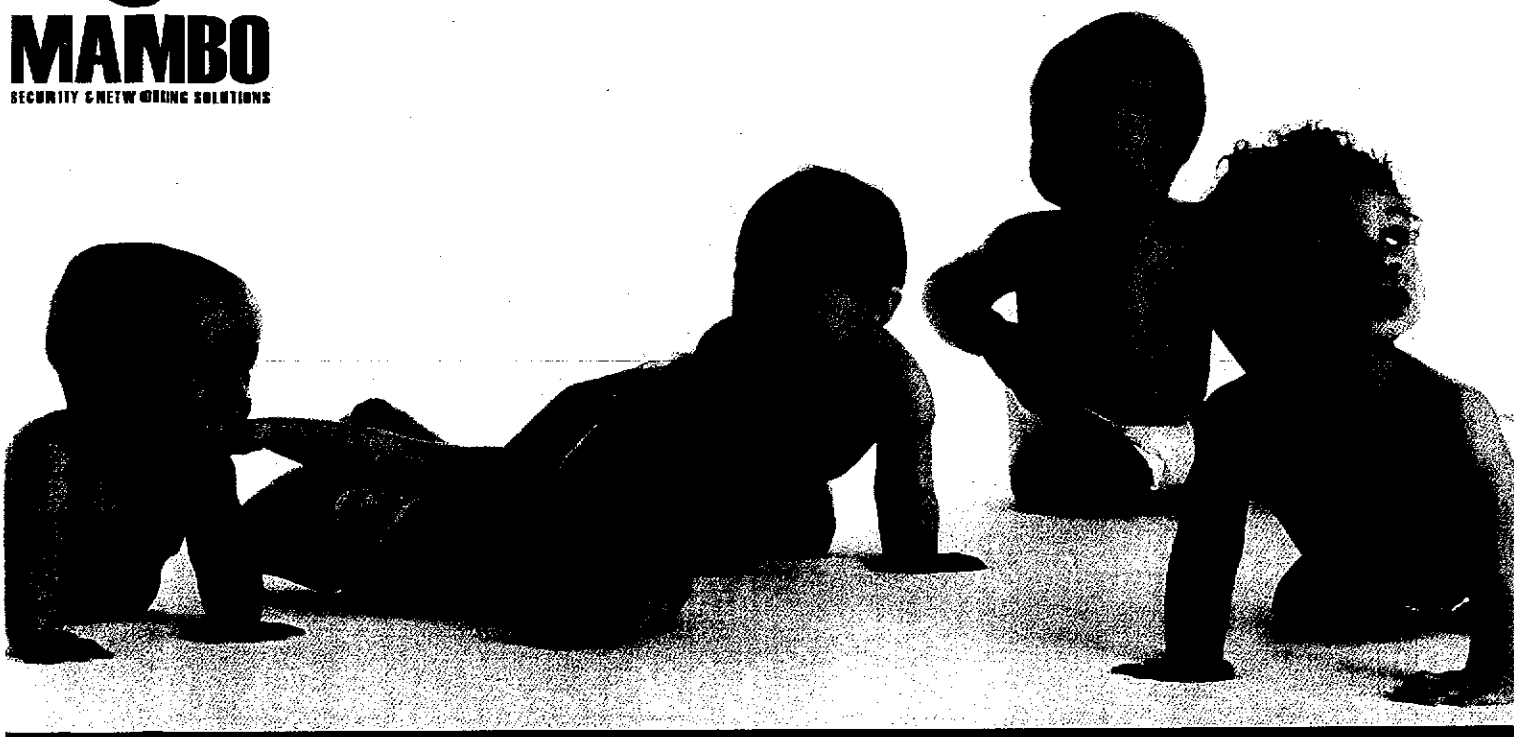
e.Security
European Security

Revista profesional especializada en seguridad de la información y las comunicaciones

Nº 1 - Septiembre 2004

Llega una nueva generación

MAMBO
SECURITY & NETWORKING SOLUTIONS



Mambo le presenta 5 nuevas soluciones
para la seguridad informática y las comunicaciones

En materia de seguridad informática y comunicaciones, soluciones novedosas que aporten un valor añadido pueden contarse con los dedos de una mano.

Mambo Technology, mayorista especializado en seguridad y comunicaciones, ha seleccionado en mercados internacionales los productos de su catálogo basándose en estrictos controles de calidad. El resultado: **una oferta de 5 nuevas soluciones con más rendimiento y hasta un 50% más económicas** que otras similares en el mercado.

