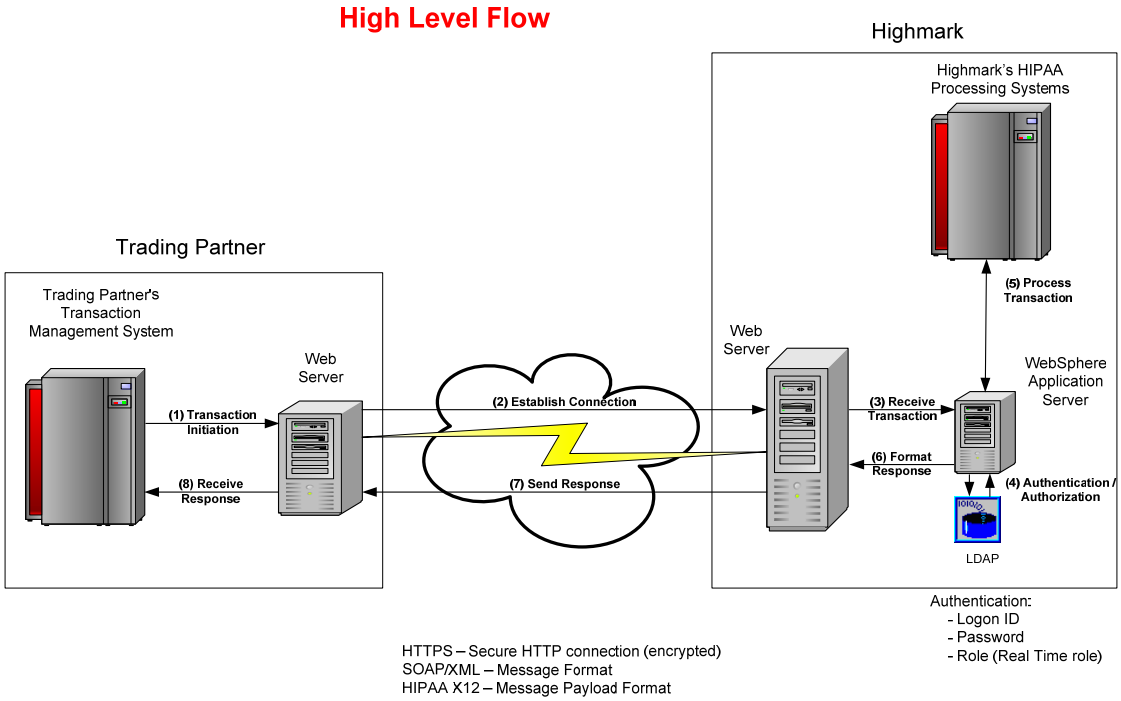
Real-Time Claim Adjudication and Estimation Connectivity Specifications

Mountain State Blue Cross Blue Shield
June 18, 2009

Contents

1. Overview

The Real-Time Claim Adjudication and Estimation process provides the capability to submit and receive ASC X-12N transactions in a real-time mode. Real-Time transactions utilize Simple Object Access Protocol (SOAP). SOAP is a simple XML based protocol to let applications exchange information over HTTP. Since the Internet is being utilized to transport the data, encryption will be utilized to secure messages in the same way financial transactions are secured over the Internet. Access to Mountain States BCBS's networks will follow the same security model in place today, which requires a Login/Password. For additional information regarding HIPAA X-12 transactions, please refer to the EDI Reference Guide.



In order to understand the lifecycle of the transaction, processes have been outlined below:

(1) Transaction Initiation

Mountain State Trading Partner's Transaction Management System will initiate a Real-time X12 HIPAA transaction.

(2) Establish Connection

The Trading Partner's Transaction Management System will establish a secure Internet connection (HTTPS) to Mountain State and send an encrypted SOAP message that contains a HIPAA X12 transaction payload, along with the Trading Partner logon id, and password assigned by Mountain State.

(3) Receive Transaction

Mountain State receives the Real-time request on its Web Server.

(4) Authentication/Authorization

When the SOAP message is received by Mountain State's WebSphere application, the SOAP message will be validated and the Trading Partner's logon id, password and a defined role is authenticated using LDAP (Lightweight Directory Access Protocol). Only Trading Partners that have signed a Mountain State Trading Partner Agreement are granted a logon id's, passwords and defined role.

If the Trading Partner is not authorized to submit a Real-time request, the WebSphere application will return a SOAP invalid security/unauthorized message to the Trading Partner via the secure Internet connection (HTTPS).

(5) Process Transaction

Trading Partners authorized to submit real time requests will have their transactions routed through the WebSphere application to the target system. The target system will generate the Real-time response.

(6) Format Response

The WebSphere Application Server will envelope the response in a SOAP response message.

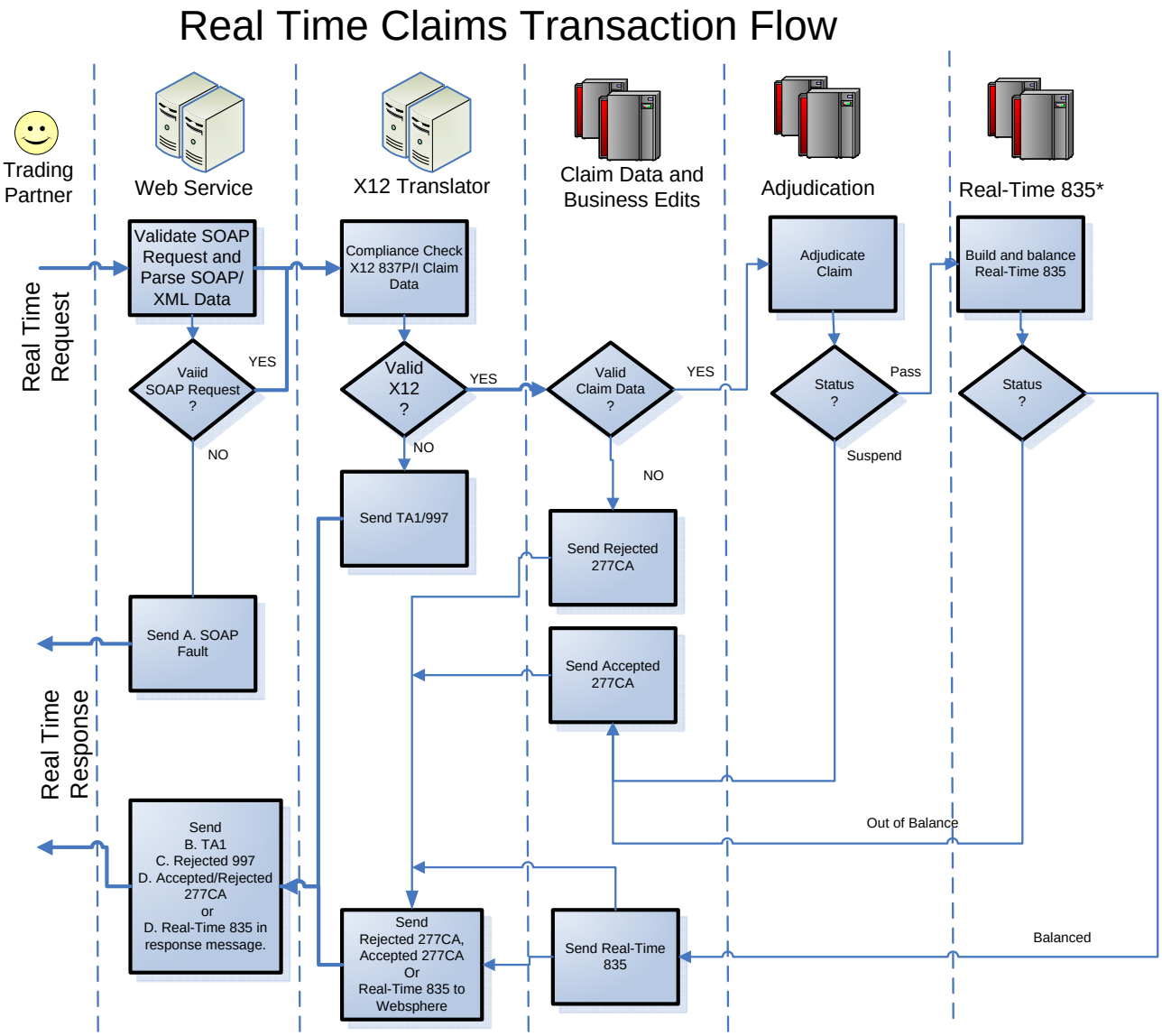
(7) Send Response

The responses will be encrypted, and returned to the Trading Partner via the secure Internet (HTTPS) connection.

(8) Receive Response

The Trading Partner's Web Server will return the response message to the Trading Partner's Transaction Management System that initiated the request.

Real-Time Claim Adjudication/Estimation Transaction Flow:



*Based on the type of Real-Time request indicated by the Trading Partner, the Real-Time 835 is the resulting data from either a real claim adjudication or estimation.

2. Connectivity Requirements for Real-Time Claims

- Trading Partners must submit claim transactions using HTTPS over a public line.

- Trading Partners must be able to connect to the following URLs to send either Demo or Production claims:

    - Trading Partners can connect to the following URL to demo their connectivity and functionality in the Mountain State production region. This URL will only accept Estimation requests and the claim will not be adjudicated in the Mountain State production claims processing system. When using this URL the claims must be transmitted with the ISA15 value of 'T'.
      https://services.highmark.com/rtcrpc/services/demo/RealTimeClaims

    - Trading Partners must be able to connect to the following URL to send Production claims. This URL will accept both an Estimation of liability request, and an Adjudication request for payment. When using this URL a claim must be transmitted with the ISA15 value of 'P'.
      https://services.highmark.com/rtcrpc/services/RealTimeClaims

- Trading Partners must ensure that only authorized persons and/or applications will be able to submit requests to Mountain State with their "logon ID" and password.

- Mountain State Real-Time transactions (Request and Response) are based on standard SOAP 1.1 formats (see the SOAP 1.1 specification at http://www.w3.org/TR/2000/NOTE-SOAP-20000508/ for details of the SOAP 1.1 standards).

- You **MUST** obtain the WSDL files to create your SOAP messages by downloading them from the following URL:
  https://services.highmark.com/rtcrpc/wsdl/RealTimeClaimsService.wsdl

***Note** – Trading Partners will need to add the SOAP header to the WSDL file.

The **HTTP protocol header** must contain the following required properties for all Mountain State Real-Time transactions:

- **Content-Type** = 'text/xml"

- **SOAPAction** = "" No explicit value is necessary and will be ignored (see SOAP 1.1 specification, section 6.1.1)

The **SOAP message header** must contain the following required data elements for all Mountain State Real-Time transactions:

- **Username** = (7 positions, Upper Case) Mountain State assigned login id.

- **Password** = (8 positions) Mountain State assigned password.

The **SOAP message body** must contain the following required data elements for all Mountain State Real-Time transactions:

- **Adjudicate or Estimate** = must contain 'adjudicate' or 'estimate'

  A. **Adjudicate** = SOAP request body must contain this as a beginning and ending tag if a claim is to be submitted for payment.

  B**. Estimate** = SOAP request body must contain this as a beginning and ending tag if a claim is to be submitted for an estimation of patient liability for the service submitted.

- **NaicCode** = must contain 'NAIC Code'

  A. '54771' (Highmark)
  B. '54828' (Mountain State)
  C. '71768' (Highmark Health Ins. Co.)

- **ClientUserId** = (1 to 20 positions) Trading Partner defined (used if Trading Partner wants to uniquely identify the specific user submitting the message. Will also be returned in the SOAP Response).

- **ClientStateData** = (1 to 40 positions) Trading Partner defined (used if Trading Partner wants to return data in the SOAP Response).

NOTE: Although **ClientUserId** and **ClientStateData** are required tags, Mountain State **<u>will not</u>** authenticate/validate content of the data in these fields.

- **X12TypeVersion** = same value as GS08 in the X12 request
  A. '004010X096A1' (837I)
  B. '004010X098A1' (837P)

- The Trading Partner must use a '~' as the segment terminator, the '^' element delimiter and the ':' Component Element Separator.

- The Trading Partner must include a prefix of “R” along with their sender Mountain State BCBS assigned Trading Partner number in data element GS02 of the X-12 837 file.

- The ‘X12’ tag in the SOAP body can only contain a single claim with no more than 50 lines of service. Multiple claims cannot be submitted through the Real-Time process.

- The Trading Partner will be responsible to evaluate the response returned and to resubmit the request with corrections required as indicated by the SOAP fault.

- No XML exception characters (&, <, >, “) or non-printable characters will be used as a delimiter or contained within the data of the message. NOTE: Mountain State recommends the CDATA tag to handle special characters. (See examples of SOAP Message and XML Message below)

DISCLAIMER

Real-time claim transactions are designed to respond to individual end-user claim requests. For typical requests, the average response time should be within 30 seconds. Actual response time will be dependent upon Real-time transaction activity. Batched claim requests will receive rejected 997s.

3. SOAP REQUEST MESSAGE – The following is an example of valid Mountain State Real-Time claim request transaction with a properly formatted SOAP envelope.

Sample 837 Request Message:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope
        xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:rtc="https://services.highmark.com/rtcrpc/schemas/2008/07"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SOAP-ENV:Header>
                <wss:Security
                        xmlns:wss="http://schemas.xmlsoap.org/ws/2003/06/secext">
                        <wss:UsernameToken>
                                <wss:Username>V999999</wss:Username>
                                <wss:Password>xxxxxxxx</wss:Password>
                        </wss:UsernameToken>
                </wss:Security>
        </SOAP-ENV:Header>
        <SOAP-ENV:Body>
```

<rtc:estimate> or <**rtc:adjudicate**>
<rtc:request**>**

<rtc:clientStateData>XXXXXXXXXXX</rtc:clientStateData>
<rtc:clientUserId>XXXXXXXXXX</rtc:clientUserId>
<rtc:naicCode>XXXXX</rtc:naicCode>
<rtc:x12><![CDATA[ISA^00^ ^00^ ^ZZ^EDI0001
^33^54828 ^031020^0929^U^00401^000000315^1^P^:~
GS^HC^R490000^54828^20040810^0928^316^X^004010X096A1~
ST^837^837PHMR1~
BHT^0019^00^490000^20040315^09500000^CH~
REF^87^004010X096A1~
NM1^41^2^TEST SUBMITTER^^^^^46^490000~
PER^IC^CONTACT NAME^TE^9999999999~
NM1^40^2^MOUNTAIN STATE BLUE CROSS /BLUE SHIELD^^^^^46^54828~
HL^1^^20^1~
PRV^BI^ZZ^9999999999~
NM1^85^2^TEST PROVIDER^^^^^XX^9999999999~
N3^SUITE 100^999 JOHN ROAD~
N4^CITY^WV^999999999~
REF^EI^999999999~
HL^2^1^22^0~
SBR^P^18^^^^^^^BL~
NM1^IL^1^JOHN^DOE^^^^MI^999999999~
N3^226 SAMPLE DRIVE~
N4^CITY^WV^99999~
DMG^D8^19810311^F~
NM1^PR^2^ MOUNTAIN STATE BLUE CROSS /BLUE SHIELD ^^^^^PI^54828~
N3^614 MARKET ST~
N4^CITY^WV^99999~
CLM^837PHMR1^280.00^^^11::1^Y^A^Y^A^B^^^^^^P~
DTP^454^D8^20040201~
REF^G1^999~
REF^F8^99999999999~
REF^EA^9999999999999999~
HI^BK:99999~
NM1^DN^1^DOE^BARBARA^^^M.D.^XX^9999999999~
PRV^RF^ZZ^9999999999~
REF^EI^999999999~
NM1^82^1^DOE^PETER^^^^XX^9999999999~
REF^EI^999999999~
LX^1~
SV1^HC:71010^40.00^UN^1^^^1~
DTP^472^RD8^20041106-20041106~
REF^6R^99999999~
LX^2~
SV1^HC:99212^240.00^UN^1^^^1~
DTP^472^RD8^20041108-20041108~
REF^6R^99999999~
SE^41^837PHMR1~
GE^1^316~
IEA^1^000000315~]]></rtc:x12>
<rtc:x12TypeVersion>004010X096A1</rtc:x12TypeVersion>
</rtc:request>
</rtc:estimate> or </rtc:adjudicate>
</SOAP-ENV:Body>

```
</SOAP-ENV:Envelope>
```

4. SOAP RESPONSE MESSAGES – The following are examples of valid Mountain State Real-Time claim response transactions with properly formatted SOAP envelopes.

A. SOAP Faults – When a Real-Time transaction fails validation for the format or content of the SOAP message, the following error codes will be used when responding to the Trading Partner.

Fault Message	FAULTCODE	ClientStateData returned *
Could Not Respond	SOAP-ENV:Server	When Available
Real-Time Not Available	SOAP-ENV:Server	When Available
Faultstring will give Trading Partner a detailed description of failure	SOAP-ENV:Client	When Available
Invalid X12 Interchange Control Header	SOAP-ENV: Client	When Available

An example of a SOAP Fault response with <ClientStateData>:

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <soapenv:Fault>
                        <faultcode>Client</faultcode>
                        <faultstring><![CDATA[error message]]></faultstring>
                        <detail>
                                <clientStateData><![CDATA[state data]]></clientStateData>
                        </detail>
                </soapenv:Fault>
        </soapenv:Body>
</soapenv:Envelope>
```

An example of a SOAP Fault response without <ClientStateData>:

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <soapenv:Fault>
                        <faultcode>Client</faultcode>
                        <faultstring><![CDATA[error message]]></faultstring>
                </soapenv:Fault>
```

```
        </soapenv:Body>
</soapenv:Envelope>
```

NOTE: A “good” (non-SOAP fault) SOAP response message will send an HTTP return code of 2xx (see SOAP 1.1 specification, section 6.2)

B. Rejected TA1

The ASC X12 Interchange Acknowledgment, or TA1, provides the sender a negative confirmation of the interchange control envelopes of the EDI file transmission. If the interchange envelopes (header and trailer) are invalid (i.e. the data is corrupt or the trading partner relationship does not exist) the edit will reject and a TA1, along with the data, will be returned. The entire transmission is rejected at the header level.

Sample TA1 Response Message

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope
        xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:rtc="https://services.highmark.com/rtcrpc/schemas/2008/07"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SOAP-ENV:Body>
                <rtc:estimateResponse>
                        <rtc:estimateReturn>
                          or
                <rtc:adjudicateResponse>
                        <rtc:adjudicateReturn>
                                <rtc:clientStateData><![CDATA[XXXXXXXXXXX]]></rtc:clientStateData>
                                <rtc:clientUserId>XXXXXXXXXX</rtc:clientUserId>
                                <rtc:naicCode>XXXXX</rtc:naicCode>
                                <rtc:x12><![CDATA[ISA*00* *00* *33*54828 *ZZ*EDIR403
*080806*1227*U*00401*000000001*0*P*:~
TA1*000000315*031020*0929*R*008~
IEA*0*000000001~]]></rtc:x12>
                                <rtc:x12TypeVersion>004010X098A1</rtc:x12TypeVersion>
                        </rtc:estimateReturn>
                </rtc:estimateResponse>
                          or
                        </rtc:adjudicateReturn>
                </rtc:adjudicateResponse>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

C. Rejected 997

The ASC X12 997, or Functional Acknowledgment, provides the sender negative confirmation of the structure of the ASC X12N 837P/I EDI file. If the EDI file contained syntactical errors, the segment(s) and element(s) where the error(s) occurred may be reported.

Sample 997 Response Message:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope
        xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:rtc="https://services.highmark.com/rtcrpc/schemas/2008/07"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SOAP-ENV:Body>
                <rtc:estimateResponse>
                        <rtc:estimateReturn>
                          or
                <rtc:adjudicateResponse>
                        <rtc:adjudicateReturn>
                                <rtc:clientStateData><![CDATA[XXXXXXXXXXX]]></rtc:clientStateData>
                                <rtc:clientUserId>XXXXXXXXXX</rtc:clientUserId>
                                <rtc:naicCode>XXXXX</rtc:naicCode>
                                <rtc:x12><![CDATA[ISA^00^ ^00^ ^33^54828 ^ZZ^EDIR403
^080806^1230^U^00401^000000001^0^P^:~
GS^FA^54828^R499952^20080806^123000^1^X^004010~
ST^997^0001~
AK1^HC^316~
AK2^837^837PHMR11~
AK3^NM1^4^1000A^1~
AK3^NM1^4^1000A^8~
AK4^1^98^7^99~
AK5^R^5~
AK9^R^1^1^0~
SE^9^0001~
GE^1^1~
IEA^1^000000001~]]></rtc:x12>
                                <rtc:x12TypeVersion>004010X098A1</rtc:x12TypeVersion>
                        </rtc:estimateReturn>
                </rtc:estimateResponse>
                          or
                        </rtc:adjudicateReturn>
                </rtc:adjudicateResponse>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

D. Accepted/Rejected 277CA (Claim Acknowledgment)

The 277 Claim Acknowledgment (277CA) is a Mountain State created version of a Claim Acknowledgment transaction that is used to return a reply of “accepted” or “not accepted” for claims or estimates submitted via the 837P/I transaction. Acceptance at this level is based on 837P/I Implementation Guides and Mountain State’s front-end edits.

Sample 277 Response Message:

```
<?xml version="1.0"?>
```

```
<SOAP-ENV:Envelope
        xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:rtc="https://services.highmark.com/rtcrpc/schemas/2008/07"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SOAP-ENV:Body>
                <rtc:estimateResponse>
                        <rtc:estimateReturn>
                          or
                <rtc:adjudicateResponse>
                        <rtc:adjudicateReturn>
                                <rtc:clientStateData><![CDATA[XXXXXXXXXXX]]></rtc:clientStateData>
                                <rtc:clientUserId>XXXXXXXXXX</rtc:clientUserId>
                                <rtc:naicCode>XXXXX</rtc:naicCode>
                                <rtc:x12><![CDATA[ISA^00^          ^00^          ^33^54828
^ZZ^EDI0001       ^070116^1604^U^00401^007139232^0^P^:~
GS^HN^54828^R490000^20070116^104551^16302356^X^004010H01~
ST^277^0002~
BHT^0010^06^000000053^20070116^^TH~
NM1^41^2^MOUNTAIN STATE BLUE CROSS/BLUE SHIELD^^^^^NI^54828~
HL^1^^20^1~
NM1^PR^2^ MOUNTAIN STATE BLUE CROSS/BLUE SHIELD^^^^^NI^54828~
HL^2^1^21^1~
NM1^40^2^^^^^^93^490000~
HL^3^2^19^1~
NM1^85^2^TEST PROVIDER^^^^^XX^9999999999~
HL^4^3^22^1~
NM1^IL^1^JOHN^DOE^^^^MI^999999999~
HL^5^4^23^0~
DMG^D8^19960507~
NM1^03^1^DOE^BARBARA~
TRN^2^2589~
STC^A2^20^^^115~
REF^1K^1234567899999~
DTP^050^D8^20070116~
DTP^232^D8^20070105~
SE^19^0002~
GE^1^16302356~
IEA^1^007139232~]]></rtc:x12>
                                <rtc:x12TypeVersion>004010X098A1</rtc:x12TypeVersion>
                        </rtc:estimateReturn>
                </rtc:estimateResponse>
                          or
                        </rtc:adjudicateReturn>
                </rtc:adjudicateResponse>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

NOTE: A “good” (non-SOAP fault) SOAP response message will send an HTTP return code of 2xx (see SOAP 1.1 specification, section 6.2)

E. Real-Time 835 Response

The Real-Time 835 response will be based on the ASC X12N 835 Transaction adopted under the HIPAA Administrative Simplification Electronic Transaction rule. The Real-Time 835 will contain the results from a successful estimation request or claim adjudication (without the actual payment/check information). Estimation requests will not result in claim payment.

Sample 835 Response Message:

<?xml version="1.0"?>
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:rtc="https://services.highmark.com/rtcrpc/schemas/2008/07"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<SOAP-ENV:Body>
<**rtc:estimateResponse**>
<rtc:estimateReturn>
or
<**rtc:adjudicateResponse**>
<rtc:adjudicateReturn>
<rtc:clientStateData><![CDATA[XXXXXXXXXXX]]></rtc:clientStateData>
<rtc:clientUserId>XXXXXXXXXX</rtc:clientUserId>
<rtc:naicCode>XXXXX</rtc:naicCode>
<**rtc:x12**>**<![CDATA[**ISA^00^ ^00^ ^33^54828
^ZZ^EDIR403 ^081006^1059^U^00401^000000315^0^P^>~
GS^HP^54828^R499952^20081006^10590642^316^X^004010X091A1~
ST^835^093B711DD~
BPR^H^0^C^NON^^^^^^^^^^^20081006~
TRN^1^7801636695^1231294723~
REF^EV^499952~
DTM^405^20081006~
N1^PR^ MOUNTAIN STATE BLUE CROSS/BLUE SHIELD~
N3^614 MARKET STREET~
N4^PARKERSBURG^WV^26101~
REF^NF^54828~
PER^CX^^TE^8669755054~
N1^PE^SOME DOCTORS OFFICEI^FI^999999999~
N3^123 MAIN STREET^SUITE 100 B~
N4^ANYTOWN^WV^999996459~
REF^PQ^9999999~
LX^1~
CLP^A837PHM01^4^480^0^480^16^08280551402~
NM1^QC^1^PATIENT^TEST^J^^^MI^123456789~
NM1^82^1^^^^^^XX^111111111~
REF^CE^SG~
DTM^050^20081006~
PER^CX^^TE^9999999999~
SVC^HC>99212^240^0~
DTM^472^20041208~
CAS^PR^31^240~
REF^6R^POCT0073~
SVC^HC>99212^240^0~

DTM^472^20041210~
CAS^PR^31^240~
REF^6R^POCT0073~
SE^30^093B711DD~
GE^1^316~
IEA^1^000000315]]></rtc:x12>
<rtc:x12TypeVersion>004010X091A1</rtc:x12TypeVersion>
</**rtc:estimateReturn**>
</rtc:estimateResponse>
or
</rtc:adjudicateReturn>
</**rtc:adjudicateResponse**>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

NOTE: A "good" (non-SOAP fault) SOAP response message will send an HTTP return code of 2xx (see SOAP 1.1 specification, section 6.2)

5. Highmark EDI WebServices Certificate

This Section will explain how to save to a file the certificate used by the Highmark Web Services Gateway. Highmark offers the use of web services to perform Mountain State BCBS EDI transactions. Since these transactions require the utmost security, all data is encrypted and transmitted over Secure Sockets Layer Protocol (SSL). The document will provide some links to information about SSL and instructions for downloading to a file the Highmark certificate that would be required to be setup as a Truststore to establish a SSL connection with the web services gateway server. Note: This document is meant for individuals whom have information technology experience and an understanding of SSL and web services.

A. Introduction

Prior to obtaining the Highmark Public Certificate for the enablement of the Mountain State BCBS EDI web services one should have an understanding of SSL. Here's a link to a SSL Introduction:

Introduction to SSL

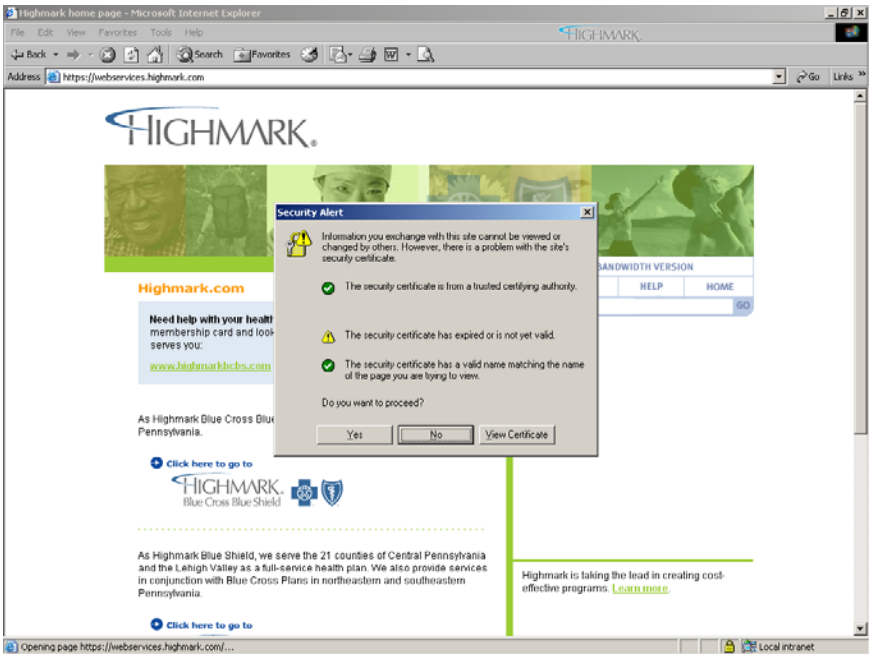
B. Downloading the Digital Certificate.

These instructions are for Windows Internet Explorer.

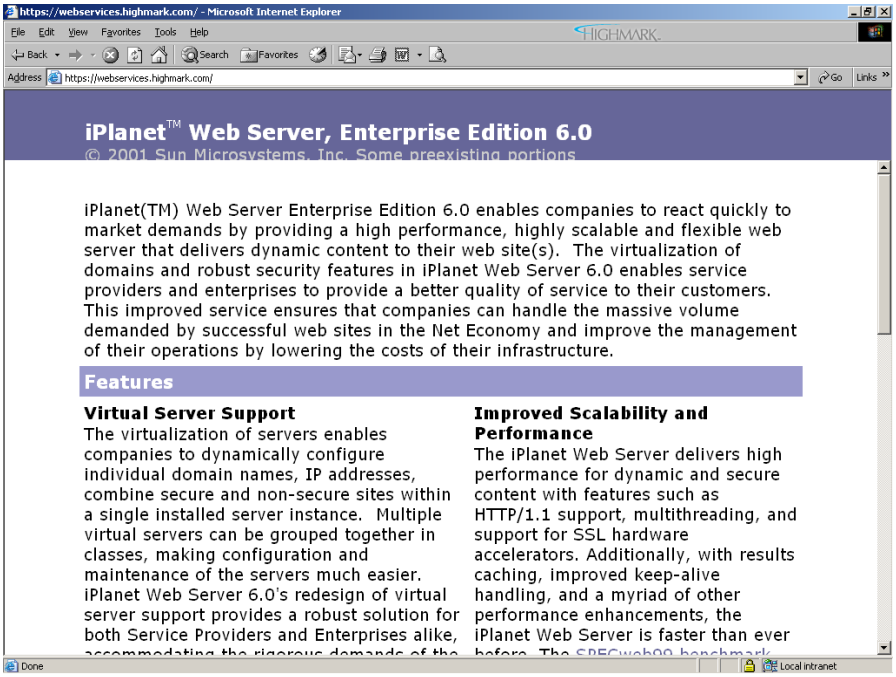
First, open a web browser to the **https://services.highmark.com** home page. You should notice a "Security Alert" window on this window select the View Certificate

button. (Note: if you do not see the “Security Alert” window, skip to the next screen example)

NOTE: The following snap shots are only examples that do not reflect current data.



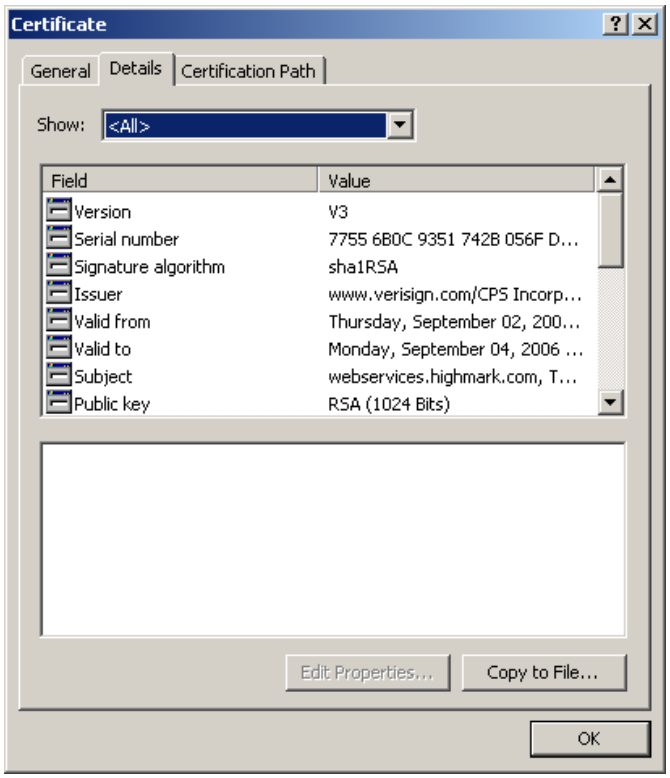
If you not did not see the Security Alert window, double click on the gold “LOCK” icon at the bottom right status bar of your Windows Internet Explorer Browser.


https://webservices.highmark.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
HIGHMARK.
Back Search Favorites
Address https://webservices.highmark.com/
Go Links
iPlanet™ Web Server, Enterprise Edition 6.0
© 2001 Sun Microsystems, Inc. Some preexisting portions
iPlanet(TM) Web Server Enterprise Edition 6.0 enables companies to react quickly to market demands by providing a high performance, highly scalable and flexible web server that delivers dynamic content to their web site(s). The virtualization of domains and robust security features in iPlanet Web Server 6.0 enables service providers and enterprises to provide a better quality of service to their customers. This improved service ensures that companies can handle the massive volume demanded by successful web sites in the Net Economy and improve the management of their operations by lowering the costs of their infrastructure.
Features
Virtual Server Support
The virtualization of servers enables companies to dynamically configure individual domain names, IP addresses, combine secure and non-secure sites within a single installed server instance. Multiple virtual servers can be grouped together in classes, making configuration and maintenance of the servers much easier. iPlanet Web Server 6.0's redesign of virtual server support provides a robust solution for both Service Providers and Enterprises alike,
Improved Scalability and Performance
The iPlanet Web Server delivers high performance for dynamic and secure content with features such as HTTP/1.1 support, multithreading, and support for SSL hardware accelerators. Additionally, with results caching, improved keep-alive handling, and a myriad of other performance enhancements, the iPlanet Web Server is faster than ever
Done
Local intranet

Right Here

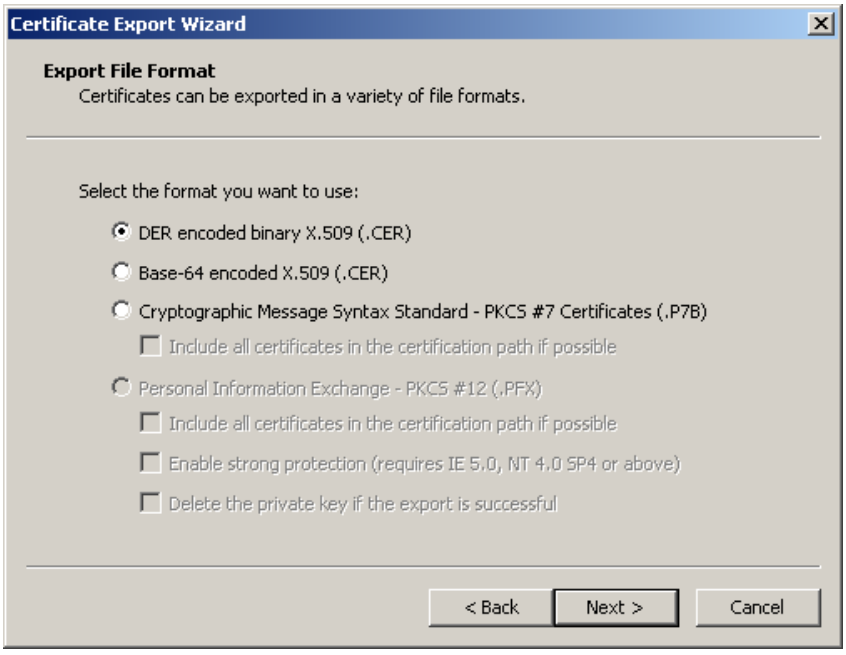
Next, you'll see the Certificate Window which displays the general information about the Certificate. Select the Details tab.

On the Details tab, select the “Copy to File…” button at the lower right corner.

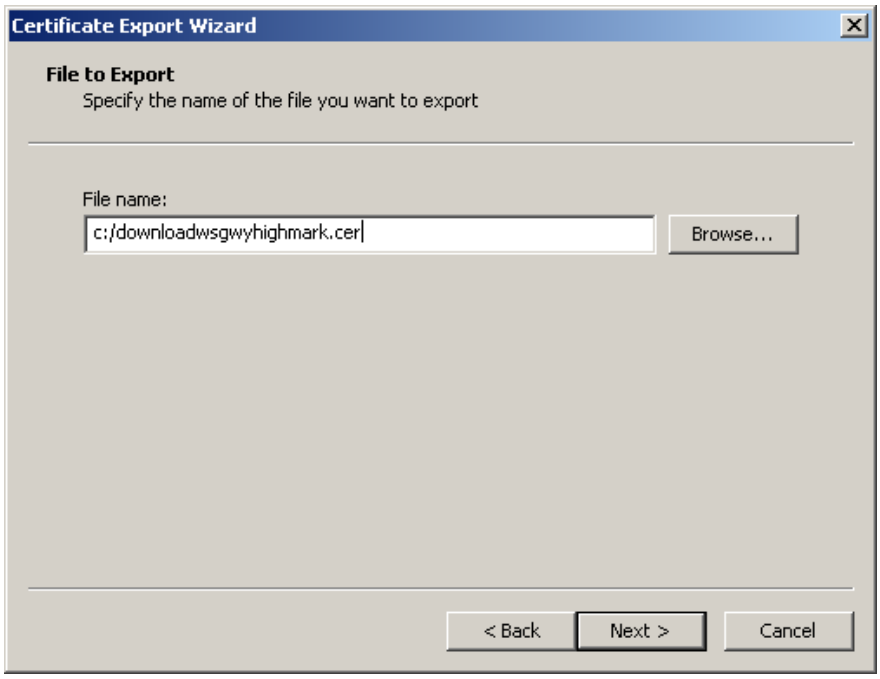


You should now see the Welcome window for the Certificate Export Wizard for windows. Select the Next Button.

Select the File Format. In this example, the default DER encoded binary X.509 is selected. Click Next.



Enter the file name to save the certificate under. In this example **C:/downloadwsgwyhighmark.cer** was used. Click Next.



Select Finish Button…

C. What to do next.

In order to establish a SSL connection via a web services client usually one needs to load the certificate to the "Truststore" file configured for the client's platform in which the web service will be invoked. Since, there are too many web services client platforms to mention in this guide, one will need to review the documentation associated with the web services client platform. For example, to obtain information for a client platform like IBM's WebSphere Application Server one could perform a search on Google(www.google.com) for: "ibm websphere Truststore how to" or examine the Websphere Information Center Documentation.

D. Renewing the Certificate

Digital Certificates have a specific expiration date and will need to be renewed. In the example below the **General Tab** identifies the **Valid To and From dates** for the Certificate. Each Real-Time Trading Partner will receive an email 4 weeks before the certificate expires. (Note: Email addresses should be supplied by the EDI Trading Partner upon applying for Real-Time access.) The email will include the date the new certificate will be available for download and the date the new certificate will be activated. Repeat the above steps to incorporate the renewed certificate in your application.