Seguridad en servicios web: como garantia de control en la interoperabilidad de la información geográfica

Luis Fernando Ortiz[1], Néstor Fabio Roldán Torres[2]

Resumen

El Instituto Geográfico Agustín Codazzi (IGAC), es la entidad responsable de producir la cartografía oficial de la República de Colombia. Su Centro de Investigación y Desarrollo en Información Geográfica (CIAF) tiene como misión investigar, apropiar y transferir tecnologías para la gestión de la información geográfica y de las Infraestructuras de Datos Espaciales, mediante el uso de la Percepción Remota, Sistemas de Información Geográfica y herramientas afines, para apoyar el fortalecimiento institucional, así como el desarrollo sostenible del país y de la región.

Esta oficina tiene más de 40 años de experiencia en cuanto a la transferencia de conocimiento, al capacitar profesionales de diversas nacionalidades a través de estrategias y mecanismos pedagógicos impartidos de manera presencial, con personal docente altamente especializado, y con el fin de transferir conocimiento y educación de alta calidad.

En este sentido, desde 2008, el Grupo Geoservicios puso en funcionamiento una serie de herramientas web bajo la filosofía del software libre, que promueven una manera de trabajar en el campo de la investigación, la educación y la difusión en torno a la información geográfica, y que están basadas en un espíritu participativo y abierto. Dichas herramientas se encuentran implementadas en una serie de servicios web y aplicaciones (en el caso del componente geográfico), que en años anteriores se desarrollaron con gran éxito, sobre todo en materia de hacer dicha información interoperable con las distintas instituciones que integran la Infraestructura Colombiana de Datos Espaciales (ICDE).

Las diferentes tecnologías y herramientas utilizadas por el grupo parten de una filosofía orientada a servicios web. A pesar de promover el uso de las herramientas de software libre para el manejo de información geográfica, el grupo también cuenta con conocimientos en herramientas propietarias SIG, como todo el paquete tecnológico de ArcGis.

Sin embargo, y dado el creciente interés de las instituciones de proteger la información que entregan al ciudadano mediante servicios web, se debe pensar en estrategias que garanticen que esta información llegue a quien corresponde. Por lo anterior, el presente artículo abordará el proceso de la implementación de seguridad para los servicios web del nodo IGAC de la ICDE, acompañado de todas las licencias generadas en el componente de políticas y estándares del Grupo Infraestructuras de Datos Espaciales del CIAF, y se mostrará, a nivel tecnológico, con qué componentes de software se cuenta actualmente en el mercado para tal fin.

Palabras claves

estándar, geográfica, información, interoperabilidad, política, servicio, tecnología, web.

1 Ingeniero de Sistemas. Especialista en Proyectos Informáticos. Instituto Geográfico Agustín Codazzi. Cra. 30 48-51 Oficina CIAF. E-mail: lortiz@igac.gov.co.

2. Ingeniero de sistemas, Especialista en Sistemas de información Geográfica SIG. Instituto Geográfico Agustín Codazzi. Cra. 30 48-51 Oficina CIAF. E-mail: nfroldan@igac.gov.co

Security on web services: an essential component on interoperability of geographic information

Abstract
The "Instituto Geográfico Agustín Codazzi – IGAC" is the entity responsible for producing the official maps of the Republic of Colombia. In the same way, the "Centro de Investigación y Desarrollo en Información Geográfica – CIAF" is responsible for detecting, appropriate and transfer technologies for the management of geographic information and spatial data infrastructures through the use of Remote Sensing, Information Systems Geographic and related tools, to support institutional strengthening and sustainable development of the country and the region.

This office has over 40 years of experience with the transfer of knowledge, to train professionals of diverse nationalities through mechanisms and strategies taught in a classroom teaching with highly qualified teaching staff, and for the purpose of transferring knowledge and education high quality.

So, since 2008 the Geoservices Group is putting in operation a variety of web tools under open source software philosophy that promote a new way to work in the research, education and diffusion around geographic information, and that are based on an open and participative spirit. These tools are implemented through web services and applications (in case of the geographic component), that on earlier years had been developed with success, especially in order to make this information interoperable with other institutions that form the Colombian Spatial Data Infrastructure.

The different technologies and tools used by the group arises in an oriented services philosophy. While promoting the use of these open source tools for the geographic information management, the group also has knowledge in GIS proprietary tools, like all the ArcGIS technology package.

However, and because of the growing interest of many institutions in protect the information given to the citizens through web services, we have to think in strategies that assure this information gets where it belongs, especially when dealing with sensitive information such as the geographical.

The previous is the main motivator of this article, because it is currently in the process the study on implementation of security for web services of the IGAC node of ICDE, together with all licenses generated in the policies and standards component of the Spatial Data Infrastructure Group of CIAF, and is interesting from a technological view to show how software components are currently in the world market for this purpose.

Key words
Standard, geographic, information, interoperability, politics, service, technologies, web.

Introducción

Las especificaciones del Open Geospatial Consortium (OGC) se enfocan en la correcta operación técnica de las funciones que cada servicio web geográfico soporta, desatendiendo aspectos importantes para los sistemas distribuidos, como los mecanismos propios de seguridad.

Sin embargo, para las instituciones que producen y mantienen información geográfica, la seguridad y la conservación de la propiedad intelectual constituyen temas cruciales al momento de servirla a través de la internet. Por esto, el OGC ha conformado dos grupos para atender dichos aspectos, el GeoRM (Geo Rights Manager) y el Security WG (Security Working Group). El primero se ocupa de garantizar formas de proteger la propiedad intelectual sobre la información geográfica, y el segundo apoya el uso de estándares para definir seguridad en servicios web.

En el presente artículo serán expuestos los conceptos básicos de seguridad de servicios web de mapas y se hará un repaso por diferentes estándares relativos a seguridad de servicios web establecidos por entidades como el World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS) o el Open Geospatial Consortium (OGC).

Así mismo, se presentarán varios proyectos de clientes y servidores para mapeo web que permiten definir seguridad en servicios web geoespaciales, de tal forma que se puedan evaluar las posibilidades con las que cuenta el grupo de Geoservicios del CIAF en la implementación de una o varias de estas herramientas.

Se concluirá con algunas recomendaciones para la implementación de alguno de los proyectos expuestos.

1. Seguridad en servicios web

El concepto de seguridad en la web ha sido delimitado por el Departamento de Defensa de los Estados Unidos, señalando que la seguridad controla el acceso a la información, de tal forma que solo usuarios debidamente autorizados, o procesos que operan bajo su responsabilidad, pueden acceder a leer, escribir, crear o borrar información.

