Ministerio Secretaría General de la Presidencia
Proyecto Reforma y Modernización del Estado

Guía 1: Implementación de Modelo de Firma Electrónica Simple con Identificador/Clave

Proyecto Reforma y Modernización del Estado
Agustinas 1291, piso 5°, ofic. G - Santiago de Chile
F: (56 2) 694 5808 / (56 2) 694 5964 - Fax: (56 2) 694 5965
http://www.modernizacion.gov.cl

Tabla de contenidos

La última versión de este documento, puede obtenerse en http://www.e2g.gov.cl/efirma.html

1. Introducción

1.1 Objetivo y alcance del documento

Este documento es una parte integrante de la serie de documentos generados por el Comité de Firma Electrónica Simple, que ha sesionado durante el 2003, y cuya misión ha sido generar modelos de Firma Electrónica Simple para su uso al interior de la Administración Pública. Ha sido actualizado sucesivamente por el Proyecto de Reforma y Modernización del Estado, para responder a las necesidades reales planteadas por los servicios públicos en el proceso de implementación y adopción de mecanismos de Firma Electrónica.

El objetivo de este documento es servir de guía básica para implementar el modelo de Firma Electrónica Simple Nº1: esto es, Firma Electrónica con identificador y clave.

Los modelos de Firma Electrónica Simple propuestos son descritos y fundamentados en el documento "*Modelos de Firma Electrónica Simple para la Administración Pública*". Para obtener una descripción general de los tres modelos, consulte ese documento.

1.2 Contenido de este documento

Esta guía pretende explicar, en forma muy breve, los principios básicos necesarios para implementar un mecanismo de firma electrónica vía identificador y clave. A pesar de que se suponen conocidos los conceptos entregados en el documento "*Modelos de Firma Electrónica Simple para la Administración Pública*", se hace una revisión básica de la parte fundacional del modelo.

En el capítulo 2, se explica el modelo de firma electrónica con identificador y clave, independientemente de la tecnología que se utilice para implementarlo.

En el capítulo 3, se entregan observaciones técnicas básicas acerca de la implementación del modelo.

1.3 Breve fundamento de la Firma Electrónica Simple

El 25 de marzo de 2002 se promulgó la Ley de Documento y Firma Electrónica, Nº 19.799. En esta ley existen al menos dos definiciones importantes: **Firma Electrónica** y **Firma Electrónica Avanzada**. Debido a la cercanía de las definiciones, para diferenciar una de la otra se ha llamado "simple" a la primera.

Técnicamente, la definición de firma electrónica avanzada corresponde a lo que se conoce como PKI (tecnología que ha sido descrita en el documento "*Modelos de Firma Electrónica Simple para la Administración Pública*"). Por tanto, para utilizar lo que según la Ley es Firma Electrónica Avanzada, debe adquirirse un certificado digital de una empresa que haya sido acreditada por la Subsecretaría de Economía.

Sin embargo, este requisito se limita (según la Ley) sólo a aquellos documentos que constituyen "Instrumentos Públicos". Por tanto, la Ley incentiva el uso de algún mecanismo de firma simple para todos aquellos documentos que no constituyan "Instrumento Público". Por ejemplo, para todos aquellos documentos intercambiados al interior de un servicio público, o para todas aquellas comunicaciones enviadas a ciudadanos que no sean instrumentos públicos, debe utilizarse algún mecanismo de firma simple.

Para ello el Comité de Firma Simple, bajo el Comité de Normas y Estándares para el Documento Electrónico, ha sugerido 3 modelos de firma simple, de los cuales el descrito en esta guía es el primero: firma electrónica con identificador y clave.

2. Firma Electrónica Indirecta vía identificador y clave

2.1 Fundamento del modelo

En general, la forma más sencilla (y consecuentemente, la más ambigua) de identificar a una persona en un sistema computacional, es a través de un identificador único y de una clave asociada. Este hecho se basa en dos procesos básicos que ocurren en una comunicación[1]:

1. La **identificación**, que es el proceso mediante el cual el emisor anuncia quién es (identificación activa), o el receptor determina quién es su interlocutor (identificación pasiva).
2. La **verificación**, que es el proceso (posiblemente separado de la comunicación) mediante el cual el receptor se asegura de que el emisor es quien dice ser.

En los sistemas computacionales, suele utilizarse como identificador una palabra única, que se asigna a cada usuario del sistema; esta palabra se conoce como '*username*'. De la misma forma, a cada username va asociado una clave, que permite a la persona comprobar ante el sistema que es quien dice ser: esta clave suele llamarse '*password*'.

Una vez que nos identificamos ante un sistema, es posible que (bajo ciertos medios técnicos), el sistema realice un "seguimiento" automático de todas nuestras acciones. Este "seguimiento" puede ser utilizado para asegurar (bajo ciertas condiciones técnicas mínimas) que la persona que acaba de identificarse delante del sistema se responsabilice por sus acciones dentro del sistema, durante el tiempo que permanece "conectada al sistema".

