

Certificad0s Digital3s F.N.M.T.

Universidad de Oviedo
Seguridad de Sistemas Informáticos
Mayo, 2017

Autores

Guillermo Facundo Colunga, Samuel Fernández Cabello,
Katia Fernández Fernández, Daniel González García y
Rubén Gutiérrez Guerrero

Revisiones Documento

Fecha	Versión	Descripción	Autor
05/04/17	1	Listas de Anulación de Certificados	Katia Fernández Fernández
05/04/17	1	Autoridades Certificadoras	Katia Fernández Fernández
05/04/17	1	FNMT Qué es y Cómo actúa	Daniel González Gracia
05/04/17	1	Certificados que expide la FNMT	Daniel González Gracia
18/04/17	1	Infraestructura Clave Pública	Rubén Gutiérrez Guerrero
18/04/17	1	Introducción a los Certificados Digitales	Samuel Fernández Cabello
19/04/17	1	Obtener Certificado Digital de la FNMT	Guillermo Facundo Colunga
19/04/17	1	Casos de uso de certificados digitales	Guillermo Facundo Colunga
28/04/17	1.2	Revisión Completa Documento	TODOS

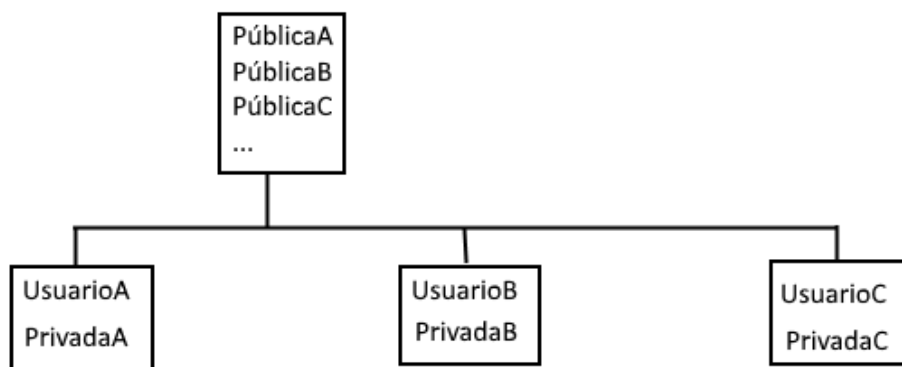
Tabla de Contenidos

Introducción a los certificados digitales	3
Clave pública y privada	3
Casos prácticos de los algoritmos de clave asimétrica	3
Certificados, firmas y otros usos	4
Anulación de Certificados	6
Autoridades Certificadoras	7
¿Qué es y cómo actúa la FNMT?	8
Certificados que expide la FNMT	9
Persona física	9
Certificado de representante	9
Administración pública	9
Certificado de componente	9
Obtener un Certificado Digital de la FNMT	10
Consideraciones Previas	10
Solicitar Certificado	11
Acreditar Identidad	12
Descargar Certificado	13
Caso de uso en la Administración Pública	14
Acceder a la Sede Electrónica	14
Inicio de Sesión en la Sede Electrónica	15
Realización Proceso en la Sede Electrónica	16
Caso de uso en la Universidad de Oviedo	17
Acceder a la intranet de la Universidad de Oviedo	17
Acceder al curso de Seguridad en Sistemas Informáticos	18
Bibliografía	20

Introducción a los certificados digitales

Clave pública y privada

La criptografía de clave pública y privada consiste en un directorio (O conjunto de ellos) en los que tenemos disponible las claves públicas de distintos usuarios, o empresas, y que usaremos para poder descifrar los mensajes de estos usuarios. La utilidad de esta manera de encriptar es que la clave privada para descifrar sólo funciona para la clave pública que le corresponda:



Supongamos que el usuario A desea enviarle un mensaje a C. El proceso sería el siguiente:

1. Obtenemos el mensaje C que es el resultado de cifrar el mensaje original M con la clave PúblicaC

UsuarioA: $C = \text{Cifrar}(M, \text{PúblicaC})$

2. Ahora UsuarioA no podrá descifrar el mensaje pero podrá enviarlo con la seguridad de que sólo UsuarioC podrá hacerlo.
3. UsuarioA envía el mensaje y UsuarioC lo recibe
4. Ahora UsuarioC obtiene el mensaje M a partir de su clave PrivadaC

UsuarioC: $M = \text{Descifrar}(C, \text{PrivadaC})$

Este es el funcionamiento básico y conceptual de la clave pública y privada. Esto significa que no siempre habrá un directorio de claves o se usarán únicamente con la finalidad de encriptar el mensaje ya, por ejemplo, este modo de encriptación es muy pesado y lento de realizar. A continuación entramos en detalle de su creación u usos.

Casos prácticos de los algoritmos de clave asimétrica

Podemos encontrar diferentes algoritmos de criptografía asimétrica, tales como el RSA, DSA, protocolo criptográfico Diffie-Hellman, criptografía de curva elíptica... El funcionamiento es diverso pero en todos conseguimos el objetivo del "Funcionamiento básico" de los algoritmos de clave asimétrica.

Por ejemplo veamos el funcionamiento del RSA, usado comúnmente para la transmisión de mensajes:

Primero debemos crear la clave multiplicando dos números primos p y q : " $n=p*q$ ", así obtenemos n que será usado como módulo.

A continuación se calcula $\text{funcionEuler}(n)=(p-1)(q-1)$, escogemos un número positivo e que sea menor que $\text{funcionEuler}(n)$ y coprimo con $\text{funcionEuler}(n)$

Esta e será el exponente clave pública.

Buscamos una d que satisfaga: $e*d = 1 + \text{mod}(\text{funcionEuler}(n))$.

Esta d será el exponente de la clave privada.

El cifrado consiste en (n, e) y el descifrado en (n, d) siendo el cálculo del cifrado " $c = m^e \text{mod}(n)$ " y el cálculo del descifrado

La m se corresponde con el mensaje y c con el mensaje cifrado.

