IMS General Web Services Security Profile

Version 1.0 Final Specification

IPR and Distribution Notices

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

IMS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on IMS's procedures with respect to rights in IMS specifications can be found at the IMS Intellectual Property Rights web page: http://www.imsglobal.org/ipr/imsipr_policyFinal.pdf.

If you wish to copy or distribute this document, you must complete a valid Registered User license registration with IMS and receive an email from IMS granting the license to distribute the specification. To register, follow the instructions on the IMS website: http://www.imsglobal.org/specificationdownload.cfm.

This document may be copied and furnished to others by Registered Users who have registered on the IMS website provided that the above copyright notice and this paragraph are included on all such copies. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to IMS, except as needed for the purpose of developing IMS specifications, under the auspices of a chartered IMS project group.

Use of this specification to develop products or services is governed by the license with IMS found on the IMS website: http://www.imsglobal.org/license.html.

The limited permissions granted above are perpetual and will not be revoked by IMS or its successors or assigns.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE CONSORTIUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Document Name: IMS General Web Services Security Profile

Date: 19 December 2005

Executive Summary

The IMS General Web Service Base Profile provides a basic structure for the definition of Web Services. It consists of a set of non-proprietary Web Services specifications, along with clarifications and amendments to those specifications that promote interoperability. The General Web Services Base Profile addresses the most common problems experienced when implementing web service specifications. The General Web Services Base Profile defines the selection of mechanisms within referenced specifications that are well understood, widely implemented and useful.

The IMS General Web Services (GWS) Base Profile promotes interoperability across web specifications implementations on different software and vendor platforms. The IMS GWS Base Profile focuses on a core set of web service specifications and the most common problems experienced implementing the identified web service specifications. It is not a goal of the IMS GWS Base Profile to create a plug-and-play architecture for web services or to guarantee complete interoperability. The IMS GWS Base Profile addresses interoperability in the application layer, in particular, the description of behaviors exposed via Web Services.

The IMS General Web Service Security Profile extends the IMS GWS Base Profile to allow the support of a range of secure architectures. The Web Service Interoperability (WS-I) Organization is developing their Basic Security Profile. This profile is too immature for immediate adoption by IMS Global Learning Consortium (IMS/GLC). Therefore, the IMS GWS Security Profile contains only general recommendations and these will be revisited once the WS-I Basic Security Profile has matured.

Security for web services, as with any network-oriented information technology, is vital. Web services security builds on existing security standards for confidentiality, integrity, non-repudiation, authentication and authorization at the transport, platform and application level. The key to security is analyzing the potential threats and implementing countermeasures to reduce risk to an acceptable level. Selecting the appropriate countermeasures and defining the acceptable level of risk is best done on an individual basis for each implementation. Securing the network traffic is a simple way to provide message integrity and confidentiality between points. Mechanisms for securing network traffic include Secure Socket layer, Transport Layer Security, Virtual Private Network and IP Security.

Table of Contents

EXECUTIVE SUMMARY **2**
1. INTRODUCTION **4**
1.1 SCOPE AND CONTEXT 4
1.2 STRUCTURE OF THIS DOCUMENT 4
1.3 NOMENCLATURE 4
1.4 REFERENCES 5
2. SECURITY PROFILE GUIDELINES **6**
2.1 WS-I BASIC SECURITY PROFILE 6
2.2 GENERAL RECOMMENDATIONS 6
APPENDIX A – GLOSSARY OF TERMS **7**
ABOUT THIS DOCUMENT **9**
LIST OF CONTRIBUTORS 9
REVISION HISTORY **10**
INDEX **11**

1. Introduction

1.1 Scope and Context

The IMS General Web Services (GWS) Base Profile (GWSBP) [GWS, 05] provides a basic structure for the definition of Web Services. It consists of a set of non-proprietary Web Services specifications, along with clarifications and amendments to those specifications that promote interoperability. The IMS GWS Base Profile addresses the most common problems experienced implementing web service specifications. The IMS GWS Base Profile defines the selection of mechanisms within referenced specifications that are well understood, widely implemented and useful.

The IMS GWS Security Profile extends the IMS GWS Base Profile to allow the support of a range of secure architectures. The Web Service Interoperability (WS-I) Organization is developing their Basic Security Profile. This profile is too immature for immediate adoption by IMS Global Learning Consortium (IMS/GLC). Therefore, this profile contains only general recommendations and these will be revisited once the WS-I Basic Security Profile has matured.

