Seguridad en servicios web

Carlos Gutiérrez[1], Eduardo Fernández-Medina[2] y Mario Piattini[2]
(1) Sistemas Técnicos de Loterías del Estado.
Calle Manuel Tovar 9, 28034, Madrid. (España). Tel: 34 91 348 92 61
carlos.gutierrez@stl.es
(2) Grupo de Investigación Alarcos. Universidad de Castilla-La Mancha.
Paseo de la Universidad 4, 13071, Ciudad Real. (España). Tel: 34 926 29 53 00
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen. Durante los últimos años se está llevando a cabo un grandísimo esfuerzo en el proceso de estandarización de las tecnologías basadas en servicios web. A raíz de este trabajo, existen multitud de estándares que establecen las líneas básicas a seguir para todos aquellos participantes de la industria que deseen dotar de soluciones estándares a sus desarrollos en dicha tecnología. El problema lo encontramos cuando centramos nuestra atención en los estándares relacionados con la seguridad. Si bien es verdad que ha existido y existe una gran actividad en este campo, todavía existe un largo camino que recorrer en el proceso de estandarizar todos los aspectos de seguridad que esta tecnología impone. Este artículo realiza un estudio del panorama de la seguridad en los servicios web desde la perspectiva de los estándares señalando las iniciativas principales existentes hoy en día. Para cada especificación se indica qué aspectos de seguridad de su campo quedan pendientes por resolver.

1. INTRODUCCIÓN

En los últimos tiempos las tecnologías basadas en servicios web han alcanzado tal grado de madurez que han evolucionado de ser una promesa tecnológica para convertirse en una realidad sobre la que multitud de departamentos de sistemas de la información están fundamentando su operaciones con el objeto de alcanzar "una alineación directa con las operaciones del negocio que soportan". De hecho, en función a lo expresado en recientes estudios elaborados por el IDC, aproximadamente se pusieron en marcha alrededor de 3300 proyectos basados en la tecnología en cuestión por todo Norte América en el año 2002 y se esperaba que el año 2003 se superara la cifra de 3 billones de dólares. Podemos asumir estas cantidades si revisamos las valiosas ventajas proporcionadas por esta tecnología:

- Tecnología middleware basada en estándares.
- Sencilla reutilización e interoperación de los servicios de empresa.
- Aprovechamiento de sistemas de legado de manera sencilla.
- Integración fácil entre sistemas heterogéneos.

Debido a estos beneficios tan inmediatos, las mayoría de los departamentos I+D están implementando esta tecnología con el objetivo prioritario de su puesta en producción dejando a un lado, al menos hasta etapas posteriores, los problemas relacionados con la seguridad. En general, la industria se muestra todavía reticente a incorporar esta tecnología debido a la poca comprensión de la que disponen sobre los aspectos de seguridad implicados y en la falsa creencia de que tendrán que realizar grandes reinversiones en sus infraestructuras de seguridad.

Los servicios web como sistemas descentralizados, distribuidos que proporcionan una interfaz bien definida a un conjunto de clientes, debe preocuparse de los problemas de seguridad típicos heredados del esquema de comunicación entre dos o más partes a través de canales comprometidos.

1.2 Principales Aspectos de Seguridad en servicios web

A continuación describimos los aspectos de seguridad principales que las tecnologías basadas en servicios web deberán resolver :

Autenticación: cualquier servicio web que participe en una interacción podría requerir una prueba de las credenciales de identidad al otro extremo. Cuando cierto servicio A realiza una petición a otro servicio B, éste último podría requerir a A sus credenciales de identidad junto con una demostración de su pertenencia (p.e.: un par usuario/contraseña o un certificado X.509v3).

Autorización: los servicios web deberían incluir mecanismos que les permitan controlar el acceso a los servicios que ofrecen. Deberían ser capaces de determinar quién puede hacer qué y cómo sobre sus recursos.

Confidencialidad: mantener la información confidencial entre dos nodos de servicios web es otra de las propiedades principales que debería estar garantizada si queremos considerar el canal cómo seguro. La confidencialidad de los datos se obtiene aplicando técnicas de cifrado.

Integridad: esta propiedad garantiza que la información recibida por un servicio web permanece exactamente igual que aquella que fue enviada desde un cliente. Una sencilla suma de verificación podría ofrecer este servicio básico de seguridad.

No repudio: en el panorama de los servicios web, se vuelve muy necesario ser capaz de probar que un cliente utilizó cierto servicio (no repudio del solicitante) y que ese servicio procesó la petición del cliente (no repudio del proveedor del servicio). Este aspecto de seguridad es resuelto aplicando técnicas de firma digital sobre la información intercambiada.

Disponibilidad: la necesidad de tomar medidas preventivas contra ataques a la disponibilidad (p.e.: ataques de denegación de servicios o planificación de sistemas de redundancia) se revela como un punto crucial en este paradigma. Sobre todo, en aquellos escenarios en los que los servicios proporcionados son en tiempo real y críticos (p.e.: transacciones bancarias u obtención de Listas de Revocación de Certificados en infraestructuras PKI).

Seguridad extremo a extremo: las topologías de red requieren que se mantenga la seguridad de extremo a extremo a través de todos los intermediarios encontrados en el camino del mensaje. "Cuando los datos son recibidos y reenviados por un intermediario por encima de la capa de transporte tanto la integridad de los datos 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".

