Esquema de Seguridad en SOAP Basado en OpenSAML
SOAP Security Scheme Based on OpenSAML

Isabel Del C. Leguías Ayala
Universidad Tecnológica de Panamá
Facultad de Ingeniería de Sistemas Computacionales
isabel.leguias@utp.ac.pa

RESUMEN
SOAP es un protocolo de comunicación basado en XML para el intercambio de información entre aplicaciones en un entorno distribuido. SOAP no cuenta con mecanismos propios de seguridad para la transmisión segura de sus mensajes. De manera que no cifra la información y está viaja en claro por la red. Para suplir esta carencia, SOAP hace uso del estándar WS-Security implementando el XMLSignature y XMLEncryptation para garantizar la confiabilidad (cifrado) e integridad (firma) de los mensajes en los servicios Web. En este artículo se presenta un esquema de seguridad para servicios Web basado en OpenSAML que garantiza la transmisión segura de los mensajes SOAP.

ABSTRACT
SOAP is communication protocol base on XML to Exchange information between applications in a distributed environment. SOAP does not have its own security mechanisms for secure transmission of you message. So it does not encrypt the data and is traveling in the clear over the network. To fill this gap, SOAP makes use of the WS-Security and implementing the XMLSignature, XMLEncryptation to ensure reliability (encryption) and integrity(signature) of messages in Web services. This article presents a SOAP Security Scheme for Web services based on OpenSAML ensuring the secure transmission of SOAP messages.

Categories and Subject Descriptors
D.4.6.[Security and Protections(K.6.5)]:Access Control, Authentication, Verification

General Terms
Web Security, Implementaion

Keywords
XML signature, XML encryption, WS-Security, seguridad Web, SOAP message, OpenSAML

Palabras Clave
XML signature, XML encryption, WS-Security, seguridad Web, SOAP message, OpenSAML.

1. INTRODUCCION
El rápido desarrollo del comercio electrónico en los últimos años, ha propiciado el desarrollo de plataformas, totalmente nuevas basadas en el intercambio de información a través de servicios Web.

Los servicios Web como una tecnología emergente de información basada en Internet, permiten a los usuarios remotos obtener información remota desde diversos lugares, por medio de los protocolos TCP/IP. También hacen uso de XML para la comunicación a nivel de aplicación. Sin embargo, la seguridad en la comunicación es la base para que el servicio Web pueda ser ampliamente utilizado en Internet. Otro problema es la cantidad de aplicaciones web desarrolladas, donde los usuarios necesitan recordar sus diferentes contraseñas para poder autenticarse. Es por ello que se hace necesario el desarrollo de entornos de recuperación de firmas y contraseñas de manera transparente al usuario.

Los servicios Web son un excelente medio para ofrecer servicios de comercio electrónico, bibliotecas digitales, seguimiento de mensajería, etc., que los hace atractivos para un atacante que, en el caso de detectar sus vulnerabilidades, podrá obtener acceso a las aplicaciones de programación y de base de datos que manejan toda la información relacionada con el servicio Web.

Actualmente hay un crecimiento en las especificaciones de estándares, especialmente en el área de seguridad web. Los aspectos de funcionalidad y ejecución de estos estándares se han hecho gracias a las investigaciones en los servicios Web.

Existe un número considerable de implementaciones de SOAP, servicios de seguridad XML y SAML [1] [2].

La problemática que presenta SOAP es que no tiene una norma de confianza para sus mensajes, ya que la seguridad es proporcionada por HTTPS, el cual no puede brindar los requerimientos de seguridad dado que los mensajes SOAP son cada vez más complejos, el mismo no cuenta con mecanismos propios para la transmisión segura de los mensajes. El escenario propuesto es utilizar mensajes SOAP, integrando el estándar SAML a través de las librerías de OpenSAML. Con este esquema se busca proteger la integridad del mensaje e incluir mecanismos de autenticación, autorización, y confidencialidad para el mismo.

