GOBIERNO DE CHILE
SERVICIO DE ADUANAS

Formato de Firmas Electrónicas en Documentos XML

PROYECTO ISIDORA

Formato de Firmas Electrónicas en Documentos XML

La firma digital implementada por el SNA

El Servicio Nacional de Aduanas a centrado el desarrollo de sus sistemas computacionales en la utilización de tecnologías de vanguardia, que han alcanzado una posición predominante en lo relativo a tendencias tecnológicas.
Sobre la base del texto anterior, las transacciones electrónica se realizan en formato XML y son firmada siguiendo las especificaciones de firma XML (XMLDSIG) emitidas por la W3C y la IETF.
Lo anterior define un marco de trabajo basado en estándares internacionales, los cuales permiten a desarrolladores externos, interactuar con nuestros sistemas utilizando herramientas que soporten dichos estándares o por el simple echo de basarse en los mismos.

Descripción de XMLDSIG

A continuación se presenta una estructura general de un elemento XML que incorpora la estructura definida por xmlsig.

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

Figura 1: La figura describe la estructura genérica de la firma basada en XMLDSIG

En la figura anterior la notación asociada a ocurrencia de elementos es la siguiente:
? : Cero o una.
+ : Uno o más ocurrencias.
* : Cero o más ocurrencias

Como podemos observar en la figura anterior, se puede dividir la estructura de la firma digital en las siguientes áreas:

- SignedInfo

- SignatureValue
- KeyInfo
- Object

El elemento **SignedInfo** es el que realmente es firmado; éste contiene información sobre los algoritmos de canonización y firma, los cuales serán utilizados para obtener el contenido del elemento **SignatureValue.** SignedInfo también contiene el elemento **Reference** para cada uno de los objetos firmados, éste elemento establece una referencia (Basado en una URI) al objeto de datos de interés. Dentro del objeto **Reference** se encuentra la descripción del algoritmo hash (Función de resumen) utilizada para calcular el valor hash (Valor resumen), Los "tag" asociados a estos valores son **DigestMethod** y **DigestValue** respectivamente. Por último el elemento **Reference** también puede tener asociada transformaciones (**Transforms**), dichas transformaciones se aplicaran sobre el objeto referenciado y la salida de estas es entregada a la función hash que se este ocupando.
El elemento Keyinfo contiene información sobre la clave pública que será utilizada para validar la firma, pudiendo contener claves, certificados u otra información asociada. Es importante destacar que los valores que contenga este elemento dependerán de la forma de trabajo adoptada. Para ser más específicos si consideramos el caso en que una organización valida todas las firmas sobre la base de la información de certificados disponibles en una base de datos de la organización, el elemento KeyInfo puede ser obviado (No presentará contenido).
Por último el elemento **Object** se utiliza para incluir objetos arbitrarios dentro de **Siganture**, que pueden o no ser firmados.

Configuración de los algoritmos

El SNA ha definido los siguientes algoritmo para realizar el proceso de firma:

- Algoritmos de firma : RSA/SHA1
- Algoritmo Hash : SHA1

Estos algoritmos tienen que ser definidos antes de realizar el proceso de firma. La forma en que son configurados varía según la API de firma (Con soporte XMLDSIG) que se utilice.

Consideraciones del proceso de firma.

A continuación se detallan las consideraciones definida por el SNA:

- Cada elemento que se firme, debe de ir incrustado en el documento de firmas, es decir, no se aceptan referencias a documentos para ser firmados, si estas son referencias a un objeto que se encuentra fuera del sobre de firma.
- El documento se firma completamente.
- Al firmar no se incorpora información de los certificados en el objeto **KeyInfo.**
- Los certificados de los firmantes tienen que ser entregados al SNA para que queden registrados en el Base de datos de los usuarios del sistema.
- Un documento puede ser firmado por más de una persona.

Herramientas de desarrollo disponibles

La implementación de XMLDSIG es provista para un conjunto de plataformas y lenguajes, de manera tal, que los programadores pueden seleccionar las herramientas que consideren más idóneas según su entorno de trabajo.
A continuación se entrega una lista de algunos link, de proveedores que entregan Toolkits y SDKs para los desarrolladores.

- Baltimore
- DataPower
- Entrust/Toolkit™ ; for Java™
- IAIK XML Signature Library (IXSIL)
- IBM XML Security Suite
- Infomosaic
- Microsoft
- NEC XMLDSIG
- Phaos
- RSA BSAFE Cert-J
- Ubisecure
- Verisign
- Wedgetail

Es importante destacar, que cada proveedor implementa sus propias funciones o clases para soportar el estándar XMLDSIG, por lo tanto, cada proveedor entregará la documentación necesaria para utilizar los servicios de su API en particular.