Hasta aquí, hemos repasado brevemente los problemas clásicos de seguridad íntimamente relacionados con la computación distribuida. Además de tener en cuenta todos estos aspectos, los servicios web deberán proporcionar soluciones a aquellos problemas de la seguridad surgidos por las nuevas amenazas que supone la puesta en producción de esta tecnología:

- Número de especificaciones de estándares muy alto y diverso que no facilitan una visión clara de los problemas de seguridad y sus soluciones.
- El estado de borrador en el que se encuentran la mayor parte de las especificaciones de los estándares.
- La publicación en Internet de una interfaz bien documentada y completa que permite el acceso a los datos y operaciones de la empresa.
- La necesidad de crear multitud de vocabularios XML estándar que permita estructurar la información relacionada con la seguridad.
- El hecho de que las comunicaciones contengan información del negocio y deba ser establecida la seguridad de extremo a extremo mediante un sólo contexto de seguridad.
- Necesidad de hacer que los requisitos y los elementos de seguridad sean interoperables.
- Hacer posible una auditoría distribuida con elementos auditables existentes en distintos dominios o incluso organizaciones o corporaciones cada una con sus políticas de seguridad propias.
- Definir procesos de contingencia automáticos e inteligentes debido a que la mayor parte de la interacción es entre máquinas y no necesita intervención manual alguna por parte de los humanos.
- La creación de complejas redes de dependencia entre servicios que conduce a que la ejecución de los procesos de negocio dependa de un número de servicios web desconocidos.
- Gestión de la disponibilidad en línea para los procesos de negocio críticos.
- Gestión de la confianza distribuida permitiendo que servicios web que no se "conocen" a priori puedan descubrir sus servicios de forma dinámica sin que esto suponga riesgos de seguridad.
- Garantizar la privacidad y el anonimato de las identidades de los usuarios.
- Gestión de las políticas de seguridad en entornos de servicios web de gran escala.

El resto de éste artículo está dividido en 4 partes. En la primera, se realiza un repaso de las especificaciones fundamentales sobre las que se sustentan los servicios web. En la segunda parte, se explican las especificaciones de seguridad fundamentales comentando aquellos aspectos de seguridad que aún necesitan ser resueltos. En la tercera y cuarta parte, se introducen las principales iniciativas así cómo se estudian las especificaciones relativas a la seguridad que cada una de ellas está desarrollando.

2. ESTÁNDARES FUNDAMENTALES DE LOS SERVICIOS WEB

En esta sección, echaremos un vistazo a los cuatro estándares fundamentales implicados en la creación de servicios web operativos (lo que no implica que sean seguros). La figura 1 muestra las especificaciones fundamentales y las más importantes relativas a la seguridad que actualmente se encuentran en desarrollo. Se encuentran agrupadas de la siguiente manera:

- Servicios web base: contiene las especificaciones básicas de los servicios web. Se corresponden con los estándares sobre los que el resto están construidos.
- Seguridad básica: estándares que proporcionan las primitivas de más bajo nivel en XML como el cifrado o la firma digital.
- WS-Security: familia de especificaciones desarrolladas entre otros por IBM y Microsoft y que se encuentran bajo el proceso de estandarización del consorcio OASIS. Se agrupan de manera independiente ya que sus creadores tienen entidad propia y no son comités propios de OASIS.
- OASIS: especificaciones de seguridad desarrolladas por el cuerpo de comités del consorcio OASIS.
- El Proyecto Liberty Alliance: representa el grupo de especificaciones desarrolladas por el proyecto con igual nombre y cuyo objetivo fundamental es la federación en los servicios web.

"Los servicios básicos, sus descripciones, y las operaciones básicas (publicación, descubrimiento, selección y vinculación) que producen o utilizan tales descripciones constituyen la base fundacional de las arquitecturas SOA". Los servicios web están construidos sobre una arquitectura SOA (Service-oriented architecture). De hecho, la arquitectura de los servicios web es una instanciación de SOA. Por esa razón, las características fundamentales descritas por SOA son las que han dirigido el trabajo de estandarización inicial de la industria. Las especificaciones fundacionales de la arquitectura de los servicios web son: XML , SOAP , WSDL , y UDDI.