En este artículo se presenta un esquema de seguridad para servicios Web que garantiza la transmisión segura de mensajes SOAP basándose en OpenSAML. Además, dada la transferencia, se hace necesario proteger la integridad de los datos, brindar mecanismos de autenticación, autorización y, de confidencialidad. En la sección 2, se discute la estructura de estándar SOAP, las vulnerabilidades y ataques. En la sección 3, las implementaciones de seguridad que sobre el estándar SOAP tratan de ofrecer robustez en el intercambio de los mensajes (SOAP message). Seguidamente, se aborda la integración de cada una de las especificaciones SAML, que es la base de implementación de OpenSAML, en SOAP. En la sección 4, la discusión y finalmente la sección 5, se presentan las conclusiones.

2. PROTOCOLO SOAP
El Protocolo Simple de Acceso a Objetos (SOAP) [3-5] es un protocolo ligero para intercambiar información entre entornos descentralizados, distribuidos. Es un protocolo basado en XML

que permite la interacción entre varios dispositivos y tiene la capacidad de transmitir información compleja. Los mensajes son independientes del sistema operativo y los protocolos, se pueden transportar utilizando varios protocolos de Internet, como por ejemplo HTTP y SMTP. Mensaje SOAP está formado por un sobre (*envelope*) es el elemento principal del mensaje y su estructura está compuesta por los siguientes elementos: cabecera (*header*) y cuerpo (*body*). Figura 1.

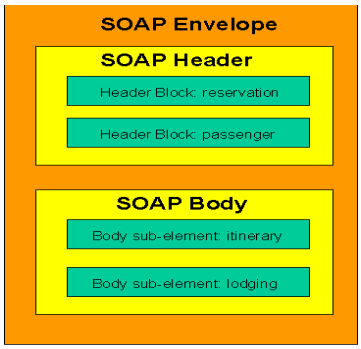

Figura 1 [5] Estructura del mensaje SOAP

Sobre [4] es el contenedor del mensaje SOAP. La cabecera es el elemento principal del sobre, se trata un mecanismo de extensión que incorpora información extra en el mensaje SOAP (como seguridad, transacciones, etc.). Además incluye varios bloques de cabecera, que es una forma para agrupar la información. El cuerpo especifica una solicitud para efectuar alguna operación, un resultado o error. El elemento Fault que se encuentra dentro del cuerpo que indica un error en el procesamiento del mensaje SOAP, y está formado de cinco sub-elementos: code, reason, detail, node (opcional) y role (opcional). La versión actual de SOAP es la 1.2 y consiste de:

- Un sobre que define un marco para describir lo que está en el mensaje y cómo procesarlo.
- Un transporte. Obligatorio para el intercambio de mensajes utilizando protocolos subyacentes.
- Una conjunto de reglas de codificación para expresar instancias de tipos de datos definidos en la aplicación.
- Una convención para representar llamadas a procedimientos remotos y respuestas.

Un mensaje SOAP [6] fundamentalmente es una vía de transmisión de información desde un emisor a un receptor. El mensaje puede pasar a través de varios intermediarios que, a su vez, pueden tratar el mensaje. El conjunto de intermediarios por donde viaja el mensaje se conoce como ruta del mensaje. Todos los usuarios que intervienen en la ruta por la que viaja el mensaje se conocen como actores. SOAP especifica un mecanismo para identificar qué partes del mensaje SOAP están destinadas a la transformación de los actores específicos en la ruta del mensaje. Este mecanismo se conoce como "orientación" y sólo se puede utilizar en relación con los bloques de encabezado, y cuerpo del sobre SOAP, no puede ser explícitamente dirigido a un nodo concreto. El valor del atributo actor es el identificador único de la mediación como objetivo. Los intermediarios que no coinciden con el atributo actor deben ignorar el bloque de cabecera. Además, la construcción de un camino de mensajes (la definición de los nodos por los que pasa un mensaje) no está cubierto por la especificación SOAP. Se dan varias extensiones de SOAP, WS-Routing que han surgido para llenar ese vacío. En el caso de WS-Routing, se define un estándar de encabezado de bloque SOAP para expresar la información de enrutamiento. Su función es definir la secuencia exacta de los intermediarios a través de los cuales pasar un mensaje.

