# WS-Security (Web Services Security) aplicado en dispositivos datapower (XS40)

Ing. Luz Esmeralda Gamba Pachón
esmeluz1@hotmail.com
Universidad Piloto de Colombia – Especialización en seguridad informática

***ABSTRACT:*** *Currently WS-Security (Web Services Security) plays an important role in the integration and sharing of information within and outside companies. Because it allows to establish a methodology to monitor services globally rather than individually. By implementing WS-Security (Web Services Security) datapower devices, will enable better management and governance functionality in high-performance services, providing security, routing and complexity without making changes to the application code. By using WS-Security Policy (Web Services Security) you may access information in a comprehensive and safely increasing message processing, access control and encryption of these applications.*

***RESUMEN:*** *Actualmente WS-Security (Web Services Security) juega un papel importante en la integración e intercambio de información dentro y fuera de las compañías. Debido a que permite establecer una metodología para controlar los servicios de manera global en vez de en forma individual. Al implementar WS-Security (Web Services Security) en dispositivos datapower, permitirá un mejor manejo en la funcionalidad y gobernabilidad en servicios de alto rendimiento, facilitando la seguridad, enrutamiento y complejidad sin necesidad de realizar cambios en el código de las aplicaciones. Al hacer uso de políticas WS-Security (Web Services Security) se podrá acceder a la información de manera integral y segura aumentando el procesamiento de mensajes, control de acceso y cifrado entre dichas aplicaciones.*

**PALABRAS CLAVE:** Datapower, XS40, WS-Security, SOAP, WSDL, XML.

## 1 INTRODUCCION

Hoy en día las compañías buscan la interoperabilidad de sus aplicaciones en forma de servicios web de manera dinámica, para establecer una gobernabilidad que no dependan de la plataforma o de la aplicación. Es por esto que WS-Security (Web Services Security) como estándar en el intercambio de datos, permite bajo los requerimientos que especifica la máquina y el manejo de metadatos, tomar decisiones para la creación de aplicaciones automatizadas. Al realizar la creación de dichas aplicaciones existe una organización web de interoperabilidad (WS-I Organización), que busca estandarizar la forma en la que se entregan y se solicitan los servicios web. Creando así, varias especificaciones que incluyen a Microsoft, IBM y VeriSign.

WS-Security (Web Services Security) ofrece varias mejoras asociadas a la mensajería como la protección de los datos, la integridad, confidencialidad y la autenticación del remitente. Lo anterior basado en el protocolo de SOAP (Simple Object Access Protocol). En los mensajes SOAP, WS-Security utiliza la capa de mensajes, para la autorización, cifrado y autenticación de los metadatos en el cuerpo del mensaje. WS-Security junto con el cifrado XML son fundamentales para la seguridad de servicios web, dicho cifrado es muy importante ya que garantiza que los datos o la información va a ser leída desde internet.

[1] Para el desarrollo de software, los servicios web son muy importantes ya que inicialmente las aplicaciones no se comunicaban entre ellas, se manejaban los procesos por lotes para pasarlos de una máquina a otra, este proceso no se realizaba en tiempo real. Con la llegada de los sistemas distribuidos se mejora en gran medida la comunicación entre las aplicaciones, ya que se adaptan componentes como NTS, Corba, EJBs, entre otros, que permiten conectar las aplicaciones de otros sistemas como si estuvieran en la máquina local. Sin embargo, estas hacían uso de middleware orientado a mensajes y el servidor cliente necesariamente tenía que manejar el mismo componente para establecer la comunicación entre las aplicaciones.

A partir de ahí aparece un nuevo concepto llamado servicios web que inicialmente permiten el intercambio de mensajes basados en SOAP. Los mensajes que se manejan bajo SOAP, internamente son XML (Extensible Markup Language) que son accesibles desde cualquier aplicación, luego el servidor receptor interpreta el mensaje enviado y este lo retorna mediante otro mensaje SOAP.

