Formación para Registradores

Departamento de CERES

Área de Registro de Usuarios

MINISTERIO DE ECONOMÍA Y HACIENDA
Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Índice

Cambio de la Administración en la forma de comunicarse con los ciudadanos.

Factores del cambio:

✓ Desarrollo de nuevos factores tecnológicos (Internet, telefonía móvil, etc.), que abren nuevos campos en las comunicaciones.

✓ Demanda de los ciudadanos de una Administración ágil y moderna

Resultados:

✓ Por parte de las Administraciones Públicas, este cambio ha dado lugar al desarrollo de aplicaciones que utilizan los nuevos canales de comunicación.

Que se persigue

✓ Promover la gestión de la calidad en las Administraciones Públicas

✓ Mejorar la atención al ciudadano y establecer un sistema integral de la comunicación

✓ Configurar una organización flexible y eficaz

Internet es una red descentralizada, sometida a potenciales ataques.

RIESGOS DEL USO DE INTERNET

- Acciones fraudulentas. Sabotaje en datos y redes.
- Obtención de información privilegiada y confidencial
- Pérdidas económicas debidas a violaciones de la seguridad informática.

Canal SEGURO de comunicaciones

Permite autenticar y garantizar la confidencialidad de las comunicaciones a través de redes abiertas

Requisitos de una comunicación segura

- **Autenticación.-** Asegurar que la persona con quien nos comunicamos es quien dice ser.
- **Integridad.-** La información no puede ser manipulada
- **Identificación.-** Puede identificarse al emisor de un mensaje.
- **Confidencialidad.-** Nadie no autorizado puede leer el mensaje.

Autenticación | Integridad | No Repudio

FIRMA ELECTRÓNICA

Confidencialidad ⇒ **CIFRADO**

Cifrado digital

Si a un mensaje en claro se le aplica un algoritmo de cifrado se genera un mensaje cifrado

- **CLAVES SIMÉTRICAS, donde la clave de cifrado y la clave de descifrado son idénticas. El problema de este tipo de claves es que hay que enviar la clave por el canal de comunicaciones, con lo que podría ser interceptada .**

Gran velocidad. Cifrado de grandes cantidades de datos

- **CLAVES ASIMÉTRICAS, donde tenemos una clave de cifrado y otra de descifrado diferente. De esta forma no es necesario enviar ninguna clave por el canal de comunicaciones, ya que una de ellas es pública.**

Operación lenta

Para cifrar se utiliza: algoritmo de clave pública + clave simétrica

Envío de un mensaje cifrado

El mensaje se cifra con el sistema de criptografía de clave simétrica

(clave de sesión)

Envío de la clave de sesión cifrada con la clave pública del destinatario

(criptografía de clave asimétrica)

El destinatario recibe el mensaje cifrado con la clave de sesión

Y la clave de sesión cifrada con su clave pública

Para leer el mensaje el destinatario utiliza su clave privada para descifrar la clave de sesión

Una vez obtenida la clave de sesión ya puede descifrar el mensaje

La Firma Electrónica

La firma electrónica es **el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.**