Esto permite cifrar números, por tanto mensajes transformados.

Certificados, firmas y otros usos

Certificados

Un certificado es un fichero que asegura que el contenido de un fichero es verídico. Se debe tener en cuenta que no deja de ser un asunto de "confianza" debes confiar en la unidad certificadora para poder asegurar esta veracidad.

Generalmente la generación de un certificado sigue los siguientes pasos:

1. El solicitante genera una clave pública y privada.
2. Enviar aquello que se quiere certificar cifrado con la clave privada, también enviar la clave pública. Esto se envía a la unidad certificadora.
3. La entidad comprueba la identidad del solicitante.
4. La entidad genera el certificado con la clave pública proporcionada, fecha de vencimiento y lo firma con su clave privada.
5. La entidad envía el certificado al solicitante que podrá verificarlo con la clave pública de la entidad. Además el certificado se almacena en el ordenador del solicitante.

Firmas

En el ejemplo del apartado anterior, en el que hablamos de las claves públicas y privadas, también podemos usar estas para firmar documentos, es decir, asegurar que nosotros (o una entidad) hemos enviado ese documento ¿Cómo? Podemos encriptar el documento (o su resumen, obtenido mediante un hash) con nuestra clave privada y enviarlo. Y el receptor deberá desencriptar con nuestra clave pública. Como nosotros somos los únicos con nuestra clave privada estamos asegurando que el mensaje enviado ha sido enviado por nosotros.

La criptografía de clave asimétrica, como ya hemos comentado, es más costosa de realizar que la de clave simétrica y, en algunos casos, la información a encriptar "no es tan importante". Es decir, si el dato es variable en el tiempo (Si es algo que cambia cada tres meses) no importa que lo desencripten mediante un ataque de fuerza bruta que ha durado dos años. Así que hay casos en los que no merece la pena el coste de encriptar asimétricamente.

Lo que se hace en esos casos es encriptar asimétricamente una clave de criptografía simétrica para asegurar que llegará en secreto a su destino y usar, a partir de aquí, criptografía simétrica.

Anulación de Certificados

Las listas de anulación de certificados (CRL) son un mecanismo mediante el cual la autoridad certificadora publica información relacionada con los certificados anulados.

Los certificados tienen un período de validez limitado, que se incluye en el certificado. El período de validez varía. Por ejemplo, si un certificado de Persona Física fue emitido por AC FNTM Usuarios su validez es de 4 años; si fue emitido por FNMT Clase 2, su período de validez es de 3 años. Durante el período de validez del certificado, la entidad certificadora que lo generó conserva información sobre el certificado. Entre la información que guarda, se incluye el estado de anulación, que indica que la validez del certificado terminó y no es confiable.

Además se puede anular un certificado por distintas circunstancias. Una firma digital realizada con un certificado revocado no tiene validez. Por ello, es importante comprobar el estado del certificado o validarlo en la lista de revocados.

Se entiende por revocar un certificado hacer un cambio en su estado que da lugar a la pérdida de validez por un motivo diferente a la caducidad del mismo. Los motivos por los que se puede revocar un certificado están definidos en la "Declaración de Prácticas de Certificación", siendo algunos de los más comunes los siguientes:

- Defunción del suscriptor.
- Petición voluntaria.
- Cambios en los datos del suscriptor.
- Pérdida o daños en el soporte del certificado digital.

Solicitar la anulación de un certificado permite invalidar el certificado antes de la fecha de caducidad establecida y se puede realizar en cualquier momento, siempre que se encuentre dentro del período de validez del mismo. Además sólo podrá ser solicitada por una persona con suficientes facultades de representación según lo establecido en las "Políticas y Prácticas de Certificación Particulares." La encargada de emitir y formar las listas de certificados es la FNMT-RCM.

El procedimiento para anular un certificado expedido por la FNTM-RCM depende de si el representante posee el certificado o no. En el caso de que posea el certificado, se realizará a través de Internet, siendo soportados únicamente los navegadores Internet Explorer y Mozilla Firefox. Si no posee el certificado, debe acudir a una Oficina de Acreditación para proceder a su identificación y posterior firma de la solicitud de revocación del certificado.

Autoridades Certificadoras

Una autoridad de certificación es una entidad de confianza, que verifica la identidad del solicitante a través del certificado, que garantiza la autenticidad y veracidad de los datos firmados con el certificado expedido. También ofrece el servicio de verificar la validez de los certificados, ya que pueden estar caducados o ser revocados. Las principales Autoridades de Certificación de España son:

- **Fábrica Nacional de Moneda y Timbre (FNMT):** nace con la fusión de la Casa de la Moneda y la Fábrica del Sello en 1893. Su sede central es en Madrid y tiene actividad también en Burgos.
- **Agencia Notarial de Certificación (ANCERT):** encargado de la prestación de servicios de certificación para asegurar todas las relaciones entre personas físicas y jurídicas.
- **Autoridad de Certificación de la Abogacía (ACA)**
- **Camerfirma:** encargado de la seguridad en las cámaras de comercio españolas.
- **Firma Profesional.**

Existen algunas autoridades certificadoras provinciales como **IZENPE** (Euskadi), **Autoritat de Certificació de la Comunitat Valenciana** o **Agència Catalana de Certificació**.

¿Qué es y cómo actúa la FNMT?

La FNMT (Fábrica Nacional de Moneda y Timbre) nació de la fusión de la Casa de la Moneda y la Fábrica del Sello, administraciones que compartían edificio a pesar de ser independientes, en 1893. La empresa ha estado en una continua expansión desde entonces.

La FNMT es una entidad pública empresarial adscrita al Ministerio de Hacienda y Función Pública. El carácter de la empresa se podría clasificar como de servicio público. Colabora con entidades privadas en los ámbitos correspondientes a la seguridad y al control de la producción.

