El presente documento pretende describir el proceso a seguir para configurar su certificado personal emitido por la ACCV en el cliente de correo-e Mozilla Thunderbird para el envío de mensajes de correo-e firmados digitalmente y/o cifrados sobre Windows, Mac OS X o GNU\Linux.

ÍNDICE

1. IREQUISITOS PREVIOS

CERTIFICADO DIGITAL

Para poder firmar digitalmente y/o cifrar sus mensajes de correo-e usted debe disponer al menos de un certificado reconocido de persona física (de Ciudadano, de Empleado Público o de Pertenencia a Empresa) o de persona jurídica (de Entidad) emitido por la ACCV y en vigor.

Dicho certificado digital **deberá estar asociado a la cuenta de correo-e** que desee emplear para el envío de correos-e firmados y/o cifrados.

MOZILLA THUNDERBIRD

Debe tener instalado en su equipo el cliente de correo-e Mozilla Thunderbird, el cual puede descargar desde https://www.mozilla.org/es-ES/thunderbird/.

Adicionalmente, deberá haber configurado su cuenta de correo-e en Mozilla Thunderbird para la recepción y envío de mensajes. Si tiene dudas sobre cómo realizar esta configuración, consulte la documentación de Mozilla.

2. CONFIGURACIÓN DE SU CERTIFICADO EN MOZILLA THUNDERBIRD

Antes de comenzar a enviar mensajes de correo-e firmados y/o cifrados es necesario:

- Indicar a Mozilla Thunderbird que debe confiar en los certificados digitales que emite la ACCV.
- Instalar su certificado personal en Mozilla Thunderbird. La instalación variará dependiendo de si su certificado es en soporte software o en tarjeta criptográfica.

2.1. CONFIAR EN LOS CERTIIFICADOS QUE EMITE LA ACCV

1. Abra la página http://www.accv.es y pulse en el icono **Descargar Certificados ACCV** (zona inferior derecha).

2. Selecciones los siguientes certificados digitales y guárdelos en su **Escritorio**:

   - *Certificado de la Autoridad de Certificación Raíz: ACCV Raíz 1 (CRT 4KB) - Vigente hasta 31/12/2030*
   - *Certificado de la Autoridad de Certificación Raíz: Root CA Generalitat Valenciana (CRT 3KB) - Vigente hasta 01/07/2021*
   - *Certificado de la Autoridad de Certificación para personas físicas y otros usos (EJBCA): ACCV-CA2 (CRT 3KB)*
   - *Certificado de la Autoridad de Certificación de certificados para personas jurídicas: ACCV-CA1 (CRT 3KB)*
   - *Certificado de la Autoridad de Certificación para personas físicas y otros usos (Nueva Jerarquía): ACCVCA-120*
   - *Certificado de la Autoridad de Certificación de certificados para entidades (Nueva jerarquía): ACCVCA-110)*

3. A continuación abra Mozilla Thunderbird y acuda al menú de **Opciones** (o *Preferencias*, según versión). Seleccione **Avanzado**, pestaña **Certificados** (o *Cifrado*, según versión) y haga clic en el botón **Ver certificados**.

4. Esta acción abrirá el *Administrador de certificados* de Mozilla Thunderbird. Escoja la pestaña **Autoridades**, presione sobre el botón **Importar...** y escoja de su *Escritorio* el primero de los certificados que ha descargado hace un momento (*ACCV Raíz 1*) para añadirlo al listado de certificados de confianza.

   Le aparecerá una ventana donde deberá **marcar las tres casillas de verificación** y pulsar **Aceptar**.

5. Repita esta última acción para el resto de certificados que ha descargado hasta haberlos importado todos al listado.

2.2. INSTALAR SU CERTIFICADO PERSONAL

En el caso de los **certificados reconocidos de Ciudadano**, la ACCV provee a sus usuarios de dos certificados, uno con el uso de FIRMA y otro con el de CIFRADO. El de FIRMA es el principal, ya que se utiliza para identificarse telemáticamente en los trámites, así como para firmar electrónicamente documentos o mensajes. El de CIFRADO se utiliza sólo para cifrar información, normalmente en el envío y recepción de correos-e.

Cuando este tipo de certificados se emiten en tarjeta criptográfica, ambos certificados se encuentran en el interior de la tarjeta. Cuando se emiten en soporte software, el usuario generá el de FIRMA mediante un *Código de Generación* en su equipo, mientras que el de CIFRADO puede descargarlo en formato fichero .p12 desde el *Área Personal de Servicios de Certificación* (APSC) de la ACCV. Dispone de información al respecto en:

http://www.accv.es/fileadmin/Archivos/manuales_ayuda/Manual-APSC.pdf

Para los **otros tipos de certificados,** ya sea en soporte tarjeta o software, se genera un único certificado que cuenta con ambos usos: CIFRADO y FIRMA.

