



# Manual de usuario

## Software Criptográfico FNMT-RCM

**Versión 1.05**



## INDICE DEL DOCUMENTO

<b>Manual de usuario .....</b>	<b>1</b>
INDICE DEL DOCUMENTO .....	2
<b>1 DESCRIPCIÓN. ....</b>	<b>4</b>
<b>2 REQUERIMIENTOS.....</b>	<b>6</b>
<b>3 TARJETAS FNMT-RCM.....</b>	<b>8</b>
3.1 Tarjeta chip SLE66CX320P .....	9
3.1.1 Características principales del chip SLE66CX320P.....	9
3.1.2 Características del Sistema Operativo FN19. ....	9
3.2 Tarjeta chip ST19XL34V2. ....	10
3.2.1 Características principales del chip ST19XL34V2.....	10
3.2.2 Características del Sistema Operativo Ceres v.2.0 .....	11
<b>4 NOCIONES BÁSICAS SOBRE CRIPTOGRAFÍA. ....</b>	<b>13</b>
4.1 Cifrado Digital.....	13
4.1.1 Criptografía de Clave Simétrica .....	14
4.1.2 Criptografía de Clave Pública.....	15
4.2 Firma Digital.....	18
4.3 Certificado Digital .....	20
4.3.1 Autoridad de Certificación .....	21
4.3.2 Certificado Digital X.509 Versión 3.....	21
<b>5 CONTENIDO DEL CD.....</b>	<b>22</b>
<b>6 INSTALACIÓN. ....</b>	<b>24</b>
<b>7 SERVICIOS OFRECIDOS POR LA FNMT-RCM.....</b>	<b>28</b>
7.1 Formatos de instalación. ....	29
7.2 Exportación de certificados digitales. ....	29
7.3 Importación de certificados digitales. ....	30
7.4 Correo seguro.....	30
7.5 Comunicación segura en navegadores de Internet.....	30
<b>8 FUNCIONES ESPECIALES.....</b>	<b>31</b>
8.1 Claves precargadas .....	31
<b>9 MÓDULOS CRIPTOGRÁFICOS.....</b>	<b>33</b>
9.1 Ceres Crypto Service Provider (CeresCSP). ....	34
9.1.1 Descripción de la librería. ....	34
9.1.2 Utilidades del CeresCSP.....	35
9.1.3 Versiones recientes. ....	36
9.2 Librería PKCS#11: pkcsv2gk.dll .....	37
9.2.1 Descripción de la librería. ....	38
9.2.2 Utilidades del PKCS#11.....	38
9.2.3 Versiones recientes. ....	39
<b>10 HERRAMIENTAS CRIPTOGRÁFICAS DE LA FNMT-RCM.....</b>	<b>40</b>
10.1 Panel de Control. ....	41
10.1.1 Desbloqueo de tarjeta. ....	42
10.1.2 Netscape.....	43
10.1.3 Generación de números aleatorios. ....	44
10.1.4 Importación de certificados. ....	45
10.1.5 Configuración del mecanismo de hash. ....	46



10.2	Desbloqueo de tarjeta. ....	47
10.3	Herramientas para gestión de certificados en Microsoft. ....	52
10.3.1	Gestión de certificados digitales mediante CERESMON. ....	53
10.3.2	Gestión de certificados digitales mediante CERESCERTSTORE. ....	55
<b>11</b>	<b>SOLICITUD Y DESCARGA DE CERTIFICADOS CLASE 2CA. ....</b>	<b>58</b>
11.1	Clase 2CA con Microsoft Internet Explorer. ....	59
11.1.1	Solicitud de certificados Clase 2CA. ....	60
11.1.2	Descarga de certificados Clase 2CA. ....	63
11.2	Clase 2CA con Netscape Navigator. ....	68
11.2.1	Solicitud de certificados Clase 2CA. ....	69
11.2.2	Descarga de certificados Clase 2CA. ....	73
<b>12</b>	<b>EXPORTACIÓN DE CERTIFICADOS. ....</b>	<b>75</b>
12.1	Exportación de certificados en Microsoft Internet Explorer. ....	75
12.2	Exportación de certificados mediante Netscape Navigator. ....	81
<b>13</b>	<b>IMPORTACIÓN DE CERTIFICADOS. ....</b>	<b>85</b>
13.1	Importación mediante Microsoft Internet Explorer. ....	85
13.2	Importación mediante CeresImportCertificate. ....	92
13.3	Importación mediante Netscape Navigator. ....	96
13.4	Importación mediante Mozilla FireFox. ....	100
13.4.1	Proceso previo: Instalación del módulo criptográfico:....	100
13.4.2	Importación de certificados en FireFox.....	103
<b>14</b>	<b>CORREO SEGURO. ....</b>	<b>109</b>
14.1	Correo seguro con Microsoft Outlook Express. ....	109
14.1.1	Añadiendo un certificado a la cuenta.....	109
14.1.2	Firma y verificación de mensajes. ....	112
14.1.3	Cifrado y descifrado de mensajes. ....	115
14.2	Correo seguro con Netscape Messenger. ....	120
14.2.1	Añadiendo un certificado a la cuenta.....	120
14.2.2	Firma y verificación de mensajes. ....	122
14.2.3	Cifrado y descifrado de mensajes. ....	125
<b>15</b>	<b>CONEXIÓN SEGURA. ....</b>	<b>129</b>
15.1	Conexión segura en Microsoft Internet Explorer. ....	129
15.2	Conexión segura en Netscape Navigator. ....	132
<b>16</b>	<b>WINDOWS LOGON .....</b>	<b>135</b>
16.1	Selección de certificado por defecto. ....	137
<b>17</b>	<b>VERSIONES DE NAVEGADORES VÁLIDAS.....</b>	<b>140</b>

# Capítulo 1



# *Descripción*



## 1 DESCRIPCIÓN.

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (**FNMT-RCM**), dentro de su departamento **CERES**, ha desarrollado un software criptográfico destinado a operar con tarjetas inteligentes y proporcionar al usuario un medio de comunicación seguro a través de la Red.

Permite el uso de los navegadores *Microsoft Internet Explorer* y *Netscape Navigator*, así como los clientes de correo *Microsoft Outlook Express*, *Outlook 2000* y *Netscape Messenger*. Todas estas aplicaciones serán capaces, utilizando el software proporcionado por la FNMT-RCM, de trabajar con certificados digitales almacenados en tarjeta inteligente, para la autenticación del usuario y el correo seguro.



---

El presente documento tiene como objetivo explicar detalladamente todo el software criptográfico desarrollado por la FNMT-RCM, su funcionalidad, la interacción con otras aplicaciones, etc. En los siguientes apartados veremos desde los requisitos para la instalación y uso del software criptográfico hasta los programas que nos permiten trabajar con la **tarjeta FNMT-RCM**.

La versión actual de este documento es la **1.04**, y fue creado el **viernes, 12 de noviembre de 2004**.

## Capítulo 2



# *Requerimientos*



## **2 REQUERIMIENTOS.**

Para el correcto funcionamiento del software criptográfico de la FNMT es necesario tener instalado alguno de los siguientes sistemas operativos:

- Windows 98 Segunda Edición
- Windows Millenium
- Windows NT 4.0 con Service Pack 6 o posterior.



- Windows 2000
- Windows XP

#### **Hardware necesario**

- Lector de tarjetas inteligentes PC/SC, junto con sus drivers
- Tarjeta inteligente FNMT-RCM

#### **Perfiles criptográficos**

- FNMT-RCM Clase 2

#### **Navegadores y Clientes de correo soportados**

- Microsoft Internet Explorer
- Microsoft Outlook Express
- Microsoft Outlook 98, 2000
- Netscape Messenger
- Netscape Navigator

## **Capítulo 3**



# *Tarjetas FNMT-RCM*



## **3 TARJETAS FNMT-RCM.**

En la actualidad la **Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda** dispone de dos chips distintos para sus tarjetas inteligentes, con su propio sistema operativo desarrollado también por la FNMT.

Las tarjetas FNMT-RCM están especialmente diseñadas para **infraestructuras de clave pública** en las que se requiere autenticación de una entidad, integridad, confidencialidad de datos y el no repudio en origen. Mantienen el material sensible criptográfico siempre interno a la tarjeta y, protegen su uso mediante control de acceso. De esta forma, se

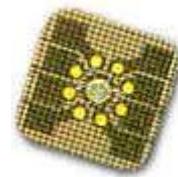


obtiene una considerable ventaja en términos de seguridad y portabilidad sobre las soluciones software.

Los dos modelos disponibles de tarjeta inteligente son el de Siemens **SLE66CX320P** y el de ST **ST19XL34**.

### 3.1 Tarjeta chip SLE66CX320P

#### 3.1.1 Características principales del chip SLE66CX320P



- **CPU** de 16 bits de alto rendimiento.
- 64 Kbytes de **ROM** para código
- 256 bytes **RAM** interna (+700 bytes) + 2 Kbytes de memoria RAM extendida
- 32 Kbytes de **EEPROM**
  - Tiempo de borrado-escritura de EEPROM de 4.5ms.
  - Retención de datos en EEPROM de un mínimo de 10 años.
- **Periféricos integrados**
  - Cripto-procesador avanzado de 1100 bits.
  - Generación real de números aleatorios.
  - Módulo de cálculo de CRCs.
  - Módulo para la transferencia asíncrona de datos.
  - Generador de frecuencia de trabajo interna.
- Características de **seguridad**
  - Cifrado dinámico de memorias y buses
  - Sensores para control de tensión y frecuencia
  - Escudo activo sensible a manipulaciones del hardware
  - Generador aleatorio de estados de espera y picos de consumo
  - Identificación única para cada chip
  - Sensor Óptico y Funciones adicionales
  - Modo de ahorro de energía.
  - Rango de frecuencia externa 1-5Mhz.
  - Frecuencia interna de hasta 10Mhz

#### 3.1.2 Características del Sistema Operativo FN19.

Los tiempos de respuesta expuestos a continuación son aproximados y han sido tomados en un entorno basado en los Componentes base de Microsoft.

- **32 Kbytes de EEPROM** disponibles para aplicaciones, de los cuales 16 Kbytes pueden ser usados para extender la funcionalidad del S.O.
- **Adecuación a la norma ISO 7816-1/-2/-3.** Protocolo de transmisión T=0 certificado por el Laboratori General D'Assaigs I Investigacions de Barcelona.
- **Almacenamiento seguro de datos sensibles:**
  - Claves RSA 1024 bits de firma y confidencialidad.

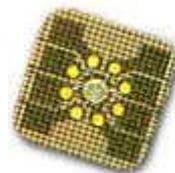


- Carga externa de claves RSA en claro o cifradas (inactivas).
- Claves Triple DES.
- Códigos secretos de usuario (PIN).
- Claves secretas de usuario para autenticación.
- Claves de aplicación.
- **Servicios criptográficos.**
  - Algoritmo de hash SHA-1 (230 ms). Posibilidad de realizarlo completo dentro de la tarjeta o sólo el último bucle, para ganar velocidad. Configurable según personalización.
  - Firmas digitales RSA de 1024 bits de tamaño de clave (511 ms). Posibilidad de realizar el relleno PKCS#1 dentro o fuera de la tarjeta, según personalización.
  - Intercambio de claves de sesión o simétricas entre dos entidades (511 ms) basado en RSA de 1024 bits.
  - Cifrado simétrico Triple DES (481 ms).
  - Generación de claves RSA de 1024 bits según el estándar PKCS#1.
  - Mecanismo propietario de activación de claves RSA.
- **Servicios de autenticación.**
  - Interna o de la tarjeta por la aplicación, RSA.
  - De usuario ante la tarjeta, con claves de aplicación.
  - De la aplicación ante la tarjeta, RSA o por claves de aplicación.
  - Entre entidades remotas. Protocolos one-way y two-way.
- **Control de acceso definible para cada fichero.**
- **Securización de comandos por criptograma.** Destinados a garantizar la integridad del comando y su autenticidad.
- Estructura interna de ficheros según el **estándar PKCS#15**.



### 3.2 Tarjeta chip ST19XL34V2.

#### 3.2.1 Características principales del chip ST19XL34V2.



- **CPU** de 8 bits avanzado con modos extendidos de direccionamiento.
- 96 Kbytes de **ROM** para código organizable en particiones.
- 4 Kbytes de **RAM** organizable en particiones.
- 34 Kbytes de **EEPROM**
  - Zona de seguridad de tipo PROM
  - Borrado/escritura hasta 64 bytes de EEPROM en 2ms.
  - Retención de datos en EEPROM de un mínimo de 10 años.



- 500.000 ciclos de borrado/escritura garantizados.
- Organización basada en particiones.
- Cripto-procesador hardware avanzado de 1088 bits.
  - Exponenciaciones y multiplicaciones modulares basadas en el método Montgomery.
  - Librería criptográfica implementada en firmware.
  - Operadores de hasta 2176 bits.
- Acelerador hardware con medidas de seguridad avanzadas para el cálculo de **Triple Des**.
- Firewalls de seguridad entre particiones de memoria; permite especificar restricciones de acceso entre las diferentes áreas.
- Reloj interno asíncrono de hasta 10Mhz.
- 2 generadores internos de números impredecibles.
- 3 timers de 8 bits.
- Módulo para la transferencia asíncrona de datos.
- Tensión de alimentación de 3 y 5 voltios.
- Módulo para el cálculo de CRC iso 3309.
- Características de seguridad
  - Identificación única para cada chip
  - Características adicionales de seguridad de última generación
- Funciones adicionales
  - Modo Standby de ahorro de energía
  - Rango de frecuencia externa 1-10Mhz.
  - Tensión de trabajo entre 2.7 y 5.5 voltios.
- Certificación de seguridad **Common Criteria EAL 4 +**.
  - Certificación a fecha de 3-10-2002 de los primeros productos de la familia ST19.
  - La certificación incluye tanto el hardware como las librerías criptográficas RSA y DES.

### 3.2.2 Características del Sistema Operativo Ceres v.2.0

- 32 Kbytes de **EEPROM** disponibles para aplicaciones.
- Adecuación a la norma **ISO 7816-1/2/3**. Protocolo de transmisión T=0. Certificación por el Laboratori General D'Assaigs I Investigacions de Barcelona (LGAI) previsto para los primeros chips.
- Interfaz de comandos según **ISO 7816-4 y PC/SC**.
- Control de acceso a datos sensibles
  - Definible para cada fichero.
  - Clave administrativa para las operaciones de escritura/lectura de datos, creación de ficheros y almacenamiento de claves.



- Control de acceso de tipo ‘Only-Once’; obliga a que la condición de acceso sea satisfecha justamente antes de realizar la operación.
- **RSA.**
  - Soporte para claves en formato **CRT** y en formato normal (exponente privado, exponente público y módulo).
  - Soporte para componentes p y q de longitud variable
  - Se puede almacenar, generar y usar claves de cualquier longitud de hasta 2176 bits en formato CRT y de hasta 1088 bits en formato normal.
  - Test de primalidad de números primos basado en Miller-Rabin
  - Operaciones de firma digital.
  - Intercambio de claves de sesión o simétricas entre dos entidades basado en RSA.
  - Optimización de las contramedidas ante ataques de tipo SPA y DPA.
  - Claves almacenadas en ficheros independientes.
  - Condiciones de acceso independientes para cada clave.
  - Se pueden crear nuevos ficheros de clave durante la fase de vida de usuario. (P.ej. hasta 15 certificados con claves en formato normal de 1024 bits).
- Otros **servicios criptográficos**
  - Algoritmo de hash **SHA-1**
  - Cifrado simétrico **Triple DES**.
  - Dos modos de funcionamiento: Relleno de datos PKCS#1 opcional.
  - Generación de claves RSA según el estándar PKCS#1.
  - Mecanismo propietario de activación de claves RSA.
  - Posibilidad de realizar solamente la última vuelta del algoritmo hash en la tarjeta.
- **Servicios de autenticación**
  - interna de la tarjeta
  - de usuario ante la tarjeta a diferentes niveles.
  - de la aplicación ante la tarjeta a diferentes niveles.
  - entre entidades remotas
- Estructura interna de ficheros según el estándar **PKCS#15**.

## Capítulo 4



# Nociones básicas sobre criptografía



## 4 NOCIONES BÁSICAS SOBRE CRIPTOGRAFÍA.

### 4.1 Cifrado Digital

El concepto de cifrado digital es muy sencillo: dado un mensaje *en claro*, es decir, mensaje reconocible, al que se le aplique un algoritmo de cifrado, se generará como resultado un mensaje *cifrado* que sólo podrá ser descifrado por aquellos que conozcan el algoritmo utilizado y la clave que se ha empleado.



El cifrado ofrece el soporte técnico para la **confidencialidad** en la información. Esto es, tener la seguridad de que el mensaje sólo podrá ser leído por la persona a la que le fue enviado.

#### 4.1.1 Criptografía de Clave Simétrica

Un cifrado de *clave simétrica* es aquel en el que se emplea la misma clave para cifrar y descifrar el mensaje.

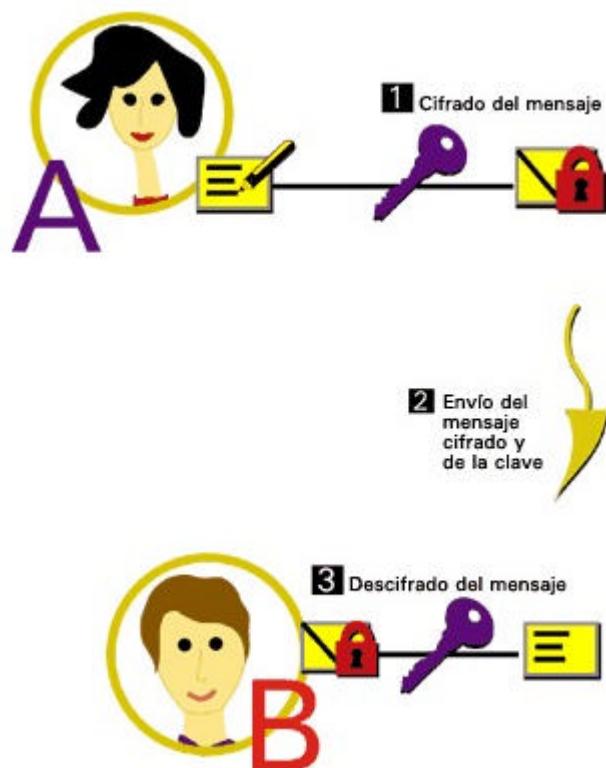


Figura 1: Cifrado simétrico.

El beneficio más importante de la criptografía de clave simétrica es su velocidad, lo cual hace que éste tipo de algoritmos sean los más apropiados para el cifrado de grandes cantidades de datos.

Los algoritmos criptográficos de clave simétrica más importantes son los siguientes:

- **DEA (Data Encryption Algorithm)** fue descrito en el Estándar de Cifrado de Datos (DES, Data Encryption Standard) como mejora del algoritmo Lucifer, desarrollado por IBM al principio de los años 70. En ocasiones, el algoritmo DEA se conoce con el nombre del estándar, DES. DEA utiliza una longitud de clave de 56 bits y un bloque cifrador de 64 bits.



- **Triple-DES**, que consiste en la aplicación de 3 operaciones de cifrado consecutivas con el cifrador de 64 bits del algoritmo DEA. Por lo tanto, se necesitan 3 claves para realizar la operación o, lo que es lo mismo, una clave de un tamaño 3 veces superior a la de DEA:  $3 \times 56 = 168$  bits.
- **AES (Advanced Encryption Standard)** es un conjunto de especificaciones que el Instituto Nacional de Estándares y Tecnología (NIST) del Gobierno de los Estados Unidos ha emitido orientadas a que expertos en criptografía desarrollen un algoritmo criptográfico de mayor calidad que DES (o la aplicación sucesiva de DES). Las especificaciones incluían el tamaño del bloque cifrador (128 bits), el tamaño mínimo de la clave (a partir de 128 bits) y un conjunto de consideraciones tales como que pudiera ser implementado utilizando cualquier elemento software o hardware. Los algoritmos propuestos a concurso han sido Rijndael, desarrollado por dos criptógrafos de nacionalidad belga, Joan Daemen y Vincent Rijmen, RC-6, desarrollado por los laboratorios RSA, MARS, desarrollado por IBM, Twofish, desarrollado por Counterpane y Serpent, desarrollado por Ross Andersen, Eli Biham y Lars Knudsen. Recientemente ha resultado ganador el algoritmo Rijndael.

#### 4.1.2 Criptografía de Clave Pública

El problema que presenta la criptografía de clave simétrica es la necesidad de distribuir la clave que se emplea para el cifrado por lo que, si alguien consigue hacerse tanto con el mensaje como con la clave utilizada, podrá descifrar el mensaje. La criptografía de clave pública está basada en que cada usuario del sistema criptográfico ha de poseer una pareja de claves: una privada, que será custodiada por su propietario y que no se la dará a conocer a ningún otro, y una pública, que será conocida por todos los usuarios.





Figura 2: Claves de un sistema de clave Pública.

La particularidad de los algoritmos de clave pública es que la operación de cifrado realizada con una de las claves sólo podrá ser descifrada por la otra y viceversa. Utilizando ésta propiedad se puede fácilmente definir un procedimiento para el cifrado de datos: con realizar un cifrado de los datos utilizando la clave pública (conocida por todos) del usuario al que se le van a enviar esos datos se tiene la certeza de que únicamente ese usuario podrá descifrarlos, ya que sólo él posee la clave privada asociada a dicha clave pública.



Figura 3: Cifrado asimétrico.

El problema fundamental de los algoritmos de clave pública es que son mucho más lentos que los de clave simétrica. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica de la siguiente forma:

- Se genera aleatoriamente una clave para el cifrado simétrico del mensaje. Dicha clave se conoce con el nombre de **clave de sesión**.



- Se realiza el cifrado del mensaje utilizando dicha clave.
- Para distribuir la clave simétrica de tal forma que se tenga la seguridad de que únicamente los usuarios para los cuales está destinado el mensaje tengan la posibilidad de conocerla, se realiza un cifrado de la clave de sesión utilizando cada una de las claves públicas de los usuarios destinatarios. De tal forma, el mensaje cifrado con la clave de sesión junto a tantas claves de sesión cifradas con sendas claves públicas es empaquetado y enviado a los usuarios finales.
- Cuando el mensaje encapsulado llega a cada uno de los destinatarios, lo único que tendrán que hacer es localizar su versión de la clave de sesión que puedan descifrar (por que esté cifrada utilizando la clave pública correspondiente), descifrarla y, con ella, descifrar el mensaje.

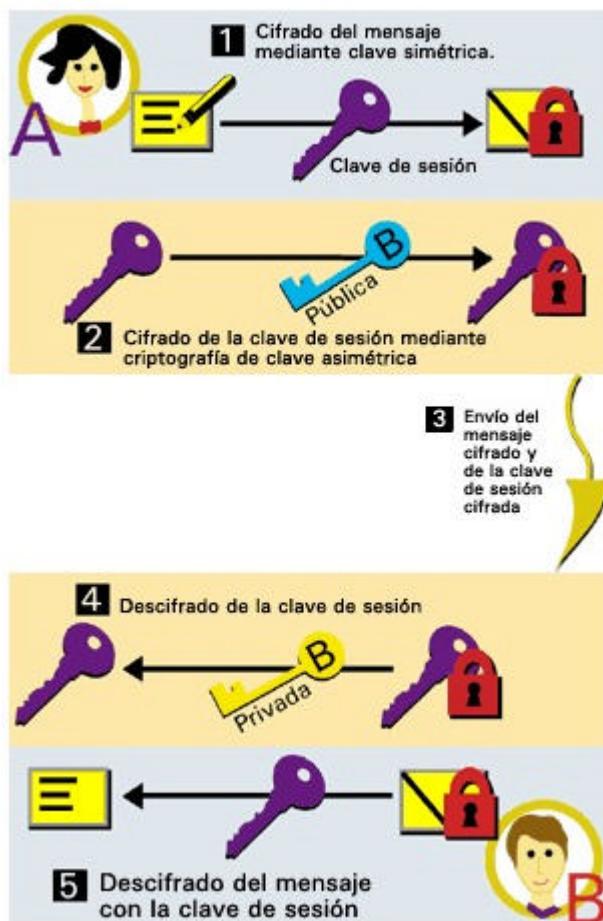


Figura 4: Cifrado con claves de sesión.

