Autoritat de Certificació de la Comunitat Valenciana

Manual de uso de correo seguro en Mozilla Mail

Fecha: 22/03/2006	**Versión:** 1.1
	Nº de páginas: 15

GENERALITAT VALENCIANA

Secretaria Autonòmica de Telecomunicacions i Societat de la Informació

Conselleria d'Infraestructures i Transport

Este documento es propiedad de la Generalitat Valenciana.
Queda prohibida su reproducción total o parcial sin autorización previa de la Generalitat Valenciana

Tabla de Contenido

1. Qué son las firmas digitales y el cifrado

Al redactar un mensaje de correo, tiene la posibilidad de adjuntar una firma digital. La firma digital permite a los destinatarios del mensaje comprobar que el mensaje viene realmente de usted y que no ha sido manipulado desde el momento del envío.

Al redactar un mensaje de correo, también puede cifrarlo si lo desea. El cifrado hace que resulte muy difícil para cualquiera, excepto el destinatario, leer el mensaje mientras éste viaja por Internet.

Antes de firmar o cifrar un mensaje, debe seguir estos pasos configurar los valores de seguridad de su cuenta de correo. Si desea más información, consulte el apartado 2.2 de este manual.

Cuando haya seguido todos los pasos, siga las instrucciones que aparecen en los apartados 3, 4 y 5 de este manual, para enviar y recibir correos firmados y cifrados.

1.1.1. Cómo funcionan las firmas digitales

Para crear una firma digital para un mensaje electrónico que vaya a enviar, le hacen falta dos cosas:

- Un **certificado de firma** que lo identifique para este propósito. Cada vez que firme un mensaje, su certificado de firma se enviará con él. El certificado incorpora una **clave pública**. La presencia del certificado en el mensaje permite al destinatario comprobar su firma digital.
- Una **clave privada**, que se crea y se almacena en el ordenador al obtener un certificado por vez primera.

  La clave privada se protege mediante una **contraseña maestra**, y el navegador no la revela a nadie. Las aplicaciones con firma, como por ejemplo el cliente de correo, emplean la clave privada para crear una firma digital única y comprobable para todos los mensajes que desee firmar.

1.1.2. Cómo funciona el cifrado

Para cifrar un mensaje de correo, debe tener un **certificado de cifrado** para cada uno de los destinatarios del mensaje. La clave pública de cada certificado se usa para cifrar el mensaje para el destinatario en cuestión.

Si no posee un certificado para todos y cada uno de los destinatarios, el mensaje no podrá cifrarse. En este manual se describe cómo obtener la clave pública de otros usuarios.

El programa del destinatario usa la clave privada del destinatario, que permanece en su propio ordenador, para descifrar el mensaje.

2. Configuración de Mozilla Mail

2.1. Requisitos previos

Esta guía asume que el usuario dispone de:

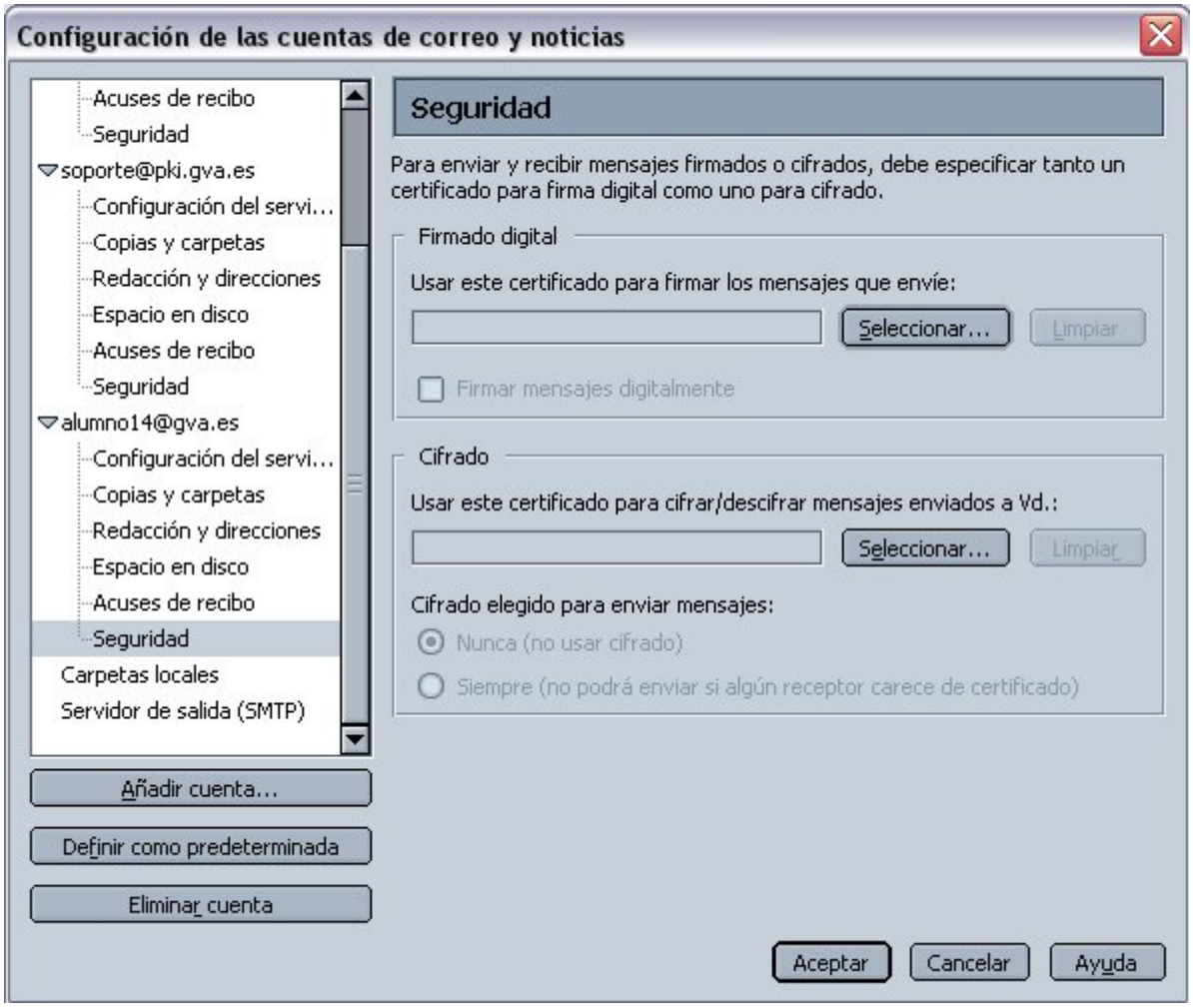
- Una **cuenta de correo configurada en Mozilla Mail** para el envío y recepción de correo electrónico desde un servidor de correo.
- Los **certificados digitales registrados en el navegador de Mozilla**. y en el *Manual de instalación de los certificados digitales en fichero*.Firmar y cifrar mensajes

2.2. Configuración de seguridad

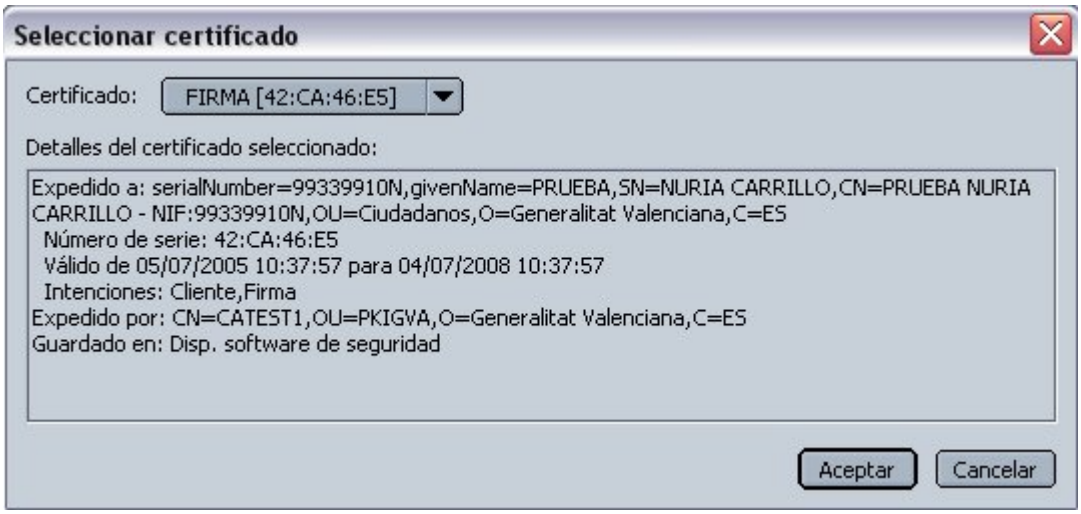
Una vez que haya obtenido un certificado deberá especificar los certificados que quiera usar para firmar y cifrar mensajes. Previamente debe haber realizado el registro de los certificados digitales en Mozilla.