Al utilizar aplicaciones sencillas se recomienda manejar especificaciones como: XML y REST. REST (Transferencia de Estado Representacional), es un servicio que permite acceder a un usuario o una URL y la respuesta de esta transferencia se presenta como un documento XML. Cuando se trata de aplicaciones empresariales que necesitan intercomunicarse local o remotamente, se recomienda manejar especificaciones basadas en SOAP. Hay dos tipos de especificaciones SOAP: La básica y las ampliadas:

### 1.1 ESPECIFICACIONES BÁSICAS

SOAP (Simple Object Access Protocol): Los servicios web basados en SOAP manejan varios aspectos del mensaje, como el encabezado permitiendo crear varias aplicaciones en la que los mensajes pasan a través de distintos puntos antes de llegar al servidor final.

WSDL (Web Services Description Language): Esta especificación maneja claramente el rumbo que deben tomar los mensajes y definir cuál es su destino.

UDDI (Universal Description, Discovery and Integration): Se creó como un repositorio global, para que las empresas accedieran a los servicios web que necesitaran. Sin embargo, no tuvo mayor éxito ya que las

compañías tenían que exponer sus sistemas y esto genero un ambiente de desconfianza.

## 1.2 ESPECIFICACIONES AMPLIADAS:

WS-Security: Permite crear aplicaciones para que los mensajes que se envían no sean interceptados o espiados, para esto maneja las firmas digitales y el encriptado.

WS-Policy: Esta especificación maneja políticas de seguridad para los servicios web. Es una ampliación del estándar WS-Security, ya que permite definir que aplicaciones van hacer uso del servicio web.

Existen otras especificaciones que son más específicos al momento de trabajar con servicios web como por ejemplo: WS-BPEL que permite la ejecución de procesos de negocios de servicios web. La especificación WS-Reliable Messaging, permite confirmar que el mensaje fue entregado o recibido y se recibe una copia de este proceso.

Al momento de exponer los servicios web en la red, los mensajes que están en tránsito requieren garantizar la integridad y la protección de los datos, para que estos no sean leídos o alterados, esta característica la ofrece [2] WS-Security que permite autenticar al cliente por medio de los tokens de seguridad a través de los mensajes SOAP, firmas digitales y cifrado con el fin de asegurar el envío y la recepción de los mismos.

# 2 DISPOSITIVO DATAPOWER

Los servicios web juegan un papel importante en la integración de la información dentro y fuera de las empresas. Con el Datapower se tiene un gran respaldo al acceder a las aplicaciones de forma segura manteniendo la integridad de los datos, disminuyendo notablemente los costos, administrando de manera óptima el rendimiento de recursos a nivel de infraestructura, procesamiento ágil en todos los mensajes y servicios que se hayan activado en el dispositivo, brindando así seguridad y filtrado de mensajes, validación de firmas y cifrados entre las aplicaciones, esto permite un mejor control y gobernabilidad sobre los servicios web.

El dispositivo datapower disminuye las amenazas que se puedan presentar dentro y fuera de las compañías evitando el acceso no autorizado, esto con el fin de prevenir configuraciones maliciosas en la red de forma intencional o accidental. Este control de acceso, el datapower lo realiza mediante ACL (Lista de control de acceso) donde se definen las IP de los clientes que se van a conectar al dispositivo, sin embargo es necesario que una vez se identifique la IP el cliente debe ingresar el usuario y la clave, ya que la autorización y la autenticación persiste. El proceso de autenticación en el datapower consiste en que el usuario se autentica contra un repositorio de usuarios, este repositorio o base de datos se puede alojar local o remotamente. Luego de que se realiza la autenticación, el dispositivo datapower realiza la validación de privilegios para acceder a los recursos que previamente se hayan configurado en el perfil del usuario. Una de las características del datapower es que define de manera clara las responsabilidades y roles tanto para los desarrolladores como los administradores.

