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

Modelos de Firma Electrónica Simple para la Administración Pública

Base técnica para comprender la aplicación e implementación de los modelos, sugeridos por el Comité de Firma Electrónica Simple

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 Resumen ejecutivo

La firma en general se utiliza como un medio de verificación de la identidad de una persona. Al firmar un documento escrito se supone la comprensión de éste, su aceptación y compromiso. Es así como la Firma Electrónica o Digital se utiliza para verificar la identidad del emisor de un Documento Electrónico.

Debido al incremento, a nivel mundial, en las transacciones realizadas vía Internet ha sido necesario regular estas actividades, con especial consideración para la firma electrónica como medio de verificación de identidad. La Comisión de Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) desarrolló una estructura legal como referencia para el desarrollo de la leyes respectivas en los países, promoviendo la neutralidad tecnológica, la equivalencia funcional y la autonomía de voluntad. Basándose en esta estructura, durante el año 2002 en Chile se promulgó la Ley 19.799 sobre Firma Electrónica, Documento Electrónico y Servicios de Certificación.

En lo referente a firma la Ley define la Firma Electrónica como cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar formalmente a su autor, y la Firma Electrónica Avanzada como aquella certificada por un prestador acreditado, que cumple con ciertas características de verificación. A partir de éstas se deduce la existencia y definición de la *Firma Electrónica Simple*: aquella que no cumple con todas las condiciones para ser avanzada.

En el artículo 39 de la mencionada Ley se establece que los órganos de la Administración del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. Además, se establece que todo documento que revista la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de éstos, deberán suscribirse mediante firma electrónica avanzada. De esta manera, **el Estado de Chile explícitamente privilegia el uso de la firma electrónica simple** para documentos electrónicos en la Administración Pública, **excepto cuando se trate de documentos que revistan el carácter de instrumentos públicos**.

El Comité de Firma Electrónica Simple, creado a partir del Comité de Normas para el Documento Electrónico, durante sesiones de trabajo realizadas durante el año 2003, ha propuesto tres modelos de Firma Electrónica Simple para su utilización en la Administración Pública. Estos son: la *Firma Electrónica Indirecta* a través de la utilización de un *username* y *password*, la *Firma Electrónica en E-mail* y la *Firma Electrónica en Documento*. Los criterios para la elección de estos tres modelos fueron: simplicidad, utilización de los recursos existentes y niveles de seguridad congruentes con las condiciones de autenticación, integridad y no repudio del documento electrónico.

Este documento tiene tres objetivos principales:

1. Servir de introducción a los conceptos legales y técnicos relacionados con Firma Electrónica.
2. Describir tres modelos de Firma Electrónica Simple, susceptibles de ser implementados en Servicios Públicos.
3. Servir de guía para implementar cada uno de los tres modelos en las distintas plataformas tecnológicas existentes.

Finalmente, existirá dentro de poco un sitio Web[1] provisto por el Proyecto de Reforma y Modernización del Estado, que complementa el contenido de este documento.

[1] *Próximamente en http://www.e2g.gov.cl.*

1.2 Contenido

El presente capítulo entrega un resumen ejecutivo, una descripción del contenido del documento completo y una serie de referencias para aquellos lectores que deseen profundizar en el tema.

En el capítulo dos se introduce el concepto de Documento Electrónico, que es anterior al de Firma Electrónica, se hace mención a la Ley de Firma Electrónica y Documento Electrónico (Ley Nº 19.799) y se describen los dos tipos de Firma que la Ley define. A continuación se explica porqué es necesario normar acerca de la Firma Electrónica Simple.

En el capítulo tres se realiza una introducción a algunos conceptos técnicos en criptografía, necesarios para comprender la terminología ocupada en el área y para sentar las bases de los modelos descritos posteriormente.

En el capítulo cuatro se describen los tres modelos propuestos de Firma Electrónica Simple y se entregan ejemplos de cada uno.

En el capítulo cinco se describen aquellas medidas de seguridad básicas que siempre deben ir asociadas a cualquiera de los tres modelos que se utilice.

Finalmente, en los anexos se entrega un ejemplo mencionado a lo largo del texto, relacionado con la obtención de llaves públicas y privadas, y una lista de preguntas y respuestas que muy frecuentemente se realizan respecto al uso y aplicación de Firma Electrónica, tanto al interior del Gobierno como en la empresa privada.

1.3 Referencias

A continuación y a modo de guía se entregan algunas referencias sobre criptografía y firma electrónica para aquellos lectores que deseen profundizar en estos temas.

Sobre criptografía

- "Criptografía", Porras, Manuel. Disponible Online [visitado 26 Agosto 2003], http://www.microteknologias.cl/bib_cripto.html
- "Criptografía", Wikipedia, la Enciclopedia Libre. Disponible Online [visitado 27 Agosto 2003], http://es.wikipedia.org/wiki/Criptograf%EDa
- "Cryptography, PGP and Pine", Dell'Omodarme, Matteo. Linux@Gazette, Disponible Online [visitado 27 Agosto 2003], http://www.linuxgazette.com/issue58/dellomodarme.html

Sobre Firma Electrónica

- "¿Se usa la Firma Digital en Chile?", Bluth, Andrea. EL Mercurio Online [visitado 25 Agosto 2003], http://www.emol.com/Diario_ElMercurio/modulos/Buscar/_portada/detalle_diario.asp?idnoticia=0124112002001A0230131
- "Firma Digital y Certificados Digitales", Angel, José. HTML Web [visitado 25 Agosto 2003], http://www.htmlweb.net/seguridad/varios/firma_certificados.html
- "Reglamento de la Ley Nº 19.799 sobre firma y documentos electrónicos". Accesible Online [visitado 25 Agosto 2003], http://www.paisdigital.org/html/biblioteca/busqueda.asp?tema=2

2. Acerca de la Firma Manuscrita y la Firma Electrónica

2.1 ¿Por qué firmamos?

En la vida diaria, aunque muchas veces no nos demos cuenta de ello, contraemos permanentemente obligaciones y compromisos, verbalmente o por escrito, y hasta con un simple gesto de asentimiento. Si escribimos nuestros compromisos, estos pueden ser o no firmados. Pese a que, en términos éticos, una compromiso legítimamente contraído obliga a su cumplimiento, no importa si éste fue o no escrito o firmado, lo cierto es que cuando firmamos por escrito asignamos un mayor grado de "formalidad". En este sentido la firma supone comprensión del texto, aceptación de lo convenido y compromiso.

La razón por la que podemos desear un mayor grado de formalidad para algunos compromisos se relaciona con la posibilidad de conflictos o diferencias entre lo que dos o más partes acuerdan. La memoria humana es frágil y la interpretación de los hechos que ocurren a nuestro alrededor puede ser radicalmente diferente de la que realizan quienes que nos rodean. Cuando escribimos y firmamos un documento, disminuimos la posibilidad de conflicto en lo que ha quedado por escrito.

2.2 ¿Dejaremos de firmar papeles en el futuro?

Las tecnologías de información han cambiado radicalmente nuestro quehacer cotidiano. La existencia de documentos electrónicos y su masificación en ámbitos técnicos (universidades) y luego en la cultura organizacional nacional permite pensar que, algún día, los documentos que conocemos en papel serán reemplazados por sus versiones electrónicas.

Pero ¿Es ésta una posibilidad real? ¿Será reemplazado el papel por las representaciones digitales de documentos?

Al parecer la transición no será completa ni inmediata. Destacados "futurólogos" estiman que, a pesar de lo que muchos "gurús" de la tecnología anuncian, el papel no será reemplazado durante las próximas décadas porque es un instrumento útil, que permite a las personas trabajar, comunicarse y divertirse de manera sencilla. Gran parte de las razones para ello tienen que ver con que el papel es barato, tremendamente flexible, puede transportarse fácilmente, nos permite observarlo sin cansancio visual (cosa que no ocurre con las pantallas de computador, por ejemplo) y nos permite comprender rápidamente qué contiene. De hecho, cuando recibimos un documento a través de un correo electrónico, lo más probable es que en la mayor parte de los casos imprimamos el documento para leerlo.

Sin embargo, el cambio radical que se espera para los próximos años no tiene relación con la ausencia de papel en nuestros trabajos: se refiere al transporte o circulación, clasificación, almacenamiento[2], búsqueda, manejo y responsabilidad sobre los documentos antes de que lleguen a nuestras manos para su lectura.

2.3 ¿Qué es una firma?

Una firma es **un medio de verificación de la identidad de una persona**. Para comprender qué significa esto debemos explicar primero dos conceptos fundamentales: la **identificación** y la **verificación de identidad**.

[2] *Es decir, habrá un cambio en el almacenamiento tradicional (archivo) de documentos.*

En una comunicación corriente entre dos personas existe en todo momento una persona que emite un mensaje ("emisor") y otra que recibe el mensaje ("receptor"). Antes de comenzar la comunicación se realizan dos procesos:

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.

Por ejemplo, supongamos que caminando por un parque nos encontramos con un amigo. Antes de comenzar a hablar, hemos visto su cara y su figura, y hemos reconocido y asociado dicha cara y figura con una "identidad": sabemos que él es Juan Pérez, a quien conocimos mientras estudiábamos en el colegio. Una vez que comenzamos a hablar, confirmamos que él es quien pensábamos. A pesar de que es posible que alguien se haya disfrazado como él, existen varios hechos sutiles (sus facciones, su voz, su apariencia) que nos permiten, con un alto grado de seguridad, asegurar que Juan es quien dice ser. En este proceso, hemos identificado y verificado la identidad de nuestro amigo sin siquiera darnos cuenta de ello.

Sin embargo, si nuestro amigo nos envía una carta, primero tendrá que **identificarse** ("Hola, yo soy tu amigo Juan Pérez..."). Al final de la carta, colocará una firma, que nos permita **verificar su identidad** (en caso de que tengamos alguna duda de que se trata de él).

En un documento, el nombre escrito debajo de la firma de una persona es su **identificación**, y su firma holográfica (aquella escrita sobre papel, "de puño y letra") es un medio de **verificación de identidad** de la persona. Si le pedimos a la persona su **cédula de identidad**, podemos verificar si la firma del documento y de la cédula son iguales. En tal caso, nos habremos asegurado de que la persona es quien dice ser.

En el mundo electrónico, este proceso ha sido generalizado para permitir que las personas puedan identificarse y permitir a otros verificar su identidad, antes de iniciar cualquier transacción o proceso de intercambio de información. Una de las formas más comunes en que una persona se identifica en un sistema computacional es a través de un *nombre de usuario*[3]; la forma en que demuestra que es quien dice ser, es a través de una *clave de acceso*[4].

