CAPÍTULO 8: INTRODUCCIÓN A SAML

Basándonos en el marco de seguridad que tenemos que tener en nuestro proyecto, introducimos la especificación SAML (*Security Assertions Markup Language*). Será por medio de SAML por lo que intentemos crear el citado marco de seguridad.

En este punto se trata de presentar datos que nos servirán para ir conociendo el tema de manera general. A continuación hablamos de la historia de la especificación, haciendo un recorrido entre las distintas versiones de ésta, y detallamos las nuevas ventajas y características que ofrece la última versión. Terminamos esta parte indicando la relación que tiene SAML con los estándares que ya existían y se dedicaban a realizar parte de las funcionalidades de la especificación, entre ellas autentificación y seguridad.

8.1.- Introducción

SAML (*Security Assertions Markup Language*) es un entorno basado en XML para servicios Web que permite el intercambio de información de autorización y autenticación entre diferentes sitios Web.

Está desarrollado por los comités técnicos de servicios de seguridad de OASIS (*Organization for the Advancement of Structured Information Standards*). Ofrece a los desarrolladores de espacios Web un estándar abierto que permitirá que los usuarios puedan visitar múltiples sitios Web de comercio electrónico sin necesidad de identificarse nada más que una vez.

Además permite, a los visitantes, visitar dichos sitios alojados por distintas compañías, facilitando la adquisición de productos o servicios en los mismos, al no requerir que estos usuarios tengan que registrarse y dar sus datos personales a través de Internet cada vez que entren en una Web.

SAML es flexible y extensible y está diseñado para ser utilizado por otros estándares. Integra protocolos y entornos de mensajería ya presentes en la industria, como XML Signature, XML Encryption y SOAP. La especificación puede integrarse en entornos de estándares como HTTP y navegadores Web estándares. Como ejemplo, ya adoptaron este protocolo:

- Liberty Alliance.
- Internet2 Shibboleth
- OASIS Web Services Security (WS-Security), etc.

8.2.- Historia de SAML

La versión SAML 1.0 llegó a ser un estándar de OASIS en noviembre de 2002. Le siguió la versión SAML 1.1 en septiembre de 2003 y ha visto un éxito significativo dentro de la industria, ganando ímpetu en servicios financieros. La versión definitiva, SAML 2.0, se publicó el 15 de Marzo de 2005

SAML ha sido puesto en ejecución ampliamente por todos los vendedores importantes de la gestión del acceso Web. Está también apoyado en los principales productos de aplicaciones de servidor y respalda tanto a los gestores de Servicios Web como a los vendedores de seguridad.

La versión SAML 2.0 se construye sobre ese éxito. Unifica los bloques dispares de construcción de identidad federados anteriores de SAML 1.1, con la entrada en la iniciativa de Shibboleth y el marco de la federación de identidad de Liberty Alliance. Como tal, SAML 2.0 es un paso crítico hacia la convergencia completa de los estándares de identidad federados.

8.3.- Ventajas que aporta

La versión definitiva de la especificación aporta nuevas e importantes ventajas que le confieren un gran potencial para que tenga éxito con respecto a su uso. Entre las ventajas que SAML incluye están:

- **Plataforma neutral**: SAML abstrae el marco de la seguridad lejos de puestas en práctica y de arquitecturas particulares de vendedores.

- **Acoplador flojo de directorios**: SAML no requiere la información del usuario para ser mantenido y sincronizado entre principales.

- **Experiencia en línea mejorada para usuarios finales**: las aserciones de la autentificación de SAML permiten “single sign-on” consintiendo que los usuarios se autentifiquen en un proveedor de identidad y después tengan acceso a servicios/recursos en los proveedores de servicio sin autentificación adicional.

- **Costes administrativos reducidos para los proveedores de servicio**: el uso de SAML para la federación entre los dominios de identidad puede reducir el coste de mantenimiento de la información de la cuenta (por ejemplo el nombre de usuario y la contraseña). Esta carga se pone en el proveedor de identidad.

- **Transferencia del riesgo**: SAML puede ceder la responsabilidad de la gestión de las identidades al proveedor de identidad, que es a menudo más compatible con su modelo de negocios que el de un proveedor de servicios.

8.4.- Características nuevas que incorpora

Otra de las cuestiones por las que se ha producido un incremento en el uso de SAML 2.0 son las características nuevas que incorpora, que junto con sus ventajas le proporcionan unas potencialidades muy importantes para ser el estándar más usado en cuestiones de autentificación e información de identidad. SAML 2.0 incorpora las siguientes ventajas:

- **Seudónimos**: SAML 2.0 define cómo un identificador pseudo-aleatorio opaco sin correspondencia discernible con los identificadores significativos (por ejemplo los e-mail o los nombres de cuenta) se puede utilizar entre los proveedores para representar a los principales. Los seudónimos son una llave privada que permite la tecnología porque inhiben la colusión entre proveedores múltiples (cuando sea posible con un identificador global como en direcciones de e-mail).