Las actividades propias de la empresa están basadas en la fabricación de:

- Monedas (circulantes y de colección)
- Billetes de banco
- Papel de seguridad
- Documentos de identificación
- Productos Gráficos (relacionados con los juegos de azar, sellos de correos, etiquetas de seguridad...)
- Tarjetas
- Medallas

Y la seguridad integral:

- Seguridad aplicada en los procesos de producción
- Seguridad en los productos
- Seguridad en el tratamiento de la información
- Seguridad en las instalaciones.

La administración de la FMNT puso en marcha la iniciativa CERES(CERTificación ESpañola) que consiste en establecer una Entidad Pública de Certificación, permitiendo la autenticación y garantía de la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y Administraciones Públicas a través de las redes abiertas a la comunicación.

Certificados que expide la FNMT

Persona física

El certificado digital FNMT de Persona Física, también llamado certificado de ciudadano o de usuario, es la certificación electrónica que, contiene sus datos identificativos y mediante firma confirman la identidad de su suscriptor. Permite a su suscriptor identificarse en Internet e intercambiar información con personas u organismos con la garantía y seguridad que de que sólo las personas u organismos que intercambian la información pueden acceder a ella.

Utilidad: Permite realizar trámites de manera segura con la Administración Pública o con entidades privadas por Internet, ahorrando posibles desplazamientos y esperas innecesarias.

Certificado de representante

Hay 3 tipos de certificados de representantes:

- **Para administrador único o solidario:** Cuando hay un solo administrador o, existiendo más de un administrador las decisiones pueden tomarlas un solo administrador sin falta del consentimiento o firma del resto de administradores. Se expide a los administrador únicos o solidarios.
- **Para persona jurídica:** Se expide a las personas físicas.
- **Para Entidad sin Personalidad Jurídica:** Se expide a las personas físicas como representantes de las entidades.

Utilidad: Se usa en las relaciones con administraciones públicas, entidades y organismos públicos, permitiendo una mayor agilidad y abaratando gestiones con la administración pública así como aumentando la productividad y competitividad y sobre todo, cumpliendo así con sus obligaciones legales.

Administración pública

Utilidad: Regula los sistemas de identificación de las administraciones públicas, los sistemas del personal al servicio de las administraciones públicas y el sello electrónico para la actuación administrativa automatizada.

Certificado de componente

Hay 4 tipos diferentes de certificados de componente:

- De servidor SSL/TLS, wildcard y SAN multidominio.
- De sello de entidad.
- Para firma de código
- De sede y sello para la administración pública

Utilidad: Sirva para dar la confianza que acredita la FNMT como autoridad de certificación.

Obtener un Certificado Digital de la FNMT¹

Para realizar cualquier trámite online con alguna Administración Pública Española será necesario poseer un certificado digital expedido por una CA autorizada. Por norma general, se estableció que, todas las administraciones públicas confíen en los certificados digitales expedidos por la Fábrica Nacional de Moneda y Timbre.

Para este ejemplo haremos las veces de persona física que quiere obtener su certificado digital en soporte software a través de la página web de la FNMT para interactuar con la Administración Pública.

Los datos del dominio de este ejemplo serán:

Equipo: iMac finales de 2012.

S.O.: macOS Sierra.

Navegador: Mozilla Firefox 52.0.2 (64-bit).

Nombre y Apellidos: Esther, Colunga García.

DNI: 11401223P.

Ciudad: Oviedo.

Teléfono: 123456789.

Email: mailesther@mail.com.

Consideraciones Previas²

Debido a que vamos a trabajar con la sede electrónica de la Administración Pública nuestro navegador deberá cumplir con algunos estándares. Y, por lo tanto, deberemos de realizar algunas configuraciones para obtener nuestro certificado. Así mismo debemos de tener en cuenta una serie de recordatorios imprescindibles:

- No formatear el ordenador entre el proceso de solicitud y el de descarga del certificado.
- Todo el proceso se debe realizar desde el mismo equipo, usuario y navegador.
- No actualizar el equipo mientras dure el proceso.

La Administración Pública requiere como estándar la utilización de las últimas versiones de Internet Explorer o Mozilla Firefox. Por lo que es preciso descargar la última versión del navegador que vayamos a utilizar. En nuestro caso como marcan los datos del dominio del ejemplo será la última versión del navegador Mozilla Firefox, ya que es el único de la lista soportado en macOS Sierra.

¹ Fábrica Nacional de Moneda y Timbre.

² Todas las Consideraciones Previas pueden encontrarse en <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/consideraciones-previas>

Así mismo para que nuestro equipo confíe en los certificados de la sede electrónica de la FNMT hemos de proceder a instalar los siguientes certificados: AC Raíz FNMT-RCM, FNMT Clase 2 CA, AC FNMT Usuarios, AC Componentes Informáticos.

Solicitar Certificado³

Tras haber instalado los certificados de la FNMT necesarios procederemos a realizar la solicitud de nuestro certificador de persona física. Para ello tendremos que introducir nuestro número de DNI, Primer Apellido, Correo Electrónico dos veces y la longitud de la clave generada (2048).

Persona Física
Obtener Certificado Software
Consideraciones Previas
Solicitar Certificado
Acreditar Identidad
Descargar Certificado
Copia de Seguridad
Obtener Certificado con Android
Obtener Certificado con DNle
Verificar estado
Renovar
Anular
Certificado de Representante
Administración Pública
Certificados de componente
Soporte Técnico

 **Solicitar Certificado (paso 2)**

SOLICITUD DE CERTIFICADO FNMT DE PERSONA FÍSICA
Para tramitar la solicitud de su Certificado FNMT de Persona Física, por favor introduzca la información requerida:

Nº DEL DOCUMENTO DE IDENTIFICACIÓN

11401223P

PRIMER APELLIDO(tal y como aparece en su documento de identificación)

Colunga

CORREO ELECTRÓNICO

mailesther@mail.com

Confirme aquí su CORREO ELECTRÓNICO

mailesther@mail.com

Elija longitud de clave 2048 (Grado Alto)

Grado alto

INSTRUCCIONES:

- Recuerde que para evitar problemas en la solicitud y descarga de su certificado es necesario haber configurado correctamente su navegador. En nuestra sede electrónica encontrará el software de configuración automática.
- El nº del documento de identificación (NIF / NIE) deberá tener una longitud de 9 caracteres. Rellene con ceros a la izquierda si es necesario
- Asegúrese de que el correo electrónico asociado a su certificado es correcto, ya que a través de éste se enviarán todas las notificaciones sobre el ciclo de vida de su certificado.