Un mecanismo de identificación, en cuanto a su aplicación a individuos, debe permitir distinguir en forma **precisa** a una persona, a partir de los atributos que definen dicha identidad en un **contexto determinado**. Ejemplos de identificación son el RUT a nivel nacional, el username asignado en un sistema de administración centralizada, la dirección de correo electrónico en un dominio, etc. Con alta probabilidad, al interior de una organización, los nombres y apellidos de una persona son suficientes para identificar a una persona en forma precisa, pero no son suficientes en el ámbito de un país, ya que en ese universo, la duplicidad de nombres es de muy alta probabilidad.

Los mecanismos de validación o verificación de identidad persiguen comprobar que una identidad declarada es efectiva, por la vía de un procedimiento de comparación con ciertos atributos considerados como suficientes para validar dicha identidad en un contexto. Por ejemplo, para validar la identidad de una persona en Chile, se utiliza la **cédula de identidad**, siendo la tenencia de la cédula y la comparación con la foto, mecanismos de chequeo suficientes para la persona que lo recibe, y que permite entonces afirmar con muy alta probabilidad "éste es su RUT y éste es su nombre". En el caso del sistema financiero, la identificación es el número de cuenta corriente o cuenta vista (incluida en la tarjeta magnética para ser utilizada en cajeros automáticos o

[3] *Técnicamente, un "username".*
[4] *Técnicamente, un "password". El proceso completo de identificación y verificación de identidad en un sistema computacional, se conoce típicamente como "login".*

dispositivos de auto-atención), siendo el mecanismo de validación la tenencia física del plástico (que incluye los atributos de identidad) y el ingreso del PIN (*Personal Identification Number*).

Estas distinciones permiten entonces mostrar que una foto **no** es una Identidad (por ejemplo, en el caso de gemelos o personas muy parecidas, a través de la foto no es posible identificar cuál es cuál) ni el PIN (la clave de acceso) tampoco permite identificar a un usuario (los PIN se pueden duplicar, aún cuando estén asociados a cuentas corrientes distintas).

2.4 Antecedentes de Firma Electrónica en Chile y en el mundo

2.4.1 Legislación sobre Firma electrónica en el mundo

Las legislaciones que regulan las actividades relacionadas con transacciones electrónicas en el mundo presentan un aumento sostenido, siendo la firma electrónica una de las consideraciones principales en este ámbito. Es así como distintos países han establecido la creación de normas lo más homogéneas posible, que permitan asegurar que no se negará la validez de un documento firmado digitalmente. A raíz de lo anterior, diversos organismos ligados al derecho y las TIC comenzaron a discutir estas materias a partir de 1995, registrándose en la actualidad avances importantes en los marcos jurídicos respectivos.

Uno de los organismos internacionales más importantes en el desarrollo de la firma electrónica es la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL)[5], institución que ha desarrollado una estructura legal tipo para que los países la adopten en sus legislaciones internas. Los principios directores de UNCITRAL incluyen su característica de "Ley Marco" (sólo determina aspectos mínimos que debe contemplar una legislación sobre el tema), la **neutralidad tecnológica** (que las legislaciones no estén atadas a una solución específica), la **equivalencia funcional** (que a los documentos firmados electrónicamente se les asigne el mismo valor que a sus equivalentes en papel) y la **autonomía de la voluntad** (que las partes son soberanas para determinar las formas de actuar y de contratar electrónicamente).

El cuadro siguiente provee una perspectiva temporal de legislaciones de firma electrónica en el mundo.

Italia	Mayo 1997	*Puerto Rico*	Agosto 1998
Alemania	Noviembre 1997	*Colombia*	Agosto 1999
Singapur	Febrero 1999	*México*	Mayo 2000
Austria	Mayo 1999	*Estados Unidos*	Enero 2000
España	Septiembre 1999	*Perú*	Junio 2000
Inglaterra	Febrero 2000	*Ecuador*	Febrero 2001
Francia	Marzo 2000	*Venezuela*	Marzo 2001
Japón	Abril 2000	*Canadá*	Marzo 2001
Australia	Junio 2000	*Panamá*	Junio 2001
Bélgica	Julio 2000	*Brasil*	Agosto 2001
Finlandia	Enero 2003	*Argentina*	Diciembre 2001

En Chile, durante el año 2002 fue promulgada la Ley sobre "*Firma Electrónica, Documento Electrónico y Servicios de Certificación*" [6], que fue elaborada precisamente sobre la base de los principios declarados por la UNCITRAL: neutralidad tecnológica, equivalencia funcional y autonomía de voluntad.

[5] *UNCITRAL, http://www.uncitral.org/*
[6] *Ley Nº 19.799, publicada en el diario oficial el 25 de marzo de 2002.*

2.4.2 Ley chilena sobre Firma Electrónica

La Ley de Firma Electrónica en nuestro país, define el concepto de **documento electrónico**, y establece un marco legal que otorga a los actos y contratos celebrados por medios electrónicos el mismo valor y protección de que gozan los contratos y documentos celebrados en formato papel. Establece además la existencia de la **firma electrónica**, como símil a la firma holográfica (aquella "de puño y letra", que hacemos sobre papel).

En esta ley, y en el reglamento asociado[7], se establecen una serie de condiciones que deben cumplir las empresas que presten **servicios de certificación**, esto es, la generación de firmas electrónicas para personas naturales y jurídicas. Esto porque, como recurso técnico complejo, una firma electrónica no puede ser generada por una persona natural, espontáneamente, tal como se hace en los primeros años de vida de una persona, con la firma hológrafa.

Para comprender cómo se lleva a cabo este proceso técnico de "generar" una firma electrónica, debemos revisar antes algunos conceptos básicos, tanto legales como técnicos. Pero antes revisaremos algunos casos cotidianos de uso de Firma Electrónica.

2.4.3 Casos cotidianos de uso de Firma Electrónica

Ciertamente la Firma Electrónica no es un cambio radical frente a lo que actualmente hacemos en nuestra vida diaria.

Muchas personas hacen uso hoy en día de los "cajeros automáticos". En éstos, la persona introduce su tarjeta magnética por una ranura, y luego ingresa una clave numérica de cuatro dígitos. Ya que la tarjeta magnética contiene información que permite identificar a su propietario, en este proceso la persona se **identifica** frente al sistema. Con el ingreso de su clave, el sistema **verifica la identidad** de la persona. Al extraer dinero de la máquina con cargo a una cuenta corriente[8], la transacción quedará almacenada en algún punto del sistema, constituyéndose toda la información en un documento electrónico, que puede considerarse firmado con Firma Electrónica.

La mayor parte de los bancos comerciales hoy en día cuentan con un sistema automatizado de atención telefónica. Si una persona decide realizar una transacción con su banco a través del teléfono, le pedirá en primer lugar **identificarse** con su RUT, y luego **confirmar su identidad** a través del ingreso de una clave numérica. La mayor parte de las veces, el sistema advertirá que las transacciones serán almacenadas, y esto significa que todas las operaciones constituyen un documento electrónico firmado electrónicamente.

Así, podemos observar que la Firma Electrónica es parte de nuestro quehacer cotidiano, y que los nuevos esquemas de Firma Electrónica propuestos no son más que una extensión de los ejemplos anteriores.

2.5 Conceptos básicos

2.5.1 Firma Electrónica

Hasta ahora, no hemos respondido una pregunta fundamental, que es la que debiera encabezar cualquier guía de recomendaciones sobre Firma Electrónica: **¿qué es una firma electrónica?**

[7] *Reglamento de la Ley Nº 19.799, publicado en julio de 2002.*
[8] *En este ejemplo particular, este tipo de tarjeta es llamada "de débito".*

En el artículo 2º, letra f) de la Ley de Firma Electrónica, aparece la siguiente definición de Firma Electrónica:

> ***Firma Electrónica**: Cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un **documento electrónico** identificar al menos formalmente a su autor.*

Lo primero que debemos hacer notar es que una firma electrónica presupone la existencia de un documento electrónico para ser firmado. De hecho, la firma electrónica no tiene existencia individual: sólo existe asociada a un documento, que es firmado por un "autor", y recibido por un "receptor".

En el mismo artículo, letra d), se encuentra la siguiente definición:

> ***Documento electrónico**: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.*

Existe, finalmente, en la letra g), la siguiente definición:

> ***Firma electrónica avanzada**: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.*

De acuerdo con lo anterior, se puede deducir de la definición de **Firma Electrónica** y **Firma Electrónica Avanzada**, que existe algo que hemos llamado **Firma Electrónica Simple**, que no es más que aquella firma electrónica que no cumple con todas las condiciones necesarias para ser avanzada.

A continuación, se presentan características del documento electrónico, luego se presenta la firma electrónica avanzada, y luego se introducen algunas características que servirán de base para definir la firma electrónica simple en el resto del documento.

2.5.2 Documento electrónico

Documento electrónico es "*toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior*".

Detengámonos por un momento a analizar las características de un documento electrónico. Según la definición de más arriba, son cinco las características fundamentales de un documento electrónico:

1	*Que sea representación de un hecho, imagen o idea...*	
2	*Que sea representado por medios electrónicos...*	Es decir, excluye los documentos físicos (papel).
3	*Que sea almacenado...*	Es decir, si no es almacenado en alguna clase de medio, no constituye documento electrónico.
4	*Que dicho almacenamiento sea idóneo...*	Es decir, el almacenamiento del documento debe ser adecuado para el propósito del documento. Esencialmente, el almacenamiento debe ser electrónico.
5	*Que permita su uso posterior.*	Es decir, debe permitir que el documento pueda ser reutilizado cuantas veces sea necesario.

Por tanto, algunos ejemplos de documento electrónico son los siguientes:

1. Un correo electrónico almacenado en el punto de origen y/o de destino.
2. Un documento escrito en MS Word, almacenado en una carpeta compartida dentro de un dominio de MS Windows NT.
3. Un formulario ingresado a través de una página Web, siempre y cuando los datos ingresados sean almacenados en una base de datos, previo a su proceso.
4. Una bitácora de logs, es decir, un registro de acceso de escritura y lectura de un recurso compartido en la red (por ejemplo, un registro de accesos (usuario, fecha, hora y descripción de la acción realizada) a una máquina determinada, en una red Windows NT).

Algunos ejemplos que no constituyen documentos electrónicos son los siguientes:

1. Una videoconferencia realizada entre varios puntos, que no es almacenada (si no es almacenada para su uso posterior, no constituye documento).
2. Un archivo cifrado con un algoritmo simétrico, para el cual se ha perdido la llave con que fue cifrado (si no permite su uso posterior, por ninguna persona, no constituye un documento electrónico).

Resuelto este punto, debemos volver a la definición de Firma Electrónica. Una de las primeras cosas que saltan de la Ley es que existe una definición para "Firma Electrónica" y otra para "Firma Electrónica Avanzada".

2.5.3 Firma Electrónica Avanzada

Una firma electrónica avanzada es "*aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría*".