Los algoritmos criptográficos de clave pública más importantes son los siguientes:

- **RSA.** Es un algoritmo de clave pública desarrollado en 1977 que ofrece la posibilidad de realizar tanto cifrado de clave pública como firma digital de datos, descrita a continuación. Se basa en la dificultad de, dado un número resultante de multiplicar dos números primos de gran tamaño, encontrar los dos factores de los que está compuesto. Cada clave RSA está compuesta por dos



elementos: un módulo y un exponente. Cuando se habla de la longitud de una clave RSA, normalmente se está refiriendo al número de bits del módulo. Actualmente se considera que el tamaño de una clave RSA ha de ser igual o superior a 1024 bits para considerarse segura (difícil de “romper”), teniendo en cuenta que cuanto mayor sea la longitud de la clave, más difícil será romper el algoritmo, pero también será más lento.

- **DSA (Digital Signature Algorithm)** está definido en el estándar DSS (Digital Signature Standard) desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) del Gobierno de los Estados Unidos. Es un algoritmo de clave pública que se basa en el problema del logaritmo discreto y es utilizado para realizar firmas digitales y verificaciones de firmas.
- **ElGamal.** Se basa en el problema del algoritmo discreto e implementa tanto firma digital como cifrado de datos. Sin embargo, el cifrado de datos no se realiza de la misma forma que la verificación de la firma digital y el descifrado tampoco se realiza de la misma manera que la firma. El algoritmo DSA está basado en ElGamal.
- **Algoritmo de Curvas Elípticas.** Como su propio nombre indica, está basado en operaciones matemáticas definidas sobre curvas elípticas. Tiene la ventaja respecto de los otros algoritmos comentados que logra un nivel de seguridad semejante al resto, utilizando una longitud de clave menor.

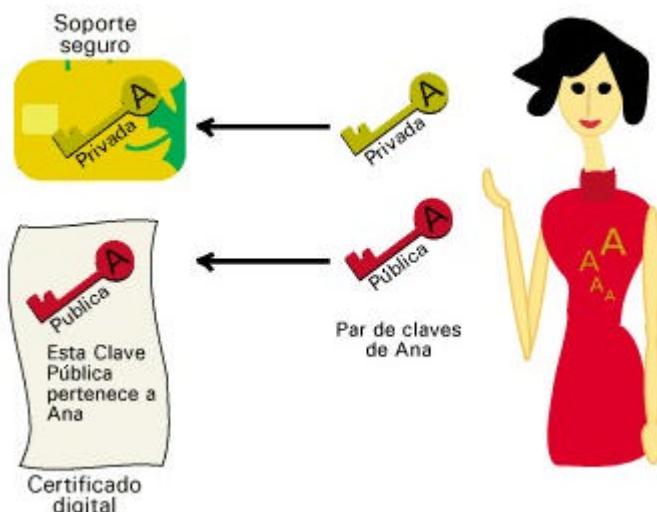


Figura 5: Soporte para claves.

## 4.2 Firma Digital

Una de las principales ventajas de la criptografía de clave pública es que ofrece un método para el desarrollo de **firmas digitales**. La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como comprobar si dicha información ha sido o no modificada desde su generación. De este modo, la firma digital ofrece el soporte para la *autenticación* e *integridad* de los datos así como para el



*no repudio* en origen, ya que el emisor de un mensaje firmado digitalmente no puede decir que no lo es.

Una firma digital está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

La firma digital se basa en la propiedad ya comentada sobre que un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

Sin embargo ya se ha comentado el principal inconveniente de los algoritmos de clave pública: su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar este problema, la firma digital hace uso de funciones *hash*. Una función hash es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado *resumen* de los datos originales, de tamaño fijo e independiente el tamaño original que, además, tiene la propiedad de estar asociado únicamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico. Los algoritmos hash más utilizados en la actualidad son **SHA-1, MD2, MD5 y RIPE**.

Por tanto, la firma digital consiste en el siguiente proceso:

- Se realiza una operación *hash* sobre los datos a cifrar obteniendo un resumen de tamaño fijo y asociado únicamente a los datos originales. Es decir, se puede concluir que, si se tiene el resumen del documento, es como si se tuviese el documento original.
- Se realiza un cifrado del resumen utilizando la clave privada del usuario que realiza la firma. Dicho resumen cifrado constituirá la firma digital del documento original:

Para realizar la verificación de una firma se utiliza el procedimiento inverso:

- Se realiza el descifrado del resumen cifrado del documento utilizando para ello la clave pública del usuario que dice haber firmado el documento, obteniendo, por tanto, el resumen de dicho documento.



- Como se conoce el documento original y se ha de conocer la función hash utilizada, el usuario que realiza la verificación de la firma generará el resumen del documento.
- Si ambos resúmenes (el realizado por el verificador y el obtenido del descifrado de la firma) coinciden, la firma digital será correcta. En caso contrario, no se puede garantizar que el documento firmado por el firmante sea el mismo que el destinatario ha recibido.

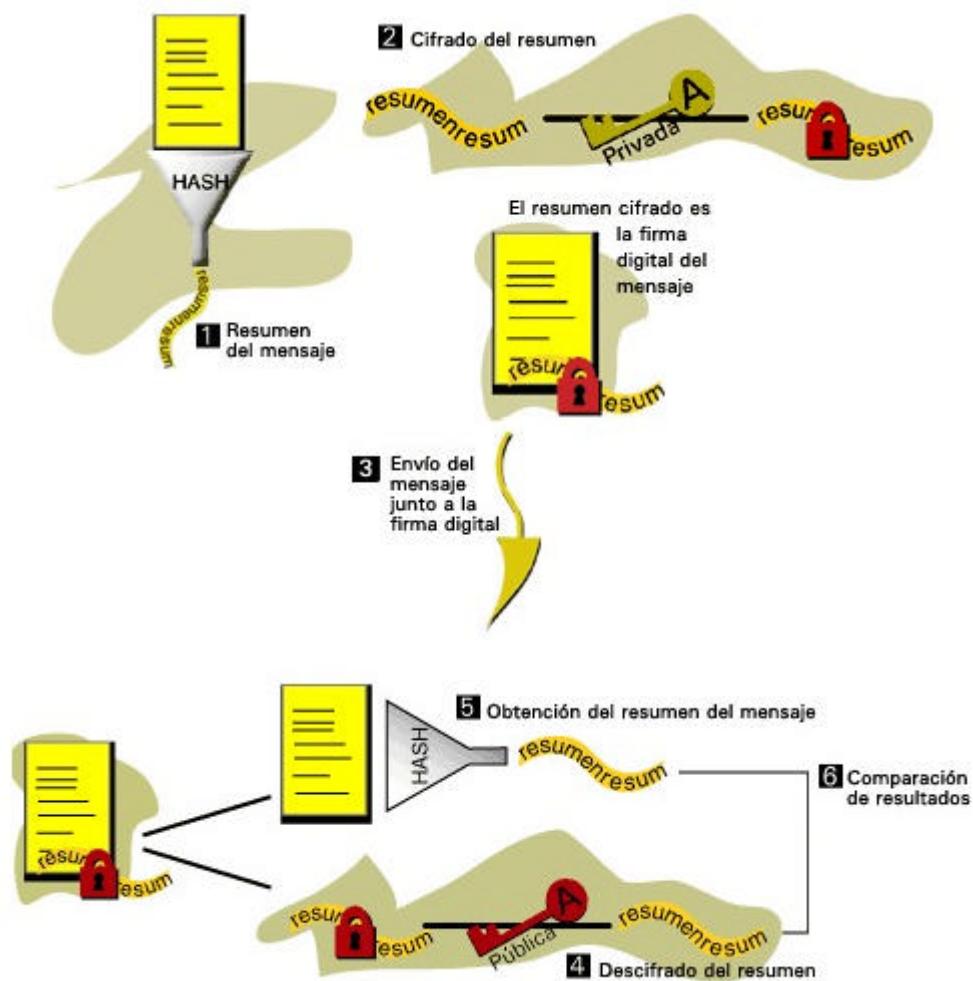


Figura 6: Esquema del proceso de firma digital.

### 4.3 Certificado Digital

Según se ha venido comentado en los apartados anteriores, la eficacia de las operaciones de cifrado y firma digital basadas en criptografía de clave pública sólo está garantizada si se tiene la certeza de que la clave privada de los usuarios sólo es conocida por dichos usuarios y que la pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios.



El mecanismo que existe de realizar una correspondencia entre una clave pública y la identidad de la entidad (persona o componente informático) titular de dicha clave pública es la emisión de **certificados digitales**. Un certificado digital es, por tanto, un documento electrónico que asocia una clave pública con la identidad de su propietario.

#### **4.3.1 Autoridad de Certificación**

La **Autoridad de Certificación (CA)** es una entidad confiable cuya responsabilidad fundamental es la emisión de los certificados digitales de los usuarios de la PKI, es decir, firmar digitalmente el documento electrónico que asocia la clave pública de cada usuario con su identidad. Opcionalmente, la CA también se encarga de la generación de las claves de los usuarios, utilizando un mecanismo aleatorio de alta calidad.

La CA es responsable del certificado durante toda su vida, no sólo en el momento de la emisión. Así, otra de las misiones de la CA será la revocación de los certificados que han dejado de estar en uso o han dejado de ser confiables.

Los elementos de una PKI que no son Autoridades de Certificación se denominan Entidades Finales (EEs, End Entities). Una Entidad Final puede ser un usuario humano, una computadora o, incluso, una aplicación software.

#### **4.3.2 Certificado Digital X.509 Versión 3**

La recomendación que indica el formato de los certificados digitales emitidos por una Autoridad de Certificación es la **X.509v3**.

Según se ha comentado en el apartado antes, un certificado digital es, básicamente, un documento electrónico que asocia una clave pública con la identidad de su propietario. En el caso concreto de los certificados X.509 v3, debido a que son emitidos por una Autoridad de Certificación, el certificado está firmado digitalmente utilizando la clave privada de la Autoridad de Certificación.



## Capítulo 5

### *Contenido del cd de instalación*



#### 5 CONTENIDO DEL CD.

En el cd suministrado por la FNMT-RCM encontramos multitud de archivos y carpetas, cuyos contenidos más destacables resumiremos a continuación.



- 📁 **Acrobat Reader.** Carpeta que contiene el programa de visualización de archivos .pdf, necesario para leer los manuales incluidos en el cd.
- 📁 **Certificados.** En esta carpeta están almacenados los certificados de la Autoridad de Certificación (CA) de la FNMT-RCM. Son necesarios para que los navegadores reconozcan como válidos los certificados emitidos por ella.
- 📁 **Cryptotool.** Herramienta para realizar operaciones criptográficas sobre ficheros.
- 📁 **Manuales.** Almacena manuales muy útiles para aprender el funcionamiento de la tarjeta FNMT-RCM.
- 📁 **Librerías tarjeta inteligente.** Aquí se encuentran todas las librerías (archivos .dll) necesarias para el funcionamiento de las tarjetas FNMT-RCM.
- 📁 **Útiles tarjeta.** Esta carpeta contiene una serie de aplicaciones útiles para la instalación y la gestión de certificados de las tarjetas FNMT-RCM.

Cuando queramos instalar el software criptográfico de la FNMT-RCM, simplemente deberemos ejecutar la aplicación ‘**Setup.exe**’, contenida en el directorio principal del cd. Esta aplicación instalará automáticamente todas las librerías, aplicaciones, documentación, etc. necesarias para el correcto funcionamiento de la tarjeta.



Figura 7: Pantalla inicial de instalación.



## Capítulo 6

### *Instalación del software*



#### 6 INSTALACIÓN.

El software criptográfico de la FNMT-RCM se suministra en un instalable que almacena en el sistema todas las librerías y las herramientas necesarias para el uso de las tarjetas FNMT-RCM.

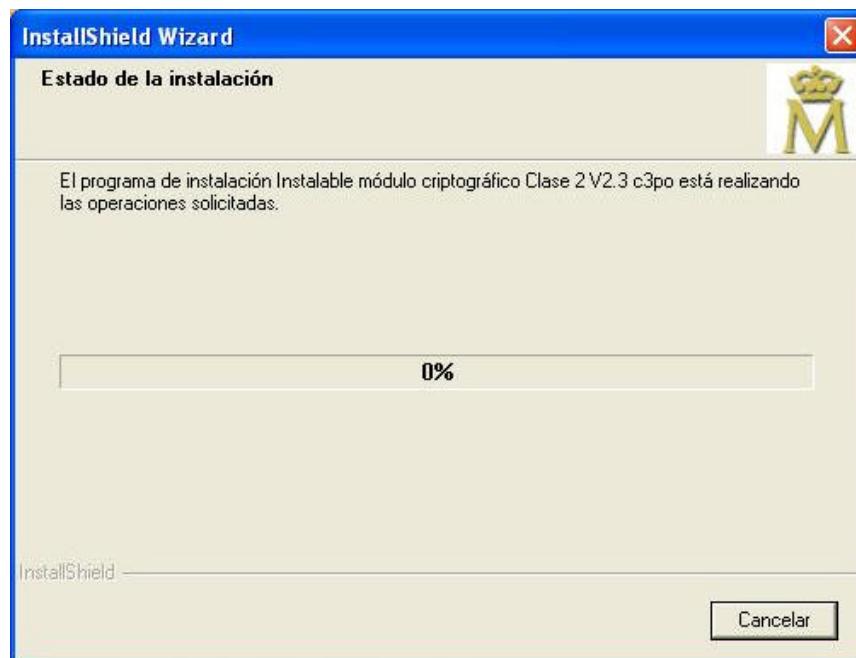


Para instalarlo simplemente debemos ejecutar la aplicación “**Setup.exe**” del cd. Esta aplicación lanzará un asistente que realizará automáticamente el proceso completo.



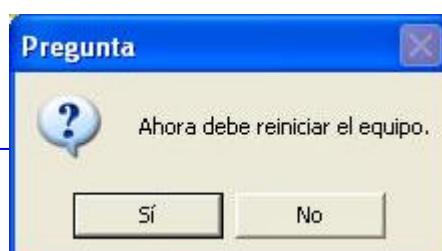
**Figura 8:** Inicio del asistente de instalación.

Una vez que ha sido preparado el asistente, comenzará automáticamente la instalación del software. El usuario no tiene que indicarle nada al asistente, ya que por defecto se utilizará para la instalación la ruta “**C:\FNMT-RCM**”. En esa carpeta quedarán instalados todos los programas necesarios, mientras que las librerías se guardarán en el directorio **Windows\System** o **Windows\System32**, según el sistema operativo que tengamos instalado en el equipo.



**Figura 9:** Progreso de la instalación.

Tras completarse la instalación del software, el asistente nos solicitará que reiniciemos la máquina para que los cambios tengan efecto.





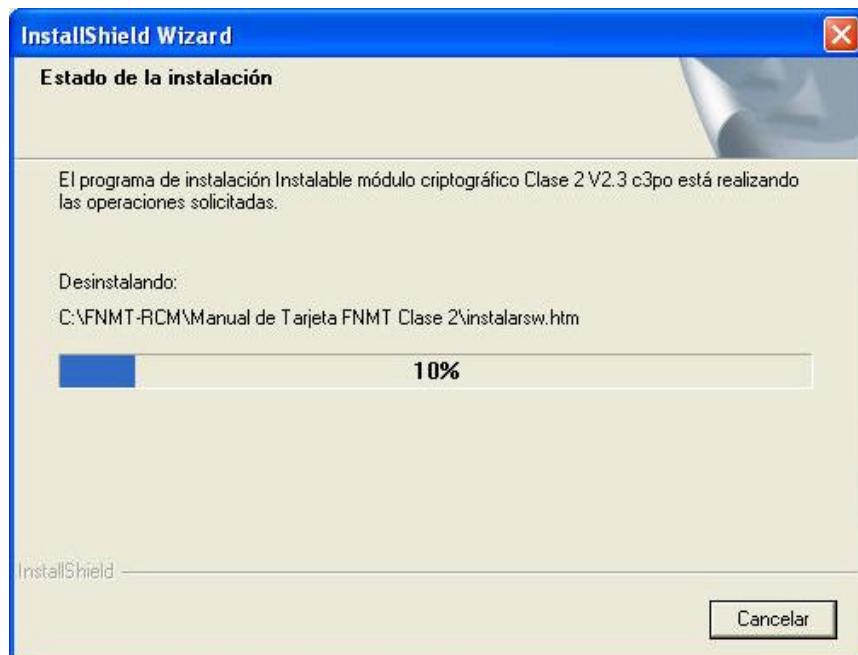
**Figura 10:** Solicitud de reinicio del sistema.

En caso de que antes de comenzar la instalación el asistente encuentre una versión previa del software, nos preguntará si queremos desinstalarla.



**Figura 11:** Detección de versión previa instalada en el sistema.

En caso afirmativo comenzará el proceso de desinstalación, que se realizará de forma totalmente automática.



**Figura 12:** Progreso de la desinstalación.

Al igual que ocurría en la instalación, tras desinstalar el software el asistente nos solicitará reiniciar el sistema.

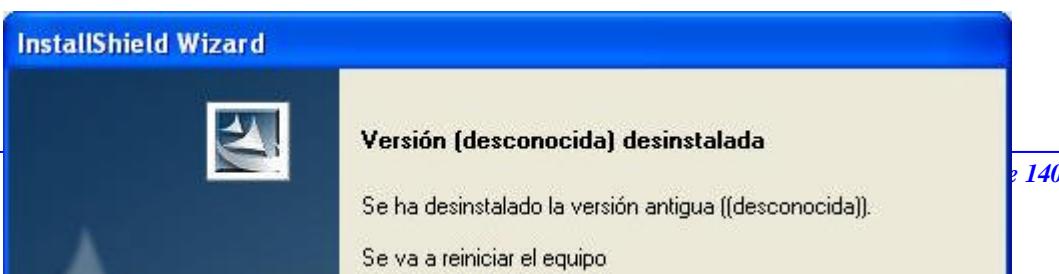




Figura 13: Solicitud de reinicio del sistema.

Cuando hayamos reiniciado la máquina podremos volver a ejecutar **setup.exe** e instalar la nueva versión del software FNMT-RCM.. Una vez instalado todo el software criptográfico, en el menú **Programas** aparecerá una nueva entrada con los enlaces al nuevo software instalado.

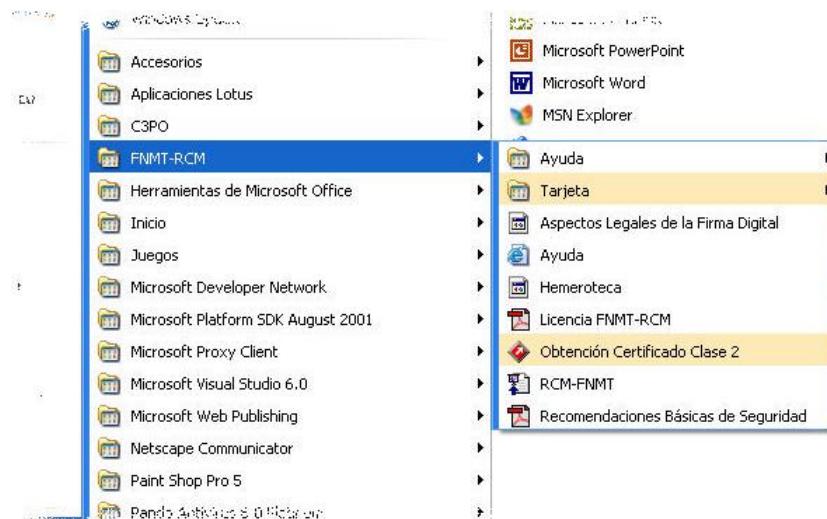


Figura 14: Entrada FNMT-RCM en “Programas”.



## Capítulo 7

### *Servicios ofrecidos por la FNMT-RCM*



#### 7 SERVICIOS OFRECIDOS POR LA FNMT-RCM.

En este capítulo vamos a comentar brevemente todos los servicios que ofrece la FNMT-RCM para sus tarjetas criptográficas. La idea es proporcionar al lector una idea general sobre los distintos servicios disponibles y su utilidad. En capítulos posteriores se



explicarán con detalle, viendo de una forma mucho más profunda su funcionamiento y su utilidad.

### 7.1 Formatos de instalación.

Debido al uso que hace CryptoAPI del sistema y al diseño de las aplicaciones y las librerías de la FNMT-RCM, el uso simultáneo de **Ceresmon.exe** y **CeresCertStore.dll** es **incompatible**.

En función de las necesidades del cliente, el software de instalación que se le suministra estará basado o bien en Ceresmon o bien en CeresCertStore, pero siempre evitando la coincidencia de ambos. En cualquier caso, una vez instalado el software el funcionamiento resultará completamente transparente para el usuario.

- **Características propias basadas en Ceresmon.** Ceresmon es una **aplicación** que corre en segundo plano comprobando si se introduce una nueva tarjeta en el lector, para así instalar en el sistema los nuevos certificados que encuentre en ella. También permite instalar el certificado en la tarjeta cuando se realiza su descarga. Estas funcionalidades también las presenta la librería CeresCertStore de una manera más eficiente, incluso. La diferencia está en que al realizar solicitudes de nuevos perfiles criptográficos con **Microsoft Internet Explorer**, Ceresmon guarda en la tarjeta los datos de esa solicitud, permitiendo que se realice la descarga en otro equipo diferente. Esto es muy útil en sistemas que vayan a utilizarse como puestos de registro de usuarios, ya que pueden ser registrados en un único ordenador pero después les permite realizar la descarga en tarjeta del certificado en cualquier otro lugar. En **Netscape** no existe esta limitación ya que todos los objetos se almacenan directamente en la tarjeta, con lo que la descarga puede realizarse en cualquier equipo.
- **Características propias basadas en CeresCertStore.** A esta **librería** sólo se accede cuando alguna aplicación basada en **CryptoAPI** quiere trabajar con los certificados instalados en el sistema. Por esta razón funciona de manera más eficiente que Ceresmon, que se ejecuta en segundo plano. Lo único que no puede realizar CeresCertStore es almacenar los datos de la solicitud en **Microsoft Internet Explorer**, con lo que la descarga deberá realizarse en el mismo equipo desde el que se pidió el certificado.

Serán los requerimientos del cliente los que marquen el tipo de instalación que se deberá realizar.

### 7.2 Exportación de certificados digitales.

Definiremos exportación como el proceso de **extraer un certificado digital a un fichero electrónico**. Esto puede interesarnos por motivos de portabilidad, por seguridad, para poderlo importar después a una tarjeta inteligente, etc. Podemos hacer



esta operación con perfiles criptográficos instalados tanto en ***Internet Explorer*** como desde ***Navigator***. El proceso varía ligeramente de uno a otro, pero el resultado en ambos casos será un fichero electrónico que contendrá el certificado digital completo.

### 7.3 Importación de certificados digitales.

Es el proceso contrario a la exportación. La importación **consiste en instalar un certificado** (que se encuentra contenido en un fichero electrónico) **en el sistema o en una tarjeta inteligente**. Las librerías *CeresCSP.dll* y *pkcsv2gk.dll* permiten realizar esta operación desde los dos navegadores de Internet, pero además existe la posibilidad de importar certificados a la tarjeta utilizando la aplicación *CeresImportCertificate.exe*. Esta aplicación permite almacenar fácilmente en una tarjeta FNMT-RCM un perfil guardado en fichero electrónico.

### 7.4 Correo seguro.

Mediante las librerías suministradas por la FNMT-RCM podremos conseguir correo seguro tanto con clientes de correo de **Microsoft** (*Outlook Express*, *Outlook 2000*, etc.), como de **Netscape** (*Messenger*). Estas librerías nos permitirán, mediante el uso de los certificados digitales de usuario, enviar y recibir correos cifrado y/o firmados digitalmente y que posteriormente podrán ser descifrados y/o verificados.

El uso de una librería u otra dependerá del cliente de correo utilizado. Los de Microsoft se basan en el uso del CryptoAPI del sistema, por lo que requieren una librería que funcione también sobre él. Para ello se creó **CeresCSP.dll**. En cambio Netscape sigue la recomendación PKCS#11, cuya implementación para la FNMT-RCM está desarrollada en la librería **pkcsv2gk.dll**.

El uso de un cliente de correo u otro es completamente compatible, permitiendo intercambiar mensajes criptográficos entre ambas aplicaciones. En otras palabras, podríamos enviar, por ejemplo, un mensaje cifrado desde *Outlook Express* y no tendríamos ningún problema para descifrarlo con *Messenger*.

### 7.5 Comunicación segura en navegadores de Internet.

Las librerías **CeresCSP.dll** y **pkcsv2gk.dll** permiten interactuar a la tarjeta FNMT-RCM con los navegadores *Microsoft Internet Explorer* y *Netscape Navigator*, respectivamente. De esta manera podremos establecer conexiones seguras con los sitios Web que lo soliciten utilizando los certificados digitales (*profiles*) almacenados en la tarjeta, solicitar y descargar nuevos perfiles criptográficos, etc.



