EXTENSIÓN DEL ESTÁNDAR SAML PARA ESCENARIOS SSO CON VARIAS FUENTES DE AUTENTICACIÓN

PhD. Oiner Gómez Baryolo
Doctor en Ciencias Informáticas.
Decano y docente de la Facultad de Sistemas y Telecomunicaciones de la Universidad Tecnológica ECOTEC.
ogomez@ecotec.edu.ec

PhD. Vivian Estrada Sentí
Doctora en Ciencias Informáticas.
Docente y directiva de la Universidad de Las Ciencias Informáticas, La Habana, Cuba.
vivian@uci.cu

Ing. Abraham Torres Calas
Ingeniero informático.
Universidad de las Ciencias Informáticas, Cuba.
abraham@uci.cu

Recibido: 5 de enero de 2015.
Aceptado: 3 de febrero de 2015.

RESUMEN

El desarrollo de aplicaciones web de gestión que informaticen los procesos presentes en las organizaciones se ha convertido en una práctica cotidiana que les permite mantenerse en un nivel competitivo. La criticidad que tienen estos sistemas para el correcto funcionamiento de los procesos empresariales, constituyen una debilidad que en muchas ocasiones es aprovechada por personas y organizaciones malintencionadas para ejecutar ataques informáticos. Por esta razón resulta necesario fortalecer el control de acceso a través de los procesos de identificación, autenticación, autorización y auditoría. La propuesta presentada en este trabajo se centra en los procesos de identificación y autenticación, tomando como base uno de los estándares más utilizados en la actualidad. Proponiendo una extensión que permita aumentar su nivel de aplicación e integración con múltiples fuentes de datos y el uso de varios mecanismos criptográficos de forma concurrente. La propuesta se materializa en un estudio de casos que

refleja su validez y forma de aplicación de una arquitectura *Single Sign-On* para entornos empresariales.

Palabras Clave: seguridad, identificación, autenticación, Single Sign-On.

ABSTRACT

The develop of management web applications to computerize the organizations processes has become a daily practice that allows them to stay at a competitive level. The criticality of these systems for the proper functioning of business processes constitute a weakness that often is used by individuals and organizations to execute malicious attacks. For this reason it is necessary to strengthen access control through the processes of identification, authentication, authorization and auditing. The proposal presented in this paper is focused on the processes of identification and authentication, based on one of the standards used today. Proposing an extension that allows increase their level of implementation and integration with multiple data sources and the use of various cryptographic mechanisms concurrently. The proposal is materialized in a study of case that reflects its validity and method of application of Single Sign-On architecture for enterprise environments.

Keywords: security, identification, authentication, Single Sign-On.

INTRODUCCIÓN

El vertiginoso desarrollo alcanzado en las nuevas tecnologías de la informática y las comunicaciones ha llevado a la sociedad a entrar en lo que se ha denominado como "era de la información". La información puede existir en muchas formas, impresa o escrita en papel, almacenada digitalmente, transmitida por correo postal o utilizando medios digitales, presentada en imágenes o expuesta en una conversación. Cualquiera que sea la forma que adquiere la información es un recurso que, como el resto de los activos importantes tiene un gran valor, siendo a veces incalculable, por contener la "vida" de una organización; es por eso que debe ser debidamente protegida independientemente de los medios por los cuales se distribuye o almacena.

Con el paso del tiempo se ha incrementado la necesidad de contar con información confiable,

íntegra y oportuna para el cumplimiento de los objetivos estratégicos de las organizaciones. Una de las respuestas más sólidas para esta tendencia está reflejada en los sistemas de gestión y dentro de ellos los Sistemas de Planeación de Recursos Empresariales (ERP2), que se concretan como solución luego de un intenso período de transformación que tuvo sus inicios en la década del ´60.

Los ERP pueden definirse como sistemas que integran y manejan muchas de las prácticas de los negocios asociados con las operaciones de producción y los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios. Es un sistema estructurado para satisfacer la demanda de soluciones de gestión empresarial, basado en el ofrecimiento de una solución completa que permite a las empresas evaluar, implementar y administrar con mayor facilidad su negocio.