2.1.Ventajas de los mensajes SOAP

1. Las extensiones SOAP [7-8] solo pueden ser definidas en términos de un modelo de datos y procesamiento, ya definidos en SOAP 1.2.
2. Las aplicaciones pueden aprovechar el conjunto de tecnologías disponibles para el procesamiento XML.
3. La descripción de interfaz puede proporcionar un modelo sencillo y coherente para los desarrolladores y herramientas.
4. La interfaz de programación expone un modelo sencillo de programación para el programador.
5. Es un modelo de computación distribuida de objetos que es independiente de las plataformas.
6. Implementa una serie de mecanismos para serializar tipos complejos con elementos simples en su interior.

El protocolo SOAP ha sido adoptado por W3C y otras empresas como, por ejemplo: SUN Microsystems.

2.2. Vulnerabilidades en SOAP

Debido a que SOAP está basado en XML, es vulnerable a una gran cantidad de ataques orientados al mismo [9]. Además también presenta vulnerabilidades a los ataques asociados con su protocolo de capa de aplicación, con mayor frecuencia HTTP. Como SOAP es utilizado para servicios Web sus vulnerabilidades se clasifican de la siguiente forma:

2.2.1 Vulnerabilidades estructurales

Son aquellas que derivan de la intervención en las líneas de comunicación de los participantes (usuarios, equipos intermedios, servidor) que intercambian mensajes SOAP. Dan lugar a los siguientes ataques: Interceptación de mensajes, Man-in-the-middle, Spoofing, Repetición de mensajes, Denegación de Servicio.

2.2.2 Vulnerabilidades semánticas

Son aquellas que se derivan de las debilidades en la codificación y procesamiento de los mensajes SOAP. Proporciona un modo abierto y extensible para que las aplicaciones se comuniquen a través de la Web usando mensajes. Estos se clasifican de la siguiente manera: Dan lugar a los siguientes ataques: Entradas inválidas, Control de acceso débil, Autenticación y manejo de sesión débiles, Cross Site Scripting, Buffer Overflows, Injection Flaws, Manejo inapropiado de errores, Contenido Malicioso, Denegación de servicio.

2.3. Ataques en SOAP

Según [10] un ataque a un servicio Web se clasifica, de acuerdo con el grupo de vulnerabilidades especificas que explota: Interface de servicios Web (WSDL), Pruebas de ataques (XWS1), Ataque de análisis de Fuerza Bruta XML (XWS2), Ataque de contenido Malicioso(XWS3), Ataque de referencia externa (XWS4), Ataque de Protocolo SOAP/XML (XWS5), Manipulación de Credenciales de Seguridad (XWS6), Manipulación de negociación de clave/sesión segura (XWS7).

La seguridad frente a ataques de grupos que interactúan con Grid y servicios Web está basada en proyectos realizados por

European Grid y, muy particularmente, en EGEE y GridPP donde se identifica las siguientes amenazas/ataques:

- Ataque de Credenciales de Usuarios (UCA): Este tipo de ataque está basado en el robo de credenciales de usuarios o la obtención de la mismas como consecuencia de que el sistema este comprometido.
- Ataques de Inteligencia "Wire" (WIA): Incluyen una amplia gama de ataques que puede suceder si a nivel de los servicios de comunicaciones no se está lo suficientemente protegidos contra los sniffer.
- Ataques Malifactor iniciado (MIA): Este tipo de ataque es realizado por atacantes potenciales utilizando los servicios Web tradicionales. Se incluyen aquí los que emplean técnicas específicas, sondeo WSDL, contenido malicioso XML, ataque de fuerza bruta y de diccionario.
- Ataques de Administración de Sitio (SMA): Estos ataques pueden ser causados por configuración incorrecta.
- Ataques de Servicio Final (ESA): Este tipo de ataques utilizan diferentes técnicas para construir contenidos de entrada maliciosos. Un ejemplo sería el de la inyección XML/SQL.