El datapower optimiza el balanceo de carga de forma dinámica y eficiente. Administrando los pesos en función del tráfico y las condiciones de trabajo que se estén manejando en el momento. Esto disminuye los costos ya que si esta opción se configura en el datapower no es necesario adquirir un dispositivo adicional. Para facilitar este conjunto de características del dispositivo datapower, este cuenta con la opción de crear y gestionar varios dominios lógicos para soportar las implementaciones realizadas. La creación de estos dominios se realiza a partir de una máquina física donde se dividen en varios subsistemas lógicos que comparten los mismos recursos de red, memoria y CPU que maneja el datapower. Es por esto que el administrador debe configurar estos recursos de forma adecuada para que los dominios no compitan entre sí. Aunque no hay un límite en el número de dominios que se puedan crear si es necesario evaluar que ese dominio no va a entrar en conflicto con los demás. La ventaja de manejar estos dominios es que cada unidad lógica puede tener su propia configuración.

La interfaz del datapower se puede administrar a través de SSH, Telnet, gestión de XML y SNMP. Como esta administración se hace desde la red, en el datapower se divide el tráfico de administración para que quede aislado y evitar algún ataque a la administración del dispositivo. [6] Para estas posibles amenazas, el datapower cuenta con un sistema de monitoreo que permite identificar el estado de los componentes que están conectados dentro de la red. Este monitoreo se basa en SNMP (Simple Network Management) este protocolo maneja estadísticas donde manejan alertas asociadas al sistema operativo, servicios de aplicación, consumo etc. Este monitoreo también se puede configurar a nivel de aplicación haciendo uso de la interfaz XMI (XML management interface) está orientada a validar la respuesta del servicio SOAP.

## 2.1 CARACTERÍSTICAS DEL DATAPOWER

Los dispositivos del Datapower tienen las siguientes características:

### 2.1.1 Seguridad Mejorada

Soporte sobre XML/SOAP y firewall, validación de información, control de acceso, virtualización de servicios y aceleración a nivel de SSL.

### 2.1.2 Aceleración

Minimiza las implementaciones XML y la sobrecarga de los servidores, procesando de manera ágil los servicios que se hayan configurado en el datapower. Una de las capas más relevantes dentro de la arquitectura del datapower es la capa web:

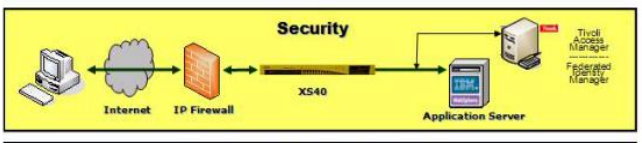


**Figura 1.** Bill Hines, John Rasmussen, Jaime Ryan, IBM WEBSPHERE DATAPOWER SOA APPLIANCE HANDBOOK, ISBN 9780137148196, 2009

### 2.1.3 Fácil instalación

Es un dispositivo fácil de mantener como dispositivo de red y a nivel de aplicación maneja estándares de servicios web XML. El datapower cuenta con una interfaz gráfica WebGUI la cual permite realizar diferentes acciones como enrutamiento, descifrado, procesamiento mediante flujos de mediación. En la figura 2 se puede observar la interfaz para crear acciones de las diferentes mediaciones configuradas en el datapower.

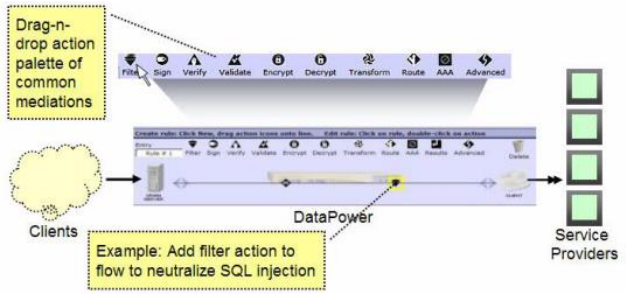


**Figura 2**. Gerry Kaplan, Jan Bechtold, Daniel Dickerson, Richard Kinard, Ronnie Mitra, Helio L. P. Mota, David Shute, John Walczyk, IBM DataPower SOA Appliance Administration, Deployment and Best Practice, 2008

Este modelo de datapower se centra en la seguridad de la información (XML). Si los mensajes están mal formados el datapower realiza la validación y protección contra posibles amenazas, desbordamientos o vulnerabilidades.

Este modelo con referencia XS40 garantiza que los archivos XML son legítimos y conservan su estructura. El XS40 maneja varios estándares de control como LDAP (Lightweight Directory Access Protocol), SSL, WS-Securty entre otros.