[Pulse aquí para consultar y aceptar las condiciones de expedición del certificado](#)

Enviar petición

Una vez realizada la petición nos se nos proporcionará un Código de Solicitud.

Estimado/a Sr/a Colunga:

A continuación le facilitamos el CÓDIGO DE SOLICITUD del Certificado FNMT de Persona Física que nos ha solicitado:

918273465

NIF asociado a la solicitud:

11401223P

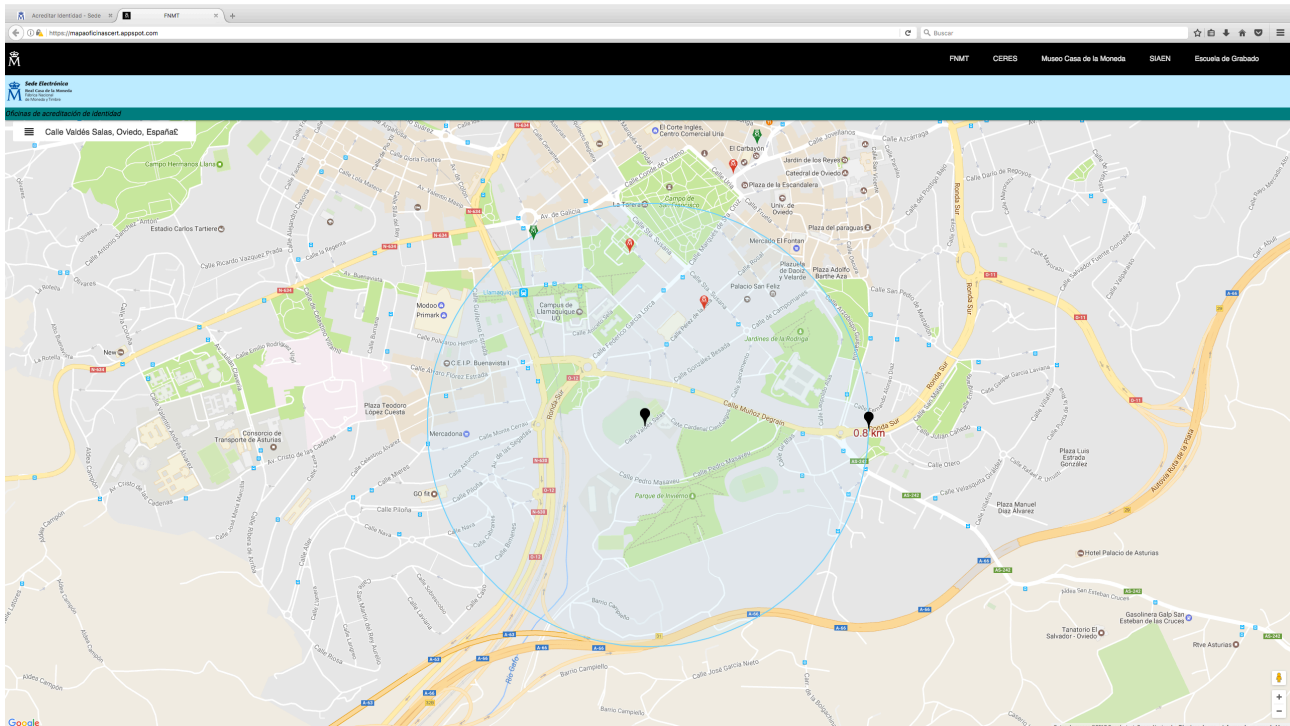
Una vez tenemos nuestro Código de Solicitud podemos continuar con el siguiente paso, que será acreditar que somos la persona que ha solicitado el certificado.

³ Sobre el formulario que se encuentra en <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/solicitar-certificado>

Acreditar Identidad⁴

Una vez tenemos nuestro Código de Solicitud tendremos que acudir personalmente a una Oficina de Registro⁵ para acreditar nuestra identidad. Para ello deberemos de ir acompañados de nuestro Código de Solicitud y DNI, Pasaporte o Carnet de Conducir.

Para encontrar las Oficinas de Registro más cercanas usaremos la siguiente aplicación:
<https://mapaoficinascert.appspot.com/>.



Gracias a esta aplicación sabemos que las oficinas más cercanas a nuestra ubicación son las de la TGSS que se ubican en C/ Pérez de la Sala, 9. Nos dirigimos a dicha oficina y una vez allí obtenemos un ticket para “Trámites con la Administración Pública”. Vamos a la mesa que se nos indica y le entregamos a la persona que allí se encuentre nuestro Código de Solicitud y nuestro DNI. Dicha persona corroborará nuestra identidad con nuestro DNI y se procederá a activar el certificado para su descarga. De la misma forma se nos notificará por SMS y email.

⁴ Instrucciones actualizadas en <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/acreditar-identidad>

⁵ Las Oficinas de Registro están disponibles en las oficinas de la Seguridad Social y las Delegaciones y Administraciones de la AEAT.

Descargar Certificado⁶

Cuando se nos notifique que nuestro certificado digital está listo para su descarga procedemos a rellenar los datos del siguiente formulario.