(1) **AVENTAIL**, líder mundial de VPN basada en SSL, que supone una alternativa *plug-n-play* a los métodos tradicionales de seguridad de acceso remoto tales como IPSec, VPNs o extranets.

(2) **FORTINET**, IDS y antivirus basado en ASIC, hasta un 50% más económico y con el doble de prestaciones que otros productos similares del mercado.

(3) **TIPPINGPOINT**, únicas soluciones del mercado en ganar el premio NSS Gold en el entorno IPS, que protegen a las organizaciones de vulnerabilidades en aplicaciones e infraestructuras, sin pérdidas de rendimiento.

(4) **BORDERWARE**, appliances para la seguridad vía email, anti-spam, firewall/VPN y DNS, primeros de su categoría en obtener la certificación Common Criteria EAL4+.

(5) **SECURE COMPUTING**, a través de Smartfilter, Sidewinder G2 y Safeword, ofrece las mejores soluciones

Aventail™

FORTINET™

TippingPoint

BorderWare™

SECURE

Una reflexión sobre el análisis de riesgos en TIC

Por Miguel A. Hervella

Todos los que trabajamos en seguridad de la información sabemos que la primera etapa de un Plan de Seguridad en TIC es realizar un análisis de riesgos. Lo hemos aprendido en la universidad (los más jóvenes), en un master de seguridad (los más estudiosos), en un curso de especialización (los más aplicados), a través del mar de datos/información que nos rodea (los más inquietos), o por abducción (los más afortunados). En general, los que participamos en este sector coincidimos en ello: las consultoras, los fabricantes, los mayoristas, los distribuidores, los responsables de seguridad e incluso nuestros jefes.

El argumento es irrebatible. Antes de implantar medidas correctoras se debe averiguar cuáles son las deficiencias. Para ello, hay que analizar las vulnerabilidades, que estarán en función de las amenazas existentes sobre los activos de información. Y aquí es donde entra en juego el análisis de riesgos.

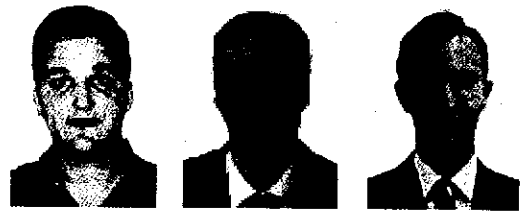
Sigue en la página 40

e.Security
European Security

Reportaje de portada

Aplicación de estándares de seguridad en servicios web

Este artículo ofrece una visión práctica de la utilización de los estándares actuales de seguridad en los servicios web. Los mecanismos aquí tratados permiten asegurar los servicios básicos en el intercambio de mensajes entre servicios web, siempre con el máximo grado de interoperabilidad. Así, en este escrito se analiza el concepto de servicio web, los aspectos básicos que necesitan ser protegidos, se desarrolla un caso de estudio que permite aplicar los estándares de seguridad paso a paso y se mencionan aspectos de seguridad avanzados, como la gestión de los dominios de confianza o la gestión distribuida de las políticas de seguridad en los servicios web.



Por Carlos Gutiérrez Fernández-Medina, Eduardo, Mario Piattini

Tal y como se menciona en el borrador de la especificación de la arquitectura de referencia de los servicios web propuesto por el W3C "*un servicio web es una pieza software identificada por una URL, cuyas interfaces y vínculos se pueden definir, describir y descubrir como artefactos XML. Un servicio web soporta interacciones directas con otros agentes software utilizando mensajes XML intercambiados mediante protocolos de Internet*" [11].

Los servicios web son un paradigma de computación distribuida cuya amplia aceptación lo convierten en una implementación de relevancia en la arquitectura orientada a servicios SOA (*Service Oriented Architecture*) [5]. Sus principales características son: piezas software auto-contenidas, auto-descritas, modulares, estructurables en componentes, dinámicas, pueden ser publicados, localizadas e invocadas a través de la web, son independientes del lenguaje de implementación e interoperables, autónomas de la plataforma e inherentemente basados en estándares [4].

La seguridad es un concepto más de la calidad del servicio (*QoS*) de los servicios web (los otros tres son la transaccionalidad, la confiabilidad, y la gestión/administración) Los servicios de seguridad básicos mencionados por la ISO 7498-2 son la confidencialidad, la integridad, la autenticidad de origen, el no repudio y el control de acceso. En estos aspectos se centrará el caso de estudio.