Según Opincaru (2008) la seguridad para servicios web está enfocada a la protección de información, la cual puede encontrarse en dos estados: en reposo y en tránsito. La seguridad de la información en reposo es básicamente atribuible al sistema operativo del servidor web y al servidor web en sí mismo, mientras que la seguridad de la información en tránsito se refiere generalmente al uso de Firewalls.

La seguridad de servicios web se puede definir en varios niveles. Según la International Organization for Standarization (ISO), existen siete capas en las que un servicio web puede recibir protección; estas son: la capa física, el enlace de datos, la red, el transporte, la sesión, la presentación y la aplicación. La Figura 1 muestra gráficamente la disposición de las capas en una implementación real, así como las diferentes tecnologías y protocolos asociados con cada una de las capas.

En el contexto de los servicios web de mapas, la seguridad se entiende como el mecanismo que permite llevar a cabo una administración del acceso a los elementos geográficos. Dicha administración comprende la definición de políticas de uso, la creación de usuarios y grupos con diferentes niveles de confianza y la implementación de restricciones que puede darse a distintos niveles.

2. Estándares para la implementación de seguridad en servicios web

En los últimos años varias organizaciones sin ánimo de lucro han trabajado en el establecimiento de estándares y especificaciones para mejorar la interoperabilidad entre aplicaciones. De esta manera, la seguridad en los servicios web puede manejarse entre grupos de organizaciones actuando en forma federada.

La Figura 2 muestra un panorama de los diferentes estándares relativos a servicios web y seguridad definidos por varias organizaciones del sector de la informática:

Cada uno de los estándares constituye un elemento de un sistema de seguridad, por sí mismo no representa una implementación completa en el tema. La Figura 3 evidencia la interdependencia entre dichos estándares.

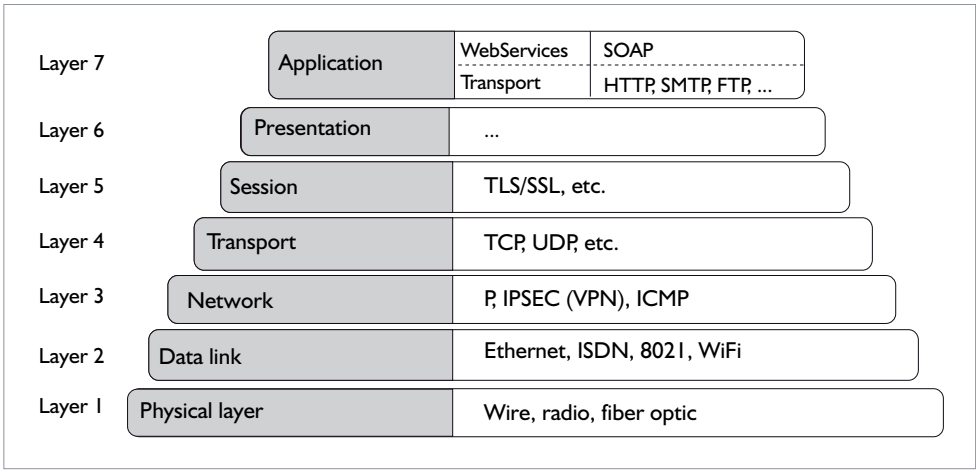

Figura 1.
Capas de seguridad para servicios web
Fuente: Cristian Aurel Opincaru, 2008

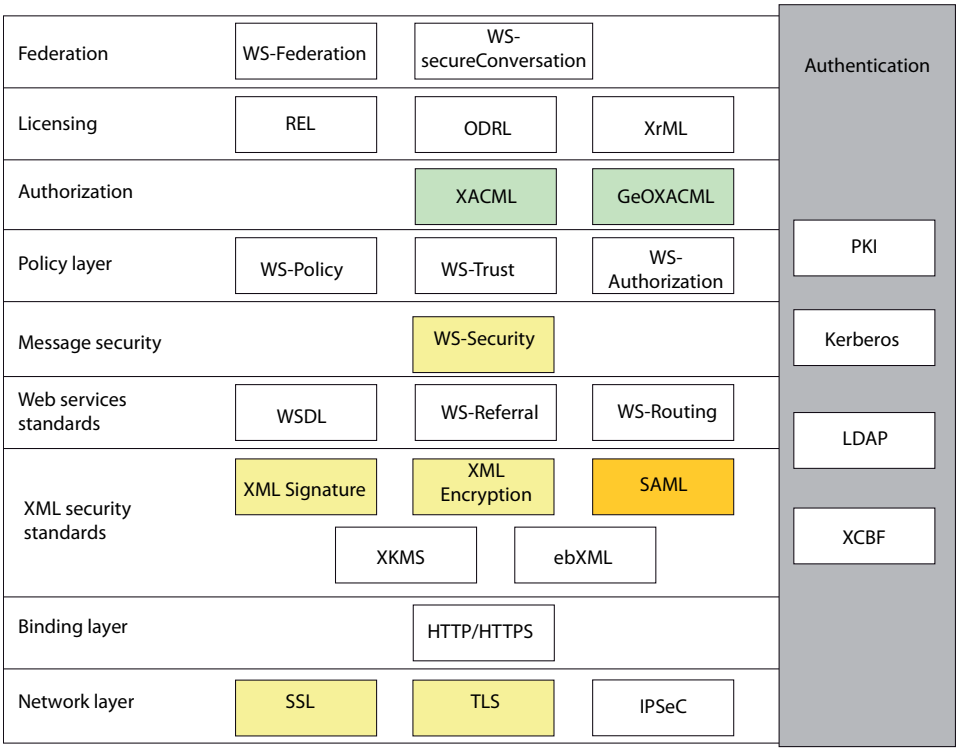

Figura 2.
Estándares para la web y para la seguridad en la web
Fuente: Open Geospatial Consortium