1.2 Structure of this Document

The structure of this document is:

2. Security Profile Guidelines	The guidelines that are recommended when extending the IMS GWS Base Profile for secure applications;
Appendix A – Glossary of Terms	Definition of the concepts, terms and technologies used within this document. This material complements the Abstract framework Glossary.

1.3 Nomenclature

GWSBP	General Web Services Base Profile
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol over Secure Socket Layer
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	IP Security
RSA	Rivest, Shamir and Adleman
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WS-I	Web Services Interoperability Organization
XML	Extensible Mark-up Language
XSD	XML Schema Definition

1.4 References

[GWS, 05] *IMS General Web Services Base Profile v1.0 Final Release*, C.Schroeder, J.Simon and C.Smythe, V1.0 IMS/GLC, December 2005.

[WSI, 04a] *Web Services Interoperability Basic Profile Version 1.1*, Eds K.Ballinger, D.Ehnebuske, C.Ferris, M.Gudgin, C.K.Liu, M.Nottingham and P.Yendluri, Web Services-Interoperability Organization, August 2004.

[WSI, 05] *WS-I Basic Security Profile Version 1.0 (Working Group Draft)*, A.babir, M.Gudgin, M.McIntosh and K.Scott, Web Services-Interoperability Organization, August 2005.

2. Security Profile Guidelines

2.1 WS-I Basic Security Profile

The WS-I has recently issued its draft Basic Security Profile [WSI, 05]. From the perspective of IMS/GLC this work is too immature for adoption, i.e., it is still a work in progress. Once this specification has been finalized then IMS/GLC will undertake a formal review with respect to full adoption. While IMS/GLC cannot formally state that the WS-I Basic Security Profile will be adopted as part of the IMS GWS specification it is recommended that wherever possible the current guidance by WS-I should be followed.

2.2 General Recommendations

Security for web services, as with any network-oriented information technology, is vital. Web services security builds on existing security standards for confidentiality, integrity, non-repudiation, authentication and authorization at the transport, platform and application level. The key to security is analyzing the potential threats and implementing countermeasures to reduce risk to an acceptable level. Selecting the appropriate countermeasures and defining the acceptable level of risk is best done on an individual basis for each implementation.

Securing the network traffic is a simple way to provide message integrity and confidentiality between points. Mechanisms for securing network traffic include Secure Socket Layer (SSL), Transport Layer Security (TLS), Virtual Private Network (VPN) and IP Security (IPSEC). The most widely used pattern for encrypted transport connections is HTTPS with SSL/TLS. In the WS-I Basic Profile 1.1 [WSI, 04a] normative statements R5000, R5001, and R5010, the use of HTTPS with SSL/TLS is recommended but not mandated. Other security technologies may be used as well. HTTPS with client-side certificates may be used to provide client authentication.

Appendix A – Glossary of Terms

Throughout the General Web Services documents a variety of key terms, concepts and descriptions have been introduced. These terms, concepts and descriptions and defined below but where appropriate the normative definition from the IAF Glossary is referenced [AbsGloss, 03].

HTTP over Secure Socket Layer (HTTPS)	HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS and SSL support the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the sender. SSL is an open nonproprietary protocol that Netscape has proposed as a standard to the World Wide Consortium (W3C). HTTPS is not to be confused with S-HTTP a security-enhanced version of HTTP developed and proposed as a standard by EIT.
IPSEC	IPSEC, short for IP Security, is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement *Virtual Private Networks* (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.
Secure Socket Layer (SSL)	The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by *Transport Layer Security* (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.
Transport Layer Security (TLS)	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the *Secure Sockets Layer* (SSL). TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard. The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. The TLS protocol is based on Netscape's SSL 3.0 protocol. However, TLS and SSL are not interoperable.