La arquitectura de referencia planteada por el W3C para los servicios web [11] hace mención a que para garantizar la seguridad son necesarios un amplio espectro de mecanismos que solventen problemas como la autenticación, el control de acceso basado en roles, la aplicación efectiva de políticas de seguridad distribuidas o la seguridad a nivel de los mensajes.

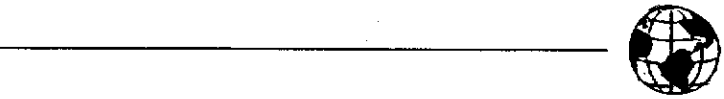
Caso de estudio

En nuestro caso de estudio tenemos a un usuario, Pedro, que posee una cuenta en el sitio web *www.example.com*. Este sitio es una web tipo agencia de viajes que actúa como intermediaria entre el cliente y otros sitios web especializados en reserva de vuelos y coches.

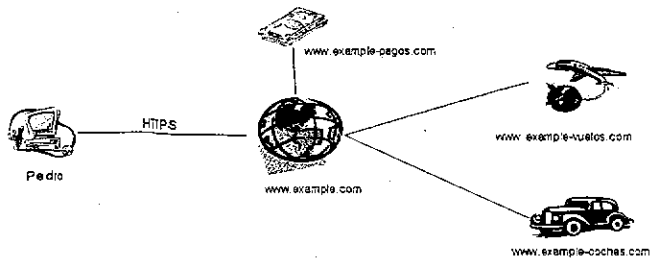
El usuario puede realizar dos operaciones en *www.example.com*: consultar itinerarios y reservar vuelos y coches para un itinerario dado. En el primer caso, el usuario envía una petición con un itinerario y el sistema le devuelve distintos presupuestos en función de la petición realizada. En el segundo caso, el usuario envía, además del itinerario seleccionado, cierta información personal junto con información del medio de pago que utiliza (p.e.: los datos de su tarjeta de crédito) Como medida de seguridad básica y tradicional, el sitio web ofrece un servicio HTTPS para el segundo caso de uso.

Nuestra web de ejemplo dispone de acuerdos comerciales con otros sitios especializados en cada uno de los productos que vende a sus usuarios finales: *www.example-coches.com* para el alquiler de coches y *www.example-vuelos.com* para la reserva de vuelos. Además, utiliza *n* pasarelas de pagos cada una de ellas ubicadas en su servicio *www.example-pagos-n.com*.

El sitio puede disponer de un repositorio UDDI [2] donde almacena la información de los servicios que dispone hasta la fecha. Cada vez que llegue a un acuerdo con una nueva web podría dar de alta este servicio en su UDDI privado para su posterior uso. Todos aquellos servicios web nuevos que se vayan incorporando (que alquilen coches o reserven vuelos) deberán aceptar el contrato semántico [11] y tendrán que ofrecer sus servicios mediante la interfaz web definida (que podría proporcionar *off line* mediante un fichero



(WSDL) Asumimos que *www.example.com* acepta las políticas de seguridad establecidas por los servicios web que utiliza (y de las que puede disponer a través de su directorio UDDI)



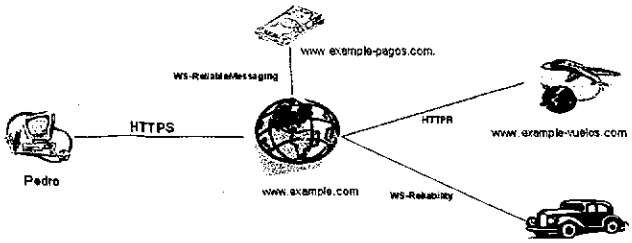
Esquema básico del caso de estudio

Salvo entre Pedro y *www.example.com*, que es puramente HTTPS, las conexiones reflejadas entre los distintos elementos suponen diálogos llevados a cabo a través de Internet mediante mensajes SOAP sobre HTTPS que contienen los datos de negocio en formato XML.