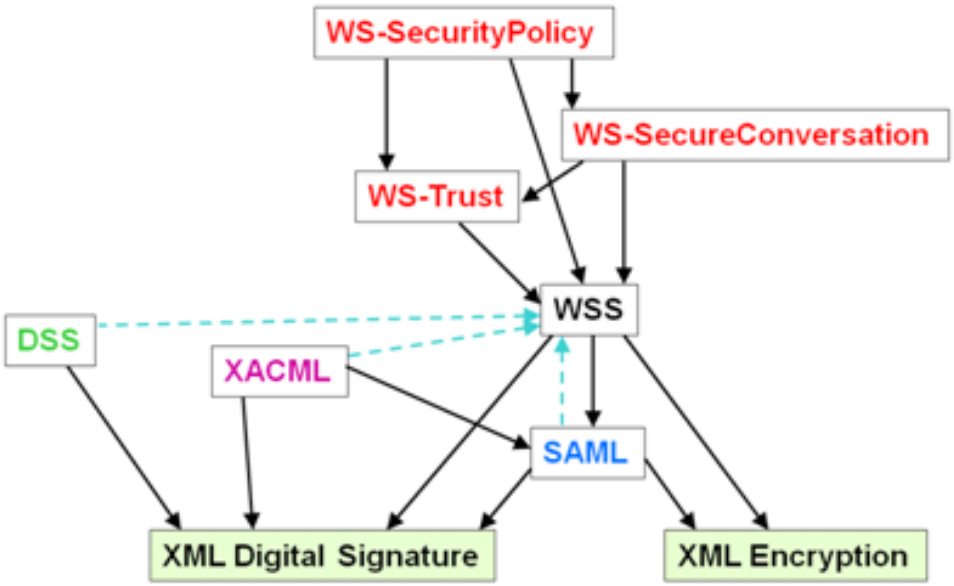

Figura 3.
Interdependencia entre estándares para la seguridad de servicios web
Fuente: Hal Lockhart

A continuación se extienden los principales estándares agrupados en organizaciones, con el fin de proveer un marco conceptual suficiente para comprender la adopción que realiza el OGC en materia de servicios web geográficos.

2.1 World Wide Web Consortium (W3C)

El W3C es una comunidad internacional encargada de desarrollar estándares para la web con el fin de incrementar su potencial. Uno de los estándares más importantes desarrollados y mantenidos por el W3C para asegurar la interoperabilidad en la web es el XML.

2.1.1 Extensible Markup Language (XML)

Según el W3C, el Lenguaje de Marcado Extensible es un formato de representación de datos estructurados, basado en texto plano. Es la base de una serie de estándares diseñados para atender diferentes aspectos relativos a la web, como el transporte de datos y la seguridad. El W3C recomienda utilizar XML y sus estándares derivados para el almacenamiento y el manejo de información. XML garantiza la escalabilidad permitiendo responder a diferentes requerimientos en cuanto a volumen de información.

Los estándares basados en XML más representativos en el tema de seguridad son:

- **Encriptación basada en XML:** Provee seguridad de principio a fin para aplicaciones que requieren intercambio seguro de información estructurada.
- **Sintaxis y procesamiento de firmas XML (Digital Signature Services):** Provee integridad, autenticación de mensajes y servicios de autenticación de firmantes.
- **Certificados digitales:** Son archivos electrónicos que actúan como pasaportes en línea. Son emitidos por una autoridad que verifica la identidad del poseedor del certificado.

- **Administración de claves XML (XKMS):** XKMS simplifica el aseguramiento de transacciones de internet basadas en XML usando infraestructura de llaves públicas (Public Key Infrastructure) y certificados digitales.

Los servicios web están basados en tres estándares principales que pueden ser definidos mediante XML:

- **SOAP:** El Protocolo de Acceso a Entidades Simples (Simple Object Access Protocol) está enfocado a la transmisión de datos.

- **WSDL:** El Lenguaje de Descripción de Servicios Web (Web Services Description Language).

- **UDDI:** (Universal Description, Discovery and Integration). Es un registro para localizar servicios web.

En general, un proyecto basado en servicios web que requiera seguridad necesita tener en cuenta los siguientes dos aspectos:

- Restricción de acceso a servicios web basados en XML para usuarios autorizados: Esto es manejado por **XACML** (Extensible Access Control Markup Language) y estándares **WS-Policy** (Políticas para Servicios Web).

- Protección de la integridad y confidencialidad de intercambio de mensajes XML en un ambiente de servicios web: Esto es manejado por los estándares Web Services Security **(WSS)** y Security Assertion Markup Language **(SAML)**.

A continuación se describen en mayor detalle los estándares WS-Policy, WSS, SAML y XACML.

2.1.1.1 WS-Policy:

WS-Policy provee una gramática flexible y extensible para expresar las capacidades, requerimientos y características generales de entidades en un sistema basado en servicios web XML. WS-Policy define un *framework* y un modelo para expresar dichas propiedades como políticas. Las expresiones de políticas permiten hacer afirmaciones simples y complejas.

La representación XML de una afirmación de políticas se conoce como expresión de políticas. Varias afirmaciones de políticas se pueden combinar utilizando operadores de políticas como: All, ExactlyOne, OneOrMore, entre otras. Para la administración, se requiere un repositorio de políticas. La herramienta de administración que se adopte para una organización particular debe proveer interfaces para insertar, modificar y eliminar políticas, y debería hacerlo con la ayuda de una base de datos XML.

2.1.1.2 Web Services Security (WSS):

Define una manera estándar para aplicar firmas digitales y encriptación a documentos SOAP empleando estándares de seguridad XML. WSS especifica cómo proteger mensajes SOAP mientras son transportados a través de la red. Esto incluye la autenticación, protección de la integridad y confidencialidad.

WSS usa la sintaxis y procesamiento de firmas XML y el estándar de encriptación XML desarrollado en la W3C. WSS funciona insertando un elemento XML llamado seguridad en el encabezado SOAP. Dicho encabezado contiene toda la información acerca de la autenticación, firmas digitales y encriptación que hayan sido aplicados al mensaje. Esto le da al receptor la información necesaria para desencriptar y validar el mensaje. La clave y la información de la autorización pueden ser especificadas usando varios métodos como certificados X.509, tiquetes Kerberos y afirmaciones SAML, entre otros.

2.2 Organization for the Advancement of Structured Information Standards (OASIS)

OASIS es un consorcio sin ánimo de lucro que busca promover el desarrollo y la adopción de estándares para la sociedad de la información. El consorcio produce más estándares para los servicios web que cualquier otra organización. Fue fundado en 1993 y tiene más de cinco mil participantes representando más de seiscientas organizaciones y miembros independientes en cien países. El consorcio se caracteriza por su transparencia en temas como la selección de los que cumplen el rol de líderes, los cuales se distinguen por méritos propios y no por la financiación que otorgan. Entre sus principales objetivos se encuentran los estándares para la seguridad en servicios web.

2.2.1 WS-Security

Esta especificación y sus perfiles asociados (Username, X.509, SAML, Kerberos, REL y SOAP con anexos) dan la base para aplicar funciones relativas a la seguridad como la integridad y confidencialidad en mensajes, implementando un alto nivel para los servicios web. WS-Security hace referencia a un conjunto de extensiones y módulos conocido como "Web Services Security: SOAP Message Security" o "WSS: SOAP Message Security".