Por la importancia que tiene la información que gestionan los sistemas ERP, persisten las razones y motivos para mantener mecanismos de control de acceso sobre las áreas (seguridad física) y la información (seguridad lógica) que se desea proteger. El control de acceso es el proceso de conceder permisos a usuarios o grupos de acceder a objetos tales como ficheros, direcciones, datos, entre otros. Está basado en tres conceptos fundamentales: autenticación, autorización y auditoría. En términos técnicos o lógicos el control de acceso proviene de la interacción entre un sujeto y un objeto que forman un flujo de información de uno al otro. El sujeto es la entidad que recibe o modifica la información o los datos contenidos en los objetos, puede ser un usuario, programa, proceso, entre otros. Un objeto es la entidad que provee o contiene la información o los datos, puede ser un fichero, una base de datos, una computadora, un programa, entre otros [1, 2]. Este proceso incluye autenticar la identidad de los usuarios o grupos, autorizar el acceso a datos o recursos y almacenar las trazas o log que permiten realizar auditorías para identificar violaciones.

El proceso de autenticación se inicia cuando un usuario o cliente requiere acceso a la red, debe presentar información personal que permita establecer de manera unívoca su identidad dentro del entorno. El usuario podrá presentar cualquier tipo de credencial de identidad (nombre de usuario y contraseña, certificado de identidad, secreto compartido), usando para ello algunos de los mecanismos de control de acceso. El servidor AAA y concretamente su servicio de

autenticación, deberá obtener dichas credenciales y de forma interna (mediante bases de datos, políticas de autenticación, servicios auxiliares) determinar si ese usuario es realmente quien dice ser. [3-5] [6-8]

Existen estándares internacionales que describen detalladamente los aspectos, herramientas y políticas a tener en cuenta en los procesos que componen los sistemas de control de acceso, para la autenticación, el más utilizado a nivel mundial es SAML[1], que ha sido creado y recomendado por la OASIS[2] *[9] [10] [11]*. La necesidad de autenticación se evidencia en actividades que se realizan hoy en día a través de Internet como el gobierno electrónico, banca electrónica, educación virtual, gestión y planificación de recursos, entre otros.*[12] [13]*

En marzo del 2005 OASIS adoptó como estándar SAML en su versión 2.0. SAML es un estándar para intercambiar información de autenticación y autorización entre dominios. Está diseñado para ofrecer SSO para interacciones automáticas o manuales entre sistemas. Permite el intercambio de información de autenticación y autorización sobre usuarios, dispositivos o cualquier entidad identificable llamados sujetos. Usando sintaxis de XML, SAML define el protocolo petición-respuesta por el que los sistemas aceptan o rechazan sujetos basados en aserciones. SAML define además dos conceptos fundamentales que son el Proveedor de Servicios[3] y el Proveedor de Identidad[4] que van a ser las partes que intervienen en la comunicación SAML, garantizando así que cualquier aplicación pueda intercambiar información de autenticación abstrayéndose del cómo.

La comunicación establece como conceptos las aserciones, protocolos, enlaces y perfiles, basándose en el estándar XML. Un enlace SAML determina como las peticiones y respuestas SAML son mapeadas en protocolos de mensajes y comunicaciones estándares.

[1] **(SAML):** Lenguaje de enmarcado de aserciones de seguridad.

[2] **(OASIS):** Organización de estándares avanzados de información estructurada.

[3] Un **proveedor de servicios** es un componente que ofrece servicios de acceso a recursos a sus subscriptores a través de la web.

[4] Un **proveedor de identidad** es un componente que provee un certificado digital o token de seguridad a sus subscriptores para la identificación. Se aplica a arquitecturas como SSO.

Figura 1. Elementos de la Arquitectura del estándar SAML.

El estándar SAML describe con detalle las especificaciones para lograr SSO en el proceso de autenticación de usuarios que intentan acceder a un recurso. Este proceso puede implementarse de varias maneras dependiendo del escenario de despliegue y las tecnologías que se utilicen.

La Fig. 2 muestra la arquitectura que adopta SAML para un escenario de autenticación utilizando enlaces HTTP POST para entregar la petición de autenticación SAML (Petición de autenticación PA) <AuthnRequest> al proveedor de identidades y un mensaje SAML (Respuesta de autenticación RA) <Response> es devuelto.