CERTIFICADO DIGITAL EN SOPORTE SOFTWARE

Deberá disponer de su certificado en un fichero con extensión .p12. Si tiene instalado su certificado en su navegador web, puede exportarlo a un fichero .p12 siguiendo el manual correspondiente del siguiente enlace:

http://www.accv.es/ayuda/exportar-el-certificado-digital-desde-el-navegador-web-a-fichero/

⚠ Recuerde que si su certificado es de Ciudadano en soporte software, deberá disponer de dos ficheros .p12, uno con el certificado de FIRMA y otro con el de CIFRADO.

Le recomendamos que guarde su certificado/s en fichero .p12 en su **Escritorio**. A continuación, deberá registrarlo/s en Mozilla Thunderbird siguiendo los pasos a continuación:

1. Abra Mozilla Thunderbird y acuda al menú de **Opciones** (o *Preferencias*, según versión). Seleccione **Avanzado**, pestaña **Certificados** (o *Cifrado*, según versión) y haga clic en el botón **Ver certificados**.

2. Esta acción abrirá el *Administrador de certificados* de Mozilla Thunderbird. Escoja la pestaña **Sus certificados**, presione sobre el botón **Importar...** y escoja de su *Escritorio* el fichero .p12 para instalarlo.

   Introduzca el PIN/contraseña que protege dicho fichero .p12 cuando Thunderbird se lo solicite y pulse **Aceptar**.

3. Finalmente, si su certificado es reconocido de Ciudadano, entonces debe repetir el paso anterior para el segundo fichero .p12 que posee.

Llegados a este punto, si ha realizado todos los pasos correctamente, tendrá configurado su certificado o certificados en Mozilla Thunderbird, listo para ser usado.

CERTIFICADO DIGITAL EN SOPORTE TARJETA

Su certificado personal en tarjeta y su lector deben haber sido configurados previamente en su equipo. De no ser así, consulte la información sobre cómo lograrlo en:

http://www.accv.es/ayuda/instalar-la-tarjeta-criptografica-manual/

Con la tarjeta y lector configurados, los pasos que debe seguir en Mozilla Thunderbird son:

1. Abra Mozilla Thunderbird y acuda al menú de **Opciones** (o *Preferencias*, según versión). Seleccione **Avanzado**, pestaña **Certificados** (o *Cifrado*, según versión) y haga clic en el botón **Dispositivos de seguridad**.

2. Se le mostrará la ventana del *Administrador de dispositivos*. Haga clic en el botón Cargar y rellene los campos del siguiente modo atendiendo al fabricante de su tarjeta y tipo de Sistema Operativo:

TIPO DE TARJETA	SISTEMA	CAMPOS
Gieseke & Devrient (G&D)	Windows	Nombre: ACCV SafeSign PKCS#11 Archivo: C:\WINDOWS\system32\aetpkss1.dll
	Mac OS X	Nombre: ACCV SafeSign PKCS#11 Archivo: /usr/local/lib/libaetpkss.dylib
	Linux	Nombre: ACCV SafeSign PKCS#11 Archivo: /usr/lib/libaetpkss.so
SIEMENS	Windows	Nombre: ACCV SIEMENS PKCS#11 Archivo: C:\WINDOWS\system32\CardOS_PKCS11.dll
	Mac OS X	No es posible emplear las tarjetas de este fabricante en sistemas Mac OS X.
	Linux	Nombre: ACCV SIEMENS PKCS#11 Archivo: /usr/local/lib/libsiecap11.so

   Pulse **Aceptar** tras rellenar los campos.

   Si desconoce el fabricante de su tarjeta, puede emplear el siguiente asistente para sistemas Windows que la ACCV ha desarrollado para informar a sus usuarios sobre este dato: http://www.accv.es/fileadmin/Archivos/software/ACCV_detectar_tarjeta.exe

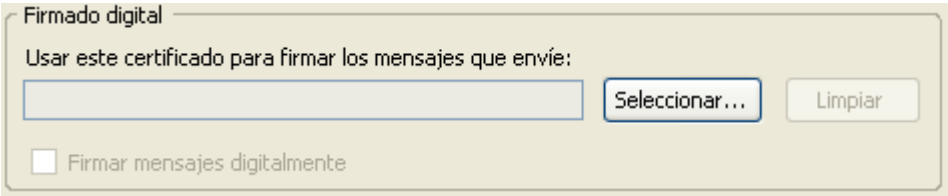
3. Finalmente otra ventana le indicará que la instalación del módulo de seguridad se ha llevado a cabo con éxito. Pulse **Aceptar**.

3. CONFIGURACIÓN PARA EL ENVÍO DE MENSAJES FIRMADOS Y/O CIFRADOS

Registrados sus certificados personales y configurada la confianza de Mozilla Thunderbird en la ACCV, ya es posible indicarle al citado cliente de correo-e que debe emplear sus certificados siempre que usted desee firmar digitalmente y/o cifrar sus mensajes. Para ello:

⚠ Si su certificado es en tarjeta criptográfica, su lector deberá estar conectado al ordenador y su tarjeta criptográfica insertada en él antes de abrir Mozilla Thunderbird.