Detengámonos en el concepto de Firma Electrónica Avanzada. Las características esenciales de una Firma Electrónica Avanzada son las siguientes:

1	*Aquella firma certificada...*	Es decir, aquella firma que un organismo específico "certifica" como poseedora de ciertas características.
2	*...por un prestador acreditado...*	Es decir, el organismo que certifica la firma debe estar "acreditado", es decir, debe probar a una entidad fiscalizadora, que cumple con ciertos estándares técnicos mínimos de seguridad.
3	*...creada bajo exclusivo control del titular...*	Es decir, el titular de la firma debe poseer completo control sobre el proceso de creación de su firma.
4	*...permitiendo detectar modificaciones...*	El proceso de creación de la firma debe asegurar que la firma generada permite detectar modificaciones en los documentos firmados con ella. Esta característica se conoce como aseguramiento de "integridad".
5	*...permitiendo verificar la identidad del titular...*	De la misma forma, la firma generada sobre un documento debe permitir verificar la identidad del autor del documento. Esta característica se conoce como "autenticidad".
6	*...e impidiendo que el titular desconozca la autoría...*	Finalmente, la firma generada sobre un documento debe asegurar que el autor no niegue la autoría de dicho documento. Esta característica se conoce como "no-repudio" o "no-desconocimiento".

Esta definición, sin decirlo explícitamente, corresponde a lo que técnicamente se conoce como una "Infraestructura de Llave Pública" (*Public Key Infrastructure*, PKI). La razón por la cual no se menciona en la ley este término, es que todo lo que tenga que ver con tecnología avanza inevitablemente más rápido que la propia legislación. Es por eso que se incluyeron en la ley muchas

características técnicas, pero dejando la puerta abierta a cambiar la tecnología que subyace detrás de todo esto, a condición de que siga cumpliendo con ciertas características fundamentales.

2.5.4 Firma Electrónica Simple

Una firma electrónica (o firma electrónica "simple", para diferenciarla de la "avanzada"), es "c*ualquier sonido, símbolo o proceso electrónico, que permite al receptor de un* ***documento electrónico*** *identificar al menos formalmente a su autor*". En general, se dice que la firma electrónica "simple" está definida en forma residual: corresponde a todo aquella firma que no es avanzada.

Siendo consecuentes con esta definición, puede existir una amplia gama de tipos de firma electrónica, siendo ejemplos - con niveles crecientes de complejidad y aseguramiento - un pie de firma en un correo electrónico, la dirección de correo electrónico de un originador, el nombre del autor en la portada de un documento, el UserId único de un usuario sobre una transacción, un RUN, un código de autorización personal, etc.

Un aspecto complementario a la definición de **firma electrónica** es la naturaleza o "calidad" de la firma, la cual debería poseer atributos mínimos que aseguren un nivel mínimo de confiabilidad, dependiendo de la naturaleza, importancia y pertinencia del documento electrónico asociado.

Por ejemplo, para efectos de comunicar una decisión simple, la dirección origen de un correo electrónico podría ser considerado un mecanismo de firma electrónica suficiente para dicha operación, acompañado de los procedimientos de verificación y auditoría complementarios. No obstante, desde un punto de vista técnico, es ampliamente reconocido que la suplantación de una dirección de correo electrónico es un proceso sumamente sencillo (en forma independiente de la validez tácita que en el día a día se le da a los correos electrónicos), siendo insuficiente para ser aceptado como medio de prueba válido para otros procesos con mayores exigencias de validación de autoría.

De igual forma, en la versión digital de un documento de texto, la identificación del autor en la portada es un mecanismo de firma electrónica, pero su validez es discutible por la indudable facilidad de ser alterado el texto respectivo. Lo mismo puede ser aplicable a un registro de una conversación telefónica, donde al inicio de dicha conversación se identifique exclusivamente a los participantes por su nombre.

Debido a la ambigüedad presente en la definición antedicha, durante Mayo de 2003 se formó un Comité de Firma Electrónica Simple, como subgrupo del Comité de Normas para el Documento Electrónico[9]. En este Comité, se discutieron propuestas de modelos de Firma Electrónica Simple, para su uso y aplicación al interior de la Administración Pública. Es a partir de estos modelos propuestos y largamente discutidos, que el presente documento fue generado.

A lo largo del resto de este documento, se describen los tres modelos de Firma Electrónica Simple propuestos por el Comité de Firma Electrónica Simple. Sin embargo, para describir de manera inteligible estos modelos, es necesario que introduzcamos algunos conceptos básicos relacionados con una rama de la matemática, que fue desarrollada casi completamente durante la segunda mitad del siglo XX, y que posee muchas aplicaciones interesantes: nos referimos a la criptografía.

[9] Este Comité fue creado por el artículo 47 del Reglamento de la Ley 19.799, y tiene por principal función asesorar al Presidente de la República, en la fijación de normas técnicas que deberán seguir los órganos de la administración del Estado, para garantizar la compatibilidad de los distintos tipos de documentos electrónicos.

3. Antecedentes técnicos

3.1 Una historia ficticia: la batalla por el kuchen de frambuesa

La criptografía es una rama aplicada de la matemática discreta que trata sobre el "*arte de escribir con clave secreta o de un modo enigmático*"[10]. A pesar de que muchos le atribuyen un inicio muy antiguo, fue desarrollada en su forma práctica a partir de la segunda guerra mundial. En un estilo muy ameno, un sitio en Internet sobre *Las historias del milenio* publica un reportaje ficticio sobre cómo Alan Turing, matemático inglés, descifró en 1940 el código secreto alemán llamado Enigma[11].

Curiosamente, a pesar de ser una disciplina bastante compleja de entender, existe un sin número de historias muy amenas acerca del desarrollo de la criptografía. Es por eso que antes de comenzar queremos presentar a los personajes de nuestra historia:

Alicia: Una experta repostera e inventora de recetas. Alicia vive en Caburgua (un pueblito de la novena región, en la ribera sur del lago del mismo nombre). Es una cocinera excepcional que en sus muchos años de vida ha desarrollado alrededor de 140.000 recetas distintas de kuchen de frambuesa.
Roberto: Un hábil vendedor, dueño de una repostería ubicada en Santiago llamada "*San Benito*". Roberto probó una de las recetas de kuchen de frambuesa de Alicia en unas vacaciones y decidió que quería comercializar el kuchen en su repostería en Santiago (compartiendo los ingresos con Alicia).
Carolina: Una no-tan-experta-y-algo-envidiosa repostera, que vive en Santiago, y que es dueña de una repostería llamada "Al-frente-de-San-Benito". Carolina también probó el kuchen, pero (al revés de Roberto) quiso robar la receta para hacerla pasar como suya.

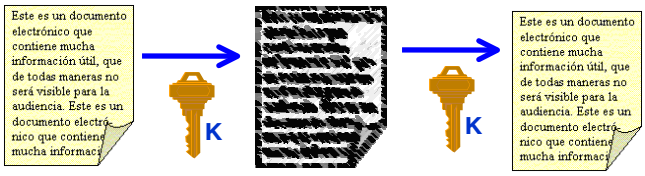
Nuestro problema, dada la situación anterior, es el siguiente: Alicia enviará a Roberto por correo una de sus muchas recetas de kuchen. Sin embargo, ambos están seguros de que Carolina intentará robar la receta en el camino. Como Carolina no pretende simplemente robarse la carta (si lo hace, al no llegar la carta Alicia y Roberto se darán cuenta de que fue robada), lo que hará será engañar al cartero para ver y copiar el contenido de la carta.

¿Pueden hacer algo Alicia y Roberto para evitar que Carolina copie la receta?

Antes de responder esta pregunta es necesario que revisemos algunos conceptos básicos de criptografía.

3.2 Algoritmos simétricos y criptosistemas de llave secreta

Un algoritmo es una secuencia de pasos para lograr algo. Un *algoritmo de cifrado simétrico* es una secuencia de pasos que permiten tomar un documento y, a través de una llave o clave, transformar ese documento y hacerlo ilegible:



[10] *Diccionario de la Real Academia Española, http://www.rae.es.*
[11] *http://www.zdnet.co.uk/athome/feature/1999/xmas/news/13.html. A pesar de que el artículo es ficticio, la historia es real. El concepto inventado por Alan Turing (llamado 'máquina de Turing'), fue un factor decisivo en la derrota de los alemanes en la Segunda Guerra Mundial.*

En el diagrama anterior tomamos un documento (por ejemplo, la "receta" de kuchen) y a través de un conjunto de pasos bien conocidos, obtenemos un documento que no es legible directamente. Para poder volver a leerlo, lo que hacemos es tomar el documento ilegible o "cifrado", aplicar los mismos pasos anteriores con la misma clave y volvemos a obtener el documento original. Esto ilustra el concepto de "algoritmo simétrico".

A partir del esquema anterior, podemos ayudar a nuestros personajes a resolver su problema. Usaremos un esquema conocido como *criptosistema de llave secreta*. En el diagrama siguiente, los objetos indicados en rojo son de "dominio público" (es decir, se supone que todo el mundo las conoce), y los objetos indicadas en azul son "privados" (es decir, se supone que son "secretos"):

En el diagrama anterior, antes de que Alicia intente enviar la receta a Roberto, ambos se ponen de acuerdo en una llave secreta común (por ejemplo, el número 123). Una vez hecho esto, Alicia puede tomar el documento, cifrarlo con la llave secreta (123) y enviarlo a Roberto. Roberto lo recibe y con la misma llave descifra el documento, obteniendo la deseada receta de kuchen de frambuesa.

Para entender el proceso anterior, podemos imaginarnos que Alicia introduce la receta dentro de un maletín, de aquellos que tienen una cerradura que consiste en rodillos con números. El maletín sólo puede abrirse cuando se colocan los rodillos en una posición única (generalmente un número de tres dígitos). Si Alicia quiere que Roberto pueda abrir el maletín y sacar la receta, es necesario que de alguna manera le haga saber cuál es el número que permite abrir el maletín. Por eso se dice que la llave es común: porque ambas personas deben conocerla para poder enviarse información.

3.3 Algunos problemas

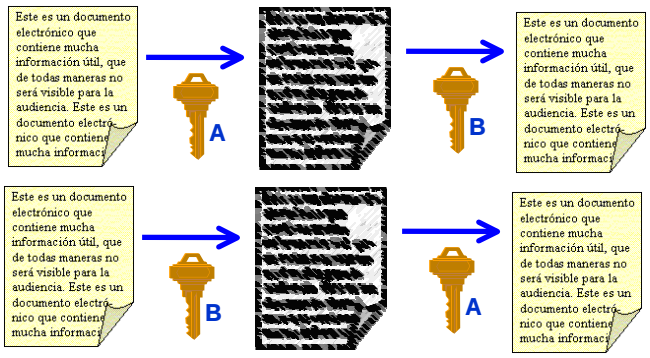
El problema obvio del esquema anterior es que Carolina puede intervenir el teléfono y escuchar la clave secreta (el número que abre el maletín) que acuerden Alicia y Roberto. Este no es un problema trivial: podemos hacer cada vez más y más seguras las llamadas telefónicas, pero debemos admitir que el teléfono, los telegramas, los correos electrónicos y las palomas mensajeras, todos son "medios inseguros" en los que no podemos confiar para el envío de información delicada.

