Certificados Digitales y Firma Electrónica

Julio Herrero
julio.herrero@coitt.es

GALPON - Grupo de Amigos de Linux de Pontevedra

5 y 6 de noviembre de 2007

Grupo de Amigos de Linux de Pontevedra

Parte I

Primera parte: seguridad y criptografía

Contenido

Introducción

Antecedentes

- Importancia creciente de Internet en el comercio y las comunicaciones.
- Internet es una red insegura: no proporciona mecanismos de autentificación, privacidad o integridad.
  - ¿Quién está al otro lado? ejemplo: configuración maliciosa del correo electrónico.
  - Los ladrones se modernizan: phishing
  - Falta de privacidad: red echelon

Introducción

Antecedentes

- Importancia creciente de Internet en el comercio y las comunicaciones.
- Internet es una red insegura: no proporciona mecanismos de autentificación, privacidad o integridad.
  - ¿Quién está al otro lado? ejemplo: configuración maliciosa del correo electrónico.
  - Los ladrones se modernizan: phishing
  - Falta de privacidad: red echelon

Introducción

Antecedentes

- Importancia creciente de Internet en el comercio y las comunicaciones.
- Internet es una red insegura: no proporciona mecanismos de autentificación, privacidad o integridad.
  - ¿Quién está al otro lado? ejemplo: configuración maliciosa del correo electrónico.
  - Los ladrones se modernizan: phishing
  - Falta de privacidad: red echelon

Introducción

Antecedentes

- Importancia creciente de Internet en el comercio y las comunicaciones.
- Internet es una red insegura: no proporciona mecanismos de autentificación, privacidad o integridad.
  - ¿Quién está al otro lado? ejemplo: configuración maliciosa del correo electrónico.
  - Los ladrones se modernizan: phishing
  - Falta de privacidad: red echelon

Introducción

Antecedentes

- Importancia creciente de Internet en el comercio y las comunicaciones.
- Internet es una red insegura: no proporciona mecanismos de autentificación, privacidad o integridad.
  - ¿Quién está al otro lado? ejemplo: configuración maliciosa del correo electrónico.
  - Los ladrones se modernizan: phishing
  - Falta de privacidad: red echelon

Introducción

Antecedentes

- El comercio, motor económico mundial que se puede aprovechar de una red rápida y barata, pero... ¿se puede comerciar en una red insegura?

Mecanismos necesarios

Necesitamos seguridad

- Hay gran interés por usar Internet para el comercio y comunicaciones confiables ya que es barata, dispone de una gran capilaridad e inmediatez de uso.
- Para ello hay que dotarla de mecanismos de Autentificación, Confidencialidad, Integridad y No repudiación.

Mecanismos necesarios

Necesitamos seguridad

- Hay gran interés por usar Internet para el comercio y comunicaciones confiables ya que es barata, dispone de una gran capilaridad e inmediatez de uso.
- Para ello hay que dotarla de mecanismos de Autentificación, Confidencialidad, Integridad y No repudiación.

Autentificación

Identificamos al interlocutor

- La autentificación nos proporciona seguridad sobre la identidad de un interlocutor o el creador de una información.
- La autentificación puede trabajar en un sentido o en ambos, así nos puede interesar identificar únicamente el origen de los datos, o bien nos puede interesar la autentificación mutua entre entidades. Ejemplo: autentificación mutua ante un banco.

Confidencialidad

Conservamos el secreto

- La confidencialidad nos debe garantizar que nuestra información, ya sea personal o empresarial, no se revela a entes no autorizados.
- Incluso sería de desear que si hacemos un pago electrónico, el banco se limite a pagar lo que le ordenemos, sin necesidad de tener información, que no necesita para nada, acerca de los bienes adquiridos.

Integridad

Evitamos falsificaciones

- Necesitamos protegernos contra la modificación, creación, alteración y borrado de datos para mantener la integridad de nuestra información.
- Ejemplo de alteración: modificación o repetición de una orden de pago.

No repudiación

No hay vuelta atrás

Es fundamental que una vez realizada una operación nadie se pueda volver atrás unilateralmente. Sería muy poco serio que el originador de una información pudiera negarla con total impunidad. Por ejemplo, si alguien ordena un pago electrónico, ese pago debe realizarse. El autor de la orden de pago no puede negar que él la ha dado.

Ejemplos cotidianos

El día a día de la necesidad de seguridad en nuestra vida cotidiana...

- **Autentificación**: carnet de identidad.
- **Confidencialidad**: sobre cerrado.
- **Integridad**: burofax.
- **No repudiación**: Notario.

Nos encontramos con estas necesidades todos los días.

Ejemplos cotidianos

El día a día de la necesidad de seguridad en nuestra vida cotidiana...

- **Autentificación**: carnet de identidad.
- **Confidencialidad**: sobre cerrado.
- **Integridad**: burofax.
- **No repudiación**: Notario.

Nos encontramos con estas necesidades todos los días.

Ejemplos cotidianos

El día a día de la necesidad de seguridad en nuestra vida cotidiana...

