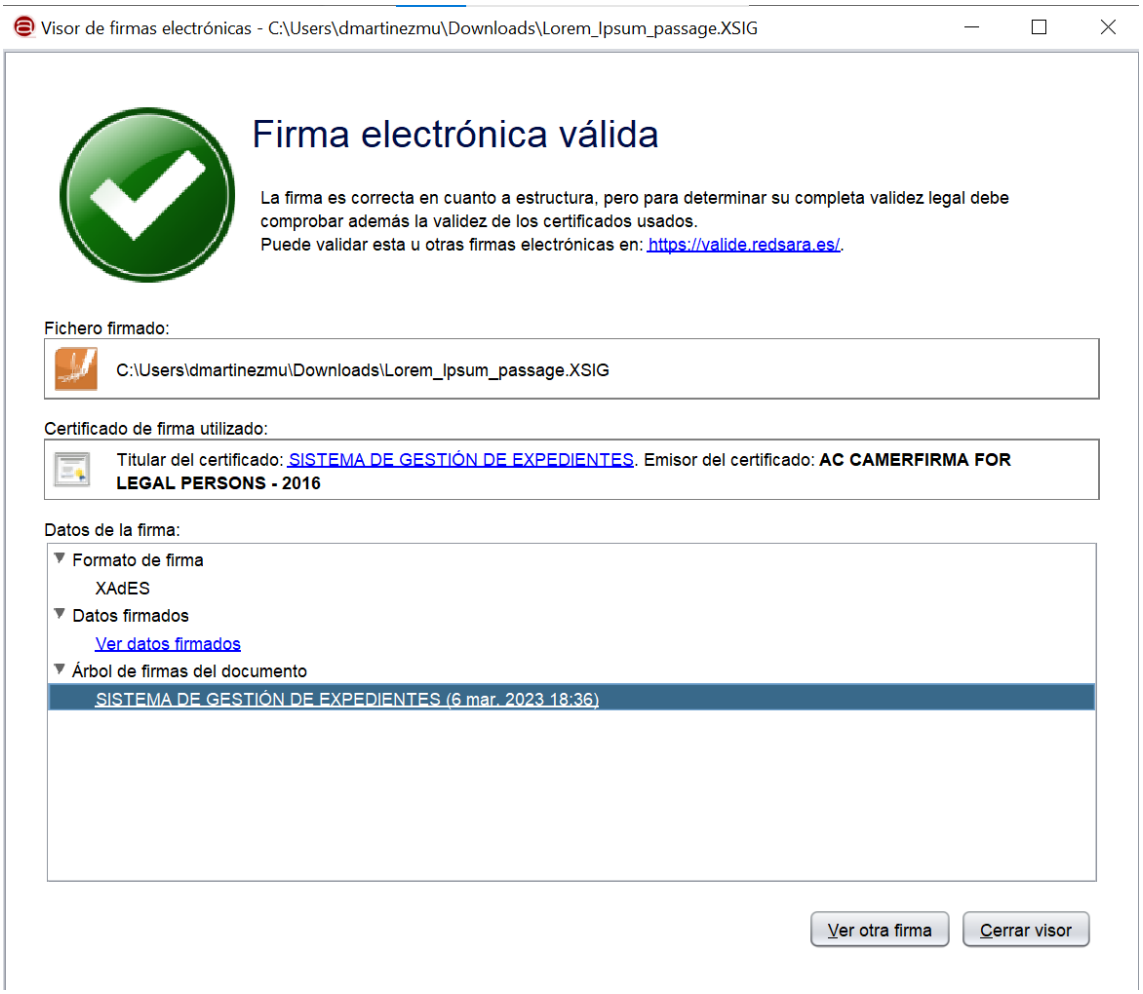
Verificación de la firma electrónica de los certificados emitidos por el CEM

Los certificados relativos a los servicios realizados por el CEM llevan incorporada una firma electrónica de acuerdo con la legislación vigente en materia de documento electrónico y documento administrativo electrónico.

- Reglamento UE y Ley de servicios de confianza
- Ley del Procedimiento Administrativo Común de las AAPP.
- Reglamento de actuación y funcionamiento del sector público por medios electrónicos

La validez y autenticidad del documento mediante de la firma electrónica puede comprobarse a través de visores (como por ejemplo Acrobat Reader) o cualquier herramienta a tal efecto como Autofirma (y Valide).