Persona Física
Obtener Certificado Software
Consideraciones Previas
Solicitar Certificado
Acreditar Identidad
Descargar Certificado
Copia de Seguridad
Obtener Certificado con Android
Obtener Certificado con DNle
Verificar estado
Renovar
Anular
Certificado de Representante
Administración Pública
Certificados de componente
Soporte Técnico

Descargar Certificado (paso 4)

Para descargar el certificado debe usar el mismo ordenador, el mismo navegador y el mismo usuario con el que realizó la Solicitud e introducir los datos requeridos exactamente tal y como los introdujo entonces.

DESCARGAR CERTIFICADO FNMT DE PERSONA FÍSICA

Para descargar e instalar su certificado introduzca la siguiente información:

Nº DEL DOCUMENTO DE IDENTIFICACIÓN	11401223P
PRIMER APELLIDO	Colunga
CÓDIGO DE SOLICITUD	918273465

[Pulse aquí para consultar y aceptar las condiciones de uso del certificado](#)

[Descargar Términos y Condiciones](#) [Descargar Certificado](#)

Recuerde que en caso de haber solicitado un certificado software, la instalación del mismo deberá llevarla a cabo en el mismo equipo en el que realizó la solicitud. Si generó su petición en tarjeta criptográfica, antes de realizar la descarga, confirme que dicha tarjeta está lista para ser usada.

A continuación se descargará nuestro formulario en formato p12⁷. Ya está ya tenemos nuestro certificado digital en nuestro ordenador.

⁶ Formulario en <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/descargar-certificado>

⁷ El formato p12 representa la copia de seguridad con clave privada de un certificado exportado desde Firefox.

Caso de uso en la Administración Pública

Una vez tenemos nuestro certificado expedido por la FNMT podemos realizar diversos trámites a través de las distintas sedes electrónicas de la Administración Pública. Como punto de acceso general a todas las sedes electrónicas tenemos:

https://administracion.gob.es/pag_Home/index.html

A través de esta página podemos acceder al resto de servicios ofrecidos por las distintas sedes.

Para este caso práctico extenderemos el dominio del caso anterior de la siguiente forma:

Equipo: iMac finales de 2012.

S.O.: macOS Sierra.

Navegador: Mozilla Firefox 52.0.2 (64-bit).

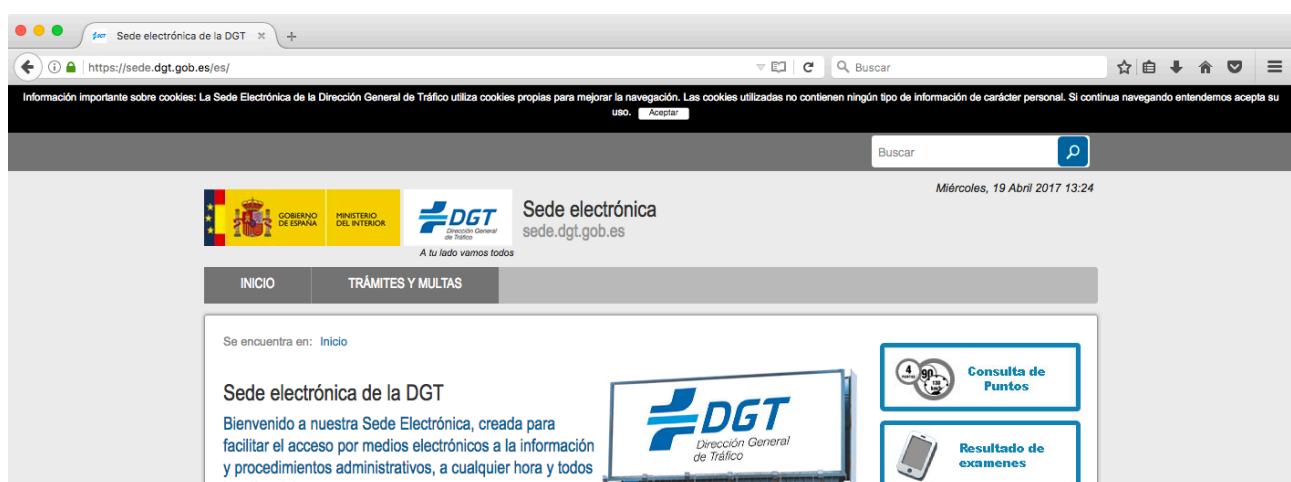
Nombre y Apellidos: Guillermo, Facundo Colunga.

DNI: 45170929X.

Trámite a realizar: Consulta de puntos en carnet de conducir a través de la sede de la DGT.