- **Autentificación**: carnet de identidad.
- **Confidencialidad**: sobre cerrado.
- **Integridad**: burofax.
- **No repudiación**: Notario.

Nos encontramos con estas necesidades todos los días.

Ejemplos cotidianos

El día a día de la necesidad de seguridad en nuestra vida cotidiana...

- **Autentificación**: carnet de identidad.
- **Confidencialidad**: sobre cerrado.
- **Integridad**: burofax.
- **No repudiación**: Notario.

Nos encontramos con estas necesidades todos los días.

Mecanismos necesarios

¿Como logramos la seguridad necesaria?

- Deberemos buscar o crear la tecnología que nos implemente los mecanismos de **autentificación, confidencialidad, integridad y no repudiación**.
- Esa tecnología será la criptografía.

Mecanismos necesarios

¿Como logramos la seguridad necesaria?

- Deberemos buscar o crear la tecnología que nos implemente los mecanismos de **autentificación, confidencialidad, integridad y no repudiación**.
- Esa tecnología será la criptografía.

Criptografía

Conceptos

- La **criptografía** se ocupa de cifrar información, es decir, cambia de tal manera una información que hace muy difícil recuperarla a menos que se disponga de la clave de cifrado.
- La criptografía es la tecnología que se usa (ya la usaba Julio César) para lograr los objetivos de autentificación, confidencialidad, integridad y no repudiación.
- Muy ligada desde siempre a entornos militares y diplomáticos.

Criptoanálisis

Conceptos

- Por otro lado, el **criptoanálisis** se ocupa de desmontar los procedimientos de cifrado para así obtener la información original. Tanto la criptografía como el criptoanálisis se han ido desarrollando de manera paralela, ya que a medida que se han ido desarrollando métodos de cifrado, también se desarrollaron los métodos de criptoanálisis correspondientes.

Criptología

Conceptos

- De manera genérica, a ambas disciplinas, criptografía y criptoanálisis, se les denomina **criptología**.

Mecanismo criptográfico

- Se genera una información.
- Se transforma mediante un algoritmo controlado por una clave.
- Se envía la información cifrada al receptor por cualquier medio, incluso inseguro.
- El receptor, conocedor de la clave, descifra el criptograma y recupera la información original.

Tipos de seguridad

Hoy en día se puede analizar matemáticamente la seguridad de los algoritmos y protocolos, con lo que podemos definir diferentes tipos de seguridad:

- **Seguridad incondicional:** seguro ante medios ilimitados.
- **Seguridad computacional:** seguro ante medios limitados.
- **Seguridad probable:** el sistema no ha sido roto, pero no se ha demostrado matemáticamente su seguridad.
- **Seguridad condicional:** cuando no se dispone de medios para atacar nuestro sistema.

Tipos de seguridad

Hoy en día se puede analizar matemáticamente la seguridad de los algoritmos y protocolos, con lo que podemos definir diferentes tipos de seguridad:

- **Seguridad incondicional:** seguro ante medios ilimitados.
- **Seguridad computacional:** seguro ante medios limitados.
- **Seguridad probable:** el sistema no ha sido roto, pero no se ha demostrado matemáticamente su seguridad.
- **Seguridad condicional:** cuando no se dispone de medios para atacar nuestro sistema.

Tipos de seguridad

Hoy en día se puede analizar matemáticamente la seguridad de los algoritmos y protocolos, con lo que podemos definir diferentes tipos de seguridad:

- **Seguridad incondicional:** seguro ante medios ilimitados.
- **Seguridad computacional:** seguro ante medios limitados.
- **Seguridad probable:** el sistema no ha sido roto, pero no se ha demostrado matemáticamente su seguridad.
- **Seguridad condicional:** cuando no se dispone de medios para atacar nuestro sistema.

Tipos de seguridad

Hoy en día se puede analizar matemáticamente la seguridad de los algoritmos y protocolos, con lo que podemos definir diferentes tipos de seguridad:

- **Seguridad incondicional:** seguro ante medios ilimitados.
- **Seguridad computacional:** seguro ante medios limitados.
- **Seguridad probable:** el sistema no ha sido roto, pero no se ha demostrado matemáticamente su seguridad.
- **Seguridad condicional:** cuando no se dispone de medios para atacar nuestro sistema.

Un poco de historia

Transposición y sustitución

- Método de transposición: Se altera el orden de las letras.
- Ejemplo de escítala lacedemonia, que usa la transposición.
- Método de sustitución: se cambian las letras del mensaje original por otras del mismo o diferente alfabeto.
- Ejemplos: cifrado de César, CARACOLA se convierte en FDUDFROD. Cine y rot13. Ambos usan la sustitución.

Un poco de historia

Mayor complejidad

- Cifrados polialfabéticos para complicar el criptoanálisis.
- Industrialización de la criptografía: enigma.
- Criptografía actual: simétrica y asimétrica apoyándose en algoritmos matemáticos conocidos y analizados.

