Blue Cross Blue Shield of Michigan

EDI Real Time SOAP/HTTPS Services:

Trading Partner Guide (ANSI 270/271, ANSI 276/277, ANSI 835)
Blue Cross Blue Shield of Michigan
EDI Real Time SOAP/HTTPS Services: Trading Partner Guide (ANSI 270/271, ANSI 276/277, ANSI 835)

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/20/2012</td>
<td>1.0</td>
<td>Initial doc</td>
<td>BCBSM</td>
</tr>
<tr>
<td>02/22/2013</td>
<td>1.1</td>
<td>Added SSL Client Authentication</td>
<td>BCBSM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrections in the service endpoints</td>
<td></td>
</tr>
<tr>
<td>09/23/2013</td>
<td>2.0</td>
<td>Revised to accommodate ERA/835 HTTPS</td>
<td>BCBSM</td>
</tr>
<tr>
<td>11/01/2013</td>
<td>2.1</td>
<td>Revised Section 2.1 End Point URL to include ERA/835</td>
<td>BCBSM</td>
</tr>
</tbody>
</table>

Table of Contents

Scope: ..................................................................................................................... 3
Audience: .................................................................................................................... 3
1 Service Overview........................................................................................................ 4
1.1 Service Description .............................................................................................. 4
1.2 Service Access ........................................................................................................ 4
   1.2.1 Requesting Schema Components.................................................................. 4
   1.2.2 Client CA (Certificate Authority) signed cert........................................ 4
   1.2.3 Enabling Components for HTTPS/SOAP messaging..................................... 5
   1.2.4 Sizing your usage..................................................................................... 5
   1.2.5 Hours of Availability ............................................................................. 5
2 Service Specification .................................................................................................. 6
2.1 Endpoint URL .......................................................................................................... 6
2.2 SSL Server certificate ............................................................................................ 6
2.3 SSL client certificate ............................................................................................. 7
2.4 Authentication/Authorization.................................................................................. 8
2.5 Sample SOAP/Request ............................................................................................. 8
2.6 SOAP fault ............................................................................................................. 8
Appendix A: Example in obtaining the BCBSM certificate........................................... 10
Appendix B: Example in obtaining Entrust CA Cert .................................................... 15
Appendix C: Recommended decision for certificate key Lengths and Renewal: .......... 17
Scope:
This guide contains steps regarding connecting to the BCBSM EDI Real Time gateway for processing of ANSI 270/271 and ANSI 276/277 transactions as well as connecting to the BCBSM batch processing system for the ANSI 835 transaction. This connectivity is per CORE (Committee on Operating Rules for Information Exchange) guidelines.

Audience:
1) External partners
2) BCBSM support personnel
1 Service Overview

1.1 Service Description

The implementation will conform to standards being set up by CORE (Committee on Operating Rules for Information Exchange) and support SOAP/HTTPS as a transport standard.

Note: Blue Cross Blue Shield Michigan is utilizing the IBM DataPower device to proxy EDI services.

For details about the CORE standards please refer to:
http://www.caqh.org/SOAP/WSDL/

HTTP Version 1.1
SSL Version 3.0
SOAP Version 1.2
WSDL Version 1.1
Web Services-Security 1.1

Note: BCBSM is utilizing the CORE 270 Phase II CORE 270 Connectivity Rule Version 2.2.0 for the 835 as per Section 4.1 of Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule.

1.2 Service Access

1.2.1 Requesting Schema Components

Trading partner should request WSDL and Schema documents from BCBSM’s EDI department. The email request and response need to be in encrypted format. Please note BCBSM uses ZixSelect to encrypt the outgoing information. To request the documents please send an email with your contact information to the EDICustMgmt@bcbsm.com mailbox.

1.2.2 Client CA (Certificate Authority) signed cert

HTTPS/SSL will require client authentication in the https handshake. Towards that end, client app needs to use a commercial CA signed certificate, and submit this certificate to BCBSM to be loaded in the system.
1.2.3 Enabling Components for HTTPS/SOAP messaging
BCBSM will provide you the WSDL and Schema to help create a client side request.

1.2.4 Sizing your usage
Before access can be granted to a new consuming application for the ANSI 270/271 and ANSI 276/277, a statement as to the usage requirements for that consumer will need to be provided in order to identify possible issues in the service’s utilization or risks associated with its Service Level Agreement. Please note that when the HTTPS/SOAP connection is being used for the ANSI 270/271 and ANSI 276/277 you agree that the connection is solely for “Real Time” usage of Eligibility/Benefits/Claim Status Inquiry/Response, and the channel should not be used to submit batched up ANSI 270/276 transactions.

1.2.5 Hours of Availability
EDI Real Time system availability (ANSI 270/271 and 276/277) or EDI batch processing (ANSI 835) is as follows:

Mon – Sun 1:00 AM – 1:00 AM EST
Sun – 1:00 AM – 6:00 PM EST

- Any planned or unplanned system outages for the ANSI 270/271 and ANSI 276/277 will be communicated as an alert on the real time webpage of bcbsm.com.

- Any planned or unplanned system outages for the ANSI 835 will be communicated through one of the following:
  - HTTPS will be communicated through an e-mail broadcast.
  - SFTP will be communicated through an EDDI or WebDENIS communication posting.