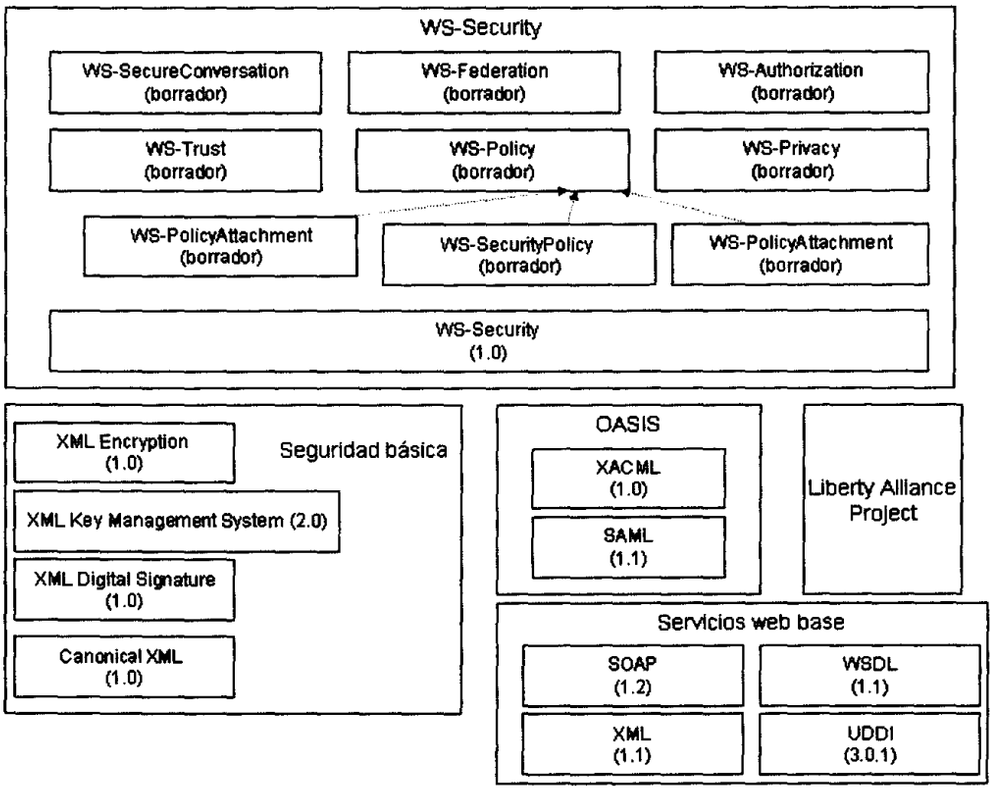

Fig. 1. Estándares de seguridad actuales agrupados por la organización responsable de su proceso de estandarización.

XML, recomendación del W3C desde 1998, ofrece una vía estándar de estructurar la información de manera que sea consumible por humanos y/o máquinas y permitiendo su intercambio entre nodos heterogéneos. Es por tanto XML el lenguaje utilizado para transportar la carga útil o de negocio de los mensajes que deben ser intercambiados entre nodos de servicios web.

El estándar SOAP (Simple Object Access Protocol), estándar del W3C en su versión 1.2, especifica "un protocolo ligero cuyo propósito es el intercambio de información estructurada en un entorno descentralizado y distribuido. Utiliza las tecnologías XML para definir un marco de trabajo extensible proporcionando un constructor de mensajes que pueden ser intercambiados sobre diversos protocolo de transporte subyacentes".

Por su parte, WSDL (Web Service Description Language) resuelve uno de los requisitos básicos de toda arquitectura SOA: proporcionar una descripción de los servicios procesable por las computadoras. De esta forma, un proveedor de servicios web puede definir su interfaz en un lenguaje estándar para que otras partes, computadoras o humanos, puedan conocer los servicios que ofrece y los mensajes necesarios para invocarlos.

UDDI (Universal Description Discovery & Integration) cubre el requisito de publicación y descubrimiento de los servicios de manera dinámica. Un proveedor de servicios web puede publicar los servicios que ofrece en un repositorio de forma que un servicio web solicitante pueda buscar en él y encontrar, los servicios que le interese. En definitiva, UDDI ofrece un marco en el que se define la manera de estructurar la información de un negocio, de los servicios que éste ofrece y de proporcionar un punto de acceso y una definición de la interfaz programática que permite la interacción con dichos servicios.

En resumen, XML, WSDL, SOAP, UDDI constituyen los bloques básicos de construcción sobre los que diseñar sistemas basados en servicios web, además de ser ampliamente utilizados y soportados por los principales vendedores de herramientas y desarrolladores de la industria. La mala noticia es que estas cuatro especificaciones sí permiten crear servicios web operativos pero no dicen nada sobre cómo hacerlos seguros. Es más, ellas mismas contienen problemas de seguridad que deben ser resueltos:

- XML y SOAP: no dicen nada de como conseguir integridad, confidencialidad y autenticidad de la información que representan y transportan respectivamente.
- UDDI y WSDL: deben contestar a las preguntas ¿está el registro UDDI ubicado en un lugar de confianza?,¿los datos publicados no han sido manipulados y modificados maliciosamente?, ¿los datos publicados de una empresa fueron realmente publicados por dicha empresa?, ¿es la última información posible la que encontramos en el repositorio?, ¿los servicios publicados por cierto negocio son de confianza y están disponibles en el momento?.En se realiza un estudio sobre los problemas de segu-

ridad que una arquitectura UDDI, en la que las descripciones de los servicios se ofrecen en formato WSDL, contiene y cuáles ya resuelve el estándar y cuáles no. Entre los puntos de seguridad no resueltos describe cómo todavía no se puede asegurar la confianza en las transacciones de negocio realizadas por los usuarios de un servicio web publicado en un registro UDDI.

Estas especificaciones, que han sido ampliamente aceptadas por la industria, constituyen los bloques de construcción básicos sobre los cuáles las tecnologías de los servicios web deben ser diseñadas e implementadas.

Pese a todos estos inconvenientes estos estándares han madurado y la industria ha adoptado e implementado la mayor parte de ellos, quedándose ante el desafío de resolver el problema de la seguridad que adquiere gran relevancia dada la naturaleza de la arquitectura SOA que, como ya se ha dicho, es la arquitectura de referencia de los servicios web.

Actualmente, las principales iniciativas, cuyo propósito es "estandarizar" el mundo de los servicios web son las llevadas a cabo por el consorcio W3C (http://www.w3c.org) y la organización OASIS (Organization for the Advancement of Structured Information Standards - http://www.oasis-open.org).