2.4. Seguridad en Mensajes SOAP

SOAP [11-12] aún no tiene una norma de confianza para sus mensajes y [13] no cuenta con mecanismos propios de seguridad para la trasmisión segura de los mensajes. En muchos casos la seguridad es proporcionada por el protocolo que le sirve de transporte, típicamente HTTPS, pero este tipo de soluciones está dejando de ser válido poco a poco fundamentalmente porque el grado de complejidad de los mensajes SOAP y de los requisitos de seguridad demandados son cada vez más elevados. SOAP utiliza los protocolos tradicionales de seguridad como SSL, TLS y HTTPS que cifran los mensajes transferidos entre dos puntos, estos protocolos no brindan seguridad de extremo a extremo a nivel del mensaje. Como resultado, OASIS desarrollo Web Services Security (WSS) para proporcionar protección a nivel de mensajes entre dos extremos (clientes y servicios Web) garantizando la integridad, confidencialidad y autenticación del mensaje.

WS-Security [14], tiene como uno de sus objetivos el permitir que las aplicaciones construyan intercambios seguros de mensajes SOAP. Otro objetivo es el garantizar la seguridad a nivel del mensaje de extremo a extremo. WS-Policy define un modelo genérico y una sintaxis para describir y comunicar las políticas de seguridad de los servicios Web. WS-Trust define extensiones que se construyen sobre WS-Security y amplían las capacidades de los mecanismos de seguridad definido por el mismo, permitiendo la solicitud, emisión e intercambio de tokens de seguridad y la gestión de las relaciones de confianza.
El estándar de seguridad WEB Service Security involucra la utilización de XML Signature para hacer la prueba de autenticación del origen e integridad al contenido XML del mensaje (permitiendo firmar tanto el mensaje SOAP completo como una parte de él). XML Signature es un estándar de W3C que permite autenticar al remitente y asegurar la integridad del documento transportado. A través de la firma digital nos permite ofrecer garantías de autenticidad de los datos, la identificación de la identidad del emisor del mensaje, la validación de autenticidad e integridad del mensaje, y la propiedad de no repudio en los mensajes. La estructura de XML Signature se muestra en la figura 2.

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod>
    <SignatureMethod>
            <Reference (URI) >
            <Transforms >
            <DigestMethod >
            <(DigestValue >
            </Reference>
  </SignedInfo>
<SignatureValue>
<KeyInfo />
<Object />
</Signature>
```

Figura 2 [15] Estructura del XML Signature

XML Encryption es un estándar de W3C que describe cómo utilizar XML para representar recursos de forma digital y codificada. XML Encryption admite el cifrado usando distintos algoritmos de cifrado, tanto simétrico como asimétrico. La estructura del XML Encryption se muestra en la figura 3.

