Universitat d'Alacant
Universidad de Alicante

BIBLIOTECA UNIVERSITARIA

Certificados digitales

Material formativo

BUA
Biblioteca de la Universitat d' Alacant
Biblioteca de la Universidad de Alicante

CI2
COMPETENCIAS
INFORMÁTICAS E
INFORMACIONALES

INDICE

Para empezar: el certificado digital	2
Clave digital	2
Obtención del certificado	3
Principales Autoridades de Certificación (AC)	4
Renovación del Certificado	5
Revocación de un Certificado	7
Trabajar con certificados digitales en el navegador y ordenador	9
¿Qué puedo hacer en la UA con los certificados digitales?	16
Para finalizar	17
Para saber más	17

CERTIFICADOS DIGITALES

Para empezar: El certificado digital

Es un documento electrónico expedido por una Autoridad de Certificación e identifica a una persona (física o jurídica) con un par de claves.

Tiene como ***misión*** validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.

Contiene la información necesaria para firmar electrónicamente e identificar a su propietario o propietaria con sus datos: nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide.

La Autoridad de Certificación da fe de que la firma electrónica se corresponde con una persona concreta. Esa es la razón por la que los certificados están firmados, a su vez, por la Autoridad de Certificación.

Clave digital

En un Certificado, las claves digitales son los elementos esenciales para la firma e identificación de la persona firmante. Existen dos claves, la clave privada y clave

pública, y trabajan de forma complementaria. Lo que cifra o codifica una clave sólo lo puede descifrar o decodificar la otra.

La diferencia entre ellas es que la clave privada está pensada para que nunca salga del certificado y esté siempre bajo el control de la persona firmante. En cambio, la clave pública se puede repartir o enviar a otras personas.

En ocasiones, se habla de Certificado Privado para referirse al certificado que contiene la clave privada y la pública y del Certificado Público para referirse al certificado que sólo contiene la clave pública.

Importante: Si envías tu certificado a un tercero, asegúrate de que es el certificado público (que contiene sólo la clave pública).

Obtención del certificado

Obtener el Certificado Digital depende de si el certificado está contenido **en una tarjeta**, como el DNIe, o de si el certificado se guarda en **un fichero software**.

En ambos procesos hay un paso que es la identificación de la persona responsable o persona usuaria del certificado, lo cual requiere que ésta se persone en las oficinas de una Autoridad de Registro. Estas oficinas corroboran la identidad.

En el caso de los certificados software, el propio navegador del usuario/a crea las claves. Pero, en el Certificado de tarjeta, quien crea e introduce las claves es el Proveedor de Certificación.

Obtención de Certificado en tarjeta (DNIe)

Los certificados contenidos en tarjetas deben ser entregados directamente a la persona.

En el caso concreto del DNIe, hay que personarse en las oficinas de la Dirección General de Policía, que es la Autoridad Certificadora.

Solicitud de certificado software

La solicitud y descarga del Certificado se realizan desde el navegador.

En los siguientes enlaces podrás encontrar el proceso a seguir para algunos de los Proveedores de Certificación existentes:

FNMT-Ceres, creada por la Fábrica Nacional de Moneda y Timbre.

CATCert, Agència Catalana de Certificación

ACCV, Autoritat de Certificació de la Comunitat Valenciana

IZENPE: la autoridad de certificación impulsada por el Gobierno Vasco y las Diputaciones Forales

Principales Autoridades de Certificación (AC)

Una Autoridad de certificación es una entidad de confianza, responsable de emitir y revocar los certificados digitales o electrónicos, utilizados en la firma electrónica. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

A continuación te mostramos las principales Autoridades de Certificación españolas que emiten certificados electrónicos de Persona Física.

- Fábrica Nacional de Moneda y Timbre (FNMT)
- Agència Catalana de Certificació (CATCert)
- Agencia Notarial de Certificación (ANCERT)
- ANF Autoridad de Certificación (ANF AC)
- Autoridad de Certificación de la Abogacía (ACA)
- Autoridad de Certificación HealthSign
- Autoritat de Certificació de la Comunitat Valenciana (ACCV)
- Banco de España
- Banco Español de Crédito S.A. (Banesto)
- Banco de Santander
- Camerfirma
- EDICOM
- Firma Profesional
- Gerencia de Informática de la Seguridad Social (GISS)
- IZENPE
- Ministerio de Defensa
- Ministerio de Trabajo e Inmigración

Nota Importante: Debes utilizar el **mismo navegador** durante todo el proceso, desde la solicitud hasta la descarga final del certificado.