Por tanto, las acciones realizadas durante el tiempo que la persona permanezca "conectada" al sistema se consideran "firmadas"; esto debido a que, si existe una forma de verificar que la persona es quien dice ser, entonces la persona es responsable de esas acciones.

2.2 Descripción del modelo

Este modelo, el más sencillo de los tres, consiste en **la identificación y verificación de identidad de una persona**, a través de **un username y un password** (clave de uso personal), en **un sistema que cumpla con un conjunto de características mínimas**. Estas características mínimas son las siguientes:

1. Existe un ambiente en red, donde dos o más usuarios tienen acceso a un recurso común,
2. El acceso a este recurso común es controlado a través del ingreso de un identificador personal (username, RUT, etc). y una clave (password),
3. Cada persona posee un, y sólo un identificador y clave,
4. El sistema permite registrar **en forma automática** el acceso a este recurso común, con al menos los siguientes datos:
   a) Identificador del usuario que realizó la operación,
   b) Identificación del recurso sobre el que se realizó la operación (a través de un nombre único),
   c) Tipo de operación realizada (creación/modificación/recuperación/eliminación),
   d) Fecha y hora del acceso.

[1] *Esta parte es mencionada en el documento "Modelos de Firma Electrónica Simple para la Administración Pública". Para más fundamento, consultar dicho documento.*

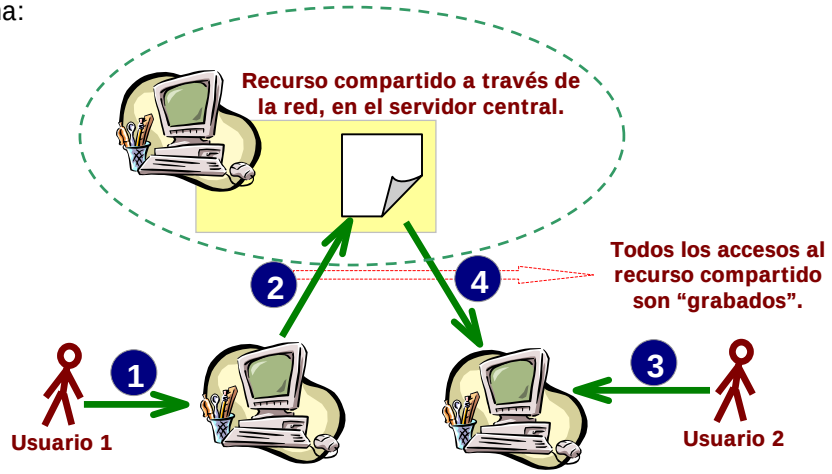
Este conjunto de condiciones pueden ser satisfechas por numerosas arquitecturas técnicas posibles, y puede por tanto ser implementada de muchas formas diferentes.

2.3 Esquema de funcionamiento

En la figura siguiente, existen los siguientes elementos genéricos:

1. Un ambiente en red, con recursos compartidos a los que un conjunto de usuarios (en teoría) tienen acceso por igual.
2. Un sistema automático de identificación. Esto es, un sistema que permita a los usuarios identificarse a través de username y password.
3. Un registro automático de acciones realizadas por los usuarios.
4. Un repositorio de documentos electrónicos donde es posible realizar alguna de las siguientes operaciones:
    a. Crear un documento,
    b. Modificar un documento,
    c. Eliminar un documento,
    d. Ver un documento.

Dado el conjunto anterior de elementos, una operación de "firma" puede visualizarse de la siguiente forma:



Para firmar e intercambiar un documento en este esquema, dos funcionarios siguen los siguientes pasos:

1. El usuario Nº1 se identifica a través de un identificador (un *username* o "nombre de usuario") y una clave (o *password*).

   El sistema automático de seguimiento registra que el usuario Nº1 ingresó, y en qué momento exacto ingresó (de acuerdo con la fecha y hora del sistema).

2. El usuario Nº1 coloca un documento en el "**recurso compartido**", a través de las facilidades que otorgue el sistema utilizado. Luego, posiblemente se desconecta del sistema.

   En este punto, el sistema automático de seguimiento registra la creación de un documento en el recurso compartido, junto con el identificador del usuario 1. En caso de que el usuario se desconecte, registra también el momento exacto en que salió del sistema.

3	El usuario Nº2 se identifica en el sistema, con su propio nombre de usuario y clave.
4	El usuario Nº2 obtiene el documento desde el "**recurso compartido**", y de acuerdo con las capacidades del sistema utilizado, obtiene la identificación de quién colocó el documento dentro del "**recurso compartido**". Este documento, una vez verificada la identidad de la persona que lo colocó en el recurso, es considerado "firmado" por la primera persona.

Todos los accesos al recurso compartido son registrados en el sistema. Cada acceso lleva asociado el identificador del usuario, tipo de acceso (escritura en el primer caso, lectura en el segundo caso), fecha y hora del acceso y nombre del documento accesado.

2.4 Plataformas técnicas posibles

Existen muchas plataformas técnicas, de las que podría interpretarse que cumplen con las condiciones anteriores. Mencionamos aquí algunas de ellas, exclusivamente a modo de ejemplo.

2.4.1 Carpeta compartida del sistema operativo

Hoy en día todos los sistemas operativos trabajan en red. Esencialmente todos también poseen el concepto de "carpeta compartida", es decir, un directorio con archivos que pueden ser vistos por muchos usuarios a la vez. La mayor parte de las veces, es posible también registrar de manera automática (a través de servicios o "demonios", que son programas que ejecutan permanentemente en la memoria de un computador), los accesos a estas carpetas compartidas.

En el caso de Microsoft Windows, tanto en Windows NT como en Windows 95, 98, 2000 y XP pueden configurarse carpetas públicas compartida, donde se guarden documentos (de MS Office, PDF, MS Powerpoint, etc.). Activando algunas opciones de auditoría de estas carpetas, es posible registrar los accesos a los documentos dentro de estas carpetas. Más datos, consultarlos en los manuales de administración de Microsoft Windows.

Aquí, la identificación ante el sistema es la que se realiza para ingresar a un computador específico (es decir, el username y password para ingresar a la máquina), o bien la que se realiza al ingresar a la carpeta (es posible configurar también un password de acceso a la carpeta).

En el caso de Unix y sistemas similares (Linux con todas sus distribuciones), es posible también fijar carpetas compartidas (como /tmp), y confiar en el sistema de archivos para identificar de manera razonable quién realizó una acción sobre un archivo en esta carpeta. Aquí la identificación es la que se realiza al conectarse a un servidor determinado.

2.4.2 Recursos disponibles en un sitio Web

Un sitio Web que posea zonas públicas y zonas privadas (accesibles sólo a través del ingreso de un username y una clave) también son una posibilidad de implementación. La intranet de una institución, por ejemplo, donde se provea la facilidad de subir o bajar archivos, constituye un sistema de firma simple pues los servidores Web proveen, normalmente, la funcionalidad de registro de todos los requerimientos de tipo HTTP realizados a un sitio Web determinado, con un registro de fecha y hora en que fueron realizados.

Por otro lado, una aplicación Web bien construida podría perfectamente implementar el registro de qué cosas se realizan sobre el sistema, una vez que un usuario se identifica.

Este caso merece atención especial, pues presenta numerosas ventajas sobre las anteriores:

1. Es fácilmente accesible e implementable, y no requiere de hardware especial (puede incluso ser accesada desde fuera de la institución[2]),
2. Los usuarios en general saben cómo navegar en el Web, y esto les facilita el aprendizaje de un esquema como éste,
3. La implementación es en general más barata que aquellas plataformas comerciales disponibles en el mercado,
4. Este esquema permite la utilización de tecnologías avanzadas, que incrementan la seguridad de las comunicaciones y permiten reutilizar esquemas conocidos (por ejemplo, si una Intranet está montada sobre el protocolo seguro SSL/TLS, esto otorga seguridad a las transacciones de documentos).

Por otro lado, existen numerosas implementaciones de sistemas Web de manejo de contenidos, que permiten implementar sitios Web más o menos complejos con poco esfuerzo. Todas estas aplicaciones cumplen con las condiciones exigidas a este modelo de firma, y permiten el ingreso de documentos a carpetas compartidas a los usuarios registrados en ellas. Estos software son conocidos como CMS (*Content Management Systems*), y existen (literalmente) cientos de ellos en la red.

2.4.3 Otras implementaciones posibles

Existen otras muchas formas de implementar un modelo de firma simple como el descrito en esta guía; sin embargo, no siempre es sencillo garantizar que todas las operaciones serán registradas de acuerdo con lo descrito en los puntos anteriores.

1. Microsoft Outlook provee un sistema de carpetas públicas y privadas, donde los usuarios pueden dejar o bajar documentos, solicitar recursos comunes (datashow, salas de reuniones, etc.)., colocar/leer noticias, etc., donde existe un password de acceso que puede ser distinto del username y password de cada máquina de usuario. Puede configurarse además un registro automático de los accesos a estas carpetas públicas.
2. IBM Lotus Notes provee también un sistema de repositorios públicos y bibliotecas, donde todos pueden dejar o tomar documentos, previa identificación en el sistema a través de un username y password (que son distintos de los ingresados a la máquina de cada usuario).

Para cada ejemplo, se recomienda estudiar con detención las capacidades técnicas del sistema, para verificar si se cumplen las condiciones mínimas de implementación descritas en el punto 2.2 (descripción del modelo).

2.5 Justificación de existencia

La razón por la cual este esquema es considerado como Firma Electrónica Simple, es que el registro automático de transacciones permite identificar formalmente al autor de un documento, que es lo que exige la definición en la Ley de Firma Electrónica.

[2] A pesar de que originalmente el concepto de Intranet implicaba sólo un acceso desde dentro de la institución, éste ha variado sustancialmente dentro de los últimos años y el límite entre la Intranet y la Extranet de una organización tienen un límite usualmente difícil de definir.