De manera más detallada, WS-Security genera soporte para múltiples formatos testigos de seguridad, dominios de confianza, formatos de firmas y tecnologías para la encriptación.

WS-Security provee tres mecanismos principales:

- Habilidad para enviar testigos de seguridad (security tokens) como parte de un mensaje.
- Integridad de mensajes.
- Confidencialidad de mensajes.

Cada uno de los mecanismos puede utilizarse de manera independiente, o complementaria, enviando un mensaje encriptado y firmado y suministrando un testigo de seguridad asociado a la clave que se empleó para el firmado y el encriptado.

Estos mecanismos por sí mismos no constituyen una garantía de una implementación completamente segura en lo referente a servicios web, pero sí constituyen un módulo que se integra a una solución segura.

2.2.2 WS-Trust

Esta especificación define extensiones que fueron construidas sobre WS-Security para proveer un *framework* que solicita y emite testigos de seguridad, y concreta relaciones de confianza.

WS-Trust extiende WS-Security suministrando:

- Métodos para validar testigos de seguridad.
- Maneras de establecer la presencia de evaluadores y concretar nuevas relaciones seguras.

Usando estas extensiones, las aplicaciones pueden dedicarse a comunicación segura diseñada para trabajar con el *framework* general de servicios web, incluyendo descripciones de servicios WSDL, servicios empresariales UDDI y mensajes SOAP.

2.2.3 Security Assertion Markup Language (SAML)

Esta especificación define la sintaxis y la semántica para protocolos que entregan información y para afirmaciones

XML relativas a la autenticación, atributos y autorización. En otras palabras, es un estándar diseñado para el intercambio seguro de información.

SAML define un vocabulario XML para compartir afirmaciones de seguridad, incluyendo afirmaciones de autenticación y autorización, habilitando un registro simple de usuarios y administración de dichas funciones. El vocabulario permite pasar sentencias entre diferentes nodos de confianza, información relativa al cómo y cuándo ocurrió la autenticación y autorización. SAML provee formatos estándar para expresar autenticación y atributos de usuario, y los protocolos para solicitudes y recepciones de mensajes.

SAML es un método para definir testigos en entornos federados. Hace uso de sentencias que determinan ciertas características de un sujeto, por ejemplo, la autenticación, el nombre y el rol del sujeto. SAML puede ser usado para codificar identidades de testigos y puede ser combinada con firmas XML.

SAML es una especificación muy versátil y puede utilizarse en diversos escenarios. Uno de los principales problemas que intenta resolver es el de autenticación. SAML es utilizado frecuentemente en ambientes federados en donde el usuario proviene de un dominio seguro diferente al que actúa como proveedor del servicio.

2.2.4 Extensible Access Control Markup Language (XACML)

Provee un vocabulario para expresar las reglas necesarias para construir decisiones basadas en autorización. XACML es un lenguaje para expresar las políticas de control de acceso, es decir, protege el contenido durante el intercambio de información.

XACML puede basar sus decisiones en las propiedades de los recursos disponibles o del entorno de trabajo, por ejemplo, factores como la fecha, la hora o la ubicación. Así mismo, puede basarse en las propiedades de quien realiza la petición, por ejemplo, su pertenencia a determinado rol o grupo.

XACML hace un uso extensivo de estándares XML y OASIS. Usa la estructura y los protocolos de las afirmaciones SAML para proteger y distribuir políticas, emplea el firmado XML para proteger la modificación de afirmaciones, utiliza la encriptación basada en XML para proteger la privacidad cuando las afirmaciones son almacenadas y finalmente usa SSL y WS-Security para proteger las afirmaciones en línea.

2.3 Open Geospatial Consortium (OGC)

Las especificaciones del OGC son el prerrequisito para la interoperabilidad en Infraestructuras de Datos Espaciales. A pesar de los grandes avances que en dicha materia han sido alcanzados, no se ha definido una regulación referente a mecanismos de seguridad y autenticación de usuarios, por ejemplo, a través de la dirección de internet de un servicio web de mapas (WMS) cualquier persona puede acceder a todos los mapas y los atributos de los datos. De esta manera, no es posible aplicar ninguna restricción sobre usuarios o áreas específicas. Incluso, no es posible utilizar protocolos seguros como HTTPS en los servicios web OGC puros.

Sin embargo, existen grupos de trabajo en el OGC dedicados a estudiar temas específicos y a proponer soluciones estándar. El grupo de trabajo enfocado en el tema de la seguridad en servicios web OGC se llama Security WG (Working Group) y busca fomen-

tar el uso de estándares de seguridad ya definidos en las tecnologías de la información. Los objetivos principales del grupo son:

- Autenticación
- Control de acceso
- Uso de encriptación para proteger:
  - Intercambio de mensajes y en general la comunicación entre partes.
  - Datos espaciales.
  - Licencia.

El OGC realiza encuentros que involucran a diferentes sectores de la tecnología con el fin de establecer lineamientos en el desarrollo y adopción de nuevos estándares. En el tema de la seguridad, se han realizado varias reuniones de las cuales se han generado reportes en los que se estipula que el OGC ha decidido:

- Adoptar comunicación basada en SOAP (Service Oriented Architecture Protocol) para la interfaz de servicios web.
- Comunicación segura impulsando el estándar WS-Security de OASIS.
- Control de acceso basado en XACML/GeoXACML. En este punto el OGC ha trabajado en la adaptación del estándar XACML de OASIS en un estándar con capacidades para objetos geográficos denominado GeoXACML.

Se observa que el OGC busca mejorar las especificaciones de sus servicios web de tal forma que se integren en soluciones completas que involucren temas como el de la seguridad de los datos espaciales, siempre acogiéndose a estándares ya establecidos en la industria de los servicios web.

2.3.1 Geospatial eXtensible Access Control Markup Language (GeoXACML)

La declaración de restricciones espaciales no está soportada por el estándar XACML, en particular, no soporta la codificación de tipos de geometrías y las relaciones espaciales. De cualquier manera, XACML provee posibilidad de extensión para definir las estructuras espaciales requeridas. Dicha extensión es llamada GeoXACML, una especificación del OGC.

GeoXACML define una extensión de XACML para tipos de datos espaciales y para funciones espaciales con el fin de decidir una autorización. Utiliza la codificación de GML para declarar tipos de datos estructurados, como son las geometrías. GeoXACML soporta la declaración y la aplicación flexible de permisos de acceso.