Renovación del Certificado

Los Certificados electrónicos tienen un ***periodo de validez pasado***, el cual no sirven para firmar, ni tampoco para identificarse.

Cada Proveedor de Certificación establece unos plazos antes de que el certificado caduque para poder renovarlo sin necesidad de otra identificación.

En el caso de los certificados de la FNMT, tienen una validez de 36 meses y se puede renovar durante los 2 meses anteriores a su caducidad.

Nota importante:
Todo el **proceso de renovación de un certificado**, desde la solicitud de renovación hasta la descarga final, se ha de realizar desde el mismo **navegador** en el que está instalado.

Los Certificados incluidos en la tarjeta de **DNIe** tienen una validez de **30 meses** (aunque la tarjeta del DNIe puede tener una validez de hasta 10 años dependiendo de la edad de la persona). Aquí encontrarás más información sobre cómo renovar los Certificados de tu DNIe.

Si el Certificado caduca hay que volver a realizar todo el proceso de solicitud del certificado. Sin embargo, un certificado se puede renovar antes de que caduque y el proceso no requiere una solicitud nueva.

Puedes ver si tu certificado está caducado utilizando el servicio VALIDe del Ministerio de Hacienda y Administraciones Públicas.
También puedes comprobarlo directamente en tu navegador, en el menú de opciones o herramientas.

Revocación de un Certificado

Puedes **invalidar tu Certificado** antes de que caduque por razones de seguridad**.**

Estas son las **principales causas** de revocación de un Certificado:

- Solicitud voluntaria de la persona suscriptora.
- Pérdida o daños en el soporte del Certificado.
- Fallecimiento de la persona suscriptora o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
- Finalización de la representación o extinción de la entidad representada.
- Inexactitudes en los datos aportados por la persona suscriptora para la obtención del certificado.
- Que se detecte que las claves de la persona suscriptora o de la Autoridad de Certificación han sido comprometidas.
- Una vez revocado, el certificado ya no puede ser reactivado y es necesario volver a iniciar todo el proceso de solicitud.

Para revocar los Certificados, deberá ser la propia Autoridad de Certificación la que proporcione el procedimiento, que normalmente está publicado en su página web.

Por ejemplo, la revocación de un certificado emitido por la Fábrica Nacional de Moneda y Timbre (FNMT) puede realizarse de tres formas:

- A través de **Internet**: si la persona titular del certificado o su representante, en caso de entidades, están en posesión del mismo.
- En la **Oficina de Acreditación**: si la persona titular del certificado o representante no disponen del mismo por extravío, pérdida o robo, deberá personarse en una de estas Oficinas de Acreditación para, una vez identificado, firmar el modelo de solicitud de revocación del certificado. Las Oficinas de Acreditación transmiten diariamente los registros tramitados a la FNMT para que ésta proceda a la revocación del certificado.

- **Por teléfono: 902 200 616**. Esta opción únicamente deberá utilizarse en aquellos casos en que no pudieras desplazarte a una Oficina de Acreditación o no fuera posible revocar el certificado de manera online.

En el caso del **DNIe**, debes presentarte en cualquier **Oficina de Expedición** del DNIe para revocar el Certificado. La revocación es **inmediata** a la tramitación de cada solicitud verificada como válida.

Trabajar con certificados digitales en el navegador y ordenador

El Almacén de Certificados

Siempre que vayamos a realizar un proceso de firma electrónica o identificación digital basadas en certificados, será necesario que esos certificados estén disponibles en el ordenador para la aplicación que va a realizar la firma.

Los certificados se guardan en el "***Almacén de Certificados".***

- Para los certificados contenidos en una **tarjeta digital**, como el **DNI electrónico**, la propia tarjeta es el almacén.
- Los **certificados software** se guardan en un almacén que puede estar ubicado en el sistema operativo o en el propio ordenador. Para poder usarlo primero es necesario importar o cargar el certificado en ese almacén.