- **Gestión de la federación**: SAML 2.0 define cómo dos proveedores pueden establecer y manejar posteriormente el seudónimo(s) para los principales para quienes están funcionando.

- **Gestión de la sesión**: El protocolo "*single logout*" (SLO) en SAML 2.0 proporciona un medio por el cual todas las sesiones proporcionadas por una autoridad particular de sesión puedan ser cercanas y simultáneamente terminadas. Como ejemplo, si un principal, después de autentificarse en un proveedor de identidad, estaba autentificado respecto a los proveedores de servicio múltiples ("*single sign-on*", SSO), podría ser automáticamente desconectado de todos esos proveedores de servicio a petición del proveedor de identidad.

- **Móvil**: SAML 2 introduce un nuevo soporte para el mundo móvil, tanto por los desafíos introducidos por los dispositivos y las limitaciones del ancho de banda como por las oportunidades hechas posibles al surgir los dispositivos activos o inteligentes.

- **Mecanismos de Privacidad**: SAML 2 incluye mecanismos que permiten que los proveedores se comuniquen, de unos a otros, las políticas de privacidad establecidas. Por ejemplo, el consentimiento de un principal (a una cierta operación que es realizada fundamental para la privacidad), se puede obtener en un proveedor y este hecho se puede comunicar a otros proveedores mediante las aserciones y los protocolos de SAML.

8.5.- Relación con otros estándares

Antes de sacar el estándar SAML, convivían distintas soluciones para los problemas de autentificación y manejo de la información de identidad. SAML nació con el fin de crear un estándar que englobara todas las soluciones. Así que tuvo en cuenta a todas estas soluciones en su gestación. A continuación se explican la relación con los estándares existentes:

Liberty Alliance

Es un consorcio de la industria que define los estándares para la federación de la identidad. Incluye la identificación de red federada directa sign-on simplificada usando los dispositivos actuales y que emergen del acceso de red, y el soporte y promoción de atributos basados en permisos para permitir la opción y el control de un usuario sobre el uso y el acceso de su identificación personal.

Liberty había definido su marco de ID-Federation en la base proporcionada por SAML 1.0. Reconociendo el valor de un estándar particular para SSO federado, Alliance sometió v1.2 de ID-FF en el SAML TC como entrada para SAML 2.0.

El marco de servicios ID-Web de Liberty, una plataforma para asegurar servicios Web, continúa desarrollándose dentro de Liberty Alliance. Liberty ID-WSF utiliza aserciones de SAML como formato de testigos de seguridad. Mediante ellas se comunica la información de autentificación y autorización asociada a varios agentes de servicio Web entre ellos.

Shibboleth

Es una iniciativa Internet2 [*http://www.internet2.edu/*] para compartir los recursos para los investigadores, los estudiantes graduados, etc. entre los institutos de educación superior. Como Liberty, Shibboleth perfiló SAML para sus requisitos particulares y construyó un gestor de privacidad dentro. La entrada de Shibboleth se ha realimentado en SAML 2.0.

XACML

XACML (*eXtensible Access Control Markup Language*) es un lenguaje basado en XML para el control de acceso que ha sido estandarizado en OASIS. Describe un lenguaje de políticas de control de acceso (quiénes pueden hacerlo y cuando) y un lenguaje de petición/respuesta. Éste último expresa preguntas sobre si un acceso particular debe ser permitido (las peticiones) y describe respuestas a esas preguntas (respuestas). XACML y SAML se complementan bien (a pesar de un cierto solape de ambos protocolos); una política de XACML puede especificar lo que debe hacer un proveedor cuando recibe una aserción de SAML.

WS-Security

WS-Security es un estándar de OASIS que especifica las extensiones de seguridad de SOAP que proporcionan integridad y confidencialidad de datos. Define un marco para asegurar mensajes SOAP- las especificaciones son definidas en perfiles determinados por la naturaleza de los testigos de seguridad usados para transportar la información de identidad. Así, por ejemplo, hay diversos perfiles de la WS-Security para los diferentes formatos de testigos de seguridad de los certificados X.509, de los tickets de Kerberos, y de las aserciones de SAML.

SAML también señala a la WS-Security como un mecanismo aprobado para asegurar los mensajes SOAP que llevan aserciones y mensajes de protocolo de SAML.