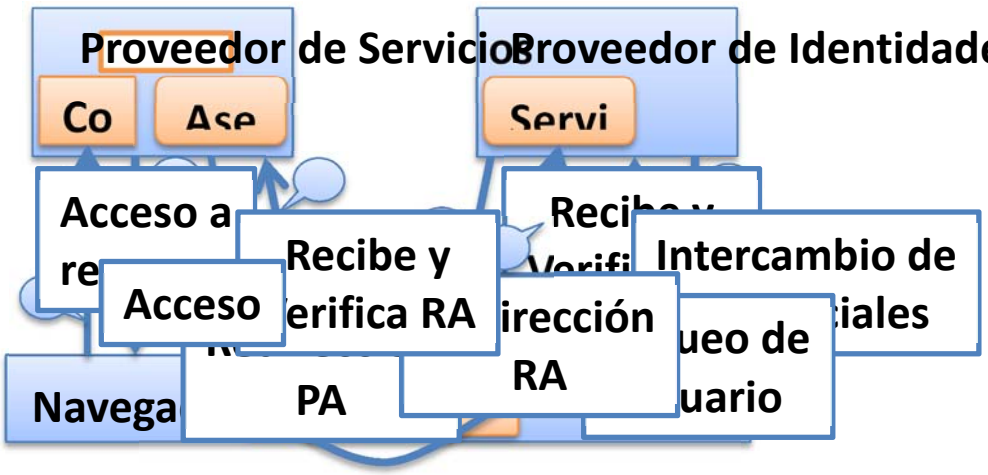

Figura 2. Autenticación utilizando el método POST.

La implementación de la arquitectura de SAML para la autenticación utilizando el protocolo SOAP, mantiene una filosofía similar a la que se describe en la **¡Error! No se encuentra el origen de la referencia.**2. Esta variante incorpora seguridad en el envío y recepción de credenciales.

La escalabilidad y capacidad de SAML se ven limitadas en entornos centralizados de de varias aplicaciones, producto a la restricción establecida para que un proveedor de identidad no pueda disponer de varias fuentes de datos simultáneamente.

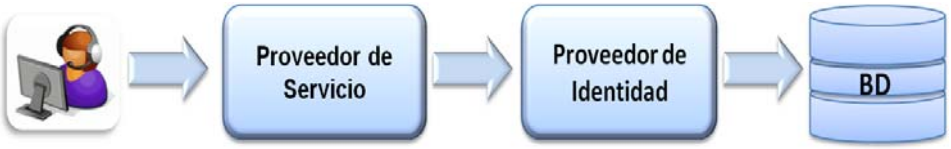

Figura 3. Flujo básico de Autenticación SAML.

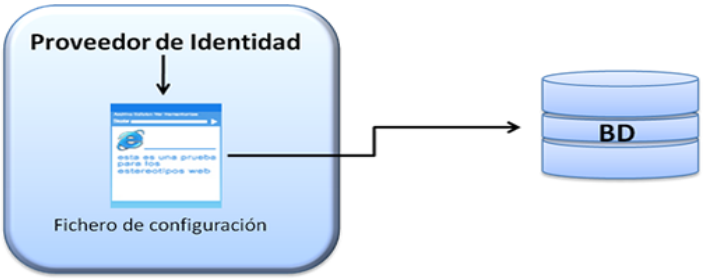

Figura 4. Descripción de acceso a fuente de autenticación.

El presente trabajo atendiendo a la problemática existe, centra sus objetivos en la extensión del estándar SAML para centralizar el proceso de autenticación en entornos de varias aplicaciones. La organización del trabajo es la siguiente: la Sección II muestra la extensión del estándar SAML para centralizar el proceso de autenticación en entornos de varias aplicaciones. La Sección III muestra un caso de estudio donde se aplica la extensión del estándar utilizando varias fuentes de autenticación. Finalmente, se pueden encontrar las conclusiones en la Sección IV.

EXTENSION DE SAML

Para minimizar los riesgos de seguridad en la autenticación de usuarios, a continuación se presentan soluciones de autenticación centralizada que garantizan la seguridad en cada uno de los escenarios de aplicación.

Escenario de autenticación básica

Un escenario de autenticación básica, cubre la necesidad de una aplicación web que necesita autenticar a los usuarios que intenten acceder a ella y para ello solicita este servicio a una fuente destinada garantizar este proceso. Para lograr este objetivo se integran varios estándares, herramientas y tecnologías reflejados en la5. El modelo está constituido por los siguientes conceptos:

- Navegador: herramienta que le permite al usuario acceder a los recursos publicados en servidores de aplicaciones, servidores ftp, entre otros atreves de la web. Entre los más utilizados a nivel mundial se encuentran Mozilla Firefox, Internet Explorer, Opera, entre otros.
- Servidor de App: los servidores de aplicaciones son los encargados de publicar las aplicaciones para que se pueda acceder atreves de un navegador web.
- App: aplicación web creada con el objetivo de informatizar uno o varios procesos dentro de una organización.
- SIGIS: Sistema de gestión integral de seguridad que tiene la responsabilidad de gestionar la autenticación de usuarios.
- BD: base de datos que contiene toda la información relacionada a los usuarios y los sistemas, en este caso forma parte de las fuentes de autenticación.
- ACL: ficheros que contienen listas de control de acceso que pueden contener las credenciales de los usuarios y los privilegios asignados.
- Directorios activos: son estructuras que forman parte de la infraestructura de una organización para garantizar servicios como la autenticación de usuarios.