Instalar el Lector de DNI electrónico

Para poder usar el DNI electrónico desde un ordenador es necesario disponer de un lector de tarjetas compatible con el DNIe. El lector debe cumplir, al menos:

- el estándar ISO 7816 (1, 2 y 3)
- soportar tarjetas asíncronas basadas en protocolos T=0 (y T=1)
- soportar velocidades de comunicación mínimas de 9.600 bps
- soportar los estándares:
    - API PC/SC (Personal Computer/Smart Card)
    - CSP (Cryptographic Service Provider, Microsoft)
    - API PKCS#11

Además, para poder interaccionar adecuadamente con las tarjetas criptográficas (DNIe) en particular, el equipo ha de tener instalados unas 'piezas' de software denominadas **módulos criptográficos.**

- En un entorno Microsoft Windows, el equipo debe tener instalado un servicio que se denomina "CryptographicServiceProvider" (CSP).
- En los entornos UNIX / Linux o MAC, podemos utilizar el DNI electrónico a través de un módulo criptográfico denominado PKCS#11.

Importar y exportar certificados

Importar certificados

La importación de certificados es el proceso que permite cargar el certificado en el ordenador o en el navegador para su uso posterior en la firma o identificación.

Los certificados pueden contener la **clave privada y la pública, o sólo la pública**. Eso depende del tipo de certificado que tengamos y de su extensión.

Al **importar** un certificado es importante que contenga la **clave privada**, ya que sin ella no vamos a poder firmar. Por tanto, asegúrate de que el fichero del certificado que importas tenga alguna de estas extensiones .pfx .p12 ó .pem.

Exportar certificados

La exportación de certificados es el proceso que permite obtener una copia del certificado instalado en el ordenador o en el navegador para su uso posterior en otro ordenador o proceso.

En ocasiones es necesario **extraer del almacén un certificado** para lo siguiente:

- Hacer un backup o copia de seguridad del certificado.
- Instalarlo en otro ordenador.
- Enviar la parte pública a otra persona.

En el proceso de exportación se nos solicitará o se podrá marcar una casilla que indique que queremos exportar la clave privada.

- **Marca la casilla si quieres que el certificado exportado se pueda utilizar para firmar**. En este caso, el archivo generado se guardará con una extensión .p12, .pfxo .pem. Recuerda que este certificado no se puede distribuir y que hay que **mantenerlo en un lugar seguro**.
- **No marques la casilla si quieres que el certificado sea público y enviar el certificado a otra persona**. En este caso, el archivo generado se guardará con una extensión .cer o .der

La exportación se debe hacer desde el almacén en el que está instalado el certificado.

En los puntos siguientes puedes ver las diferentes formas de acceder a los almacenes disponibles en el ordenador.

Instalar certificados en Windows

El almacén de certificados de Windows es utilizado por navegadores como Internet Explorer y Chrome y por otras aplicaciones como Office y Adobe Reader.

La importación de certificados en este almacén se puede realizar desde cualquiera de los dos navegadores mencionados. La forma de acceder al almacén y a las herramientas de importación es la siguiente:

En Internet Explorer:

- Opciones de Internet > Contenido > Certificados.

En Google Chrome:

- Opciones > Avanzada > HTTP/SSL > Gestionar Certificados.

En Firefox

Firefox dispone de su propio almacén de certificados independiente del almacén del sistema operativo. Por tanto, si quieres firmar documentos desde Firefox debes realizar previamente la importación de certificados desde el mismo navegador.

La forma de acceder a la gestión del almacén de Firefox es la siguiente:

- Opciones > Avanzado > Cifrado > Ver Certificados.

Validación de PDFs en Adobe

Las aplicaciones Adobe y Adobe Reader permiten la validación de las firmas contenidas en documentos pdf firmados electrónicamente. Sin embargo, para que esto sea posible, es necesario que Adobe reconozca y confíe en los certificados raíces de las Entidades Certificadoras que han emitido los certificados con que se ha firmado el documento.

Por ejemplo, para validar correctamente un documento pdf emitido por el BOE es necesario configurar el entorno Adobe para que reconozca el certificado raíz de la FNMT, ya que ha sido esta entidad la que ha emitido el certificado con el que se ha firmado el documento del BOE.

En general, Adobe se puede configurar utilizando alguno de los siguientes métodos:

Usar el almacén de certificados de Windows

1. Descargar el certificado raíz de la Autoridad de Certificación que ha emitido el certificado.

2. Instalación del certificado en el almacén de Windows. Haz doble click sobre el fichero descargado y se mostrará una ventana.

En la pestaña "**Detalles**" puedes comprobar los atributos indicados para confirmar que se trata del certificado correcto.