3. Funciones de seguridad para servicios web

Existen diferentes funciones que un sistema seguro debe proveer en el contexto de los servicios web. A continuación se listan las principales según Opincaru, 2008 y Open Geospatial Consortium, 2006 y 2009, algunas de ellas introducidas previamente en la descripción de estándares.

3.1 Autenticación

Consiste en verificar que quien solicita ejecutar alguna acción o acceder a un recurso, es en efecto quien dice ser a través de una identidad. El solicitante puede ser humano o una aplicación (por ejemplo, un servicio web).

Según Opincaru, 2008, la verificación se basa en cuatro factores: Algo que un usuario es (como la huella digital), algo que un usuario tiene (como una llave privada), algo que un usuario conoce (como una contraseña) o algo que un usuario hace (como reconocimiento de voz).

El estándar WS-Security trata la autenticación ofreciendo la posibilidad de agregar al mensaje varios testigos de seguridad (security tokens) a los mensajes SOAP.

3.2 Autorización

Es un derecho o permiso que se otorga a un usuario o aplicación para acceder a recursos o ejecutar alguna acción. Para autorizar el acceso a un recurso se debe conocer de antemano qué recurso es y su contexto, de esta manera, se toma una decisión con base en políticas de autorización. Los *frameworks* para autorización en cuanto a servicios web son:

AA A Arch: Divide la autorización en cuatro servicios: Recuperación, información, decisión y aplicación.

XACML: Ofrece un lenguaje de políticas basado en XML y un modelo de servicios para la administración, información, decisión y ejecución de la autorización.

SAML: Para intercambiar información de seguridad. SAML puede utilizarse en combinación con XACML para codificar políticas y decisiones de autorización.

3.3 Confidencialidad

Hace el contenido ilegible para usuarios no autorizados y se asegura que solo usuarios legítimos pueden verlo. La confidencialidad es asociada generalmente con tecnologías de encriptación. Las tecnologías de encriptación más relevantes son Encriptación basada en XML y WS-Security, este último describe cómo la encriptación basada en XML debería utilizarse con mensajes SOAP.

3.4 Integridad

Asegura que la información permanezca intacta y no cambie durante su transporte, debido a intentos maliciosos o por accidente. Generalmente, la integridad es implementada a través del uso de firmas digitales. Estas firmas están integradas al mensaje para protegerlo.

Las tecnologías relevantes para la integridad de servicios web son Sintaxis y procesamiento de firmas XML (XML-DSIG) y WS-Security, el cual describe cómo usar firmas digitales basadas en XML para mensajes SOAP.

3.5 No rechazo (Non-repudiation)

Es la capacidad para asegurar que un mensaje transferido haya sido enviado y recibido por las partes que dicen haberlo enviado y recibido. Se lleva a cabo a través del almacenamiento de mensajes junto a una firma válida del remitente. En otras palabras, verifica la identidad de los autores que usan firmas electrónicas. Para el no rechazo se utilizan principalmente firmas digitales, servicios de confirmación y sellos de tiempo.

3.6 Privacidad

Es el derecho de los individuos para controlar qué información asociada a ellos puede ser recogida y guardada y por quién y a quién puede ser revelada. La privacidad es requerida usualmente por leyes nacionales y servicios que piden aceptar sus términos.

No hay tecnologías específicas para privacidad, pues se trata de un tema administrativo para asegurarse de que las aplicaciones cumplan términos de privacidad.

3.7 Disponibilidad

Es la propiedad de ser accesible y usable para cumplir una demanda realiza-

da por una entidad autorizada. Una de las posibles razones por las que un servicio web no está accesible es un ataque exitoso de denegación del servicio (Denial of Service).

4. Seguridad en servicios web OGC

Si bien muchos de los mecanismos y estándares de seguridad están basados en XML y orientados a SOAP (Simple Object Access Protocol), los servicios web OGC utilizan principalmente el enfoque REST (REpresentational State Transfer), puesto que los primeros servicios del OGC fueron definidos antes de que SOAP estuviera establecido.

De cualquier forma, los nuevos servicios web OGC (por ejemplo, WFS 1.1) incorporan SOAP, por lo que es posible implementar seguridad siguiendo estándares del W3C y OASIS, generalmente enfocados en XML.

Gracias a GeoXACML es posible definir restricciones a varios niveles en servicios web geográficos del OGC, como lo muestra la Figura 4.

Restricciones por tipo de elemento espacial

Permite controlar el acceso basado en el tipo de los elementos espaciales. Por ejemplo, permite el acceso a los elementos espaciales de tipo predio.

Restricciones por atributos

Permite el control de acceso para elementos espaciales individuales, por ejemplo, predios residenciales.

Restricciones espaciales

Permite el control de acceso basado en la geometría de los elementos espaciales, por ejemplo, predios ubicados en el perímetro urbano del municipio de Fusagasugá.

5. *Frameworks* para SIG en la web con componente de seguridad

A continuación se presenta una descripción de los *frameworks* más empleados para establecer seguridad para servicios web de mapas.

5.1 52º North

52º North es una organización alemana sin ánimo de lucro dedicada a la investigación, desarrollo e innovación en el ámbito geoespacial. Participa activamente en la definición de estándares e impulsa

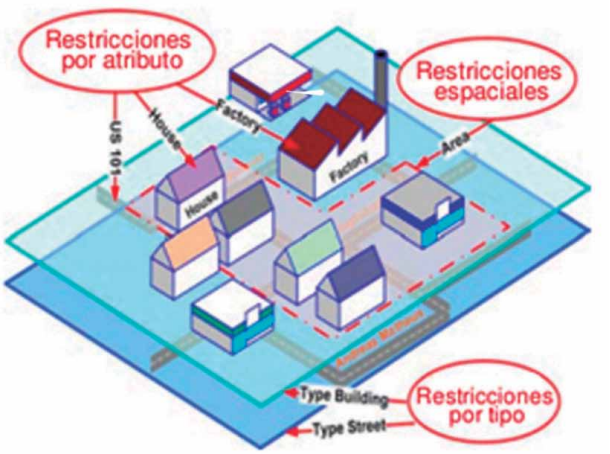

Figura 4.
Restricciones a varios niveles en servicios web geográficos
Fuente: Andreas Matheus

su adopción a nivel mundial mediante la publicación de prototipos listos para usar en ambientes de producción. Está asociada con centros de investigación como el IFGI de Alemania y el ITC de Países Bajos y con compañías como ESRI. Maneja líneas estratégicas entre las que destacan seguridad, geoprocesamiento, web semántica, geoestadística y visualización 3D. Generalmente, libera sus prototipos bajo licencias Open Source, por ejemplo, el software ILWIS, ampliamente reconocido en el trabajo de procesamiento para SIG.