Descripción

Características

- La criptografía de clave simétrica usa la misma clave para cifrar y descifrar.
- Se comparte la clave, que debe permanecer en secreto, entre los usuarios.
- Algoritmos públicos deseables, basados en sustituciones y permutaciones.
- Mecanismo: Concierto de clave, cifrado, envío, descifrado.

Descripción

Problemas

- Distribución de la clave.
- Celo de los interlocutores.
- n claves para n interlocutores.

Firma electrónica con criptografía simétrica

¿Podríamos implementar un sistema de firma electrónica?

Si, pero con muchos matices, ya que crea más problemas que los que resuelve. Ejemplo de uso de una clave simétrica: uso de los cajeros automáticos a través de un PIN.

Dos tipos de algoritmos

Algoritmos de cifrado en bloque

Se divide el mensaje en boques y se cifra cada bloque por separado. El cifrado de cada bloque puede ser independiente de los demás o no.

Algoritmos de cifrado en flujo

Se toma el mensaje como una secuencia de bits, los cuales van siendo cifrados uno a uno por una operación XOR con otra secuencia de bits que se usa como clave. Esta secuencia usada como clave es pseudoaleatoria.

Algoritmos usados en criptografía simétrica

Algoritmos de cifrado en bloque

- DES
- Triple DES
- IDEA
- AES

Algoritmos de cifrado en flujo

- RC4
- SEAL

DES

Algoritmo DES

- Probablemente el más extendido.
- Definido como estándar en 1976 para comunicaciones no clasificadas en los EEUU.
- Clave débil (influencia de la **NSA**) de 56 bits y 16 rondas de cifrado.
- Rompible por fuerza bruta en menos de 24 horas.

Triple DES

Algoritmo Triple DES

Se usan dos claves DES de 56 bits (una de ellas dos veces) para cifrar con 112 bits.

IDEA

Algoritmo IDEA

- Desarrollado en 1992.
- Usa claves de 128 bits, generando 16 subclaves de 16 bits
- Usa bloques de 64 bits que se dividen en subbloques de 16 bits.
- Realiza 8 rondas de cifrado.
- Tiene muy buena fama criptográfica.

AES

Algoritmo Advanced Encryption Standar (Rijndael)

- Surgido de un concurso inicado en 1997 para elegir al sucesor del algoritmo DES.
- El proceso finalizó en el año 2000 después de tres rondas.
- Usa un tamaño de clave variable hasta 256 bits y un número de rondas variable.
- Analizado por la comunidad criptográfica mundial, el mejor método de ataque conocido es la fuerza bruta.

RC4

Algoritmo RC4

Algoritmo generador de secuencias de bits para cifrados en flujo. Está sujeto a patentes y su código nunca se ha publiado oficialmente, aunque apareció un código en una lista de correo sobre criptografía, que genera las mismas secuencias.

SEAL

Algoritmo SEAL

Algoritmo generador de secuencias de bits para cifrados en flujo. Desarrollado en 1993, también está sujeto a patentes y optimizado para procesadores de 32 bits.

Descripción

Características

- Revolución en la criptografía en 1975, Diffie y Hellman.
- La criptografía de clave asimétrica usa dos claves para cifrar y descifrar.
- Una clave es pública. La otra clave es privada.
- Lo que cifra una clave lo descifra la otra
- Mecanismo de cifrado usando las claves públicas de los interlocutores

Descripción

Características

- Revolución en la criptografía en 1975, Diffie y Hellman.
- La criptografía de clave asimétrica usa dos claves para cifrar y descifrar.
- Una clave es pública. La otra clave es privada.
- Lo que cifra una clave lo descifra la otra
- Mecanismo de cifrado usando las claves públicas de los interlocutores

Descripción

Características

- Revolución en la criptografía en 1975, Diffie y Hellman.
- La criptografía de clave asimétrica usa dos claves para cifrar y descifrar.
- Una clave es pública. La otra clave es privada.
- Lo que cifra una clave lo descifra la otra
- Mecanismo de cifrado usando las claves públicas de los interlocutores

Descripción

Características

- Revolución en la criptografía en 1975, Diffie y Hellman.
- La criptografía de clave asimétrica usa dos claves para cifrar y descifrar.
- Una clave es pública. La otra clave es privada.
- Lo que cifra una clave lo descifra la otra
- Mecanismo de cifrado usando las claves públicas de los interlocutores

Descripción

Características

- Revolución en la criptografía en 1975, Diffie y Hellman.
- La criptografía de clave asimétrica usa dos claves para cifrar y descifrar.
- Una clave es pública. La otra clave es privada.
- Lo que cifra una clave lo descifra la otra
- Mecanismo de cifrado usando las claves públicas de los interlocutores

Descripción

Características

- Es necesario custodiar bien mis claves privadas.
- Los descuidos de los demás no nos obligan a cambiar nuestras claves.
- Mayor longitud de clave (1024 bits frente a 128 bits)
- Cada usuario tiene una pareja de claves.
- Algoritmos más lentos, aunque se puede combinar la cripografía simétrica con la asimétrica para paliar este problema.

