



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

Guía 2: Implementación de Modelo de Firma Electrónica Simple en E-Mail

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

1.	Introducción	3
1.1	<i>Objetivo y alcance del documento</i>	<i>3</i>
1.2	<i>Contenido de este documento</i>	<i>3</i>
1.3	<i>Breve fundamento de la Firma Electrónica Simple.....</i>	<i>3</i>
1.4	<i>Referencias sobre productos Microsoft.....</i>	<i>4</i>
2.	Modelo de Firma Electrónica en Email	5
2.1	<i>Fundamento del modelo.....</i>	<i>5</i>
2.2	<i>Descripción del modelo</i>	<i>6</i>
2.2.1	Introducción	6
2.2.2	Implementación del modelo	7
2.2.3	Esquema de operación (sólo firma)	9
2.2.4	Esquema de operación (firma y cifrado)	9
3.	Implementación del modelo.....	11
3.1	<i>Tecnologías que permiten implementar el modelo</i>	<i>11</i>
3.2	<i>Firma Electrónica Simple en Email con PGP/GPG.....</i>	<i>11</i>
3.2.1	Descripción	11
3.2.2	Instalación del software necesario	12
3.2.3	Cómo generar una llave pública y privada	14
3.2.4	Cómo enviar un email firmado	16
3.2.5	Cómo enviar un email encriptado.....	17
3.2.6	Cómo leer un mensaje encriptado.....	19
3.2.7	Cómo leer un email firmado	21
3.2.8	Cómo leer un email encriptado y firmado	21
3.2.9	Acerca de la instalación y uso del plug-in entre distintos clientes de correo (usuarios avanzados)	21
3.2.10	Acerca del respaldo de anillos (usuarios avanzados)	22
3.2.11	Acerca de los servidores de llaves PGP (usuarios avanzados).....	22
3.3	<i>Generación de certificados X.509 con OpenSSL (usuarios avanzados).....</i>	<i>23</i>
3.3.1	Alcance	23
3.3.2	Generación de una CA interna	23
3.3.3	Generación de un certificado de usuario.....	24
3.4	<i>FES en Email con certificados X.509 en Mozilla Mail</i>	<i>25</i>
3.4.1	Importando un certificado X.509.....	25
3.4.2	Configurando Mozilla Mail.....	28
3.4.3	Cómo enviar un email firmado	30
3.5	<i>FES en Email con certificados X.509 en MS Outlook</i>	<i>31</i>
3.5.1	Solicitud de Certificado.....	31
3.5.2	Firma de correo electrónico	34
3.5.3	Envío de Mensajes	41
3.5.4	Recepción de los mensajes.....	41
3.5.5	Recepción de mensajes con firma inválida.....	43

Todos los logos y marcas registradas contenidas en este documento o en documentos anexos son propiedad de sus respectivos dueños. Reproducido bajo las autorizaciones correspondientes. Este documento fue desarrollado por el Proyecto de Reforma y Modernización del Estado exclusivamente con propósitos instructivos para la implementación de mecanismos de Firma Electrónica al interior de la Administración Pública. La información entregada por proveedores de tecnología o software es de exclusiva responsabilidad de éstos últimos, y no implica responsabilidad alguna para el Gobierno de Chile.

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 N°2: esto es, Firma Electrónica en E-mail.

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 de los 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 a través del email. 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 la base teórica del modelo de firma electrónica en email, independientemente de la tecnología que se utilice para implementarlo.

En el capítulo 3, se explican todos los pormenores técnicos mínimos necesarios para implementar un modelo de firma electrónica simple en email, con las dos tecnologías sugeridas para esto: PGP y X.509, con clientes de correo que corren tanto en el sistema operativo MS Windows como en Linux.

1.3 Breve fundamento de la Firma Electrónica Simple

El 25 de marzo de 2002 se promulgó la Ley de Documento y Firma Electrónica, N° 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 segundo: firma electrónica en email.

1.4 Referencias sobre productos Microsoft

Sólo a modo de referencia, se incluyen aquí referencias a la página corporativa de Microsoft, con instrucciones detalladas para configurar las opciones de las herramientas de Correo Electrónico y Navegador de Internet.

Guía Paso a Paso para configurar utilidades de llave pública Outlook Express 5.0 (y versiones posteriores) (en Inglés)

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/pubkeyox.asp

Guía Paso a Paso para configurar utilidades de llave pública Outlook 2000 (en Inglés)
--

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/pubkeyol.asp

Guía Paso a Paso para configurar utilidades de autenticación de clientes basado en llave publica para Internet Explorer 5.0 (y versiones posteriores) (en Inglés)
--

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/pubkeyie.asp

2. Modelo de Firma Electrónica en Email

2.1 Fundamento del modelo

Esencialmente, el correo electrónico se ha transformado en la herramienta con la que se intercambia mayor cantidad de información digital en el mundo de hoy. Sin embargo, a pesar de que es una herramienta increíblemente versátil en lo que a intercambio se refiere, no es utilizada a todo su potencial al interior de la Administración Pública. En particular, el correo electrónico es una de las tecnologías que permite implementar procesos con intercambio de documentos electrónicos, razón por la cual es sugerida como uno de los modelos de firma electrónica simple.

De acuerdo con lo explicado en el documento “*Modelos de Firma Electrónica Simple para la Administración Pública*”, los procesos que involucran intercambio de documentos electrónicos pueden implementarse como cadenas de intercambio de documentos, en los cuales en cada punto de la cadena es posible que una o más personas realicen modificaciones sobre la información o alguna clase de transacción.

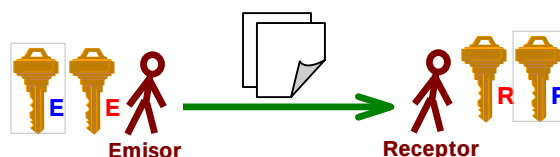
Pues bien: en esta guía, queremos presentar la idea de que cada paso de la cadena (cada envío de un documento electrónico desde un emisor hacia un receptor) puede ser implementado a través del envío de un email con un documento adjunto, firmado por el emisor, y verificado por el receptor.

Existen dos operaciones en particular (entre otras muchas posibles) para las que queremos hacer notar especialmente sus equivalentes en el mundo del papel:

Proceso en papel	Proceso electrónico
... yo envío el documento dentro de un sobre, para que nadie lo vea salvo el destinatario...	... yo encripto el email con el documento adjunto, para que nadie lo vea salvo el destinatario...
... yo firmo el documento, para que el destinatario tenga seguridad acerca de mi autoría y responsabilidad ...	... yo firmo electrónicamente el email para que el receptor tenga seguridad de mi autoría y responsabilidad ...

Entonces, si en el mundo del papel yo considero (debido a la legislación vigente, debido al contenido del documento, o debido a cualquier otra razón) que cierto documento debe ir firmado, y además dentro de un sobre para que nadie lo vea en el camino, entonces el equivalente a eso es enviar un email firmado y cifrado con un documento adjunto.

Ya que un proceso completo puede articularse a partir de sucesivas concatenaciones de envíos y recepciones de emails con documentos adjuntos, en cada paso (en cada envío de un email), existe la posibilidad de firmar y/o cifrar el email. Si nos restringimos sólo a un emisor y un receptor (como en la figura siguiente), entonces ambos deben contar con un par de llaves, una pública (indicada por una letra roja) y una privada (indicada por una letra azul y encerrada en un rectángulo). Existen al menos 4 casos posibles para un intercambio de emails:



1. **El email va sólo firmado:** En este caso, el emisor firma el email con su llave privada. El receptor siempre puede leer normalmente el email (aunque no cuente con el software adecuado o no tenga un par de llaves), pero para verificar la validez de la firma debe tener acceso a la llave pública del emisor.

2. **El email va sólo encriptado:** En este caso, el emisor debe encriptar el email con la llave pública del receptor, para que el receptor pueda desencriptarlo con su llave privada. Ambos deben tener el software adecuado instalado en sus computadores.
3. **El email va firmado y encriptado:** En este caso, es necesario que el emisor disponga de su llave privada para firmar, más la llave pública del receptor para encriptar. El receptor debe disponer de su llave privada para desencriptar, y de la llave pública del emisor para verificar la firma.
4. **El email no va firmado ni encriptado:** Este es el caso normal.

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

En el resto de este punto, se describe el modelo, en cuanto a los detalles de gestión a los que es necesario prestar atención para una implementación exitosa. En el siguiente capítulo, se describen los detalles técnicos que permiten firmar y/o cifrar emails enviados, y a su vez recibir, verificar y descifrar los emails recibidos.

2.2 Descripción del modelo

2.2.1 Introducción

Este modelo consiste en el envío de emails firmados (y posiblemente cifrados), en los cuales se adjuntan uno o más documentos, como *attachments* (documentos adjuntos). En este modelo, existe un emisor del documento (que no necesariamente es su autor) y un receptor del documento.

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

Elemento	Descripción
1. Un par de llaves (una pública y una privada) para cada usuario del sistema.	La forma de este par de llaves dependerá de la tecnología utilizada para generarlas. La razón por la cual son necesarios un par de llaves por cada usuario, está contenida en el punto anterior (2.1), y se relaciona con la capacidad de enviar emails firmados y/o encriptados.
2. Un repositorio de llaves públicas (o simplemente “ <i>repositorio</i> ”), con todas las llaves públicas de los funcionarios.	Este puede ser implementado de varias maneras: a través de la Intranet del Servicio, en una carpeta compartida (con permisos de sólo lectura) a la que todos tengan acceso, o bien a través de un servidor de llaves o “<i>ringserver</i>” (este concepto se explicará posteriormente). Existen muchas razones por las cuales es necesario un repositorio de llaves públicas. Esencialmente, cada vez que necesito enviarle a una persona un email encriptado, necesito su llave pública para que esta persona pueda desencriptar el email con su llave privada. Existen muchas formas distintas de obtener una llave pública (puede ser enviada por email, subida a un sitio Web, entregada personalmente en un diskette, etc.) Sin embargo, la forma en se obtiene una llave pública es tremendamente relevante, pues desde el momento en que uno obtenga esta llave, comenzará a confiar en la relación que existe entre esa llave y la persona a quien supuestamente pertenece.

	Por supuesto, la forma que adquiere este repositorio de llaves públicas depende grandemente de la tecnología utilizada.
3. Una dirección de correo institucional (o simplemente “ <i>dirección de respaldo</i> ”), que sirva como respaldo de la información de todos los emails firmados y/o cifrados y enviados a través del sistema. Por ejemplo, repositorio@minsegpres.cl.	Con respecto a la dirección de respaldo, la razón por la que se sugiere su implementación es que el email es, a pesar de todo, un medio de transporte inseguro. Esto quiere decir que en general existe un nivel de certeza baja con respecto a que un email cualquiera llegue o no a su destino. Por otro lado, siempre es conveniente poseer un medio de respaldo de la información enviada. Para esta dirección institucional también es necesario generar un par de llaves, y la llave pública debe colocarse en el “repositorio”, de manera que todos los envíos de emails firmados y/o encriptados sean enviados con copia a la dirección de respaldo. 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. Esto le permite a una persona con autoridad dentro de la propia institución (el Jefe de Servicio o quien sea comisionado en su nombre) verificar la información almacenada dentro de este respaldo, en caso de haber alguna diferencia respecto de su envío.

A continuación, se describe brevemente cómo implementar este modelo.

2.2.2 Implementación del modelo

Tal como fue mencionado en el documento “*Modelos de Firma Electrónica Simple para la Administración Pública*”, el explicar métodos para diagramar y analizar procesos escapa a los objetivos de esta guía. Sin embargo, se entregan a continuación una serie de pasos genéricos, a modo de orientación en la implementación de un proceso determinado, con este modelo de firma electrónica simple:

1 Catastrar los procesos con intercambio de documentos electrónicos.

Es necesario realizar un catastro de todos aquellos procesos de la institución que requieren de intercambio de información a través de documentos.

2 Escoger un proceso susceptible de ser digitalizado.

La idea 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 intercambio de documentos vía email. Esta decisión debe considerar también en qué partes del proceso se requieren firmas y/o encriptaciones (cifrado del email), cuántas personas deben intervenir en el proceso, si esas personas cuentan con computadores para su trabajo diario, 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. En el caso del modelo de firma electrónica en email, debe decidirse:

- a. Si se utilizarán certificados X.509, es necesario verificar si se cuenta con el software y el conocimiento adecuado para levantar una autoridad certificadora interna (una CA), y generar certificados para cada usuario.
- b. Si se utilizará PGP, es necesario verificar si se cuenta con plug-ins para los lectores de correo utilizados institucionalmente.

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, lo que incluye:
 - i. [Sólo para X.509] Levantamiento de una autoridad certificadora interna, y distribución de certificados para todos los usuarios del sistema.
 - ii. [Sólo para PGP] Generación de un repositorio de llaves públicas, dadas las opciones disponibles.
- c. Capacitación a todos los usuarios finales, que incluya:
 - i. Cómo enviar emails firmados y/o encriptados,
 - ii. Cómo recibir y leer emails encriptados,
 - iii. Cómo verificar la firma en un email firmado,
 - iv. Cómo cambia el proceso que está siendo digitalizado, al ser implementado a través del email firmado y/o encriptado.

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

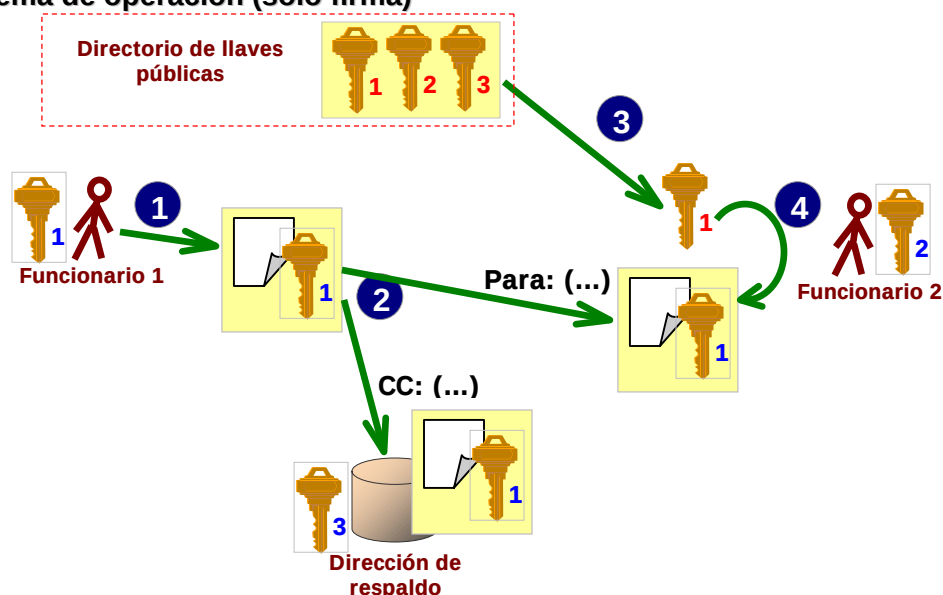
5 Ejecutar la planificación y evaluar la ejecución.

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 implementar este modelo de firma electrónica simple a través de email.

A continuación, se describe el detalle del envío de email entre un emisor y un receptor (como está descrito en el punto 2.1) en los casos relevantes (que son el envío de un email firmado, y un email firmado y encriptado).

2.2.3 Esquema de operación (sólo firma)

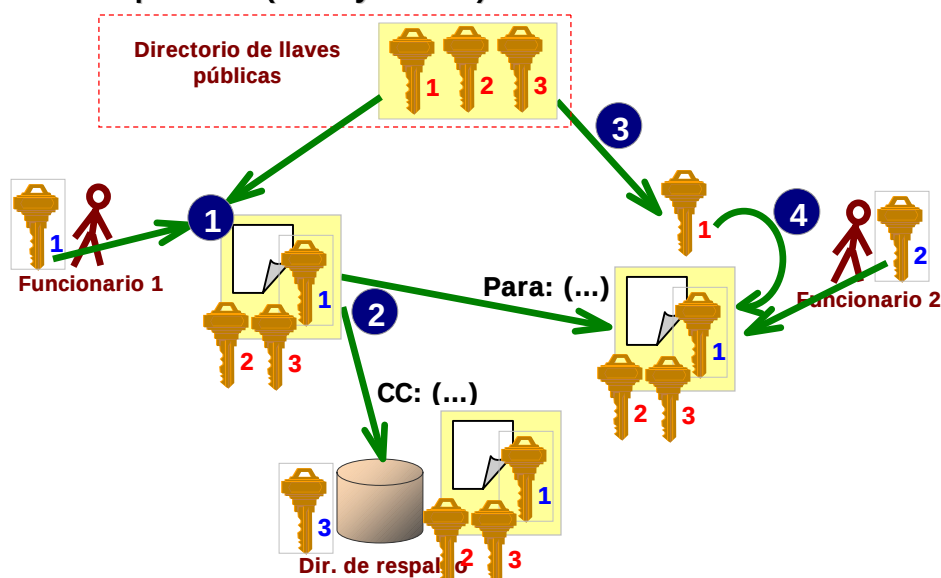


En la figura anterior, se muestra un esquema de sólo firma entre dos funcionarios. Los pasos realizados son los siguientes:

- 1 El Funcionario N°1 escribe un email, y adjunta al email un documento.
- 2 El email es **firmado** y enviado al funcionario N°2, con copia de carbón ("CC") a la dirección usada como **dirección de respaldo**.
- 3 El funcionario N°2 recibe el email firmado, y obtiene del **repositorio** (o de donde se encuentren las llaves públicas), la llave pública del emisor.
- 4 El funcionario N°2 verifica la validez de la firma del email recibido, y puede "bajar" u obtener el documento adjunto al email.