La pregunta que surge luego de reflexionar un poco sobre el esquema anterior es: ¿es posible prescindir de una clave secreta? Es decir, ¿es posible que Alicia y Roberto intercambien la receta sin necesidad de ponerse de acuerdo en una llave secreta o una palabra clave?

3.4 Algoritmos asimétricos y criptosistemas de llave pública

Para resolver el problema anterior, es necesario que introduzcamos nuevos conceptos de criptografía.

Un *algoritmo de cifrado asimétrico* es una secuencia de pasos en la que usamos no una, sino dos llaves, de manera que podemos cifrar un documento con la primera, y descifrarlo con la segunda.



En el diagrama anterior, en la parte de arriba, vemos cómo un documento (la receta de kuchen), es cifrada con una llave A, y descifrada con una llave B. El proceso también funciona a la inversa: si se cifra el documento con la llave B, es posible descrifrarla con la llave A.

El proceso anterior funciona de manera tal que el par de llaves A y B son generadas al mismo tiempo y dependen una de la otra. Si un documento es cifrado con una de las llaves, sólo puede ser descrifrado con la otra. No es posible ocupar la misma llave de cifrado, ni reemplazar la llave de descifrado con otra. En este hecho radica gran parte de la seguridad de todos los esquemas de firma electrónica, tanto simple como avanzada existentes en la actualidad.

Con el concepto anterior, podemos resolver nuevamente el problema de nuestros personajes, a través de lo que se conoce como un *criptosistema de llave pública*:

En el diagrama anterior, Alicia y Roberto tienen cada uno un par de llaves: una llave pública (marcada con una letra roja), y una llave privada (marcada con una letra azul y encerrada en un rectángulo). Alicia toma la receta, la cifra con la llave pública de Roberto y se la envía. Roberto recibe la receta cifrada, la descifra con su llave privada, y obtiene la receta original de kuchen.

Tal como sugiere la línea roja que comunica a Alicia y Roberto, ellos aún tienen que comunicarse por teléfono, para que Roberto le diga a Alicia cuál es su llave pública (de Roberto). Sin embargo,

ya no tienen que preocuparse por que Carolina pueda estar espiando las llamadas telefónicas: el dato que se comunican por teléfono es de dominio público y no provoca ningún daño que se divulgue.

Para entender el proceso anterior, imaginemos que ahora en vez de contar con un maletín de combinación numérica única, tenemos uno que funciona con dos combinaciones distintas: una abre el maletín, y otra lo cierra. Estas combinaciones dependen una de la otra, pero no pueden ser averiguadas fácilmente una a partir de la otra. Por ejemplo, si tenemos el número 123, y seguimos una serie de pasos perfectamente establecidos, podríamos obtener el número 307 [12].

Imaginemos que el maletín puede ser programado con una combinación: una vez que cerramos el maletín con una combinación (por ejemplo, 307), éste sólo puede ser abierta con la combinación que le corresponde (123).

Para que Alicia pueda enviarle la receta a Roberto, Roberto escoge dos combinaciones (por ejemplo, 307 y 123), y le comunica a Alicia la final (307). Entonces Alicia coloca la receta en el maletín, cierra el maletín con la combinación 307, y le envía el maletín a Roberto. Como sólo Roberto sabe la combinación que abre el maletín (123), sólo Roberto podrá abrir el maletín y obtener la receta.

Dentro del ejemplo que acabamos de describir, la combinación final que Roberto le comunica a Alicia (el 307) es su **llave pública**, y la combinación inicial, que sólo Roberto conoce, es su **llave privada**.

El problema original de confidencialidad, al menos en apariencia, fue resuelto con la introducción de criptosistemas de llave privada, y luego de llave pública. Los problemas que surgen ahora son más sutiles que el anterior. Carolina ya no puede ver la receta, pero existen otras formas en que puede provocar daño.

3.5 Nuevos problemas

Ahora Carolina intenta lo siguiente: intercepta el maletín con la receta en el camino y lo reemplaza por otro maletín, con una dudosa receta de *kuchen de almejas* en su interior (¿?). Como posee la clave pública de Roberto (la combinación 307), puede incluso cifrar la receta ("cerrar el maletín con la combinación 307") para que parezca que la envió Alicia.

Frente a lo anterior, la amistad entre Alicia y Roberto se resiente: Alicia asegura que ella tiene recetas extrañas, pero definitivamente ningún *kuchen de almejas*; por otro lado, Roberto comienza a hacerse nuevas preguntas:

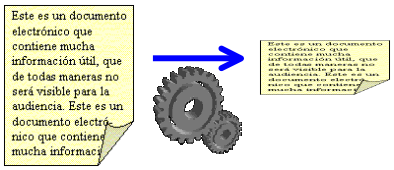
1. ¿Cómo puede Roberto estar seguro de que fue Alicia quien envió la receta?
2. ¿Cómo puede Roberto estar seguro de que Carolina no modificó la receta en el camino?
3. ¿Cómo puede Roberto asegurarse de que Alicia no niegue que envió la receta?

3.6 Algoritmos de message digest y Firma Electrónica

Para ayudar a nuestros personajes, debemos nuevamente introducir conceptos de criptografía. Un *algoritmo de hashing*[13] es una secuencia de pasos que permite generar, a partir de un documento, un trozo de información (de tamaño más pequeño). La característica especial de este pedazo de información es que si se cuenta sólo con él, no se puede obtener el documento original.

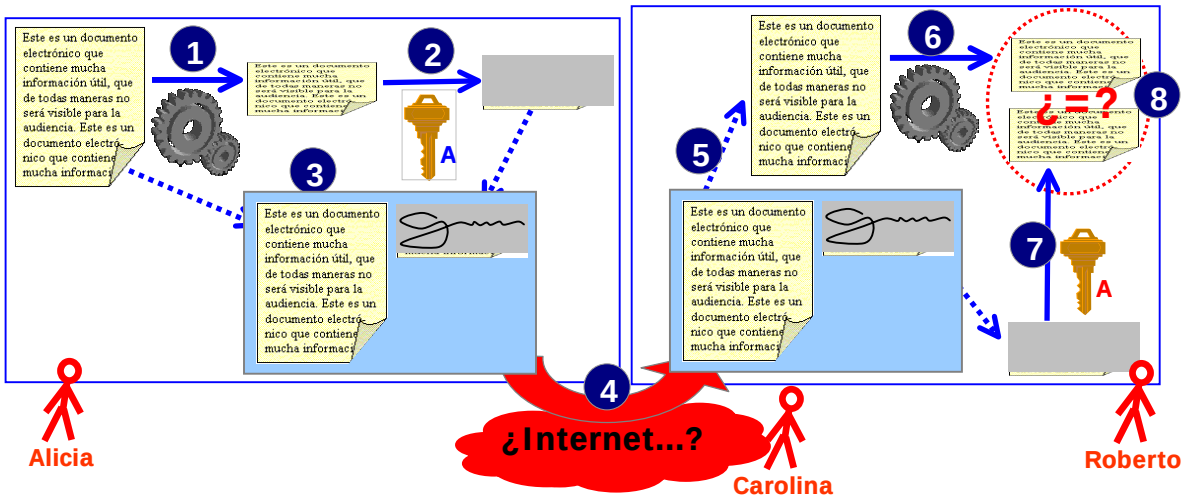
[12] *Para una explicación sobre esto, consulte el anexo 1.*
[13] *El nombre inglés completo por el que son conocidos este tipo de algoritmos es "One-way-hashing algorithms".*

Existe una clase especial de *algoritmos de hashing*, conocidos como *algoritmos de message digest*[14]. Estos algoritmos generan, a partir del documento, un "pedazo de información" cuyo tamaño es fijo e independiente del tamaño del documento original. Este "pedazo de información" sirve como "huella digital" del documento, y a partir de él no puede obtenerse el documento original. Al resultado de aplicar un algoritmo de hashing sobre un documento, le llamaremos también *message digest*.



En el diagrama anterior, se toma un documento, se le aplican una serie de transformaciones, y se obtiene su *message digest*. El *message digest* depende completamente del documento. Si el documento original es modificado (incluso en una sola letra), el *message digest* cambia. Además, si sólo poseemos el *message digest* de un documento, es imposible obtener a partir de éste el documento original.

A partir del concepto de algoritmo de *message digest*, y aplicando los conceptos anteriores, es posible ofrecerles una solución técnica a nuestros personajes, conocida como *Firma Electrónica*.



En el diagrama anterior, puede verse el esquema general relacionado con Firma Electrónica. A continuación, se explican cada uno de las operaciones:

[14] *Existen numerosos algoritmos de message digest en uso actualmente, como MD4, MD5 (desarrollados por la RSA) y SHA-1 (desarrollado por el NIST). Volveremos a esto más adelante.*

1. Alicia toma el documento y, a través de un algoritmo de hashing, obtiene un *message digest* del documento.
2. Alicia toma el *message digest* y lo cifra con su llave privada. El resultado es llamado *fingerprint* ("huella digital" del documento).
3. Alicia toma el documento original y su *fingerprint*, y los mete dentro de un "sobre" (cualquier estructura que pueda contener documentos, como un archivo XML o un email multiparte).
4. Alicia envía el sobre a Roberto, donde posiblemente pueda estarlo observando Carolina.
5. Roberto recibe el sobre, y extrae el documento y el *fingerprint*.
6. Roberto toma el documento y calcula a partir de él un *message digest*, con el mismo algoritmo que utilizó Alicia.
7. Roberto descifra el *fingerprint* contenido en el sobre, con la llave pública de Alicia (obteniendo, si todo está bien, el *message digest* del documento original).
8. Finalmente, Roberto compara los *message digest* obtenidos independientemente en los dos pasos anteriores.

Si en el último paso del proceso anterior, Roberto compara los *message digest* y estos son *exactamente iguales*, esto significa que tenemos la seguridad de que se cumplen las siguientes tres condiciones:

1. **El documento proviene indudablemente de Alicia**. Esto es así porque si Roberto pudo descifrar el *fingerprint* con la llave pública de Alicia, esto nos asegura que el *fingerprint* fue cifrado con la llave privada de Alicia.
2. **Alicia no puede negar que envió el documento**, por la misma razón anterior.
3. **Carolina no modificó la receta en el camino**. Esto no es posible porque, si hubiese modificado el documento o el *fingerprint* en el sobre, los *message digest* no hubiesen sido iguales.

Sin embargo, y pese a todos nuestros esfuerzos, volvimos a uno de nuestros problemas iniciales, la confidencialidad: ahora Carolina puede observar la receta. Y para nuestros propósitos lo importante es la información dentro del documento (es decir, las instrucciones para cocinar un *kuchen de frambuesa*) más que el documento mismo.

