TEXTO DIVULGATIVO

APLICABLE A LOS

CERTIFICADOS CORPORATIVOS DE PERSONAL ADMINISTRATIVO EN SOFTWARE

Este documento contiene las informaciones esenciales a conocer, con anterioridad a la solicitud del certificado, en relación con el servicio de certificación de la Organización Médica Colegial.

1. Información de contacto

1.1. Organización responsable

La Entidad de Certificación de la "Organización Médica Colegial", en lo sucesivo "EC-OMC", es una iniciativa de:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA – ORGANIZACIÓN MÉDICA COLEGIAL

PLAZA DE LAS CORTES, 11- 28014 MADRID

TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

1.2. Persona de contacto

Para cualquier consulta, diríjanse a:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA – ORGANIZACIÓN MÉDICA COLEGIAL

PLAZA DE LAS CORTES, 11- 28014 MADRID

TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

2. Tipo y finalidad del certificado corporativo de personal administrativo en software

Los certificados corporativos de personal administrativo en software de firma electrónica avanzada, son certificados reconocidos de acuerdo con lo que se establece en los artículos 7

y 11.1, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de personal administrativo en software no funcionan necesariamente con dispositivos seguros de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados se emiten a personal administrativo del ámbito corporativo del colegio o persona jurídica suscriptor, y no son emitidos al público en ningún caso. Este órgano tiene la consideración de poseedor de claves, así como del software complementario correspondiente.

Los certificados corporativos de personal administrativo en software son certificados a emplear en aplicaciones de Administraciones Públicas y no son emitidos al público en ningún caso. La persona que recibe el certificado corporativo de personal administrativo en software tiene la consideración de poseedor y responsable de custodia de las claves, así como del software complementario correspondiente.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la "ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria"), que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

Por otra parte, los certificados corporativos de personal administrativo en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.

b) Firma de correo electrónico seguro.

c) Otras aplicaciones de firma digital.

Finalmente, los certificados corporativos de personal administrativo en software se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

a) La clave pública del poseedor de claves indicada en el certificado.

b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que la OMC no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

Los certificados corporativos de personal administrativo en software se identifican con el identificador de objeto (OID):

1.3.6.1.4.1.26852.1.1.6

2.1. Entidad de Certificación emisora

Los certificados corporativos de personal administrativo en software son emitidos por la Entidad de Certificación OMC (EC-OMC), identificada mediante los datos indicados anteriormente.

La EC-OMC subcontrata los servicios de producción de certificados aSymantec, que siempre actúa siguiendo las indicaciones de la EC-OMC.

3. Límites de uso del certificado

3.1. Límites de uso dirigidos a los suscriptores

El suscriptor ha de utilizar el servicio de certificación de certificados corporativos de personal administrativo en software prestado por la EC-OMC exclusivamente para los usos autorizados en el convenio firmado entre OMC y la persona jurídica, y que se reproducen posteriormente (sección “obligaciones de los suscriptores”).

Asimismo, el suscriptor se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por la EC-OMC.

El suscriptor ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El suscriptor no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de la EC-OMC, sin previo permiso expreso.

3.2. Límites de uso dirigidos a los verificadores

El verificador ha de utilizar el servicio de certificación de certificados corporativos de personal administrativo en software, y el correspondiente servicio de información, prestado por la EC-OMC, exclusivamente para los usos autorizados en el documento de condiciones generales de uso del certificado corporativo de personal administrativo en software, y que se reproducen posteriormente (sección “obligaciones de los verificadores”).

Asimismo, el verificador se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por la EC-OMC.

El verificador ha de cumplir cualquier ley y regulación que pueda afectar a su derecho a utilizar las herramientas criptográficas empleadas.

El verificador no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de la EC-OMC, sin previo permiso expreso.

4. Obligaciones de los suscriptores

4.1. Generación de claves

El suscriptor autoriza a la EC-OMC a generar su propia clave, privada y pública, para la identificación y la firma electrónica y solicita la emisión del certificado corporativo para el personal administrativo.

4.2. Solicitud de certificados

El suscriptor se obliga a realizar las solicitudes de certificados corporativos de personal administrativo en software de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por la EC-OMC, de conformidad con lo que se establece en la DPC y en la documentación de operaciones de la EC-OMC.

4.3. Veracidad de la información

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a la EC-OMC de cualquier inexactitud detectada en el certificado una vez se haya emitido, así como de los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.

4.4. Obligaciones de custodia

El suscriptor se obliga a custodiar el código de identificación personal o cualquier otro soporte técnico entregado por la EC-OMC, las claves privadas y, si fuese necesario, las especificaciones propiedad de la EC-OMC que le sean suministradas, así como toda la información que genere en su actividad como entidad de registro.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el suscriptor sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas circunstancias han de ser notificadas inmediatamente a la EC-OMC.