Seguridad a nivel de transporte

La primera medida de seguridad empleada por *www.example.com* para intercambiar mensajes SOAP a través de HTTP es utilizar SSL/TLS. Ambos protocolos nos permiten garantizar autenticación de las partes, la integridad y la confidencialidad de los mensajes en comunicaciones punto a punto. Sin embargo, adoptar sólo SSL/TLS no es suficiente para garantizar la identidad de las partes, la confidencialidad y la integridad de la comunicación extremo a extremo a través de nodos intermediarios, estructura natural de las arquitecturas basadas en servicios web. Como IBM expresa, "*cuando los datos son recibidos y reenviados por un intermediario por encima de la capa de transporte, tanto la integridad como cualquier otro tipo de información que contenga, podría perderse. Esto fuerza a que cualquier procesador de mensajes posterior confíe en las evaluaciones de seguridad hechas por los intermediarios previos y a que tenga confianza plena en cómo éstos últimos hayan manipulado el contenido de los mensajes*" [6].

Además de emplear HTTPS como *binding* SOAP [12], *www.example.com* y los servicios web con los que interactúa podrían acordar el uso de mecanismos conformes con las especificaciones HTTPR [10], *WS-ReliableMessaging* [3], o *WS-Reliability* [14]. Éstos mecanismos garantizan, de una forma u otra, la confiabilidad en la entrega de los mensajes intercambiados (el equivalente a los servicios de confiabilidad proporcionados por TCP al nivel de red IP en el modelo OSI)



Autenticación

En este caso de estudio vamos a analizar la autenticación entre el servicio web cliente de *www.example.com* y cualquiera de los servicios con los que interactúa. La manera más sencilla de autenticar nuestro sitio de ejemplo es mantener una clave secreta (tipo usuario/contraseña) con cada unos de los servicios web y enviársela de manera segura.

Para solucionar este problema, el sitio web propone utilizar los mecanismos descritos en la especificación WS-Security [8] en su documento *SOAP Message Security 1.0* y emplear elementos de seguridad del tipo *UsernameToken* definidos en el perfil *Username Token Profile*. Esta especificación, cuyo proceso de estandarización está a cargo de OASIS (Organización para el Avance de Estándares de la Información Estructurados) permite asegurar los mensajes SOAP indicando una manera de aplicar las primitivas de seguridad XML de firma digital y cifrado según se expresa en los estándares liberados por el W3C *XML Digital Signature* y *XML Encryption*.

De esta forma *www.example.com* extiende el marco de trabajo de mensajería distribuido SOAP mediante un módulo SOAP que incluye una cabecera de seguridad con el nombre de usuario y clave secreta de nuestro sitio de ejemplo. En cada mensaje enviado desde *www.example.com* hacia algunos de los servicios web deberá enviar su clave de forma que demuestre su identidad.

Análogamente, los servicios deberán utilizar algún mecanismo para demostrar la identidad del origen de las respuestas. Una alternativa podría ser aplicar firmas digitales. Si *www.example.com* firma digitalmente cierta parte del mensaje, los servicios web receptores podrán validar la firma y comprobar así su identidad. Suponiendo que existe una tercera parte de confianza (o que las partes admitieran certificados auto-firmados) en la que todos los servicios involucrados confían, sería muy sencillo aplicar los mecanismos descritos por WS-Security y su perfil X.509 *Certificate Token Profile* en el esquema presentado. Hoy en día la aplicación de firmas digitales en el panorama XML está estandarizada por el W3C mediante la recomendación *XML Digital Signature*.

Imaginemos que existe una infraestructura PKI privada montada entre *www.example.com* y los servicios de alquiler de coches y reserva de vuelos y habitaciones (pensemos que ambos portales forman parte de la misma corporación) Sería muy sencillo aprovechar esta infraestructura PKI utilizando los mecanismos descritos en WS-Security. De la misma forma, podríamos extender al mundo de los servicios web una tercera parte de confianza que estuviera basada en criptología de claves simétricas, como por ejemplo, un sistema Kerberos [15]. Como vemos, WS-Security es el estándar central para garantizar la autenticación sencilla en los mensajes.

Aplicación de autenticación basada en certificados x509v3

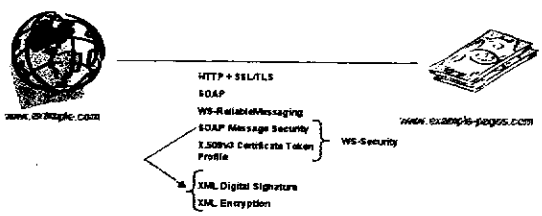
Otro escenario al que se puede adaptar fácilmente el estándar WS-Security es aquel en el que existe un acuerdo de claves simétricas *off line* entre las partes y se desea que los mensajes intercambiados se cifren mediante estas claves.