# Capítulo 8

## *Funciones especiales*



### **8 FUNCIONES ESPECIALES.**

#### **8.1 Claves precargadas**



---

Como función especial, la tarjeta FNMT-RCM soporta la **activación de claves precargadas** en tarjeta. Mediante este proceso, el usuario recibirá un sobre con su tarjeta y una clave de activación. Esta clave es necesaria para activar las claves almacenadas en la tarjeta, ya que de otra forma no será posible trabajar con ellas.

Para realizar el proceso completo se utiliza un software especial, diseñado para tal efecto, que nos guía paso a paso solicitando el PIN de la tarjeta y el código de activación. Después se conectará con la Autoridad de Certificación y procederá a la activación de las claves.



## Capítulo 9

### *Módulos criptográficos*



#### 9 MÓDULOS CRIPTOGRÁFICOS.

Para interactuar con las tarjetas de la FNMT-RCM todas las aplicaciones necesitan utilizar ciertas librerías que implementen un interfaz de comunicación con ellas. Dicho



---

interfaz debe ser suministrado por el desarrollador e implementa las rutinas necesarias para el correcto funcionamiento de la tarjeta.

Hay dos tipos de librerías diferentes suministradas por la FNMT-RCM. Por un lado tenemos el Crypto Service Provider (**CeresCSP.dll**), que permite integrar la tarjeta en el **CryptoAPI** de Windows. Es la librería utilizada por todo el software de Microsoft (*Outlook Express, Internet Explorer, etc.*).

Por otro lado tenemos la librería que implementa el interfaz **PKCS#11**, utilizado por aplicaciones que integren esa recomendación. Entre las aplicaciones más conocidas que usarán esta librería (**pkcs12gk.dll**), están todas las de Netscape (*Navigator y Messenger*), así como la mayoría de las aplicaciones de la FNMT-RCM.

Estas librerías son completamente **compatibles** entre sí. Además, pueden trabajar simultáneamente, permitiendo tener abiertas a la vez varias aplicaciones que utilicen CryptoAPI o PKCS#11.

En los siguientes apartados comentaremos el funcionamiento, las características y las particularidades de cada una de ellas.

## 9.1 Ceres Crypto Service Provider (CeresCSP).

### 9.1.1 Descripción de la librería.



La librería **CeresCSP.dll** es el proveedor de servicios criptográficos implementado para la tarjeta FNMT-RCM. En ella están implementadas las rutinas que utilizará el CryptoAPI de Windows para realizar operaciones criptográficas sobre tarjeta inteligente. El CSP es dependiente del hardware, por lo que cada suministrador deberá proveer de dicho sistema al sistema operativo para que su tarjeta funcione adecuadamente.

CeresCSP permite a las aplicaciones basadas en CryptoAPI que usen la tarjeta inteligente FNMT-RCM realizar firmas digitales, cifrar, descifrar, etc. También proporciona los mecanismos para realizar login con tarjeta en Windows 2000 y Windows XP.

Entre las aplicaciones que utilizan el CryptoAPI de Windows se encuentran *Microsoft Internet Explorer*, *Outlook Express*, *Outlook 2000*, etc. De manera que dichas aplicaciones podrán utilizar CeresCSP para interactuar con la tarjeta. En la siguiente figura podemos ver cómo se ubica CeresCSP dentro de la arquitectura del CryptoAPI de Microsoft.

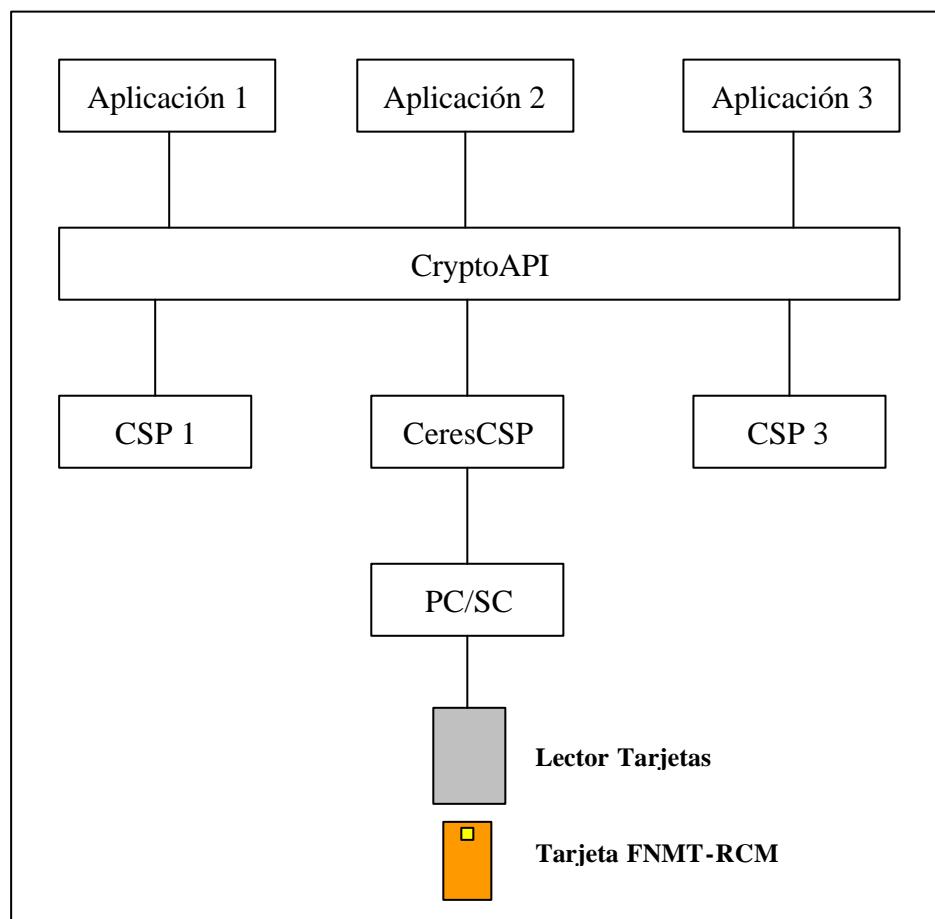


Figura 15: arquitectura de CeresCSP.dll

### 9.1.2 Utilidades del CeresCSP.

El CryptoAPI es utilizado por las aplicaciones y sistemas operativos de *Microsoft* para operar con el hardware criptográfico. A continuación comentaremos dichos usos.



- **Gestión de certificados.** La librería CeresCsp.dll nos permitirá realizar todo tipo de operaciones sobre *perfiles criptográficos* (certificados). Esto es, solicitar un nuevo perfil ([www.cert.fnmt.es](http://www.cert.fnmt.es)), descargarlo tras el proceso de registro, exportarlo a tarjeta, etc.
- **Securización de mensajes.** El correo seguro es una de las aplicaciones que más interés despierta dentro de la criptografía de clave pública. Permite intercambiar información cifrada y/o firmada entre dos usuarios, garantizando la integridad, la autenticidad del mensaje, la confidencialidad y el no repudio. Para ello es necesario que el certificado albergado en la tarjeta esté vinculado con la cuenta de correo que va a utilizar el usuario. Las aplicaciones de correo de Microsoft (*Outlook Express*, *Outlook 2000*, *Outlook 98*) soportan correo seguro utilizando CryptoAPI, por lo que también usarán la librería **CeresCSP.dll** para comunicarse con la tarjeta inteligente. Para más información, ver apartado **14.1**.
- **Autenticación del cliente.** La autenticación del cliente implica la identificación y la validación de la identidad del usuario frente a un servidor remoto, estableciendo para ello un canal de comunicaciones seguras. Este canal puede crearse mediante protocolos seguros como **Secure Socket Layer (SSL)** y requiere el uso de un certificado digital instalado en el sistema y que puede estar almacenado en hardware (*tarjeta inteligente*) o en software (*fichero electrónico*). El proceso consiste básicamente en, una vez instalado un certificado en el navegador **Internet Explorer**, intercambiar claves de sesión para establecer el canal seguro que permitirá asegurar la integridad y la confidencialidad de los datos que se envíen entre el cliente y el servidor. Para más información, ver apartado **15.1**.
- **Logon en Windows 2000 y XP.** *Windows 2000* y *Windows XP* soportan la autenticación de usuario por medio de tarjeta inteligente, reconociendo el token del lector y solicitando el PIN del usuario. Para poder realizar esta operación trabajando sobre la tarjeta FNMT-RCM es necesario el uso de la librería CeresCSP.dll.

### 9.1.3 Versiones recientes.



A lo largo de la vida de un driver, van surgiendo multitud de necesidades y optimizaciones que hacen necesarias nuevas versiones. En este apartado explicaremos algunas de esas mejoras, indicando las características que añade a la librería.

Otro concepto importante en CryptoAPI es el de **componente firmado**, que permite su ejecución en el sistema operativo. Para ello es necesario un archivo **.sig** que genera Microsoft para cada versión del CSP, previo envío de la librería. El campo ‘Fecha de recepción del archivo, firmado por Microsoft’ indica la fecha del archivo de firma para cada una de las versiones.

Versión emitida	Fecha de recepción del archivo, firmado por Microsoft	Características añadidas/ problemas resueltos.
1.3.1.4	28/03/02	<ul style="list-style-type: none"><li>• Se resuelve un problema en hash de mensajes de longitud múltiplo de la longitud de bloque.</li><li>• Se añade cuadro de diálogo para el caso de llamadas a generar claves RSA con tarjeta extraída.</li><li>• Cuando llamamos a generar claves, si no hay espacio, se elimina el último par de claves generado y que no tengan un certificado asociado.</li><li>• Solucionados detalles funcionamiento en algoritmos RC2 y RC4.</li><li>• Modificada la derivación de claves triple DES.</li><li>• Modificados los Key Usage.</li></ul>
1.4.2.1	08/06/02	<ul style="list-style-type: none"><li>• Se añade un cuadro informativo durante la generación de claves RSA.</li><li>• Modificado un Key Usage.</li><li>• Se modifica la gestión de la FAT pkcs#15 para hacerla con los mismos componentes que el driver pkcs#11.</li><li>• Cambiamos el icono de CERES.</li><li>• Se pasa a usar la misma política de ID de claves RSA que en pkcs#11.</li><li>• Se mejora la multitarea y multiproceso.</li><li>• Se añade una caché de PIN, limitada por tiempo de inactividad.</li></ul>
1.4.3.0	06/12/02	Primera compatibilidad con tarjeta sobre chip de Infineon codificado FN20.
1.4.3.1	15/01/03	Se evita que la tarjeta pierda la coherencia entre la información almacenada en la FAT pkcs#15, y el contenido de los ficheros criptográficos, en caso de haber algún problema durante la generación de claves RSA.

## 9.2 Librería PKCS#11: pkcsv2gk.dll



### 9.2.1 Descripción de la librería.

Esta recomendación del PKCS#11 de los laboratorios RSA (versión 2.01) establece un interfaz de comunicación con un *token* criptográfico (tarjeta inteligente) que almacene claves y permita la ejecución de operaciones criptográficas.

Al contrario de lo que ocurría con las aplicaciones de Microsoft, que disponen de su propio API, entre las aplicaciones que integran PKCS#11 se encuentran todas las de Netscape (*Navigator*, *Messenger*). Para el correcto funcionamiento de la tarjeta FNMT-RCM, se ha implementado la librería **pkcsv2gk.dll**, que funcionará como interfaz entre las aplicaciones que requieran PKCS#11 y la tarjeta.

En la siguiente figura podremos comprobar el esquema de uso de las librerías PKCS#11.

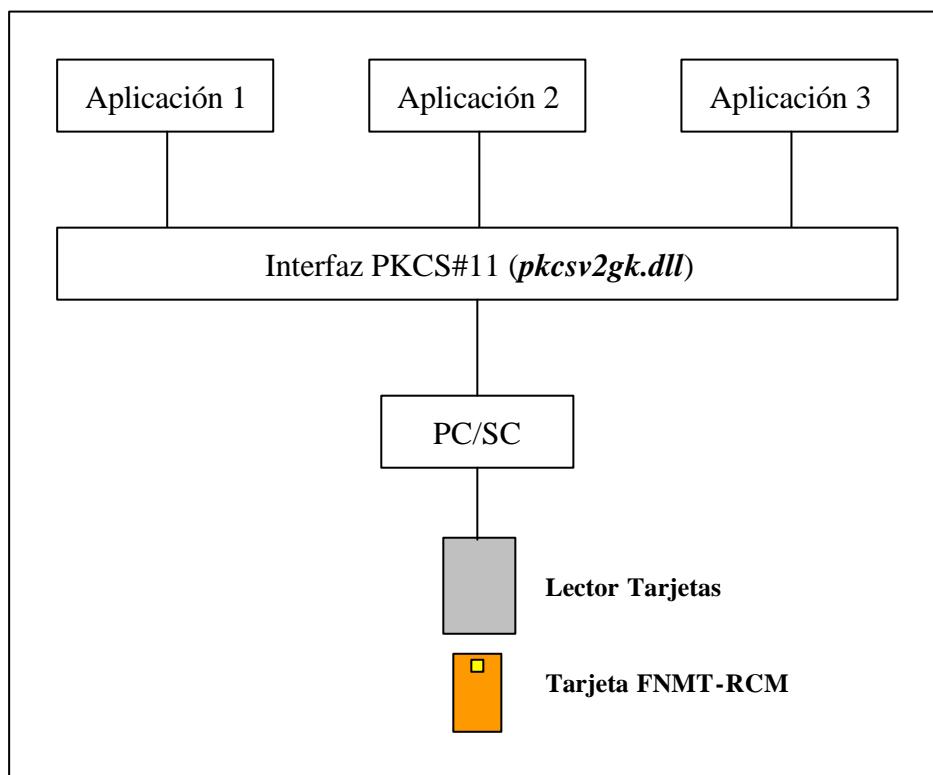


Figura 16: arquitectura de *pkcsv2gk.dll*

### 9.2.2 Utilidades del PKCS#11.



La librería PKCS#11 implementada por la FNMT-RCM proporciona más o menos los mismos servicios que la librería CryptoAPI aunque en otras aplicaciones y de una manera algo diferente. Lo que no es posible realizar mediante PKCS#11 es el Logon en *Windows 2000* y *Windows XP*. Esto es debido a que, como dijimos anteriormente, el sistema operativo utilizará CryptoAPI para comunicarse con la tarjeta y para ello se requiere un proveedor de servicios criptográficos adecuado para el hardware que se va a utilizar. En nuestro caso el sistema operativo utilizará CeresCSP.dll.

En líneas generales comentaremos que los servicios que podemos obtener de la librería **pkcsv2gk.dll** son básicamente estos:

- **Gestión de certificados.** Un uso fundamental de la librería PKCS#11 será toda la gestión de perfiles criptográficos y las operaciones relativas a ellos (solicitud, descarga, destrucción, importación, etc.).
- **Correo seguro.** Al igual que ocurría con el Csp, la librería PKCS#11 establece un interfaz de comunicación con la tarjeta que nos permitirá realizar operaciones criptográficas destinadas al cifrado y/o firmado de mensajes así como su descifrado y/o verificación. Entre las aplicaciones que utilizan PKCS#11 está el cliente de correo de Netscape, **Messenger**. Este cliente permite utilizar un certificado almacenado en la tarjeta para realizar operaciones criptográficas sobre los mensajes. Es necesario, como en el caso del CryptoAPI, que el certificado esté asociado a la cuenta del usuario. Para más información, ver apartado **14.2**.
- **Autenticación de cliente.** PKCS#11 también permite establecer un canal de comunicación seguro mediante protocolos especiales, tales como **SSL** (ver apartado **15.2**). Ahora el navegador en el que trabajaremos será **Netscape Navigator**. Cuando el cliente se conecte con un servidor seguro, el navegador mostrará un cuadro de diálogo en el que permitirá seleccionar el certificado que queremos usar para la conexión. Aquí no es necesario que esté instalado, sino que bastará con tener la tarjeta dentro del lector. Será el navegador el encargado de comprobar su contenido y mostrar los certificados disponibles en ese momento, tanto en la tarjeta como en la base de datos de Netscape.

### 9.2.3 Versiones recientes.

Las versiones más recientes de la librería **pkcsv2gk.dll** son las siguientes:

- **Versión 2.0.1.3.**
- **Versión 2.0.1.4.** Permite la gestión de datos administrativos.
- **Versión 2.0.1.5.** Lectura de información del *token*.
- **Versión 3.0.0.1.** Soporte para tarjetas **SLE66CX320P** y **ST19XL34v2**.



## Capítulo 10

### *Herramientas criptográficas de la FNMT-RCM*



#### **10 HERRAMIENTAS CRIPTOGRÁFICAS DE LA FNMT-RCM.**



---

En los siguientes apartados vamos a describir cada una de las herramientas proporcionadas por la FNMT-RCM para el uso de la tarjeta inteligente. Cada una de ellas tiene una función concreta y deber usarse en un momento determinado.

Estas herramientas son:

- Gestor de aplicaciones FNMT-RCM
  - Desbloqueo de tarjeta
  - Instalación módulo criptográfico PKCS#11
  - Generación de números aleatorios
  - Importación de certificados
  - Configuración del algoritmo de hash
- Desbloqueo de tarjetas
- Herramientas para gestión de certificados en Microsoft
  - Ceresmon.exe
  - CeresCertStore.dll

## **10.1 Panel de Control.**



Dentro del panel de control de Windows encontraremos el **Gestor de aplicaciones** de la FNMT-RCM. Dicha aplicación permite configurar determinados parámetros de las librerías criptográficas y lanzar ciertas aplicaciones, útiles para el correcto funcionamiento de la tarjeta.



**Figura 17:** Icono del Gestor de aplicaciones FNMT-RCM

En la figura 3, perteneciente al Panel de Control de Windows, vemos el ícono de “**Aplicaciones FNMT-RCM**”. La idea es centralizar todas las aplicaciones en un único lugar desde el que poder lanzarlas, acceder a la ayuda necesaria, configurar el funcionamiento de la tarjeta, etc.

En los siguientes apartados mostraremos cada una de esas funcionalidades, comentando su utilidad y explicando las razones de su existencia.

#### 10.1.1 Desbloqueo de tarjeta.



Esta página nos permite lanzar la aplicación de desbloqueo de tarjeta. Cuando queremos autenticarnos contra una tarjeta inteligente debemos presentar su *número de identificación personal (PIN)*. Si errásemos ese PIN un determinado número de veces, la tarjeta quedaría bloqueada y no podría operarse con ella. Para volver a recuperar su funcionalidad, la tarjeta debe ser desbloqueada introduciendo un código especial destinado a tal efecto. En la figura siguiente podemos ver esta página.



Figura 18: Página de desbloqueo de tarjeta.

Al pulsar el botón se lanzará la aplicación correspondiente, que nos solicitará el código de desbloqueo de la tarjeta. Es importante tener especial cuidado al introducir dicho código porque, al igual que ocurre con el PIN, si introducimos tres veces el código incorrectamente, quedaría bloqueado y la tarjeta entonces sería imposible de recuperar.

#### 10.1.2 Netscape.



Esta página del gestor de aplicaciones permite instalar el módulo criptográfico **pkcs12gk.dll** en el navegador Netscape Navigator. Esta operación consiste en indicarle a dicha aplicación la ruta y la librería que debe utilizar para poder usar la tarjeta inteligente FNMT-RCM. Una vez finalizado aparecerá un mensaje en la pantalla que nos dirá si la instalación se ha llevado a cabo correctamente o si ha ocurrido algún error.

Este es el aspecto de la página de Netscape.



**Figura 19:** Página de instalación módulo Netscape.

Para lanzar la aplicación **Netscape Navigator** se usará por defecto la ruta desde **Archivos de Programa/Netscape**. En caso de que no se encuentre, aparecerá en pantalla una ventana de selección de directorios, desde la cual indicaremos la ruta actual del software.

#### 10.1.3 Generación de números aleatorios.



Sabido es que para el establecimiento de una conexión segura es necesario el intercambio de claves de sesión entre cliente y servidor. La manera de hacerlo es solicitando al cliente un **desafío** (número aleatorio) que se usará después para construir, junto con la clave pública del perfil, la clave sesión. Ese **desafío** puede generarse de dos maneras. O bien lo genera una aplicación vía software, o bien se crea en la tarjeta de manera interna.

La tarjeta FNMT-RCM permite generar números aleatorios internamente. Esta funcionalidad es una operación mucho más costosa en tiempo de lo que supone generarlos por software. Hay algunas aplicaciones que necesitan generar gran cantidad de números aleatorios, por lo que el factor tiempo puede resultar crítico y no sería operativo generarlos internamente. En cambio puede que por cuestiones de seguridad y en caso de no tener que generar gran cantidad de números, prefiramos hacerlo de forma interna. Dado que existen esas dos posibilidades y que el modo utilizado vendrá definido por los requisitos del usuario, se creó una página dentro del gestor de aplicaciones que permitiera elegir el tipo de generación de números aleatorios que queremos utilizar.



Figura 20: Página de generación de números aleatorios.

Los cambios que hagamos en el panel de control sólo afectarán a aquellas aplicaciones que utilicen PKCS#11 (pkcsv2gk.dll), pero no a las de CryptoAPI (CeresCSP.dll).

#### 10.1.4 Importación de certificados.



Los certificados digitales pueden estar almacenados en *hardware* (tarjeta inteligente) o en *software* (fichero electrónico). En caso de que tengamos un certificado software descargado con *Netscape Navigator*, desde esa misma aplicación y simplemente con la librería **pkcs12.dll** podremos importarlo a la tarjeta. Pero si el certificado fue descargado con Microsoft Internet Explorer no es tan directo. Una de las maneras más sencillas que tenemos de realizar esta importación desde fichero hacia la tarjeta FNMT-RCM es mediante la aplicación a la accedemos desde esta página: [CeresImportCertificate](#).

Más adelante (apartado 13.2) explicaremos con detalle cada una de estas aplicaciones, pero por el momento sólo comentaremos el gestor de aplicaciones y las funcionalidades que nos ofrece. En apartados posteriores veremos el resto del software.

La página que nos muestra el gestor de aplicaciones es la de la siguiente figura.



Figura 21: Página de importación de certificados.

#### 10.1.5 Configuración del mecanismo de hash.



Al igual que ocurría con la generación de números aleatorios, que podía realizarse por *software* o *hardware* (en el interior de la propia tarjeta), la obtención del *hash SHA-1* para la firma digital con la tarjeta FNMT-RCM soporta también esas dos posibilidades.

Realizar la operación de *hash* (resumen) dentro de la tarjeta supone, como en la generación de números aleatorios, un incremento de la seguridad pero también un aumento del tiempo de ejecución. Habrá casos en los que dicho aumento no sea crítico, pero en determinadas situaciones en las que sea necesario realizar un gran número de resúmenes puede ser preferible hacerlo por software.

En la siguiente figura podemos observar la página del gestor de aplicaciones desde la que podemos configurar la generación software o hardware del hash, habilitando o deshabilitando el mecanismo de generación en tarjeta.



Figura 22: Página de configuración del hash.

Seleccionando ‘**Mecanismo inactivo**’ le indicaremos al driver PKCS#11 que **inhibile** el mecanismo **CKM\_SHA1\_RSA\_PKCS**, que permite realizar firmas y verificaciones. En cambio, si seleccionamos ‘**Mecanismo activo**’ sí será soportado por la tarjeta, realizando la firma y la verificación de manera interna.

## 10.2 Desbloqueo de tarjeta.



La tarjeta FNMT-RCM requiere para su uso la presentación del número de identificación personal (PIN), que debe ser conocido sólo por su poseedor. Presentando ese PIN se puede acceder a las funciones de firma, descifrado, etc. Este mecanismo de seguridad permite evitar que alguien pueda utilizar nuestra tarjeta para realizar operaciones en nuestro nombre.

Puede ocurrir que cuando una aplicación nos solicite nuestro PIN, nos equivoquemos al introducirlo. En ese caso se nos dará un nuevo intento. Si fallásemos tres veces al insertar el PIN la tarjeta quedaría **bloqueada**, no permitiéndonos realizar ninguna operación. Para recuperar su funcionalidad será necesario desbloquear el PIN, utilizando para ello el código de desbloqueo de la tarjeta.

La aplicación que vamos a comentar a continuación es un asistente que nos permitirá, de una manera rápida y sencilla, desbloquear el código PIN de nuestra tarjeta inteligente. Vamos a explicar paso a paso el proceso.

En primer lugar nos aparecerá una ventana en la que nos informan de la aplicación que vamos a utilizar y su uso.



Figura 23: Desbloqueo de tarjeta. Pantalla 1.

El código de desbloqueo de la tarjeta se incluye en el sobre de entrega de la misma, junto al PIN. Sin ese código de desbloqueo será imposible recuperar la tarjeta.

En la siguiente pantalla, el asistente nos pedirá que introduzcamos el nuevo PIN que queremos ponerle a la tarjeta. No tiene por qué ser el que utilizábamos antes, ni tiene ninguna restricción aparte de la longitud (debe ser mayor de cuatro caracteres).