Descripción

Características

- Es necesario custodiar bien mis claves privadas.
- Los descuidos de los demás no nos obligan a cambiar nuestras claves.
- Mayor longitud de clave (1024 bits frente a 128 bits)
- Cada usuario tiene una pareja de claves.
- Algoritmos más lentos, aunque se puede combinar la cripografía simétrica con la asimétrica para paliar este problema.

Descripción

Características

- Es necesario custodiar bien mis claves privadas.
- Los descuidos de los demás no nos obligan a cambiar nuestras claves.
- Mayor longitud de clave (1024 bits frente a 128 bits)
- Cada usuario tiene una pareja de claves.
- Algoritmos más lentos, aunque se puede combinar la cripografía simétrica con la asimétrica para paliar este problema.

Descripción

Características

- Es necesario custodiar bien mis claves privadas.
- Los descuidos de los demás no nos obligan a cambiar nuestras claves.
- Mayor longitud de clave (1024 bits frente a 128 bits)
- Cada usuario tiene una pareja de claves.
- Algoritmos más lentos, aunque se puede combinar la cripografía simétrica con la asimétrica para paliar este problema.

Descripción

Características

- Es necesario custodiar bien mis claves privadas.
- Los descuidos de los demás no nos obligan a cambiar nuestras claves.
- Mayor longitud de clave (1024 bits frente a 128 bits)
- Cada usuario tiene una pareja de claves.
- Algoritmos más lentos, aunque se puede combinar la cripografía simétrica con la asimétrica para paliar este problema.

Concepto de HASH

El hash o función resumen es una **huella digital** de un documento. Al pasar un documento por una función de hash, se genera un resumen de un número determinado de bits, dependiendo del algoritmo usado, íntimamente relacionado con el documento, de tal manera que una mínima alteración del documento produce una gran alteración en el hash.

Firma electrónica con criptografía asimétrica

¿Podríamos implementar un sistema de firma electrónica?

- Si, se facilita mucho la firma electrónica.
- Mecanismo de firma mediante el hash y la clave privada

Dos tipos de algoritmos

Cifrado y hash

En criptografía asimétrica se usan dos tipos de algoritmos dependiendo de lo que queramos hacer: hay algoritmos para el mecanismo de cifrado-firma y hay algoritmos para obtener el hash o resumen de un documento.

Algoritmos usados en criptografía asimétrica

Algoritmos de cifrado

- RSA
- ElGamal
- DSA

Algoritmos de hash

- SHA
- MD5

RSA

Algoritmo RSA

- Desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman.
- Claves obtenidas por producto de números primos muy grandes.
- El algoritmo sería roto si hubiera un mecanismo de factorización de números muy grandes.

RSA

Funcionamiento RSA

- Llamamos e a la clave pública
- Llamamos d a la clave privada
- Llamamos M al mensaje en claro
- Llamamos C al mensaje cifrado

Entonces, para cifrar usamos la expresión siguiente:

$C = M^e \bmod n$

y desciframos usando:

$M = C^d \bmod n$

ElGamal

Algoritmo ElGamal

Es similar al RSA, aunque se basa en el problema de los logaritmos discretos. fué desarrollado en 1986. En un principio se pensó para realizar firma electrónica, pero fué posteriormente ampliado para realizar cifrados.

DSA

ALgoritmo DSA

El algoritmo DSA (Digital Signature Algorithm) es una variante de ElGamal desarrollada en 1991 y fué diseñado dentro del estándar DSS, Digital Signature Standar. Requiere mucho tiempo de cómputo y está diseñado únicamente para realizar firmas.

SHA

Algoritmo SHA

Algoritmo de *hash*, diseñado por la NSA para ser incluido en el estándar DSS, al igual que el algoritmo DSA. En su versión original produce resúmenes de 160 bits a partir de bloques de 512 bits del mensaje original. Versiones posteriores cambian esos valores para producir resúmenes de más bits.

MD5

Algoritmo MD5

MD5 es un algoritmo de generación de resúmenes muy usado. Es un desarrollo de un protocolo anterior (MD4) procedente de la *factoria* RSA. Produce resúmenes de 128 bits a partir de bloques de 512 bits del mensaje original.

Parte II

Segunda parte: certificados y firma en España

Contenido

Descripción

Hasta ahora tenemos...

- Un sistema criptográfico seguro con privacidad.
- Un sistema de firma electrónica.
- Una clave privada que debemos custodiar.
- Una clave pública que debemos compartir.

Descripción

¿Como compartimos las claves públicas?

- En persona mediante un CD, papel. . . no siempre es posible.
- Publicando la clave en una **página web**. ¿Nos podemos fiar?
- Mediante un CERTIFICADO DIGITAL

Descripción

Certificado Digital

- Un Certificado Digital es un documento electrónico que asocia una clave pública con la identidad de su propietario y es emitido por autoridades en las que pueden confiar los usuarios.
- Dos usuarios pueden no conocerse, pero si ambos confían en la misma autoridad de certificación pueden obtener sus claves públicas ya que hay una tercera parte que certifica que las claves pertenecen a quien dicen pertenecer.
- La autoridad certifica el documento de asociación entre clave pública e identidad de un individuo firmando dicho documento con su clave privada.