Verificación de las copias de los documentos con código seguro de verificación CSV

Las copias auténticas de los certificados emitidos por el CEM, cuentan con la opción de comprobación mediante su código seguro de verificación.

En el lateral izquierdo del certificado se indica el código para verificar el documento y la página para efectuarlo.

Validez de los certificados con errores de comprobación de la firma emitidos con anterioridad a 2023

El Centro Español de Metrología considera válidos aquéllos certificados emitidos cuya firma da errores de comprobación en Autofirma (y Valide), cuando las circunstancias son como las que se describen en este documento.

El error producido durante el proceso de comprobación de la firma en algunos de los certificados emitidos por el CEM no indica que la firma no sea válida, tan solo que no ha podido determinar su validez. Con algunos de los certificados usados por el personal del CEM, emitidos por la Fábrica Nacional de Moneda y Timbre, y realizando la firma con un portafirmas propio del CEM, se da la circunstancia de que se están generando firmas criptográficas con un tamaño menor (128 bytes) al recomendado (256 bytes), lo cual no se considera que invalida tal firma.

Este problema no se revela con Valide, pero con Autofirma se puede comprobar acudiendo a los registros del programa. En Windows 10, tales registros se encuentran en el directorio .afirma dentro del directorio personal del usuario. Ejemplo: C:\Users\minombre\.afirma. Dentro de esa carpeta debe haber un fichero AUTOFIRMA.afirma.log.xml. Si se abre debe haber un mensaje parecido a este:

<record>

<date>2020-12-22T11:39:30.876224600Z</date>

<millis>1608637170876</millis>

<nanos>224600</nanos>

<sequence>20</sequence>

<logger>es.gob.afirma</logger>

<level>WARNING</level>

<class>es.gob.afirma.signvalidation.ValidateXMLSignature</class>

<method>validate</method>

<thread>23</thread>

<message>**No se ha podido validar la firma: javax.xml.crypto.dsig.XMLSignatureException: java.security.SignatureException: Signature length not correct: got 128 but was expecting 256**</message>

</record>

Traducido quiere decir: “Longitud de la firma no es correcta, se obtuvieron 128 bytes pero se esperaban 256”.

Comprobación

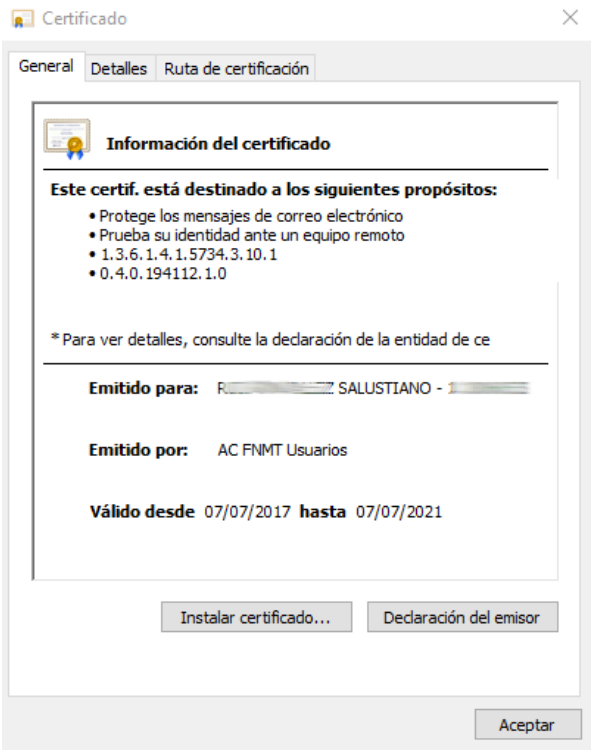
A partir del documento PDF que contiene el certificado junto con el archivo XSIG de la firma se puede:

- Obtener el documento PDF firmado a partir del XSIG, que se podrá comparar con el PDF enviado por el CEM, para ver que son idénticos.
- Extraer el certificado del firmante a partir del XSIG para comprobar su validez

Al intentar ver la firma con Autofirma (Archivo > Ver firma) nos encontramos con el siguiente error. Esto como decíamos está relacionado con que esa firma es de un tamaño menor al recomendado, por eso no se ha podido completar la validación.