Deberemos introducirlo dos veces para asegurarnos que no hemos cometido ningún error al teclearlo.



**Figura 24:** Desbloqueo de tarjeta. Pantalla de PIN.

Una vez insertado el nuevo PIN, el asistente comprobará que ambos cuadros de texto contienen la misma cadena. En caso afirmativo se activará el botón ‘**Siguiente**’ para permitirnos continuar con el proceso de desbloqueo.

Si los dos códigos introducidos no coincidiesen, el cuadro de confirmación del PIN mostraría una cadena de símbolos ###, tal y como vemos en la siguiente figura.



**Figura 25:** Desbloqueo de tarjeta. Pantalla de PIN erróneo.

Mientras la confirmación no coincida con el PIN que hemos introducido, el botón de “Siguiente” permanecerá inactivo, no permitiéndonos continuar con el proceso de desbloqueo. Una vez que sean iguales, el asistente activará dicho botón y podremos continuar con el siguiente paso.

Cuando hayamos indicado el nuevo PIN que queremos asignar a la tarjeta al finalizar la operación, el asistente nos pedirá que introduzcamos el código de desbloqueo. Es un código de **16 caracteres** que viene indicado en el sobre de la tarjeta. Contiene tanto números como letras, pero hay que tener en cuenta que no se considera el mismo



carácter una letra en minúscula que en mayúscula. Hay que teclearlo exactamente como viene en el sobre.



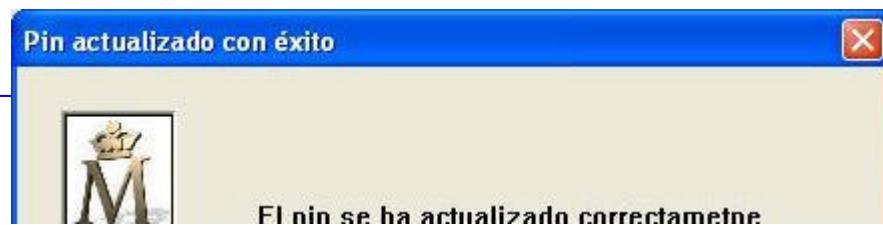
Figura 26: Desbloqueo de tarjeta. Código de desbloqueo.

Dado que la longitud del código de desbloqueo es fija, existe un indicador de progreso que no activará el botón de “**Siguiente**” hasta que no hayamos introducido los 16 caracteres que lo componen. Una vez que completemos el código, continuaremos con el desbloqueo de la tarjeta. El asistente intentará desbloquear y modificar el PIN utilizando los códigos que hayamos introducido en los pasos previos.

Es importante advertir que **el código de desbloqueo no puede ser desbloqueado**, por lo que tres intentos erróneos provocarán que la tarjeta quede inutilizada y sea imposible de recuperar.

Una vez finalizada la ejecución, nos mostrará un mensaje en pantalla informándonos de cómo terminó el proceso. En las figuras de la página siguiente podemos observar los resultados posibles.

Esta pantalla muestra que la operación se ha desarrollado correctamente, quedando el PIN de la tarjeta con el valor que habíamos introducido en la primera ventana.





**Figura 27:** Desbloqueo de tarjeta. Desbloqueo correcto de la tarjeta.

En caso de que el código de desbloqueo no sea el correcto, el asistente nos informará del error.



**Figura 28:** Desbloqueo de tarjeta. Error en el código de desbloqueo.

### 10.3 Herramientas para gestión de certificados en Microsoft.

Las aplicaciones de Microsoft utilizan **CryptoAPI**, y la gestión que realizan de los certificados es diferente de aquellas que integran **PKCS#11**. Es importante recordar que



para Microsoft si el certificado no está instalado en el registro del sistema, no lo reconocerá y por lo tanto no podrá trabajar con él.

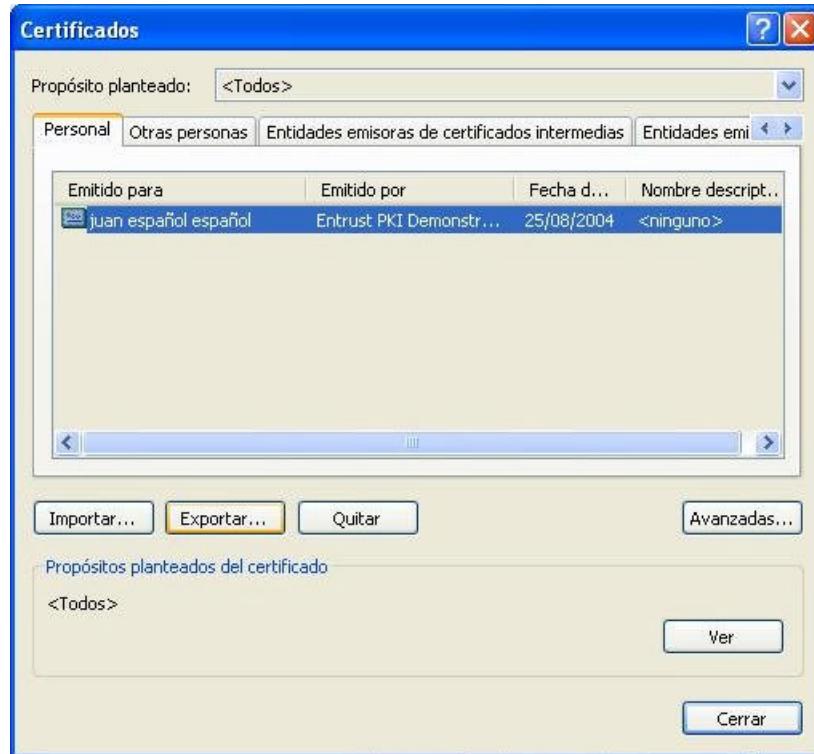


Figura 29: Certificados instalados en el sistema.

Cuando tenemos nuestro certificado digital almacenado en tarjeta es necesario transferirlo al registro para que las aplicaciones basadas en CryptoAPI puedan acceder a él. Con el software criptográfico de la FNMT-RCM hay dos formas de hacerlo. La elección de una solución u otra (son **incompatibles** entre sí) vendrá en función de las necesidades del cliente. Dichas soluciones son:

- **Ceresmon.exe.** Aplicación que se ejecuta en segundo plano comprobando la tarjeta e instalando los nuevos certificados que encuentre en ella.
- **CeresCertStore.dll.** Librería de acceso a los certificados de la tarjeta, a la que se accede sólo en caso de que la aplicación CryptoAPI lo requiera.

En los siguientes apartados explicaremos con detalle ambos métodos, sus ventajas y sus ámbitos de aplicación.

### 10.3.1 Gestión de certificados digitales mediante CERESMON.

**CeresMon** es una aplicación residente que se ejecuta en segundo plano, comprobando si se inserta una tarjeta en el lector. Su finalidad es obtener los certificados que tenga



almacenados esa tarjeta e instalarlos en el registro del sistema operativo. De esta manera, las aplicaciones que utilicen el **CryptoAPI** de Windows serán capaces de trabajar con ellos.



Figura 30: Icono de CeresMon en la barra de tareas.

Si pulsamos el botón derecho del ratón sobre el ícono del CeresMon, aparecerá un menú contextual como el siguiente.

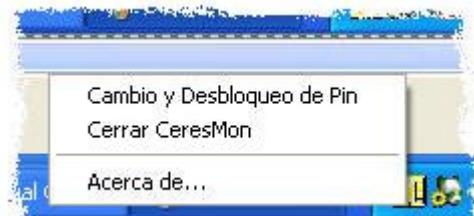


Figura 31: Menú contextual de CeresMon.

Dicho menú presenta varias opciones:

- **Cambio y desbloqueo de PIN.** Lanza la aplicación de desbloqueo de tarjeta (comentada en apartados anteriores), que nos permitirá hacerla de nuevo operativa en caso de haber fallado tres veces al insertar el PIN.
- **Cerrar CeresMon.** Cierra la aplicación. En caso de hacerlo habrá que tener en cuenta que al insertar una nueva tarjeta el sistema no instalará en el registro los certificados que tenga almacenados, y por lo tanto no estarán disponibles para las aplicaciones que utilicen CryptoAPI. Para volver a lanzar CeresMon deberá hacerse manualmente desde el directorio en que se encuentre el ejecutable.
- **Acerca de...** Muestra una ventana en la que aparece la versión del CeresMon que esté actualmente instalada en su sistema.

Cuando solicitamos un certificado con *Microsoft Internet Explorer*, se crean una serie de entradas en el registro del sistema que identificarán esa solicitud y permitirán realizar la posterior descarga, que normalmente se realizará tras un proceso de registro físico del solicitante por parte de alguna **Autoridad de Registro**. Sin esas entradas, la aplicación no identificaría la petición y no permitiría la descarga del certificado. La característica



---

más importante de Ceresmon es la posibilidad de **solicitar un certificado y descargarlo en un equipo diferente**, algo que no puede hacerse con CeresCertStore.

Para solucionar el inconveniente de tener que descargar el certificado obligatoriamente en el equipo donde se hizo la solicitud, Ceresmon copia en la tarjeta los datos que se van a almacenar en el registro. Después, al insertar la tarjeta en otro equipo, Ceresmon detecta los datos de la solicitud y los almacena en el registro. De esta forma, cuando vayamos a descargar el certificado se encontrará la información necesaria y se podrá obtener el certificado sin problemas.

Hay que recordar que esto sólo ocurre con las aplicaciones basadas en CryptoAPI (*Internet Explorer*), pero no con las que integran PKCS#11 (*Navigator*). En *Netscape* todos los datos de la solicitud necesarios para la posterior descarga se almacenan en la tarjeta. Cuando queramos descargar el certificado, simplemente deberemos introducirla en el lector y el navegador realizará las operaciones necesarias.

#### **10.3.2 Gestión de certificados digitales mediante CERESCERTSTORE.**

**CeresCertStore.dll** es una librería de acceso a los certificados de la tarjeta FNMT-RCM. Presenta dos diferencias principales con *Ceresmon*. La primera de ellas es que al no ser una aplicación que se ejecute en segundo plano, no supone para el sistema una carga tan alta en el tiempo de ejecución. A esta librería sólo se accede cuando las



---

aplicaciones que utilicen CryptoAPI intenten trabajar con un certificado digital instalado en el sistema, y cuyo almacén físico esté indicado que es la tarjeta FNMT-RCM.

La otra gran diferencia respecto a *Ceresmon* es que utilizando *CeresCertStore.dll* para solicitar y descargar certificados digitales, será indispensable que ambas operaciones se realicen en el mismo equipo. *Ceresmon* permite descargar certificados en máquinas distintas de la que se realizó la solicitud, y por esa razón su uso está recomendado para puestos de registro, donde se realizarán multitud de peticiones pero se permite la descarga en el ordenador personal del usuario. En cambio, *CeresCertStore.dll* obliga a que la descarga sea en el mismo equipo.

Esta última diferencia es la que marcará principalmente la elección por parte del cliente entre usar *CeresMon* o *CeresCertStore*. Hay que recordar que son soluciones **incompatibles** y que la instalación será diferente en función de lo que se solicite.

Al navegador de Netscape no le afecta en nada que la solución para Microsoft se base en *CeresMon* o en *CeresCertStore*. El funcionamiento será el habitual, permitiendo solicitar certificados y descargarlos en cualquier equipo. Esto es debido a que para el uso de las tarjetas FNMT-RCM, Netscape utiliza otra librería diferente: **pkcs12gk.dll**, completamente independiente.



## Capítulo 11

### *Solicitud y descarga de certificados Clase 2CA*





## **11 SOLICITUD Y DESCARGA DE CERTIFICADOS CLASE 2CA.**

Las tarjetas FNMT-RCM soportan el uso de certificados de **Clase 2CA**, expedidos por la propia **Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda**. Para tener este tipo de certificados almacenados en tarjeta podemos seguir dos procesos.

- Realizar una **solicitud** y la posterior **descarga** directamente en la tarjeta. Conectándonos con la página [www.cert.fnmt.es](http://www.cert.fnmt.es), desde donde se nos indica cómo realizar ambas operaciones.
- **Importar** a la tarjeta un certificado software. Este proceso se describe con detalle en el Capítulo 5 de este Manual de Usuario.

En los siguientes apartados vamos a explicar el primero de estos métodos para cada uno de los navegadores más comunes (*Internet Explorer* y *Navigator*).



## 11.1 Clase 2CA con Microsoft Internet Explorer.

El primer navegador sobre el que vamos a comentar la solicitud y la descarga de certificados será sobre *Internet Explorer*. La página web sobre la que realizaremos ambas operaciones es [www.cert.fnmt.es](http://www.cert.fnmt.es).



Figura 32: Web de la FNMT-RCM.

Al seleccionar “OBTENCIÓN” iremos a una pantalla en la que se nos muestra toda la información relativa a los certificados Clase 2CA: cómo solicitarlo y descargarlo, posibles usos, revocaciones, información general sobre criptografía, etc.



### 11.1.1 Solicitud de certificados Clase 2CA.

Nuestro interés se centra ahora en la solicitud de certificados para este navegador. Vemos que en la pantalla principal de los certificados de Clase2CA existe la opción de “Solicitud vía Internet de su Certificado”. Es la que deberemos seleccionar.

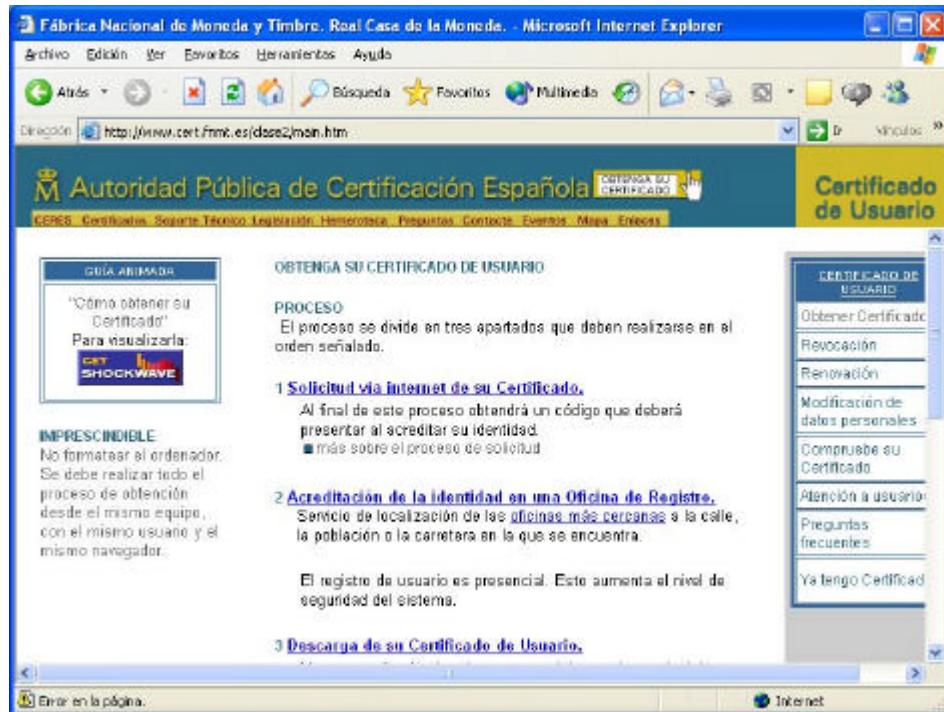


Figura 33: Pantalla principal de certificados Clase 2CA.

Entonces se nos solicitará el NIF del usuario titular del certificado.

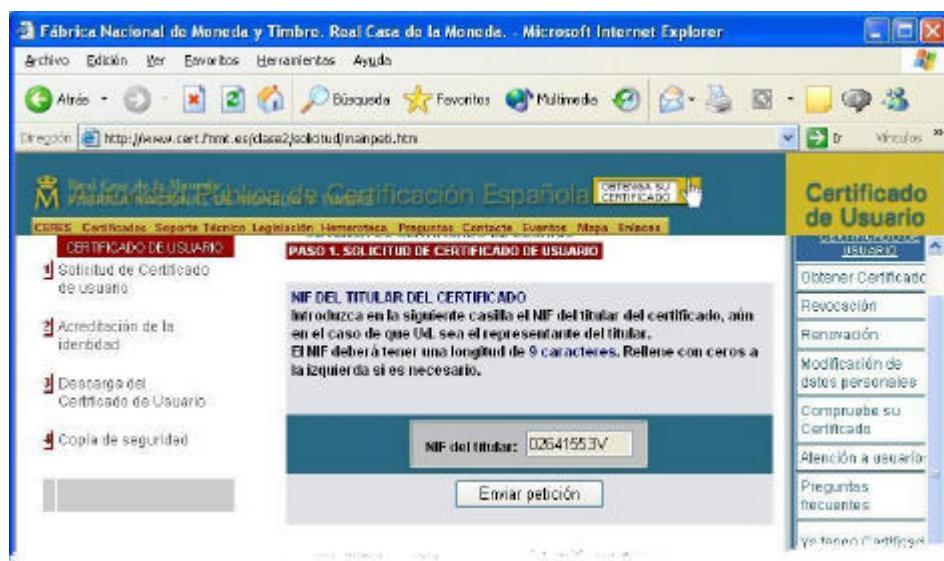


Figura 34: Solicitud del NIF del titular.



Según el nivel de seguridad que estemos utilizando en el navegador, podría aparecer una ventana informando de que se va a realizar una operación potencialmente peligrosa para el sistema. Simplemente indicaremos que sí queremos realizar la solicitud del certificado y se continuará normalmente con la solicitud del mismo.

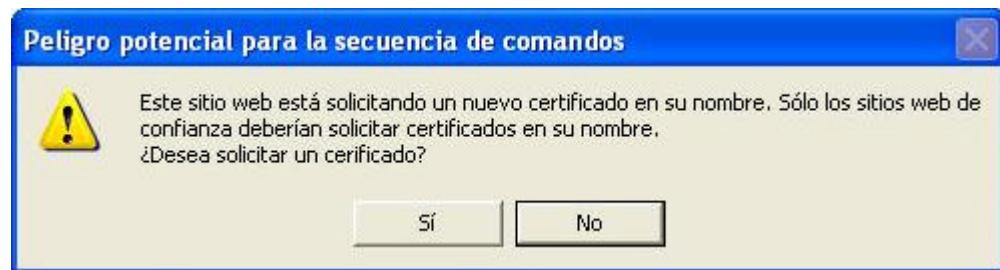


Figura 35: Aviso de peligro potencial.

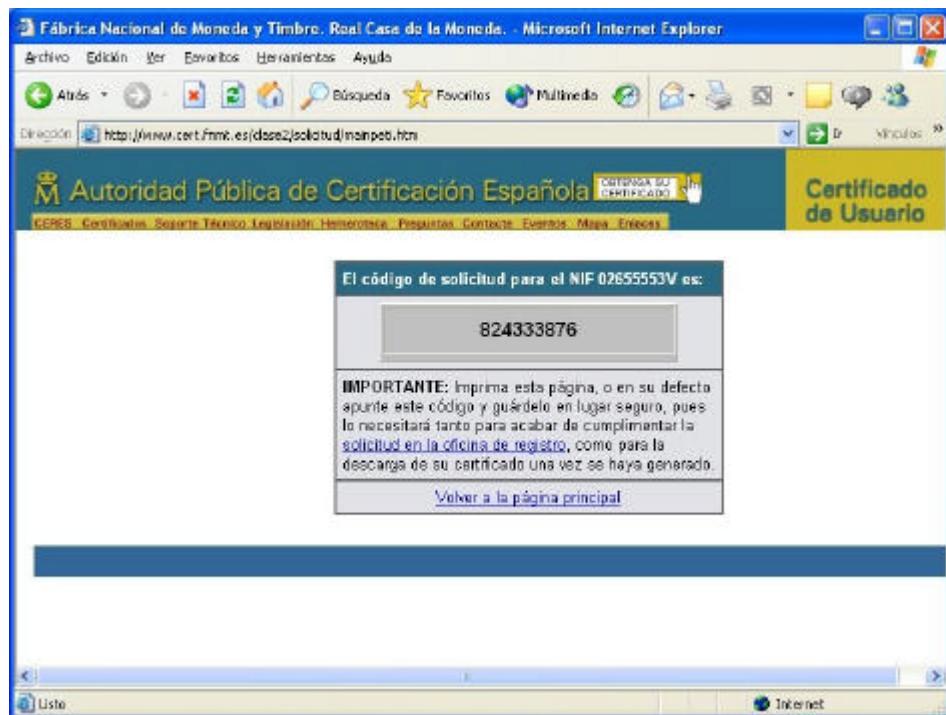
El sistema nos avisará que estamos a punto de crear un elemento protegido: las **claves del certificado**. Éstas quedan almacenadas en el registro del sistema operativo. En caso de que estemos utilizando **CERESMON** (ver **apartado 10.3.1**) las claves se generarán también en el interior de la tarjeta FNMT-RCM. Además se guardarán ciertos datos que permitirán realizar la descarga en otro equipo diferente del de la solicitud, siempre y cuando también tenga instalado CERESMON.



Figura 36: Advertencia de generación de claves.



Cuando se generen las claves del certificado, se mostrará una ventana en la que aparece un código de solicitud. Con ese código el usuario deberá acudir a una *oficina de registro* para ser acreditado. Realizado este paso intermedio, podrá descargar su certificado de **Clase 2CA**.



**Figura 37:** Código de solicitud generado para esa petición.



### 11.1.2 Descarga de certificados Clase 2CA.

Cuando el usuario se haya acreditado en la oficina de registro, se tramitará su solicitud para permitir la descarga del certificado de Clase 2CA. Para realizar este proceso deberemos seleccionar la opción de **Descarga de su certificado de usuario** de la página principal de la FNMT-RCM.

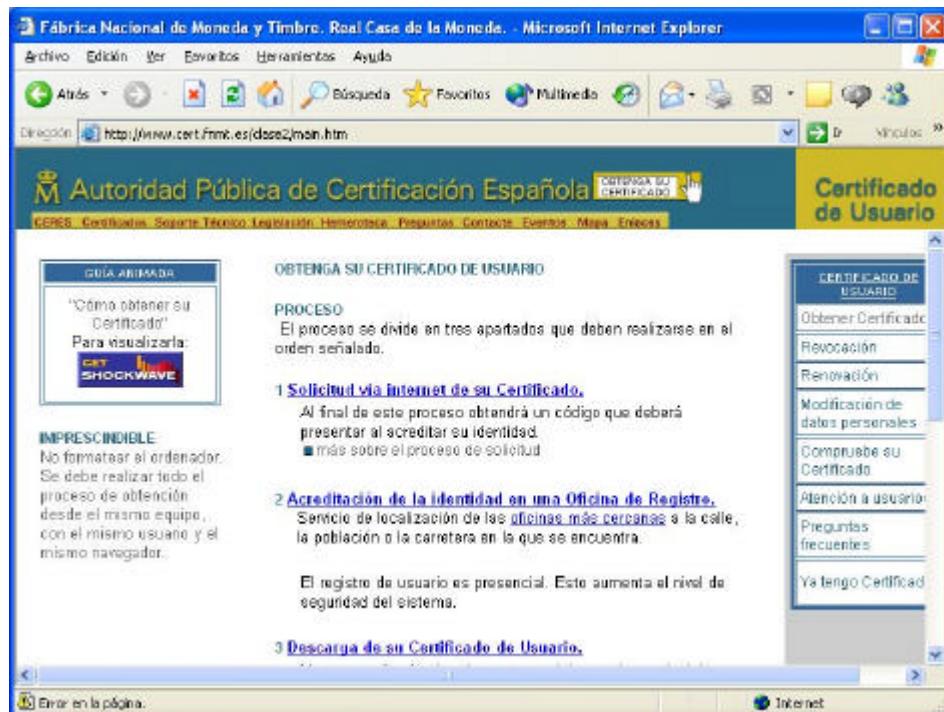


Figura 38: Pantalla principal de certificados Clase 2CA.

En este punto vamos a recordar que el uso del software **CERESMON** permite la descarga de certificados en equipos diferentes de aquellos en los que se realizó la solicitud. En su **versión 1.0.0.8**, este programa soporta la descarga en equipos con **Windows 98**, **Windows 2000** y **Windows NT**. En futuras versiones se implementará para **Windows XP**.

El uso de CERESMON está especialmente indicado para puestos de registro, destinados a realizar multitud de solicitudes de certificados. El usuario se llevará una tarjeta FNMT-RCM con las claves generadas y con los datos necesarios para realizar la descarga en su propio equipo. Para ello hay que recalcar que en dicho equipo final también deberá estar instalado CERESMON, que se encargará de extraer la información de la tarjeta y permitir la descarga final.