En el tema de seguridad provee varias herramientas a los usuarios y adopta estándares reconocidos como **WSS,** Web Authentication Service **(WAS), SAML y WS-Security.** Para empezar, 52º North dispone una **API de seguridad** como base para facilitar la implementación en Java de seguridad en servicios web de mapas. Por otro, lado ofrece un **servicio de seguridad web (WSS)**. Para poder utilizar este último, los clientes deben soportar el protocolo WSS de 52º North, lo que generalmente no se da. Por esto, adicionalmente, se provee un puente entre el cliente y el WSS, llamado **Cliente de Seguridad** (Web Security Client) tanto Web (WSC.Web) como de escritorio (WSC.Desktop), con el fin de servir de conector entre un cliente de servicios OGC convencional y el servicio de seguridad web (WSS) de 52º North.

Dentro de la implementación del WSS, 52º North provee además un **prototipo para acordar un licenciamiento** de los servicios web de mapas con los usuarios, adoptando los avances del grupo de trabajo del OGC llamado **Geo-Rights Management (GeoRM) WG**. A través de este, el usuario debe aceptar el tipo de licenciamiento que crea conveniente para posteriormente utilizar el servicio web de mapas protegido.

Así mismo, 52º North provee un servicio llamado **Gatekeeper** que sirve como alternativa basada en SOAP al WSS. Esta alternativa habilita al servicio para hacer uso del estándar de OASIS WS-Security para hacer cumplir políticas de seguridad. Esta funcionalidad se constituye como el núcleo utilizado para integrar servicios web OGC en sistemas de identificación federados.

Los prototipos de seguridad de 52º North están escritos en el lenguaje de programación **Java** y soportan los servicios web del OGC Web Mapping Service **(WMS)**, Web Feature Service **(WFS)**, Sensor Observation Service **(SOS)** y Web Processing Service **(WPS)**.

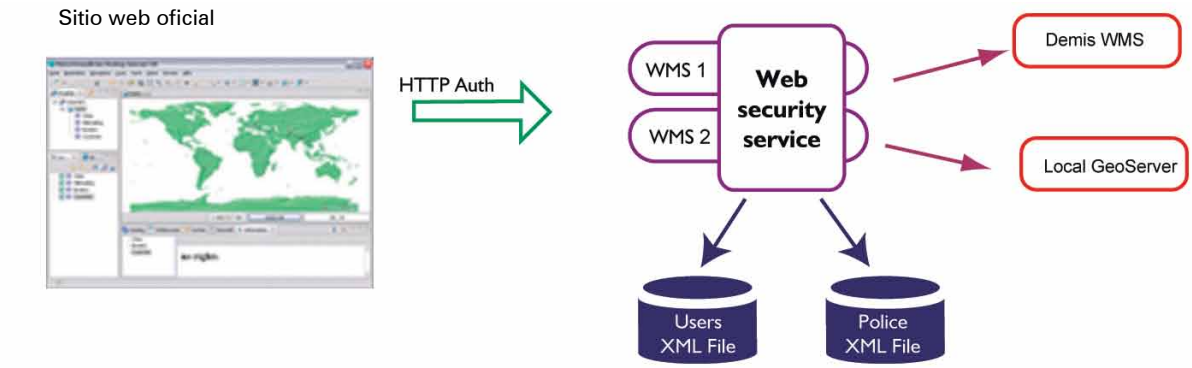

Figura 5. Arquitectura del servicio WSS de 52º North. A la izquierda el cliente web, a la derecha los servidores de mapas, y en el centro los servicios web protegidos
Fuente: 52º North. Sitio web oficial

5.2 Geomajas

Geomajas es un *framework* de código abierto escrito en **Java** que permite visualizar servicios web del OGC a través de la web. Está ampliamente enfocado en el lado del servidor, disponiendo herramientas de consulta, edición, procesamiento y seguridad de información geográfica.

En el tema de seguridad Geomajas provee un plugin de seguridad estática (Plugin Static Security) que agrega seguridad basada en configuración del *framework* de Java, Spring Security (antes Acegi Security). Spring Security es el estándar de facto para aplicaciones basadas en Spring, soporta LDAP, autenticación basic y digest, encriptación MD5 y SHA para contraseñas e implementa WSS (antes WS-Security).

La seguridad de Geomajas permite la definición de autorización en niveles específicos como una capa, un elemento espacial, un atributo e incluso a nivel de ToolBar para regular el acceso a los grupos de herramientas por parte de un usuario. El *extent* geográfico también está soportado para establecer la seguridad, de tal forma que un usuario solo pueda consultar datos en determinada región espacial.

En futuras versiones se planea incorporar más funcionalidades en cuanto a seguridad se refiere, particularmente:

- Plugin de seguridad Shiro: Será un plugin que utilice el *framework* Apache Shiro. Apache Shiro es un *framework* de seguridad que realiza autenticación, autorización, criptografía y administración de sesiones. De esta forma, las funcionalidades relativas a seguridad serán delegadas en Apache Shiro, especialmente las políticas de autenticación y recuperación.

- Encriptación de datos: Encriptación adicional será agregada para las transferencias entre cliente y servidor.

5.3 MapFish

MapFish es un *framework* de la empresa Camptocamp para construir aplicaciones enriquecidas de Internet (RIAs) con contenido geográfico. Usa OpenLayers y las librerías GeoExt y Ext JS como base. MapFish tiene un componente de servidor y uno de cliente. En el servidor utiliza Python como lenguaje de programación, mientras que en el cliente utiliza Javascript.

En el tema de seguridad MapFish provee un mecanismo de seguridad para servicios web geográficos basados en losas o teselas (Tiles), específicamente para servicios creados mediante el proyecto **TileCache**. El mecanismo está basado en el *framework* **Pylons** y en el proyecto **repoze.what** para restringir el acceso a TileCache con base en permisos de usuario.

TileCache es un proyecto de la empresa Metacarta para implementar la recomendación WMS-C (WMS Tiling Client Recommendation) para reducir el tiempo de cargue de las imágenes obtenidas de un servicio WMS.

5.4 CartoWeb

Es un *framework* de la empresa Camptocamp para generar aplicaciones web

geográficas en el lenguaje PHP. Debido a su arquitectura orientada a objetos que lo hace modular, CartoWeb es empleado hoy en día, aun cuando su desarrollo ha quedado atrás desde 2008 para dar paso a MapFish.