Acceder a la Sede Electrónica

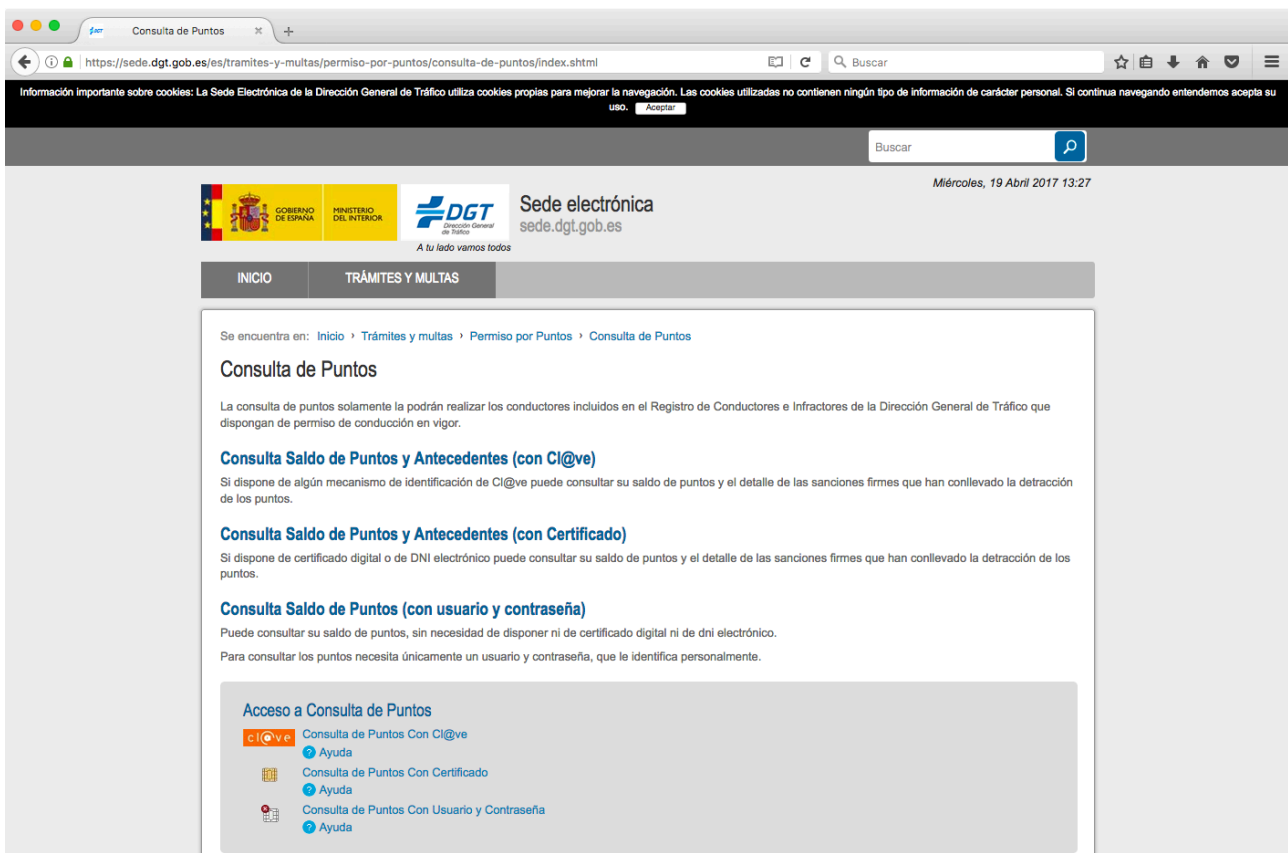
Para este caso práctico accederemos a la Sede Electrónica de la DGT⁸. Y una vez en la página de inicio de la Sede seleccionaremos el trámite que queremos realizar, en nuestro caso "Consulta de Puntos".



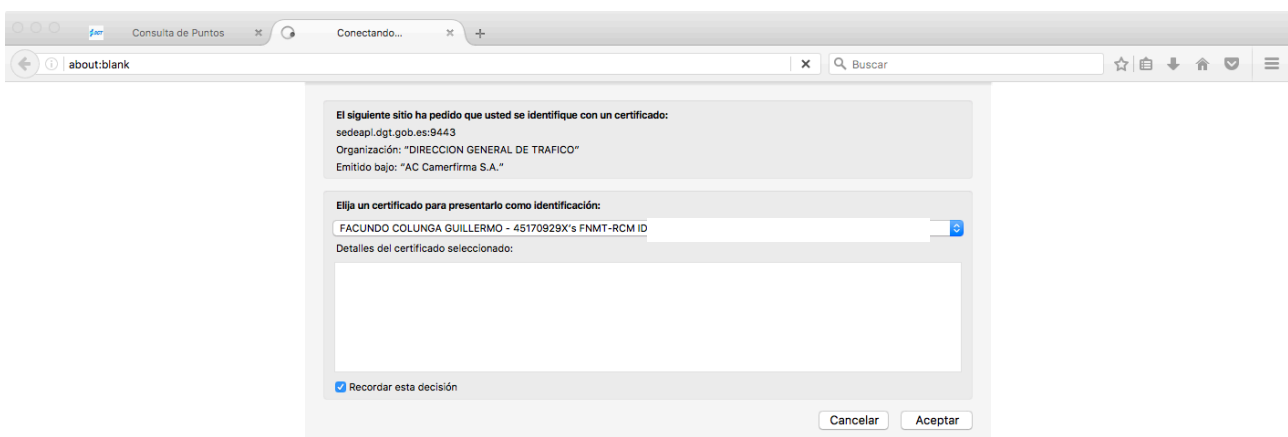
⁸ <https://sede.dgt.gob.es/es/>

Inicio de Sesión en la Sede Electrónica

Para poder realizar cualquier trámite personal en la Sede Electrónica es necesario que se inicie sesión con alguno de los mecanismos disponibles. Continuando con el ejemplo se nos muestran las distintas opciones de inicio de sesión en la sede de la DGT.



Puesto que aún no se han configurado los sistemas @Clave y Usuario y contraseña para la persona física del ejemplo usaremos el enlace que pone "(Consulta de Puntos con Certificado)". Y como es de esperar nos dice que seleccionemos uno de los certificados instalados en nuestro navegador para hacer la autenticación en la Sede.



Realización Proceso en la Sede Electrónica

Una vez que hemos seleccionado el certificado que queremos realizar y la sede comprueba que es válido se nos dirige automáticamente al trámite a realizar. En nuestro caso: Consulta de saldo actual de puntos en carnet de conducir.

The screenshot shows a web browser window with the URL https://sedeapl.dgt.gob.es:9443/WEB_COPACI3/certificado/verSaldoPuntosCert.faces. The page header includes the DGT logo and the text "consulta de saldo de Puntos". The main content area displays the "Saldo actual de puntos" for the license holder "45170929 GUILLERMO FACUNDO COLUNGA". A large box shows the current balance of "12 puntos". Below this, the "Historial de antecedentes" section contains a table with the following data:

Fecha	Puntos	Movimiento	Saldo final	Organismo	Estado
06.09.2015	+4	Movimiento de Actualización de puntos	12		Activo

Below the table, there is a link to "Imprimir" and a note: "* : Cancelado a efectos de graduación de sanciones según artículo 113.4 del LTVS". The footer of the page includes a small image of a car and the text "Aviso legal | Accesibilidad".