Solo para propósitos ilustrativos, a continuación mostramos una captura de pantalla de un ejemplo de comprobación donde la firma efectivamente no es válida

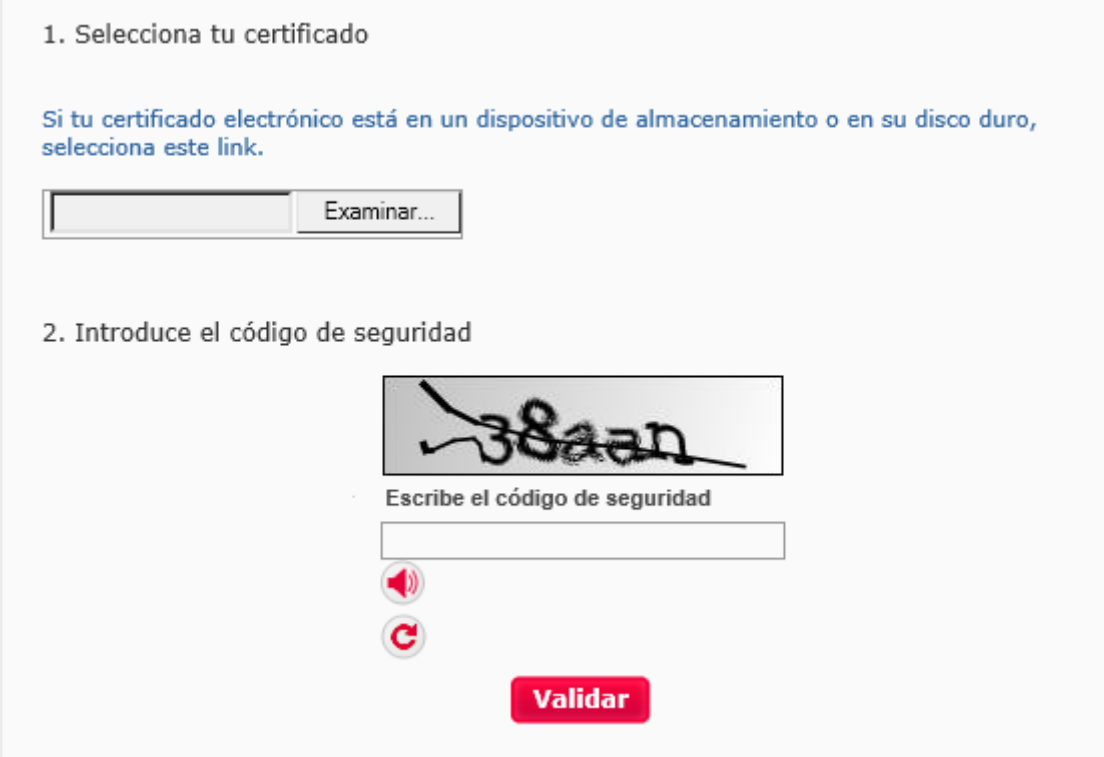
Lo primero que debemos comprobar es la validez del certificado del firmante. Pulsando en el enlace a continuación de “Titular del certificado”, Windows mostrará un cuadro con los datos leídos desde el certificado que viene junto con el XSIG. Ahí podemos ver que el certificado está en vigor:



Si vamos a la pestaña “Ruta de certificación” nos debe indicar “Certificado válido”.

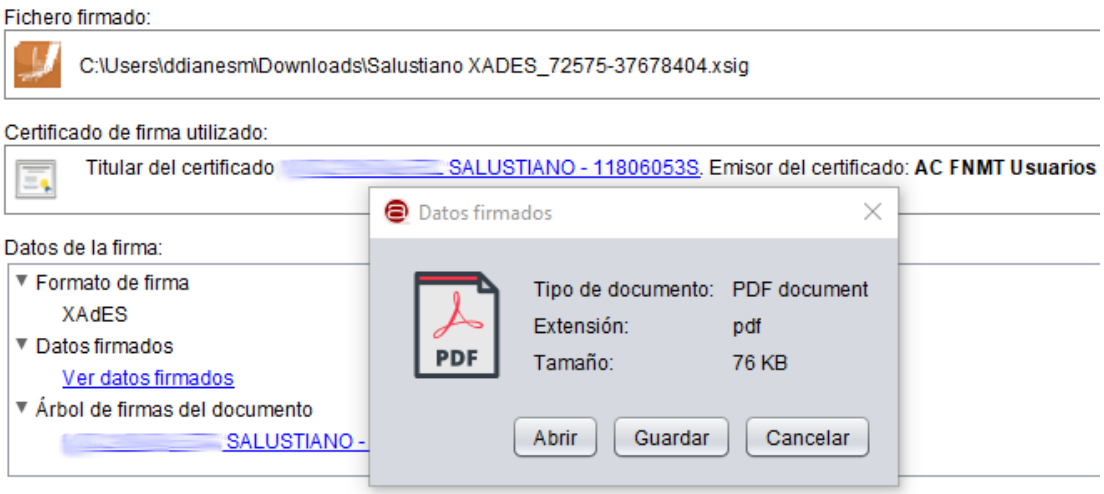
Para terminar de asegurarnos de la plena validez y vigor del certificado podemos acudir al verificador de certificados de Valide.

