, MCARE will ensure that access to the firewall is allowed only after the certificate verification step is complete.
13	What happens when an organization is revoked by their CA?	The Certificate Revocation Lists for each CA will be loaded into the production environment infrastructure and those Trading Partners that attempt submission with a revoked digital certificate will be denied access through the CMS firewall.
14	How will the Trading Partner get the WS-Policy also known as the Web Services Security Policy?	The Trading Partners should receive a copy of the WS-Policy document during on-boarding process. See Section 6.

Question Number	Question	Answer
15	The Submitter is receiving "Error getting response; javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure". What does that mean?	The 2-way SSL handshake process did not complete successfully. This is most likely due to either the Submitter not having configured a 2-way SSL on their end or an invalid or revoked digital certificate is being used.
16	What types of attachments can be included in a MIME transaction?	No attachments can be included in the MIME transaction. The 270 request must be encoded in-line to the MIME message.

## Appendix C: References

Table 13. References

Document	Hyperlink
CAQH CORE site for the CORE Connectivity & Operating Rules, SOAP Header, WSDL and XML Schema details	<a href="#">CAQH CORE – Committee on Operating Rules for Information Exchange</a>
CORE Mandated Operating Rules	<a href="https://www.caqh.org/core/operating-rules-mandate">https://www.caqh.org/core/operating-rules-mandate</a>
HETS Help website including the HDT User Guide and HETS Companion Guide	<a href="https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index">https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index</a>
HTTP Specifications	<a href="https://www.rfc-editor.org/rfc/rfc9110.html">https://www.rfc-editor.org/rfc/rfc9110.html</a>
MIME Header & Body Specifications	<a href="http://www.faqs.org/rfcs/rfc2388.html">http://www.faqs.org/rfcs/rfc2388.html</a>
SOAP Body	<a href="http://www.w3.org/TR/soap12-part1">http://www.w3.org/TR/soap12-part1</a>
Timestamp Element Format	<a href="http://www.w3.org/TR/xmlschema11-2/">http://www.w3.org/TR/xmlschema11-2/</a>
XML Schemas	<a href="http://www.w3.org/TR/SOAP-dsig">http://www.w3.org/TR/SOAP-dsig</a>

## Appendix D: Acronyms

Table 14. Acronyms

Acronym	Definition
ACA	Affordable Care Act
CA	Certificate Authority
CAQH/CORE	Council for Affordable Quality Healthcare/ Committee on Operating Rules for Information Exchange
CDATA	Character Data
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial-off-the-Shelf
CSR	Certificate Signing Request
FAQ	Frequently Asked Questions
HDT	Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) Desktop
HETS	Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
MCARE	Medicare Customer Assistance Regarding Eligibility (Help Desk)
MIME	Multipurpose Internet Mail Extensions
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
PKI	Public Key Infrastructure
RFC	Request for Comments
SID	Submitter Identification Number
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPA	Trading Partner Agreement
URL	Uniform Resource Locator
VPN	Virtual Private Network
WSDL	Web Services Description Language

Acronym	Definition
XML	Extensible Markup Language

## Appendix E: Glossary of Terms

Table 15. Glossary of Terms

Term	Acronym	Definition
Affordable Care Act	ACA	The Affordable Care Act puts families and small businesses in control of their own health care by allowing them to choose the insurance coverage that works best for them in an open, competitive insurance market.
Certificate Authority	CA	Issues digital certificates after verifying the identity of the applicant.
Council for Affordable Quality Healthcare – Committee on Operating Rules for Information Exchange	CAQH CORE	A multi-stakeholder initiative developing operating rules that streamline electronic healthcare administrative data exchange and support interoperability between payers and Providers.
Centers for Medicare & Medicaid Services	CMS	CMS is a Federal agency within the United States Department of Health and Human Services that administers the Medicare program and works in partnership with state governments to administer Medicaid, the State Children’s Health Insurance Program, and health insurance portability standards.
Certificate Signing Request	CSR	A message which is sent from an applicant to a Certificate Authority in order to apply for a digital certificate.
HIPAA Eligibility Transaction System (HETS) Desktop	HDT	The HDT is an Internet-facing application that assists Clearinghouses in validating Medicare Legacy Provider and National Provider Identifier numbers.
HIPAA Eligibility Transaction System	HETS	HETS allows the release of eligibility data to Medicare Providers, Suppliers, or their authorized billing agents for the purpose of preparing an accurate Medicare claim, determining Beneficiary liability, or determining eligibility for specific services. There are two ways to inquire for eligibility. See HETS 270/271 and HETS User Interface.
Department of Health and Human Services	HHS	HHS is a Cabinet department of the United States government with the goal of protecting the health of all Americans and providing essential human services.