Caso de uso en la Universidad de Oviedo

La Universidad de Oviedo también ofrece la posibilidad de realizar trámites con certificados digitales expedidos por la FNMT. Para este ejemplo usaremos el mismo dominio que en el caso anterior.

Equipo: iMac finales de 2012.

S.O.: macOS Sierra.

Navegador: Mozilla Firefox 52.0.2 (64-bit).

Nombre y Apellidos: Guillermo, Facundo Colunga.

DNI: 45170929X.

Trámite a realizar: Acceso al curso de Seguridad de Sistemas Informáticos del Campus Virtual de la Universidad de Oviedo con Certificado Digital.

Acceder a la intranet de la Universidad de Oviedo

Podemos acceder desde <https://intranet.uniovi.es>.

Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Español / English / Asturianu


Servicios de UniOvi en Internet - Acceso

Introduzca su Usuario y Contraseña.

Usuario:

Contraseña:

INICIAR SESIÓN **LIMPIAR**

 [Acceso con certificado digital o DNI](#)

i

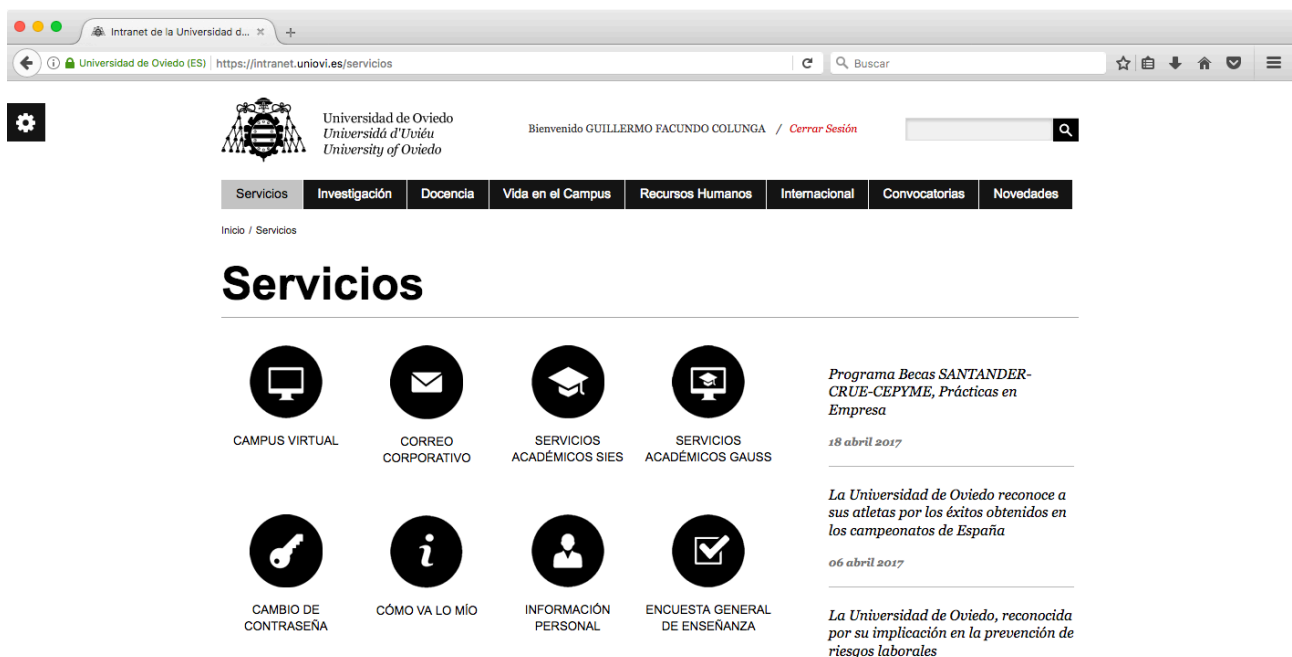
Por razones de seguridad...

1. No acceda a la plataforma desde enlaces de páginas no oficiales de la Universidad de Oviedo.
2. No comunique sus datos de acceso a terceros.
3. Recuerde cerrar la sesión y el navegador web cuando termine de utilizar los servicios.

El usuario y la contraseña para autenticarse son los utilizados para el correo electrónico de UniOvi.

© Universidad de Oviedo

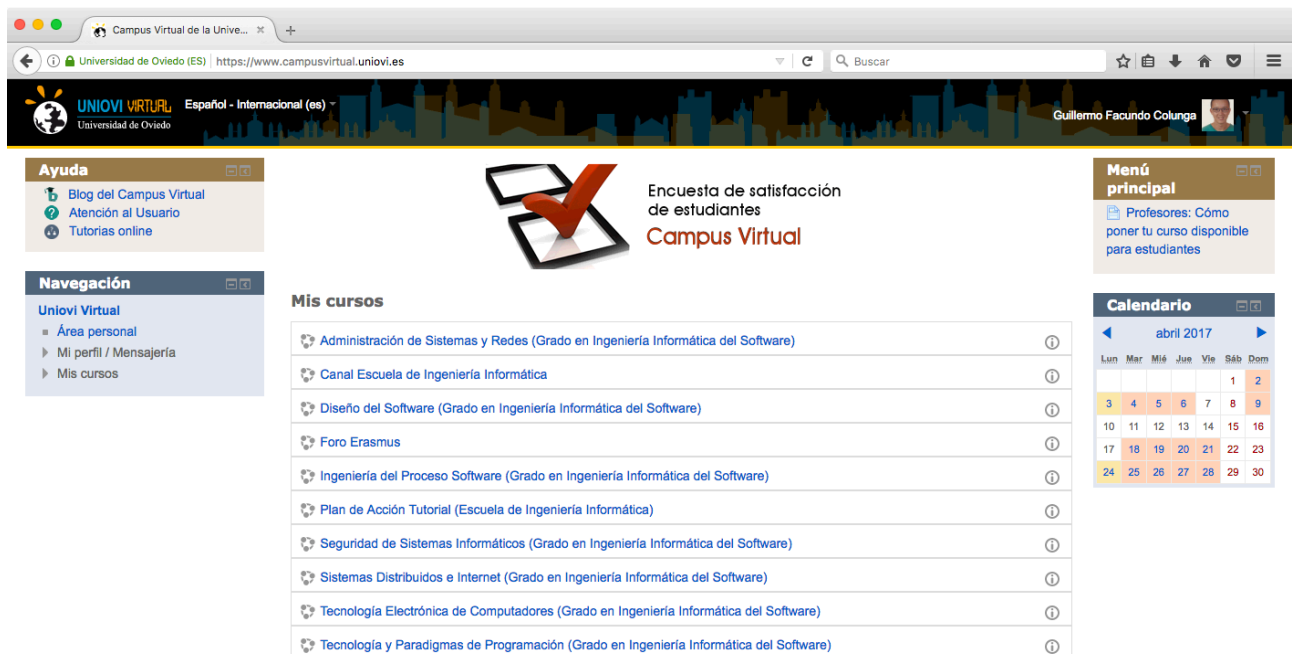
Una vez en la página de registro seleccionamos el enlace de “Acceso con certificado digital o DNI”. Que nos pedirá que seleccionemos el certificado que vamos a usar como en el ejemplo anterior. Y finalmente, si el certificado es válido, nos llevará a la página de inicio de la intranet de la Universidad de Oviedo.