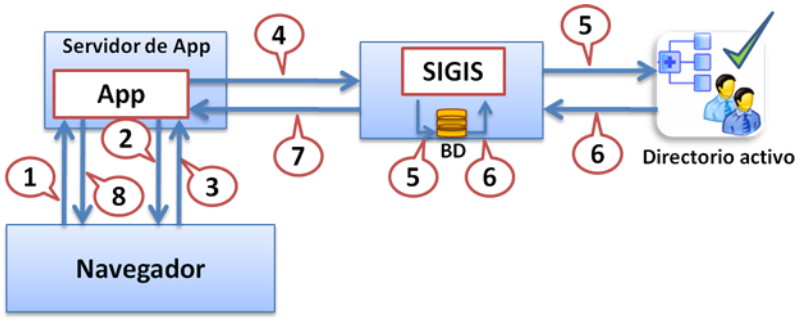

Figura 5. Escenario de autenticación básica.

La solución propuesta para dar respuesta al escenario de autenticación básica, separa la gestión

de la autenticación de la lógica de la aplicación y evita que cada aplicación tenga que implementar las vías de interacción con las fuentes de autenticación. La aplicación confía este proceso a SIGIS y se limita a consumir el servicio. Una de las ventajas que incorpora esta solución es la escalabilidad que mantiene a la hora de incorporar otras aplicaciones en el entorno de gestión de la entidad.

Para comprender mejor la solución propuesta, a continuación se describen los pasos a seguir para lograr la autenticación de los usuarios.

1. El proceso de autenticación se inicia cuando el usuario intenta acceder a una aplicación, objeto o acción por medio de un navegador web.
2. La aplicación recibe la petición y procede a realizar las verificaciones pertinentes para conceder el acceso. En este escenario la aplicación tiene la responsabilidad de gestionar las sesiones de usuarios (inicio, verificación y cierre).
    2.1 En caso que el usuario no tenga creada una sesión o la misma no esté activa producto al tiempo de expiración, veracidad del certificado o token de seguridad (verificado mediante el paso 7 y 8), entre otros aspectos que condicionan su valides, la aplicación procede a mostrarle la ventana de autenticación para que introduzca sus credenciales.
    2.2 Si la aplicación verifica que el usuario ya cuenta con una sesión válida, inmediatamente el proceso pasa al paso 8.
3. El usuario introduce las credenciales que serán verificadas en la fuente de autenticación.
4. La aplicación consume el servicio de autenticación mediante el protocolo de comunicación definido, enviando las credenciales del usuario y demás parámetros especificados en el contrato del servicio. Uno de los parámetros que debe enviar la aplicación es la credencial que asegura que es ella la que está solicitando el servicio. Antes de consumir el servicio debe aplicarse el método de cifrado y firma digital definido para garantizar la seguridad en la comunicación.
5. SIGIS recibe las credenciales tanto del usuario como de la aplicación y procede a realizar las verificaciones pertinentes. El identificador de la aplicación, aparte de garantizar la autenticidad de la petición, se utiliza para identificar la fuente de autenticación a utilizar para comprobar las credenciales del usuario. Las fuentes de autenticación (LDAP,

OpenLDAP, base de datos de SIGIS) se configuran con anterioridad y se asignan a nivel de aplicación o de usuario. Concluido el proceso de selección de la fuente de autenticación, SIGIS interactúa con la base de datos o directorio activo para validar las credenciales del usuario.

6. Se retorna el resultado de la verificación de las credenciales del usuario.
7. SIGIS analiza el resultado de la verificación:
   7.1. En caso positivo crea un certificado o token de seguridad para identificar el usuario, lo almacena para procesos de verificación posteriores y se lo envía a la aplicación.
   7.2. En caso negativo no crea el identificado y retorna el resultado a la aplicación.
8. La aplicación analiza el resultado de la verificación de credenciales:
   8.1. En caso positivo crea una sesión para el usuario, almacena el certificado que va a identificar al usuario en el proceso de autorización y concluyendo así la autenticación.
   8.2. En caso negativo muestra un mensaje de error y ejecuta el paso 2 para iniciar nuevamente el flujo.

Escenario de autenticación utilizando SAML sin SSO

El estándar SAML descrito en la sección 1.5.4, permite que las organizaciones decidan si el nivel de seguridad y políticas de una aplicación son suficientes para proteger sus recursos. Esta característica de SAML estimula relaciones de confianza y acuerdos operacionales entre aplicaciones web, donde cada acuerdo para adherirse a un nivel de línea base de verificación debe realizarse antes de aceptar una aserción.