Certificados X.509

Definición

- Norma que define la estructura interna de un Certificado Digital.
- Estándar del ITU-T e ISO.
- Su origen data de 1988.
- Actualmente se usa la versión 3, publicada en 1996.

Certificados X.509

Contenido

- Versión.
- Número de serie del certificado.
- Identificador del algoritmo de firmado.
- Nombre del emisor.
- Periodo de validez.
- Nombre del sujeto.
- Información de clave pública del sujeto.
- Identificador único del emisor.
- Identificador único del sujeto.
- Extensiones.

Certificados X.509

Uso de los certificados

- Navegadores de Internet.
- Clientes de correo electrónico.
- Programas específicos.
- Se pueden importar, exportar y borrar.
- Funcionamiento transparente al usuario.

PKI

Definición

- Conjunto de herramientas que permiten cubrir el ciclo de vida de un certificado. O sea, la infraestructura (autoridades, medios...) que intervienen en la creación, distribución, revocación etc...de un certificado.
- La norma fundamental que rige el funcionamiento de la PKI en relación con los certificados es el documento de prácticas de certificación.

PKI

Definición

La PKI está compuesta por la Autoridad de Certificación y la Autoridad de Registro, que nos deben proporcionar los siguientes servicios

- Registro de claves públicas.
- Emisión de certificados.
- Revocación de certificados.
- Distribución de claves mediante su publicación en repositorios públicos.

AC

Autoridad de Certificación

- Realiza la firma de los certificados con su clave privada.
- Gestiona la lista de certificados revocados.
- Debe rodearse de las mejores medidas de seguridad.

AR

Autoridad de Registro

- Su función es la de interfaz hacia el mundo exterior.
- Recibe las solicitudes de certificados y comprueba los datos de los peticionarios.
- Idem para las solicitudes de revocación.
- Traslada los certificados y revocaciones a la AC para que los firme.

CERES

Proyecto CERES

- Diferentes administraciones públicas apuestan por Internet como vía de comunicación. Cada vez hay más servicios accesibles desde Internet.
- Para dotar de seguridad a esta nueva vía de comunicación, surge el proyecto CERES, que consiste en crear una agencia pública de certificación.
- CERES provee tanto de certificados software como de tarjetas criptográficas

Otras AC en España

Diferentes AC

- FESTE. Fundación para el estudio de la seguridad de las telecomunicaciones.
- CAMERFIRMA. Autoridad de certificación de las cámaras de comercio españolas.
- ACE, Agencia de certificación electrónica