El proceso de descarga es muy sencillo. Una vez elegida la opción en la web de la FNMT-RCM, aparecerá una pantalla en la que se nos pedirá el **NIF** del titular y el **código de solicitud** con que se acreditó el titular en la oficina de registro.

The screenshot shows a Microsoft Internet Explorer window with the following details:

- Title Bar:** Fábrica Nacional de Moneda y Timbre. Real Casa de la Moneda - Microsoft Internet Explorer
- Address Bar:** http://www.cert.fnmt.es/cerse2/descarga/cert/maindesc.htm
- Content Area:**
  - M Autoridad Pública de Certificación Española**
  - CERES Certificado. Soporte Técnico. Legislación. Hemeroteca. Preguntas. Contacto. Eventos. Mapa. Índices.**
  - Solicitud de Certificado de Usuario:** A red box highlights this section.
  - Acreditación de la identidad:**
  - Descarga del Certificado de Usuario:**
  - Copia de seguridad:**
  - Para descargar el certificado debe usar el mismo ordenador que en el paso de Solicitud:**
  - FORMULARIO DE DESCARGA:** A red box highlights this section.
  - Rellene el siguiente formulario y pulse el botón "Descargar el Certificado" para completar la obtención del Certificado de Usuario de la FNMT.**
  - más sobre el proceso de descarga del certificado de usuario**
  - NIF del titular:** [Input field]
  - Código de Solicitud:** [Input field]
  - Descargar Certificado** [Button]
  - En el campo de DNI, rellene con ceros a la izda. si es necesario.**
- Right Panel:** A sidebar titled "Certificado de Usuario" with a vertical list of links:
  - Obtener Certificado
  - Revocación
  - Renovación
  - Modificación de datos personales
  - Compruebe su Certificado
  - Atención al usuario
  - Preguntas frecuentes
  - Ya tengo Certificado

Figura 39: Petición de datos para la descarga del certificado.

Cuando hayamos introducido esos valores, procederemos a la descarga del certificado. Lo primero que se hará es comprobar que la solicitud ha sido tramitada por la oficina de registro correspondiente. En caso de que el certificado aún no esté disponible, se mostrará un mensaje de error indicándolo.

The screenshot shows a Microsoft Internet Explorer window with the following details:

- Title Bar:** Fábrica Nacional de Moneda y Timbre. Real Casa de la Moneda - Microsoft Internet Explorer
- Address Bar:** http://www.cert.fnmt.es/cerse2/descarga/cert/maindesc.htm
- Content Area:**
  - Real Casa de la Moneda. FÁBRICA NACIONAL DE MONEDA Y TIMBRE. M Autoridad Pública de Certificación Española**
  - CERES Certificado. Soporte Técnico. Legislación. Hemeroteca. Preguntas. Contacto. Eventos. Mapa. Índices.**
  - Certificado de Usuario**
  - El usuario de NIF 02655553V no tiene ninguna petición en estado de descarga correspondiente a la solicitud con el código 824333876.**
  - Para obtener el certificado debe acreditarse en una oficina de registro y esperar 24 h para que se procese su solicitud**
  - Volver a intentarlo**

Figura 40: Error. El certificado aún no ha sido tramitado.



Si el certificado ya está disponible, se procederá a la descarga. Como se va a acceder a la tarjeta criptográfica de la FNMT-RCM, se nos solicitará su PIN. Es imprescindible introducirlo, ya que si no no podremos generar los componentes privados necesarios para el certificado.



**Figura 41:** Solicitud del PIN de la tarjeta.

En caso de introducirlo erróneamente, aparecerá un mensaje advirtiéndonoslo y el proceso de descarga se interrumpirá.



**Figura 42:** Error en el PIN introducido.



**Figura 43:** Mensaje de interrupción del proceso de descarga.



Si el PIN introducido es el correcto, se generarán en la tarjeta el certificado digital y las claves correspondientes. Si no quedase espacio suficiente dentro de la tarjeta para esos nuevos objetos, se mostrará un mensaje de error indicándonoslo. Mientras no eliminemos algún certificado de la tarjeta no podremos descargar en ella ninguno más.



**Figura 44:** Mensaje de error. No queda espacio para el nuevo certificado.



**Figura 45:** Advertencia de la finalización errónea del proceso de descarga.

Si la tarjeta tiene suficiente espacio libre para albergar el certificado completo, se crearán en ella los objetos necesarios. Al igual que ocurría antes, según el nivel de seguridad que tengamos indicado en el navegador, el sistema nos informará de que se está intentando hacer una operación peligrosa. Lo que está ocurriendo es que se van a crear las entradas del certificado dentro del registro de sistema y que se va a incluir también en el propio navegador. Pulsando en ‘Sí’ la operación continuará normalmente.



**Figura 46:** Advertencia de operación peligrosa.



---

Al final del proceso la página de la FNMT-RCM nos indicará que ha finalizado correctamente el proceso de descarga, quedando el certificado listo para su utilización.



## 11.2 Clase 2CA con Netscape Navigator.

Los procesos de solicitud y descarga con *Netscape Navigator* son completamente análogos a los de *Microsoft Internet Explorer*. Vamos a explicarlos brevemente y comentaremos los posibles errores que podemos obtener en cada caso.



Figura 47: Ventana principal de la Web con Netscape Navigator.



### 11.2.1 Solicitud de certificados Clase 2CA.

Este proceso tiene algunas diferencias importantes respecto a *Internet Explorer*, en cuanto a la selección del destino donde se almacenará el certificado. En el navegador de *Microsoft*, las claves de la solicitud quedaban almacenadas en el registro de sistema (a no ser que utilizásemos CERESMON, en cuyo caso también se guardaban en la tarjeta). Con *Netscape Navigator* podemos seleccionar dónde almacenar esas claves de la petición. La mayor diferencia respecto a *Internet Explorer* es que ahora, gracias a esta posibilidad de selección del destino de las claves, la solicitud y la descarga del certificado en tarjeta puede realizarse en equipos diferentes sin necesidad de software adicional.

Cuando seleccionemos la opción de Solicitud de un certificado de clase 2CA, se nos mostrará una pantalla en la que deberemos introducir el NIF del titular. Otra diferencia importante respecto a *Internet Explorer* es que ahora debemos elegir la longitud de la clave. Es necesario que seleccionemos la opción de **1024 (High Grade)**, ya que en cualquier otro caso no podremos almacenar el certificado en la tarjeta FNMT-RCM.

The screenshot shows a Netscape browser window with the following details:

- Title Bar:** Fábrica Nacional de Moneda y Timbre. Real Casa de la Moneda. - Netscape
- Menu Bar:** File, Edit, View, Go, Communicator, Help
- Toolbar:** Back, Forward, Reload, Home, Search, Netscape, Print, Security, Shop, Stop
- Address Bar:** Bookmarks, Netsite: http://www.cert.fnmt.es/clase2/solicitud/mainpeti.htm, What's Related
- Navigation Buttons:** Instant Message, WebMail, Radio, People, Yellow Pages, Download, Calendar, Channels, RealPlayer
- Content Area:**
  - M Autoridad Pública de Certificación Española**
  - CERES Certificados Soporte Técnico Legislación Hemeroteca Preguntas Contacte Eventos Mapa Enlaces**
  - NIF DEL TITULAR DEL CERTIFICADO**  
Introduzca en la siguiente casilla el NIF del titular del certificado, aún en el caso de que Ud. sea el representante del titular.  
El NIF deberá tener una longitud de 9 caracteres. Rellene con ceros a la izquierda si es necesario.
  - NIF del titular:** [Input field]
  - LONGITUD DE LA CLAVE**  
Seleccione como longitud de clave 1024 bits. Esto proporciona un alto nivel de seguridad, además de ser la única longitud soportada para la firma de Certificados.
  - Longitud clave :** 1024 (High Grade)
  - Enviar petición** [Button]
- Right Panel:** Certificado de Usuario (with a list of options: Obtener Certificado, Revocación, Renovación, Modificación de datos personal, Compruebe su Certificado, Atención a usu..., Preguntas frecuentes, Ya tengo Certifi...)

Figura 48: Pantalla de datos para la solicitud del certificado.



Cuando pulsemos el botón de **Enviar Petición**, se nos mostrará una nueva ventana en la que podemos seleccionar los distintos almacenes disponibles. Si queremos guardarla en la tarjeta FNMT-RCM, deberemos seleccionar la entrada correspondiente. De esta manera la descarga podrá realizarse en cualquier otro equipo utilizando esa tarjeta, como hemos comentado antes.



**Figura 49:** Selección del destino de las claves a generar.

Tras esto se nos pedirá el PIN de la tarjeta, siempre y cuando no nos hayamos autenticado anteriormente contra ella.



**Figura 50:** Petición del PIN de la tarjeta FNMT-RCM.

En caso de introducir un PIN erróneo, aparecerá una ventana advirtiéndonos del error y avisándonos de que repetidos fallos en la autenticación del usuario pueden provocar el bloqueo de la tarjeta. Como ya sabemos, en total disponemos de tres intentos para introducir correctamente el PIN.



**Figura 51:** Reintento por PIN erróneo.



Si ocurre algún problema con la generación de claves, Netscape nos lo indicará con un mensaje de error.

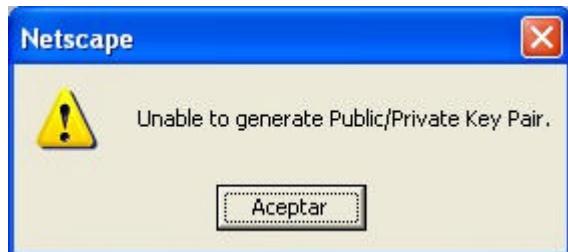


Figura 52: Ventana principal de la Web con Netscape Navigator.

Netscape utiliza este mensaje de error para cualquier fallo que pueda ocurrir durante la generación de las claves: tarjeta llena, fallo en la generación, etc. Para ver qué puede haber ocurrido podemos hacer algunas comprobaciones. En primer lugar hay que asegurarse que queda espacio en la tarjeta para introducir un nuevo certificado. Para ello podemos comprobar el módulo **Security**, donde veremos qué certificados tenemos instalados en el sistema.

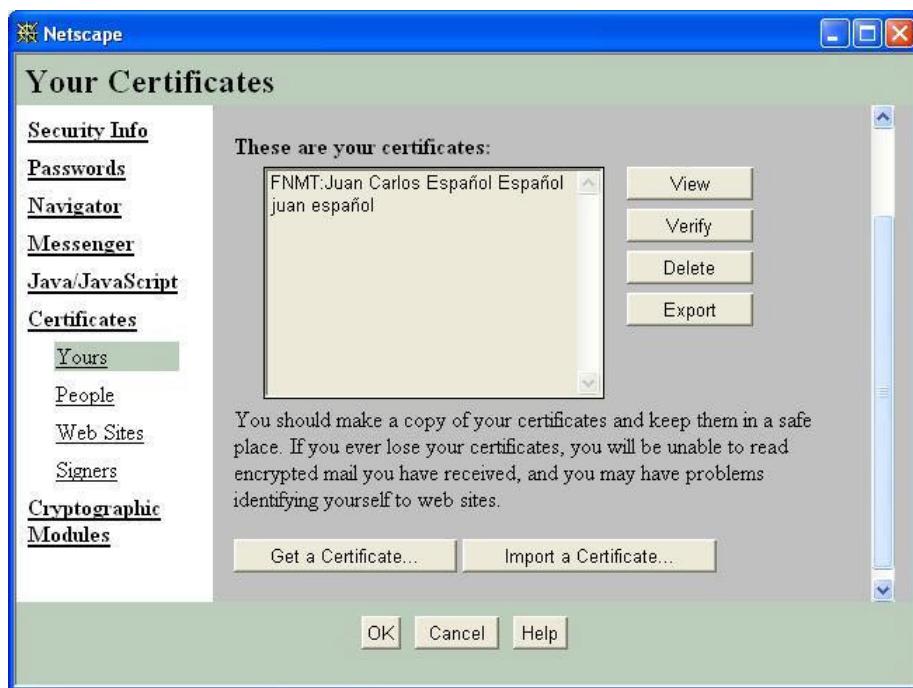
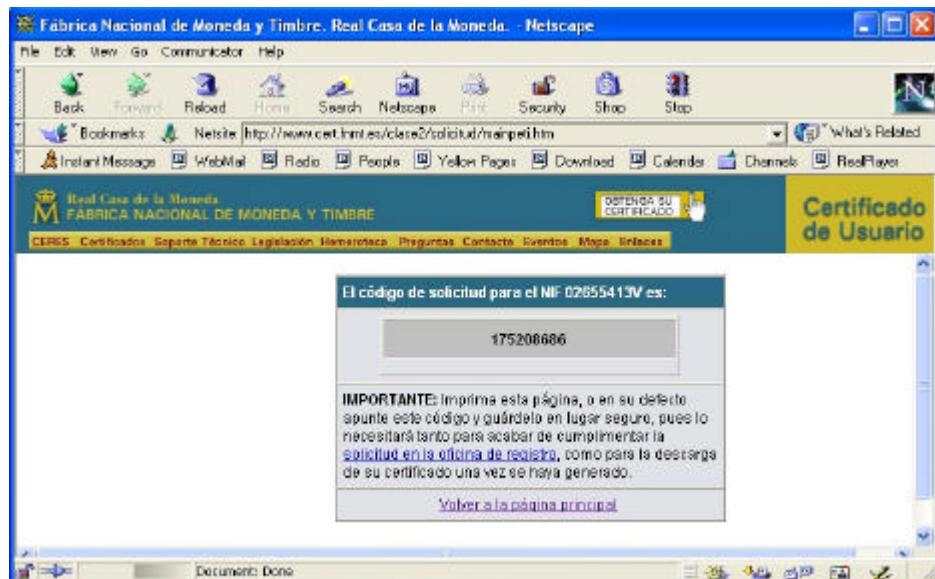


Figura 53: Certificados instalados en el sistema.

Si nos ha devuelto un error durante la generación podríamos probar a eliminar alguno de los certificados que aparezcan en esa lista (botón **Delete**) y que estén almacenado dentro de la tarjeta. En la figura anterior vemos que tenemos uno en tarjeta y otro en la base de datos propia de *Netscape*.



Cuando generemos correctamente las claves de la solicitud, aparecerá un mensaje indicándonos el código que debemos presentar en la oficina de registro para acreditarnos.



**Figura 54:** Código de solicitud obtenido con Netscape Navigator.



### 11.2.2 Descarga de certificados Clase 2CA.

El proceso de descarga en *Netscape* también es análogo al de *Microsoft*. La diferencia fundamental es, como ya hemos comentado en apartados anteriores, que si la solicitud la hicimos en tarjeta la descarga podremos realizarla en cualquier otro equipo.

Para comenzar el proceso de descarga seleccionaremos la opción de **Descargar certificado de usuario** en la pantalla principal. Después tendremos que indicar el NIF del titular y el código de solicitud que se presentó en la oficina de registro.

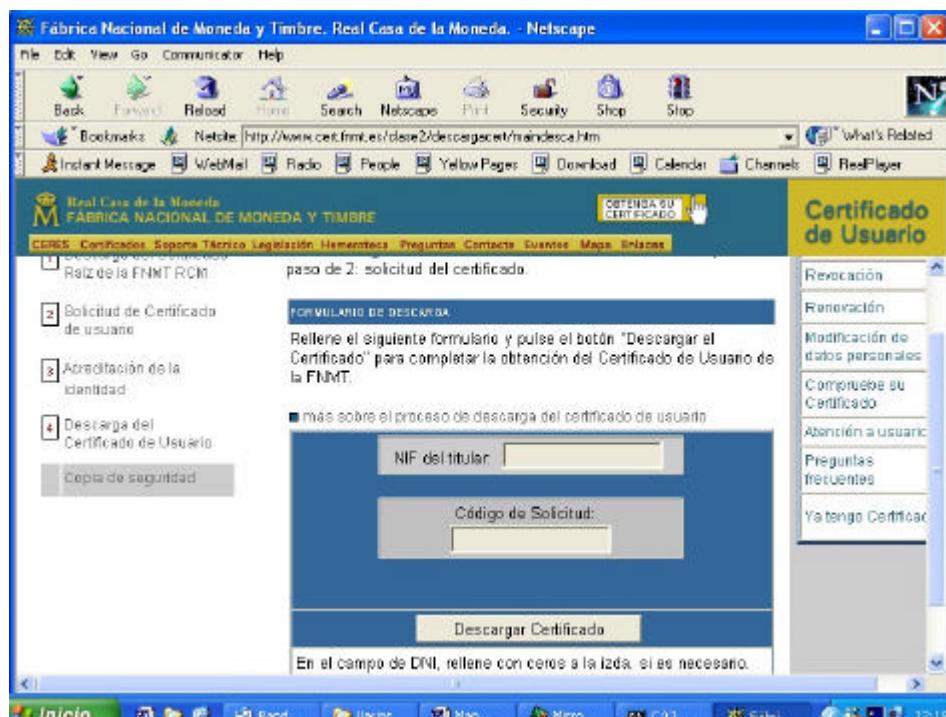


Figura 55: Datos para la descarga del certificado.

Si el certificado ya ha sido tramitado por la oficina de registro se nos pedirá el PIN de la tarjeta y se procederá a la descarga. Después se mostrará un mensaje con el resultado de la operación, ya sea para decir que el proceso se ha completado correctamente o para indicar algún posible error.



## Capítulo 12

### *Exportación de Certificados*





## 12 EXPORTACIÓN DE CERTIFICADOS.

Cuando un certificado digital queda instalado en el sistema, pasa a estar disponible para todas aquellas aplicaciones que utilicen CryptoAPI. De esta manera las aplicaciones pueden acceder a sus claves para realizar todo tipo de operaciones de firma, cifrado, etc. utilizando ese perfil.

El problema surge cuando queremos utilizar nuestro certificado en otra máquina distinta de aquella en la que lo habíamos descargado y que lo tiene convenientemente instalado. Para poder hacerlo deberemos **exportar** el certificado desde el sistema inicial a un soporte software (*fichero electrónico*) o a un soporte hardware (*tarjetas inteligentes*, por ejemplo). Después realizaremos el proceso inverso, lo que haremos será **importarlo** a la máquina de destino o a un dispositivo físico (tarjeta inteligente), dejándolo instalado para su posterior uso. Este modo de operar es igual tanto en aplicaciones CryptoAPI como en aquellas basadas en PKCS#11. A continuación vamos a explicar cómo realizar la exportación en cada uno de los sistemas.

### 12.1 Exportación de certificados en Microsoft Internet Explorer.

En *Microsoft Internet Explorer* todas las operaciones relacionadas con la gestión de certificados (*profiles*) se encuentran en la solapa **Contenido** de la pantalla de **Herramientas/Opciones de Internet**. Desde aquí podremos ejecutar el apartado de **Certificados**, donde se realizan las operaciones de importar, exportar, eliminar certificados, ver sus características, fechas de validez, etc.



Figura 56: Opciones de Internet.



Dentro del apartado de certificados encontramos una pantalla en la que se nos muestran los certificados instalados en el sistema, y una serie de botones que nos permiten realizar las operaciones comunes: importar, exportar, eliminar, ver detalles, etc. Más adelante nos ocuparemos con detenimiento del resto de opciones. Por el momento nos centraremos en la operación de exportación.

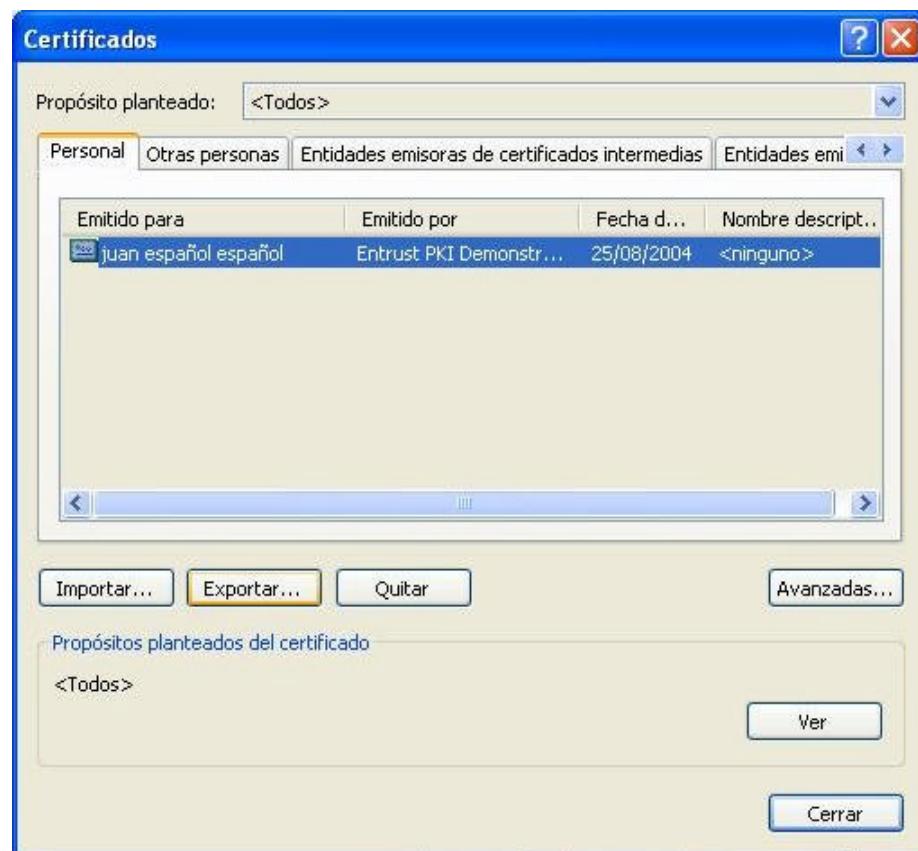


Figura 57: Certificados del sistema.

Deberemos seleccionar aquel certificado que queremos exportar del sistema. Para ver los detalles de cualquiera de ellos simplemente debemos pulsar sobre él dos veces el botón izquierdo del ratón. Aparecerá una ventana con la fecha de emisión, la caducidad, la Autoridad de Certificación (CA) que lo ha expedido, etc.

Cuando hayamos seleccionado el certificado que queremos exportar del sistema, pulsaremos el botón correspondiente para que el asistente de exportación nos indique los pasos que debemos seguir. Dicho asistente nos solicitará información sobre el tipo de exportación, el formato de salida que queremos que tenga el fichero, la ruta de salida, la contraseña para las claves, etc.



En la primera ventana se nos pregunta si queremos exportar la clave privada junto con el certificado. Sin esa clave el certificado servirá para que aquel que esté en posesión del mismo cifre correos con nuestra clave pública y pueda verificar nuestra firma digital. Esto es útil sobre todo para *aplicaciones de correo* en las que queramos utilizar criptografía. Si no exportamos la clave privada, lo que no se podrá hacer con el certificado son operaciones de firma ni descifrado.

Si queremos exportar el certificado con todas sus funcionalidades debemos hacerlo exportando también su clave privada. El fichero así obtenido contendrá el certificado completo, pudiendo realizar así todo tipo de operaciones criptográficas. Con el fin de evitar que ese fichero pudiese caer en manos no deseadas y alguien usase nuestro certificado en nuestro nombre, el fichero quedará protegido por una contraseña que indique el usuario.



**Figura 58:** Exportación de clave privada.

Al elegir exportar la clave privada, en la siguiente pantalla nos preguntará la contraseña con que queremos protegerla. Es importante recordar dicha contraseña ya que sin ella no será posible reinstalar el certificado.



En la pantalla siguiente el asistente nos preguntará acerca del formato que queremos que tenga el fichero de salida. Por defecto usaremos **PKCS#12**, que genera archivos **.pfx**.



**Figura 59:** Formato de exportación del certificado.

Tras la selección del formato, deberemos introducir la contraseña para proteger la clave privada (en caso de que hayamos decidido exportarla).



**Figura 60:** Verificación de contraseñas.



El último paso antes de la exportación es indicar la *ruta* y el *nombre* de salida del fichero. El asistente nos mostrará una pantalla en la que podemos teclearlo completo, o pulsar el botón de ‘**Examinar**’ y navegar hasta la carpeta de destino e indicar sólo el nombre que queremos darle al fichero.