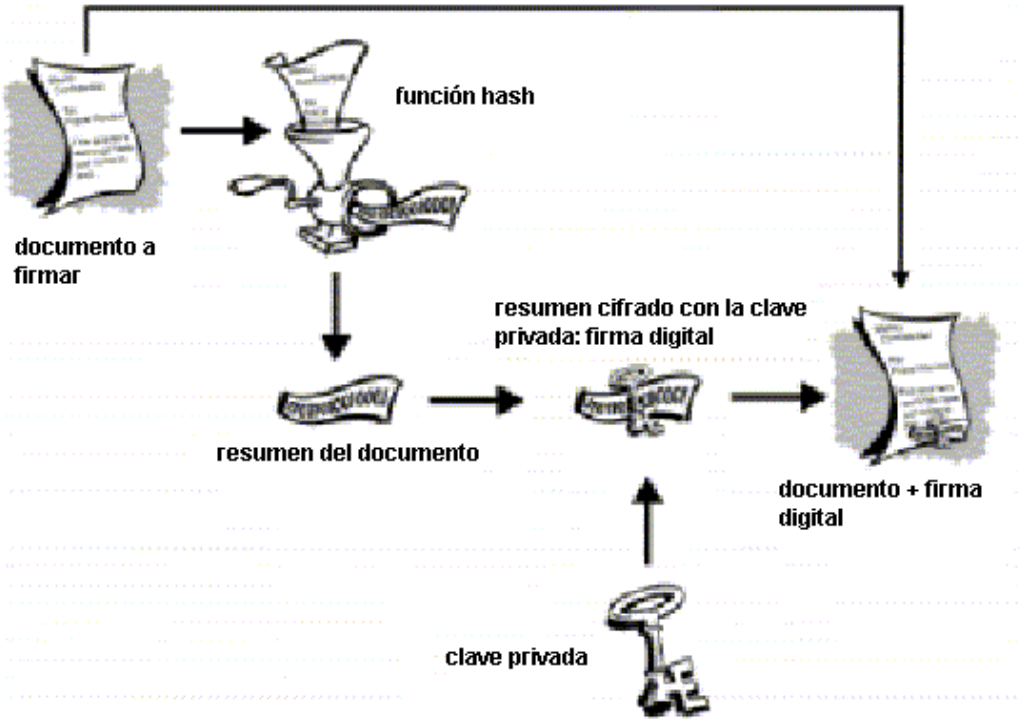
Firma electrónica avanzada.- Es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida.- Se considera firma electrónica reconocida a la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La Firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel

La Firma Electrónica: criptografía de clave asimétrica

La **ejecución** de la firma electrónica consiste en cifrar con la clave privada un resumen del documento a firmar.



La **verificación** de la firma electrónica consiste en**:**

- Descifrar, con la clave pública, el resumen previamente firmado **(Autenticación y No Repudio)**
- Hacer un nuevo resumen del documento y comparar ambos **(Integridad)**

Soporte de las claves

Soporte de clave PÚBLICA

- Los CERTIFICADOS son el soporte para la clave pública.
- La gestión de certificados es llevada a cabo por la Entidad de Certificación.

Soporte de clave PRIVADA

El soporte de la clave privada puede ser en:

- ☞ Software
- ☞ tarjeta
- ☞ Solución mixta

Certificado X.509

Es un documento electrónico que relaciona las herramientas de firma electrónica en poder de cada usuario con su identidad personal.

Conjunto de datos a ser firmado

- Versión del certificado
- Algoritmos usados en la firma
- Código identificativo del certificado
- Nombre del Prestador de Servicios de Certificación
- Fechas de validez del certificado
- Nombre y apellidos del firmante
- Clave pública

Otra información: atributos, límite de uso

- ✓ Algoritmos usados en la firma
- ✓ Firma de la Autoridad de Certificación

Garantías del CERTIFICADO

La eficacia de las operaciones de cifrado y firmado solo están garantizadas si:

La clave privada solo es conocida por el usuario

La clave pública conocida por todos sin confusión entre ellas

CERTIFICADO DE USUARIO; CERTIFICADO DE CLAVE PÚBLICA; CERTIFICADO

El certificado contiene las claves públicas de un usuario, junto con alguna otra información, hechas infalsificables por el cifrado con la clave privada de la autoridad de certificación que la emitió.

MINISTERIO DE ECONOMÍA Y HACIENDA
Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre
CERES

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

La FNMT- RCM como Prestador de Servicios de Certificación: Esquema funcional

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Entidades Públicas que utilizan el certificado de la FNMT-RCM

Implantación

Administración General del Estado

Ministerio de Economía y Hacienda
- El propio Ministerio
- AEAT, INE, CNE,,CMT,,ICO,
- Dirección General del Tesoro
- Instituto de Contabilidad y Auditoria de Cuentas

Ministerio de Industria, Turismo y Comercio
- Entidad Pública Empresarial Red.es

Ministerio de Ciencia y Tecnología
- El propio Ministerio
- Oficina Española de Patentes y Marcas
- Comisión Mercado Telecomunicaciones