Integridad, confidencialidad y no repudio

La integridad de los mensajes garantiza que no han sido alterados durante el tránsito entre las partes. Cuando trabajamos con claves públicas/privadas y certificados, la forma clásica de solucionar esta problemática consiste en cifrar con la clave privada el resultado de aplicar una función resumen sobre el contenido del que queremos asegurar la integridad. Una vez más podríamos aplicar las primitivas definidas en *XML Digital Signature* según lo indica el estándar WS-Security.

La confidencialidad de los mensajes se alcanza aplicando técnicas de cifrado sobre aquellas partes que deseamos mantener confidenciales frente a los posibles atacantes. La especificación *XML Encryption* [7], definida por el W3C, describe un modelo de procesamiento para cifrar, descifrar y formatear en XML datos cifrados. La manera de aplicar esta especificación sobre mensajes SOAP viene determinada por la especificación *SOAP Message Security 1.0* que, como ya se ha mencionado, forma parte del estándar WS-Security 1.0.

La aplicación de firmas digitales y su correspondiente soporte legal permiten garantizar la irrenunciabilidad en los mensajes intercambiados entre los servicios web. Por ello, se debe utilizar los mecanismos descritos en WS-Security para la aplicación de las firmas digitales mediante *XML Digital Signature* ofreciendo así una solución estándar a este servicio de seguridad.



Autenticación, integridad y confidencialidad de los mensajes

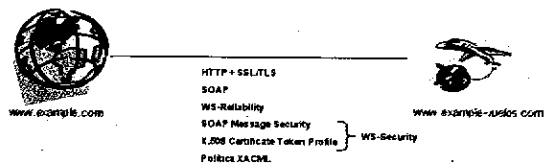
Control de Acceso

El control de acceso, hoy en día, está estandarizado gracias al XACML, a cargo del consorcio OASIS. XACML permite definir políticas de control de acceso a los servicios web.

Existe un marco de trabajo alternativo compuesto de una serie de especificaciones, que todavía no han pasado por ningún cuerpo principal de estandarización, denominado *WS-Policy Framework* [16] cuyos autores son, entre otros, IBM y Microsoft.

Si nos ajustamos tan sólo a la especificación XACML podría interesarnos introducir cierta lógica de control de acceso si nuestro sistema es *www.example-vuelos.com,* de forma que podamos restringir que las peticiones procedentes de *www.example.com* sólo sean procesadas si se reciben entre las 10:00 a.m. y las 20:00 p.m de lunes a sábado y, además, que estas peticiones sólo pueden ser de reserva de plazas de avión en clase turista. Con XACML es posible crear políticas de seguridad complejas basadas en reglas.

Quizá el modelo de control de acceso más popular es el basado en roles (RBAC) [1] OASIS lo ha tenido en cuenta y ofrece a través de su especificación *XACML Profile for RBAC* [9] un método para aplicar este modelo en el contexto de los servicios web.



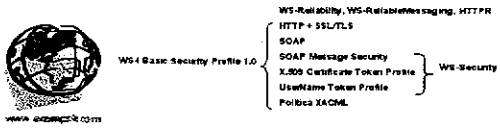
Aplicación de una política de seguridad XACML

Interoperabilidad de los estándares de seguridad

WS-I es otro consorcio abierto al que pertenecen alrededor de 150 compañías cuyo principal papel en los servicios web es promover la interoperabilidad entre plataformas, la adopción de esta forma de computación distribuida y acelerar su desarrollo actuando como guía (definiendo *best-practices),* así como cualquier otro tipo de recurso que mejore su interoperabilidad.

La seguridad no queda fuera del alcance de este propósito, ya que se encuentra actualmente en desarrollo la especificación *WS-I Basic Security Profile 1.0* [13], que define una serie de restricciones sobre el uso de los estándares de seguridad en los servicios web. Esta especificación normaliza el uso de los estándares de seguridad, indicando qué versiones y de qué manera deben ser aplicados.

De esta forma, si se dispone de un proceso de negocio que se quiere hacer accesible desde Internet y se emplean los estándares de seguridad aquí mencionados, asegurando un uso estándar y correcto de los mismos, sería ideal el ajuste a este perfil con el objeto de poder integrarlo con la mayor rapidez posible en el mercado.



Interoperabilidad de los estándares de seguridad actuales

Aspectos de seguridad avanzados

Los estándares mencionados en este artículo permiten contextualizar las primitivas de seguridad básicas estudiadas en el entorno de los servicios web.