En el esquema anterior, los emails son firmados, pero su contenido puede ser visto por cualquier persona. Sin embargo, existen también documentos que no deberían ser vistos salvo por sus destinatarios. A continuación, se presenta un esquema de firma y cifrado de emails.

2.2.4 Esquema de operación (firma y cifrado)



En la figura anterior, se muestra un esquema de firma y cifrado de emails entre dos funcionarios. El funcionamiento es algo más complejo que el caso anterior, pero esencialmente corresponde a la misma estructura. Los pasos realizados son los siguientes:

- 1** El Funcionario N°1 escribe un email, y adjunta al email un documento. El email es firmado con la llave privada 1 (del funcionario N°1), y cifrada con las llaves públicas 2 (del funcionario N°2) y 3 (de la **dirección de respaldo**).
- 2** El email es enviado al funcionario N°2, con copia de carbón ("CC") a la dirección usada como **dirección de respaldo**.
- 3** El funcionario N°2 recibe el email firmado y cifrado. Si no tiene ya una copia, obtiene del **repositorio** (o de donde se encuentren las llaves públicas), la llave pública 1 (del funcionario N°1).
- 4** El funcionario N°2 descifra el mensaje con su llave privada (la llave privada 2), verifica la validez de la firma del email recibido (con la llave pública 1), y puede "bajar" u obtener el documento adjunto al email.

Es necesario hacer notar algunos hechos de importancia:

1. Debe considerarse como documento firmado **el email completo**, no sólo el documento adjunto en el email. Esto porque, al no existir (en el contexto del ejemplo) una manera de firmar el documento directamente, una vez recibido el email, puede tomarse dicho documento, modificarlo y volver a usarlo para otros propósitos. Esto se evita verificando la firma del email completo.
2. De acuerdo con la Ley, una Firma Electrónica "simple" puede ser técnicamente tan compleja o segura como una Firma Avanzada, pero se llamará "simple" mientras no provenga de una institución que haya sido acreditada por la entidad acreditadora. Es esta la razón de que este esquema sea considerado "simple".

3. Implementación del modelo

3.1 Tecnologías que permiten implementar el modelo

Técnicamente, existen hoy en el mundo un sinnúmero de mecanismos orientados a enviar, recibir y verificar firmas en emails firmados digitalmente. Sin embargo, actualmente son dos las tecnologías más utilizadas para esto: PGP/GPG¹ y certificados X.509 (PKI). Ambas tecnologías tienen en común que utilizan criptografía de clave pública para firmar y/o encriptar emails; difieren sin embargo en tres puntos fundamentales:

1. **El modelo de confianza utilizado:** PGP/GPG utiliza un modelo llamado “de anillo”. En éste, cada persona establece y determina la confianza que posee en cada una de las personas con las que se comunica. En cambio, en PKI, existe una estructura jerárquica donde la confianza es “heredada”, de manera que todas las verificaciones terminan en un punto donde cada participante posee confianza en un ente final (una CA).
2. **La estructura y forma de utilización de las llaves pública y privada:** En PGP/GPG, no existe el concepto de certificado digital. Las llaves públicas contienen información limitada sobre una persona (típicamente, nombre e email), y son distribuidas directamente por sus dueños.
3. **La forma de verificación de los emails firmados:** Las formas de verificación son distintos en ambos casos, si bien en ambos son procesos semiautomáticos.

Es importante notar, adicionalmente, que ambos modelos **son incompatibles**, y que una llave generada en un modelo no puede utilizarse (en la práctica) directamente en el otro modelo. La incompatibilidad mencionada aquí no significa que no puedan utilizarse ambas tecnologías simultáneamente, en los mismos computadores y en los mismos sistemas.

A continuación, se explica sucesivamente:

1. Cómo implementar firma/cifrado de emails a través de PGP. Esta alternativa tiene la ventaja de ser sencilla de utilizar, barata, rápida de implementar y es interoperable entre distintos clientes de correo en distintas plataformas (salvo algunos detalles menores).
2. Cómo implementar firma/cifrado de emails a través de certificados X.509.

Para esta segunda alternativa, es necesario contar con certificados X.509, adquiridos externamente o generados al interior de una institución. Ya que la adquisición de certificados no es un problema, primero se aborda el problema de generación de certificados de manera interna a una institución², tanto a través de herramientas de software libre como con herramientas Microsoft, y luego se explica cómo firmar/cifrar emails con tres clientes de correo: Microsoft Outlook 2000, Mozilla Mail 1.6 y Thunderbird 0.7.

3.2 Firma Electrónica Simple en Email con PGP/GPG

3.2.1 Descripción

Para implementar el modelo de firma simple en email con PGP/GPG, es necesario realizar algunos cambios menores sobre los clientes de correo utilizados institucionalmente (esto es, sobre el software que se utiliza para leer correo). Estos cambios se realizan instalando un tipo de software que agrega funcionalidad al cliente. Este tipo de software se denomina genéricamente como *plugin*.

¹ GPG/PGP = GNU Privacy Guard/Pretty Good Privacy. La primera es una tecnología de código abierto, libre de costo por licencia; la segunda en cambio es una tecnología comercial sobre la que se ha basado la mayor parte de la primera.

² Una pregunta frecuente respecto a este punto es si es necesario acreditarse frente a la Subsecretaría de Economía para generar certificados X.509; otra pregunta frecuente es si los documentos firmados con estos certificados son considerados con firma avanzada. Para la respuesta a ambas preguntas, referirse al anexo del documento “Modelos de Firma Electrónica Simple para la Administración Pública”.

A pesar de que existen numerosos clientes distintos de correo, existen igualmente plug-in's para prácticamente todos los clientes de correo existentes³. No es necesario por tanto invertir en licencias de software para implementar este modelo de firma electrónica.

Para todas las explicaciones que se muestran en esta guía, se utilizó Microsoft Outlook 2000 como cliente, instalado sobre Microsoft Windows XP. Se utilizó Microsoft Exchange como servidor de correo, aunque para el servidor en el caso de PGP/GPG es transparente el servidor de correo utilizado. Cualquier otra versión de Windows (Win 95/98/NT) tienen apariencias diferentes, pero contienen funcionalidad idéntica.

Para más información o dudas sobre productos Microsoft, consulte la página corporativa de Microsoft Corporation para configurar las utilidades de llave pública Outlook Express 5.0 (y versiones posteriores) y Outlook 2000, y las utilidades de autenticación de clientes basado en llave publica para Internet Explorer 5.0 y versiones posteriores.

3.2.2 Instalación del software necesario

Antes de comenzar a firmar o encriptar emails, es necesario instalar un pequeño programa, que puede ser descargado desde la siguiente URL:

http://openpgp.vie-privee.org/courrier_en.html

Para efectos de este documento, se utilizó el plug-in para Outlook (G-Data), que es un software libre (*free software*).

Luego de bajar este software al disco duro del computador, es necesario instalarlo. Para eso, basta con hacer doble clic sobre el programa. Aparecerá la siguiente ventana:



Haga click en el botón "Next>". Aparecerá la siguiente ventana:

³ Para una lista de clientes de correo y plug-in's asociados, ver http://openpgp.vie-privee.org/courrier_en.html.



En la ventana anterior, pregunta si debe instalar sólo el plug-in o además el software de criptografía. Escoja la primera opción (plug-in más el software GnuPG) y presione "Next>". Aparecerá la siguiente ventana:



En esta ventana, se pregunta por el directorio donde debe instalarse el software. Si desea puede cambiar el directorio sugerido, pero la mayor parte de las veces es suficiente con aceptar el directorio sugerido. Una vez que esté listo, presione "Next>". Aparecerá la siguiente ventana:

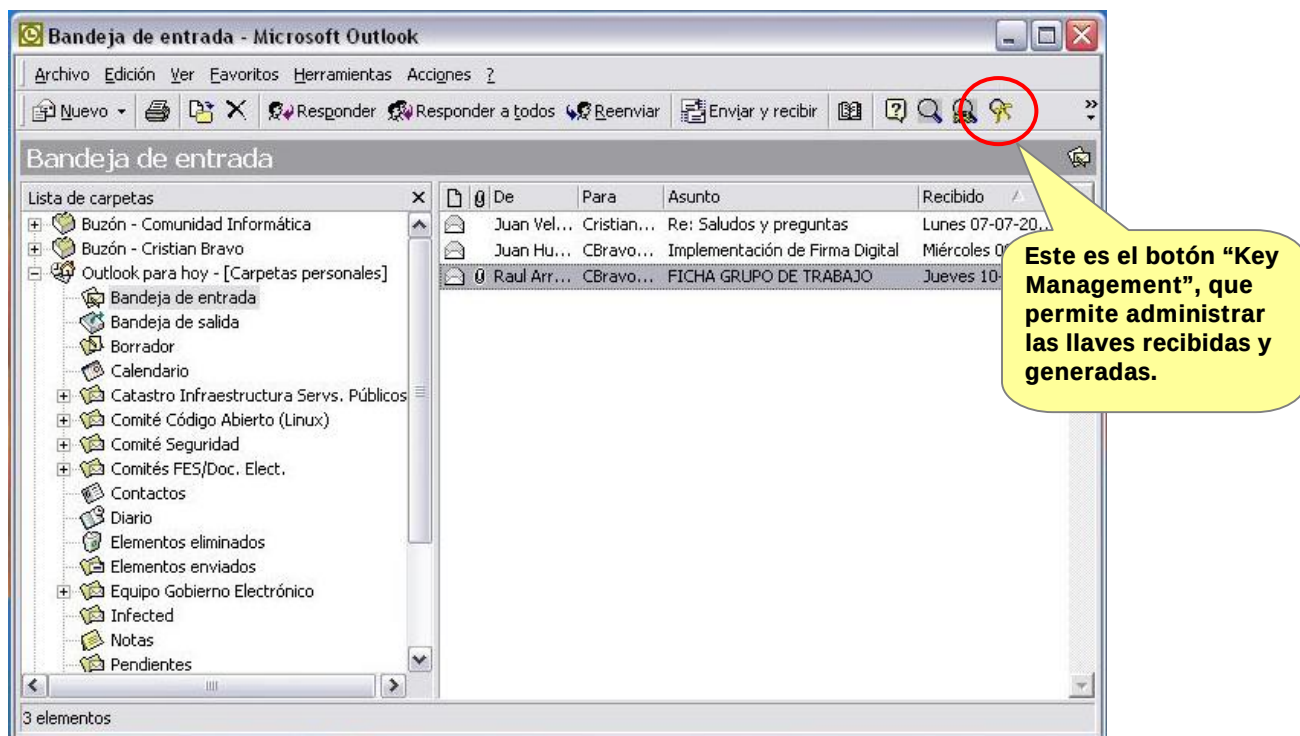


El sistema está listo para instalar el software. Para instalar, presione el botón “Install”. Si todo resulta bien, el sistema debería desplegar una ventana informando acerca de la instalación exitosa.

3.2.3 Cómo generar una llave pública y privada

Antes de comenzar a firmar o encriptar los emails enviados, y a leer emails encriptados o firmados, es necesario generar un par de llaves (una llave pública y una privada) para uso personal.

Para eso, presentaremos primero la interfaz de MS Outlook. En la imagen de abajo (que corresponde a la ventana principal de MS Outlook), se puede ver un botón arriba a la derecha, que representa un “juego de llaves”. Esta es la funcionalidad de “gestión de manejo de llaves”. Salvo por eso, la interfaz de MS Outlook sigue siendo exactamente la misma.

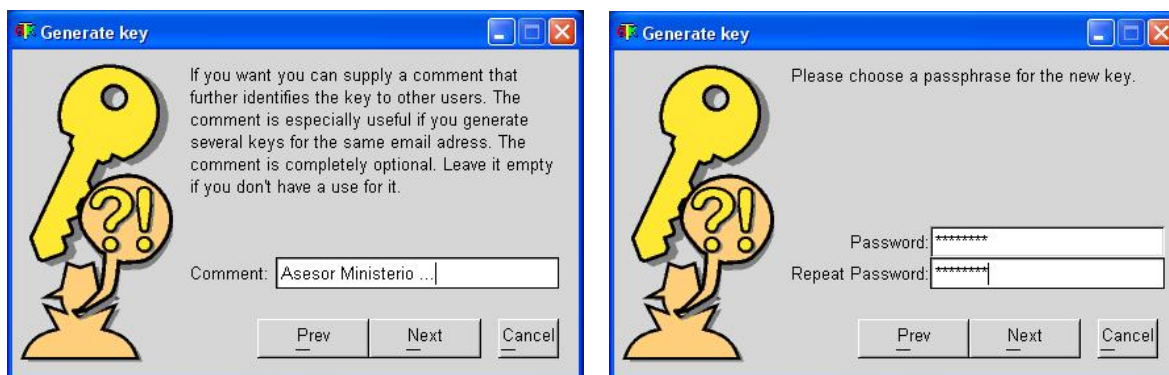


Si nunca se ha usado antes el sistema, la primera vez que se presione el botón de “*manejo de llaves*” (indicado en la imagen como “*Key Management*”), se desplegará una ventana donde se informa que no se ha generado un par de llaves, y donde se pregunta si se desea generar un par de llaves ahora. Al responder afirmativamente, se comienza el proceso de generación de llaves.



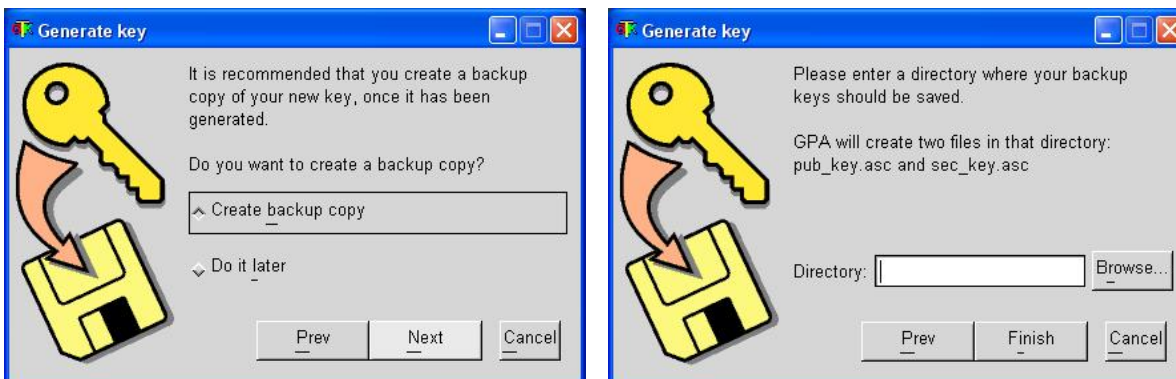
Primero aparece la ventana de la izquierda, en la imagen anterior. En ésta, se solicita el nombre completo de la persona, que será incluido dentro de las claves a generar. Luego de ingresar el nombre de la persona, presione el botón “Next”.

Luego, aparecerá la ventana de la derecha (en la imagen anterior). En ésta, debe ingresar su email. Se recomienda ingresar aquí un email institucional, que identifique a la persona como perteneciente a un Servicio Público determinado. Se desaconseja fuertemente el uso de emails gratuitos, como “Yahoo” o “Hotmail”. Cuando haya ingresado su email, presione el botón “Next”.

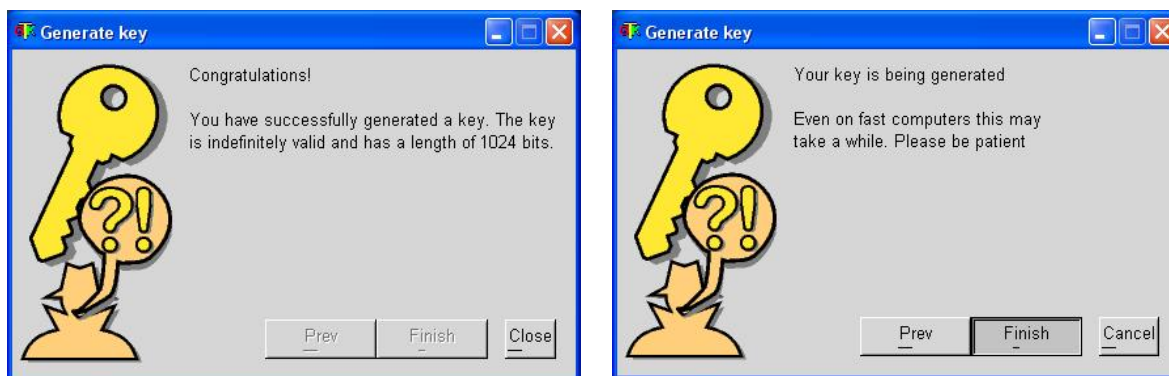


Aparecerá a continuación la ventana de arriba a la izquierda. En ésta, se solicita un comentario adicional que pueda eventualmente entregar mayor información al resto de los usuarios sobre la persona que utilizará el par de llaves que está siendo generado. Se recomienda fuertemente ingresar aquí el cargo de la persona que utilizará estas llaves. A continuación, presione “Next”.