```
<EncryptedDat>
  <EncryptionMethod/>
  <ds:KeyInfo>
    <ds:KeyName>
    <ds:RetrievalMethod>
    <ds:"">
   <EncryptedKey>
     <AgreementMethod>
 </ds:KeyInfo>
 <CipherData>
   <CipherValue>
   <CipherReference (URI)>
 </CipherData>
<EncryptionProperties>
</EncryptedData>
```

Figura 3 [15] Estructura de XML Encryption

SAML (*Segurity Assertion Markup Language*)[16], desarrollado por OASIS, es un marco de trabajo basado en XML para representar información de autenticación, derechos y atributos de usuarios. Además, permite a las organizaciones hacer afirmaciones a cerca de la identidad, atributos y autorización de un usuario a otras entidades, por ejemplo otra organización asociada u otra aplicación o proceso. SAML es un lenguaje extensible y flexible, diseñado para ser utilizado por otros estándares, y empleado en otros estándares y proyectos como, por ejemplo, The Liberty Alliance o el proyecto Shibboleth de Internet2. Las ventajas de SAML son: independencia de la plataforma, acoplamiento débil de los directorios, mejora del servicio con relación al usuario final, reducción de los costes administrativos de los proveedores de servicios y transferencia del riesgo.

SAML [17] está formado por los siguientes componentes:

- Assertion. Un Assertion es un documento producido por una autoridad SAML que puede incluir datos a partir de un acto

de autenticación, información de atributos de una entidad o información sobre decisiones de autorización acerca de un recurso. Además, está formado por tres sentencias o declaraciones: declaraciones de autenticación, de atributos y sobre decisiones de autorización. El Assertion [15] está formado por los siguientes elementos : Conditions (describe la fecha de expiración de assertion), AutenticationStatement (contiene los atributos del método de autenticación, instancia y el elemento asunto) y Signature (es la firma de la autoridad assertion).

- Protocolos de petición y respuesta. Regulan la forma en que se llevan a cabo las actividades de petición y respuesta SAML. Forman parte de este grupo el Protocolo de solicitud de autenticación, el Protocolo de cierre de sesión individual, las afirmaciones de consulta y solicitud de protocolos, el Protocolo de administración de identificador de nombres y el Protocolo de asignación de identificador de nombres.
- Binding. Expresa la manera exacta en que los mensajes SAML se transportan mediante su inclusión en otros protocolos de comunicación para la consecución del protocolo de petición y respuesta. SAML versión 2.0 define los siguientes mecanismos de binding: HTTP Redirect Binding, HTTP POST Binding, HTTP Artifact Binding, SAML SOAP Binding, Reverse SOAP (PAOS).
- Perfiles. Definen la forma en que los mensajes SAML se pueden transferir a través de sistemas de comunicación. El perfil de SOAP para SAML dicta cómo insertar los mensajes SAML en SOAP, cómo afectan los encabezados y cómo debe comportarse SOAP en caso de llegar a un estado de error. Los perfiles definidos en la versión 2 de SAML son: Web Browser SSO, Enhanced Client and Proxy, Identity Provider Discovery Profile, Single Logout Profile, Assertion Query/Request Profile, Artifact Resolution Profile, Name Identifer Management Profile y Name Identifier Mapping Profile.

SAML assertions [16] puede ser utilizado con mensajes SOAP para proporcionar seguridad e integridad de información entre los actores de servicios Web. El SAML Token Profile establecido por OASIS Web Services Security (WSS), especifica como SAML assertions puede ser utilizado con el marco WS_Security El estándar de Liberty Alliance Identity Web Service Framework (ID-WSF) [16] está basado en estas especificaciones para utilizar SAML assertion y brindar seguridad y privacidad de acceso a servicios Web. En la figura 4 se muestra la estructura del SAML.

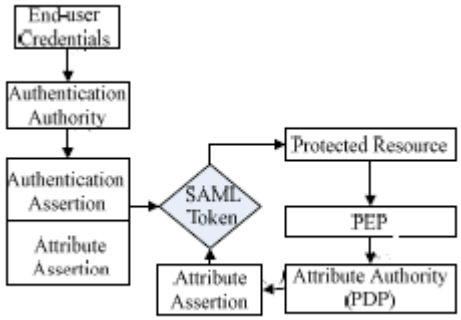

Figura 4 [18] Estructura del SAML