Para indicar los certificados de firma y cifrado que quiere usar con una cuenta concreta, comience desde la ventana principal de correo en Mozilla:

1. Abra el menú *Editar* y seleccione *Configuración de cuentas de Correo y Noticias*.
2. Haga clic en *Seguridad*, debajo del nombre de la cuenta de correo cuyos valores de seguridad desea configurar.



3. Debajo de *Firmado digital*, haga clic en *Seleccionar* . Verá un cuadro de diálogo en el que podrá seleccionar entre los certificados de firma disponibles.



4. Elija el certificado de firma que quiera usar y haga clic en *Aceptar*.

5. Siga los mismos pasos con el cifrado. Haga clic en el botón *Seleccionar*, elija el certificado de cifrado que desee usar y haga clic en Aceptar.

Opcionalmente, en esta pantalla se puede indicar también que desea firmar o cifrar habitualmente todos los mensajes enviados desde una cuenta en concreto. Para configurar los valores predeterminados de firma y cifrado, empiece desde el panel de *Seguridad de la cuenta* (como se describió anteriormente) y seleccione los valores de la forma siguiente:

- Debajo de **Firma digital**:
    - **Firmar mensajes digitalmente:** cuando esta casilla esté activada, todos los mensajes que envíe desde esta cuenta se firmarán digitalmente, a no ser que indique lo contrario antes de enviar un mensaje. Para anular esta opción predeterminada, desactive la casilla.
- Debajo de **Cifrado**: Debe elegir una de las siguientes opciones:
    - **Nunca:** cuando esta opción esté seleccionada, ninguno de los mensajes que envíe desde esta cuenta estará cifrado, a no ser que indique lo contrario antes de enviarlo.
    - **Requerido:** cuando esta opción esté seleccionada, todos los mensajes que envíe desde esta cuenta estarán cifrados, pero sólo en caso de que posea certificados válidos para cada uno de los destinatarios del mensaje. Si no posee todos los certificados necesarios, el mensaje no se enviará, a no ser que se desactive el cifrado para ese mensaje.

Cuando haya terminado de configurar los valores de seguridad, haga clic en *Aceptar* para confirmarlos.

3. Envío de mensajes firmados y cifrados digitalmente con Mozilla Mail

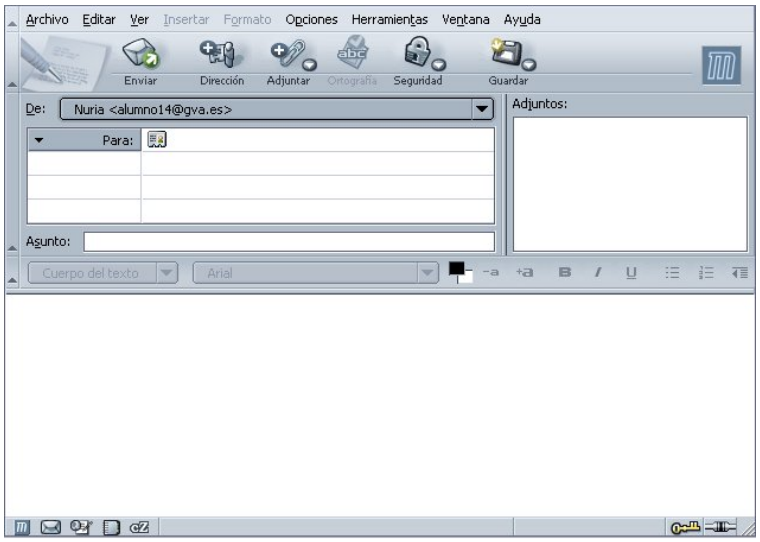
La configuración que se haya especificado en *Configuración de cuentas de correo y grupos de noticias*, *Seguridad* determinará los valores predeterminados de cada ventana de redacción de mensajes que abra cuando vaya a escribir.

Para abrir la ventana de redacción de mensajes, inicie el cliente de correo y pulse el botón *Redactar*.