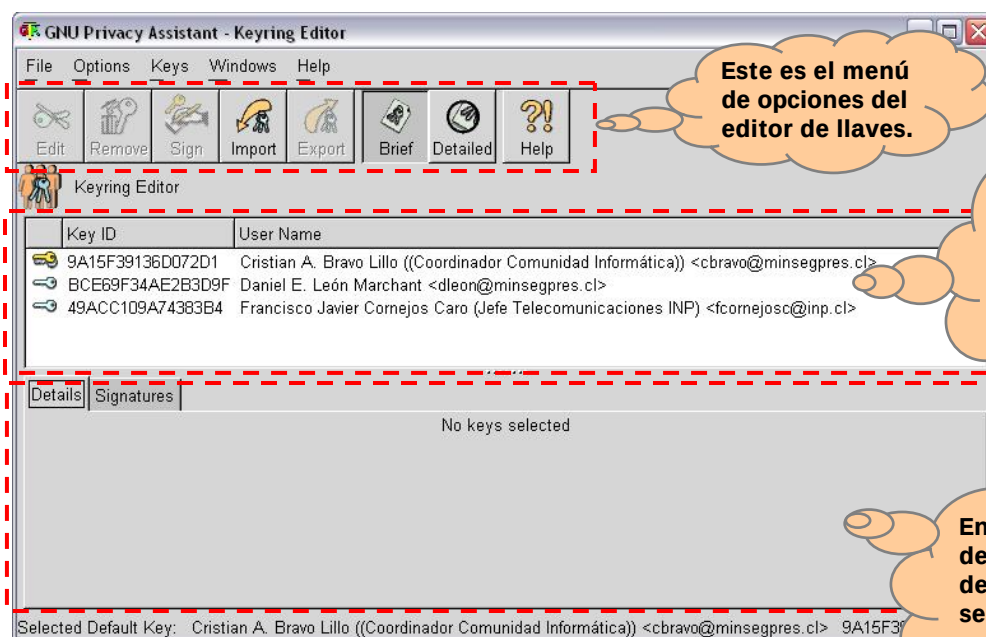
Luego aparecerá la ventana de arriba a la derecha. En ésta debe ingresar dos veces un password, para proteger la llave privada. Este password deberá ser ingresado cada vez que el sistema requiera utilizar la llave privada, por ejemplo para firmar un email o para decifrar un email enviado por otra persona. Para finalizar, presione el botón “Next”.



Aparecerá la ventana de arriba a la izquierda. En ésta se pregunta si se desea crear una copia de respaldo de la llave por generar. La opción de arriba sirve para crear una copia de respaldo, y la de abajo para hacerlo posteriormente. A pesar de que aparece como recomendable el generar una copia de respaldo de la llave (el respaldar la llave privada es más complejo), se recomienda escoger la opción de abajo, pues posteriormente se generarán los respaldos adecuados. En caso de que se escoja la opción superior y se presione el botón “Next”, aparecerá la ventana derecha, preguntando en qué directorio se desea dejar las llaves generadas. Para finalizar, presione el botón “Finnish”. Aparecerá a continuación un mensaje informativo (ventana izquierda) y un mensaje final (ventana derecha).



Una vez que se haya realizado la tarea anterior (de generación de llaves, o bien después de presionar el botón de “Key Management”), se desplegará el administrador de llaves, tal como aparece en la imagen siguiente:

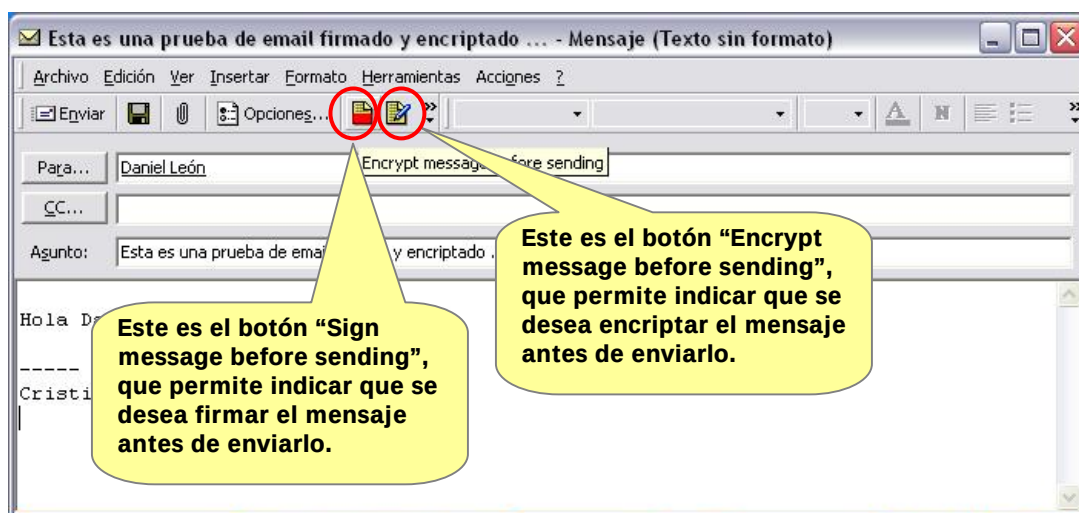


En la ventana anterior, existen dos recuadros importantes: en el de arriba, se despliegan las llaves contenidas en el “repositorio” local del computador; es decir, nuestro par de llaves pública y privada, además de las llaves públicas de las personas que nos las han enviado. En el recuadro de abajo, se despliegan los detalles de una llave determinada, cuando la seleccionamos en el recuadro de arriba.

A pesar de que el editor de llaves posee gran cantidad de funcionalidades, éstas no se explicarán aquí para mantener la simplicidad de este documento.

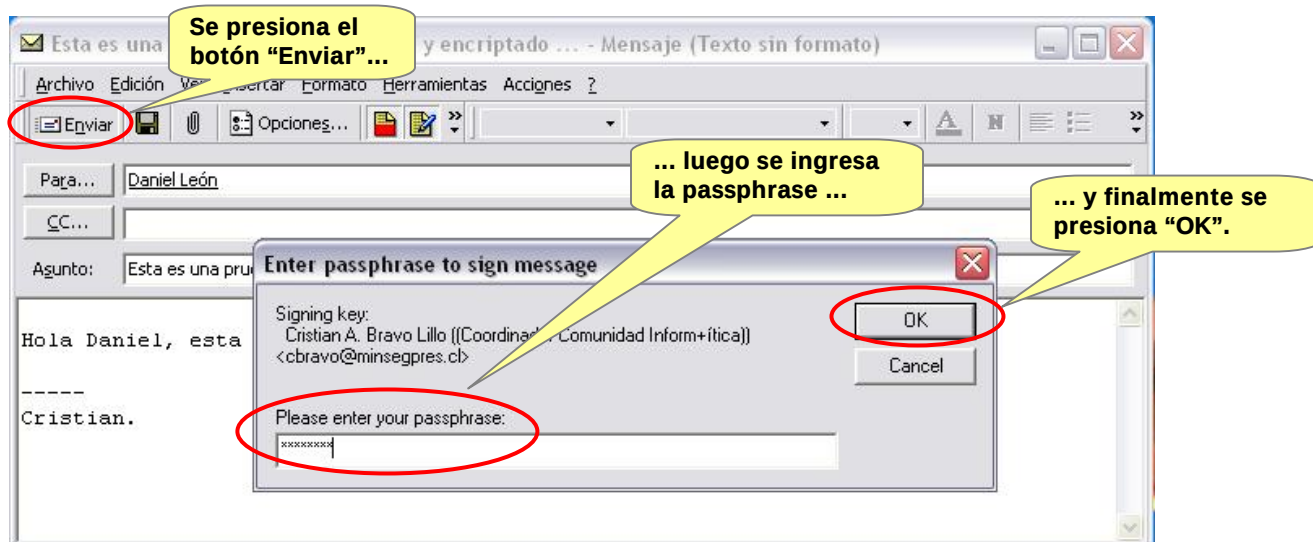
3.2.4 Cómo enviar un email firmado

En la imagen siguiente, se está “componiendo” un nuevo email. En esta ventana aparecen dos nuevos botones: el de firma de email, y el de cifrado o “encriptación” de email.



Los dos botones descritos en la imagen anterior son como interruptores: cuando uno los presiona, no pasa nada inmediato, salvo que el botón queda "presionado". Uno puede activar uno de los dos botones, ambos, o ninguno de los dos. El resultado sólo se verá cuando uno termine de componer el email, y presione el botón "Enviar".

En la figura siguiente, se presionó el botón para firma, y una vez que se terminó de escribir el email, se presionó el botón "Enviar". Aparece entonces la siguiente ventana:



En la ventana anterior, el sistema espera que uno ingrese su password personal (el mismo que se ingresó al generar el par de llaves). Una vez que lo ingresamos, se presiona "OK" y el email es firmado y enviado a su destinatario.

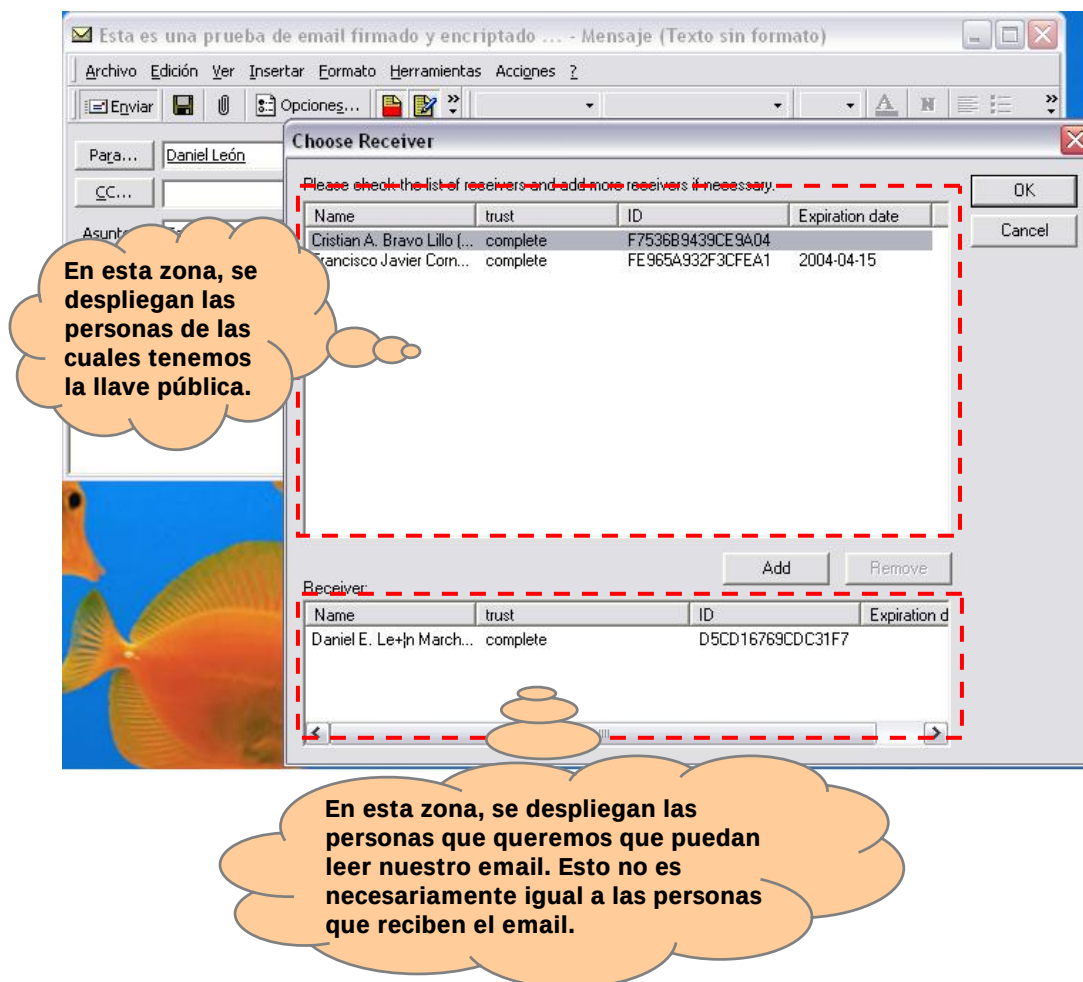
3.2.5 Cómo enviar un email encriptado

Para enviar un email encriptado a una persona, tenemos que asegurarnos de que poseemos en nuestro computador su llave pública. Sólo en ese caso, podremos enviar un email encriptado que sólo esa persona pueda descifrar.

Para obtener la llave pública de una persona, podemos pedirle simplemente que la envíe adjunta (attachment) en un email. No es necesario que nos preocupemos de la seguridad de este email, porque la llave pública es precisamente de conocimiento público.

Para saber cómo obtener la llave pública de una persona, o cómo enviar la llave pública propia, consulte “*Cómo obtener la llave pública de otra persona*”, en este documento.

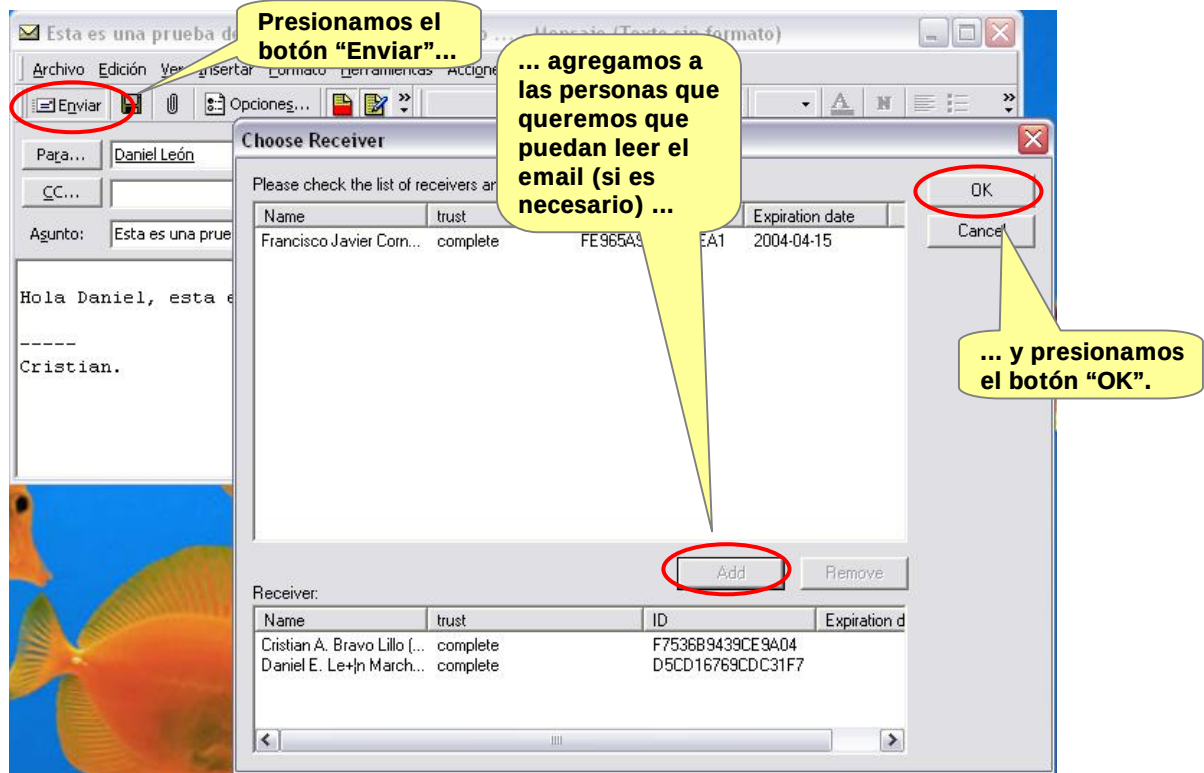
Para enviar un email encriptado, el primer paso es escribir el email. Antes de enviarlo, tenemos que presionar el botón de encriptado. Una vez que hemos terminado de escribir el email, presionamos el botón “Enviar”. Aparece la siguiente ventana:



Luego de presionar el botón enviar, aparece una ventana con título “*Choose receiver*”. En esta ventana, tenemos que elegir las personas que queremos que sean capaces de leer el email, una vez que sea encriptado. Es necesario hacer notar que éstas no son necesariamente iguales a las personas a las que se les envía el email. Si le enviamos un email encriptado a una persona, pero no la incluimos dentro de la lista de personas que pueden leer el email, la persona recibirá el email pero sencillamente no podrá leerlo.

Otra observación curiosa que surge de esto es que si no nos incluimos nosotros mismos dentro de la lista de personas que pueden leer el email, simplemente no podremos leerlo una vez que lo enviemos.

Entonces: si es necesario, incluimos a más personas haciendo clic sobre ellas en el recuadro superior, donde está la lista de personas de las cuales tenemos su llave pública. Luego de hacer clic sobre una persona, presionamos el botón “*Add*” para agregarla a la lista de personas que podrán leer el email (que aparece en el recuadro de abajo).

