# Security

## HTTPS

An HTTPS connection will be required to access the web service (which will be hosted on an internet accessible web server). The use of HTTPS protects sensitive subscriber information from being read by unauthorized third parties.

The SSL Certificate was deployed and is maintained by Verisign.

## WSS

Web Service Security (WSS) will also be employed to ensure that the party calling the web service is authorized to access it.

See <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd> for a detailed XML schema of the WSS SOAP extension.

To authorize, a valid WSS security section must be added to the SOAP header. The password type is 'PasswordDigest'. This is an example header for a user with the name "test":

<soapenv:Header>

<wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-open.org/

wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">

<wsse:UsernameToken wsu:Id="UsernameToken-18356845"

xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-

utility-1.0.xsd">

<wsse:Username>test</wsse:Username>

<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-

username-token-profile1.0#PasswordDigest">

eXrPjBcilJFOG2FPQC/FQCdEd9s=

</wsse:Password>

<wsse:Nonce>

s3POm7QyECq86HJJ2LMWIw==

</wsse:Nonce>

<wsu:Created>

2010-07-10T11:14:01.301Z

</wsu:Created>

</wsse:UsernameToken>

</wsse:Security>

</soapenv:Header>

Please note that 'Password', 'Nonce' and 'Created' XML tags have to conform to the WSS specification and are usually auto-generated by the web service framework in use. The actual username and password to be used will be supplied separately to this document.

For deployment in Axis under Apache-Tomcat, please refer to the documentation in <http://ws.apache.org/wss4j/axis.html>. For Jboss, please refer to this documentation site : <http://docs.redhat.com/docs/en-US/JBoss_Enterprise_Web_Platform/5/html/JBoss_WS_CXF_User_Guide/ch11.html>

The whole specification of the security schema is published at

http://www.oasis-open.org/standards#wssv1.1

http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

(attached in this document) 

Information about OASIS (taken from the About page from their site)

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

OASIS is distinguished by its transparent governance and operating procedures. Members themselves set the OASIS technical agenda, using a lightweight process expressly designed to promote industry consensus and unite disparate efforts. Completed work is ratified by open ballot. Governance is accountable and unrestricted. Officers of both the OASIS Board of Directors and Technical Advisory Board are chosen by democratic election to serve two-year terms. Consortium leadership is based on individual merit and is not tied to financial contribution, corporate standing, or special appointment.

The Consortium hosts two of the most widely respected information portals on XML and Web services standards, Cover Pages and XML.org. OASIS Member Sections include Blue, CGM Open, COSL, eGov, Emergency, IDtrust, LegalXML, Open CSA, and Telecom.

SGML Open

OASIS was founded in 1993 under the name SGML Open as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). OASIS changed its name in 1998 to reflect an expanded scope of technical work, including the Extensible Markup Language (XML) and other related standards.

## Web Service Security Schema

Inside the Web Service, additional security is maintained:

There are two types of permissions for the web service:

1.3.1 By IP address

There is a list of "trusted" ip addresses, which usually reside in the organization, and are maintained for internal platforms. These ones are trusted to use the web service without using a username and password.

1.3.2. By username and password

There is also a list of username and passwords, which can use the webservice. These users must use the username/password security schema of WS Security, maintained by OASIS, using the Password Digest security token. Additionally, there is an additional security which allows only certain IP addresses to use this username and password.

Both security schemas are maintained in the internal database, and for each type, there is a specific list of methods that the user of the web service can use.