4.5. Obligaciones de uso correcto

El suscriptor tiene que utilizar el servicio de certificación de certificados corporativos de personal administrativo en software prestado por la EC-OMC, exclusivamente

para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El suscriptor tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El suscriptor no podrá adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

El suscriptor reconocerá:

a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, habrá aceptado dicho certificado y estará operativo.

b) Que no actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.

4.6. Transacciones prohibidas

El suscriptor se obliga a no utilizar sus claves privadas, los certificados o cualquier otro soporte técnico entregado por la EC-OMC en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital prestados por la EC-OMC no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

5. Obligaciones de los verificadores

5.1. Decisión informada

La EC-OMC informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de la EC-OMC, se rigen por la DPC de la EC-OMC y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

5.2. Requisitos de verificación de la firma electrónica

Para proceder a cifrar un mensaje o documento por una persona, se ha de utilizar la clave pública propia del destinatario. Dicha clave pública se puede obtener a partir de su certificado corporativo de órgano colegial.

Por lo tanto, es necesario verificar este certificado antes de proceder al cifrado.

La comprobación de la firma electrónica del certificado es imprescindible para determinar que la clave pública contenida en el certificado corresponde al suscriptor, y que la correspondiente clave privada permite descifrar el mensaje.

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.
- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.
- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de la EC-OMC (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.
- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el poseedor de la clave, ya que existe la posibilidad de qué alguno de los certificados incluyan límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.
- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el signatario.

5.3. Confianza en un certificado no verificado

Queda prohibido cifrar mensajes para un destinatario sin haber verificado con éxito su certificado.

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

5.4. Efecto de la verificación

En virtud de la correcta verificación de certificados corporativos de personal administrativo en software, de conformidad con estas condiciones de uso, el verificador puede confiar en la identificación y, en su caso, clave pública del poseedor de claves, dentro de las limitaciones de uso correspondientes, para generar mensajes cifrados.

5.5. Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por la EC-OMC, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de la EC-OMC, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación de la EC-OMC.

Los servicios de certificación digital prestados por la EC-OMC no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

6. Garantías limitadas y rechazo de garantías

6.1. Garantía de la EC-OMC por los servicios de certificación digital

La EC-OMC garantiza que:

a) La clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a menos que la EC-OMC no haya comunicado lo contrario mediante el Registro de certificación, de acuerdo con la DPC.

b) No ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por el suscriptor y validada por la EC-OMC, en el momento de la emisión del certificado.

c) Todos los certificados cumplen los requisitos formales y de contenido de la DPC, incluyendo todos los requisitos legales en vigor y aplicables.

d) Queda vinculada por los procedimientos operativos y de seguridad descritos en la DPC.

6.2. Exclusión de la garantía

La EC-OMC no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por la EC-OMC, excepto en los casos en que exista una declaración escrita en sentido contrario.

7. Acuerdos aplicables y DPC

7.1. Acuerdos aplicables

Los acuerdos aplicables al certificado corporativo de personal administrativo en software son los siguientes:

- Convenio de colaboración de servicios de certificación, que regula la relación entre la EC-OMC y el colegio o persona jurídica suscriptor de los certificados.
- Condiciones Generales de Uso, que regula la relación entre la EC-OMC y las personas físicas o jurídicas que emplean los certificados, también denominados "verificadores".

7.2. Declaración de prácticas de certificación

Los servicios de certificación de la EC-OMC se regulan técnicamente y operativamente por las Declaraciones de prácticas de certificación de la EC-OMC y de VeriSign Inc., por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: http://www.cgcom.es/registro.

7.3. Política de certificación

La EC-OMC dispone de una política de certificación que detalla los requisitos de carácter técnico, jurídico, operativo, así como de regulación del certificado corporativo de personal administrativo en software, a disposición de la comunidad de usuarios que la soliciten.

8. Reglas de confianza para firmas longevas

El punto b.2 del artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica hace referencia a la obligación de las entidades de certificación de informar a los solicitantes de los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

La EC-OMC informa a los solicitantes de los certificados corporativos de personal administrativo en software que no ofrece un servicio que garantice la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

La EC-OMC recomienda, para la fiabilidad de la firma electrónica de un documento a lo largo del tiempo, el uso de los estándares indicados en el apartado 7.3 (reglas de confianza para firmas longevas) de la Guía de Aplicación de la Norma Técnica de Interoperabilidad "Política de Firma Electrónica y de certificados de la Administración".

Las consideraciones generales para las reglas de confianza de firmas longevas se recogen en el subapartado IV.3 de la NTI de firma electrónica:

IV.3 Reglas de confianza para firmas longevas.