Ambos consorcios están tratando de estandarizar su visión (incluyendo la seguridad) sobre lo que los servicios web deben ser y deben aportar. Este paralelismo está provocando la existencia de especificaciones desarrolladas independientemente por ambos grupos que resuelven los mismos problemas. Por lo tanto, en un futuro se deberán hacer esfuerzos por todas las partes con el fin de integrar sus visiones y estándares de los servicios web para lograr un marco de trabajo común y único.

3. ESTÁNDARES DE SEGURIDAD FUNDACIONALES

El consorcio W3C es el encargado del proceso de estandarización de las consideradas especificaciones núcleo de la seguridad en el panorama de las tecnologías XML que son:

- W3C XML Encryption.
- W3C XML Digital Signature.
- W3C XML Key Management System.

3.1. XML Encryption

W3C XML Encryption es una propuesta de recomendación desde el 2002 que ofrece un esquema XML para representar datos XML cifrados:

- Documentos XML completos.
- Elementos únicos (y todos sus descendientes) dentro de un documento XML.
- El contenido de un elemento (algunos o todos los nodos hijos incluyendo todos sus descendientes) localizado dentro de un documento XML.
- Contenidos binarios arbitrarios ubicados fuera de un documento XML.

XML Encryption es la solución al problema de la confidencialidad de los mensajes SOAP intercambiados entre los servicios web. XML Encryption, además de describir la estructura y la sintaxis de los elementos XML necesarios para presentar información cifrada, especifica los pasos que se deben seguir a la hora cifrar y descifrar documentos XML (o partes de ellos).

La filosofía a la hora de aplicar el cifrado sobre la totalidad o parte de un documento XML, es que las partes cifradas son substituidas por elementos definidos en la especificación XML Encryption que transportan el cifrado. De la misma manera, la información cifrada será convertida en la información original cuando se realice el descifrado.

Los servicios web utilizan XML para transportar la meta-información necesaria (en forma de cabeceras SOAP), y para transportar la carga útil o información de negocio. Por tanto, pueden aprovechar esta primitiva de seguridad para cifrar/descifrar aquellas partes de los mensajes que crean oportunas. XML Encryption no define específicamente como cifrar los mensajes intercambiados entre los servicios web, dejando esta tarea a especificaciones de más alto nivel que definen las reglas de uso de esta primitiva en el contexto del intercambio de información XML mediante mensajes SOAP. Esta especificación también describe el método a utilizar para cifrar contenido cifrado (super-encryption) así como el mecanismo para cifrar claves utilizadas en el proceso de cifrado.

Si nos remontamos al principio de ésta sección donde se listan los tipos de datos que XML Encryption puede cifrar, podemos echar en falta la posibilidad de cifrar nodos de un árbol sin tener por qué cifrar sub-árboles completos. Una solución al problema es extraer los nodos a cifrar del documento original, cifrar cada uno de ellos, y recopilarlos en un "pool" de nodos ya cifrados. Al recipiente le llegaría el documento con los nodos extraídos así como el "pool" de nodos cifrados y sería capaz de descifrar y reubicar en el árbol original sólo aquellos nodos destinados para él.

Otro problema de seguridad es la declaración explícita que se realiza de las partes que han sido cifradas. Tal y como indica la especificación, la información que es cifrada es substituida por elementos XML que contienen la información cifrada. Esto puede ser un problema cuando la documentación XML se enfrenta ante ataques de análisis de información.

La recursividad es otro problema que la especificación señala pero que no resuelve: la clave cifrada A puede requerir la clave cifrada B pero esta a su vez necesita la clave cifrada A.

Otro punto, más organizativo que de seguridad, que se debe resolver es la dependencia establecida con la especificación XML Digital Signature para temas tan sencillos como la información del material de clave utilizado para el cifrado. Actualmente la recomendación indica el uso del elemento del espacio de nombres *ds:* (comúnmente asociado con el espacio de nombres que contiene los elementos definidos en XML Digital Signature XML) en vez agrupar estos elementos de utilidad de seguridad en un espacio de nombres independiente como por ejemplo se define en la familia WS-Security.

3.2 XML Digital Signature

XML Digital Signature es una recomendación del W3C desde el 2002, fruto del esfuerzo conjunto entre el W3C y

el IETF. Esta especificación define cómo aplicar firmas digitales sobre contenido XML y cómo representar, definiendo un esquema XML, dicha información. Las firmas digitales son un mecanismo que garantiza la integridad de la información y se muestran como una evidencia no repudiable del generador de la misma. De esta forma, una entidad no podrá negar la autoría de una hipotética transferencia bancaria firmada digitalmente que llevó a cabo a través de un servicio web.

En XML Digital Signature una firma digital puede ser aplicada a cualquier contenido digital incluyendo XML. Una firma digital puede ser aplicada al contenido de uno o más recursos. Además, la especificación define los procesos de creación de las firmas y su verificación.

Al igual que ocurre con la especificación XML Encryption, esta especificación es independiente de la tecnología que la quiera utilizar de forma que se necesitan mecanismos adicionales que normalicen su uso en el intercambio de mensajes entre servcios web.

Existen problemas de seguridad que deben ser tenidos en cuenta por las aplicaciones que utilicen esta especificación en combinación con el cifrado. La especificación recomienda a las aplicaciones o protocolos de nivel superior que utilicen ambas primitivas las siguientes recomendaciones:

- Cuando los datos son cifrados cualquier resumen o firma sobre los datos deberían ser cifrados también de forma que se prevenga de ataques de adivinación de texto plano.
- Utilizar la transformación XML Decryption Transform durante el procesamiento de verificación de una firma.