Term	Acronym	Definition
Health Insurance Portability and Accountability Act	HIPAA	Title I of the Health Insurance Portability and Accountability Act protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of the Health Insurance Portability and Accountability Act, known as the Administrative Simplification provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for Providers, health insurance plans, and employers.
Hypertext Transfer Protocol	HTTP	An application-level protocol for distributed, collaborative, hypermedia information systems.
Medicare Customer Assistance Regarding Eligibility Help Desk	MCARE Help Desk	The MCARE Help Desk is a single point of contact for all Submitters facing inquiries regarding the HETS eligibility systems.
Multipurpose Internet Mail Extensions	MIME	An internet standard that extends the format of email to support header and text in email that uses text attachments and multiple part message bodies.
National Provider Identifier	NPI	An NPI is a unique 10-digit identification number issued to health care Providers in the United States by Centers for Medicare & Medicaid Services. Covered health care Providers and all health plans and health care Clearinghouses must use the NPI in the administrative and financial transactions adopted under Health Insurance Portability and Accountability Act.
Submitter ID Number	SID	The Submitter ID number is the value that identifies your organization to the HETS 270/271 system.
Simple Object Access Protocol	SOAP	A protocol specification for exchanging structured information in the implementation of Web Service in computer networks that relies on XML Information Set for its message format.
Transmission Control Protocol/Internet Protocol	TCP/IP	Defines the rules that computers must follow to communicate with each other over the internet.
Transport Layer Security	TLS	A protocol that ensures privacy between communicating applications and their user on the Internet. This protocol replaces the Secure Socket Layer (SSL).
Web Services Description Language	WSDL	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document or procedure-oriented information.
Extensible Markup Language	XML	Defines a set of rules for encoding documents.

## Appendix F: Revision History

**Table 16. Revision History**

Version	Date	Revision/Change Description	Pages Affected
8.0	5/12/2025	Updated section 2.1 to include IdentTrust information, including new section 2.1.3 IdenTrust	3, 4, 5
7.0	11/18/2024	Finalization of document and remediation.	All
6.1	11/8/2024	Removed SOAP/MIME URLs	Multiple
6.0	11/6/2024	Updated document links, updated release date, finalized	Multiple
5.0	6/28/2024	Updated final Release Date	All
4.8	3/29/2024	Added Note to Table 3 SOAP Request Message Structure under SOAP Header Signature Value	18
4.8	1/9/2024	Updated content in Section 4.1 MIME Data Requirements advising Submitters that incorrectly constructed MIME headers will receive an error	18
4.8	1/9/2024	Updated content in Section 3.1 SOAP Data Requirements advising Submitters that incorrectly constructed SOAP headers will receive an error	10
4.8	1/9/2024	Updated content in Section 2. Authentication and Authorization Handling advising Submitters that IP addresses must be added to the TPA	7
4.8	1/9/2024	Added a third bullet item in introduction reminding Submitters to complete certificate maintenance	5
4.3	11/16/2020	Updated URL references to CAQH CORE to reflect changes on the CAQH website	Multiple
4.2	08/24/2020	Updated CAQH CORE URLs throughout the document to reflect organizational changes to their website Removed previous section 2.1.3 which detailed information for Certification Authority (CA) Symantec. Symantec's certificate business was previously acquired by Digicert.	Multiple
4.1	03/31/2020	Tables 5, 8 & 9 – Update to reflect minor changes in processing in the HETS high availability environment	Multiple