En primer lugar tenemos que exportar el certificado a partir del XSIG. Comenzando desde la ventana anterior vamos a la pestaña “Detalles” y desde ahí pulsamos “Copiar en archivo” y lo exportamos en formato “X.509 codificado base 64 (.CER)”. Ese archivo exportado es el que debemos subir al verificador de certificados de Valide (la pantalla siguiente es usando Internet Explorer):



A partir de esa verificación no queda ninguna duda de la validez del certificado con el que se ha firmado el documento:

El siguiente punto que se puede comprobar es que lo que se ha firmado es realmente igual a lo que se envía por parte del CEM. Para ello hay que usar el enlace “Ver datos firmados” de la pantalla de ver firma en Autofirma.

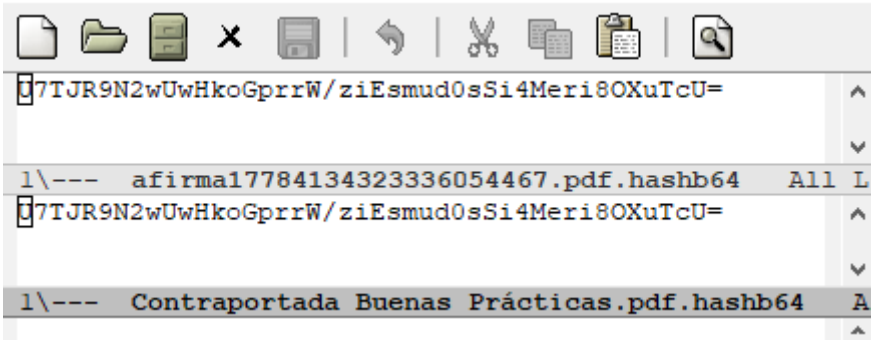


Este PDF debe ser exactamente igual al PDF enviado por correo electrónico por parte del CEM.

Para terminar de comprobar que el documento enviado por correo electrónico en PDF coincide exactamente con el documento PDF extraído desde el XSIG se puede utilizar la funcionalidad de cálculo de huellas digitales de Autofirma (Herramientas > Huellas digitales > Fichero > Calcular huella digital). La huella digital es una cadena que cumple las siguientes características:

- Es única para cada documento, es decir, no se da la circunstancia de que una misma huella tenga origen en dos documentos distintos
- No se puede generar el documento a partir de la huella (hash inverso)

En la siguiente captura se ve el resultado de calcular las huellas desde el documento PDF adjunto al correo y del documento PDF extraído desde el XSIG y se ve que son idénticas:



No obstante lo anterior, recuerde que puede solicitar una copia electrónica autentica del documento original a través de su contacto comercial con el CEM.

Finalmente, si tiene cualquier duda o necesita cualquier aclaración sobre la validez de los documentos electrónicos emitidos por el Centro Español de Metrología, puede contactar con nosotros a través de nuestra página web **https://www.cem.es** o a través del correo electrónico **cem@cem.es**

IMPORTANTE: Por motivos de confidencialidad y protección de datos, si no se es titular del documento solicitado, ni se es Administración pública competente, ni miembro de la Comisión de Metrología Legal del Consejo Superior de Metrología, tal como contempla el apartado 7 del Artículo 36 de la Sección Octava del Capítulo III del RD244/2016 , de 3 de junio, por el que se desarrolla la Ley 32/2014, de 22 de diciembre, de Metrología, no se podrá facilitar más información que la correspondencia entre CSV y número de certificado. Únicamente podríamos facilitarle más información por requerimiento judicial.