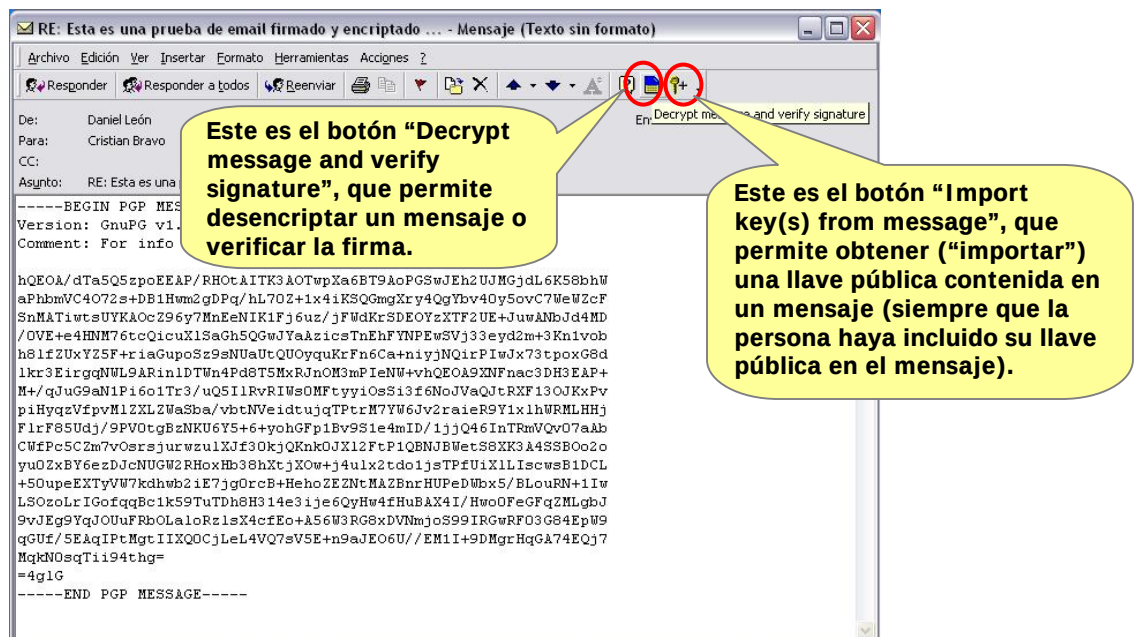


En la imagen anterior, primero se presionó el botón “Enviar”, y apareció la ventana “Choose receiver”. Luego se hizo clic sobre un usuario en el recuadro de arriba, y se presionó el botón “Add”, (y con eso se agregó el usuario a la lista de personas que pueden leer el email). Luego, se presiona el botón “OK”.

3.2.6 Cómo leer un mensaje encriptado

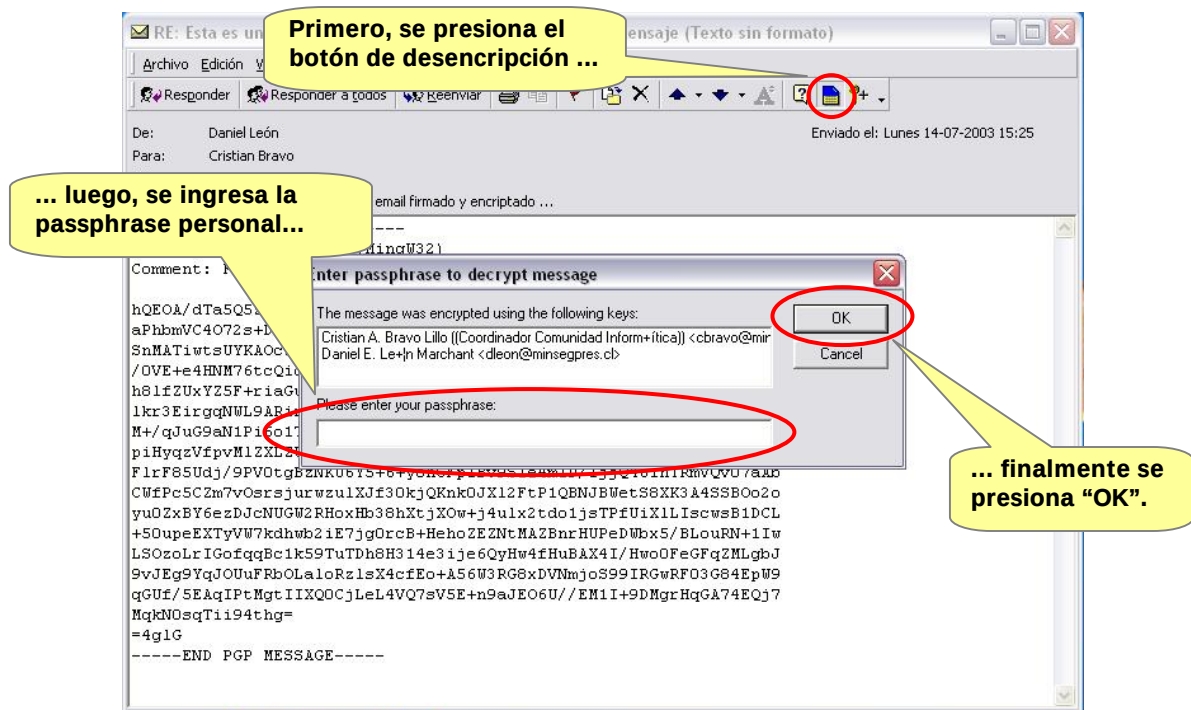
Cuando se recibe un mensaje encriptado, el mensaje llegará con un texto ilegible. Sólo podremos leerlo si fue encriptado con nuestra llave pública, es decir, si la persona que envió el email nos incluyó dentro de la lista de personas que podían efectivamente leer el email.

Un email encriptado se ve de la siguiente forma:



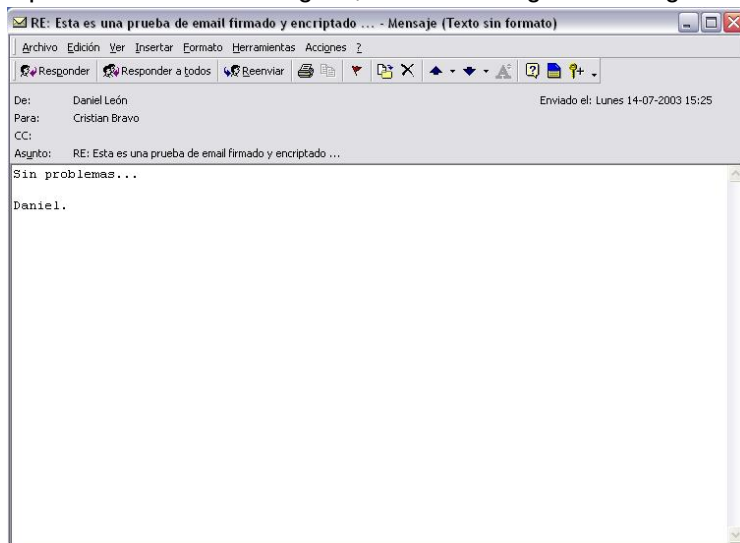
Una vez que hacemos clic sobre un email que hemos recibido en forma encriptada, podremos ver algo así como la imagen de arriba. Es necesario hacer notar que, en esta ventana, hay dos botones nuevos: el botón de “*Decrypt message and verify signature*”, y el botón de “*Import key(s) from message*”. El primero (de la izquierda) sirve para descryptar un email cuando está encriptado, y el segundo (de la derecha) para extraer la llave pública de la persona que envía el email (en caso de que la persona haya incluido su llave pública en el email).

Para leer el contenido del email, se presiona el botón de la izquierda (de descryptación del mensaje). Una vez presionado, el sistema mostrará la siguiente ventana:



En la imagen anterior, primero se presionó el botón de descryptación (o decifrado). El sistema muestra una ventana con título “*Enter passphrase to decrypt message*”. En esta ventana, se muestran las personas que están autorizadas para leer el email, que corresponde a las personas que fueron originalmente incluidas en la lista de personas que podían leer el email.

Es necesario ingresar el passphrase y luego presionar el botón “OK”. Cuando se hace eso, el email se descrypta y aparece el contenido original, como en la siguiente imagen:

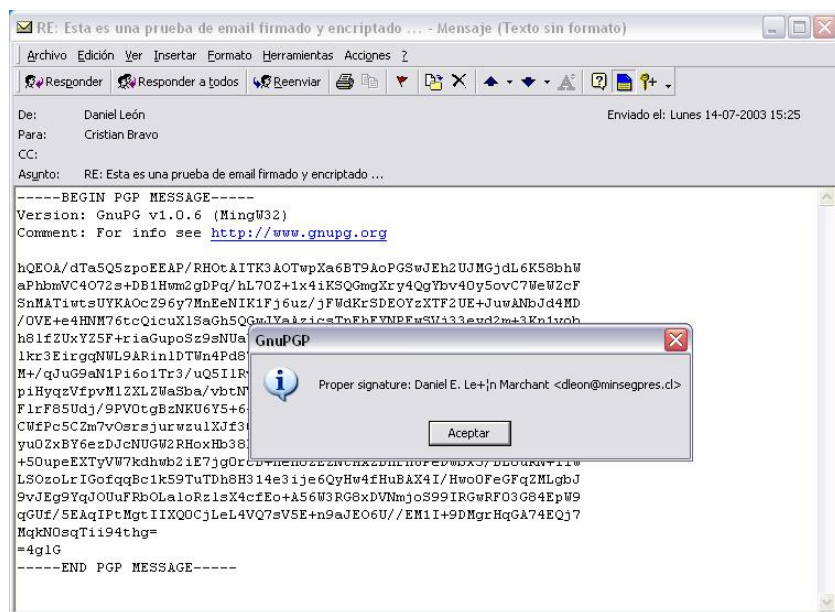


3.2.7 Cómo leer un email firmado

En realidad, dado que un email firmado es perfectamente legible, no es necesario hacer ningún procedimiento especial para firmarlo. Sin embargo, una de las acciones que uno desearía realizar es verificar que la persona que envió el email es quien dice ser; en otras palabras, verificar la validez de la firma.

Para verificar una firma, primero es necesario visualizar el email. Luego, en la ventana donde aparece el email, es necesario presionar el botón de descifrado, exactamente igual que en la sección anterior ("Cómo leer un email encriptado"), tal como si el email estuviese encriptado. Una vez que se presione este botón, se verificará la firma en el email; en caso de que estuviera correcta, se muestra un mensaje en inglés, diciendo "Proper signature" ("*firma correcta*"), seguido de la identificación de la persona que firmó el email.

En la siguiente imagen, se muestra el resultado exitoso de una verificación de firma:



3.2.8 Cómo leer un email encriptado y firmado

El proceso para leer un email encriptado y firmado, es exactamente igual al que se realiza cuando el email está sólo encriptado. La diferencia es que, durante el proceso de descifrado, el sistema además verificará automáticamente la validez de la firma e informará del resultado, tal como aparece en la última imagen del punto anterior.

3.2.9 Acerca de la instalación y uso del plug-in entre distintos clientes de correo (usuarios avanzados)

El uso del plug-in para PGP/GPG mostrado en las secciones anteriores, no es idéntico entre distintos clientes de correo, y existen pequeñas diferencias de operación entre distintos clientes de correo en distintas plataformas. Se han realizado pruebas de intercambio y verificación de correo firmado y encriptado entre un cliente Microsoft Outlook 2000 sobre MS Windows XP, y un cliente Mozilla Mail 1.6 sobre Linux RedHat 9.2; en estas pruebas se ha observado que ciertos clientes de correo en Linux envíen el texto encriptado como archivo adjunto, y que el cliente de correo de Microsoft no sabe cómo abrirlo directamente. Hasta ahora, no se ha resuelto de manera definitiva este problema; una solución parcial (muy incómoda) es reenviar el email copiando el texto encriptado en el cuerpo del email.

Otra observación importante es que, para funcionar correctamente, los emails deben ser siempre enviados **en texto plano**. Un email enviado en HTML o en texto enriquecido (lo que es usual en los clientes de correo de Microsoft) incorpora todos los TAGS propios de HTML, lo que imposibilita la lectura de las llaves o encriptaciones de PGP por parte de los plug-ins.

3.2.10 Acerca del respaldo de anillos (usuarios avanzados)

Todas las llaves públicas almacenadas para ser usadas dentro del “asistente de llaves” en un computador determinado, están almacenadas dentro de un repositorio especial llamado “anillo”. Usualmente, siempre coexisten dos anillos distintos: uno es el anillo de llaves públicas (que contiene todas las llaves públicas que hemos almacenado localmente en el computador), y el anillo de llaves privadas (que usualmente sólo contiene una o dos llaves privadas, que hemos generado para nuestro propio uso).

Usualmente el anillo público está contenido en un archivo de nombre ‘pubring.gpg’, y el anillo privado en un archivo llamado ‘secring.gpg’.

Cuando un usuario se cambia de computador, es necesario exportar su llave privada o respaldar el anillo privado, pues de otro modo la llave privada se pierde irremediamente y es necesario generar un nuevo par de llaves (con todo el problema que ello conlleva). Lo mejor en este caso es respaldar los archivos ‘secring.gpg’ y ‘pubring.gpg’ del computador antiguo, instalar PGP en el nuevo computador, y sobrescribir los archivos homólogos en el nuevo computador.

Para respaldar sólo la llave privada y realizar otras operaciones relacionadas con los anillos, se puede utilizar directamente el programa de consola ‘pgp.exe’ (en MS Windows, generalmente en ‘c:\Archivos de Programas\GNUPGExch\pgp.exe’).

Para exportar las llaves privadas contenidas en un anillo, se puede ejecutar el siguiente comando:

```
%pgp -a -o privada.key --export-secret-keys
```

Lo anterior dejará las llaves privadas en un archivo de nombre ‘privada.key’. En todo caso, esto constituye un riesgo de seguridad y debe tratar de evitarse.

Existen otros muchos comandos que pueden ser usados directamente en consola; pero cuyo tratamiento excede los propósitos de esta guía.

3.2.11 Acerca de los servidores de llaves PGP (usuarios avanzados)

En general, uno de los problemas más complejos dentro del esquema de PGP es la distribución razonable de las llaves públicas de las personas dentro de una institución. Mientras se trate de una institución pequeña (una división u oficina de un servicio público, con no más de 30 personas), es posible mantener una solución manual de repositorio de llaves públicas, como alguna de las siguientes:

1. Una carpeta compartida con sólo permisos de lectura, donde el administrador es el encargado de recibir las llaves públicas generadas por cada persona y de colocarlas dentro de esta carpeta.
2. Una página HTML dentro de la Intranet de la institución, donde simplemente se coloquen links a las llaves públicas de las personas. Nuevamente, el administrador será el encargado de recibir y actualizar las llaves dentro de la página.

Sin embargo, la solución anterior no es escalable. Eventualmente, ante un número grande de usuarios, será necesario pensar en alguna forma de administración automática de llaves públicas.

Un servidor de llaves (o 'ringserver') es un servicio brindado a través de múltiples medios (existen servidores basados en Web, en Email y en FTP), a partir del cual cada persona puede obtener las llaves públicas de las personas con las que desea comunicarse. Cada persona además es encargada de subir su propia llave pública a este servidor, para que las demás puedan encontrar su llave.

Algunos servidores de llaves basados en Web alrededor del mundo son los siguientes:

1. <http://pgp.mit.edu/>
2. <http://keyserver.veridis.com/en/>
3. <http://www.uk.pgp.net/pgpnet/wwwkeys.html>

Algunos de estos servicios entregan incluso el código para generar un servidor de llaves propio, y en teoría no es difícil generar un servidor de llaves.

3.3 Generación de certificados X.509 con OpenSSL⁴ (usuarios avanzados)

3.3.1 Alcance

La generación de certificados X.509 es, en general, una tarea altamente configurable, y que requiere de múltiples pasos. Lo reseñado aquí, por tanto, debe tomarse como una orientación y una guía básica, de ningún modo como una recomendación o buena práctica.

Esencialmente, OpenSSL es una herramienta de software libre, disponible al menos en las distribuciones de Linux Mandrake, RedHat y (posteriormente) Fedora. Es una herramienta de consola (es decir, no posee una interfaz gráfica, a pesar de que existen numerosas herramientas gráficas construidas sobre OpenSSL), y permite (entre otras muchas tareas) levantar una CA interna, y generar certificados para usuarios, que permitan firmar emails de distintos clientes de correo.

3.3.2 Generación de una CA interna

Para generar una CA interna a una institución con OpenSSL, se requiere:

1. Configurar el archivo principal de OpenSSL. Dependiendo de la distribución obtenida, este archivo puede encontrarse en `/usr/local/ssl/openssl.cnf`, en `/usr/share/openssl/openssl.cnf`, o en otra ubicación. Generalmente, las opciones que vienen por defecto son suficientes para generar las primeras llaves, que sirven para investigar y realizar pruebas.
2. Generar un par de llaves (privada y pública).
3. Crear un certificado autofirmado por la CA; es decir, generar un certificado firmado con la misma llave privada.

Para generar un par de llaves con el algoritmo RSA, se debe ejecutar el siguiente comando:

```
% openssl genrsa -des3 -out ca.key 2048
```

En la línea anterior, el comando 'genrsa' indica que se desea generar un par de llaves bajo el algoritmo RSA; el modificador '-des3' indica que se usará el algoritmo DES3 para encriptar el par de llaves; el modificador '-out ca.key' indica que las llaves deben escribirse en el archivo 'ca.key'; finalmente, el argumento '2048' es un parámetro de seguridad respecto al largo de las claves siendo generadas.