3.3 XML Key Management System

XML Key Management System , es una especificación estandarizada por el W3C que propone un formato de información así como los protocolos necesarios para convertir una infraestructura PKI en un servicio web de forma que se pueda:

- Registrar pares de clave privada/pública.
- Localizar claves públicas.
- Validar la clave.
- Revocación de clave.
- Recuperación de clave.

De esta forma toda la infraestructura PKI se extiende al mundo XML y permite delegar las decisiones de confianza a sistemas especializados simplificando el desarrollo de las aplicaciones. Esta especificación se compone de dos partes:

- X-KISS (XML Key Information Service Specification): define los protocolos necesarios para soportar el procesamiento de la información de clave asociada con una firma digital o datos XML cifrados.
- X-KRSS (XML Key Registration Service Specification): define los protocolos necesarios para soportar el registro de un par de claves por un poseedor de pares de clave.

XKMS se presenta como la solución para la creación de un servicio distribuido que ofrezca todos los servicios de una PKI. Por contra, hereda todos los problemas ya existentes en la misma:

- En cuanto a los certificados X.509:
- ¿Cómo averiguar la clave pública de una autoridad de certificación con total seguridad?
- La identidad asegurada por la Autoridad de Certificación ¿es útil?
- El problemas de los "Objects ID" para procesado automático y su explosivo y continuo crecimiento.
- PKI a nivel global (Internet):
- Puesto que no existe una autoridad de certificación única y reconocida mundialmente no está claro cómo instrumentar el mundo de forma que dos sistemas (Ej: servicios web) desconocidos puedan establecer una relación de confianza a través de una tercera parte en tiempo de ejecución sin la necesidad de procesos off-line.

4. SEGURIDAD EN LOS SERVICIOS WEB: ESTÁNDARES Y ASPECTOS DE LA SEGURIDAD RESUELTOS

Tras haber repasado los estándares fundacionales de los servicios web y su seguridad pasaremos a desarrollar las tecnologías y especificaciones emergentes que utilizan estos estándares como base.

En primer lugar explicaremos la necesidad de mejorar la seguridad del perímetro ampliando la funcionalidad de los firewalls clásicos, para que incluyan lógica que permita filtrar las invocaciones y las respuestas de los servicios web.

En segundo lugar daremos un breve paseo por las especificaciones WS-* cuyos principales valedores son IBM y Microsoft.

En tercer y cuarto lugar hablaremos sobre los estándares SAML y XACML, liberados ya por la organización OASIS en sus primeras versiones, y cuyo objeto es, respectivamente, la representación de la información y de las políticas de seguridad.

En quinto lugar comentaremos brevemente el proyecto Liberty Alliance liderado por Sun Microsystems y en sexto, y último lugar, mostraremos a modo de resumen una matriz en la que se enmarcan todas las especificaciones cubiertas en este artículo señalando cuáles han sido liberadas y cuáles continúan en estado de borrador.

4.1 Necesidad de Ampliación de la Seguridad de Perímetro

Uno de los principales problemas de seguridad con la adopción de los servicios web se origina a partir de la publicación en Internet de interfaces de negocio a través del puerto HTTP 80 o HTTPS 443. La incorporación de los servicios web para habilitar el acceso a sistemas del negocio posiblemente críticos es un nuevo riesgo que debe ser analizado cuidadosamente. Esta característica intrínseca ha obligado a los fabricantes de firewalls a ampliar las capacidades de sus productos para permitir el análisis de los paquetes a nivel de protocolo de aplicación de forma que se puedan tomar decisiones de seguridad de acceso perimetral en función a los resultados de analizar y validar los contenidos XML de los mensajes intercambiados.

Con el tiempo estos firewalls XML han añadido funciones de seguridad como cifrado mediante W3C XML Encryption o creación/verificación de firmas digitales mediante W3C XML Digital Signature proporcionando así, en el dominio de las tecnologías XML, el equivalente a lo proporcionado por el Secure Socket Layer para la seguridad en la capa de transporte.