Inmediatamente identificará los valores de seguridad predeterminados por la presencia o ausencia de estos iconos en la esquina inferior derecha de la ventana:

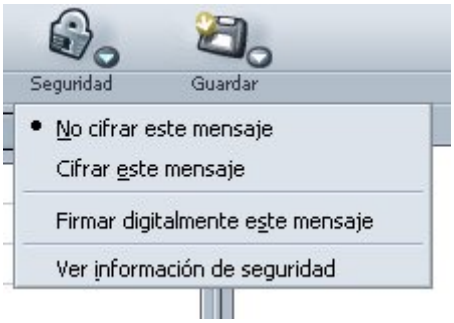
El mensaje estará firmado digitalmente (siempre que posea un certificado de correo válido que lo identifique).

El mensaje estará cifrado (siempre que posea certificados válidos para todos los destinatarios).



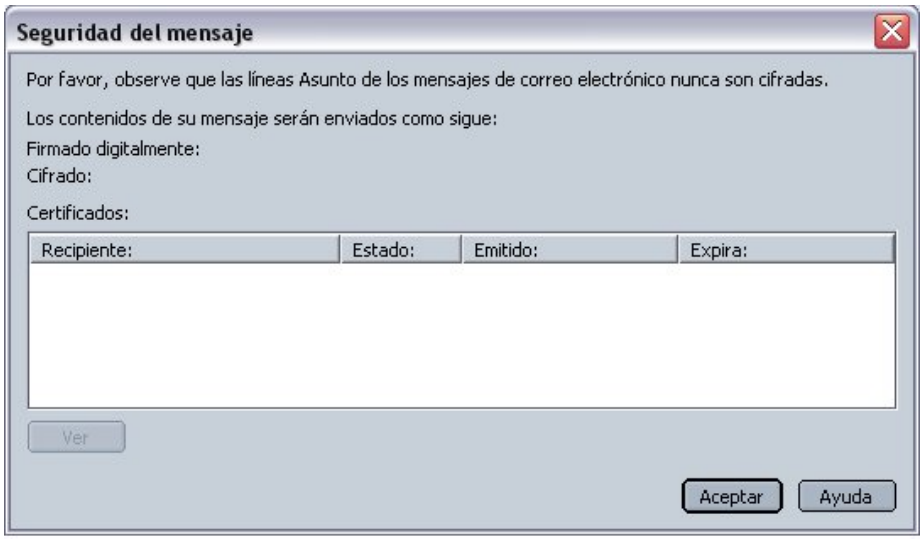
Para activar o desactivar estos valores, haga clic en la flecha que está justo debajo del icono de *Seguridad* de la barra de herramientas de mensajes, hacia la parte superior de la ventana.

Luego, en la lista desplegable, seleccione el elemento que desee.



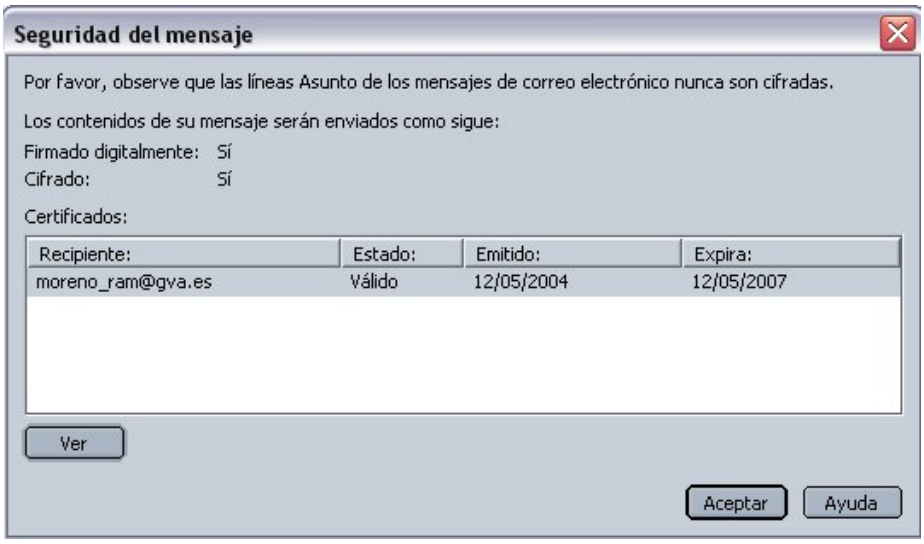
- **No cifrar este mensaje:** elija este elemento para desactivar el cifrado en este mensaje. El mensaje se enviará sin cifrar por Internet.
- **Cifrar este mensaje:** elija este elemento para activar el cifrado en este mensaje. El mensaje se enviará cifrado. No obstante, no podrá enviarse a no ser que posea certificados válidos para todos los destinatarios.
- **Firmar digitalmente este mensaje:** elija este elemento para activar o desactivar la firma digital en este mensaje. Si hay una marca de verificación, significa que el mensaje se firmará.
- **Ver información de seguridad:** elija esta opción para ver información detallada sobre el estado de seguridad de este mensaje; lo ayudará a determinar, por ejemplo, si necesita obtener un certificado para uno de los destinatarios. Para acceder a esta opción, Ver información de seguridad, también puede hacer clic en el icono de la llave o el candado.