Ya hemos accedido a la intranet de nuestra Universidad sin tener que introducir ni nuestro usuario ni nuestra contraseña.

Acceder al curso de Seguridad en Sistemas Informáticos

Para ello accederemos al Campus virtual a través del enlace⁹ proporcionado en el apartado de "Servicios".



Una vez hemos accedido al campus virtual sólo tenemos que hacer click sobre el enlace del curso de Seguridad de Sistemas Informáticos.

⁹ La posición del enlace puede variar e incluso no estar visible, dependiendo de la configuración única que cada usuario haya realizado sobre su sesión de la intranet. Si no estuviese visible bastaría con hacer click en el engranaje de la parte superior izquierda y clicar sobre campus virtual.

The screenshot shows a web browser window with the URL <https://www.campusvirtual.uniovi.es/course/view.php?id=123>. The page header includes the UNIOVI VIRTUAL logo, the text 'Español - Internacional (es)', and the user's name 'Guillermo Facundo Colunga'. The main content area is titled 'Información general de la asignatura' and lists several links: 'Novedades', 'Foro de uso general', 'Evaluación', 'Presentación de la asignatura', and 'Glosario de la asignatura'. Below this, there is a section for 'Calificaciones de la asignatura' with links for 'Fecha del Primer parcial' and 'Forma de evaluación Seminarios'. The left sidebar contains navigation links for 'Personas', 'Navegación', and 'Accesos Directos'. The right sidebar shows 'Actividad reciente' and 'NUEVOS MENSAJES EN FOROS'.

Y de esta forma hemos conseguido acceder al curso de Seguridad en Sistemas Informáticos de la Universidad de Oviedo, ubicado en su Campus virtual, sin necesidad de introducir ni usuario ni contraseña.

Este mismo proceso se podría realizar para cualquier otro trámite online con la Universidad de Oviedo gracias a que esta entidad confía en los certificados digitales emitidos por la Fábrica Nacional de Moneda y Timbre.

Bibliografía

- Página web de la Universidad de Valencia: <http://www.uv.es/sto/cursos/seguridad.java/html/sjava-19.html>
- Sede Electrónica Fábrica Nacional de Moneda y Timbre: <https://www.sede.fnmt.gob.es>
- Agencia Tributaria Española: http://www.agenciatributaria.es/AEAT.internet/Inicio/Ayuda/_comp_Consultas_informaticas/Categorias/Firma_digital_certificado_o_DNle_y_sistema_Cl_ve_PIN/Certificados_electronicos/Como_anular_su_certificado_electronico/Como_anular_su_certificado_electronico.shtml
- CamerFirma: <http://www.camerfirma.com/area-de-usuario/revocacion-de-certificados/>
- Anular Certificado FNMT: <https://www.sede.fnmt.gob.es/certificados/certificado-de-representante/anular>
- Portal Administración Electrónica: <http://firmaelectronica.gob.es/Home/Empresas/Autoridades-Certificacion.html>
- Junta de Andalucía - Autoridades Certificadoras: <http://e-administracion.cea.es/autoridades>
- Web Fábrica Nacional de Moneda y Timbre: <http://www.fnmt.es/>
- Wikipedia - Agencia Notarial de Certificación: https://es.wikipedia.org/wiki/Agencia_Notarial_de_Certificaci%C3%B3n
- Wikipedia - CamerFirma: https://es.wikipedia.org/wiki/AC_Camerfirma
- Presentación Sistemas de la Información, Criptografía – UAB.

AUTORIZACIÓN PARA PUBLICACIÓN DE DATOS PERSONALES

Yo, **Guillermo Facundo Colunga** con D.N.I. **45170929-X**, autorizo que mis siguientes datos personales sean incluidos en el correspondiente proyecto sobre **Certificados Digitales** de la asignatura de **Seguridad en Sistemas Informáticos** de la **Universidad de Oviedo** con periodicidad **2017**. _____

_____ DATOS PERMITIDOS _____

- Nombre. _____
- Apellidos. _____
- Documento Nacional de Identidad. _____
- Saldo de Puntos en el Carnet de Conducir y posible historial.-
- Pantalla de inicio de la Intranet de la Universidad de Oviedo.
- Pantalla de inicio Campus Virtual de la Universidad de Oviedo.
- Contenido personal del Campus Virtual del curso Seguridad de Sistemas Informáticos. _____

_____ FIN DATOS PERMITIDOS _____

Cualquier otro dato no incluido en la anterior lista se considerará no permitido para su inclusión en el proyecto. _____=



Salinas, 2017, Abril, 17.