Un escenario de autenticación donde se utilice SAML sin Single Sign-On (SSO), fusiona los conceptos proveedor de servicios (PS) y proveedor de identidades (PI) en un mismo directorio de publicación. Este escenario de aplicación se produce cuando la solución SAML convive con la aplicación en un mismo directorio de publicación como se muestra en Figura. A partir de este momento cada aplicación contará con su PS-PI y se pierde la posibilidad de garantizar un entorno SSO.

La decisión de asumir la implementación de una solución de este tipo, evita que las aplicaciones tengan que gestionar todo lo relacionado con la autenticación. El componente PS-PI asume todo lo relacionado con el logueo de usuarios, gestión de sesiones (inicio, verificación y cierre), cifrado

de los datos y comunicación con SIGIS. Cuando el usuario intente acceder a la aplicación, la misma sólo tendrá que redireccionar la petición al componente PS-PI.

El modelo propuesto para ser aplicado en escenarios de este tipo incorpora conceptos que no están presentes en la solución del escenario anterior, a continuación se procede a describir cada uno de ellos.

- SP-PI: radica en la fusión de dos conceptos que especifica el estándar SAML, el PS y el PI. Un proveedor de servicios es un componente que ofrece servicios de acceso a recursos a sus subscriptores a través de la web y un proveedor de identidad es un componente que provee un certificado digital o token de seguridad a sus subscriptores para la identificación.

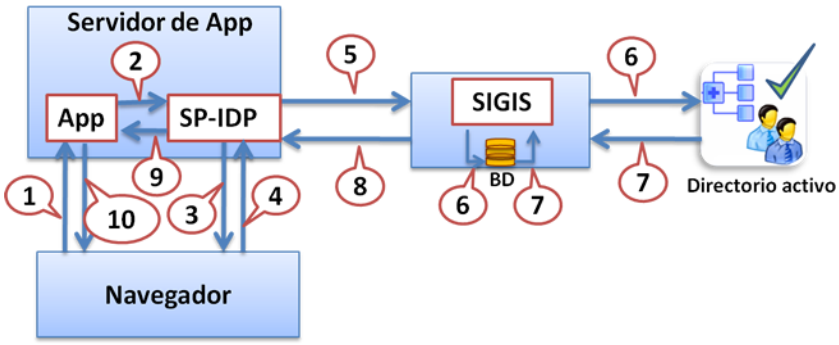

Figura 6. Escenario de autenticación utilizando SAML sin SSO.

La solución propuesta para este escenario, mantiene la misma filosofía que la anterior e incorpora las ventajas que brindan las soluciones desarrolladas bajo el estándar SAML. Al introducir un nuevo concepto, el flujo de pasos para llevar a cabo la autenticación presenta las variaciones que se especifican a continuación.

2. La aplicación recibe la solicitud de acceso del usuario e instancia al componente PS-PI.
3. El componente PS-PI ejecuta las acciones que realizaba la aplicación en el paso 2 del escenario anterior.
9. El componente PS-PI ejecuta las acciones que realizaba la aplicación en el paso 8 del escenario anterior.
   9.1. En caso positivo le envía a la aplicación el certificado asignado al usuario autenticado para que inicie el proceso de autorización.
   9.2. En caso negativo muestra un error de autenticación y ejecuta el paso 3 para que se inicie el proceso nuevamente.

Escenario de autenticación utilizando SAML utilizando SSO

Los escenarios que aplican SAML, definen declaraciones de contextos de autenticación. El objetivo es poder dar información adicional acerca del nivel de confianza en la autenticación, que se deriva directamente de las tecnologías, protocolos y procesos que se han utilizado para dicha autenticación. En el estándar se definen ocho asociaciones distintas de protocolos y transportes específicos a un caso de uso/aplicación (Web SSO profile, Attribute profile, entre otros). La solución propuesta aplica el caso típico de uso del Single Sign-On (SSO), que permite a los usuarios acceder a diversos sitios en la federación con una única autenticación.

El escenario a resolver plantea que un usuario puede acceder desde un mismo cliente a varias aplicaciones simultáneamente, manteniendo las características de un entorno SSO. Para cumplir este objetivo, las aplicaciones a las que accede el usuario, deben garantizar el uso de un mismo PI y predeterminar en SIGIS la fuente de autenticación para garantizar la seguridad del proceso. En el caso de los PS, cada aplicación puede adoptar una solución diferente siempre que cumpla con el estándar y utilicen el mismo PI. Aunque las aplicaciones pueden encontrarse en servidores web diferentes, es necesario que se registren y configuren en SIGIS con anterioridad.