1. Abra Mozilla Thunderbird, acuda al menú **Herramientas** (o *Edición*, según versión) y escoja la opción **Configuración de cuenta**.
2. Se mostrará la ventana de *Configuración de las cuentas*. Seleccione la cuenta sobre la que quiere realizar la configuración de seguridad y haga clic sobre el submenú **Seguridad** de dicha cuenta.
3. Dentro del cuadro titulado como *Firmado digital*, haga clic en **Seleccionar...**



4. Elija su certificado de FIRMA y haga clic en **Aceptar**.

   Mozilla Thunderbird le preguntará si desea usar ese mismo certificado para cifrar. Debe responder negativamente, seleccionando **Cancelar**.

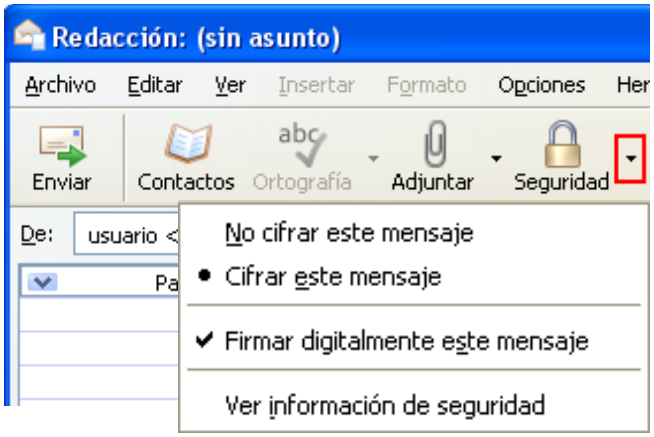
5. Siga los mismos pasos para el cifrado. Haga clic en el botón **Seleccionar** del cuadro titulado como *Cifrado*, elija el certificado de CIFRADO que desee usar y haga clic en **Aceptar**.

   Nótese que, a excepción del caso de los certificados reconocidos de Ciudadano, el certificado escogido para la FIRMA y el CIFRADO deberá ser el mismo.

6. Finalmente, haga clic en el botón **Aceptar** de la ventana de *Configuración de las cuentas* para confirmarlos los cambios.

4. ENVÍO DE MENSAJES FIRMADOS Y/O CIFRADOS

Si ha realizado correctamente los pasos anteriores, cada vez que se disponga a redactar un nuevo mensaje dispondrá de la posibilidad de emplear el menú **Seguridad** (o *S/MIME*, según versión), donde podrá decidir si desea enviar dicho mensaje firmado y/o cifrado.



En el caso del envío de mensajes cifrados, deberá considerar lo que se indica en el siguiente apartado.

5. OBTENCIÓN DE LA CLAVE PÚBLICA DE CIFRADO DE UN DESTINATARIO

Para enviar un mensaje de correo electrónico cifrado a un usuario es necesario disponer de la clave pública que alberga su certificado de cifrado.

Cada vez que un usuario envía un mensaje firmado digitalmente, si ha configurado correctamente su cliente de correo-e, automáticamente envía con el mensaje su certificado de cifrado que contiene su clave pública de cifrado. Por ello, la forma más sencilla de obtener la clave pública de otra persona es que dicha persona le envíe un mensaje firmado digitalmente. Cuando reciba un mensaje de ese tipo, el *Administrador de certificados*, que es la parte de Mozilla Thunderbird que controla los certificados, almacenará automáticamente el certificado del remitente para que usted pueda enviarle mensajes cifrados cuando lo desee.

No obstante, existen otra forma de obtener la clave pública de otros usuarios para poder enviarles mensajes cifrados:

1. Abra su navegador web y acceda a la página web http://www.accv.es/ayuda, donde debe acudir a la sección **Estado de los certificados digitales** al final de la página.
2. Deberá hacer clic sobre el enlace que se corresponda al tipo de certificado que posea el destinatario del mensaje que desea cifrar.

   Esta acción abrirá una página de búsqueda donde podrá obtener los certificados, de un tipo específico, que una determinada persona posee.
3. Únicamente deberá fijarse en el certificado que tenga el uso de CIFRADO y que esté en vigor (estado válido), presionando sobre el botón **Descargar** asociado al mismo.

   Guarde el certificado en su **Escritorio**.
4. Abra Mozilla Thunderbird y acuda al menú de **Opciones** (o *Preferencias*, según versión). Seleccione **Avanzado**, pestaña **Certificados** (o *Cifrado*, según versión) y haga clic en el botón **Ver certificados**.

   Esta acción abrirá el *Administrador de certificados* de Mozilla Thunderbird. Escoja la pestaña **De otras personas**, presione sobre el botón **Importar...** y escoja de su *Escritorio* el certificado del destinatario que acaba de descargar.
5. Compruebe que el certificado que acaba de importar se encuentra en la lista de certificados y pulse **Aceptar** para acabar con la importación.

Hecho esto, ya podrá enviarle mensajes de correo-e cifrados a la cuenta que dicha persona haya asociado al certificado que acaba de registrar.