  La ventana Seguridad del mensaje describe el modo en que se enviará el mensaje:



- **Firmado digitalmente:** esta línea indica si el mensaje irá firmado. Hay tres posibilidades:
    - **Sí:** se ha activado la firma digital para este mensaje, hay un certificado válido que lo identifica y el mensaje puede firmarse.
    - **No:** se ha desactivado la firma digital para este mensaje.
    - **Imposible:** se ha activado la firma digital para este mensaje. Sin embargo, no dispone de un certificado válido que lo identifique o hay otros problemas que imposibilitan la firma del mensaje.
- **Cifrado:** esta línea indica si el mensaje irá cifrado. Hay tres posibilidades:
    - **Sí:** se ha activado el cifrado para este mensaje, hay certificados válidos para todos los destinatarios y el mensaje se puede cifrar.
    - **No:** se ha desactivado el cifrado o bien no es posible para este mensaje.
    - **Imposible:** se ha activado el cifrado para este mensaje. Sin embargo, faltan certificados para al menos uno de los destinatarios de la lista, no hay ningún destinatario en la lista, o hay problemas de otro tipo que imposibilitan el cifrado.

La ventana Seguridad del mensaje también lista los certificados de los que se dispone para los destinatarios del mensaje:



- **Ver.** Para ver los detalles de cualquier certificado de la lista, seleccione el nombre y haga clic en *Ver*.

4. Obtención de la clave pública de otros usuarios

Para enviar correo cifrado a un usuario es necesario disponer de la clave pública del mismo. A continuación describimos las formas posibles de la clave pública de un usuario.

Cada vez que envíe un mensaje firmado digitalmente, automáticamente enviará con él su certificado de cifrado. Por ello, una la forma más sencilla de obtener el certificado de otra persona es **que dicha persona le envíe un mensaje cifrado digitalmente**.

Cuando reciba un mensaje de ese tipo, **el administrador de certificados**, que es la parte del navegador que controla los certificados, almacenará automáticamente el certificado del remitente.

Además existen otras dos formas de obtener la clave pública de otros usuarios, que pasamos a describir a continuación:

- Desde el Directorio GVA.
- Desde la página web de la ACCV.

Desde el Directorio GVA.

Esta opción sólo es válida para funcionarios de la Generalitat Valenciana ya que se trata de configurar el directorio LDAP corporativo, que contiene sus direcciones de correo y certificados digitales.

Una vez configurado, permitirá a su Libreta de Direcciones buscar automáticamente en el directorio direcciones de correo y otra información de contacto, como los certificados digitales.

Así, cuando utiliza una cuenta que está configurada para buscar direcciones en un directorio, se usará ese mismo directorio para buscar los certificados correspondientes cuando intente enviar un mensaje cifrado a uno o más destinatarios de los cuales no se disponga el certificado en un archivo local.

También se acudirá al directorio para aquellos certificados que falten localmente cuando abra el menú desplegable bajo el icono Seguridad en la ventana Componer y escoja Ver información de seguridad.