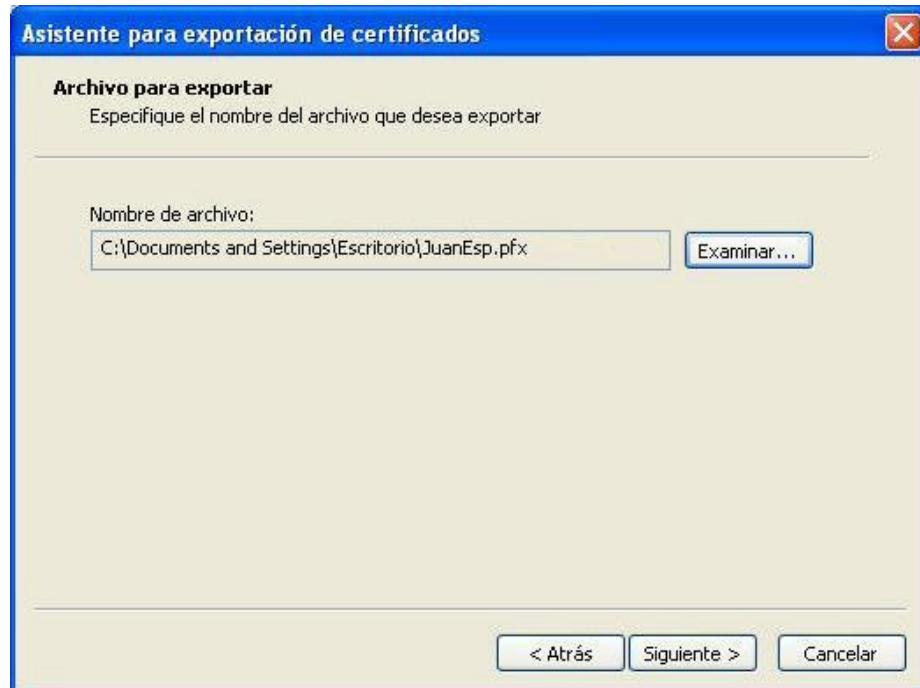


Figura 61: Ruta y nombre del fichero de salida.

Al pulsar en “Siguiente” se mostrará una ventana con la información final del fichero.



Figura 62: Pantalla resumen del fichero de exportación.



Cuando pulsemos el botón de “**Finalizar**”, el asistente realizará la exportación a fichero. En caso de que todo vaya correctamente se nos mostrará un mensaje de verificación. El fichero se habrá generado en la ruta indicada en pantallas anteriores y estará listo para ser **importado** a cualquier otro sistema.



**Figura 63:** Confirmación de la exportación del certificado.

En los próximos apartados explicaremos con detalle el proceso de importación al sistema, mediante el cual se instalará el certificado en el almacén seleccionado.



## 12.2 Exportación de certificados mediante Netscape Navigator.

El navegador de Netscape también nos permite trabajar con certificados digitales en tarjeta criptográfica siguiendo la recomendación **PKCS#11**. Desde esta aplicación podremos exportar perfiles, importarlos, ver su contenido, etc. Para acceder a todas estas funciones deberemos pulsar en el botón ‘**Security**’, que nos mostrará una pantalla como la de la siguiente figura.



Figura 64: Pantalla de seguridad en Netscape.

En el apartado “**Certificates**” aparecen todos los certificados instalados en nuestro sistema y reconocidos por cada *módulo criptográfico*. Vimos en el apartado sobre el gestor de aplicación de la FNMT-RCM en el Panel de Control (ver apartado **10.1.2**), que la solapa de Netscape instalaba un módulo criptográfico. Esto no es más que una referencia a la librería que implementa la interfaz PKCS#11 que debe usar *Netscape* para poder utilizar un determinado dispositivo (como por ejemplo en nuestro caso, a *pkcs12gk.dll* para la tarjeta FNMT-RCM).

En esta pantalla podemos ver cómo aparece el nombre del dispositivo (también llamado *token*) seguido del titular del certificado. Si sólo aparece el nombre del titular significa que ese certificado está instalado en la base de datos genérica de Netscape. En la figura del ejemplo aparecen dos certificados, el primero de ellos precedido de **FNMT**, que es el nombre del *token* que lo contiene, y el segundo sin él. Esto nos indica que el primer certificado está almacenado en la tarjeta inteligente FNMT-RCM, mientras que el segundo se guarda en la base de datos de la aplicación.



Si queremos exportar un certificado **instalado en el sistema** a un fichero electrónico, elegiremos la opción ‘**Export**’. Hay que tener en cuenta que los certificados que estén almacenados dentro de la tarjeta **no pueden ser exportados**. Esto se debe a motivos de seguridad, ya que la tarjeta FNMT-RCM no permite que la clave privada del certificado sea extraída. Al no poder sacar la clave privada, el certificado no puede ser exportado.

Cuando tengamos seleccionado el certificado, pulsaremos el botón de exportación y comenzaremos con el proceso. En este caso es más sencillo que con Microsoft Internet Explorer. Lo primero que debemos indicar es la **contraseña** con la que vamos a proteger la clave privada. Al igual que ocurría en Microsoft, sin esa contraseña será imposible importar después el certificado.



Figura 65: Solicitud de contraseña para la clave privada.

Tras pedirnos una confirmación de la contraseña utilizada, el navegador nos mostrará una ventana en la que indicaremos la ruta y el nombre del fichero de salida al que se exportará el certificado. A diferencia de como ocurría en *Internet Explorer* el formato por defecto del fichero de exportación en *Netscape* es **.p12**, que sigue la recomendación **PKCS#12** sobre la sintaxis para el intercambio de información.

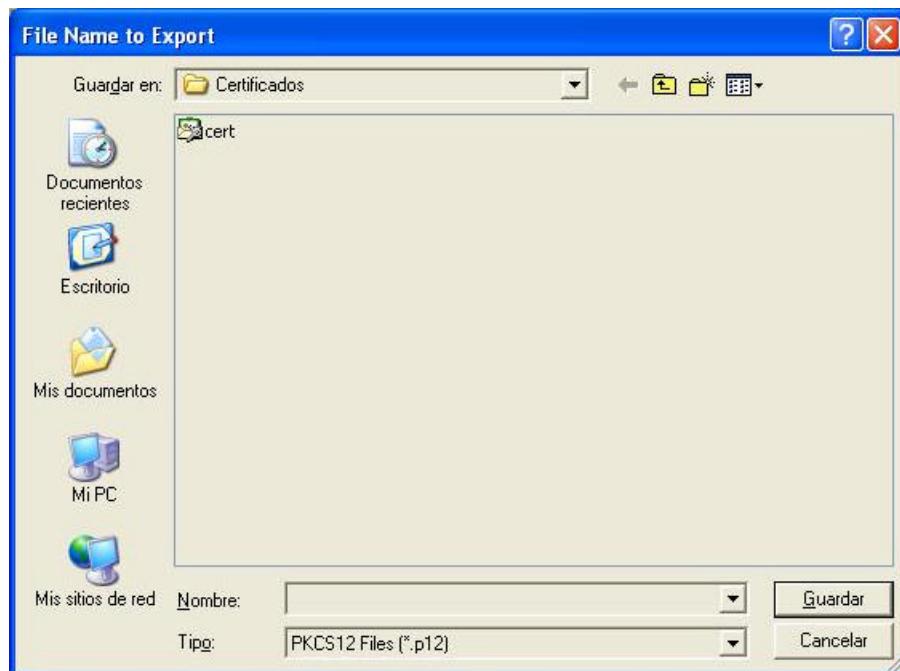


Figura 66: Selección de ruta y formato de archivo.



Posteriormente el navegador generará un fichero de salida con el formato deseado en la ruta especificada. En cualquier caso se nos mostrará un mensaje de información en el que nos indique cuál ha sido el resultado de la operación de exportación del certificado.



**Figura 67:** Exportación completada correctamente.

Si el navegador no encontrase las claves del certificado o hubiese cualquier problema con la exportación de las mismas, la aplicación mostrará en pantalla una ventana con el error.



**Figura 68:** Error en la exportación.

Este es el proceso completo de exportación de certificados mediante *Netscape Navigator*. Al finalizar dispondremos de un fichero donde se encuentra almacenado nuestro certificado digital y que podrá ser importado a otro sistema para su uso posterior. En los siguientes apartados vamos a detallar cómo podemos realizar ese proceso de importación.



## Capítulo 13

### *Importación de Certificados*





## 13 IMPORTACIÓN DE CERTIFICADOS.

Las tarjetas inteligentes proporcionan un mecanismo idóneo para la portabilidad de perfiles digitales y la seguridad en operaciones criptográficas. Pero puede ocurrir que inicialmente ya tuviésemos nuestro perfil en *software* (fichero electrónico) y queramos introducirlo en una tarjeta inteligente. Para ello se diseñó una aplicación específica para la importación de certificados a la tarjeta, **CeresImportCertificate**. Además de esta aplicación también es posible realizar dicha operación mediante el uso de los navegadores **Microsoft Internet Explorer** y **Netscape Navigator**. En los siguientes apartados explicaremos con detalle el proceso para cada una de las dos posibilidades.

### 13.1 Importación mediante Microsoft Internet Explorer.

Hemos visto en los apartados anteriores las opciones que presenta el navegador de *Microsoft Internet Explorer* para trabajar con la importación y la exportación de certificados. A la hora de importar un certificado desde soporte software (fichero electrónico) a un *almacén de certificados*, nos encontramos que dicho almacén puede ser lógico (una carpeta del sistema) o físico (una tarjeta inteligente). Durante el proceso de importación deberemos indicar si lo que queremos realizar es una importación al sistema, con el fin de que el certificado quede disponible para las aplicaciones CryptoAPI, o bien si lo que queremos es almacenarlo en otro soporte físico distinto del fichero.

Para realizar las importaciones a la tarjeta y facilitar la instalación del certificado a la hora de descargarlo, se ha desarrollado una librería que gestione dichas operaciones. La librería, **CeresCertStore.dll**, se instalará de forma simultánea junto con el resto del software de la FNMT-RCM. En concreto, se almacenará en el directorio **Windows/System** o **Windows/System32**, según el sistema operativo que esté instalado.

**CeresCertStore.dll** permite instalar certificados software en la tarjeta, descargarlos directamente en ella, etc.



El proceso de importación comenzará desde la ventana de certificados (**Herramientas/Opciones de Internet/Contenido/Certificados**).



Figura 69: Herramientas de Internet.

Ahí pulsaremos el botón de **'Importar'** para empezar el proceso, como vemos en la siguiente figura.

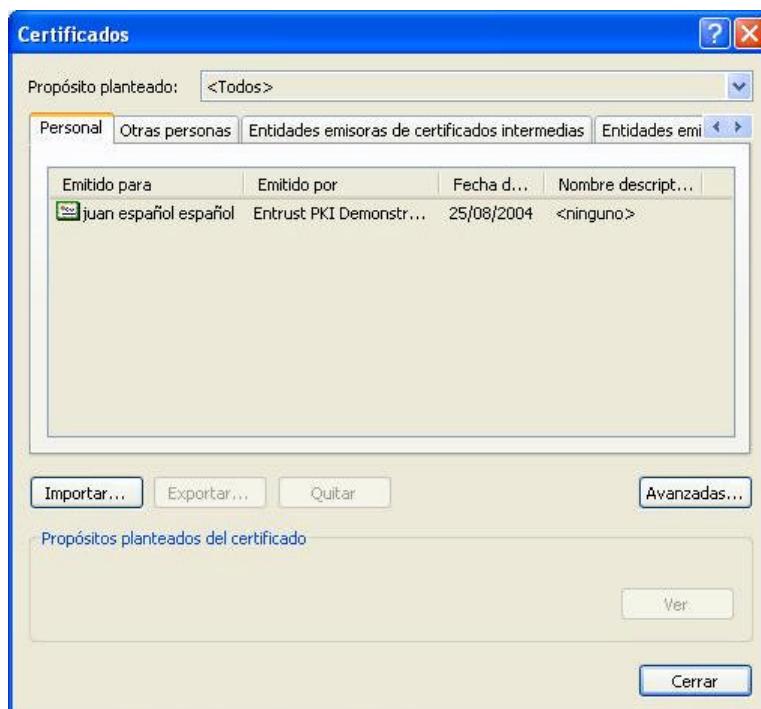


Figura 70: Página de certificados.



En ese momento se ejecutará el asistente que nos indicará los pasos a seguir para realizar correctamente la importación del certificado. Lo primero que deberemos hacer es indicar qué fichero contiene el certificado que queremos importar. Para ello aparecerá una ventana en la que podremos escribir la ruta completa o bien examinar nuestra estructura de archivos hasta encontrarlo.

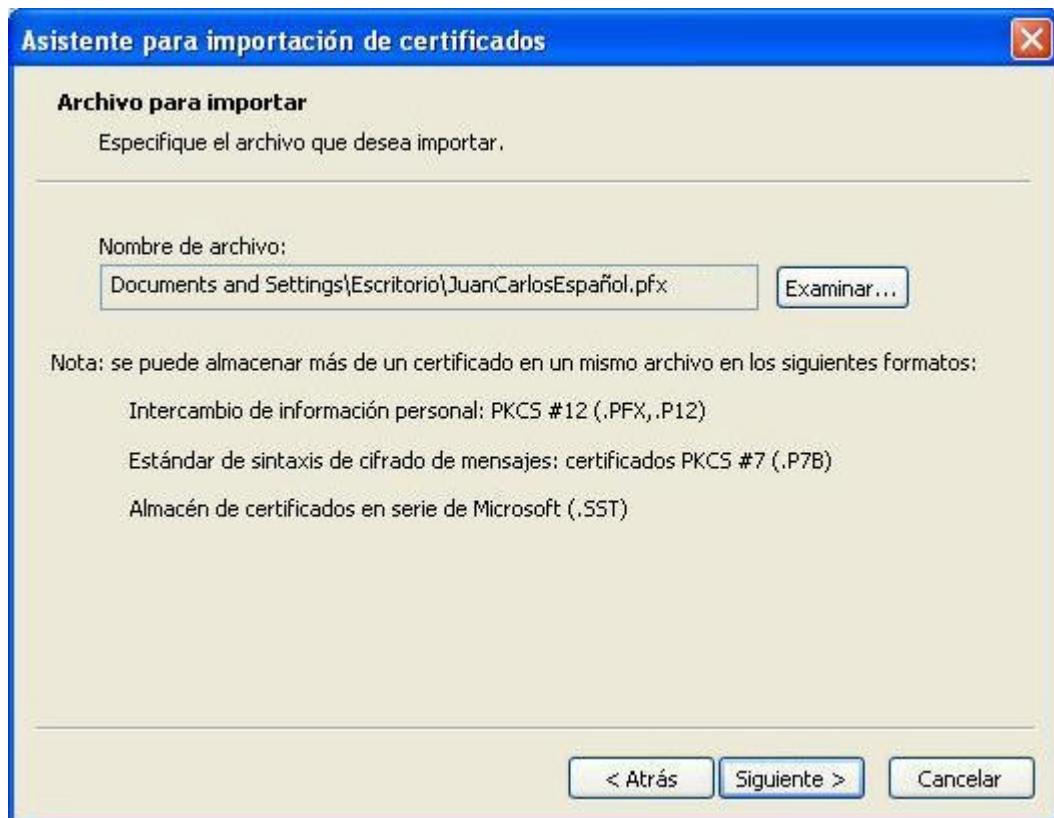


Figura 71: Selección de fichero.

Si pulsamos el botón de ‘**Examinar**’ en la ventana de selección de fichero podemos seleccionar, además del nombre del fichero a abrir, varios formatos de almacenamiento. Para certificados que hayan sido exportados a fichero desde *Microsoft Internet Explorer*, el formato por defecto será **.pfx**. Dicho formato no es el que aparece seleccionado en el navegador de ficheros (aparecen **.p12** y **.cer**, usados en *Netscape*), por lo que deberemos indicarle el adecuado. Si no lo hacemos, no se mostrarán en pantalla y podríamos pensar que el sistema no los está reconociendo. Si el certificado fue exportado a fichero desde *Netscape Navigator*, el formato será **.cer**. *Microsoft Internet Explorer* reconoce también esos ficheros, permitiéndonos importarlos a un nuevo almacén siguiendo el mismo proceso que estamos detallando. No existe diferencia a la hora de realizarlo.

Cuando hayamos seleccionado el fichero que vamos a importar, pulsaremos el botón ‘**Siguiente**’ para continuar con el proceso.



El siguiente paso será verificar que tenemos acceso al fichero de certificado. Para ello introduciremos la contraseña que se utilizó a la hora de exportar el certificado al fichero. Si no la conocemos será imposible realizar la importación, ya que no tendremos acceso a las claves almacenadas en él.

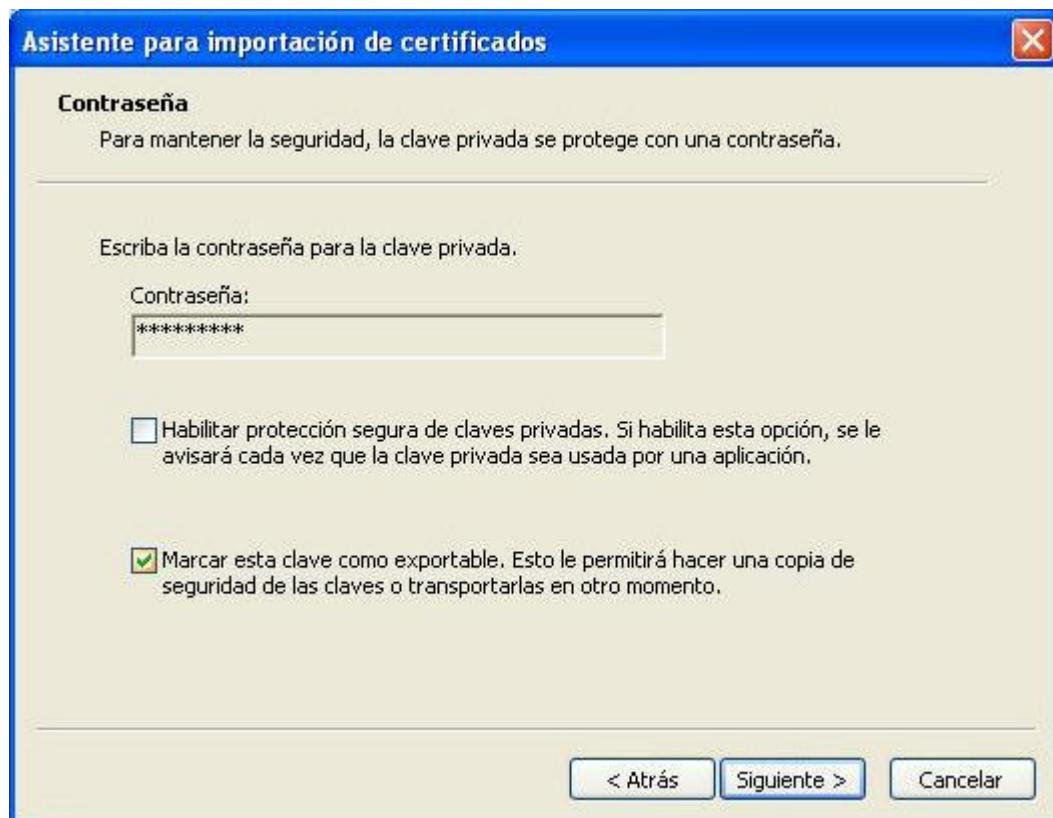


Figura 72: Presentación de la contraseña.

En esta pantalla podemos ver que hemos marcado el cuadro de ‘**Marcar esta clave como exportable**’. Esto será imprescindible si queremos importar el certificado a la tarjeta FNMT-RCM, ya que permite almacenar la clave privada en la tarjeta. Si simplemente quisiésemos instalar el certificado en el sistema, dejaríamos sin marcar ninguna de las dos casillas.

Una vez indicada la contraseña y marcada la casilla adecuada, pasaremos al siguiente paso de la importación, en el que deberemos seleccionar el almacén donde queremos guardar el certificado.



Hay dos tipos de almacenes de certificados: **lógicos** y **físicos**. Para ver todos los almacenes en los que el sistema nos va a permitir importar el certificado, deberemos pulsar el botón ‘**Examinar**’.



Figura 73: Selección de almacén de certificados.

Al examinar los almacenes disponibles, aparecerá una lista con todos ellos y una casilla sin marcar cuyo texto dice “**Mostrar almacenes físicos**”. Si nuestra intención es guardar el certificado en la tarjeta FNMT-RCM debemos marcar esa casilla. Entonces aparecerán más almacenes posibles. El que debemos seleccionar será el de **Tarjeta CERES**, situado en la carpeta **Personal**.



Figura 74: Selección de almacén tarjeta FNMT-RCM.



Cuando hayamos seleccionado el almacén de la tarjeta CERES, pasaremos a realizar la importación del certificado.

Al pulsar el botón ‘Siguiente’, el sistema comenzará con la importación al almacén seleccionado. Cuando el sistema detecta que estamos intentando almacenar un certificado en un determinado almacén, aparecerá en pantalla un mensaje que nos preguntará si queremos realizar la importación sobre la tarjeta FNMT-RCM. Si habíamos seleccionado como almacén físico de destino el de **Tarjeta CERES**, podremos pulsar el botón de “Sí” y la operación seguirá su curso.



Figura 75: Confirmación de importación a tarjeta.

En caso de que no hayamos seleccionado dicho almacén o no hayamos seguido los pasos anteriores, marcando las casillas de exportar clave privada, etc., debemos pulsar en “No”. De lo contrario aparecerá en pantalla un mensaje indicándonos que la importación no ha podido ser realizada.



Figura 76: Confirmación de importación a tarjeta.



Si el proceso se desarrolla correctamente, la aplicación deberá acceder a la tarjeta para crear en ella las claves y los objetos necesarios para importar el certificado. En caso de que no tengamos insertada la tarjeta o que por algún motivo la comunicación con el lector no funcione correctamente, la librería nos mostrará en pantalla un mensaje de error y la operación se detendrá.



**Figura 77:** Error en la comunicación con la tarjeta FNMT-RCM.

Si el sistema ha podido conectar con la tarjeta, nos solicitará su PIN para así poder comenzar a crear los objetos necesarios.



**Figura 78:** Error al acceder al almacén de certificado.

Si introducimos el PIN correctamente el certificado quedará almacenado en la tarjeta. Además se instalará en el registro para su posterior uso, siempre y cuando se utilice junto con la tarjeta, que es donde habrán quedado almacenadas las claves.



**Figura 79:** Importación correcta.



### 13.2 Importación mediante CeresImportCertificate.

Además de la exportación por medio de los navegadores de Internet, existe una aplicación que nos permitirá almacenar en la tarjeta un certificado software: **CeresImportCertificate**. Dicha aplicación es un asistente que nos guiará paso a paso durante la importación a la tarjeta del certificado.

Inicialmente nos muestra una ventana con información sobre el proceso que vamos a seguir, además de información adicional sobre qué es un certificado digital, su utilidad y las ventajas de almacenarlo en tarjeta inteligente. Despues nos indicará los pasos que debemos ir cumpliendo para realizar correctamente la importación.



Figura 80: presentación de CeresImportCertificate.



La segunda pantalla del asistente nos va a solicitar la ruta en la que se encuentra el archivo **pfx** o **p12** en el que está almacenado el certificado que queremos importar a la tarjeta. Dicho archivo se habrá generado mediante una operación previa de exportación, realizada desde el navegador **Microsoft Internet Explorer** o desde **Netscape Navigator**. En capítulos anteriores vimos cómo se realiza dicha exportación a fichero, por lo que para cualquier duda puede remitirse al apartado **12.1**.

La ventana de selección de fichero contiene un botón “**Examinar**” que nos permite navegar a través del explorador de archivos hasta encontrar la ruta adecuada. De esta manera evitaremos tener que escribir la ruta completa.

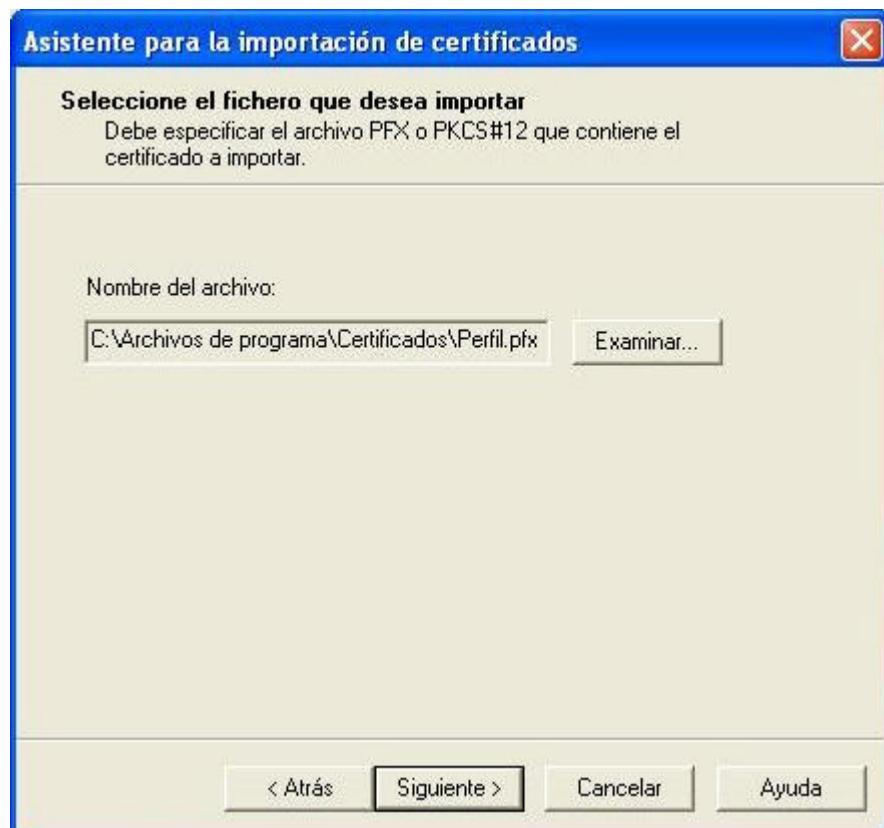


Figura 81: Selección de fichero para importación.