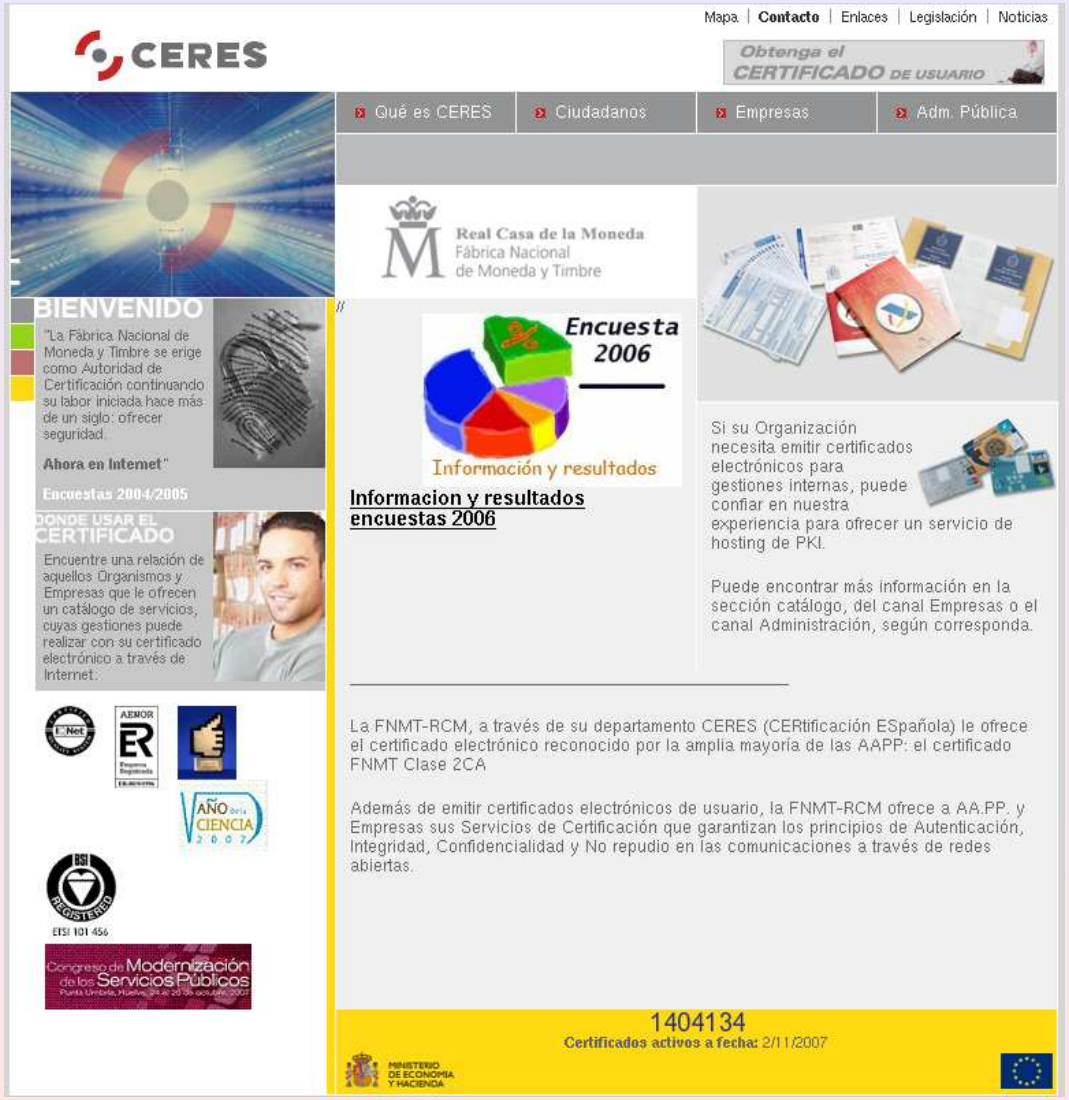
Proceso de petición de certificado

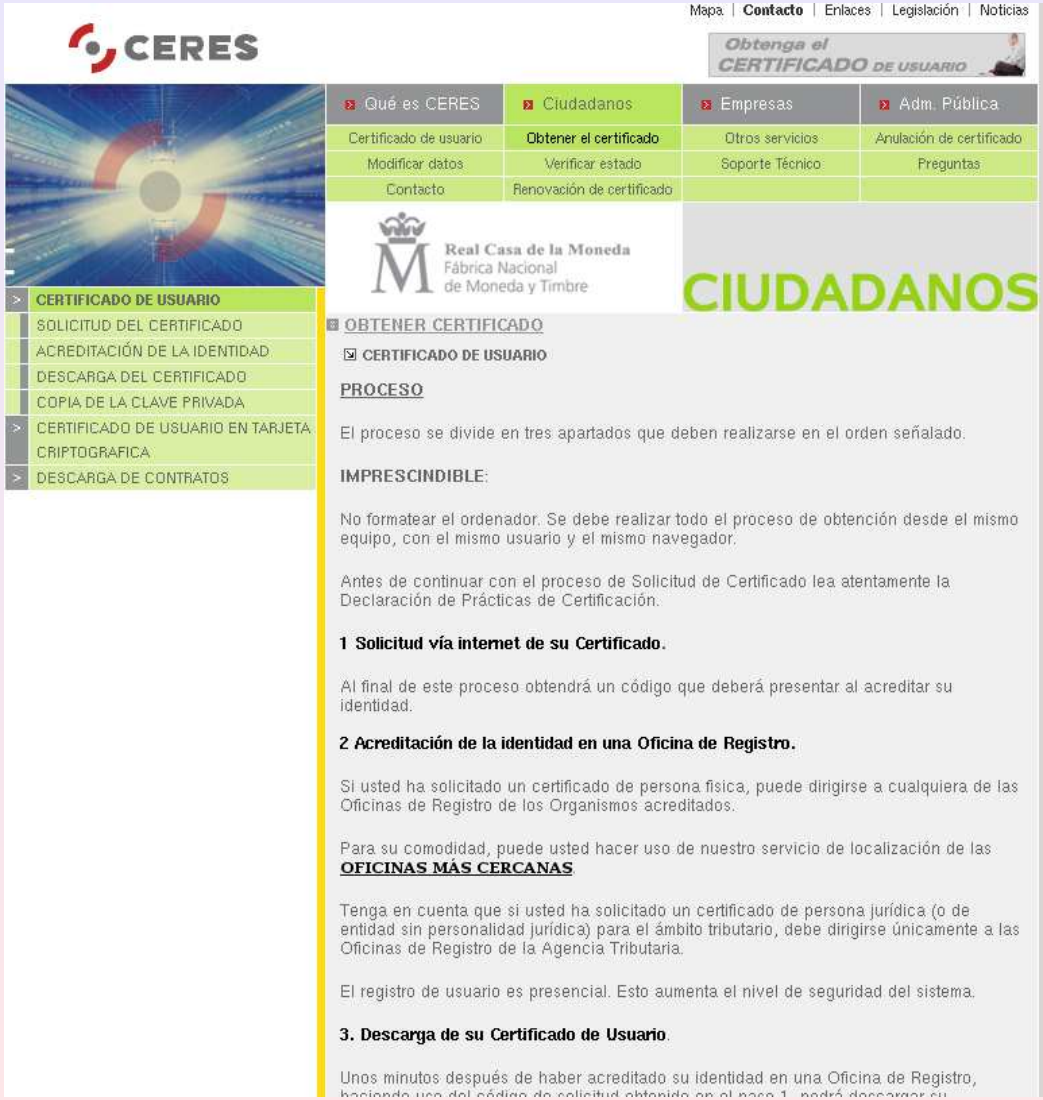
Petición

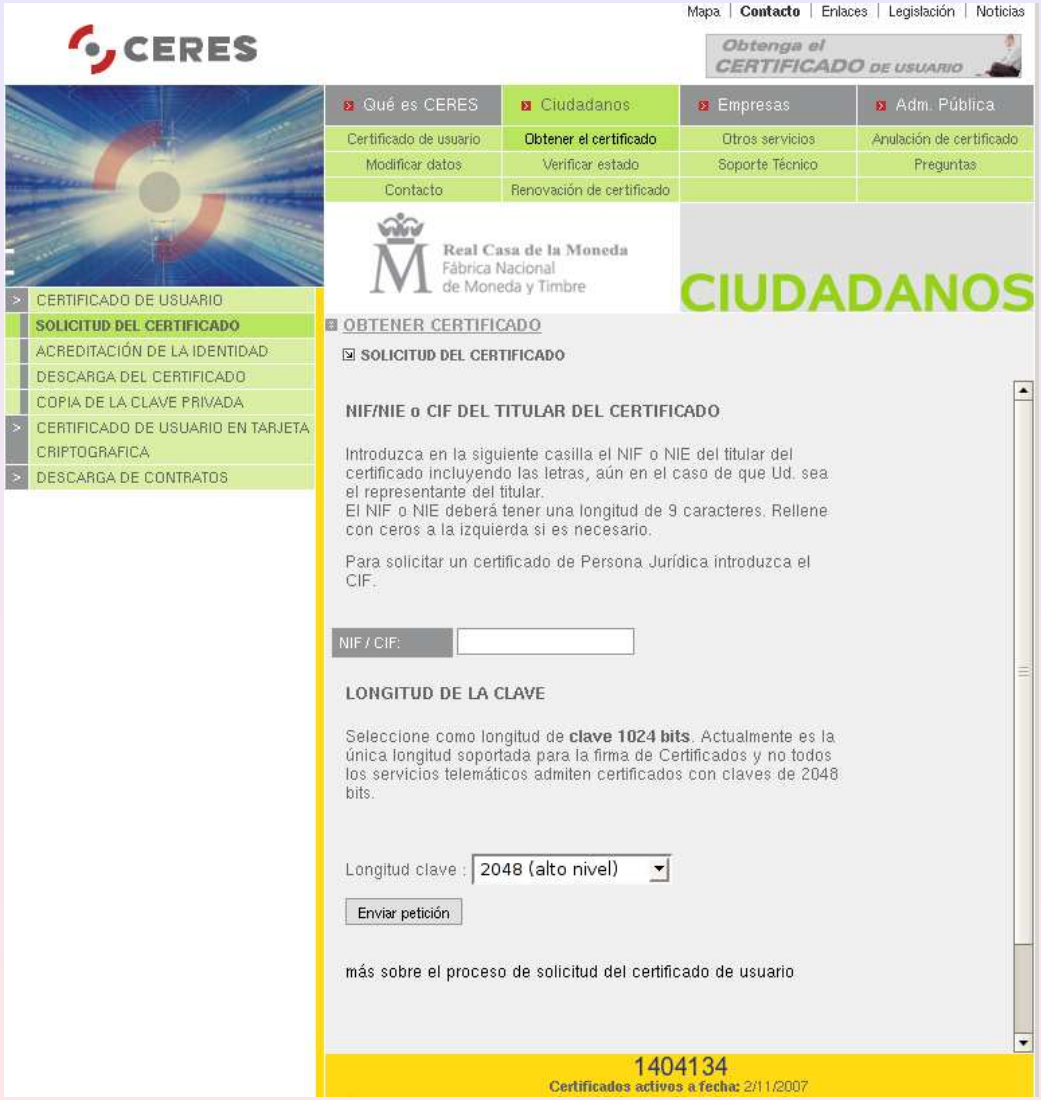
- Primero acudimos a la web de la FNMT.
- Pinchamos el enlace a CERES.
- Pinchamos en el enlace a Obtenga el certificado
- Pinchamos en solicitud del certificado.
- Rellenamos con el NIF y pinchamos en enviar petición