Version	Date	Revision/Change Description	Pages Affected
4.0	09/06/2019	<p>Changes related to the HETS 270/271 High Availability transition include:</p> <p>Section 1 – Updated URL for HETS Companion Guide and HDT User Guide</p> <p>Section 2.1 – Reorganized this Section for clarity</p> <p>Section 2.2 – Removed TLS_RSA_WITH_3DES_EDE_CBC_SHA from the list of supported cipher suites</p> <p>Section 3 – Updated SOAP destination URL</p> <p>Section 3.1.1 – Updated to note canonicalization method algorithm requirements</p> <p>Table 4 – Updated SOAP destination URL and HETS Companion Guide reference URL. Also updated CanonicalizationMethod Algorithm in the SOAP Header Signature example.</p> <p>Table 5 – Updated URL for HETS Companion Guide. Also updated CanonicalizationMethod Algorithm in the SOAP Header Signature example.</p> <p>Table 6 – Updated URL for HETS Companion Guide</p> <p>Table 8 – Updated MIME destination URL and HETS Companion Guide reference URL</p> <p>Table 9 – Updated URL for HETS Companion Guide</p> <p>Section 5.4 – Updated URL for HETS Companion Guide</p> <p>Appendix B – Updated FAQ #16 to clarify that MIME attachments are not accepted</p> <p>Appendix C – Removed extraneous references</p> <p>Appendix D – Added acronyms COTS, PKI &amp; VPN</p>	1, 3, 4, 6, 7, 8, 11, 14, 16, 18, 20, 27, 29, 30
3.2	8/21/2017	<p>Section 1 – Updated URL for HETS Companion Guide</p> <p>Table 4 – Updated URL for HETS Companion Guide</p> <p>Table 5 – Updated URL for HETS Companion Guide</p> <p>Table 6 – Updated URL for HETS Companion Guide</p> <p>Table 8 – Updated URL for HETS Companion Guide</p> <p>Table 9 – Updated URL for HETS Companion Guide</p> <p>Table 15 – Updated Symantec URLs</p>	1, 9, 11, 12, 13, 14, 24
3.1	12/5/2016	<p>Table 8 – Updated MIME Body Content</p> <p>Table 9 – Updated MIME Body Content</p>	13, 14

3.0	3/24/16	<p>Modified document for R2016Q300 Redesign Release. Changes Include:</p> <p>Updated Title Page to remove OIS and 508 compliant check</p> <p>Section 1 – Updated HETS Help website, removed references to HPG and replaced with HDT, added URL for HDT User Manual</p> <p>Section 2 – Removed references to TLS 1.1 and December 31, 2015 deadline to utilize TLS 1.2 and a SHA2-256 certificate as this deadline has passed</p> <p>Section 2.1 – Removed references to December 31, 2015 deadline to utilize TLS 1.2 and a SHA2-256 certificate as this deadline has passed</p> <p>Section 2.1.2 – Removed outdated Certification Authorities for Entrust</p> <p>Section 2.2 – Removed reference to January 1, 2016 requirement as this deadline has passed and replaced SHA1 with SHA2</p> <p>Section 3 – Updated SOAP URL</p> <p>Section 3.1, Table 2 and 3 description – Updated 271 Responses to X12 Responses</p> <p>Section 3.1, Table 2 and 3 – Updated TimeStamp description</p> <p>Section 3.2, Table 4 – Updated HTTP Header Content with new SOAP URL, and SOAP Header Timestamp Content with generic value, PayloadID Content with an example, TimeStamp Content with generic value</p> <p>Section 4 – Updated MIME URL</p> <p>Section 4.1, Table 6 and 7 description – Updated 271 Responses to X12 Responses</p> <p>Section 4.1, Table 6 and 7 – Updated TimeStamp description</p> <p>Section 4.2 – Added note that examples are for illustrative purposes only</p> <p>Section 4.2, Table 8 – Updated MIME Header Content with new MIME URL, PayloadID Content with an example, TimeStamp Content with generic value</p> <p>Section 4.2, Table 9 – Updated MIME Header and Body Content</p> <p>Section 5.2, Table 10 - Updated VersionMismatch Description and removed InvalidPayload</p> <p>Section 5.2, Table 11 – Added Unauthorized error and removed other errors</p> <p>Section 5.4 – Removed MIME Specific Processing Errors as they no longer apply</p> <p>Appendix B – Updated FAQ 12 and 16</p>	Multiple
-----	---------	--	----------

Version	Date	Revision/Change Description	Pages Affected
		Appendix C – Replaced HPG User Guide Reference to HDT User Guide Appendix D – Replaced HPG with HDT	
2.1	9/2/2015	Added Entrust L1K/L1M certificate list and added additional values which can return in the PayloadType field for MIME responses.	4, 12
2.0	06/19/15	Added clarification on requirement of SHA2-256 and Transport Layer Security (TLS) 1.2 requirement as well as clarified existing SOAP/MIME processing.	Multiple
1.1	02/24/2014	Added clarification that only those characters referenced in the Basic and the Extended Character Sets noted in the Appendix of the ASCX12 270/271 version 005010X279A1 TR3 including the 005010X279E1 Errata are acceptable within a HETS 270 inquiry.	5, 10 and 23
1.0	08/15/2013	Initial release.	All