Una de las características más relevantes presentes en la solución del escenario, es que a pesar de no incorporar ningún concepto diferente a los utilizados en solución del escenario anterior, separa los conceptos PS y PI. El objetivo de esta separación radica en la necesidad de garantizar un entorno SSO de acceso a las aplicaciones. La 7muestra la solución propuesta para dar solución al escenario planteado.

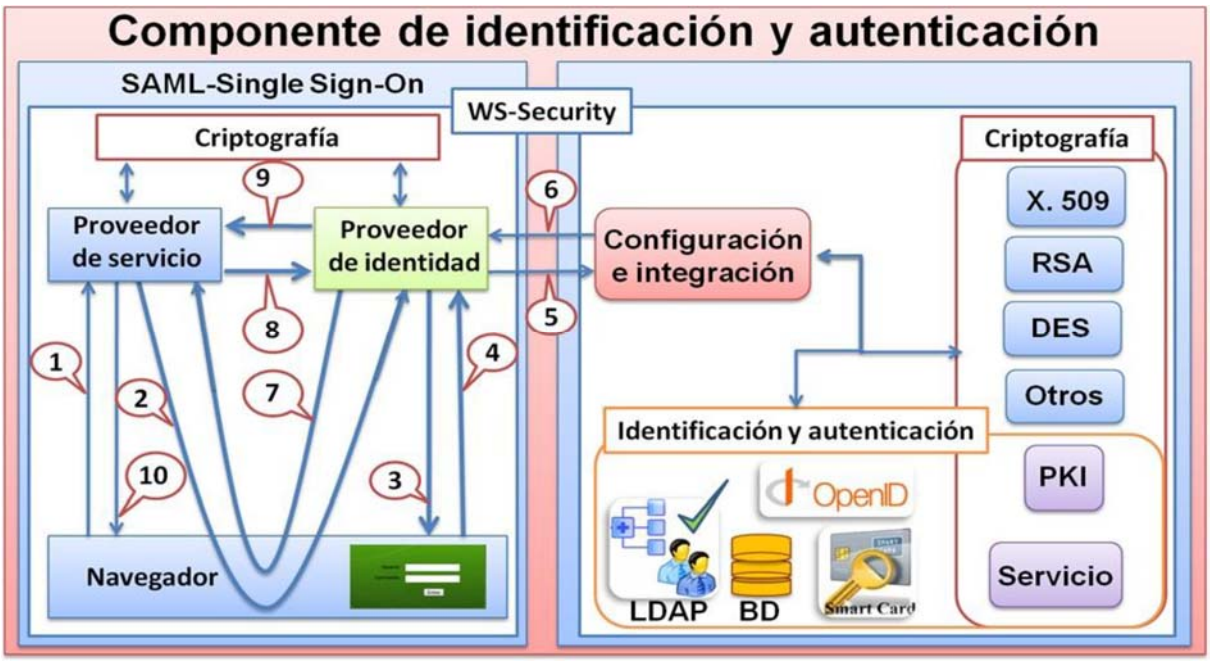

Figura 7. Escenario de autenticación utilizando SAML utilizando SSO.

En un entorno SSO como el que se desea garantizar, el flujo de comunicación varía con respecto a los escenarios anteriores, como se refleja en la7. El SSO se gestiona por el PI. A continuación se describen los pasos que sigue la solución propuesta para garantizar una autenticación de usuarios segura, escalable y eficiente en entornos SSO.

1. El proceso de autenticación se inicia cuando el usuario intenta acceder a una aplicación, objeto o acción por medio de un navegador web.
2. La aplicación recibe la petición e instancia a su PS.
3. El PS recibe la petición de la aplicación con los parámetros que la identifica e inicia las verificaciones pertinentes para conceder el acceso. El PS tiene la responsabilidad verifica la valides de la sesión del usuario utilizando las credenciales suministradas. En caso que el usuario no tenga creada una sesión o no esté activa producto al tiempo de expiración, veracidad del certificado o token de seguridad, entre otros aspectos que condicionan su valides, el proveedor de servicios estructura los datos, aplica el método de cifrado y firma digital establecido y redirecciona la petición con los parámetros descritos en el estándar al PI.
4. El PI recibe la petición del PS con los parámetros que especifica el estándar en la comunicación SAML y utilizando el método de cifrado y firma digital establecido,

verifica la relación de confianza en la comunicación SAML para el PS que hizo la solicitud.

4.1. Si la verificación del paso anterior es positiva, el PI utilizando el identificador de la aplicación enviada en los parámetros desde el PS, chequea si existe una sesión activa para el navegador utilizado por el usuario para acceder a la aplicación.