En el modelo de datapower XS40 las compañías pueden centralizar sus aplicaciones y la seguridad en un solo dispositivo, por medio de enrutamientos y normas de seguridad. Una de las ventajas que maneja el datapower XS40 es su administración de servicios web ya que se puede realizar local o remotamente.

## 2.2 VENTAJAS DEL DATAPOWER XS40

Cumplen un papel importante en un ambiente SOA, ya que permiten le gestión y el control centralizado. Realizando un monitoreo de los servicios, solicitudes y respuestas sin afectar el rendimiento del Datapower.

Permite realizar seguimiento de tráfico a bajo nivel haciendo uso del módulo de estadísticas, donde en tiempo real muestra las transacciones, los mensajes y sus correspondientes tamaños, errores y rendimiento en general del dispositivo.

Permite la integración con múltiples aplicaciones de monitorización como IBM Tivoli Monitoring, IBM Tivoli Composite, Netegrity SiteMinder entre otros.

Con WS-Security implementado en el datapower las empresas manejan los temas de seguridad y control de acceso validando y rechazando los mensajes que estén sin firmar. Esta validación se realiza mediante la implementación de un firewall XML propio del datapower que filtra y valida la información que entra y sale en forma de mensaje. Ofreciendo protección contra virus, inyecciones de código SQL, ataques de diccionario y demás amenazas. Debido a que hoy en día las empresas integran más aplicaciones a sus sistemas, requieren hacer uso de los servicios web orientados a SOA, sin consumir un alto porcentaje de procesamiento para esto, el datapower maneja en forma independiente el procesamiento XML para no sobrecargar los servidores de aplicaciones.

### 2.2.1 WS- Security Capacidades de Cifrado / Descifrado

La seguridad basada en http no es suficiente cuando la información tiene que realizar varios saltos antes de llegar al destino. Datapower ofrece una solución más compleja que permite controlar y mantener la seguridad en cada uno de los puntos por los que pasa la información. WS-Security mediante los tokens de seguridad y la firma XML permite mantener la integridad de los mensajes y notificar cuando se realicen modificaciones en los mensajes.

### 2.2.2 Firma digital en el Datapower

Para el manejo de la integridad de los mensajes, el Datapower utiliza medios criptográficos y tiene su propio almacén de certificados con el fin de protegerse contra el acceso externo.

## 2.3 ESPECIFICACIONES SOPORTADAS POR EL DATAPOWER

En la Figura 3 se puede observar las especificaciones soportadas por el dispositivo Datapower:

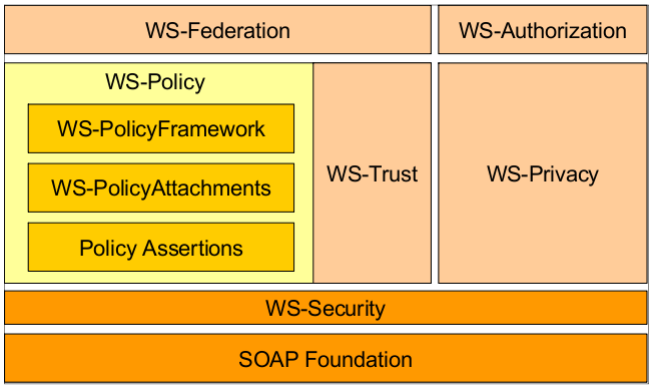


**Figura 3**. Mike Ebbers, Bill Barrus, Servais Bonazebi, Peter Daly, Charlton Lee, DataPower Architectural Design Patterns, 2008

WS-Policy es una especificación que permite establecer políticas en materia de calidad de servicio, seguridad utilizando XML. Estas políticas son implementadas en los intermediarios o puntos finales como por ejemplo los tokens, los algoritmos de seguridad entre otros.

WS-Trust es un estándar que permite establecer una comunicación segura dentro del marco de los servicios web, específicamente se centra en la renovación,

validación, la correlación de la identidad de los tokens de seguridad

WS-Conversation es una especificación basado en los estándares WS-Security que utiliza un contexto para el intercambio continuo de mensajes.