1. *En el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya trascurrido el periodo de precaución o periodo de gracia.*
2. *Para la conversión de una firma electrónica a firma electrónica longeva:*
   a) *Se verificará la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES y las referencias.*
   b) *Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:*
      I. *Certificados: incluyendo los certificados del firmante y de la cadena de certificación.*
      II. *Informaciones de estado de los certificados, CRLs o las respuestas OCSP.*
   c) *Aplicación del sellado a las referencias a los certificados y a las informaciones de estado.*
3. *Para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP.*

4. *Las políticas de firma contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable.*

8.1. Formato XAdES

Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora dos propiedades no firmadas:

I. *CompleteCertificateRefs: contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.*

II. *CompleteRevocationRefs: contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación los certificados.*

En el caso que se desee incorporar a la firma esta información de validación, se recomienda utilizar el formato XAdES-X, que añade un sello de tiempo a la información anterior.

El formato XAdES-XL, además de la información incluida en XAdES-X, incluye dos nuevas propiedades no firmadas: CertificateValues y RevocationValues que incluyen:

I. *Referencias a la información de validación.*

II. *Cadena de confianza completa.*

III. *CRL o respuesta OCSP obtenida en la validación.*

En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato XADES-A, que añade un sello de tiempo a la información anterior. En este caso se recomienda usar validación mediante OCSP, ya que mediante este método las propiedades CertificateValues y RevocationValues son de menor tamaño.

8.2. Formato CAdES

Dentro del formato de firma CAdES, el formato extendido CAdES-C incorpora dos atributos:

I. *Complete-certificate-references: contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma.*

II. *Complete-revocation-references: contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de la firma.*

El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos certificate-values y revocation-values que incluyen:

I. *Referencias a la información de validación.*
II. *Cadena de confianza completa.*
III. *CRL o respuesta OCSP obtenida en la validación.*

En el caso que se desee incorporar a la firma esta información de validación, la validación mediante OCSP favorece la obtención que las propiedades certificate-values y revocationvalues son de menor tamaño.

Por tanto, según el tipo de validación, se recomienda el uso de los siguientes formatos.

I. *En el caso que la validación se realice mediante consulta OCSP: los formatos CAdES-X Long type 1 o CAdES-X Long type 2, que añaden un sellado de tiempo a la información incluida en una firma CAdES-X Long. En este caso se incorporan los atributos certificatevalues y revocation-values puesto que la respuesta a una consulta OCSP no ocupa mucho espacio.*
II. *En el caso que la validación no pueda realizarse mediante OCSP y se realice mediante consulta a una CRL: los formatos CAdES-X type 1 o CAdES-X type 2, que incluyen un sellado de tiempo a la información incluida en una firma CAdES-C, es decir, a las referencias a las CRL consultada y los certificados de la cadena de confianza. No se recomienda incluir los atributos certificate-values y revocation-values ya que pueden ser muy voluminosos.*

En el caso que se esté próximo a la caducidad del sello de tiempo añadido para construir la firma longeva, se puede transformar la firma CAdES-X Long type 1 o CAdES-X Long type 2, en una firma CAdES-A, añadiendo un sellado de tiempo de archivo a la firma anterior.

8.3. Formato PAdES

En caso de forma PAdES, se recomendaría el uso del formato PAdES-Long Term.

Al igual que en los casos anteriores, se recomienda usar validación mediante OCSP, ya que el tamaño de la información de validación a añadir es menor.

Además se podría añadir un sello de tiempo que incluyese dicha información de validación, ya que la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

9. Política de intimidad

La EC-OMC no puede divulgar ni puede ser obligada a divulgar información confidencial alguna en lo referente a certificados sin una solicitud específica previa que provenga de:

a) la persona con respecto a la cual la EC-OMC tiene el deber de mantener la información confidencial, o

b) una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Sin embargo, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, será incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tendrá carácter confidencial, por imperativo legal.

La EC-OMC no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

La comunicación de dichos datos a los colaboradores de la EC-OMC en la prestación de los servicios de registro y de certificación (en especial,Symantec) se produce en el marco de un contrato de encargado de tratamiento, en los términos de la vigente LOPD, y por tanto no tiene la consideración de cesión.

10. Política de reintegro

La EC-OMC no reintegrará el coste del servicio de certificación en ningún caso.

11. Ley aplicable y jurisdicción competente

Las relaciones con la EC-OMC se regirán por las leyes españolas, y, en concreto para la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como por la legislación civil y mercantil aplicable.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

12. Acreditaciones y sellos de calidad

La EC-OMC dispone de documentación acreditativa del cumplimiento de las siguientes auditorías:

- WebTrust para Autoridades de Certificación, aplicable al Centro de procesamiento de datos de Symantec.
- Procedimientos de la especificación técnica voluntaria ETSI TS 101 456.