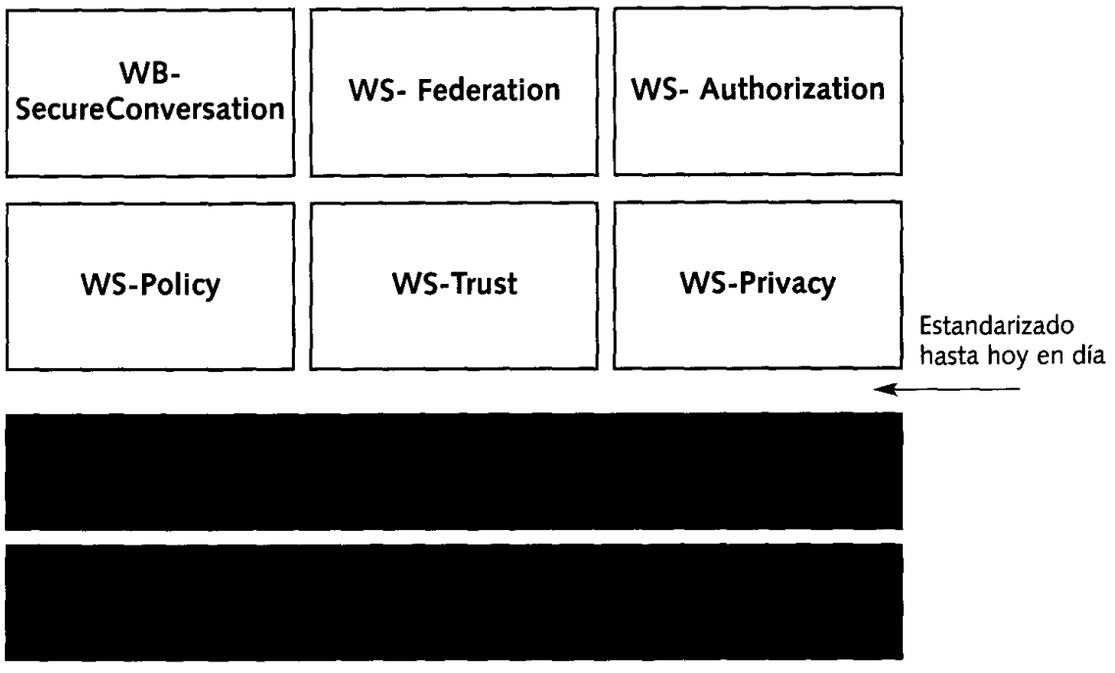

Fig 2. Familia de especificaciones de seguridad WS-*

4.2 Familia de especificaciones WS-Security

IBM Corporation y Microsoft, junto con otras grandes compañías tecnológicas, han definido un modelo de seguridad para servicios web de forma que se garantice la seguridad de extremo a extremo de la comunicación.

Estas compañías están elaborando conjuntamente una serie de especificaciones que componen un arquitectura, bautizada por Microsoft como *Global XML Web Services Architecture*, de forma que dirija el desarrollo de la industria de los servicios web consiguiendo que los distintos productos elaborados sean interoperables en un contexto seguro. El núcleo de estas especificaciones son: WS-Addressing, WS-Coordination, WS-Inspection, WS-Policy, WS-Referral, WS-ReliableMessaging, WS-Routing, WS-AtomicTransaction, WS-Security.

Prestaremos atención a la última: WS-Security. En realidad, WS-Security está compuesta por conjunto de especificaciones. Dichas especificaciones asientan las bases sobre las que están definiéndose, algunas en versiones ya publicadas, documentos adicionales que cubran todos los aspectos de seguridad en el panorama de los servicios web. WS-Security se sitúa como la especificación de seguridad base en la pila de especificaciones de seguridad. Su propósito es proporcionar Calidad de la Protección (Quality of Protection) a la interacción agregando las siguientes propiedades sobre la comunicación y los mensajes: integridad de mensajes, confidencialidad y autenticación simple de un mensaje. WS-Security permite que la incorporación de los modelos de seguridad existentes, como PKI o Kerberos, sea muy sencilla.

Las principales especificaciones de seguridad que se están elaborando a partir de WS-Security son las mostradas en el figura 2.

Una de las especificaciones que merece la pena destacar por su similitud con la anteriormente mencionada W3C XKMS es WS-Trust. WS-Trust, aún en estado de borrador, define un esquema XML así como protocolos que permiten la obtención, validación e intercambio de elementos de seguridad. Pero este problema no es nuevo ya que la especificación XKMS ya resuelve esta problemática cuando la infraestructura de seguridad subyacente es PKI. Entonces, si tenemos una PKI que queremos extender como servicios web, ¿cuál de los dos estándares deberemos seguir? La obtención permitiría a un cliente obtener la información de seguridad necesaria de un servicio WS-Trust para poder interactuar con un servicio web. El servicio web objetivo tendría de alguna manera preestablecida una relación de confianza con el servicio WS-Trust. La validación serviría para que el servicio WS-Trust fuera el responsable de la autenticación de los sistemas clientes de cierto servicio web.

Otra especificación que merece la pena comentar es WS-Policy y las especificaciones relacionadas: WS-SecurityPolicy, WS-PolicyAssertions, WS-PolicyAttachment. Estas especificaciones definen:

- Sintaxis XML para la definición de políticas (WS-Policy) en servicios web.
- Cómo asociar las políticas a elementos XML, entradas UDDI o descripciones WSDL.
- Un conjunto de afirmaciones de políticas de carácter general (WS-Policy-Assertions).
- Un conjunto de afirmaciones de política con carácter de seguridad (WS-SecurityPolicy).