En el tema de seguridad, CartoWeb permite el **manejo de autenticación, administración basada en roles y contraseñas en md5.** Maneja un plugin llamado "Auth plugin" para almacenar los usuarios y las contraseñas con base en un archivo (.ini), en una base de datos PostgreSQL, o en el sistema LDAP. En CartoWeb es posible restringir el acceso a nivel de toda la aplicación web, a capas geográficas o a la impresión de documentos PDF.

5.5 Deegree

Deegree es más que un servidor web. Es un proyecto que implementa servicios web del OGC y provee un geoportal, una aplicación de escritorio, mecanismos de seguridad y varias herramientas para el procesamiento y administración de datos espaciales. Tiene licencia LGPL, está escrito en Java y cumple estándares ISO y OGC.

En cuanto a la seguridad, Deegree provee un módulo llamado iGeoSecurity que cuenta con varios componentes como:

- OwsProxy: Proxy para un servicio web abierto como WMS, WFS o CSW. Consiste en un módulo que se ubica en el medio del cliente y del servicio, administrando el acceso con base en mecanismos de autenticación y autorización. Este componente fue diseñado pensando en ampliar el alcance de las especificaciones OGC, que no incluyen una implementación en materia de seguridad.
- Usuarios, permisos, roles y recursos (U3R): Base de datos para la administración de usuarios y permisos de acceso, incluyendo una interfaz web.
- Servicio web de seguridad.
- Servicio web de autenticación.
- Cliente web de autenticación.
- Módulo de seguridad.

Con el módulo iGeoSecurity, Deegree permite implementar los siguientes casos de uso:

- Acceso regulado a capas específicas.
- Permitir acceso solo a algunos usuarios a capas específicas.
- Acceso restringido espacialmente.
- La salida puede ser filtrada, por ejemplo, es posible definir la calidad de la salida, el tamaño del mapa o la resolución.
- La salida puede ser modificada con base en permisos específicos, por ejemplo, el documento de capacidades o el GetFeatureInfo pueden ser filtrados, o se puede agregar una marca de agua.
- Usar conexiones seguras y mecanismos de autentificación.

5.6 Mapbender

Mapbender es un *framework* que contiene funcionalidades de servidor y de cliente. Provee herramientas gestión de seguridad de servicios web e interfaces para la administración de usuarios y grupos. Recientemente se agregó OpenLayers como alternativa para el

renderizado y JQuery para mejorar la integración con AJAX.

En el tema de seguridad, Mapbender maneja el acceso basado en permisos a servicios y a módulos. Mapbender provee tres módulos de seguridad principales: OWS Proxy, HTTP_AUTH y OWS Security Proxy.

OWS Proxy:

Este módulo sirve para recibir y regular las llamadas a los servicios web. Sin embargo, una vez configurado el Proxy, se debe asegurar el servidor, puesto que este módulo no lo hace. Las peticiones desde el navegador no son enviadas al WMS sino al módulo OWS Proxy de Mapbender, el cual actúa como un WMS transfiriendo la petición para uso interno.

OWS Proxy se basa en variables de sesión que construye para que un usuario tenga acceso a los servicios; cuando la sesión expira, el usuario debe volver a autenticarse para poder acceder a los servicios protegidos.

Mapbender provee una alternativa más segura, el módulo Http_Auth.

HTTP Authentication (Http_Auth):

Hay dos tipos de autenticación HTTP:

- Basic: No es considerada como segura porque el usuario y la contraseña viajan en texto plano a través de la red. Se recomienda usarla con un sistema de seguridad externo como SSL (Secure Sockets Layer).
- Digest: Así como la autenticación Basic, Digest verifica que ambas partes en una comunicación conozcan un secreto compartido (una contraseña), pero a diferencia de la Basic, esta verificación en Digest ocurre sin enviar la contraseña en texto plano, lo cual es la principal debilidad del método Basic.

La autenticación HTTP tiene debilidades, puesto que la gran amenaza para este tipo de protocolos es la interceptación en la red. Tanto en Basic como en Digest puede interceptarse la comunicación y realizar un ataque, sin embargo, en Digest el daño es ciertamente menor.

OWS Security Proxy:

Implementa el control de acceso y la administración de servicios OGC. El acceso a los servicios de mapas es concedido después de una autorización y autenticación del usuario. La interfaz web para la administración de usuarios puede ser usada para denegar o conceder el acceso a usuarios individuales, grupos y operaciones. Adicionalmente, pueden habilitarse protocolos para registrar cada acción de un usuario autenticado.

Mapbender permite manejar la seguridad en los siguientes niveles:

- Servicio (ejemplo: WMS).
- Capa de un servicio.
- Consulta de características (GetFeatureInfo) dentro de una capa WMS.
- Consulta para elementos espaciales individuales dentro de una capa WMS.
- Restricción espacial: basada en la extensión del mapa (*map extent*).
- Restricción de lectura de objetos WFS identificados por atributos.

- Restricción de edición de objetos WFS identificados por atributos.

5.7 GeoServer

GeoServer es un servidor web de mapas escrito en Java que permite compartir y editar datos espaciales. Está diseñado para favorecer la interoperabilidad soportando los formatos usados comúnmente en geomática y utilizando estándares abiertos.

En cuanto a la seguridad, GeoServer se basa en **ACEGI Security**, que ha evolucionado en Spring Security (ver descripción de Geomajas).

GeoServer maneja autenticación tipo **HTTP Basic** y provee seguridad basada en roles, esto es, se da permiso a los roles para acceder a características y los usuarios se enlazan al rol. La seguridad en GeoServer está a dos niveles: a nivel de servicio y a nivel de capas, pero ambas no pueden ser combinadas. Por ejemplo, no se puede definir seguridad para una capa específica de un servicio web del OGC.

Seguridad a nivel de servicio: Permite configurar los permisos que cada rol tendrá cuando intente acceder a cualquier método (petición) del servicio web geográfico.

Seguridad a nivel de capa: Permite configurar los permisos de lectura y escritura para cada rol.

Adicionalmente, Geoserver cuenta con seguridad basada en la arquitectura **Representational State Transfer (REST)** como alternativa a la seguridad de ACEGI. Esto requiere configurar el módulo REST de Geoserver.

Conclusiones

- Es necesario profundizar en el aspecto técnico de la seguridad de servicios web geográficos para que organizaciones productoras de datos espaciales compartan su información a través de políticas claras de acceso y uso, que permitirán aprovecharla por parte de los usuarios generando posiblemente trabajos derivados, obteniendo un valor agregado sobre la información geográfica del país.