Para crear el certificado autofirmado, debe ejecutarse el siguiente comando:

⁴ La información contenida en este punto fue obtenida del documento "The Open-source PKI Book", cuya última versión está disponible en <http://ospkibook.sourceforge.net>.

```
% openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

En la línea anterior, el comando 'req' indica que se está solicitando un certificado (técnicamente, se está generando un *certificate signing request* o CSR); el modificador '-new' indica que se trata de un certificado nuevo; el modificador '-x509' indica que se trata de un certificado X.509; el modificador '-days 365' indica el período de validez del certificado (365 días a partir de la fecha actual del sistema donde se realiza la operación); el modificador '-key ca.key' indica que debe utilizarse la llave contenida en el archivo 'ca.key'; finalmente, el modificador '-out ca.crt' indica que debe generarse el certificado final en el archivo 'ca.crt'.

3.3.3 Generación de un certificado de usuario

Para la generación de un certificado de usuario, se realizan tres pasos:

1. Se genera un par de llaves para el usuario.
2. Se genera una solicitud de firma de las llaves, a ser firmada por la CA⁵. En este paso se incorporan datos de identificación para el usuario (nombre, email, etc.).
3. Si la CA está segura de los datos contenidos en la solicitud, firma la solicitud y genera un certificado para el usuario.

Para generar un par de llaves para el usuario, se ejecuta un comando muy similar al indicado en el punto anterior:

```
% openssl genrsa -des3 -out usuario.key 2048
```

En la línea anterior, se generará un par de llaves contenidos en el archivo 'usuario.key'.

Para generar un CSR, debe ejecutarse el siguiente comando:

```
% openssl req -new -key usuario.key -out usuario.csr
```

La línea anterior es análoga a la indicada en el punto anterior, para generar el certificado autofirmado. Aquí, el certificado del usuario será generado en el archivo 'usuario.csr'.

Para firmar (en nombre de la CA) la solicitud generada anteriormente, se debe ejecutar el siguiente comando:

```
% openssl ca -config openssl.cnf -infiles usuario.csr -out usuario.crt
```

En la línea anterior, el comando 'ca' indica que se firmarán uno o más certificados; el modificador '-infiles usuario.csr' indica que se deben considerar los CSR contenidos en el archivo 'usuario.csr'; el modificador '-out usuario.crt' indica que el certificado firmado debe dejarse en el archivo 'usuario.crt'. El modificador '-config openssl.cnf' simplemente indica que la configuración para la firma del CSR debe tomarse del archivo principal de configuración de OpenSSL.

Para verificar la correcta generación del certificado, puede ejecutarse el siguiente comando:

```
% openssl verify -Cafile ca.crt usuario.crt
```

⁵ Esta "solicitud" se conoce como CSR (Certificate Signing Request).

En la línea anterior, el comando 'verify' indica que se desea verificar un certificado; el modificador '-Cafile ca.crt' indica la ubicación del certificado de la CA (el mismo generado en el punto anterior).

Una vez hecho lo anterior, ya se dispone de un certificado para un 'usuario'. Sin embargo, este certificado no es directamente utilizable por las aplicaciones de firma. Para ello, se debe ejecutar un comando que "transforma" el certificado a un formato especial (PKCS#12), que sí es utilizable por las aplicaciones de firma. Este comando es el siguiente:

```
% openssl pkcs12 -export -clcerts -des3 -in usuario.crt -out usuario.p12  
-inkey usuario.key
```

En la línea anterior, el comando 'pkcs12' es el que permite realizar una serie de operaciones relacionadas con el estándar PKCS12; la opción '-exports' indica que se desea exportar un certificado determinado a partir de un certificado base (indicado por los modificadores '-in usuario.crt', y '-inkey usuario.key'); finalmente, el modificador '-clcerts' indica que se desea exportar el certificado "cliente" y "público" (es decir, no la llave privada, ni las llaves asociadas a la CA).

El resultado de la operación anterior, es la generación de un archivo 'usuario.p12'. Este archivo sí es utilizable por las diversas aplicaciones de firma (en lo sucesivo, llamaremos a este archivo simplemente "*certificado digital*"), y puede ser utilizado en los ejemplos de firma citados en los puntos siguientes.

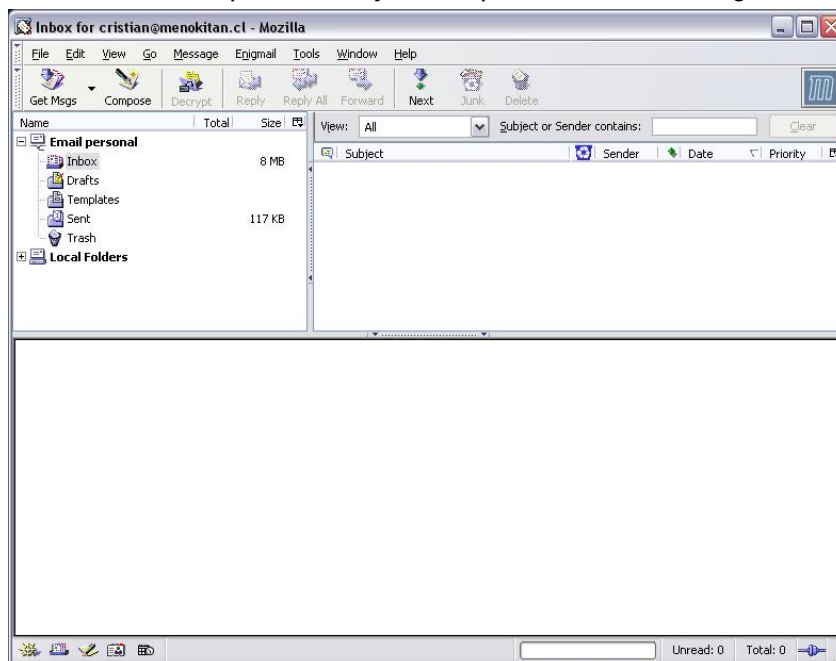
3.4 FES en Email con certificados X.509 en Mozilla Mail

Para firmar un email con certificado X.509 en Mozilla, es necesario contar con un certificado de usuario, como el generado en el punto anterior.

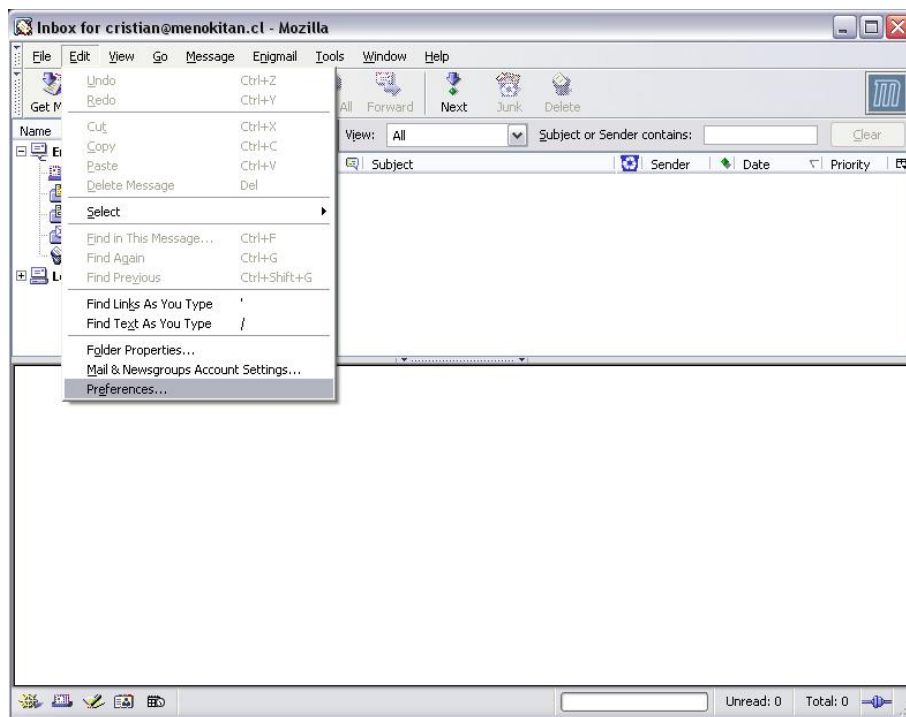
Todos los ejemplos siguientes fueron realizados con la utilidad de firma de Mozilla 1.6, browser de código abierto disponible en <http://www.mozilla.org>.

3.4.1 Importando un certificado X.509

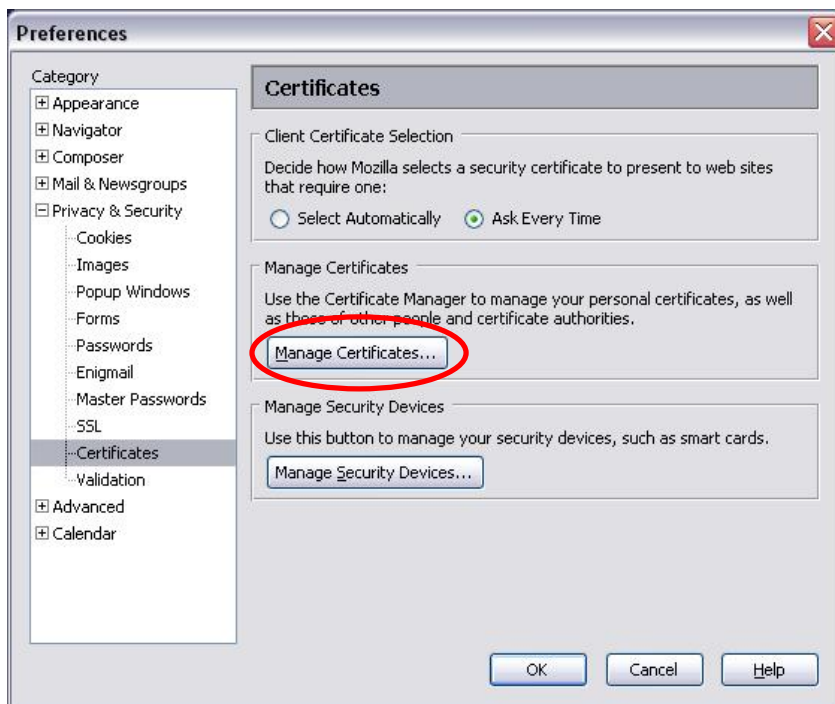
En primer lugar, es necesario importar un certificado al repositorio local de la aplicación, para que permita utilizar este certificado para firmar y/o encriptar los emails. La siguiente es la interfaz de Mozilla Mail:



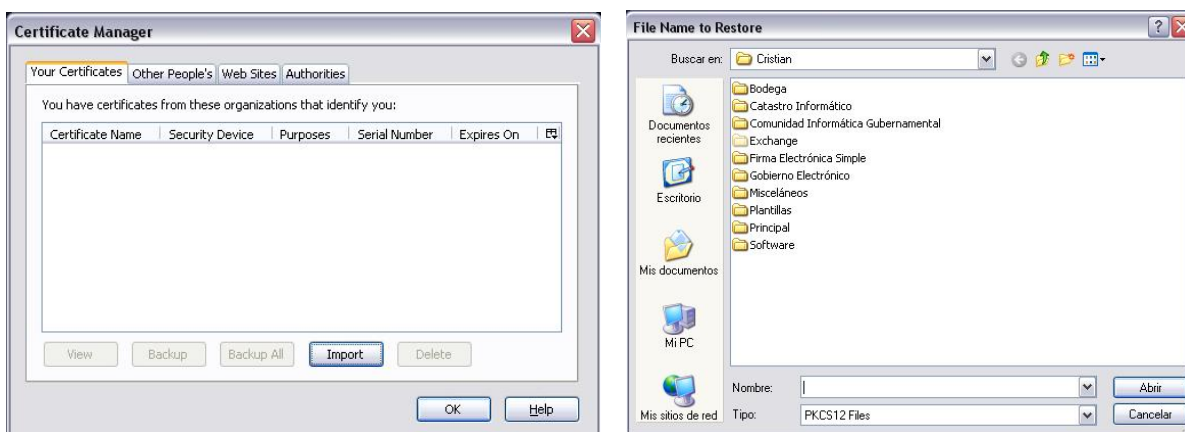
En el menú **'Edit'**, escoger la opción **'Preferences...'**, indicada en la figura siguiente:



Aparecerá la siguiente ventana:



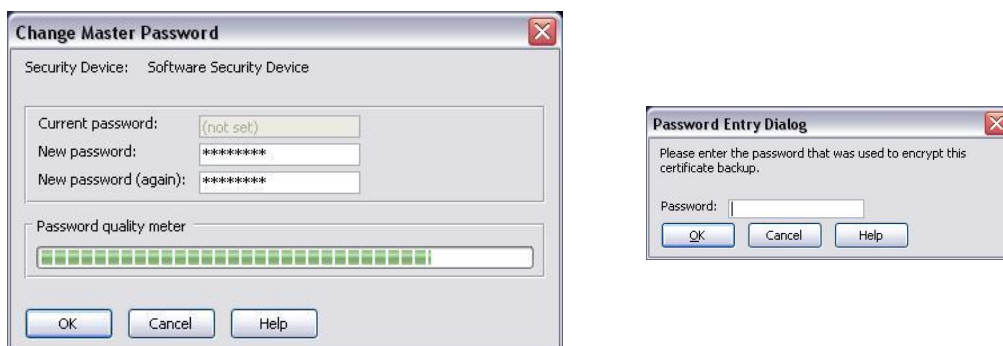
En la figura anterior, en la columna izquierda, se presenta una serie de opciones de configuración, que determinan el comportamiento del browser. En el grupo de opciones **'Privacy & Security'**, que contiene en general las opciones relacionadas con privacidad y seguridad, se debe escoger la opción **'Certificates'**. Aparecerán las opciones mostradas en la parte derecha de la ventana. Luego, se debe presionar el botón **'Manage Certificates...'**. Aparecerá la siguiente ventana (figura izquierda):



En la ventana anterior (figura izquierda), aparecen todos los certificados almacenados por el browser, incluyendo tanto los propios como los de terceros. En la primera “pestaña” (“**Your certificates**”), presionar el botón “**Import**”. Aparecerá una ventana (figura derecha) donde se solicita escoger el archivo donde se encuentra el certificado. Este archivo debe tener la extensión “.p12” o bien “.pfx”.

Una vez escogido el certificado, la primera vez que se realice esta operación el browser solicitará un password para el repositorio de llaves y certificados manejado por la aplicación. El password fijado para este repositorio (llamado “*Software Security Device*”), **no es el mismo que el solicitado para el certificado**; de ser posible, deben usarse passwords distintos para ambas cosas.

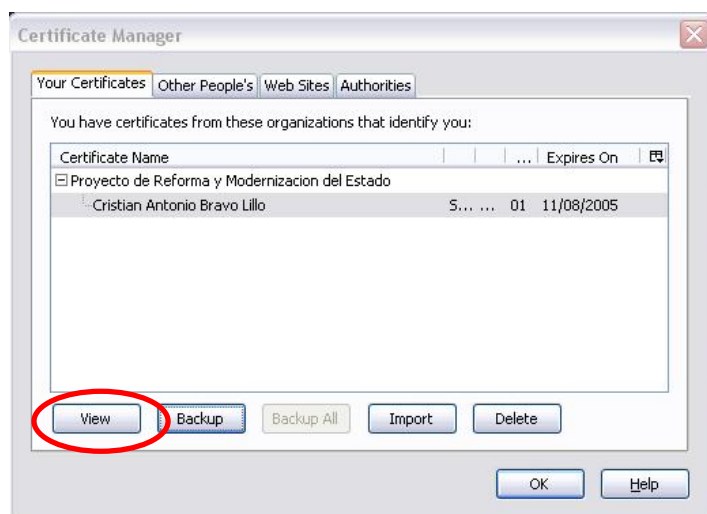
En la siguiente figura (izquierda), se muestra la ventana donde se solicita un nuevo password para el “*Software Security Device*”. Debe ingresarse un password y confirmarlo, y luego presionar el botón ‘**OK**’.



El indicador ‘**Password quality meter**’ es una herramienta útil, que indica la calidad del password ingresado.

Una vez que se ingresa el password anterior, la aplicación solicitará el password del certificado de usuario (figura derecha). Una vez que se ingresa el password del certificado, si todo está bien aparece un mensaje informativo indicando que se realizó correctamente la operación.

Luego, aparecerá en la ventana de despliegue de certificados, el certificado recién importado. Pueden observarse las características del certificado presionando el botón ‘**View**’, en la parte inferior izquierda de la ventana.

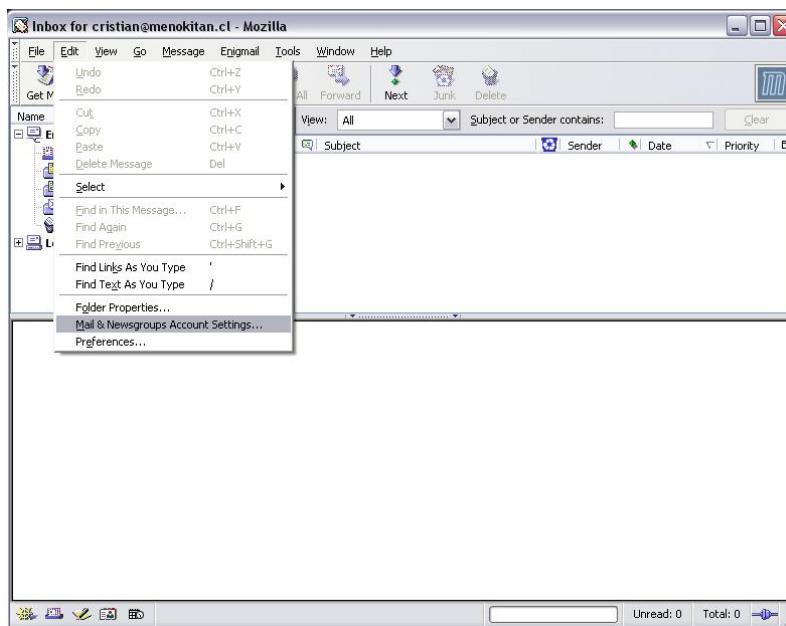


3.4.2 Configurando Mozilla Mail

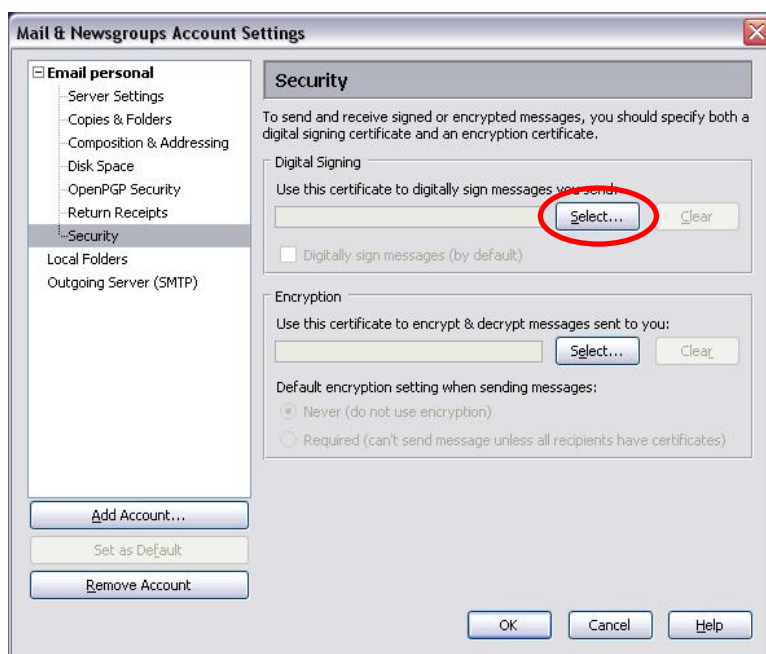
Lo siguiente es configurar el cliente de correo para que utilice el certificado que acabamos de importar para firmar y/o encriptar los emails.

A pesar de que es posible firmar y encriptar con el mismo certificado, en general esta práctica no se recomienda, y se sugiere que cada usuario tenga dos certificados distintos, uno para firmar y otro para permitir encriptar las comunicaciones dirigidas a él/ella.

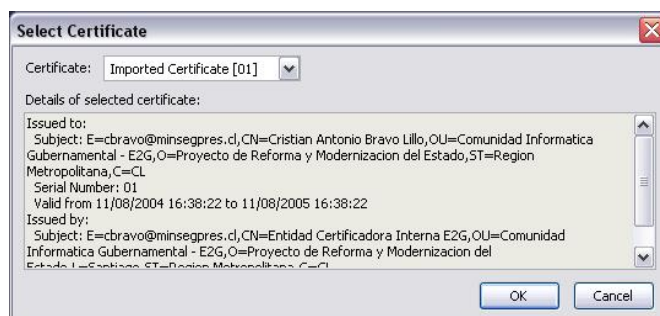