Existen muchas aplicaciones[19] en el mercado que hacen uso del SAML v1.1 o v2.0. También existen aplicaciones de código abierto que lo utilizan, como por ejemplo OpenSAML, un conjunto de herramientas de código abierto para apoyar a los desarrolladores que trabajan con SAML. Es el caso de Shibboleth que utiliza OpenSAML en sus desarrollos. Sun Microsystems tiene un producto llamado OpenSSO que es una versión de código abierto de su versión comercial. Independientemente del producto seleccionado, siempre y cuando cumpla con las normas de SAML, todos los productos se pueden intercambiar sin ningún problema de compatibilidad.

3. IMPLEMENTACION

OpenSAML [20] [21] es un conjunto de librerías Java y C++ de código abierto que se utiliza para construir, transportar y analizar mensajes SAML. Es capaz de almacenar de forma individual los campos de información que componen un mensaje SAML y construir de manera correcta su representación XML, así como también realizar el proceso contrario, descomprimir un documento XML en sus elementos individuales para entregarlos a un destinatario.

También permite utilizar SOAP Binding para el intercambio de peticiones y respuestas SAML. Además, da soporte adicional en la implementación de sistemas Web que emplean single sing-on mediante perfiles SAML que impliquen el uso de un browser, redirecciones y mensajes POST.

OpenSAML es extensible e integra una amplia gama de "modelos de confianza" y requisitos de seguridad, aunque por el momento se está orientado a transacciones protegidas mediante PKI y TLS/SSL [22] . Fue creado por Scott Cantor de la universidad Ohio State, y es el componente principal de Shibboleth, es un software libremente modificable y distribuible, probado con éxito en Windows XP/200, Red Hat Linux y Solaris. OpenSAML sirven para autenticar usuarios que intentan acceder un servicio Web, autenticación, autorización entre partes. Proporciona servicios de confianza en el intercambio de datos.

Figura 5 Modelo de Seguridad SOAP

Por lo tanto, nuestra propuesta es integrar la seguridad en la estructura del SOAP, haciendo uso del estándar SAML y demostrar su viabilidad mediante la implementación haciendo uso de OPENSAML[20][22]. Con este esquema se busca proteger la integridad del mensaje e, incluir mecanismos de autenticación, autorización, y confidencialidad para el mismo.

4. DISCUSIÓN

El problema que presenta SOAP es caracterizado por no contar con norma de confianza para sus transferencias de mensajes. Además la escasa seguridad que puede ofrecer el HTTPS para con el entorno SOAP. De igual manera estos escasos requerimientos de confianza generan inconsistencias en la interpretación del mensaje y su contenido.

Los objetivos propuestos para un esquema de seguridad en SOAP basado en OpenSAML son los siguientes:

- Estudiar la estructura del estándar SOAP, identificando sus características y componentes.
- Estudiar la estructura del estándar SAML, características, componentes, uso y aplicación.
- Integrar las librerías apropiadas para la seguridad del SOAP, de tal manera que brinde confiabilidad, autenticidad e integridad del mensaje.
- Implementar SOAP basado en OpenSAML para determinar su funcionalidad y reglas utilizadas través de un servicio web.
- Elaborar un portal web con la estructura SOAP.
- Realizar las pruebas necesarias del mensaje SOAP por medio de un portal Grid.
- Presentar resultados sobre el esquema de seguridad SOAP basado en OpenSAML

Los objetivos expresados anteriormente, se implementaran a través de un esquema innovador de seguridad como parte de la estructura de SOAP, haciendo uso de la estructura del SAML un lenguaje extensible y flexible que es utilizado por otros estándares. Se hará uso de OpenSAML. Con las características del OpenSAML se busca proteger la integridad del paso de mensaje entre nodos Grid, el proceso de cálculo en los nodos del Grid. De igual forma, incluir mecanismos de autenticación y autorización, al igual que la confidencialidad de los procesos activos en los nodos Grid.

El conjunto de acciones de seguridad del esquema que desarrollamos, se implementará sobre la infraestructura del Grid experimental de la Universidad Tecnológica de Panamá, como parte de las estrategias de adecuación científica sobre el Grid experimental, y la conformación de una infraestructura virtual para el cálculo y la computación científica.