En caso de que el fichero no se encuentre en la ruta especificada o esté dañado, se nos mostrará un mensaje en pantalla en el que nos informará de esa situación.



Figura 82: Error en la búsqueda del fichero.



Una vez indicada la ruta al fichero, el asistente nos solicitará la contraseña para acceder al certificado. Dicha clave se la asigna el usuario al fichero en el momento de exportarlo desde el navegador hacia el archivo **pfx**. Sin ella será imposible realizar la importación a la tarjeta ya que no se tendrá acceso a las claves del certificado.

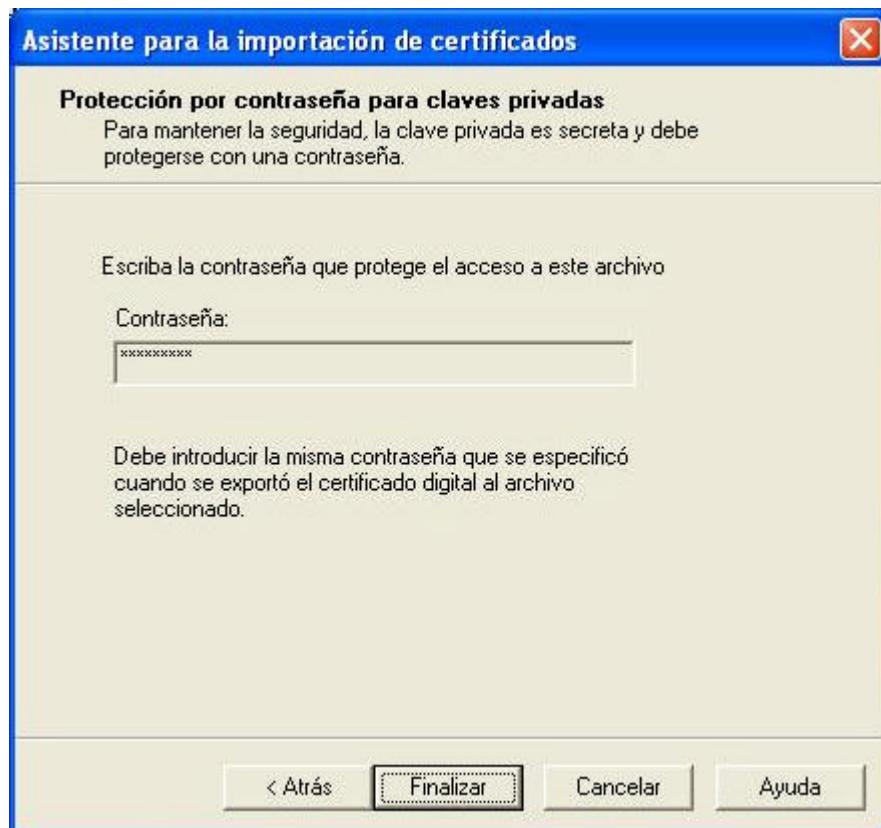


Figura 83: presentación de la contraseña del certificado.

Cuando tecleemos la contraseña y tengamos introducida la tarjeta en el lector, podremos pulsar el botón de “Finalizar” para que comience la importación a la tarjeta. Lo primero que hará la aplicación es comprobar que la contraseña es correcta e intentar obtener las claves del certificado software. Si no lo fuese, el asistente nos mostrará un mensaje de error.



Figura 84: Error en la presentación de la contraseña.



Una vez verificada la contraseña, se extraen las claves del certificado y se intentarán importar a la tarjeta inteligente. En caso de que hayamos olvidado introducir la tarjeta, aparecerá un mensaje de error avisándonos de ello.

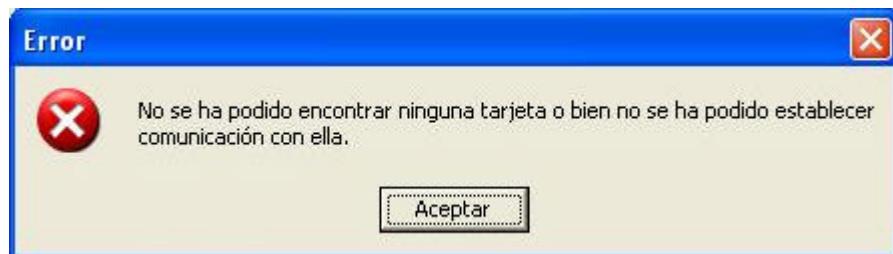


Figura 85: Error en la importación a la tarjeta.

Cuando tengamos la tarjeta introducida en el lector, comenzará la importación del certificado software. Para poder acceder a la tarjeta, el asistente nos solicitará que insertemos el PIN. De esta manera quedaremos autenticados contra ella y tendremos acceso a la creación de objetos.



Figura 86: solicitud de autenticación de la tarjeta.

Si todo ha ido correctamente, el certificado quedará almacenado en la tarjeta y será idéntico al software, pero con las ventajas añadidas de guardarla en un soporte hardware.

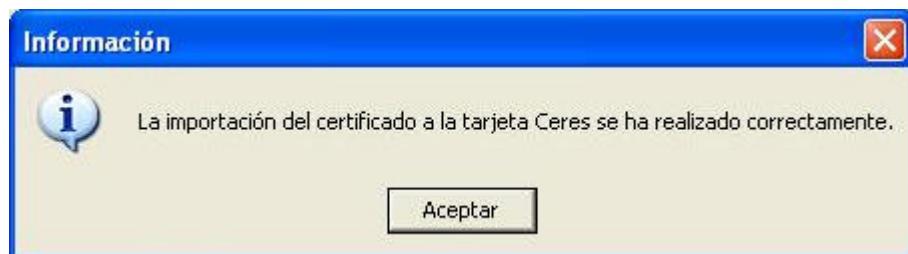


Figura 87: Proceso de importación completado correctamente.



### 13.3 Importación mediante Netscape Navigator.

La importación de certificados en *Netscape* nos permite, al igual que con *Microsoft Internet Explorer*, importar el certificado tanto a la tarjeta como a la base de datos de la aplicación. La principal diferencia entre ambas aplicaciones es que en *Netscape* para utilizar el certificado no necesita estar instalado previamente, sino que basta con tenerlo en la tarjeta inteligente. Con *Microsoft* no ocurría esto y por eso debía ser instalado en el registro de sistema, permitiendo así que las aplicaciones pudiesen acceder a él.

Para importar certificados debemos acceder al módulo de seguridad (botón “**Security**”), tal y como se hacía en la exportación (ver apartado 12.2).



Figura 88: Pantalla de Seguridad en Netscape Navigator.

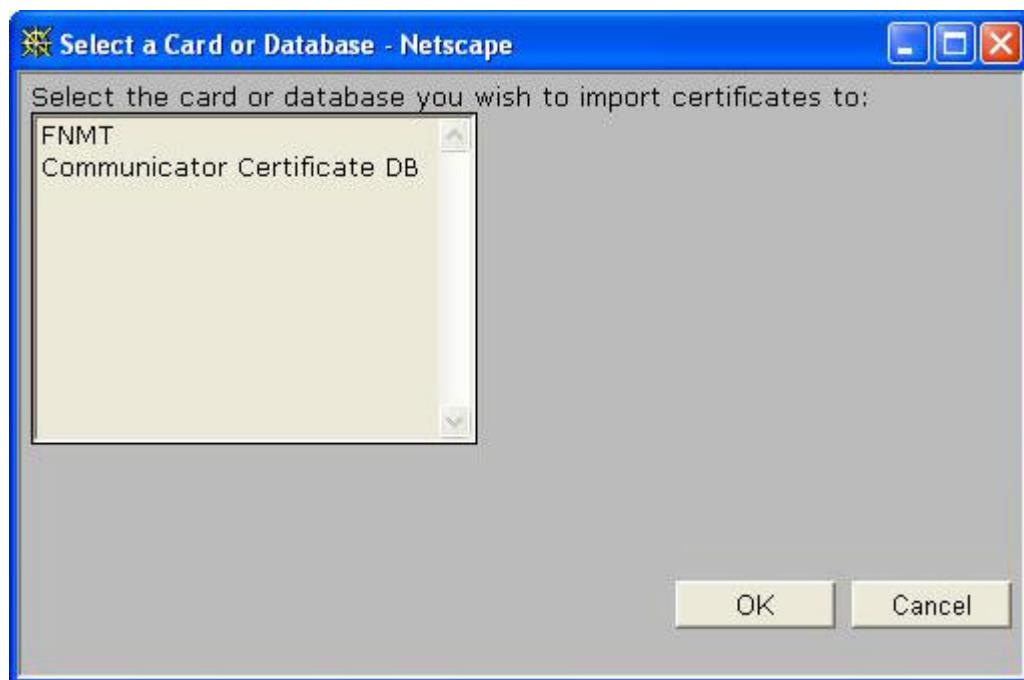
En la parte inferior de la pantalla podemos ver el botón ‘**Import a Certificate...**’, que es el que nos interesa. El proceso es similar al de *Microsoft*, pero algo más sencillo, como veremos a continuación. La única diferencia es que al importar con *Microsoft* el certificado importado quedaba instalado en el registro y, si queríamos, también almacenado en la tarjeta. Con *Netscape* elegiremos el destino del certificado, que podrá ser un dispositivo o la propia base de datos de la aplicación.

Además de esto hay que indicar que el formato de archivos de importación que soporta *Netscape* es **.p12**, que sigue la recomendación **PKCS#12** para la sintaxis del intercambio de información personal.



Cuando comencemos el proceso de importación del certificado, Netscape nos pedirá que indiquemos el destino de la importación. Como hemos comentado antes, podemos instalarlo en la base de datos de la aplicación o en cualquier dispositivo que esté correctamente instalado mediante su *módulo criptográfico* (ver apartado **10.1.2** para obtener información sobre la instalación del módulo criptográfico de la FNMT-RCM).

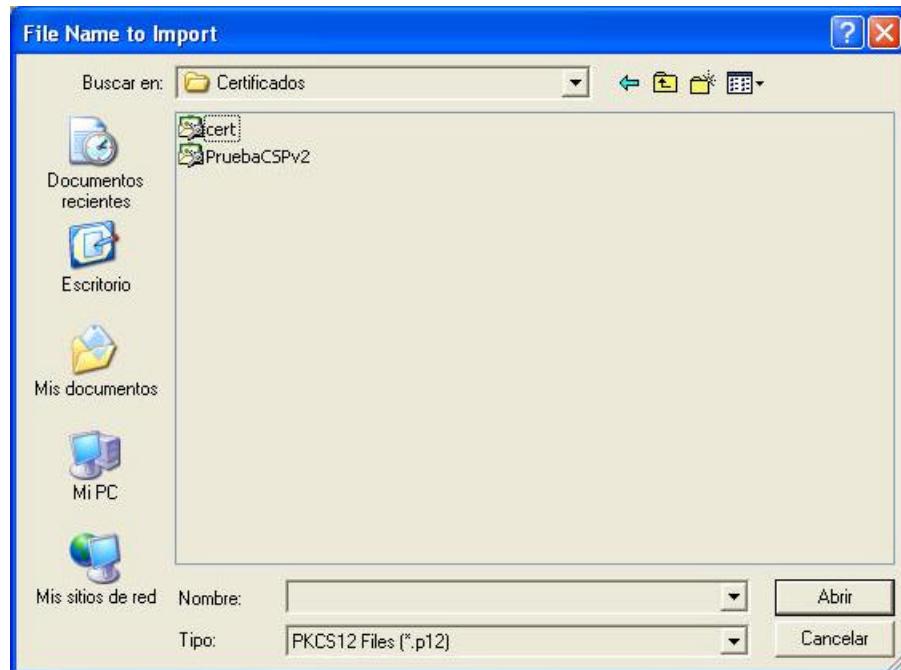
En nuestro caso, para importarlo a la tarjeta seleccionaremos la entrada indicada como **FNMT** que aparece en el cuadro de la siguiente figura. Si luego quisiésemos instalarlo en la base de datos genérica habría que repetir la operación de nuevo, pero indicando que la importación se haga sobre “**Communicator Certificate DB**”.



**Figura 89:** Selección de destino de la importación.



Una vez seleccionado el destino de la importación, Netscape nos solicitará la ruta y el nombre del archivo que contiene el certificado. Para ello mostrará la habitual ventana de selección de carpetas, donde podremos buscarlo fácilmente.



**Figura 90:** Búsqueda del fichero de importación.

Después *Netscape* nos pedirá la contraseña que protege el certificado. Ya sabemos que sin esa contraseña sería imposible recuperarlo.



**Figura 91:** Solicitud de contraseña para la importación.

Cuando introduzcamos la contraseña, la aplicación intentará obtener las claves del fichero. Si la contraseña no es correcta, nos avisará.



**Figura 92:** Solicitud de contraseña para la importación.



Al finalizar la importación, *Netscape* nos mostrará un mensaje informándonos si la operación se ha realizado correctamente. En la ventana de los certificados actuales veremos cómo aparece una nueva entrada con el nombre del nuevo certificado que acabamos de importar, precedido del nombre del dispositivo en el que se encuentra (si no es la base de datos de *Netscape*).



Figura 93: Confirmación de la importación correcta.

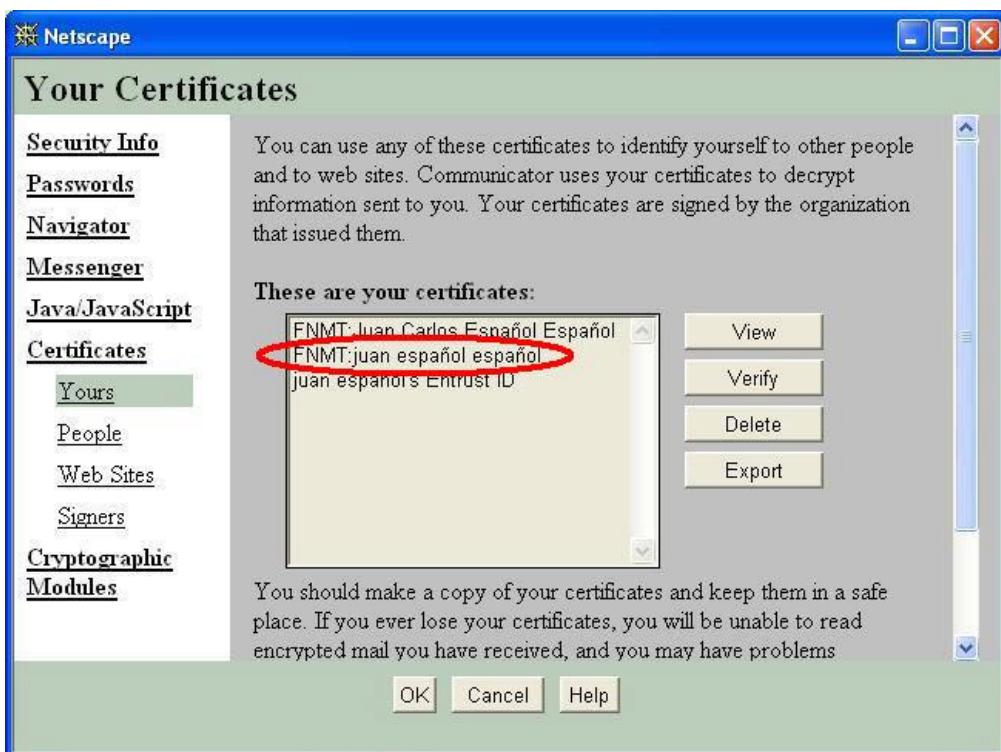


Figura 94: Nuevo certificado importado al sistema.

Si quisieramos importar un certificado a la tarjeta y ésta ya estuviese llena, el navegador nos mostraría un mensaje como el de la siguiente figura para informarnos de ello.



Figura 95: Nuevo certificado importado al sistema.



## 13.4 Importación mediante Mozilla FireFox.

### 13.4.1 Proceso previo: Instalación del módulo criptográfico:

El instalable actual no automatiza la configuración del navegador FireFox, por lo que se ha de realizar manualmente. El proceso es sencillo:

En tramos en las opciones del navegador:

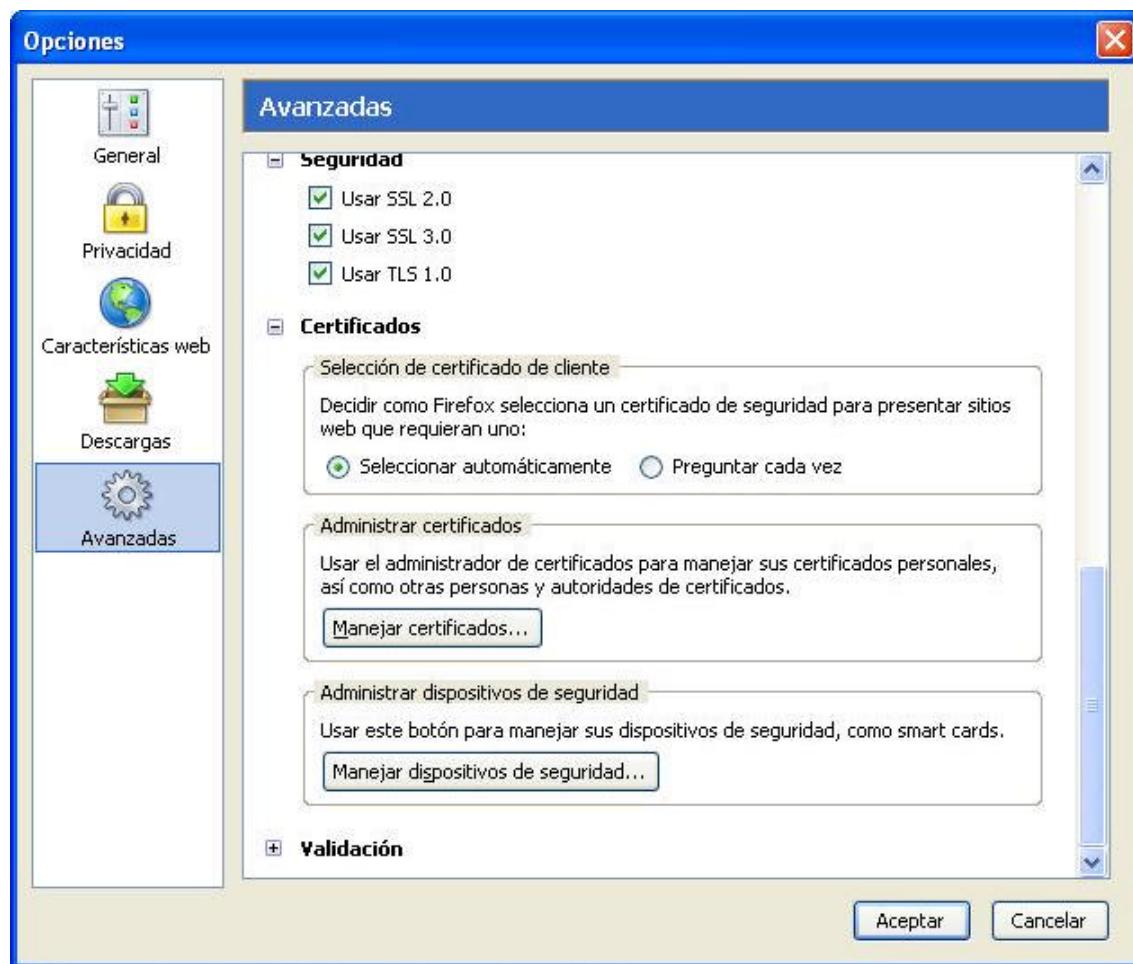


Figura 96: Fichas de opciones de FireFox.

Pulsamos la opción de “Manejar dispositivos de seguridad”, para añadir el driver PKCS#11 de la FNMT-RCM:

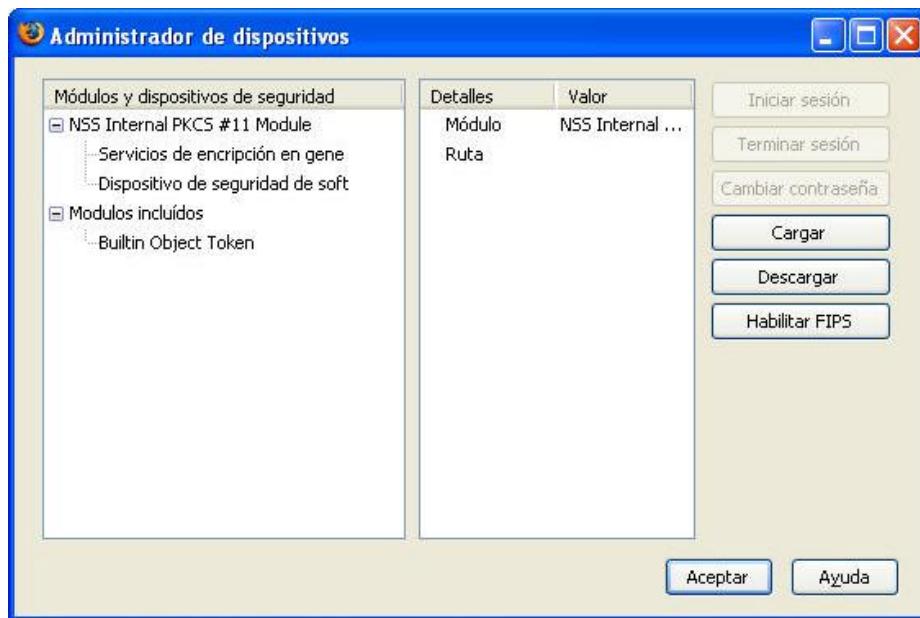


Figura 97: Módulos de seguridad instalados por defecto.

Pulsamos el botón “Cargar”, para añadir la Dll cabecera del driver, de nombre: PkcsV2GK.dll

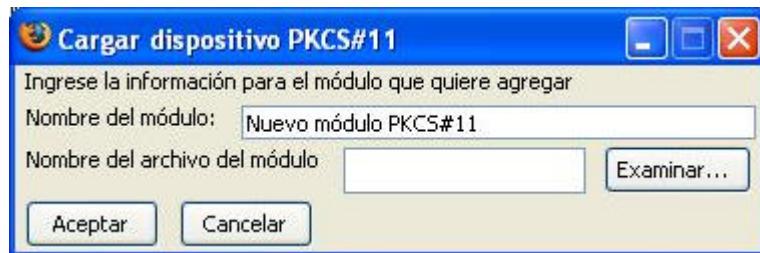


Figura 98: Añadir nuevo módulo de seguridad.

Rellenamos los campos:

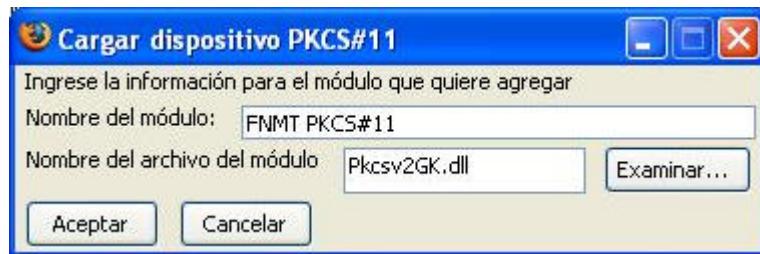
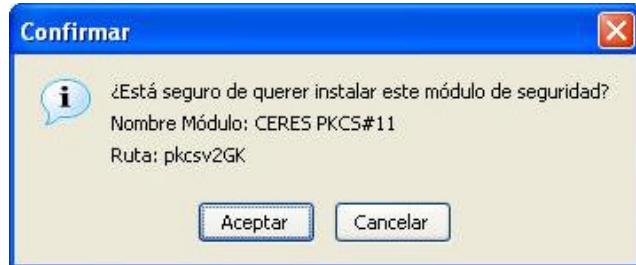


Figura 99: Añadir módulo de seguridad de la FNMT.