Para configurar Mozilla Mail con el certificado recién importado, en la interfaz principal se debe escoger la opción '**Mail & Newsgroups Account Settings...**', en el menú '**Edit**', tal como muestra la siguiente figura:



Una vez escogida dicha opción, aparecerá la siguiente ventana:



En la ventana anterior, se debe escoger la opción '**Security**', dentro del grupo de opciones disponibles para el perfil de correo personal. Luego, se debe presionar el botón '**Select**' que corresponde a '**Digital Signing**' (indicado en un óvalo rojo en la figura anterior). Aparecerá la ventana indicada en la siguiente figura:

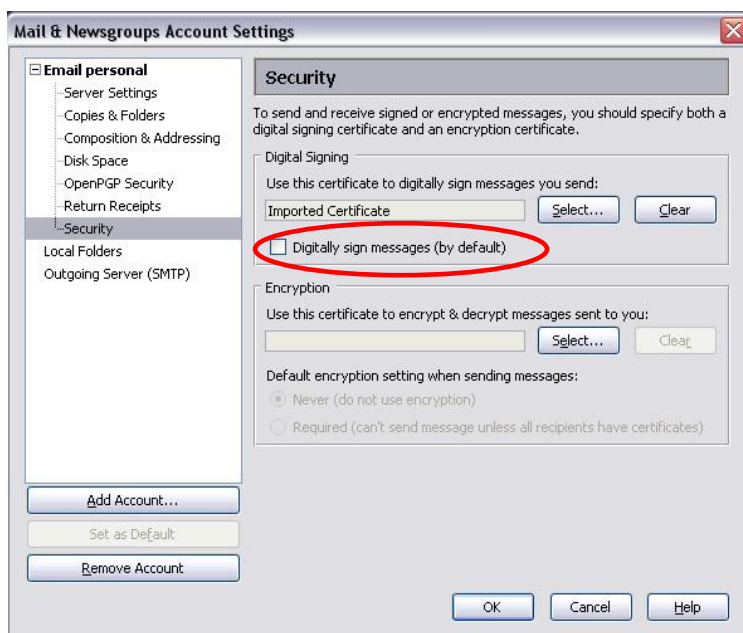


En la ventana anterior, es necesario generar escoger del menú el certificado que acaba de ser incorporado en el repositorio y presionar el botón '**OK**'. Aparecerá la siguiente ventana:



En el mensaje anterior, se ofrece la posibilidad de utilizar el mismo certificado usado para firmar mensajes, como certificado de encriptación, para que el resto del mundo pueda enviar al usuario mensajes encriptados. Si se presiona '**OK**', se usará el certificado para ambos propósitos; si se presiona '**Cancel**', se usará exclusivamente para firmar los emails que se envían.

El proceso de configuración está terminado en este punto, y debería aparecer la siguiente ventana:

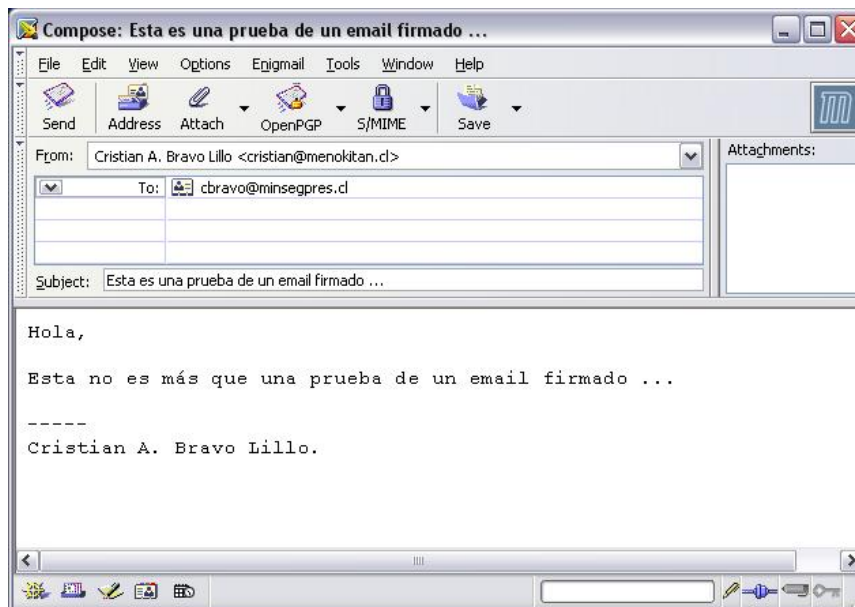


Para que todos los emails enviados sean firmados por default, debe marcarse el checkbox indicado en la figura superior.

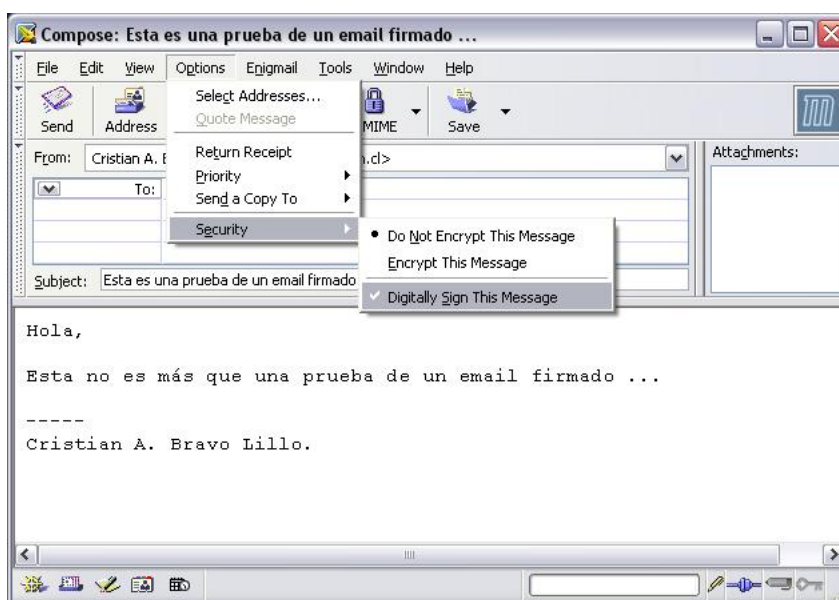
3.4.3 Cómo enviar un email firmado

A partir de lo explicado en los puntos anteriores, los emails serán firmados automáticamente, salvo que se especifique lo contrario.

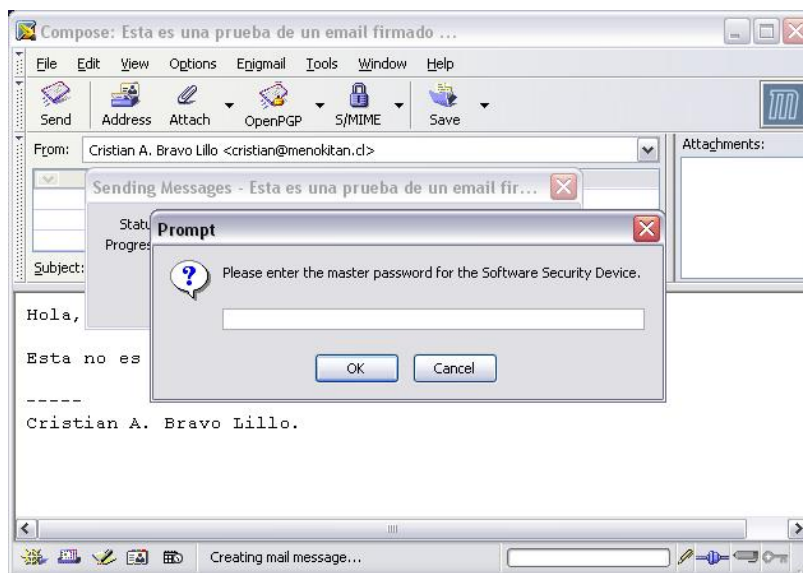
En la figura siguiente, se muestra la interfaz de envío de email de Mozilla Mail.



Es posible verificar si el email será efectivamente enviado firmado o no (y cambiar este comportamiento), a través del menú '**Options**', en la opción '**Security**' (figura siguiente). La última opción ('**Digitally Sign This Message**') es la que indica si el email será firmado. Si no se desea firmar el email, se puede desactivar esta opción.



Una vez que se presione el botón 'Send' para enviar el email, el sistema preguntará por el password del repositorio de certificados y llaves (figura siguiente). Una vez que se ingrese este password, se enviará el email firmado de manera normal.



La recepción de emails firmados es absolutamente trivial, por lo que no será explicado aquí. De igual forma, se dejará para una versión futura la verificación de la firma de un email.

3.5 FES en Email con certificados X.509 en MS Outlook

3.5.1 Solicitud de Certificado

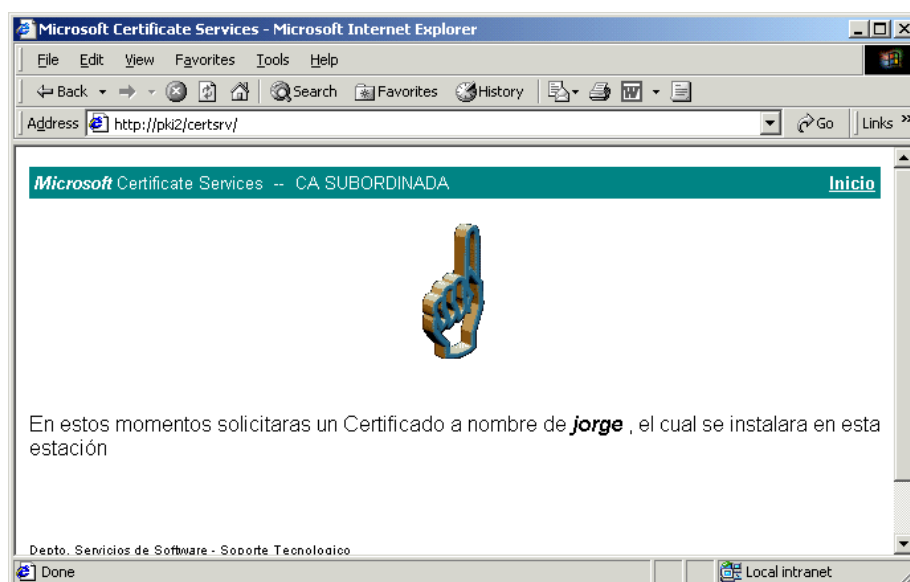
Los siguientes ejemplos fueron desarrollados a partir de una autoridad certificadora interna a una institución, levantada a través del software **Certificate Server** de Microsoft Windows 2000. El siguiente contenido es de exclusiva responsabilidad de Microsoft Chile, y fue elaborado íntegramente por Microsoft.

En primer lugar el usuario debe poseer un certificado digital emitido por alguna de las entidades certificadoras. Para ello debe utilizar el browser y acceder al sitio dispuesto para tal efecto.

Una vez ahí se despliega la siguiente pantalla para el ingreso de las credenciales del usuario. Esta pantalla es utilizada como un mecanismo de seguridad para evitar que otra persona tome el control de la estación de trabajo y solicite un certificado en lugar del usuario correspondiente.



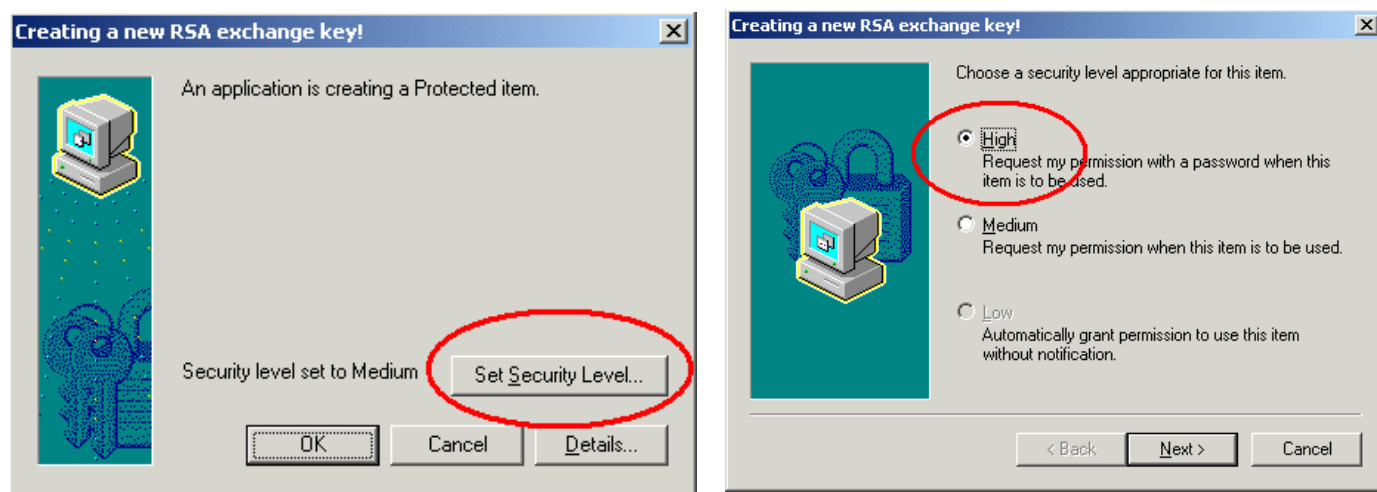
A continuación se realiza una breve navegación por la entidad certificadora, la cual culmina con la instalación del certificado.



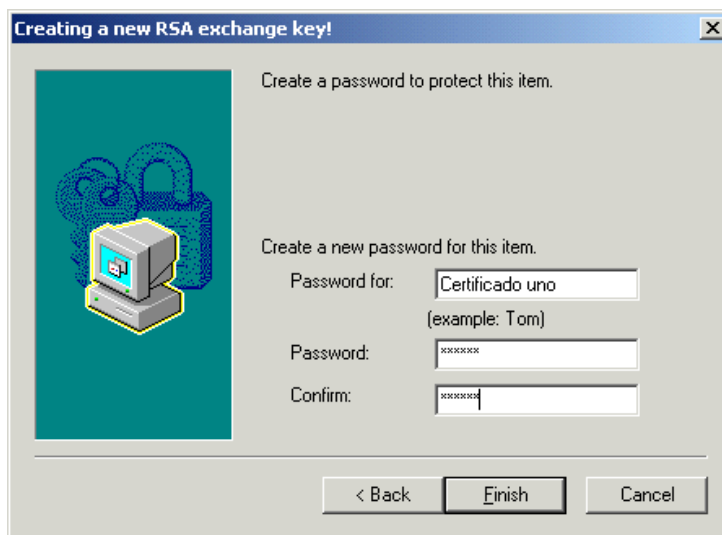
Para darle mayor seguridad a la firma electrónica, es necesario que el usuario le incorpore una clave de uso, la cual le será solicitada en el momento de firmar algún documento con dicha firma.

Los pasos que debe seguir son los siguientes:

1. **Seleccionar el nivel de seguridad en Alto (High).** Las pantallas estarán en idioma ingles, ya que los servidores fueron instalados en esa modalidad.



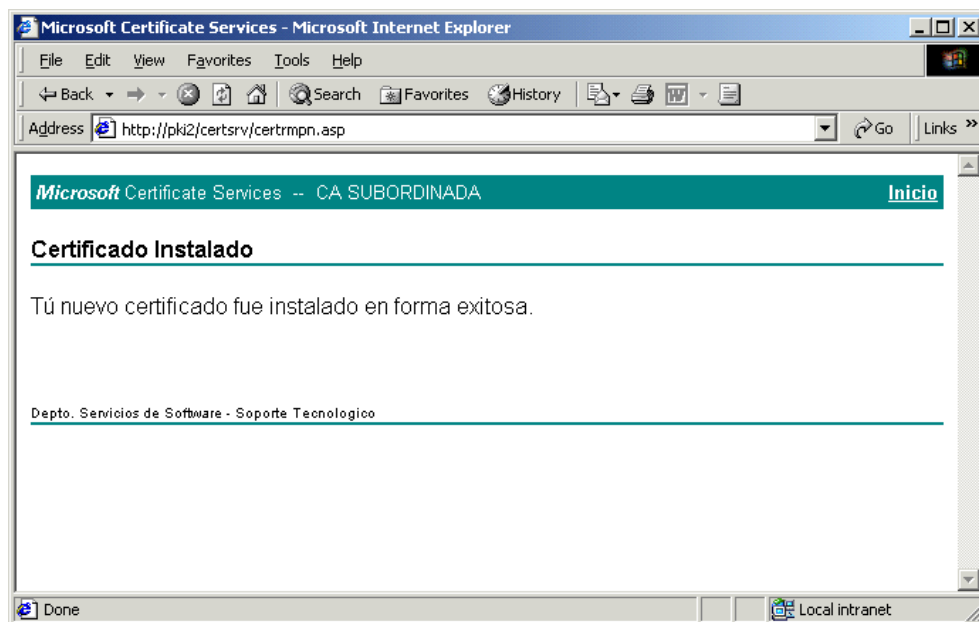
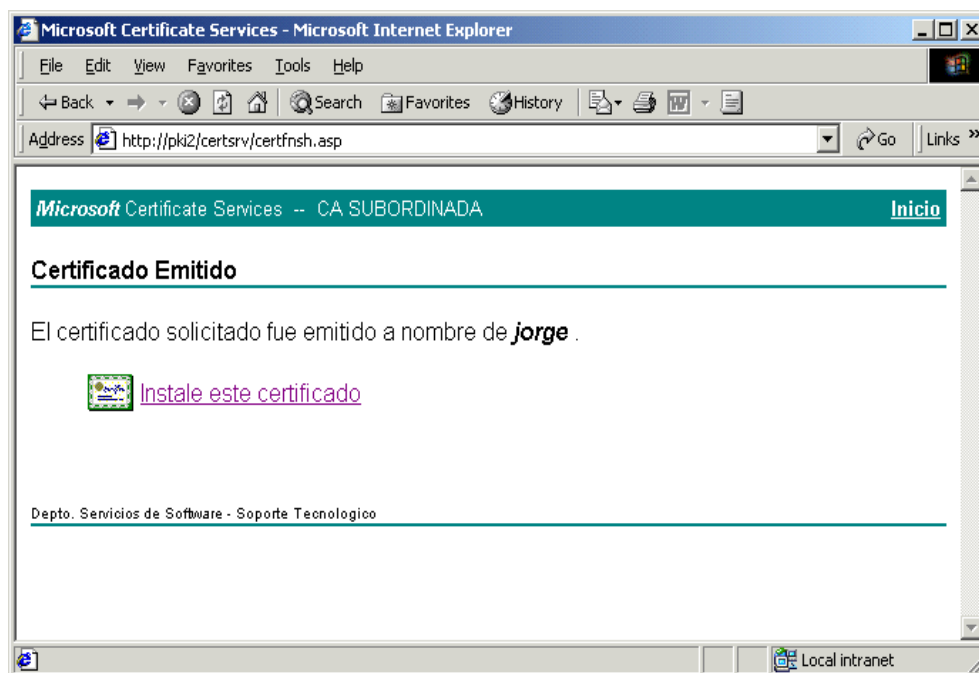
2. **A continuación se ingresa la clave de seguridad**, en conjunto con el nombre que tendrá la firma.



3. **Finalmente presione OK** y estará en condiciones de instalar el certificado con la siguiente pantalla:



- Una vez configurada la seguridad, la siguiente pantalla del browser le solicitará que instale el certificado.



Con esta pantalla de confirmación de la instalación, el usuario cuenta con un certificado y puede comenzar a utilizarlo.