Para añadir un nuevo directorio, comenzando desde la ventana de la Libreta de Direcciones:

1. Abra el menú *Archivo* y escoja *Nuevo*, y a continuación *Directorio LDAP*. Verá el cuadro de diálogo de Servidores de directorio LDAP.
2. Escriba la siguiente información en la pestaña *General*:

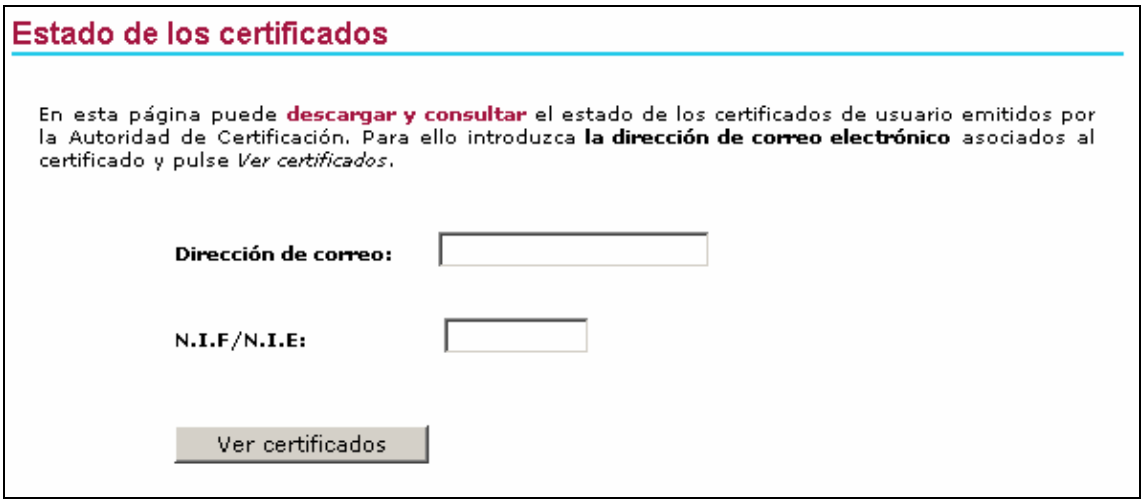
- **Nombre**: introduzca el nombre del servicio de directorio (por ejemplo, LDAP GVA).
- **Hostname**: introduzca el nombre del servidor, **ldap.gva.es**.
- **DN base**: esta opción se usa para configurar el DN base, para restringir la búsqueda. Debe indicar **o=Generalitat Valenciana,c=ES**.
- **Número de puerto**: Introduzca el puerto del servidor LDAP. El predeterminado es el 389.

3. Pulse *Aceptar* para cerrar el cuadro de diálogo de *propiedades del servidor de directorio* y confirmar la configuración. Compruebe que el directorio añadido aparece en la lista de la Libreta de Direcciones.

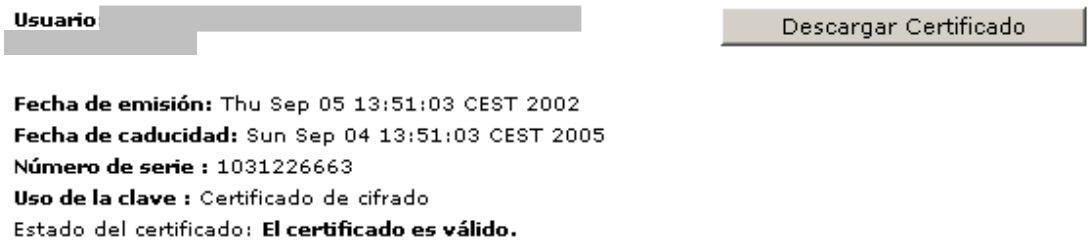
Importar certificados de otras personas

En el caso particular de los certificados emitidos por la Autoridad de Certificación de la Generalitat Valenciana, otra alternativa para obtener la clave pública de otros usuarios es hacerlo a través de la página web, www.accv.es, pulsando el icono a continuación:

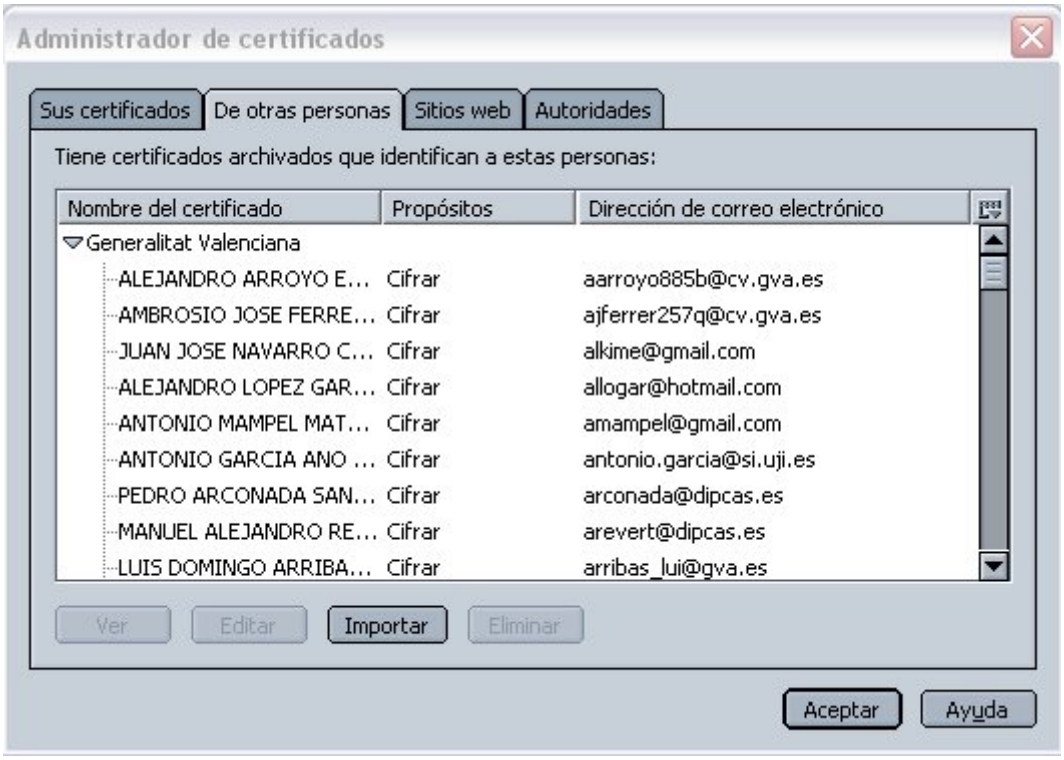
Aparecerá la siguiente pantalla:



En la siguiente pantalla aparece un listado con los certificados del usuario e información sobre ellos. Pulsa el botón **Descargar certificado**, **Instalar certificado**, **Guardar**. Indica la ubicación de tu PC dónde quieres guardar el fichero del certificado.



Una vez descargado, abra el cliente de correo Mozilla y vaya a *Editar, Preferencias, Privacidad&Seguridad, Certificados, Administrar Certificados*. Seleccione la pestaña *De otras personas*.



Pulse el botón *Importar*. A continuación se abrirá una ventana en la que debe indicar la ubicación del fichero a importar, donde lo haya descargado previamente.

Pulse *Aceptar* para confirmar la importación. A continuación vuelva a entrar en *Administrar Certificados, De otras personas*, para comprobar que la importación se realizó con éxito.

5. Seguridad de los mensajes mensajes recibidos

Esta sección describe la ventana de Seguridad del mensaje, que se puede abrir para cualquier mensaje que haya recibido. Si aún no ha llegado a la ventana Seguridad del mensaje de un mensaje recibido, siga estos pasos:

1. En la ventana *Correo*, seleccione el mensaje cuya información de seguridad desea ver.
2. Abra el menú *Ver* y seleccione *Información de seguridad del mensaje*.

La ventana de Seguridad del mensaje muestra la siguiente información:

- **Firma digital:** la sección superior indica si el mensaje está firmado digitalmente y, de ser así, si la firma es válida.

  Si la firma no es válida debido a un problema de los valores de confianza de algún certificado, puede usar el *Administrador de certificados* para ver o modificar estas opciones.

- **Ver certificado de firma.** Si el mensaje está firmado, haga clic en este botón para ver el certificado que se usó para firmarlo.

- **Cifrado.** La sección inferior indica si el mensaje está cifrado y si existen problemas de cifrado.

  - Si el contenido del mensaje se ha alterado por el camino, debería pedirle al remitente que volviera a enviárselo. Es posible que los cambios se deban a problemas de red.

  - Si no tiene una copia de su propio certificado (el que usó el remitente para cifrar el mensaje) en el ordenador, no podrá recuperarse la clave privada necesaria para descifrar el mensaje. La única solución es importar una copia de seguridad del certificado y su clave privada correspondiente (consulte *Sus certificados* si desea más información). Si no tiene acceso a la copia de seguridad del certificado, no podrá descifrar el mensaje.