Existe una gran abanico de aspectos de la seguridad en los servicios web no mencionados, como por ejemplo, la gestión de dominios de confianza y su federación (p.e.: soluciones de autenticación de acceso único), la gestión distribuida de las políticas de seguridad a gran escala, la privacidad, los contextos de seguridad, la integración con la seguridad a nivel de red, la ampliación de la funcionalidad en los elementos empleados para seguridad del perímetro, la seguridad de la web semántica, etc.

Se está realizando un gran esfuerzo por parte de la industria para elaborar especificaciones que cumplan y estandaricen la definición y aplicación de estos aspectos. Se espera una considerable evolución en los próximos dos años.

Conclusiones

Tanto si disponemos de servicios corporativos abiertos al mundo Internet como si planeamos hacerlo, ya existen a nuestra disposición un conjunto de estándares, cuyo núcleo principal es WS-Security 1.0, que nos permitirá asegurar los servicios básicos, así como proveer la interoperabilidad de nuestras soluciones, facilitando y acelerando, de este modo, el acceso al mercado de nuestros servicios web de empresa.

Carlos Gutiérrez García
Analista de seguridad
Sistemas Técnicos de Loterías del Estado
carlos.gutierrez@stl.es

Eduardo Fernández-Medina
Escuela Superior de Informática
Universidad de Castilla-La Mancha
eduardo.fdezmedina@uclm.es

Mario Piattini Velthuis
Escuela Superior de Informática
Universidad de Castilla-La Mancha
mario.piattini@uclm.es

Referencias

[1] National Institute of Standards and Technology. Role-based Access Control - Draft 4 April 2003 (2003). Ver *http://csrc.nist.gov/rbac/rbac-std-ncits.pdf*

[2] UDDI Version 3.0.1 - UDDI Spec Technical Committee Specification 14 October 2003 (2003). Ver *http://uddi.org/pubs/uddi-v3.0.1-20031014.htm*

[3] Web Services Reliable Messaging Protocol (WS-ReliableMessaging) (2004). Ver *http://msdn.microsoft.com/webservices/understanding/specs/default.aspx?pull=/library/en-us/dnglobspec/html/ws-reliablemessaging.asp*

[4] Endrei, M., J. Ang, A. Arsanjani, S. Chua, P. Comte, P. Krogdahl, M. Luo and T. Newling *Patterns: Services Oriented Architectures and Web Services.* IBM Redbook, ed. IBM. (2004)

[5] Erl, T. *Service Oriented Architecture. A Field Guide to Integrating XML and Web Services.* 1st ed. Prentice Hall PTR. 536. (2004)

[6] IBM and Microsoft. Security in a Web Services World: A Proposed Architecture and Roadmap - technical whitepaper 7 April 2002 (2002). *Ver http://msdn.microsoft.com/ws-security/*

[7] W3C XML Encryption Syntax and Processing - W3C Recommendation 10 December 2002 (2002). Ver *http://www.w3.org/TR/xmlenc-core/*

[8] Web Services Security (WS-Security) - Specification 6 April 2004 (2004). Ver *http://www-106.ibm.com/developerworks/webservices/library/ws-secure*

[9] XACML Profile for Role Based Access Control (RBAC) (2004). Ver *http://docs.oasis-open.org/xacml/cd-xacml-rbac-profile-01.pdf*

[10] A Primer for HTTPR. An overview of the reliable HTTP protocol. (2002). Ver *http://www-106.ibm.com/developerworks/webservices/library/ws-phtt/*

[11] Web Services Architecture (2004). Ver *http://www.w3.org/TR/ws-arch/*

[12] W3C SOAP Version 1.2 Part 0: Primer (2003). Ver *http://www.w3.org/TR/2003/REC-soap12-part0-20030624/*

[13] Basic Profile Version 1.0 (2004). Ver *http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html*

[14] Web Services Reliability 1.0 (2003). Ver: *http://otn.oracle.com/tech/webservices/htdocs/spec/WS-ReliabilityV1.0.pdf*

[15] Web Services Security Kerberos Token Profile (2003). Ver: *http://www.oasis-open.org/committees/download.php/1049/WSS-Kerberos-03.pdf*

[16] Web Services Policy Framwork (2003).Ver: *http://www-106.ibm.com/developerworks/library/ws-polfram/*