Pulsa el botón "**Instalar Certificado**"

Pulsa el botón "**Siguiente** >"

Pulsa el botón "**Examinar**" y selecciona "**Entidades emisoras de confianza**"

Pulsa el botón "**Siguiente** >" y en la última pantalla "**Finalizar**"

Dado que se trata del certificado de una Autoridad de Certificación raíz aparecerá una ventana para solicitar confirmación

Pulsa el botón "**Si**"

3. Configurar Adobe Acrobat Reader para confiar en el almacén de Windows.

Iniciar Adobe Reader e ir al menú "**Edición > Preferencias**".

Selecciona la sección "**Seguridad**" y pulsar el botón "**Preferencias Avanzadas**".

Selecciona la pestaña "**Integración de Windows**" y chequea la opción "**Validando Firmas**".

Pulsa el botón "**Aceptar**" para finalizar

Usar el almacén de certificados de Acrobat Reader

Acrobat Reader dispone de su propio almacén de certificados de confianza, que por defecto, es el que utiliza.

El procedimiento de instalación y configuración es el siguiente:

1. Descargar el certificado raíz de la Autoridad de Certificación que ha emitido el certificado.
2. Importar el certificado de la autoridad certificación descargado.

Inicia Adobe Acrobat Reader y selecciona el menú "**Avanzadas > Administrar identidades de Confianza**".

En las versiones más modernas, este menú se encuentra en "**Documentos > Administrar identidades de Confianza**".

Pulsa el botón "**Agregar Contacto**"

Pulsa el botón "**Examinar**" y selecciona el certificado descargado anteriormente

En la ventana que se abre selecciona el Contacto recién importado.

A continuación se muestran los certificados contenidos en dicho fichero

Selecciona el certificado de la Autoridad de Certificación y pulsa el botón "**Confiar**"

Chequea la opción "**Firmas y como una raíz de confianza**" y pulsa el botón "**Aceptar**"

Pulsa el botón "**Importar**"

Pulsa el botón "**Aceptar**"

¿Qué puedo hacer en la UA con los certificados digitales?

La oficina central del Registro General de la Universidad de Alicante es punto de registro de usuario (PRU) de firma digital de la Agencia de Tecnología y Certificación Electrónica de la Comunidad Valenciana, de acuerdo con el convenio firmado con la Generalitat Valenciana.

La firma digital expedida en la oficina central del Registro General se puede utilizar para:

- Recepción y envío de documentos a las Administraciones Central, Autonómica y Local (certificados de vida laboral, declaración de la Renta, o trámites con SUMA, entre otros).
- Firmar y cifrar los mensajes de correos electrónicos evitando el SPAM.
- Firmar facturas electrónicas.

Para solicitar un certificado digital es necesario personarse en la oficina central del Registro General con el DNI, NIE, carnet de conducir en formato tarjeta o pasaporte español en vigor.

Con el fin de agilizar los trámites, sugerimos que utilices este servicio entre las 9:00 y las 10:00 horas de la mañana.

Para finalizar

En esta unidad del curso de CI2 de nivel intermedio dedicado a los certificados digitales hemos aprendido:

- Definir que es un certificado digital
- Elementos que componen el certificado digital: La clave digital
- Cómo se obtiene un certificado digital
- Principales entidades emisoras de certificados
- Cómo se renueva y cómo se revoca un certificado
- Cómo trabajar con certificados digitales en el ordenador y en los navegadores.
- Qué se puede hacer en la UA con los certificados digitales

PARA SABER MÁS

Enlaces:
https://www.sede.fnmt.gob.es/certificados/persona-fisica
https://www.sede.fnmt.gob.es/certificados
http://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html
https://sede.dgt.gob.es/es/contenidos/donde-obtener-certificado.shtml
https://es.wikipedia.org/wiki/Certificado_digital
https://www.accv.es/ayuda/instalar-el-certificado-digital-en-fichero/
Tutoriales
https://www.youtube.com/watch?v=p19J0TOpIks
https://www.youtube.com/watch?v=98NXoYUoffo

https://www.youtube.com/watch?v=nuCsdjngj8s
https://www.youtube.com/watch?v=8ab88NLomY8
https://www.youtube.com/watch?v=p19J0TOpIks&t=7s
https://www.youtube.com/watch?v=fLKPsy2_2Og
https://www.youtube.com/watch?v=RdONJ_0CXAU