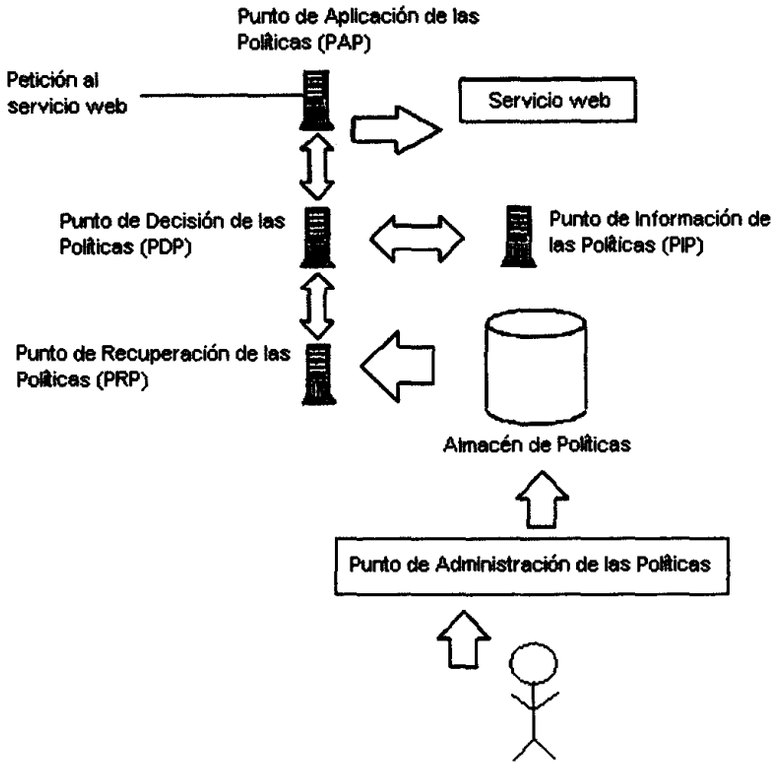

Fig. 3. Arquitectura de Servicios de Políticas en XACML

Cómo veremos más adelante, existe un estándar estable y ampliamente aceptado del consorcio OASIS denominado XACML que ya resuelve todas estas cuestiones.

En la familia WS-Security todavía se encuentran en estado de borrador especificaciones que resuelven:

- Privacidad: WS-Privacy.
- Autorización: WS-Authorization.
- Contextos de seguridad: WS-SecureConversation.
- Federación (Single Sign-on): WS-Federation.

4.3. SAML

SAML (Secure Assertion Markup Language) es una especificación desarrollada por OASIS y se encuentra en estado de "OASIS Open Standard" desde el 2002.

Esta especificación contiene dos partes:

- Esquema XML para la definición de afirmaciones de confianza (autenticación, autorización o atributo). Este esquema puede ser utilizado como una solución parcial de una solución general para transferir en un formato estándar el contexto de seguridad entre aplicaciones.
- Protocolos cliente/servidor para realizar peticiones de autenticación, autorización o de atributos mediante XML. Define el término "binding"como la forma estándar de realizar el intercambio de mensajes sobre cierto protocolo de transporte subyacente. Define dos "binding": uno para el protocolo HTTP y otro para SOAP. Además también define el término "profile" que describe cómo estos protocolos transmiten las afirmaciones SAML de una aplicación a otra.

Esta especificación no resuelve todos los problemas asociados con la transferencia interoperable de los datos de seguridad pero sí representa un progreso significativo. Por ejemplo, SAML no soluciona la transferencia interoperable de la evidencia de autenticación misma, cosa que, por ejemplo sí hace WS-Security mediante los security token UsernameToken o BinarySecurityToken. SAML se limita a definir documentos XML que contengan afirmaciones, probadas por una tercera parte de confianza, de que una autenticación o una autorización se ha llevada a cabo con éxito o de que cierto sujeto tiene ciertos atributos de seguridad asociados, también respaldados por una tercera parte de confianza. Además SAML no definía la manera de introducir afirmaciones SAML en bloques de cabecera SOAP wsse:Security, de forma que fue la especificación WS-Security la que en Agosto del 2002 definió el mecanismo en "The WS-Security Profile for XML-based Tokens".

4.4. XACML

XACML (eXtensible Access Control Markup Language) es un estándar creado por OASIS y su principal propósito es definir un vocabulario XML para especificar las reglas a partir de las cuáles se pueden realizar las decisiones de control de acceso.

XACML define reglas para permitir el acceso a los recursos en función a las características del solicitante, el protocolo utilizado para realizar la solicitud, y el método de autenticación utilizado. XACML tiene una similitud muy grande, en cuanto al problema de seguridad que resuelve, con el modelo y el lenguaje de políticas definido por la familia de especificaciones WS-Policy vistas anteriormente. Esta "coincidencia" supone otro ejemplo más del esfuerzo de unificación que tendrá que ser realizado en un futuro para definir un único modelo y lenguaje de políticas en el mundo de los servicios web.

XACML define una arquitectura de servicios que debe implementar toda infraestructura de políticas de acceso completas:

En la figura 3 se muestran los servicios, y los diálogos entablados entre los mismos, que intervienen en la toma de decisión de autorizar el acceso de una petición SOAP a cierto servicio web.

La petición SOAP que viaja hacia el servicio web es interceptada por el PAP (Punto de Aplicación de las Políticas) cuya tarea es asegurar la aplicación de la lógica de políticas sobre la petición. El PAP pregunta al PDP (Punto de Decisión de las Políticas) mediante un mensaje SAML de autorización. El PDP debe decidir si se autoriza o no la petición. Para ello, y en el caso en que no disponga de las políticas necesarias, realiza una petición XACML de políticas al PRP (Punto de Recuperación de las Políticas) que le devuelve las políticas en formato XACML necesarias para evaluar la petición. Tras recibir las políticas el PDP podría necesitar obtener información, en forma de atributos, sobre el sujeto o su entorno, con el fin de poder evaluar la política. El PDP solicitará esta información al PIP (Punto de Información de las Políticas) que le devolverá las afirmaciones de atributos SAML necesarias. Finalmente el PDP evaluará la política y si la petición es autorizada devolverá una afirmación de autorización SAML al PEP, alcanzado así, la petición, el servicio web destino.