Ministerio de la Presidencia
- Boletín Oficial del Estado

Ministerio de Fomento
- RENFE
- Dirección General de Transportes por Carretera

Ministerio de Interior
- Dirección General de la Guardia Civil

Ministerio de Trabajo y Asuntos Sociales
- El propio Ministerio
- Tesorería General de la Seguridad Social

Ministerio de Justicia

Ministerio de Sanidad y Consumo

Ministerio de Administraciones Públicas

Ministerio de Medio Ambiente

Ministerio de Educación y Ciencia

Ministerio de Cultura

Otros Organismos
- Consejo General del Poder Judicial
- Consejo de Seguridad Nacional
- Banco de España
- Comisión Nacional del Mercado de Valores
- Fundación Tripartita para la Formación y el Empleo
- S.A.E. Correos y Telégrafos S.A.
- Paradores Nacionales de Turismo
- Universidades

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Entidades Públicas que utilizan el certificado de la FNMT-RCM

Administración Autonómica

Administración Local

Colegios Profesionales

Comunidades Autónomas

- Xunta de Galicia
- Gobierno de Navarra
- Gobierno de Canarias
- Junta de Andalucía
- Gobierno de la Comunidad de Madrid
- Gobierno de la Rioja
- Junta de Castilla y León
- Junta de Comunidades de Castilla – La Mancha
- Comunidad Autónoma de la Región de Murcia
- Principado de Asturias
- Junta de Extremadura

Colegios profesionales

- Consejo General del Notariado
- Ilustre Colegio de Registradores de la Propiedad y Mercantiles de España
- Ilustre Colegio de Abogados de Madrid
- Ilustre Consejo General de Colegios Oficiales de Odontólogos y Estomatólogos
- Ilustre Colegio de Ingenieros Industriales de Madrid
- COIT de Telecomunicaciones

Diputaciones Provinciales o Cabildos

- Barcelona
- A Coruña
- Lugo
- Orense
- Pontevedra
- Córdoba
- Jaén
- Huelva
- Sevilla
- Granada
- Almería
- Cádiz
- Málaga

Ayuntamientos

- Madrid, **Valencia, Salamanca**
- **Jaén, Córdoba, Huelva, Granada**
- **Torrelavega,** Laredo
- **Pozuelo de Alarcón,** San Sebastián de los Reyes
- **Alboraya, Catarroja,** Quart de Poblet, **Totana**
- Villanueva de Gállego, Tarazona

Más de 150 Ayuntamientos menores de 50.000 habitantes de la C.A. de Andalucía.

www.cert.fnmt.es

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

CERES presta cobertura a:

- **14 Ministerios**
- Multitud de organismos autónomos de la Administración General del Estado
- **16 CCAA**
- más de 6.000 Ayuntamientos
- **gran número de empresas privadas y**
- **numerosas Universidades**

Administración General del Estado

Administración Autonómica

Administración Local

Colegios Profesionales

Algunos servicios disponibles en la red

- Presentación de recursos y reclamaciones
- Comprar y vender Deuda del Estado
- Cumplimentar los datos del censo de población y viviendas
- Capturar y validar los préstamos de mediación que concede el ICO
- Presentación y liquidación de impuestos
- Pago de multas
- Consultas y trámites para la solicitud de subvenciones
- Consultas de empresas al registro de éstas y al estado de sus expedientes
- Consulta e inscripción en el padrón municipal
- Constitución de depósitos y participación en subastas On–line
- Firma digital de documentos oficiales y expedición de copias compulsadas

La FNMT-RCM en su actividad como PSC
Certificados que ofrece

Certificados emitidos y gestionados por la FNMT-RCM bajo la denominación de Certificados FNMT Clase 2 CA:

- Para Personas Físicas
- Para Personas Jurídicas
- Para Componentes y Firma de Sw.

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

La FNMT- RCM como Prestador de Servicios de Certificación: Servicio de atención al ciudadano

La FNMT-RCM pone a su disposición una serie de servicios para resolver sus dudas y recoger sus sugerencias.

1. RESPUESTA A LAS PREGUNTAS MÁS FRECUENTES

- El servicio se actualiza de forma periódica.
- Incluye todas las preguntas frecuentes.
- Proporciona una información precisa sobre cómo solucionar el problema expuesto.