Help Desk Support for connection issues: 1-800-859-BLUE (2583)
2 Service Specification

2.1 Endpoint URL

Non-Production
https://webservicesqa.bcbsm.com/EDI/serviceURI

For example
https://webservicesqa.bcbsm.com/EDI/CAQH270Service
https://webservicesqa.bcbsm.com/EDI/CAQH835Service

Production
https://webservices.bcbsm.com/EDI/serviceURI

For example
https://webservices.bcbsm.com/EDI/CAQH270Service
https://webservices.bcbsm.com/EDI/CAQH835Service

2.2 SSL Server Certificate

Non-production (QA) certificate will be the IBM DataPower self signed certificate. The application can acquire the BCBSM certificate from the SSL handshaking process, with web browser or cURL. See appendix for an example using Firefox.

At this time, the certificate is in PEM format. The content in the file appears as follows:

-----BEGIN CERTIFICATE-----
MIIECTCCAvgAwIBAgIETSTANBgkqhkiG9w0BAQUDFADBfMwQswCQDVQQGEwJVUzELMAkGA1UEBhMCTElkIhJvaQIwJGQhMjIwNzE1MTUyWhcNMTIwNzE1MTUyWz4xDDA How the certificate is installed as trusted.

Consumer application will install the certificate as trusted.
Production certificate will be commercial CA signed certificate. So if consumer has the CA loaded as trusted, it is not necessary to load our production certificate. Our production cert is issued by entrust.

You need to load Entrust Certification Authority -1LC in your trust store, which in turn will verify our cert. (See appendix B)

### 2.3 SSL client certificate

As a security requirement, in HTTPS/SSL handshake process, the client will be authenticated. This requires client commercial CA signed certificate to be loaded in BCBSM system.

Client app should follow client side environment procedure to have a key store and CA signed certificate. The HTTPS client should employ the defined key store to call BCBSM WebService end point.
2.4 Authentication/Authorization

Payload authentications will occur using mutual Certificate verification. The Authorization of transaction will occur in EDI System using Provider Authorization lookup completed during TPA process.

2.5 Sample SOAP/Request

The following is the format of a SOAP request:

```xml
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.0.1.xsd">
  <soap:Header/>
  <soap:Body>
    <cor:COREEnvelopeRealTimeRequest>
      <PayloadType/>?
      <ProcessingMode/>?
      <PayloadID/>?
      <!--Optional:-->
      <PayloadLength/>?
      <TimeStamp/>?
      <SenderID/>?
      <ReceiverID/>?
      <CORERuleVersion/>?
      <!--Optional:-->
      <CheckSum/>?
      <!--Optional:-->
      <Payload>cid:387759958045</Payload>
    </cor:COREEnvelopeRealTimeRequest>
  </soap:Body>
</soap:Envelope>
```

2.6 SOAP fault

Based on SOAP specifications, all SOAP applications are required to handle SOAP fault. This is in addition to the application error code. IBM DataPower will return the SOAP1.2 fault in the event of a communication/internal/authentication error. Detail format will be communicated in the SOAP fault message..

<table>
<thead>
<tr>
<th>Error code</th>
<th>Response Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>M0006</td>
<td>Unknown URL (Cannot connect to service)</td>
</tr>
<tr>
<td>M0021</td>
<td>Proxy error (SLM violations, etc.)</td>
</tr>
<tr>
<td>M9999</td>
<td>Unable to process due to unknown or uncategorized error.</td>
</tr>
</tbody>
</table>
Appendix A: Example in obtaining the BCBSM certificate

Using Web Browser
http://servicesdev.bcbsm.com

Click “Exception”
Select ‘View’ to review the certificate.
Select the “Details” tab
Select ‘Export’ and export contents to a file.
The content in the file in the PEM format is as the following.

-----BEGIN CERTIFICATE-----
MIIECTCCAvGgAwIBAgIEJ6eTSTANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJV
UzELMAkGA1UEBhMCTmFukEDAOBgNVBAcTB1JlU0NhbGUx亲
8688DQQGMB4GCSqGSIb3DQEBAQUAA4IBgQBBoQrHbU9y0KdpcaDv7g284MaJc0qBj
86u0bC09Fkm5UWJQYU5A4jkDytaZ4Wz55PhvO5c5595g47CIMP/wh9qDf3epk WHERE
-----END CERTIFICATE-----
Appendix B: Example in obtaining Entrust CA Cert

Firefox → Tools → Options → Advanced → Encryption

Client View Certificates
Export the cert to be loaded in your trusted store.
Appendix C: BCBSM PKI certificate requirements:

The following asymmetric encryption algorithms below are approved for use and should be used in the following order of preference. A maximum key life for each key length is provided and, where possible, key lengths should be selected based on the length of time that certificate renewal will be required to occur – the shorter the key length, the more frequent the renewal period and thus increased administrative overhead.

As a guideline, use key length to allow certificate renewal every 2 years, for e.g., RSA Key length 1792 bits with renewal every 2 years (Refer below RSA table).

### Rivest, Shamir, Adleman (RSA):

<table>
<thead>
<tr>
<th>Key Length (bits)</th>
<th>Maximum Key Life (years)</th>
<th>Key Length (bits)</th>
<th>Maximum Key Life (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1792</td>
<td>2</td>
<td>192</td>
<td>2</td>
</tr>
<tr>
<td>2048</td>
<td>3</td>
<td>256</td>
<td>3</td>
</tr>
<tr>
<td>3072</td>
<td>5</td>
<td>384</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512</td>
<td>7</td>
</tr>
</tbody>
</table>