Sin embargo, es importante destacar que el esquema anterior resuelve las preguntas que se plantearon al final del punto anterior.

3.7 Más problemas

En el proceso surgen dos nuevos problemas. Uno de ellos es evidente y ya ha sido planteado (Carolina puede ver el documento). El otro es bastante más sutil y requiere de mayor explicación.

Dentro de su descontento Alicia no quiere tener nada más que ver con maletines ni con envíos de recetas y desea enviar de una vez sus 140.000 recetas diferentes de kuchen de frambuesa. Si quisiéramos enviar esa cantidad de documentos en un email nos daríamos cuenta de un problema que hasta ahora no habíamos enfrentado: la cantidad de recursos computacionales necesarios para

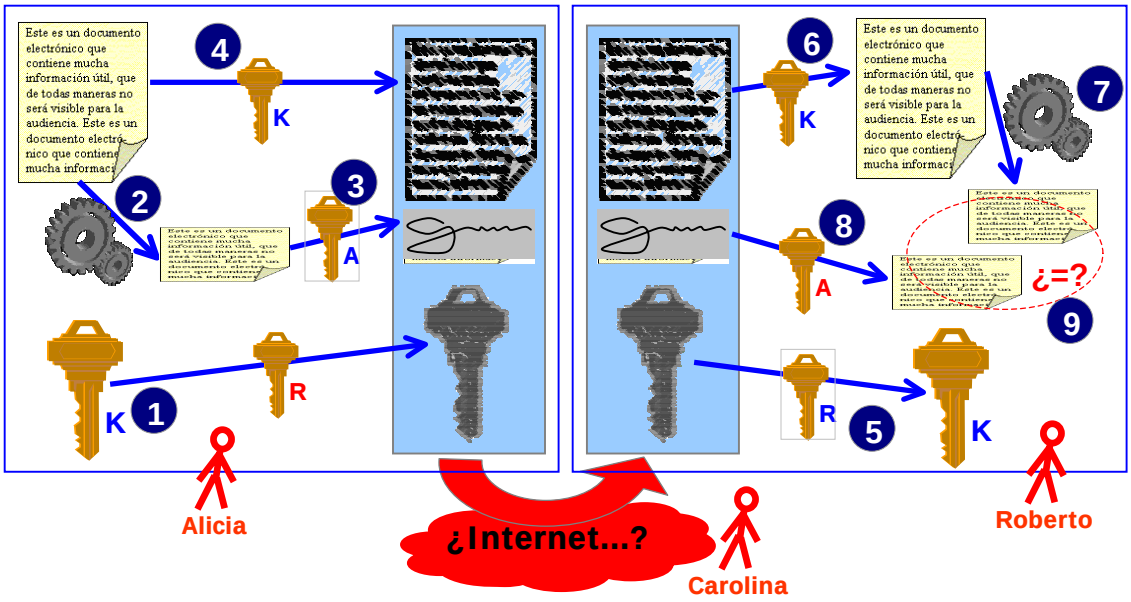
realizar el proceso completo. De alguna manera, siguiendo el ejemplo del maletín, necesitaríamos un maletín enorme para introducir tal cantidad de recetas[15].

Dado lo anterior, necesitamos un proceso que nos permita enviar eficientemente documentos a través de medios electrónicos, que no permita ver el contenido y que nos asegure las mismas tres condiciones que detallamos en el punto anterior.

Una vez más, ¿podremos resolver el problema?

3.8 Solución final: Firma Electrónica + Cifrado

Ya hemos presentado prácticamente toda la tecnología disponible, necesaria para resolver el problema final de nuestros personajes. A continuación, presentaremos una solución que resuelve todos los problemas que hemos planteado anteriormente.



En el diagrama anterior, puede verse el esquema de operación del envío de un documento firmado y cifrado. A continuación, se presenta la descripción de cada uno de los pasos:

1. Alicia escoge una *llave de sesión*, que será una llave secreta que se usará sólo una vez, y que no necesita comunicar a Roberto. Luego toma esta llave de sesión, la cifra con la llave pública de Roberto, y la introduce en un *sobre* (un *contenedor*, que permita incluir en su interior tanto la receta, como la firma y la llave).

2. Alicia toma la receta, le aplica un algoritmo y obtiene un *Message Digest* de la receta.

[15] *Los algoritmos asimétricos (o de llave pública) son, en general, mucho más complejos que los simétricos (de llave privada). En relación con la capacidad de los computadores usados para todos estos procesos, un algoritmo asimétrico consume entre 100 y 1000 veces más recursos que un algoritmo simétrico. Esto puede ser interpretado de varias maneras. Por ejemplo, puede decirse que demora de 100 a 1000 veces más, que ocupa entre 100 y 1000 veces más memoria, que ocupa entre 100 y 1000 veces más capacidad de proceso, etc. También puede ser una combinación de todas las características anteriores. Debido a esto, todas las operaciones antedichas demoran un tiempo considerablemente mayor. Por ejemplo, si todas las operaciones anteriores demorasen 0,01 segundos con un algoritmo simétrico, las mismas operaciones demorarían entre 1 y 10 segundos con un algoritmo asimétrico. Si consideramos que la mayor parte de estas operaciones se realizan a través de Internet, que requiere de cada vez mayores velocidades, se comprenderá porqué estas cantidades son consideradas como muy altas.*

3. Luego toma el *Message Digest* obtenido y lo cifra con su propia llave privada, obteniendo una firma electrónica de la receta. Luego introduce esta firma en el *contenedor*.

4. Finalmente, Alicia toma la receta, la cifra con la *llave de sesión*, y la introduce en el *contenedor*; acto seguido, envía el sobre completo a Roberto, donde pudiera estar observándolo Carolina.

5. Roberto recibe el sobre, extrae la *llave de sesión* cifrada y la descifra con su propia llave privada.

6. Luego, Roberto extrae la receta cifrada, y la descifra con la *llave de sesión* que acaba de obtener en la paso anterior.

7. Roberto toma la receta que acaba de obtener, y calcula un *Message Digest* de la receta, con el mismo algoritmo que utilizó Alicia. Este será usado posteriormente para verificación.

8. Roberto extrae la firma electrónica generada por Alicia, y la descifra con la llave pública de Alicia. Obtiene entonces otro *Message Digest*, que usará para compararlo con el obtenido en el paso anterior.

9. Finalmente, Roberto compara los *message digest* obtenidos en forma independiente en los dos pasos anteriores.

Con el esquema anterior, hemos resuelto todos los problemas que nos hemos planteado a lo largo de la historia de nuestros personajes. Si en el paso Nº9, los *Message Digest* comparados son iguales, entonces podemos asegurar las siguientes condiciones:

1. **Autenticación**: Es posible verificar la identidad de las persona que emitió el documento firmado (en este caso Alicia).
2. **Integridad**: Es posible verificar si el documento enviado fue o no modificado durante su transporte.
3. **No-repudio**: Es posible asegurar que la persona que envió el documento (Alicia), efectivamente participó en el proceso de generación y firma del documento.
4. **Confidencialidad**: Los documentos enviados no serán vistos por personas distintas del emisor (Alicia) y el receptor (Roberto).

Sin embargo, aún existen algunos problemas de los que Carolina puede sacar ventaja.

3.9 Carolina intenta nuevos métodos...

Dados todos los esquemas anteriores, sigue persistiendo un problema que no se había discutido hasta ahora: el del almacenamiento y comunicación de las llaves públicas. Cuando Alicia quiere enviarle a Roberto una receta, tiene que llamarlo por teléfono (o enviarle un correo, o reunirse con él) para pedirle su llave pública. A pesar de que esta es información de conocimiento público, de todas maneras representa un problema del cual un observador podría eventualmente sacar provecho.

Carolina decide entonces intervenir el teléfono, una vez más, y hacerse pasar por Roberto con un complejo aparato para falsear la voz. Cuando Alicia le pide a Roberto su llave pública, Carolina

(haciéndose pasar por Roberto) envía a Alicia su propia llave pública. Como resultado, todos los documentos que Alicia cifre con la llave pública de Carolina, sólo podrá descifrarlos Carolina.

Frente a este peligro, Alicia y Roberto deciden recurrir a la ayuda de una empresa externa. Esta empresa, llamada HAL, guardará las llaves públicas de Alicia, Roberto y de cualquier persona que así lo solicite. Cuando cualquier persona se comunique con la empresa queriendo saber la llave pública de un tercero, la empresa informará de esta llave.

A pesar de que este nuevo esquema parece contar con el mismo problema (Carolina puede intervenir la comunicación entre HAL y Alicia o Roberto), permite centralizar la comunicación, transporte y almacenamiento de llaves y, por tanto, permite atacar de mucho mejor manera el problema de la seguridad.

Frente a la aparición de HAL, Carolina centra sus esfuerzos en esta empresa, e intenta dos cosas:

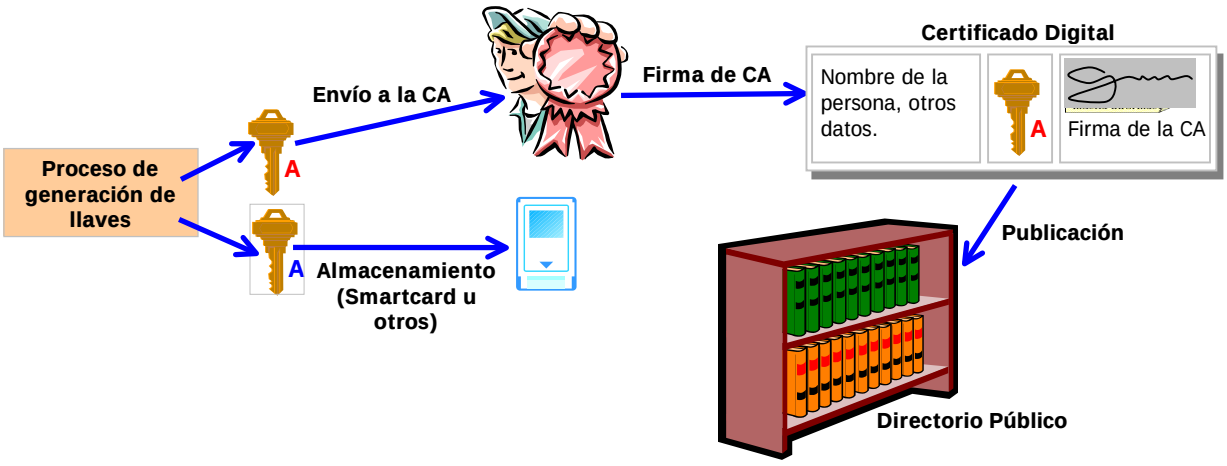
1. Crackear[16] los servidores de HAL para destruir la llave pública de Roberto y Alicia.
2. Incendiar las instalaciones de HAL para lograr el mismo objetivo.