4.1.1. En caso positivo se verifica que la fuente de datos predeterminada para la aplicación, coincide con la fuente de datos activa en la sesión existente.

4.1.1.1. En caso de que no coincidan o no exista una sesión activa para el navegador, se le muestra al usuario la ventana de autenticación.

4.1.1.2. Si las fuentes de daos coinciden, PI obtiene el certificado o token de seguridad y demás datos almacenado en la sesión activa, aplica el método de cifrado y firma digital y reenvía al PS la respuesta con estos datos.

5. El usuario introduce las credenciales que serán verificadas en la fuente de autenticación.
6. El PI recibe las credenciales del usuario y consume el servicio de autenticación mediante el protocolo establecido, enviando las credenciales del usuario, identificador de la aplicación que desea acceder y demás parámetros especificados en el contrato del servicio.
7. SIGIS recibe las credenciales tanto del usuario como de la aplicación y procede a realizar las verificaciones pertinentes. El identificador de la aplicación, aparte de garantizar la autenticidad de la petición, se utiliza para identificar la fuente de autenticación a utilizar en la verificación de las credenciales del usuario. Las fuentes de autenticación (LDAP, OpenLDAP, base de datos de SIGIS) se configuran con anterioridad y se asignan a nivel de aplicación o de usuario. Concluido el proceso de selección de la fuente de autenticación, SIGIS interactúa con la base de datos o directorio activo para validar las credenciales del usuario.
8. SIGIS analiza el resultado de la verificación:

8.1. En caso positivo crea un certificado o token de seguridad para identificar el usuario, lo almacena para procesos de verificación posteriores y se lo envía a la aplicación.

8.2. En caso negativo no crea el certificado o token de seguridad y retorna el mensaje de error a la aplicación.

9. El PI recibe y analiza la respuesta enviada por SIGIS:
   9.1. En caso de ser negativa la respuesta de SIGIS, muestra un error y la ventana de autenticación para iniciar nuevamente el proceso desde el paso 5.
   9.2. En caso de ser positiva verifica si ya existe una sesión activa y la elimina para crear una nueva sesión con el nuevo certificado.
   9.3. Si no existe una sesión previa, la crea con el nuevo certificado.
10. El PI envía una respuesta SAML al PS con el certificado y otros datos especificados en el contrato.
11. Este paso (opcional) se ejecuta si se utiliza un método inseguro de comunicación o no se emplea ningún método de cifrado y firma digital que garantice la seguridad en la comunicación, enviando los datos recibidos y el identificador de la petición mediante el protocolo de comunicación establecido.
12. El PI obtiene los datos, los verifica y envía la respuesta al PS para que:
    12.1. En caso de ser positiva la respuesta ejecute el paso 13.
    12.2. En caso de ser negativa ejecute el paso 3.
13. El PS obtiene el certificado y otros datos pertenecientes al usuario y se los envía a la aplicación para que inicie el proceso de autorización.

Los escenarios descritos permiten implementar soluciones de autenticación desde la más simple hasta la más compleja. Lógicamente el control de acceso no garantiza la seguridad de la información si se implementa solo este proceso. Es necesario incorporar al modelo los procesos de autorización y el de auditoría para garantizar un control estricto en el acceso a los datos. La autenticación de los usuarios constituye el eslabón inicial del control de acceso y tiene la responsabilidad de gestionar las sesiones de usuarios, las mismas contienen los datos (certificado, perfiles, entre otros) que los van a identificar a lo largo de todo el proceso. Cuando el usuario solicite acceder a un recurso lo primero que se verifica es la autenticidad del certificado antes de otorgar el acceso.

CASO DE ESTUDIO

En esta Sección se muestra un caso de estudio, donde se aplica la extensión realizada al estándar SAML en el desarrollo de la próxima versión del Sistema de Gestión Integral de Seguridad (ACAXIA).

Se describirá paso a paso el caso de estudio para una mejor comprensión.

1. Se agrega un servidor de autenticación en el módulo de configuración mencionado en la sección anterior (para este caso de estudio en concreto se usa el LDAP).

Figura 8. Ventana para adicionar servidor de autenticación.

2. Luego se agrega el recurso (entiéndase por recurso, aplicaciones, subsistemas, etc.).

Figura 9. Ventana para adicionar el recurso.

3. El cliente trata de acceder al recurso y este lo redirecciona al Proveedor de Identidad enviándole su identidad. Si no existe una sesión para el recurso el Proveedor de Identidad muestra la ventana de autenticación.