### 2.3.1 Datapower XS40 AAA (Autenticación, Autorización y Auditoría

AAA viene del acrónico Autenticación, Autorización y Auditoría. Es utilizado por el datapower para el control de acceso y determinar si un usuario puede acceder a determinado recurso. [3] Independientemente de la referencia del datapower la acción AAA puede ser utilizada en cualquier servicio como Gateway multiprotocolo, firewall XML etc. Una vez se establezca el servicio se debe crear o configurar la política AAA dependiendo de los requerimientos de la aplicación. Los requerimientos mínimos para crear una política AAA son:

Extraer la identidad: Identifica quien es el usuario que está realizando la solicitud de ingreso al sistema. Estos datos vienen registrados en el encabezado HTTP, en el contenido del XML, en los mensajes SOAP. Una vez se identifica el usuario, se pasa a la siguiente etapa que es la autenticación, está se puede realizar por medio de un directorio activo, LDAP, Tivoli, en donde se tiene una plantilla con el listado de los usuarios autenticados. Ya identificado el usuario que desea ingresar al sistema se procede a identificar a que recurso va a acceder y se cierra el ciclo con la autorización al sistema una vez haya validado los puntos mencionados. Aunque no es obligatorio también es recomendable adicionar WS-Security al mensaje y la activación de la auditoría para confirmar si el acceso fue satisfactorio o fallido.

## 3 CONCLUSIONES

Se puede concluir que WS-Security es la mejor opción de implementación en dispositivos datapower XS40, cuando se van a realizar conexiones múltiples con otros servidores o servicios, ya que mantiene la integridad y la autenticidad de los datos. Mientras que SSL en cierto punto tiene limitantes ya que solo opera en conexiones directas con el cliente.

Al utilizar WS-Security se mantiene la integridad de los datos en un alto porcentaje ya que permite asegurar que los mensajes no fueron manipulados durante su trayecto. A su vez garantiza la autenticidad de los mensajes a través de firmas digitales y tokens de seguridad y es posible guardar un documento con los usuarios que se han autenticado, dado el caso que se requiera alguna auditoría. A diferencia de SSL que en ocasiones no es tan fácil guardar la secuencia de información entre cliente-servidor.

Cada vez más las compañías que manejan un alto volumen de transaccionalidad, implementan dentro de su arquitectura dispositivos como el datapower ya que proporciona características de seguridad, integración, escalabilidad porque mejora el rendimiento de los recursos y disminución de costos.

El datapower XS40 es un dispositivo que ofrece configuraciones en alta disponibilidad, auto-balanceo, monitoreo de recursos y aplicaciones, garantizando la continuidad del negocio. El datapower optimiza los firewall al encontrarse dentro de una DMZ en temas de seguridad, ya que constantemente esta inspeccionando la construcción de los mensajes que llegan o salen del dispositivo.

## 4 REFERENCIAS


[1] Rosenberg, Jothy; Remy, David, Securing Web Services with WS-Security,vol. 1, n. 1, pp. 1-448, 2004

[2] Sanjiva Weerawarana, Francisco Curbera, Frank Leymann, Tony Storey, Donald F. Ferguson, Web Services Platform Architecture, ISBN: 0-13-148874-0, 2005

[3] Bill Hines, John Rasmussen, Jaime Ryan, IBM WEBSPHERE DATAPOWER SOA APPLIANCE HANDBOOK, ISBN 9780137148196, 2009

[4] Juan R. Rodriguez, Somesh Adiraju, Joel Gauci, Markus Grohmann, Davin Holmes, Tamika Moody, Srinivasan Muralidharan, Christian Ramirez, IBMAdolfo Rodriguez, WebSphere DataPower SOA Appliances, 2008

[5] Mike Ebbers, Bill Barrus, Servais Bonazebi, Peter Daly, Charlton Lee, DataPower Architectural Design Patterns, 2008

[6] Gerry Kaplan, Jan Bechtold, Daniel Dickerson, Richard Kinard, Ronnie Mitra, Helio L. P. Mota, David hute, John Walczyk, IBM DataPower SOA Appliance Administration, Deployment and Best Practice, 2008