La pregunta obvia es: ¿Se puede solucionar esta vez el problema?

3.10 Infraestructura de llave pública (PKI)

3.10.1 Esquema de una PKI

La forma de resolver los últimos problemas planteados se relaciona con un concepto muy reciente conocido como Infraestructura de Llave Pública, o PKI (por sus siglas en inglés, *Public Key Infrastructure*). Dentro de esta infraestructura lo que hemos conocido como *llave pública* y *llave privada* es llevado un paso más allá con la aparición de *certificados digitales*.



En la figura anterior, se esquematiza lo que corresponde al esquema de generación de un par de llaves para una persona, y la generación del certificado digital correspondiente, a partir de la llave pública de la persona.

3.10.2 Entidades que interactúan en una PKI

En PKI existen una serie de entidades que interactúan para asegurar un nivel mínimo de confiabilidad. Estas son:

[16] *"Crackear" (anglicismo) significa "ingresar" ilegalmente a un sistema informático, con la intención explícita de provocar daño.*

1. **Prestadoras de servicios de certificación**: Son aquellas empresas que prestan servicios de certificación, incluyendo la generación de certificados digitales y mantención de un repositorio de certificados digitales de acceso público.
2. **Entidad acreditadora**: Es la entidad encargada de fiscalizar a las prestadoras de servicios de certificación, para asegurarse de que cumplen con los estándares tecnológicos mínimos necesarios para garantizar la confidencialidad y correcta generación de ellos.
3. **Personas**: Todas aquellas personas que adquieren para sí un certificado digital, sean naturales o jurídicas.

Dentro del marco legal de nuestro país la entidad acreditadora, de acuerdo con la Ley vigente de Firma Electrónica, es la Subsecretaría de Economía, Fomento y Reconstrucción[17]. De esta manera, es dicha Subsecretaría la encargada y responsable de acreditar que las distintas empresas chilenas que presten servicios de certificación cumplan tanto con los estándares técnicos mínimos exigidos, como con las condiciones establecidas en la Ley y en el Reglamento de Firma Electrónica.

3.10.3 Certificados digitales

Un **certificado digital** es un documento electrónico que pertenece a una persona (natural o jurídica), que fue generado bajo medios tecnológicos controlados y que contiene ciertos datos básicos. De acuerdo con el estándar X.509 versión 3, los atributos presentes en un certificado digital deben ser los siguientes:

- Versión (v3)
- Número serial.
- Algoritmo de firma utilizado.
- Período de validez del certificado.
- Extensiones (opcional).
- Nombre de la persona.
- Llave pública de la persona.
- Identificador único de la persona.
- Nombre de la entidad certificadora.
- Identificador único de la entidad certificadora.
- Firma de la entidad certificadora.

De acuerdo con la Ley chilena de Firma Electrónica, un certificado digital debe contener al menos los siguientes elementos[18]:

1. Un identificador único del certificado (un número de serie),
2. La llave pública de la persona propietaria del certificado,
3. Datos adicionales de la persona: nombre completo, email y RUT,
4. Datos oficiales de la institución que generó este certificado: nombre o razón social, email y RUT,
5. La firma electrónica de la entidad que generó el certificado,
6. Dos fechas, que indican el período de validez del certificado (fecha de inicio de validez y fecha de término de validez).

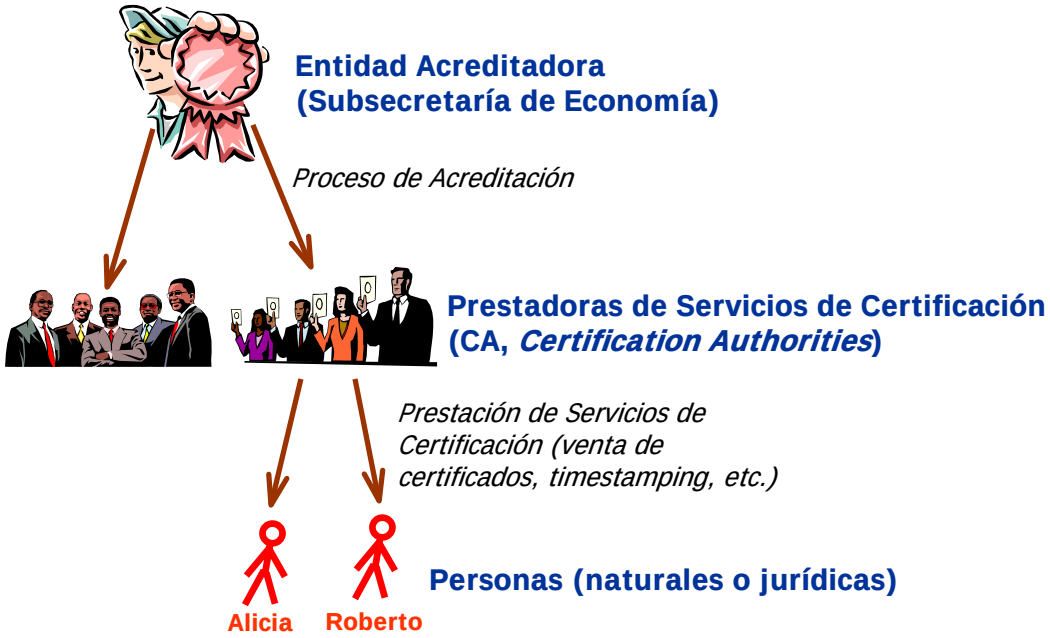
Así, la empresa prestadora de servicios de certificación tiene la obligación de informar a todas aquellas personas que lo requieran el certificado digital de una persona específica.

[17] *Esto se establece en la letra e) del artículo 2 de la Ley. Más información en http://www.entidadacreditadora.cl.*
[18] *Estas condiciones están contenidas en el artículo 15 de la Ley Nº19.799, de Firma Electrónica. Se agrega a la lista exclusivamente la llave pública de la persona, puesto que sin ella el certificado no tiene sentido..*

Por otro lado, la llave privada de la persona es manejada en algún medio que sea "de exclusivo control del propietario". Normalmente esto significa que es almacenada en un medio físico permanente como una SmartCard (tarjeta inteligente, similar a una tarjeta de crédito, que puede ser leído por un aparato especial), de donde puede ser recuperada con hardware especialmente construido para tal propósito, mediante el ingreso de una clave adicional. A esta clave de seguridad, generalmente se le conoce como *passphrase*.

3.10.4 PKI en Chile

De acuerdo con la Ley de Firma Electrónica y su respectivo reglamento, la forma en que se ha organizado la PKI en Chile corresponde al siguiente esquema:



En Chile, la Subsecretaría de Economía cumple el papel de Entidad Acreditadora; es decir, es la entidad que por Ley audita y fiscaliza a las distintas instituciones que deseen prestar servicios de certificación "oficiales". Debemos hacer hincapié en lo de "servicios de certificación oficiales" pues cualquier institución puede ofrecer, comercialmente o no, certificados digitales bajo la tecnología PKI, sin necesidad de contar con autorización explícita para ello. Sin embargo, para que los documentos firmados con estos certificados sean considerados legalmente firmados con firma electrónica avanzada, la institución debe haber pasado por el proceso de acreditación oficial de la Subsecretaría de Economía.

Una vez que una institución determinada ha sido acreditada por la Subsecretaría de Economía, puede vender certificados digitales a personas naturales o jurídicas[19].

[19] *Para más información sobre la Entidad Acreditadora o sobre las empresas acreditadas por Ley para prestar servicios de certificación, ver http://www.entidadacreditadora.cl.*

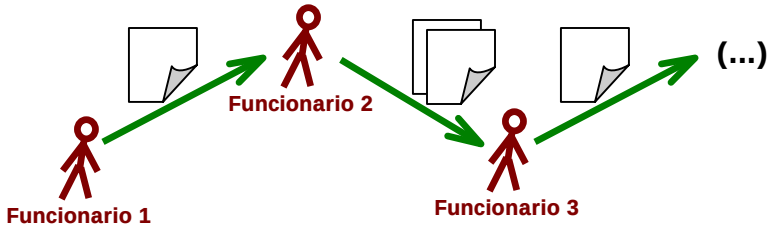
4. Modelos de Firma Electrónica Simple

4.1 Introducción

4.1.1 Fundamento de los modelos de Firma Simple

La mayor parte de los procesos llevados a cabo al interior de la Administración Pública consisten en cadenas o flujos de documentos, donde en ciertos puntos específicos se realizan modificaciones diversas sobre los documentos. Estas modificaciones pueden corresponder a operaciones sobre el contenido de los documentos (agregar/modificar/eliminar información), o bien realizar operaciones sobre los documentos (firmar el documento, autorizar una transacción, etc.).

Estos procesos deben llevarse a cabo de una determinada manera, en un orden específico; sin embargo, en la inmensa mayoría de los casos la tecnología que se utilice no condiciona este orden específico. Dicho de otra manera: el proceso se desarrolla de la misma forma, no importa si los documentos son transportados en papel físicamente de una oficina a otra, si son transmitidos por señales de humo, o si son documentos electrónicos intercambiados a través de alguna tecnología específica.



La Firma (ya sea porque autoriza algo, toma conocimiento de algo o da fe de algo) es una de las operaciones presentes en tales procesos. La descripción de modelos de Firma Electrónica Simple apunta a ofrecer maneras de replicar la firma manuscrita de documentos, al interior de procesos desarrollados por una institución.

4.1.2 Correspondencia entre operaciones físicas y técnicas

Antes de implementar cualquier clase de proceso a través de una tecnología, es absolutamente indispensable estudiar el proceso y representarlo de alguna manera gráfica, lo que nos permitirá estudiar qué operaciones se requieren sobre la información, y cómo cada una de estas operaciones puede interpretarse en función de los medios técnicos disponibles.

La explicación sobre cómo representar modelos de manera gráfica va más allá de los propósitos de este documento, pero existe abundante literatura al respecto tanto en libros técnicos como en Internet.

A modo de ejemplo, a continuación se listan algunas de las operaciones típicas que se realizan sobre un documento dentro de un proceso determinado:

Proceso en papel	Proceso electrónico
... el documento es firmado de puño y letra ...	*... el documento es firmado a través de algún mecanismo de firma electrónica ...*
... el documento es enviado a su destinatario ...	*... el documento es transmitido a través de algún mecanismo electrónico (email, servicio http, servicio FTP, etc.) a su destinatario...*

... el documento es introducido en un sobre cerrado para evitar que sea leído durante su transporte ...	*... el documento es encriptado para evitar que pueda ser leído durante su transmisión ...*

Es necesario hacer notar que, a la hora de transformar un proceso en electrónico, y de introducir firma electrónica de los documentos intercambiados en el proceso, es absolutamente necesario tener claridad acerca de los detalles del proceso mismo: **qué** se hace, **cuándo** se hace, **cómo** se hace, **porqué** se hace.

En la descripción de los modelos de firma electrónica simple contenidos en este documento y las guías de implementación asociadas, se describe sólo la forma de implementar **un paso** al interior de un proceso: esto es, el envío de un documento electrónico entre un emisor y un receptor. Para encadenar procesos completos, es necesario que cada institución realice un análisis de sus procesos y detalle cada paso por separado, identificando qué operaciones son requeridas en cada punto.

4.1.3 Introduciendo firma electrónica simple a un proceso

Tal como se menciona en el punto anterior, el explicar métodos para diagramar y analizar procesos escapa a los objetivos perseguidos con esta guía. Sin embargo, se entrega a continuación una serie de pasos genéricos, exclusivamente a modo de orientación en la implementación de un proceso determinado, con alguno de los modelos de firma electrónica simple:

1. **Catastrar los procesos con intercambio de documentos electrónicos.**

   Es necesario realizar un catastro de todos aquellos procesos dentro de la institución que requieren de intercambio de información a través de documentos, ya sea bajo la forma de oficios, decretos, resoluciones, memorandums, licitaciones, bases, especificaciones, etc., o cualquier otro documento que sea intercambiado en formato papel.

2. **Escoger un proceso susceptible de ser digitalizado.**

   La idea en este punto es analizar qué procesos son digitalizables (es decir, cuáles son susceptibles de ser transformados para reemplazar los documentos en papel por documentos electrónicos), y escoger cuál de ellos será implementado a través de alguno de los tres modelos de firma simple descritos en este documento. Esta decisión debe tomarse basada en criterios como los siguientes:

   a. En qué partes del proceso se requieren “autorizaciones”, “vistos buenos”, “toma de conocimiento” o cualquier otra operación que pueda ser homologada como la firma electrónica de una persona determinada,
   b. Cuántas personas deben intervenir en el proceso,
   c. Si esas personas cuentan con computadores para su trabajo diario,
   d. Etc.

3. **Escoger la tecnología a utilizar.**

   En este punto, debe escogerse la tecnología a utilizar para implementar el proceso escogido, basado en los recursos disponibles y posiblemente en otros criterios.

4 **Planificar la digitalización del proceso.**

Es en este punto en que se debe planificar la digitalización del proceso, de acuerdo con los recursos disponibles, la cantidad de personas involucradas, etc. Algunos de los puntos que deberían estar presentes en cualquier planificación son (en el orden en que deberían realizarse):

a. Formación o adquisición de las capacidades necesarias en el área de informática (o en el grupo de personas que realice soporte informático al interior de la institución),
b. Instalación de la plataforma tecnológica necesaria,
c. Capacitación a todos los usuarios finales, que incluya:
    i. Cómo firmar y/o encriptar a través de la tecnología escogida,
    ii. Cómo verificar la firma de una persona determinada,
    iii. Cómo cambia el proceso que está siendo digitalizado, al ser implementado a través del modelo de firma escogido.

Se sugiere que el proyecto completo de implementación no dure más de 6 meses.

5 **Ejecutar la planificación y evaluar la ejecución.**

Dentro de la ejecución, es necesario no olvidar la evaluación de todo el proceso de digitalización. Como resultado de la evaluación, siempre es deseable contar con métricas que indiquen de manera objetiva cómo cambió el proceso que fue intervenido.

De acuerdo con los pasos anteriormente sugeridos, es posible (a grandes rasgos) implementar un proyecto genérico de firma electrónica simple, en cualquiera de los tres modelos sugeridos.

4.1.4 Criterios orientadores respecto al uso de Firma Electrónica

El artículo 39 del Reglamento de Firma Electrónica define claramente una orientación al interior de la administración del Estado: ***privilegiar el uso de la Firma Electrónica Simple en los Documentos Electrónicos, excepto en aquellos casos claramente establecidos***.

En los diversos espacios e instancias de discusión del cuerpo normativo, y siendo un consenso entre los diversos especialistas involucrados en el proceso, el uso de la Firma Electrónica al interior de los Órganos del Estado debe responder a los siguientes criterios:

1. Generar modelos operacionales sencillos, que privilegien la firma electrónica simple, cautelando niveles mínimos de seguridad, dependiendo del tipo de documento y su importancia,
2. Exigir al mundo electrónico protecciones a lo menos equivalentes a las operaciones en el mundo del papel, que combinen adecuadamente implementaciones tecnológicas junto con procedimientos acordes a los requerimientos,
3. Fomentar una rápida masificación, considerando el universo de usuarios de la administración pública,
4. Tender a la automatización de procesos, simplificando los flujos de información y disminuyendo la “confianza en el papel” de muchos procesos existentes.

Los modelos de Firma Electrónica Simple descritos en este capítulo, fueron originalmente propuestos por el Proyecto de Reforma y Modernización del Estado, y discutidos al interior del Comité de Firma Electrónica Simple. Los criterios básicos para el diseño de estos modelos fueron los siguientes:

1. Un modelo debe ser lo suficientemente sencillo como para poder ser implementado sin una preparación técnica elevada, y sin la necesidad de contratar a consultores externos al servicio público en cuestión.
2. Un modelo no debe requerir de inversiones elevadas, ni en infraestructura tecnológica, ni en software, ni en capacitación, ni en otros recursos. Debe permitir ser implementado con los recursos que ya poseen los servicios.
3. Un modelo debe proveer de un nivel de seguridad similar o igual, en cuanto a las tres características deseables en una firma electrónica avanzada: autenticación, integridad y no repudio.

A continuación, se describen los tres modelos propuestos de Firma Electrónica Simple.

4.2 Primer modelo: Firma Electrónica Indirecta (username/password)

4.2.1 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.

Este conjunto de condiciones requeridas en una plataforma, es satisfecho por numerosas arquitecturas posibles, y puede por tanto ser implementada de muchas formas diferentes:

a) Una red Microsoft Windows NT, donde existe una carpeta pública (compartida), donde se guardan documentos públicos de la organización (imaginería, cartas tipo, circulares, archivos comunes, autorizaciones, memorándums, etc)., el acceso a esta carpeta es bajo username y password de lectura y escritura, y existe algún software instalado por el administrador de la máquina que contiene físicamente el recurso compartido, que le permite registrar los accesos al recurso.
b) 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.
c) 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).

d) La intranet de un Servicio Público, donde se ingresa un identificador ("username") y clave ("password") para ingresar, y donde se provee la facilidad de subir o bajar archivos, también constituye un ejemplo al respecto.

El último ejemplo mencionado merece atención especial, pues presenta numerosas ventajas sobre las anteriores:

1. Es fácilmente accesible, y no requiere de hardware especial (puede incluso ser accesada desde fuera de la institución[20]),
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 https, esto otorga seguridad a las transacciones de documentos).

4.2.2 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.

Para implementar este primer modelo de Firma Electrónica Simple, se recomienda fuertemente utilizar la intranet de la institución. Si no se cuenta con una intranet, se recomienda fuertemente construir una.

Para detalles de implementación de este modelo, consultar el documento "*Guía 1: Implementación de Modelo de Firma Electrónica Simple Username/Password*", en la última versión disponible.

4.3 Segundo modelo: Firma Electrónica en E-mail

4.3.1 Descripción del modelo

Este modelo consiste en el envío de un email firmado (y posiblemente cifrado), en el cual se adjuntan uno o más documentos, como *attachments*. En este modelo, existe un emisor del documento (que no necesariamente es su autor) y un receptor del documento.

1. Si el email va sólo firmado, es necesario que el emisor disponga de una llave privada para firmarlo,
2. Si el email va firmado y cifrado, es necesario que el emisor disponga de una llave privada para firmar, más la llave pública del receptor para cifrar,
3. Para que el emisor pueda confirmar la identidad del firmante, es necesario que disponga de la llave pública del emisor.

Así, para establecer una comunicación bidireccional, en la práctica es necesario que ambos interlocutores cuenten con un par de llaves, una pública y una privada.

[20] 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.

Para implementar este modelo, es necesario que el Servicio Público que desee implementarlo cuente con los siguientes elementos:

1. **Un par de llaves** (una pública y una privada) **para cada funcionario**.
2. **Un repositorio público**, con todas las llaves públicas de los funcionarios. Este puede ser implementado a través de la Intranet del Servicio, o bien en una carpeta compartida (con permisos de sólo lectura) a la que todos tengan acceso.
3. **Una dirección de correo institucional**, que sirva como repositorio de todos los emails firmados y/o cifrados. Por ejemplo, repositorio@minsegpres.cl.

Al comienzo del proceso de implementación del modelo, debe pedírsele a cada funcionario que genere personalmente un par de llaves, y que coloque su llave privada en un directorio no compartido, ojalá sin permisos de lectura ni escritura. Una vez hecho esto, debe enviar su llave pública al administrador de sistemas de la institución (o al Director de Informática, o al encargado de computación de la organización), para que la coloque en la Intranet y todos tengan acceso a ella.

La dirección de repositorio sirve para respaldar todos los emails firmados y/o cifrados. Para esta casilla también es necesario generar un par de llaves, y la llave pública debe colocarse en la Intranet, de manera que todos puedan enviar email al repositorio como si se tratase de una persona real. La llave privada del repositorio debe ser guardada y puesta a disposición del directivo del Servicio Público, de manera que sólo él/ella tenga acceso a los documentos firmados enviados por los funcionarios del Servicio, en caso de ser necesario.

4.3.2 Implementación del modelo

Para detalles de implementación de este modelo, consultar el documento "*Guía 2: Implementación de Modelo de Firma Electrónica Simple en Email*", en la última versión disponible.

4.4 Tercer modelo: Firma Electrónica en Documento

4.4.1 Descripción del modelo

Este modelo consiste en el envío de documentos electrónicos, no necesariamente a través de email[21], que contienen una firma dentro de su estructura (ver 2.2.3).

Para implementar este modelo, es necesario (igual que en el caso anterior), que cada servicio público implemente una manera de generar pares de llaves para cada uno de sus funcionarios. Sin embargo, no es necesario contar en este caso con plug-ins instalados sobre los clientes de correo, pues no necesariamente hay un envío de documento a través de email, y para efectos de la firma, sólo es necesario calcular una firma apropiada al documento, e incrustarla en el documento.

Por ejemplo: un documento que contenga la descripción de un proyecto, generado originalmente en MS Word, puede ser transformado al formato PDF 5.0 a través del software Adobe Acrobat 6.0 Professional. Una vez hecho esto, el PDF es firmado con la llave privada del emisor, la firma es incluida en el documento, y el documento es enviado vía FTP (protocolo de transferencia de archivos) a un receptor interesado en él.

[21] *El envío de documentos electrónicos podría ser también a través de protocolos como ftp, ssh, u otros.*

4.4.2 Implementación de modelo de Firma Electrónica en Documento

Actualmente, los documentos que aceptan el incluir dentro de ellos una firma electrónica simple, son los documentos de Adobe Acrobat (conocidos como PDF, de *Portable Document Format*), y los documentos de la suite Microsoft Office, a partir de la versión 2000 en adelante (esto es MS Word, MS Excel y MS PowerPoint). Sin embargo, para incluir firmas electrónicas al interior de estos documentos, es necesario contar con certificados digitales generados internamente, dentro de la institución donde se implementará el modelo.

Para detalles de implementación de este modelo, consultar el documento "*Guía 3: Implementación de Modelo de Firma Electrónica Simple en Documento*", en la última versión disponible.

5. Buenas prácticas de seguridad

5.1 Introducción

Existen numerosas razones por las cuales todo Servicio Público debiera preocuparse por la seguridad de sus sistemas computacionales y sus instalaciones, no importa qué modelo de Firma Electrónica Simple desee implementar. Sin embargo, contra lo que se cree mayoritariamente, la seguridad de un sistema computacional no depende tanto de la capacidad de los algoritmos de cifrado o de la cantidad de cortafuegos (*"firewalls"*) que protejan la red de la institución. Tiene una dependencia mucho mayor de la gestión en seguridad realizada al interior de la organización.

A pesar de que la seguridad en sí misma no ofrece un valor agregado a las operaciones o transacciones que realiza una institución, es necesario pensar en medidas de seguridad en tanto la posibilidad de perder algo valioso sea mayor. Dicho de otra manera, **la inversión en seguridad depende directamente del valor de lo que se esté protegiendo**. Si cierta información no tiene un valor grande para la institución, no vale la pena realizar grandes inversiones para protegerla. Si por el contrario, la información es de vital importancia para la institución o para el país, es lícito pensar en un gran nivel de seguridad para proteger la integridad o confidencialidad de dicha información.

Es en este mismo sentido que se recomienda **no exigir más al medio electrónico de lo que se exige al papel**.

En el mundo bien conocido del papel entregamos o enviamos ciertas cosas sin necesidad de identificarnos formalmente o de identificar al autor. Por ejemplo, a veces queremos enviar un documento trivial (un artículo de prensa, una referencia a un libro, etc.) a una persona sólo para su conocimiento. Lo que hacemos es dejarlo sobre su escritorio con una pequeña nota que dice "para su información". Muchas veces no firmamos estas notas, sólo colocamos nuestro nombre o iniciales en él. Pues bien: si para este tipo de intercambios de información no requerimos de una verificación exhaustiva de identidad, no deberíamos requerirla tampoco si el intercambio se produce electrónicamente (por ejemplo, si en vez de dejar el artículo impreso sobre el escritorio, simplemente lo enviamos por email).

Una vez establecido lo anterior, podemos decir que la seguridad la dividimos en dos tipos: **electrónica** (toda aquella relacionada con seguridad de datos, redes y transacciones) y **no-electrónica** (aquella relacionada con la gestión que se realiza sobre los recursos físicos y las personas de la organización).

Para diseñar una estrategia de seguridad se debe tener en cuenta la actividad que se desarrolle; sin embargo, se pueden considerar los siguientes tres pasos generales:

1. Crear una política global de seguridad,
2. Realizar un análisis de riesgos,
3. Aplicar las medidas correspondientes.

En este capítulo se analizan algunas recomendaciones básicas en torno al tema de la seguridad electrónica y no-electrónica, sin ahondar en marcas de sistemas específicos, comerciales o no. Para recomendaciones de seguridad en plataformas específicas, deben consultarse guías anexas a este documento.

5.2 Implementación de políticas de seguridad

El establecimiento de políticas debiera ser el primer paso a seguir en una organización para entrar en un ambiente de seguridad, puesto que reflejan la voluntad de hacer algo que permita normar el uso de los recursos, prevenir fugas de información, detener un posible ataque antes de que éste suceda (proactividad) y por ende proteger el activo más importante, la información.

Las políticas de seguridad de una organización, deben cumplir con una vieja regla del área de la calidad: deben escribirse. Pues lo no escrito, en términos prácticos, "*no existe*". Una de las actividades primordiales de toda área o gerencia de informática debiera ser la redacción de un *Plan de Seguridad*, documento que debe ser de conocimiento de todas las personas que pertenecen a la organización.

En este documento, las organizaciones elaboran un marco teórico que aclare y estandarice conceptos para las personas que pertenecen a la organización. Este documento debiera incluir:

a. Alcance; identificar los sistemas que estarán cubiertos por la Política, y los usuarios a los que estará destinada (por ejemplo, políticas generales destinadas a toda la institución y políticas específicas para un sistema o grupo de personas).
b. Objetivos y descripción clara de los elementos involucrados en su definición.
c. Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
d. Violación de la Política; definición de violaciones y de las consecuencias del no-cumplimiento de la política.
e. Responsabilidades de los usuarios con respecto a la información.
f. Conceptos generales; terminología que será utilizada en el desarrollo de la Política y que no debe ser susceptible de ambigüedad alguna por parte de los usuarios (por ejemplo, servicios, permisos, acceso, cuenta, password, etc.).

Las políticas de seguridad deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones. Es necesario transmitir a los usuarios el por qué son importantes éstos recursos o servicios, manteniendo siempre un lenguaje "común", libre de tecnicismos y términos legales que impidan una comprensión clara de las políticas.

Además, se debe especificar la(s) instancia(s) encargadas de la ejecución de las políticas (Área de Seguridad, Comité de Seguridad, etc.), sus atribuciones y responsabilidades a la hora de aplicar sanciones.

5.3 Ítems a considerar en seguridad

En los siguientes puntos, se pretende entregar una lista de ítems relacionados con seguridad, a modo de ejemplos, sin la intención de ésta sea una lista comprensiva y extensa sobre seguridad.

Todo plan de seguridad debería preocuparse de al menos dos líneas distintas: seguridad de recursos físicos (es decir, seguridad de acceso físico a instalaciones, planes de contingencia frente a catástrofes naturales, etc.), y seguridad de recursos digitales (como asegurar los recursos digitales frente a alteraciones casuales o intencionadas).

A continuación, sólo para orientar la creación de un *Plan de Seguridad*, se entregan algunos puntos acerca de los cuales es necesario preocuparse.

5.3.1 Seguridad en recursos físicos

Todas las organizaciones debieran incluir en su *Plan de Seguridad* los siguientes temas:

1. **Acceso físico de personas a las instalaciones**:
   a. Acceso a computadores conectados a la red.
   b. Acceso físico no autorizado a la red ("pinchar la red").
   c. Acceso físico a servidores críticos: Email, Web, DNS, etc.
   d. Acceso físico a alimentación de energía, distribución de datos, centrales telefónicas, salidas a Internet, etc.

2. **Posibilidad de catástrofes naturales, o de incidentes producidos intencionalmente**:
   a. Posibilidad de incendios, inundaciones, sismos, erupciones u otros incidentes de origen natural.
   b. Posibilidad de fenómenos naturales que, sin ser catástrofes, producen daños severos (filtraciones de lluvia sobre equipos eléctricos, sobrecargas o apagones ("*black-outs*") por tormentas eléctricas, corrosión por humedad o insectos, etc.).
   c. Posibilidad de atentados terroristas o de ataques malintencionados, huelgas y otros.

5.3.2 Seguridad en recursos digitales

Todas las organizaciones debieran incluir los siguientes elementos dentro de su Plan de Seguridad:

1. **Control de Acceso a la Red**: Es decir, control de acceso (conexión) de todos aquellos usuarios que pertenecen a la organización, o que por su actividad debe concedérseles un acceso temporal a los recursos de la red. Dentro de este ítem, deben considerarse elementos como:
   a. Modelo de permisos de acceso, para dar a los usuarios permisos para acceder o alterar sólo aquella información que necesitan o para la que están autorizados.
   b. Sistemas de Detección de Intrusos (IDS), para prevenir el acceso de personas no autorizadas a los recursos de la red.
   c. Autenticación (certificados digitales, passwords, biométricos, tarjetas inteligentes) de los usuarios que pertenecen a la organización.
   d. Firewalls, que filtren los accesos humanos y computacionales a los recursos de la red.
   e. Routers, Túneles o VPN's, que dirijan el tráfico de la red de acuerdo con su topología y con las necesidades de conexión.
   f. Protocolos.
   g. Registro (logs) de las acciones realizadas sobre un sistema, especialmente de accesos a los recursos críticos de la red, incluyendo respaldo adecuado de los logs generados.

2. **Protección y Resguardo de la Información**: que incluye la generación de mecanismos que permitan autentificar a los usuarios, cuando sea necesario responsabilizarlos por alguna acción o información generada o enviada. Dentro de este ítem, deben considerarse elementos como Firma Electrónica por parte de los usuarios, cifrado de documentos, etc.

3. **Respaldos**: que se refiere en términos generales al respaldo de toda clase de información generada en un sistema. Algunos elementos a considerar:
   a. Políticas de respaldo de la información de usuarios,
   b. Respaldo de bases de datos,
   c. Respaldo de información de monitoreo de sistemas (logs).

1. Anexo: Ejemplo de obtención de una llave a partir de otra

El siguiente es un ejemplo superficial sobre cómo obtener una combinación a partir de otra, de acuerdo con la situación imaginaria descrita en el capítulo 3.

La obtención de una llave a partir de otra corresponde siempre a un algoritmo más o menos complicado. En nuestro caso, hemos simplificado el proceso imaginándonos que las llaves tienen 3 dígitos de largo, y que corresponden a las combinaciones de rodillos que pueden abrir un maletín.

Si tenemos una combinación inicial de tres dígitos, la otra combinación podría obtenerse de la siguiente manera:

1. Tomamos la combinación inicial, y la elevamos al cuadrado, al cubo y a la cuarta potencia,
2. Sumamos todos los números obtenidos, incluyendo la combinación inicial,
3. De la suma, escogemos el 2do., 3er. y 4to. dígito como combinación final.

Por ejemplo, si tenemos como combinación inicial el número 123, y seguimos la fórmula anterior, obtenemos el número 307:

$$123 + 123^2 + 123^3 + 123^4 = 230.762.760$$

Por lo tanto, si escogemos los dígitos 2, 3 y 4 del número anterior, obtenemos la combinación final: 307. En nuestro caso, pudimos calcular fácilmente la combinación final a partir de la inicial, pero no puede calcularse fácilmente la inicial a partir de la final.

De una manera análoga se obtienen las llaves públicas y las privadas. Existen dos diferencias fundamentales: el largo de las llaves es considerablemente más grande (las llaves de algunos algoritmos tienen más de 300 dígitos).

La segunda diferencia es que nosotros pudimos obtener fácilmente una a partir de la otra (pues utilizamos una función muy sencilla de one-way-hashing). En criptografía de llave pública, no es posible en la práctica hacer eso, ni en una dirección ni en la otra.