2. FORMULARIO VIA WEB

- El usuario recibe un mensaje por correo electrónico con la solución a su consulta.

3. CORREO ELECTRÓNICO

- El usuario debe incluir en el correo el mensaje exacto del error para ser respondido eficazmente.

4. TELÉFONOS DE ATENCIÓN AL USUARIO (TF 902.18.16.96)

- Si el usuario tiene alguna duda sobre la obtención del certificado, la revocación del mismo o en relación a errores que se produzcan en su conexión con www.cert.fnmt.es, puede llamar por teléfono.

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

MARCO ESTATAL

- **Ley 59/2003**, de 19 de diciembre, de firma electrónica, por la que se deroga el Real Decreto Ley 14/1999, de 17 de septiembre por el cual se regula el uso **de la firma electrónica**, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación (incorpora modificaciones a dicho RDL)

- **REAL DECRETO** 1317/2001 de 30 de Noviembre, por el que se desarrolla el artículo 81 de la Ley 66 1997 de 30 de Diciembre, de Medidas Fiscales, Administrativas y del Orden Social, **en materia de prestación de servicios de seguridad, por la FNMT-RCM**, en las comunicaciones **a través de medios electrónicos, informáticos y telemáticos** con las Administraciones Públicas.

MARCO COMUNITARIO

- **DIRECTIVA** 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se **establece un marco comunitario para la firma electrónica** Diario Oficial n° L 013 de 19/01/2000 P. 0012-0020

La Oficina de Registro actúa de intermediaria entre el solicitante y el Prestador de Servicios de Certificación

Aporta sus datos

Acredita la identidad

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Envía solicitud de registro
(Información con los datos del solicitante)

Procedimiento de Solicitud de Certificados

Accede a la web de la FNMT-RCM WWW.CERT.FNMT.ES

Solicita un certificado (introduce su NIF)

La web le devuelve un Código de Solicitud

Aporta sus datos personales
Acredita su identidad
Entrega el Código de Solicitud

OFICINA DE REGISTRO

Entrega copias del contrato (3)

Firma / Entrega el contrato

Verifica firma del solicitante
Entrega copia del contrato (1)

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Envío de Solicitud
(Firmada y Cifrada)

Envío copia de contratos
(semanalmente)

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

Descarga de Certificados Clase 2

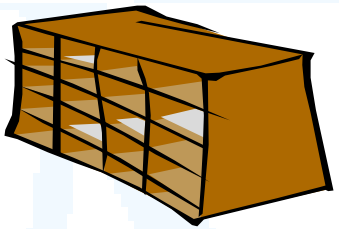
Accede a la web de la FNMT-RCM **WWW.CERT.FNMT.ES**

Se conecta a la base de datos de los certificados y solicita la descarga de su certificado

Introduce su NIF

Introduce su Código de Solicitud

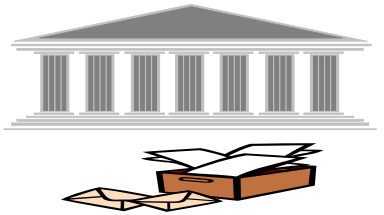
Se descarga su certificado



Deposita el certificado en una base de datos

Crea el certificado

OFICINA DE REGISTRO



Envío de Solicitud
(Firmada y Cifrada)

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

Tarjeta criptográfica: Identidad electrónica

Características

- Identifica sin error a una persona
- Protegida por un PIN
- Garantía de seguridad mediante claves de firma y encriptación

Ventajas para el usuario

- Portabilidad.
- Diversos puntos de acceso

Ventajas de seguridad

- Procesos criptográficos internos
- La clave privada nunca sale al exterior
- Imposible de duplicar
- El usuario tiene que perder PIN y tarjeta para que su identidad sea suplantada

Obtención de Certificados Clase 2 en Tarjeta Criptográfica

Para poder operar con una tarjeta criptográfica deberá disponer además de la tarjeta de un lector de tarjetas homologado

Instalar físicamente el lector de tarjetas:

- **Se conectará al puerto USB de su ordenador o al puerto serie**
- **Seguir las instrucciones del fabricante**
- **Instalar los drivers proporcionados por el proveedor del lector**

Si el sistema operativo es Windows 95/98 instalar los Componentes Base de Microsoft

Si el sistema operativo es Windows XP o 2000 no deberá instalarlos

Instalar el Módulo Criptográfico para manejo de tarjetas que integra todos los elementos necesarios para el funcionamiento de los Certificados de Usuario en tarjeta

Los elementos que se instalan son:

- **Software básico manejo de la tarjeta, desbloqueo de la tarjeta y cambio de PIN.**
- **Módulo PKCS#11, para trabajar en Netscape.**
- **Módulo CSP, para trabajar con Internet Explorer.**

Obtención de Certificados Clase 2 en Tarjeta Criptográfica

Pasos previos a la solicitud del certificado

- Instalar los drivers del lector de tarjetas

Acceder a la web de la FNMT-RCM WWW.CERT.FNMT.ES

En Soporte Técnico → Área de descarga de software

- Descargar el software para la tarjeta criptográfica

- Introducir la tarjeta en el lector

Obtención de Certificados Clase 2 en Tarjeta Criptográfica

Accede a la web de la FNMT-RCM WWW.CERT.FNMT.ES

Solicita un certificado de usuario en tarjeta criptográfica (introduce su NIF/NIE)

La web le devuelve un Código de Solicitud

Aporta sus datos personales
Acredita su identidad
Entrega el Código de Solicitud

Entrega copias del contrato (3)

Firma / Entrega el contrato

Verifica firma del solicitante
Entrega copia del contrato (1)

OFICINA DE REGISTRO

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Envío de Solicitud
(Firmada y Cifrada)

Envío copia de contratos
(semanalmente)

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Descarga de Certificados Clase 2 en Tarjeta Criptográfica

Accede a la web de la FNMT-RCM **WWW.CERT.FNMT.ES**

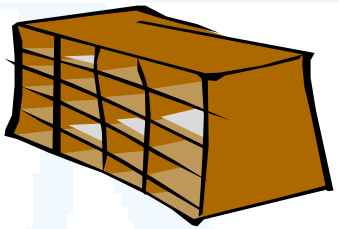
Se conecta a certificado de usuario en tarjeta criptográfica

Solicita la Descarga de su Certificado

Introduce su NIF/NIE

Introduce su Código de Solicitud

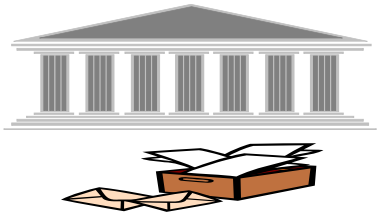
Se descarga su certificado en la tarjeta



Deposita el certificado en una base de datos

Crea el certificado

OFICINA DE REGISTRO



Envío de Solicitud
(Firmada y Cifrada)

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

MINISTERIO DE ECONOMÍA Y HACIENDA

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERES

www.cert.fnmt.es

Obtención del certificado FNMT a partir del DNIe

1.- SOLICITUD, Accede a la web de la FNMT-RCM WWW.CERT.FNMT.ES

Solicita un certificado autenticándose y firmando la solicitud con su DNIe (introduce su NIF)

La web le devuelve un Código de Solicitud

2.- ACREDITACIÓN EN OFICINA DE REGISTRO: no es necesaria ya que se realiza a través de su DNIe

3.- DESCARGA DEL CERTIFICADO: el solicitante Accede a la Web de la FNMT-RCM WWW.CERT.FNMT.ES, con el mismo ordenador desde el que realizó la solicitud, y solicita la descarga de su certificado

Introduce su NIF
Introduce su Código de Solicitud

se descarga el certificado electrónico

Fábrica Nacional de Moneda y Timbre

Apartado de Correos 50.435
Palacio de Comunicaciones
Plaza de las Cibeles, s/n
28014 Madrid

Teléfono de contacto: 91 566 69 17
91 566 69 16
91 566 66 97

Número de Fax: 91 566 69 05

www.cert.fnmt.es

E-MAIL: registro*ceres@fnmt.es*