3.5.2 Firma de correo electrónico

Una utilización del certificado es la firma de los mensajes de correo electrónico. Con ello se prueba que el mensaje enviado ha sido despachado por la persona que aparece en el remitente. Si alguien interceptó el mensaje, el sistema de correo avisará que el certificado es inválido, con lo cual el destinatario puede tomar alguna medida especial.

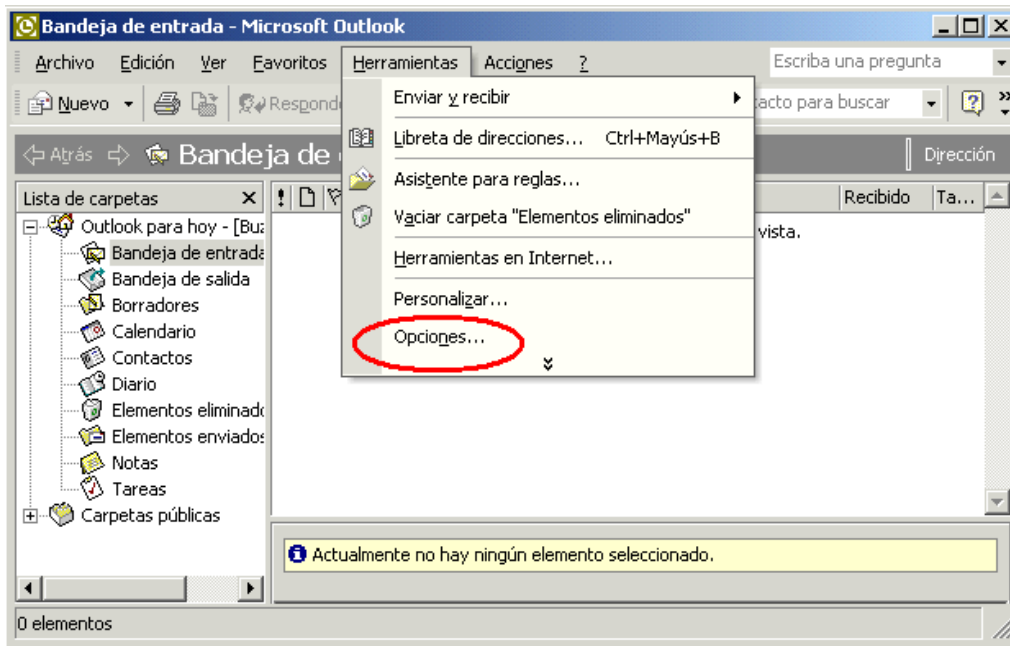
Existen dos modalidades para la firma de los mensajes.

- **Firmar todos los mensajes que salen**, lo cual significa que a cada uno de los mensajes que se envíen le será aplicada la firma digital.
- **Firmar mensajes individualmente**, lo cual significa que el usuario puede elegir cuál mensaje firma.

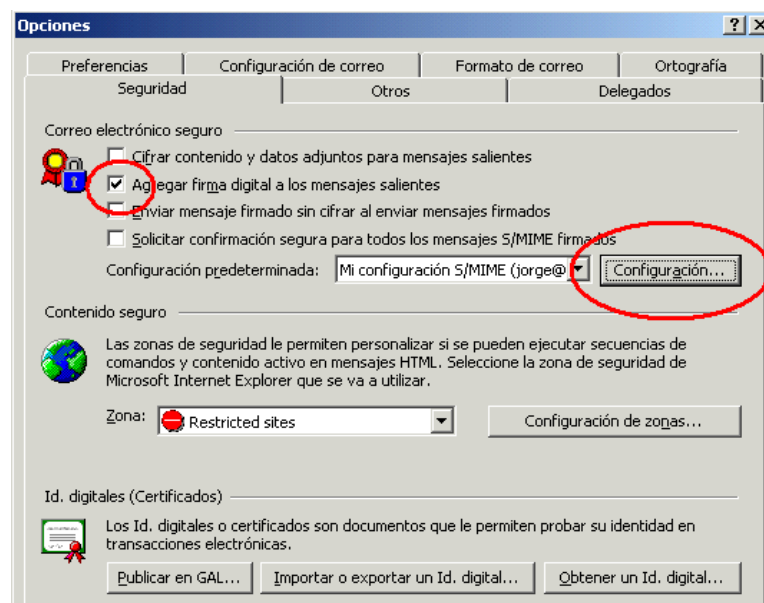
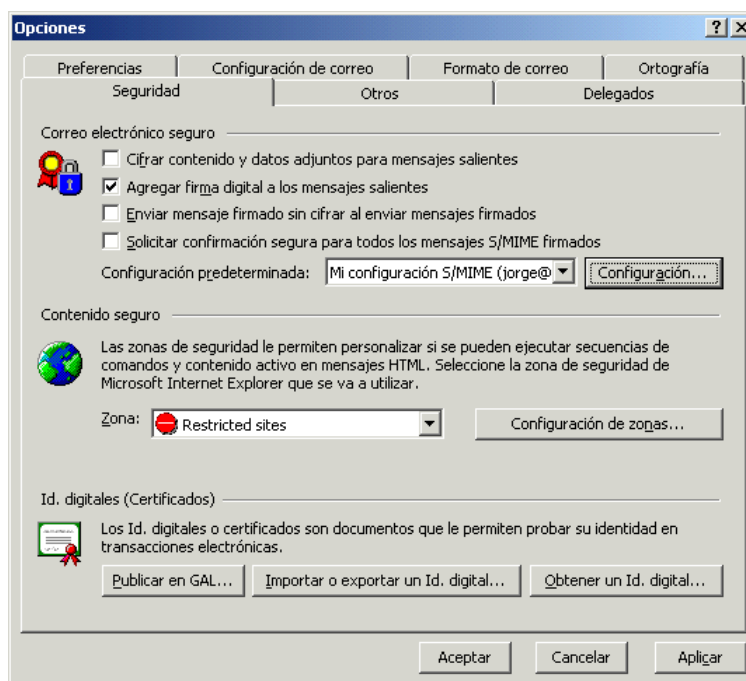
3.5.2.1 Firmar todos los mensajes que salen

En este caso se configura el Outlook 2002 de la siguiente manera:

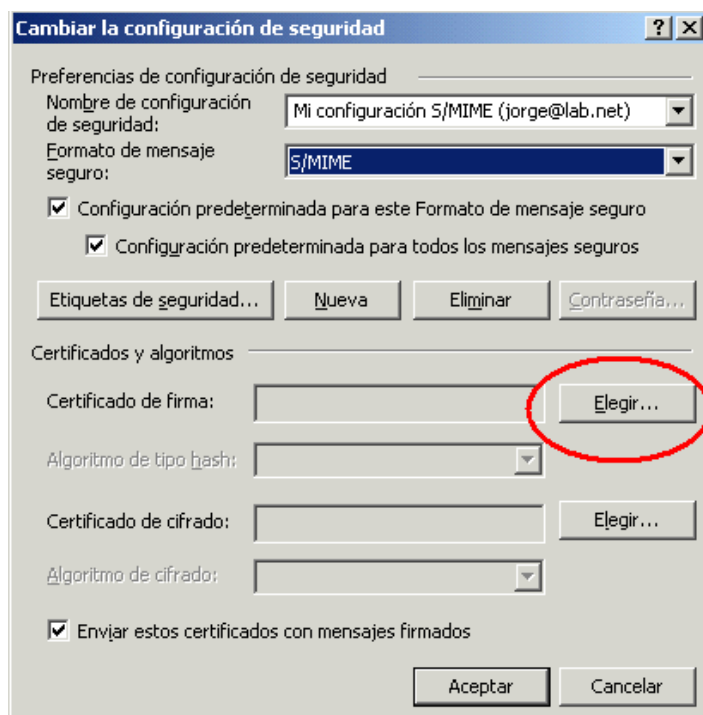
1. En la barra de **herramientas** seleccionar **opciones**:



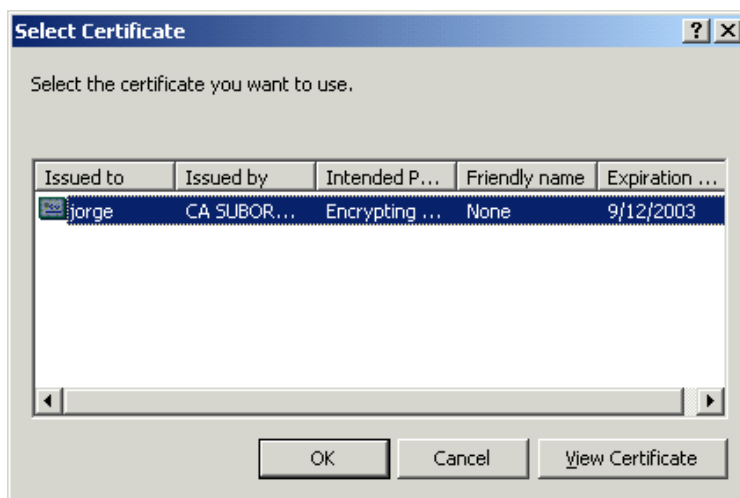
2. Seleccionar la opción: **Agregar firma digital a los mensajes salientes**



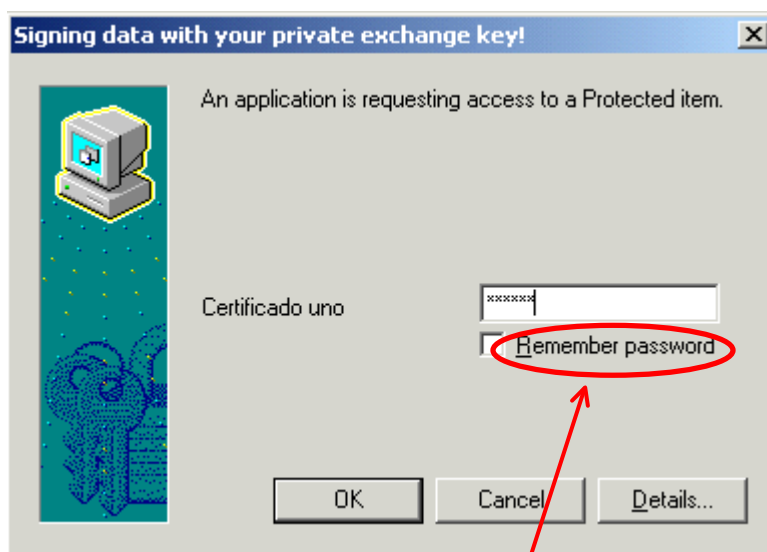
3. Presionar la opción **Configuración** para seleccionar el certificado que será utilizado.



4. Presionar elegir, y seleccionar el certificado solicitado anteriormente a la entidad certificadora. Presionar **OK**, y luego **aceptar** las restantes pantallas



5. Después se puede enviar normalmente. Antes de que se pueda enviar, aparecerá una pantalla solicitándole la clave con la cual creó el certificado. Esto permite asegurar que nadie más utilice su computador y envíe certificados firmados por usted.

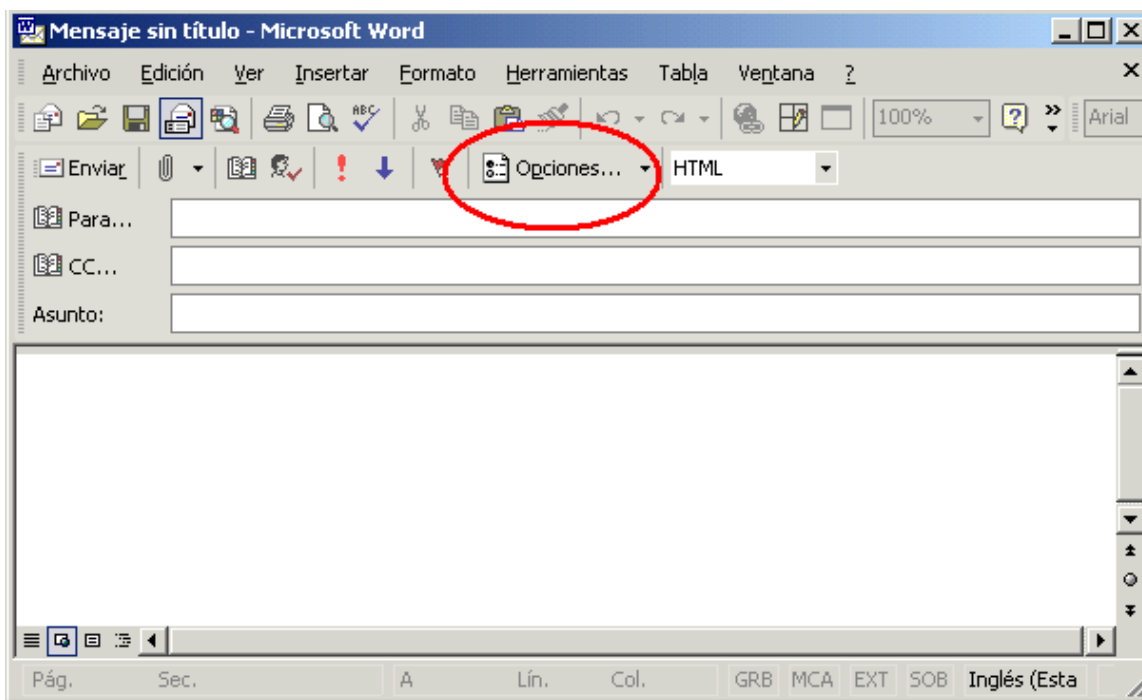


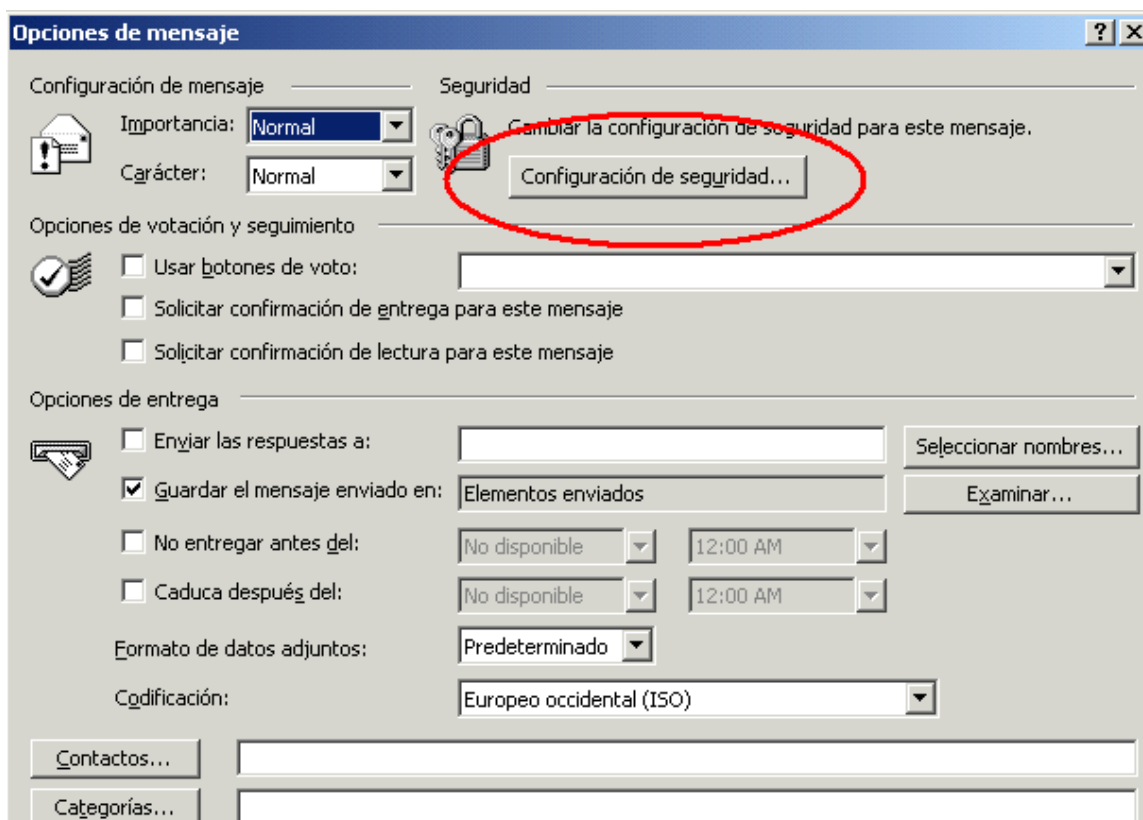
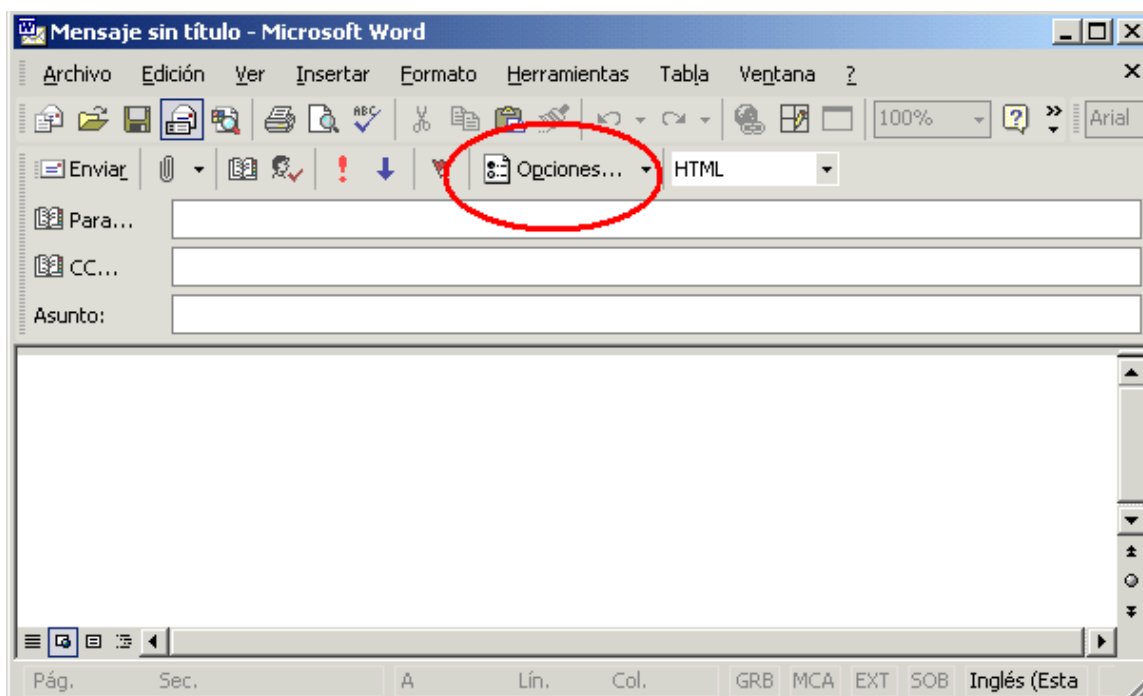
Importante: **nunca** seleccione la opción “recordar password” (*remember password*) ya que cualquier persona que utilice su computador podría utilizar su firma electrónica. Esto equivaldría a dejar un documento en blanco y firmado.

3.5.2.2 Firmar mensajes individualmente

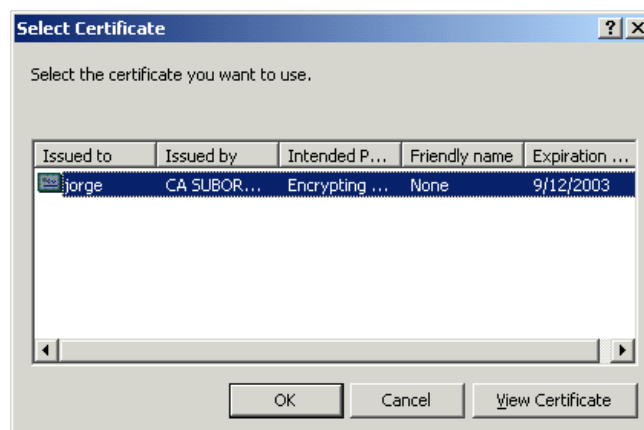
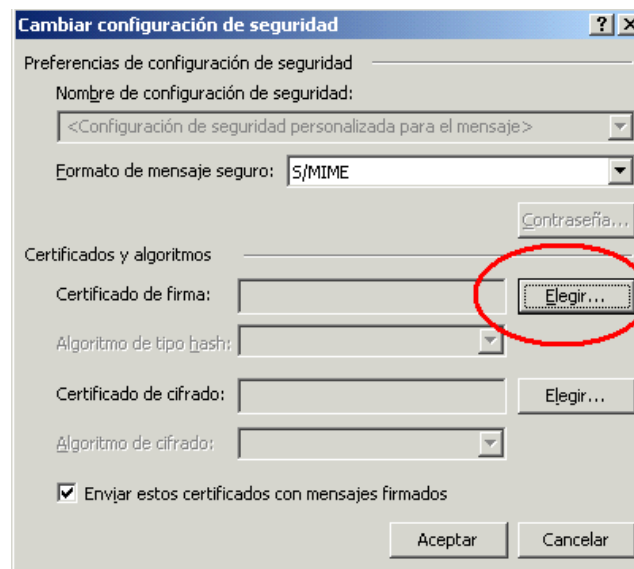
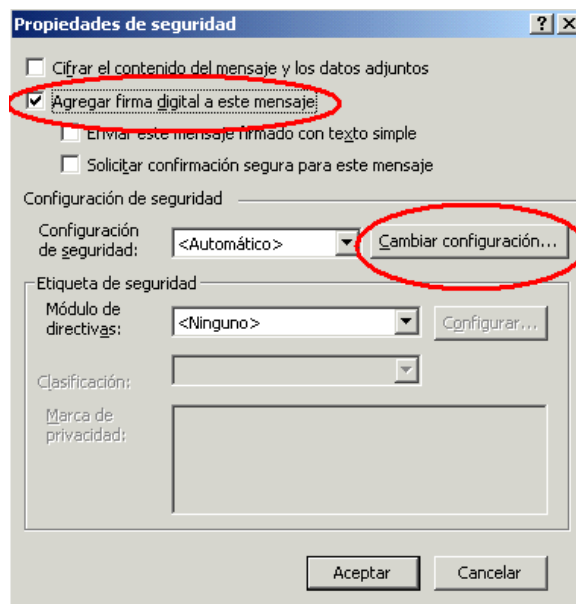
A diferencia del método anterior, en esta opción, usted puede seleccionar aquellos mensajes que desea firmar electrónicamente.

Para ello, genere un nuevo mensaje, pero en este caso el menú de opciones es el de cada mensaje:





Seleccione el botón de **Configuración de seguridad**:



Después de seleccionar el certificado, presionar **aceptar** en las pantallas siguientes y **cerrar** en la última.

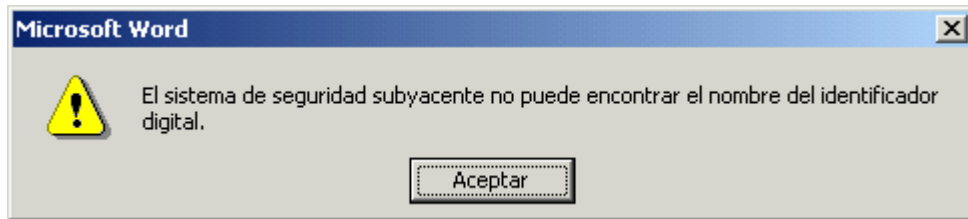
3.5.3 Envío de Mensajes

Si se utilizó alguno de los dos métodos para configurar el uso de firma electrónica en los mensajes, el envío sigue el curso normal que un mensaje normal.

Los únicos problemas que pueden ocurrir son los siguientes:

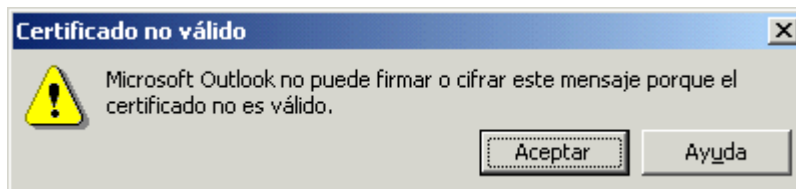
3.5.3.1 Envío de mensajes con clave inválida

Si se equivoca al ingresar la password del certificado (no la de su cuenta) aparecerá un mensaje de la siguiente forma:



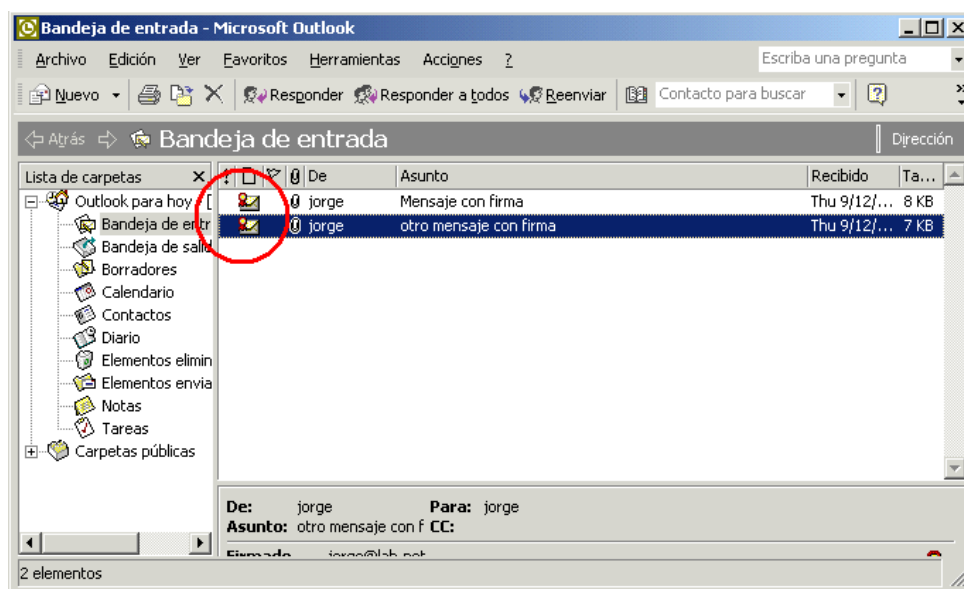
3.5.3.2 Envío de mensajes con firma inválida

Si el certificado es revocado o es inválido, el remitente no podrá enviar el mensaje, apareciéndole un mensaje de error como el siguiente:



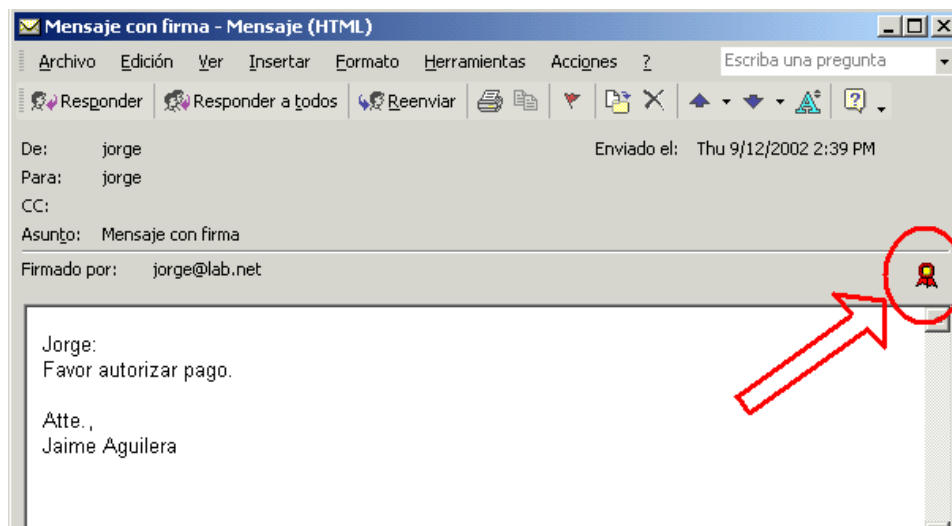
3.5.4 Recepción de los mensajes

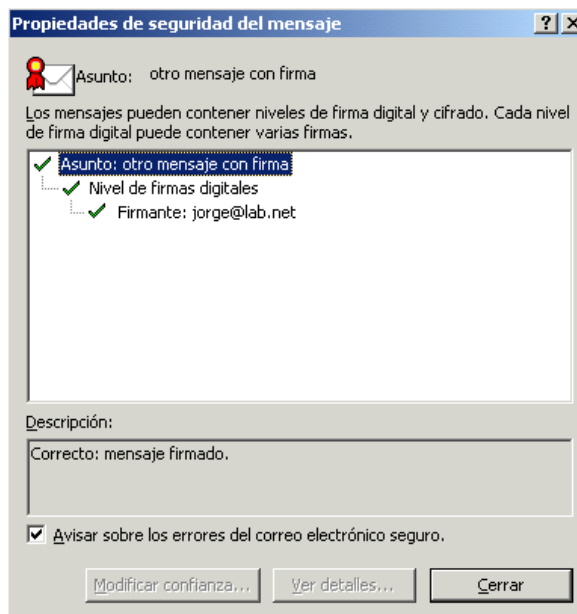
El receptor de los mensajes electrónicos firmados los recibirá de la siguiente forma:



En el cual el símbolo de un sello sobre el sobre indica que es un mensaje con firma electrónica.

La forma de verificar la firma es presionando el símbolo de certificado que aparece en el extremo:

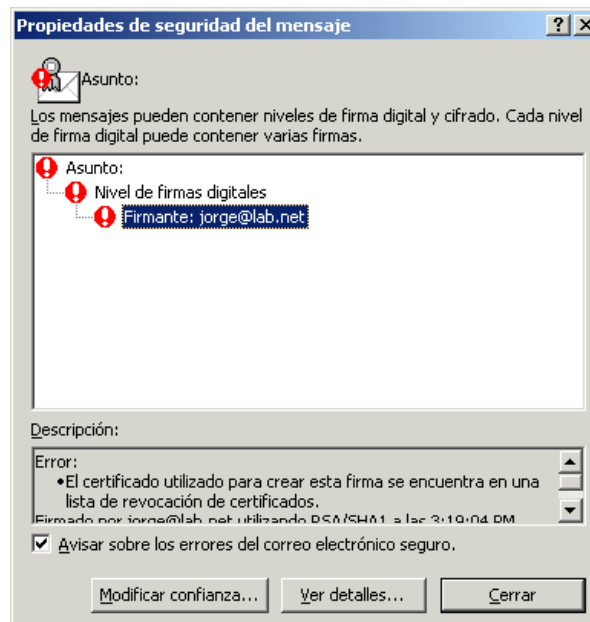




Si la firma es inválida, es decir, si el certificado es inválido, alguna de las tres opciones que aparecen en color verde, aparecerán en color amarillo si es una advertencia o rojo si existe un error.

3.5.5 Recepción de mensajes con firma inválida

Si el remitente recibe un mensaje con firma inválida, aparecerá un mensaje indicándole que la firma no corresponde por alguna razón. Por ejemplo si el certificado ha sido revocado porque el remitente ya no es un usuario válido (fue despedido, no tiene poder de firma, etc) al verificar la firma se verá una pantalla de la siguiente forma:



Con esta verificación de la firma, la cual equivale a ver la firma normal de un documento en papel, el usuario destinatario estará absolutamente seguro que el remitente es quien dice ser.