4.5. The Liberty Alliance Project

El proyecto Liberty Alliance Project está liderado por Sun Microsystems y otras 120 compañías y su objetivo es definir un marco estándar para la "federación de entidades" entre aplicaciones. Es por tanto su objetivo definir un sistema distribuido de autenticación que permita la conexión de las empresas y facilite a sus clientes experiencias más intuitivas. Pero este propósito no es nuevo, de hecho es similar al que tiene establecido la especificación WS-Federation de la familia WS-* siendo pues, éste, un ejemplo más de la necesidad de coordinar esfuerzos con el fin de evitar conflictos entre las soluciones a problemas similares.

5. RESUMEN

En este artículo hemos estudiado los estándares más significativos concernientes a la seguridad en los servicios web. Para ello, hemos comenzado mencionando los principales motivos por lo que este paradigma de computación distribuida está siendo tan popular en los departamentos tecnológicos. A continuación se ha proporcionado una breve introducción a la naturaleza y al concepto de servicio web en sí, para posteriormente estudiar las especificaciones fundacionales sobre la que se apoya.

El resto del artículo ha navegado por las principales especificaciones de seguridad elaboradas (o todavía en proceso de elaboración) por las más importantes organizaciones encargadas de su estandarización. Entonces, se han desarrollado las especificaciones que ofrecen las primitivas de seguridad básicas: autenticación, autorización, integridad y confidencialidad para, a posteriori, revisar el resto de las especificaciones (o borradores de las mismas) de seguridad existentes más importantes.

Todo este análisis ha demostrado que el campo de la seguridad en los servicios web está en fases muy tempranas de su desarrollo. Todavía existen pocos estándares, aunque se atestigua un cuantioso esfuerzo, por parte de las principales organizaciones y compañías de la industria, en forma de especificaciones todavía que todavía se encuentran en etapa de borrador.

AGRADECIMIENTOS

Este trabajo se ha realizado en el marco del proyecto CALIPO (TIC2003-07804-C05-03) y la red RETISTIC (TIC2002-12487-E), de la Dirección General de Investigación del Ministerio de Ciencia y Tecnología.

REFERENCIAS

[1] W3C Decryption Transform for XML Signature - W3C Recommendation 10 December 2002 (2002). See http://www.w3.org/TR/2002/REC-xmlenc-decrypt-20021210

[2] W3C XML Signature Syntax and Processing- W3C Recommendation 12 February 2002 (2002). See http://www.w3.org/TR/xmldsig-core/

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

[4] W3C Extensible Markup Language (XML) 1.1 - W3C Recommendation 04 February 2004 (2004). See http://www.w3.org/TR/xml11

[5] Adams, C. and S. Boeyen UDDI and WSDL Extensions for Web Services: a security framework. Proceedings of the *ACM Workshop on XML Security*. Fairfax, VA, USA.(2002)

[6] WSAS. Web Services Architecture Specification - WC3 Working Draft 8 August 2003 (2003). See http://www.w3.org/TR/2003/WD-ws-arch-20030808/

[7] Box, D. (2002) Understanding GXA (2002). See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dngxa/html/gloxmlws500.asp

[8] Casati, F., E. Shan, U. Dayal and M.-C. Shan Business-Oriented Management of Web Services. Communications of the ACM, Vol. 46, Nº 10, October 2003, pp. 25-28. (2003)

[9] Chang, S., Q. Chen and M. Hsu Managing Security Policy in Large Distributed Web Services Environment. Proceedings of the *27th Annual International Computer Software and Applications Conference (COMPSAC'03)*. Dallas, Texas.(2003)

[10] IBM and Microsoft. Web Services Framework (2001). See

http://www.w3.org/2001/03/WSWS-popa/paper51

[11] Geuer-Pollmann, C. XML Pool Encryption. Proceedings of the *Workshop on XML Security*. Fairfax, VA: ACM Press.(2002)

[12] Harman, B., D.J. Flinn, K. Beznosov and S. Kawamoto *Mastering Web Services Security*. Wiley. (2003)

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

[14] Web Services Description Language (WSDL) 1.1 - W3C Note 15 March 2001 (2001). See http://www.w3.org/TR/wsdl

[15] IDC: Web services to enable $4.3B hardware market by 2007 (2003). See http://www.computerworld.com/hardwaretopics/hardware/story/0,10801,81496,00.html

[16] Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V1.1 - OASIS Standard, 2 September 2003 (2003). See http://www.oasis-open.org/committees/download.php/3404/oasis-sstc-saml-sec-consider-1.1.pdf

[17] O'Neill, M., P. Hallam-Baker, S.M. Cann, M. Shema, E. Simon, P.A. Watters and A. White *Web Services Security*. McGraw-Hill. (2003)

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

[19] Rescorla, E. and B. Korver, *RFC 3552. Guidelines for Writing RFC Text on Security Considerations*. IETF. Network Working Group. p. 39.(2003)

[20] Web Services Security (WS-Security) - Specification 6 April 2004 (2004). See http://xml.coverpages.org/ws-security.html.

[21] W3C XML Key Management Specification (XKMS) - W3C Note 30 March 2001 (2001). See http://www.w3.org/TR/xkms/

[22] Stallings, W. *Network Security Essentials*. 2 ed. Prentice Hall. 409. (2003)

[23] WS-Security Profile for XML-based Tokens - Specification 28 August 2002 (2002). See http://www-106.ibm.com/developerworks/webservices/library/ws-sectoken.html

[24] SAML. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 (2003). See http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf