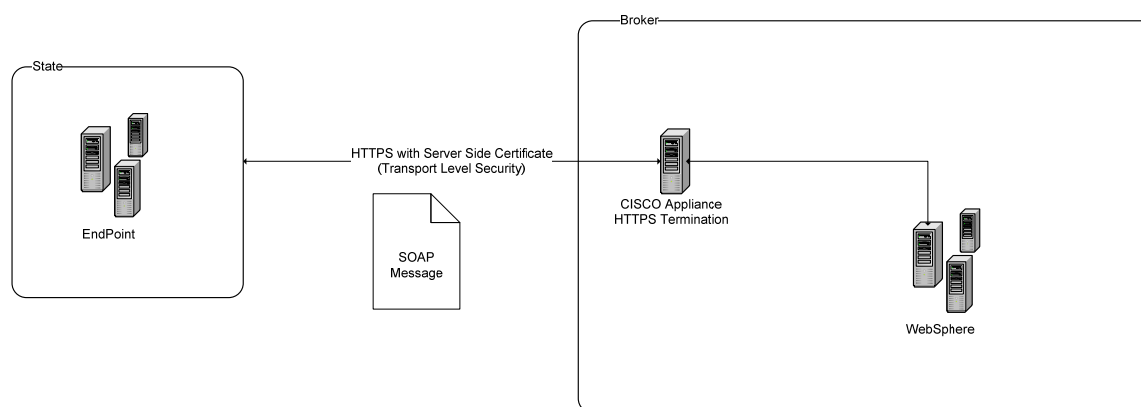


5 Security Framework

5.1 Purpose and Summary

The Security Framework describes the steps taken so that messages can be passed safely between connectors via the Broker. All messages passed between the Broker and connectors are secured using Transport-Layer Security (HTTPS/SSL) and Message-Layer security (XML Digital Signature using sender's X.509 certificate, XML Encryption and XML Secure Timestamp,). Message-Layer security is implemented according to the OASIS WS-Security 1.1 specification (<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>).



5.2 Transport-Layer Security: HTTPS

SOAP over HTTPS is the communication method that is used by SIDES. The Broker will have a server side token signed by a Certificate Authority. The HTTPS communication will be terminated by a CISCO Appliance as specified in the Bill of Materials. The resulting HTTP message will then be forwarded on to the Websphere box.

5.3 Message-Layer Security: Sender's X.509 Certificate and XML Digital Signature

The Broker and connectors use their X.509 Certificates to produce an XML Digital Signature of the SOAP message, and both the signature and the certificate are included in the message Soap header. The message receiver will use the X.509 certificates to authenticate the sender, and will validate the digital signature to ensure message integrity. If either certificate authentication or signature validation fails, the message is deleted and the http request/response pattern is terminated.

When authenticating the senders certificate, the reciever will ensure that the certificate was issued by a trusted Certificate Authority and that the certificate is not expired. The receiver will also ensure that the certificate owner matches the sender as specified in the message's From: SOAP custom header.

Connectors will provide the Broker their X.509 Certificate for authentication and signature validation purposes as part of their initial set-up procedures (**Connectors are required to procure and provide their own X.509 Certificate**). The Broker will also provide each connector a copy of its X.509 Certificate.

The Broker will store all received message XML Digital Signatures with the reporting data so that they can be accessed at a much later date.

Certificates must be generated with a Signature Algorithm of SHA1withRSA and include a SubjectKeyIdentifier.

5.4 Message-Layer Security: XML Encryption

Message sender will encrypt the payload element content (not the entire payload element) using the receiver's X.509 certificate. For example, connectors will use the Broker's certificate to encrypt the payload element content, and the Broker will use the certificate of the connector it is sending the message to. Encryption of the payload element content provides the confidentiality that is required outside of relying on the Transport-layer security mechanism.

5.5 Message-Layer Security: XML Secure Timestamp

An XML Secure Timestamp is included by the sender in the Soap header for the receiver to evaluate the length of time since the message was formulated. One of the main uses of the WS-Security message timestamp is to introduce some entropy in the message to protect against replay attacks. The timestamp expiration limit is set at 15 minutes.

5.6 Example State Post SOAP message with Message-Layer security applied

<This section deleted for security reasons>

<For the complete unredacted version of this document, please contact:
David Zemel at dzemel@itsc.org>

<This page deleted for security reasons>

<This page deleted for security reasons>

<This section deleted for security reasons>

5.7 Application of Security to the SOAP Message

<This section deleted for security reasons>

<For the complete unredacted version of this document, please contact:
David Zemel at dzemel@itsc.org>