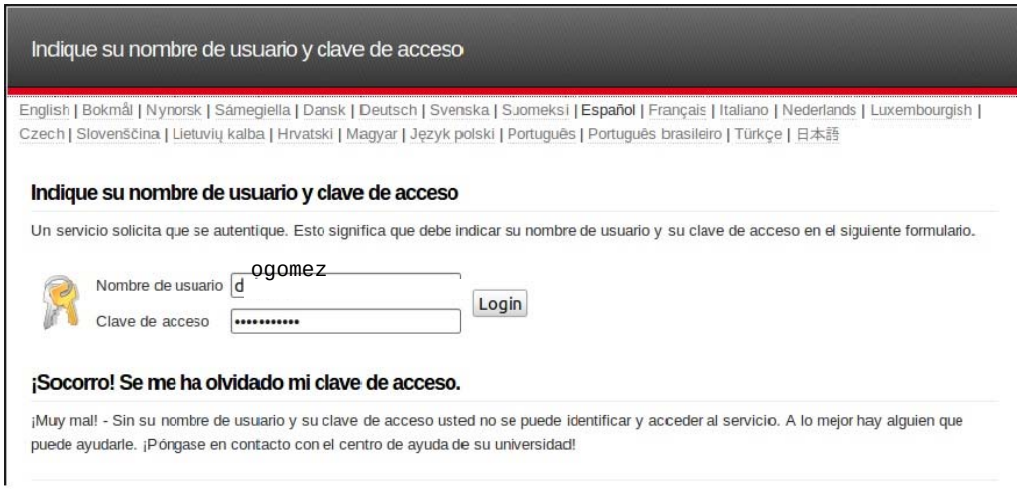

Figura 10. Ventana de autenticación del Proveedor de Identidad.

Luego que el usuario intercambia credenciales con el Proveedor de Identidad, este con la identidad del recurso gestiona la fuente de autenticación y autentica al usuario, si son correctas las credenciales permite el acceso al recurso.

Figura 11. Recurso.

CONCLUSIONES

Single Sign-On se presenta como una estrategia de seguridad, la cual puede prestar diversos beneficios dentro del contexto del grupo de desarrollo como: incrementar el contexto de seguridad y proveer un inicio de sesión único a través de todas las aplicaciones. A lo largo del artículo se presenta de manera general el concepto de SSO, beneficios y ventajas en cuanto a seguridad se refiere. Se describe la tecnología SAML y cómo esta ayuda a la fácil implementación del proceso de autenticación del modelo propuesto, sin considerar sistemas y arquitecturas complejas, usando o no Servicios Web para la comunicación entre entidades.

La propuesta presentada fue probada en un entorno de varias aplicaciones, en el que un usuario tenía acceso a varias de ellas. Además se está utilizando por la dirección técnica para centralizar la autenticación de todas las herramientas que componen un sistema ERP.

REFERENCIAS BIBLIOGRÁFICAS

de Haro, C.J. and Jordan, F.F., Prototipo de framework documental para firma electrónica: cliente. UPC, 2007.

Frías, J.A., El Control de Autoridades y el Acceso a la Información. Bibliología, 2008.

D. Recordon, S.A., M. Jones, Microsoft, J. Bufu, Ed. Independent, J. Daugherty, JanRain, N. Sakimura, and NRI, OpenID Provider Authentication Policy Extension 1.0. Imagic, 2008.

López, J.E.G.M., Organero Pedro Luis, Confianza, seguridad y privacidad en la Internet del siglo XXI a través de las tecnologías de gestión de la identidad: Una aproximación integral. 2008.

Barrera, R.N., Modelo de Single Sign-On para Herramientas del Grupo QualDev. Paradigma, 2008.

Milián, V., Seguridad en Asp.Net: Autenticación y Autorización. ASP.net, 2010.

Forsberg, D., Secure Distributed AAA with Domain and User Reputation. IEEE, 2007.

López, G.G., Antonio F.; Marín, Rafael; Cánovas, Oscar A Network Access Control Approach based on the AAA Architecture and Authorization Attributes. IEEE, 2005.

Satizábal, E.I.C., Contribución a la validación de certificados en arquitecturas de Autenticación y Autorización. TDX, 2007.

Madsen, P.N.M., Eve; Sun Microsystems, SAML V2.0 Executive Overview. 2010.

OASIS, S.S.T., Security Assertion Markup Language (SAML) V2.0 Technical Overview. OACIS, 2008.

MorgesonII, F.V., Van Amburg, D., and Mithas, S., Misplaced Trust? Exploring the Structure of the E-Government-Citizen Trust Relationship. TERPConect, 2010.

FFIEC, F.F.I.E.C., Authentication in an Internet Banking Environment. FFIEC, 2005.