Además, la metodología empleada hasta el momento es la de Revisión Sistemática para seguridad en SOAP y estándar SAML para Tecnología Grid.

En esta primera fase de investigación el esquema de seguridad que sobre SOAP se desarrolla propone garantizar la privacidad e integridad al momento que los usuarios accedan a los recursos y servicios del portal Grid de la infraestructura virtual.

5. CONCLUSIONES

El diseño de un esquema de seguridad de servicio Web busca garantizar la seguridad en la transmisión del mensaje SOAP y la operatividad total de los servicios Grid, implementando la autenticación de identidad, autorización, el control de acceso, y la integridad, a través del uso de OpenSAML. Además, es flexible, escalable, con características de diversos estándares basados en XML, de fácil mantenimiento, y sobre todo, dispuestos a brindar seguridad en los servicios Web. Se hará la integración del estándar SAML en SOAP, el cual brindara un esquema innovador de seguridad, de tal manera de proporcionar servicios de confianza en el intercambio de datos, implementado sobre la infraestructura Grid.

REFERENCIAS

[1] L. Y. Liu Wan-Jun, "Research and Implementation Based on Web Security Model," *2010 International Conference on Innovative Computing and Comunication and 2010 Asia-Pacific Conference on Information Tecnology and Ocean Enginering*, p. 4, 2010.

[2] M. I. Knap Tomas, "Towards More Secure Web Services," pp. 1-10.

[3] "SOAP Version 1.2 W3C working Draff."

[4] "Simple Object Access Protocol (SOAP)1.1".

[5] "SOAP Version 1.2 Part 0: Primer (Second Edition),W3C Recommendation 27 April 2007."

[6] Z. H. Liu Yong , Li Yaowei "Research on |Service Transmission of SOAP Message," pp. 771-776, 2008.

[7] D. B. Adam Bosworth, Martin Gudgin, Mark Nottingham, David Orchard, JeffreySchlimmer, "XML, SOAP and Binary Data," *White paper Version 1.0*, February 24 2003.

[8] A. B. R. Walled Ghossoon M., "Security Protection using Simple Object Protocol (SOAP) Message Techniques," *International Conference on Electronic Design*, pp. 1-6, 2008.

[9] A. R. Lowis Lutz, "On a Classification Approach for SOA Vulnerabilities," *IEEE COMPSAC Workshop Security Aspects of Process and Services Engineering, IEEE, 2009.*, p. 6, 2009.

[10] L. G. Demchenko Yuri , de Laat Cees , Oudenaarde Bas "Web Services and Grid Security Vulnerabilities and Threats Analysis and Model," 2005.

[11] Z. H. Liu Yong, Li Yaowei, "Reserch on Secure Transmission of SOAP Messages."

[12] H. Z. J. L. Jian Jin, Hualin Qian, ""Analysis of Web Services Security" Micro-electronics and Computer," vol. 21, pp. 19-24, 2004.

[13] Y. B. Youxiang Duan, Lijiang Pan, "A Secure Web Services Model Based on the Combination of SOAP Registration Info and Token Proxy," *International Symposium on Computer Science and Computational Technology*, pp. 15-20, 2008.

[14] W. T. Singhal Anopp, Scarfone Karen, "Guide to Secure Web Service. Recommendations of the National Institute of Standards and Technology Computer Security," pp. 1-128, August 2007 2007.

[15] B. Y. Yu Xin, "A Method for Accessing Trusted Services Based on Service-Oriented Architecture," *2009 Fifth International Conference on Information Assurance and Security*, pp. 685-688, 2009.

[16] "SAML v2.0 Executive Overview," p. 7, 12 April 2005 2005.

[17] "Security Assertion Makup Language (SAML) V2,0 Technical Overview," p. 51, 25 march 2008.

[18] Z. Shang Chaowang Yang, Liu Qingtang , Zhao Chengling "SAML Based Unified Access Control Model for Inter-Platform Educational Resources," *International Conference on Computer Science and Software Engineering*, pp. 909-912, 2008.

[19] L. J. E. Lewis Kelly D. , "Web Single Sign-On Authentication using SAML," *IJCSI International Journal of Computer Science Issues*, vol. Vol. 2, p. 8, 2009.

[20]"Home OpenSAML Internet 2 https://spaces.internet2.edu/display/OpenSAML/Home/ 20.04.2010."

[21] D. S. F. J. De Mello Emerson Ribeiro, "Mediation of Trust across Web Service," *International Conference on Web Service*, pp. 1-8, 2005.

[22] S. Rieger, "User-centric Identity Management in heterogeneous Federations," *2009 Fourth International Conference on Internet and Web Applications and Services*, pp. 527-532, 2009.