- Existen diversos estándares para implementar seguridad en servicios web geográficos, la mayoría de ellos están basados en XML y en el protocolo SOAP, el cual ha venido siendo adoptado por el Open Geospatial Consortium en las últimas versiones de sus especificaciones para servicios.

- Si bien el Open Geospatial Consortium no definió inicialmente un marco para la implementación de seguridad en servicios web geográficos, en la actualidad se encuentra trabajando en la definición de licencias (GeoRM) y aspectos técnicos (Security WG) para garantizar una asignación versátil y confiable de permisos a los usuarios.

- Existen varios *frameworks* para implementar seguridad de servicios web geográficos. Se recomienda documentar la configuración de un prototipo para conocer sus fortalezas y la manera en que permite definir permisos a distintos niveles (espacial, por atributos y por tipo de elemento espacial).

- Según lo observado en este estudio preliminar, se recomienda documentar la configuración del *framework* de seguridad de 52° North o del proyecto Deegree, puesto que permiten definir permisos a distintos niveles (espacial, por atributos y por tipo de elemento espacial).

Agradecimientos

Un gran agradecimiento y reconocimiento al ingeniero Germán Carrillo, que con su naturaleza investigativa aportó las bases del presente artículo y nos dejó grandes enseñanzas en el grupo.

Referencias bibliográficas

52° NORTH. Security & Geo-Rights Management Community. [artículo de Internet] <http://52north.org/maven/project-sites/security> [Consulta: Junio de 2011].

CAMPTOCAMP S.A. CartoWeb, Security Configuration. [artículo de Internet] <http://www.cartoweb.org/doc/cw3.4/xhtml/user.security.html> [Consulta: Junio de 2011].

CAMPTOCAMP S.A. MapFish, Secure TileCache Tutorial. [artículo de Internet] <http://www.mapfish.org/doc/tutorials/secure_tilecache.html> [Consulta: Junio de 2011].

CHRISTL, Arnulf. Introduction to Geoportal Management using Mapbender. FOSS4G 2008. South Africa, 2008. [artículo de Internet] <http://www.foss4g.org/index.php/foss4g/2008/paper/view/82> [Consulta: Junio de 2011].

FRANKS, J. MICROSOFT CORPORATION; NETSCAPE COMMUNICATIONS CORPORATION; entre otros. HTTP Authentication: Basic and Digest Access Authentication. 1999. [artículo de Internet] <http://www.ietf.org/rfc/rfc2617.txt> [Consulta: Junio de 2011].

GEOSERVER. GeoServer Security. [artículo de Internet] <http://docs.geoserver.org/latest/en/user/security/index.html> [Consulta: Junio de 2011].

LAT/LON. Deegree iGeoSecurity. [artículo de Internet] <http://www.lat-lon.de/latlon/portal/media-type/html/user/anon/page/default.psml/js_pane/produkte%2Csub_produkte_deegree-igeosec> [Consulta: Junio de 2011].

LOCKHART, Hal. Web Services Security Challenges. < http://www.omg.org/news/meetings/workshops/MDA-SOA-WS_Manual/06-1_Lockhart.pdf> [Consulta: Junio de 2011].

MATHEUS, Andreas. Geospatial eXtensible Access Control Markup Language (GeoXACML). <http://www.w3.org/Policy/pling/wiki/images/5/59/GeoXACML.pdf> [Consulta: Junio de 2011].

MATHEUS, Andreas. Security and the Open Geospatial Consortium (OGC). CEOS/WGISS-27 Workshop. Toulouse, 2009. [artículo de Internet] <http://wgiss.ceos.org/meetings/wgiss27/WGISS_27_Toulouse/05.11.2009/05.11_16.45_Security_and_the_Open_Geospatial_Consortium.ppt> [Consulta: Junio de 2011].

MATHEUS, Andreas. Geospatial eXtensible Access Control Markup Language (GeoXACML). University of the Bundeswehr. 2008. [artículo de Internet] <http://www.w3.org/Policy/pling/wiki/images/5/59/GeoXACML.pdf> [Consulta: Junio de 2011].

MATHEUS, Andreas. Access Control for Geo Web Services using GeoXACML. University of the Bundeswehr. 2005. [artículo de Internet] <http://www.unibw.de/inf3/forschung/projects/opengissec/flyergeoxacml/at_download/down2> [Consulta: Junio de 2011].

OASIS. Web Services Security (WSS) TC. [artículo de Internet] <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss> [Consulta: Junio de 2011].

OASIS. Web Services Security: SOAP Message Security 1.1. 2006. [artículo de Internet] <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf> [Consulta: Junio de 2011].

OPEN GEOSPATIAL CONSORTIUM. GeoXACML Implementation Specification. [artículo de Internet] <http://www.opengeospatial.org/standards/geoxacml> [Consulta: Junio de 2011].

OPEN GEOSPATIAL CONSORTIUM. OGC Web Services Initiative - Phase 6 (OWS-6). 2008. p. 70-74. [artículo de Internet] <https://portal.opengeospatial.org/files/?artifact_id=29191&format=pdf> [Consulta: Junio de 2011].

OPEN GEOSPATIAL CONSORTIUM. OGC OWS-6 Security Engineering Report. 2009. [artículo de Internet] <http://portal.opengeospatial.org/files/index.php?artifact_id=35461> [Consulta: Junio de 2011].

OPEN GEOSPATIAL CONSORTIUM. Página oficial Security WG. [artículo de Internet] <http://www.opengeospatial.org/projects/groups/securitywg> [Consulta: Junio de 2011].

OPINCARU, Cristian Aurel. Service Oriented Architecture applied to Spatial Data Infraestructures. Munich, Alemania. 2008. Pág. 36.

OPEN GEOSPATIAL CONSORTIUM. Secure Dimensions. <http://www.secure-dimensions.de/standards_en.html> [Consulta: Junio de 2011].

PARIKH, Ash; GURAJADA, Murty; SANGHA, Anthony. JavaWorld. Secure your SOA. 2006. [artículo de Internet] <http://www.javaworld.com/javaworld/jw-04-2006/jw-0410-webservices.html> [Consulta: Junio de 2011].

SPRINGSOURCE. Spring Security. [artículo de Internet] <http://static.springsource.org/spring-security/site/index.html> [Consulta: Junio de 2011].

VAN DER AUWERA, Joachim. Plugin Static Security, Geomajas. [artículo de Internet] <http://geomajas.org/plugin/static-security> [Consulta: Junio de 2011].

WHEREGROUP. Mapbender, OWS Security Proxy. [artículo de Internet] <http://www.mapbender.org/OWS_Security_Proxy> [Consulta: Junio de 2011].