Virtual Private Network (VPN)	A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.
WS-I Basic Security Profile	The Basic Security Profile from the Web Services Interoperability (WS-I) Organization document consists of a set of non-proprietary Web services specifications, along with clarifications to and amplifications of those specifications that promote interoperability. The Profile was developed according to a set of principles that, together, form the philosophy of the Basic Security Profile 1.0, as it relates to bringing about interoperability.
WS-Security	WS-Security defines a standard way to incorporate security information into a SOAP message using existing security standards for confidentiality, integrity, non-repudiation, authentication and authorization. WS-Security provides a method for representing security information in a SOAP message. WS-Security defines a way to pass security tokens, such as a simple username, SAML, X.509 certificates and Kerberos tickets, a mechanism using XML Signature to digitally sign all or part of a SOAP message, a mechanism using XML Encryption to encrypt part of a SOAP message and a method for attaching signature and encryption headers to a SOAP message.
WS-Security Minimalist Profile	The WS-Security Minimalist Profile defines a subset of the Web Services Security: SOAP Message Security (WS-Security) specification that constrains the core specification so that messages received by resource-limited platforms can be processed efficiently. The WS-Security specification describes a flexible method for securing SOAP Messages, providing message integrity and confidentiality, and exchanging security information through SOAP Messages. WS-Security can be used to support a wide variety of security models. WS-Security supports multiple security token formats, multiple trust domains, multiple signature formats, multiple encryption technologies and end-to-end message content security. WS-Security and WS-Security Minimalist Profile provide a framework and syntax to enable applications to exchange SOAP messages in a secure manner. The use and implementation of WS-Security or WS-Security Minimalist Profile does not negate the need to ensure that the systems constructed are not vulnerable to attacks.

About This Document

Title	IMS General Web Services Security Profile
Editor	Colin Smythe (IMS)
Team Co-Leads	Cathy Schroeder (Microsoft Corp.), James Simon (SUN Microsystems Corp.)
Version	1.0
Version Date	19 December 2005
Status	**Final Specification**
Summary	This document contains the description of the IMS approach to supporting security architectures in the IMS General Web Services Base Profile. At the present time no recommendation is made on what security standards/specifications should be used with the IMS General Web Services Base Profile. This is because there is still to much uncertainty for implementation in the area of security and Web Services.
Revision Information	19 December 2005
Purpose	This document is circulated for public adoption. This document is to be adopted by IMS and all other organizations that wish to enhance the IMS General Web Services Base Profile to support security.
Document Location	http://www.imsglobal.org/gws/gwsv1p0/imsgws_securityProfv1p0.html

To register any comments or questions about this specification please visit:
http://www.imsglobal.org/developers/ims/imsforum/categories.cfm?catid=20

List of Contributors

The following individuals contributed to the development of this document:

Name	Organization
Fred Beshears	UC Berkeley
John Evdemon	Microsoft Corp.
Ron Kleinman	SUN Micrsosystems Corp.
Sherman Mohler	Cisco Learning Institute, Inc.
Cathy Schroeder	Microsoft Corp.
James Simon	SUN Microsystems Corp.
Colin Smythe	Dunelm Services Ltd.
Scott Thorne	MIT

Revision History

Version No.	Release Date	Comments
Final v1.0	19 December 2005	This is the first formal version of the Final Release.

Index

A
Abstract Framework 8

B
Base Profile 2, 5, 10

C
Context 5

E
Encryption 8, 9

G
General Web Services Base Profile 5

I
IMS General Web Services 1, 2, 5, 6, 7, 10
  Base Profile 1, 2, 5, 6, 10
  Security Profile 1, 2, 5, 10
Internet Protocol 5
IP Security 2, 5, 7, 8

P
Protocols
  HTTP 5, 8
  HTTPS 5, 7, 8
  IP 2, 5, 7, 8
  IPSEC 2, 5, 7, 8
  SOAP 9
  SSL 5, 7, 8
  TCP 5
  TLS 5, 7, 8

S
Secure Socket Layer 5, 7, 8
Security 2, 5, 7, 8, 9
SOAP 9

T
TCP 5
TLS 5, 7, 8
Transmission Control Protocol 5
Transport Layer Security 2, 5, 7, 8

V
Virtual Private Network 2, 5, 7, 8, 9

W
W3C 5, 8
Web Services 2, 5, 6, 8, 9, 10
  SOAP 9
  WS-Security 9
Web Services Interoperability Organization 2, 5, 6, 7, 9
WS-I
  Basic Profile 7
  Basic Security Profile 2, 5, 6, 7, 9
WS-I Basic Profile 7
WS-I Basic Security Profile 2, 5, 6, 7, 9
WS-Security 9

X
XML 5, 9
XML Schema 5
XML Schema Definition 5
XSD 5