http://www.fnmt.es

http://www.cert.fnmt.es/




Mapa | Contacto | Enlaces | Legislación | Noticias
CERES
Obtenga el CERTIFICADO DE USUARIO
Qué es CERES
Ciudadanos
Empresas
Adm. Pública
Certificado de usuario
Obtener el certificado
Otros servicios
Anulación de certificado
Modificar datos
Verificar estado
Soporte Técnico
Preguntas
Contacto
Renovación de certificado
Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre
CIUDADANOS
CERTIFICADO DE USUARIO
SOLICITUD DEL CERTIFICADO
ACREDITACIÓN DE LA IDENTIDAD
DESCARGA DEL CERTIFICADO
COPIA DE LA CLAVE PRIVADA
CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRAFICA
DESCARGA DE CONTRATOS
OBTENER CERTIFICADO
CERTIFICADO DE USUARIO
PROCESO
El proceso se divide en tres apartados que deben realizarse en el orden señalado.
IMPRESCINDIBLE:
No formatear el ordenador. Se debe realizar todo el proceso de obtención desde el mismo equipo, con el mismo usuario y el mismo navegador.
Antes de continuar con el proceso de Solicitud de Certificado lea atentamente la Declaración de Prácticas de Certificación.
1 Solicitud vía internet de su Certificado.
Al final de este proceso obtendrá un código que deberá presentar al acreditar su identidad.
2 Acreditación de la identidad en una Oficina de Registro.
Si usted ha solicitado un certificado de persona física, puede dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.
Para su comodidad, puede usted hacer uso de nuestro servicio de localización de las OFICINAS MÁS CERCANAS
Tenga en cuenta que si usted ha solicitado un certificado de persona jurídica (o de entidad sin personalidad jurídica) para el ámbito tributario, debe dirigirse únicamente a las Oficinas de Registro de la Agencia Tributaria.
El registro de usuario es presencial. Esto aumenta el nivel de seguridad del sistema.
3. Descarga de su Certificado de Usuario.
Unos minutos después de haber acreditado su identidad en una Oficina de Registro,


Mapa | Contacto | Enlaces | Legislación | Noticias
CERES
Obtenga el CERTIFICADO DE USUARIO
Qué es CERES
Ciudadanos
Empresas
Adm. Pública
Certificado de usuario
Obtener el certificado
Otros servicios
Anulación de certificado
Modificar datos
Verificar estado
Soporte Técnico
Preguntas
Contacto
Renovación de certificado
Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre
CIUDADANOS
CERTIFICADO DE USUARIO
SOLICITUD DEL CERTIFICADO
ACREDITACIÓN DE LA IDENTIDAD
DESCARGA DEL CERTIFICADO
COPIA DE LA CLAVE PRIVADA
CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRAFICA
DESCARGA DE CONTRATOS
OBTENER CERTIFICADO
SOLICITUD DEL CERTIFICADO
NIF/NIE o CIF DEL TITULAR DEL CERTIFICADO
Introduzca en la siguiente casilla el NIF o NIE del titular del certificado incluyendo las letras, aún en el caso de que Ud. sea el representante del titular.
El NIF o NIE deberá tener una longitud de 9 caracteres. Rellene con ceros a la izquierda si es necesario.
Para solicitar un certificado de Persona Jurídica introduzca el CIF.
NIF / CIF:
LONGITUD DE LA CLAVE
Seleccione como longitud de clave 1024 bits. Actualmente es la única longitud soportada para la firma de Certificados y no todos los servicios telemáticos admiten certificados con claves de 2048 bits.
Longitud clave : 2048 (alto nivel)
Enviar petición
más sobre el proceso de solicitud del certificado de usuario
1404134
Certificados activos a fecha: 2/11/2007

Proceso de petición de certificado

Petición

- Se crean las claves y se envía la pública para la certificación.
- Se nos entrega un número de código que hay que conservar.
- Nos presentaremos en una oficina de registro para acreditar nuestra identidad con el DNI y el código obtenido.
- Unos dos días después ya podremos descargar el certificado usando el código anterior.
- Usar el mismo navegador y equipo con el que se hizo la petición para descargar el certificado.
- Es importante exportar el certificado y guardarlo en un CD para importarlo a otro ordenador o programa que lo necesite.

Proceso de renovación de certificado

Renovación

Si la solicitud la hacemos utilizando nuestro certificado (antes de que caduque, obviamente) el proceso será práticamente idéntico salvo que no tendremos que autentificarnos en persona. El certificado ya lo hace por nosotros.

Proceso de revocación de certificado

Revocación

La revocación anulará el certificado. Se solicita si hay sospechas de que el certificado haya sido comprometido. Se puede solicitar de tres maneras:

- Usando el certificado en la web de CERES.
- En persona en una oficina de acreditación.
- Por teléfono 902200616

Administración Central

Sitios

- Agencia Estatal de la Administración Tributaria.
- Comisión del Mercado de las Telecomunicaciones.
- Instituto de Crédito oficial.
- Instituto Nacional de Estadística.
- Ministerio de Economía
- ...

Administración Autonómica

Sitios

- Comunidad de Madrid.
- Gobierno de Canarias.
- Gobierno de Navarra.
- Gobierno de la Rioja.
- Junta de Andalucía.
- ...

Administración Local

Sitios

- Ayuntamiento de Alboraya.
- Ayuntamiento de Laredo.
- Ayuntamiento de Madrid.
- Ayuntamiento de Valencia.
- Diputación de Barcelona.
- ...

Empresas y otros

Sitios

- Asociación de Empresas en Internet.
- Consejo General del Notariado.
- Gestor de Infraestructuras S.A.
- paradores Nacionales de Turismo.
- Sociedad General de Autores y Editores.
- ...

Fin

Fin

Se acabó. . .