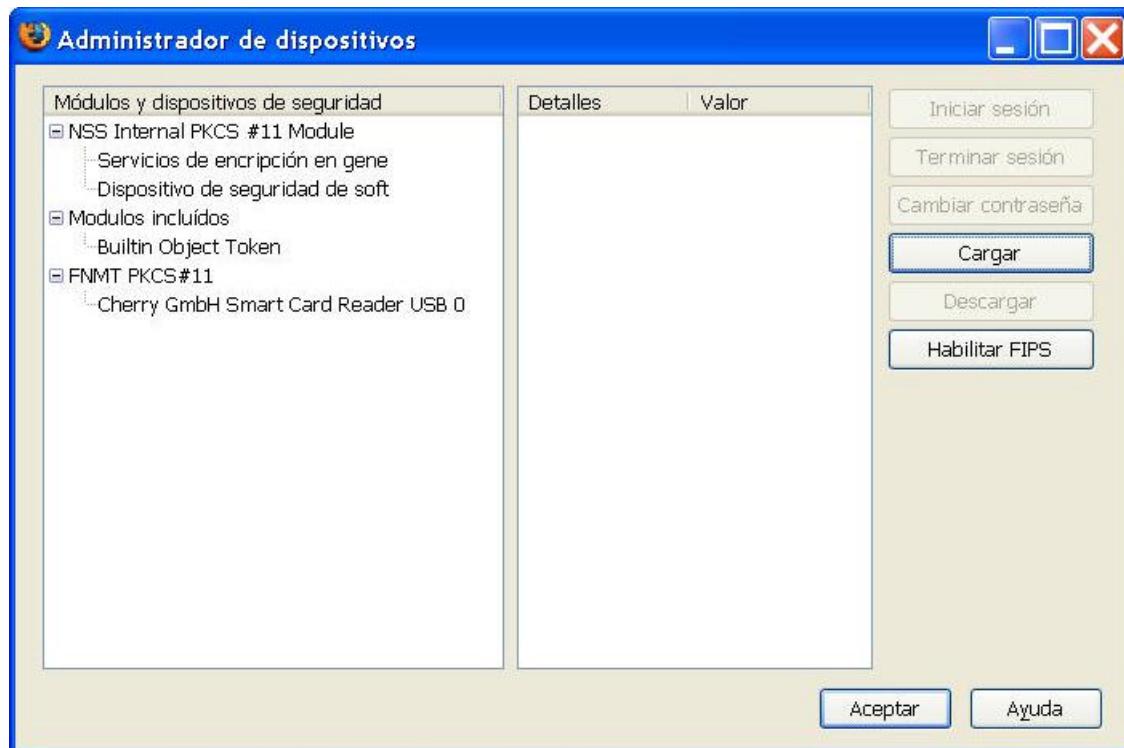


Aceptamos la confirmación que se nos solicita:



**Figura 100:** Confirmación a añadir un nuevo módulo de seguridad.

El resultado final es que el navegador dispone de un nuevo módulo criptográfico, que le permitirá acceder a la tarjeta de la FNMT:



**Figura 101:** Nuevo módulo de seguridad ya instalado.

En la imagen presentada se ve que el lector instalado en la máquina es de la marca Cherry, con conexión USB.



### 13.4.2 Importación de certificados en FireFox

La importación de certificados en **FireFox** nos permite, al igual que con *Microsoft Internet Explorer*, importar el certificado tanto a la tarjeta como a la base de datos de la aplicación. La principal diferencia entre ambas aplicaciones es que en **FireFox** para utilizar el certificado no necesita estar instalado previamente, sino que basta con tenerlo en la tarjeta inteligente. Con Microsoft no ocurría esto y por eso debía ser instalado en el registro de sistema, permitiendo así que las aplicaciones pudiesen acceder a él.

Para importar certificados debemos acceder al módulo de seguridad (botón “**Avanzadas**”) y bajar con la barra de desplazamiento hasta visualizar lo mostrado en la imagen:

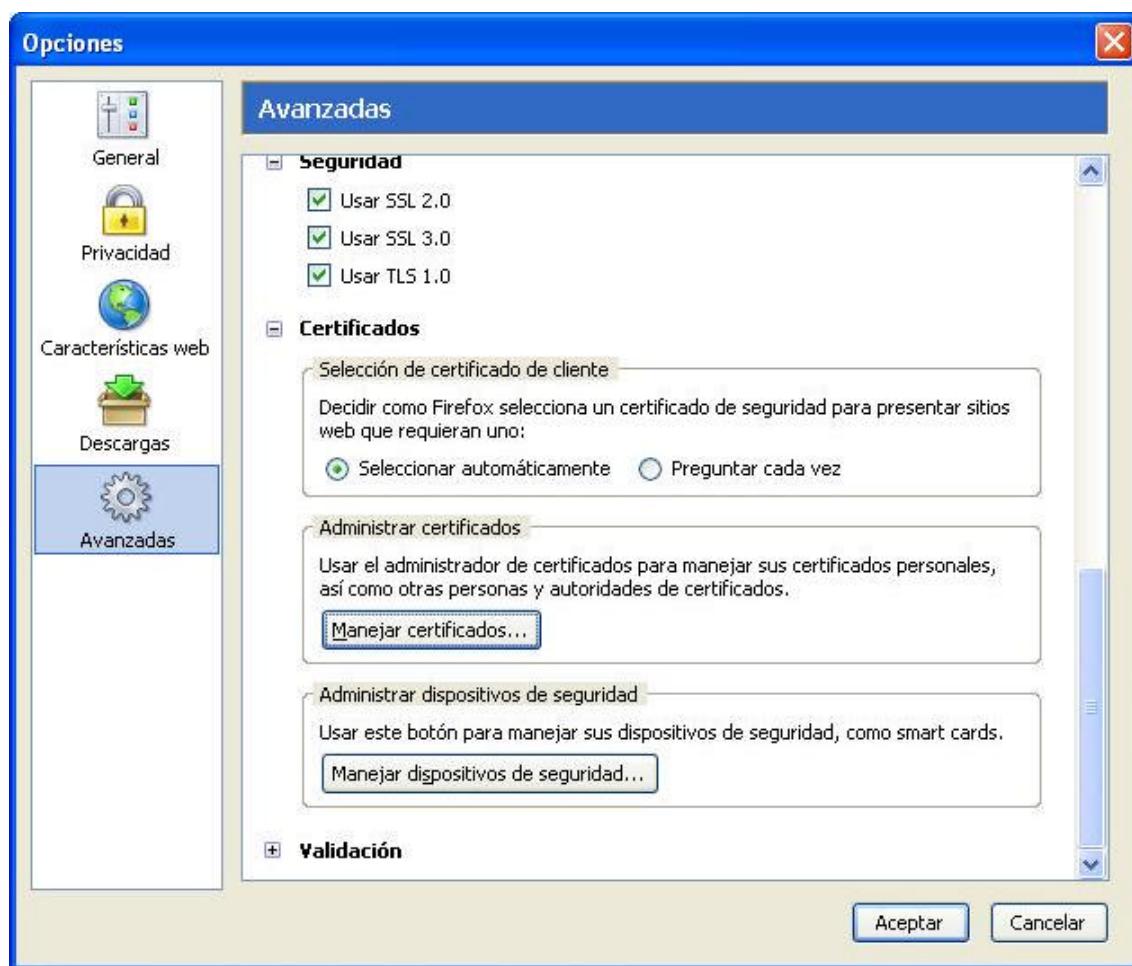


Figura 102: Pantalla de Seguridad en FireFox.

En la parte inferior de la pantalla podemos ver el botón ‘**Manejar certificados...**’, que es el que nos interesa. Con FireFox elegiremos el destino del certificado, que podrá ser un dispositivo o la propia base de datos de la aplicación.



Además de esto hay que indicar que el formato de archivos de importación que soporta Netscape es **.p12**, que sigue la recomendación **PKCS#12** para la sintaxis del intercambio de información personal.

Cuando comencemos el proceso de importación del certificado, **FireFox** nos pedirá que indiquemos el destino de la importación. Como hemos comentado antes, podemos instalarlo en la base de datos de la aplicación o en cualquier dispositivo que esté correctamente instalado mediante su *módulo criptográfico* (ver apartado **10.1.2** para obtener información sobre la instalación del módulo criptográfico de la FNMT-RCM).

En nuestro caso, para importarlo a la tarjeta seleccionaremos la entrada indicada como **V.2.1** que aparece en el cuadro de la siguiente figura. Si luego quisiésemos instalarlo en la base de datos genérica habría que repetir la operación de nuevo, pero indicando que la importación se haga sobre ‘**Dispositivo de seguridad de Soft**’.



**Figura 103:** Selección de destino de la importación.



Una vez seleccionado el destino de la importación, **FireFox** nos solicitará la ruta y el nombre del archivo que contiene el certificado. Para ello mostrará la habitual ventana de selección de carpetas, donde podremos buscarlo fácilmente.

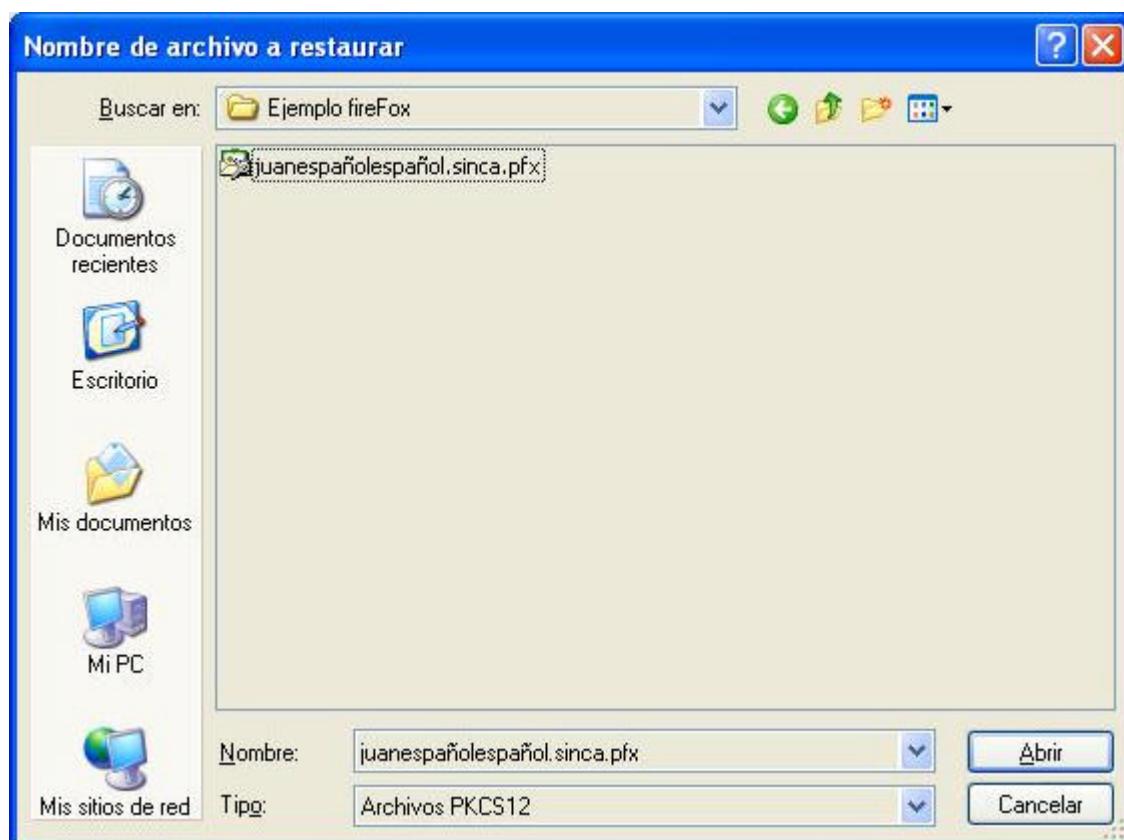
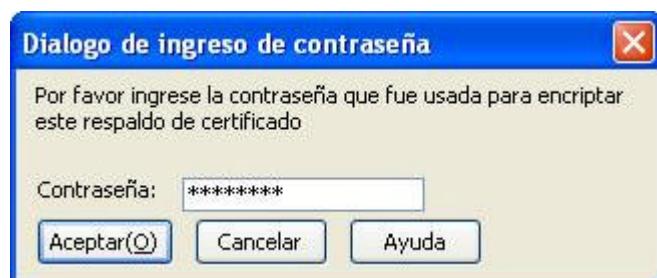


Figura 104: Búsqueda del fichero de importación.

Después **FireFox** nos pedirá la contraseña que protege el certificado. Ya sabemos que sin esa contraseña sería imposible recuperarlo.





**Figura 105:** Solicitud de contraseña para la importación.

Cuando introduzcamos la contraseña, la aplicación intentará obtener las claves del fichero. Si la contraseña no es correcta, nos avisará.



**Figura 106:** Solicitud de contraseña para la importación.

Después **FireFox** nos pedirá la contraseña que protege el token.



**Figura 107:** Solicitud de contraseña para el token.

Al finalizar la importación, *Netscape* nos mostrará un mensaje informándonos si la operación se ha realizado correctamente. En la ventana de los certificados actuales veremos cómo aparece una nueva entrada con el nombre del nuevo certificado que acabamos de importar, precedido del nombre del dispositivo en el que se encuentra (si no es la base de datos de *Netscape*).



**Figura 108:** Confirmación de la importación correcta.



**Figura 109:** Nuevo certificado importado al sistema.

Si quisiéramos importar un certificado a la tarjeta y ésta ya estuviese llena, el navegador nos mostraría un mensaje de error.



## Capítulo 14

### *Correo seguro*





## 14 CORREO SEGURO.

Hay aplicaciones de correo que permiten enviar y recibir correos cifrados y firmados digitalmente utilizando criptografía. Estas operaciones garantizan el intercambio seguro de información, proporcionando autenticación del emisor, integridad del mensaje, no repudio del origen, etc. En los siguientes apartados explicaremos detenidamente cómo tener correo seguro usando la tarjeta FNMT-RCM en los clientes de correo de Microsoft y de Netscape.

### 14.1 Correo seguro con Microsoft Outlook Express.

El intercambio seguro de información se basa en el uso de las claves públicas y privadas de usuarios. Las claves públicas son accesibles a todo el universo de usuarios y se envían junto con el certificado digital. En cambio las claves privadas son secretas y no pueden ser extraídas de la tarjeta.

*Outlook Express* utiliza CryptoAPI, con lo que para realizar operaciones criptográficas usará la librería **CeresCSP.dll**. Para utilizar todas las posibilidades del correo seguro entre dos usuarios es necesario que cada uno tenga el certificado del otro con sus claves públicas. La manera de obtenerlo es recibiendo un mensaje firmado, quedando así registrado en la libreta de direcciones.

#### 14.1.1 Añadiendo un certificado a la cuenta.

Antes de poder enviar un correo firmado debemos indicarle a la aplicación de correo qué certificado queremos asociar a nuestra cuenta. Hemos comentado en apartados anteriores que era necesario que la dirección de correo electrónico asociada al certificado fuese la que quisiésemos utilizar como cuenta de correo habitual. Para asociar el certificado con nuestra cuenta de correo debemos ir al menú **Herramientas**, y allí seleccionar la opción **Cuentas**.

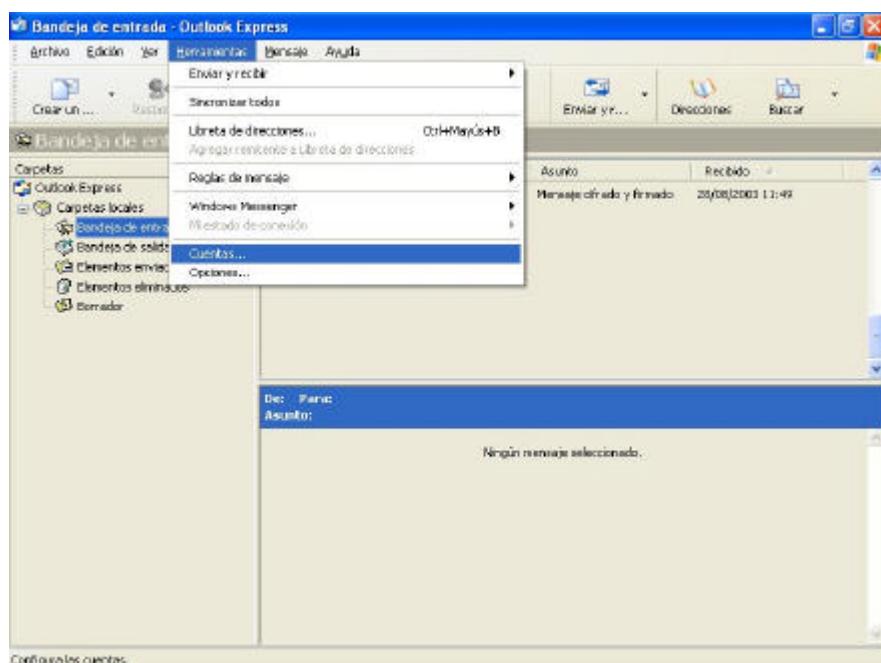




Figura 110: Cuentas de correo en Outlook Express.

Una vez seleccionada esa opción la aplicación de correo nos mostrará una ventana con las cuentas actuales del sistema. Ahí deberemos seleccionar nuestro servidor de correo y pulsar en el botón de Propiedades, desde donde pasaremos a configurar las opciones de seguridad.

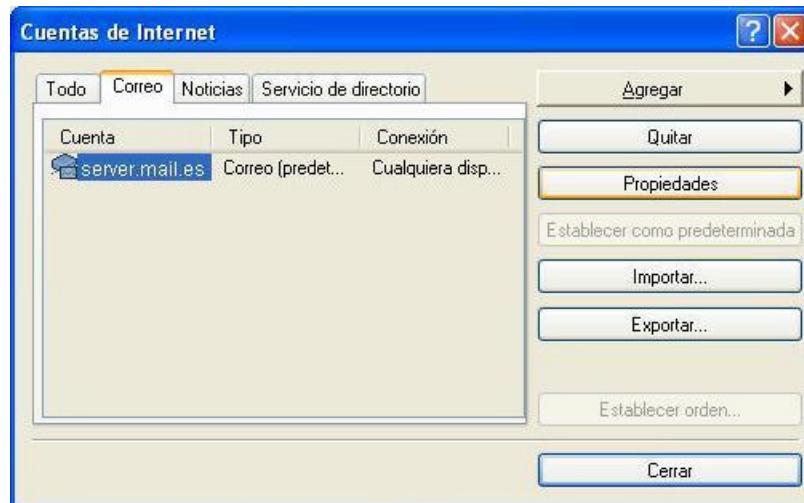


Figura 111: Cuentas de correo.

Ya dentro de las propiedades de la cuenta, si seleccionamos la solapa de **Seguridad** vemos que aparecen dos cuadros vacíos con la etiqueta de **Certificado** que indican el certificado que se usará para las operaciones de firma y de cifrado digital.





Figura 112: Certificados actuales asociados a la cuenta de correo.

Pulsando en los botones de **Seleccionar** pasaremos a la ventana de selección de certificados. Aquí se muestran los certificados instalados en el sistema y que tienen como dirección de correo asociada aquella que nosotros estamos utilizando. Puede que tengamos otros instalados y sin embargo no aparezcan en esta ventana. Será debido a que su dirección de correo es diferente.



Figura 113: Certificados asociados a la cuenta actual de correo.

Una vez tengamos seleccionado el certificado a utilizar, volveremos a la pantalla anterior y pulsaremos el botón de **Aplicar** para que los cambios tengan efecto. Ahora en los cuadros de texto que antes aparecían vacíos se mostrará el certificado que se va a usar en esa cuenta. Una vez asignada la identidad con la que vamos a realizar las operaciones criptográficas, podremos comenzar a enviar mensajes firmados digitalmente.



#### 14.1.2 Firma y verificación de mensajes.

Para realizar una **firma** digital, el usuario utilizará su **clave privada** que se encuentra almacenada, junto con el resto de componentes del perfil criptográfico, en la tarjeta FNMT-RCM. Esa clave no puede ser extraída, por lo que no pueden existir copias de ella. Cuando queramos firmar un mensaje, la aplicación de correo nos solicitará la tarjeta cuyo número de serie coincida con el de aquella que contiene el certificado asociado a esa cuenta. Además, será necesario presentar el PIN de la tarjeta para acceder y utilizar la clave privada. De esta manera, si la tarjeta cayese en manos de otro individuo no podría realizar ninguna firma ya que no debería conocer su PIN.

Si queremos enviar un correo firmado a otro usuario, crearemos un nuevo mensaje de la forma habitual. Una vez que hayamos escrito el mensaje tenemos varias formas de indicar que queremos firmarlo. Podemos acceder al menú **Herramientas** y ahí seleccionar la opción **Firmar digitalmente**, o bien pulsar el botón **Firmar** de la barra de herramientas.

En la siguiente figura vemos un mensaje que va a ser firmado digitalmente utilizando el certificado que se seleccionó previamente para esa cuenta. En la imagen vemos que ha quedado pulsado el botón de **Firmar** y ha aparecido en la parte derecha un ícono mostrando un pequeño sello rojo, indicando que el mensaje va a ser firmado antes de ser enviado. Cuando finalicemos el mensaje lo enviaremos normalmente y la aplicación de correo se realizará las operaciones de firma.

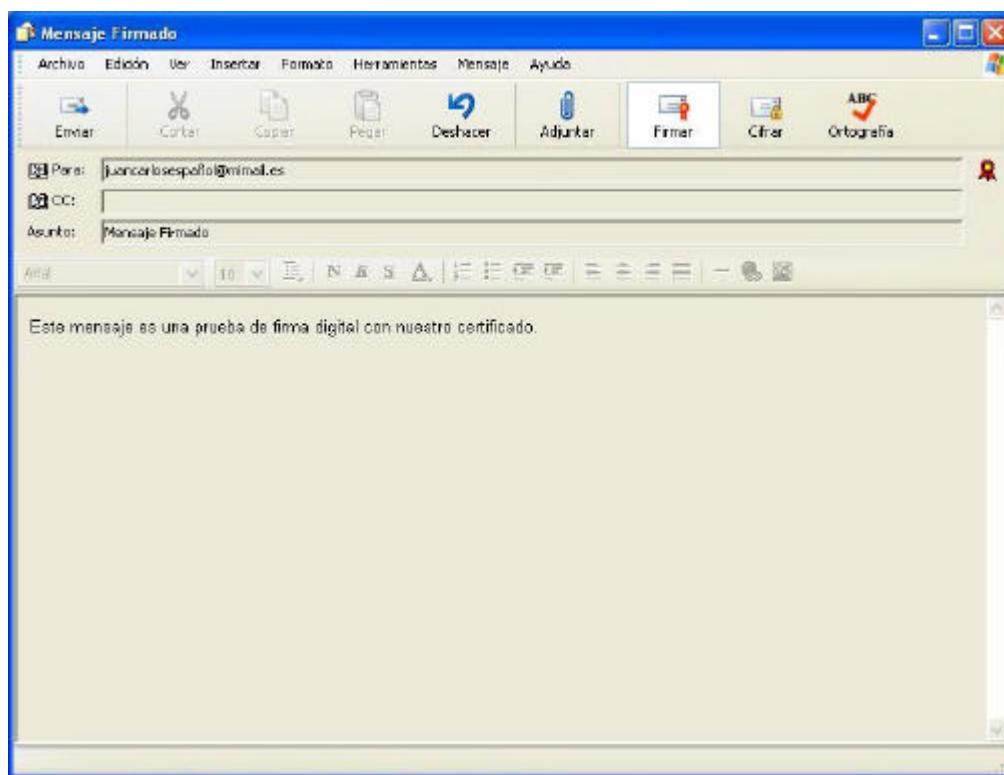


Figura 114: Mensaje firmado listo para ser enviado.



Como dijimos antes, para poder firmar digitalmente un mensaje es necesario usar nuestra clave privada, almacenada en la tarjeta, y presentar el PIN para tener acceso a ella. Por esto es imprescindible que la tarjeta que contiene el certificado se encuentre insertada en el lector. En caso de que no sea así aparecerá en pantalla una ventana solicitando la tarjeta correcta, cuyo **número de serie** debe coincidir con el indicado.



Figura 115: Solicitud de la tarjeta correcta.

Cuando la tarjeta esté disponible se solicitará su PIN. Será entonces cuando se realicen las operaciones de firma digital y se envíe el mensaje al destinatario, incluyendo el certificado del emisor.

En el cliente de correo del receptor aparecerá un nuevo mensaje con un ícono que indica que dicho mensaje está firmado digitalmente. Al incluirse el certificado en el propio mensaje, cuando lo abramos se usará para verificar la firma e indicarnos si es correcta o no.

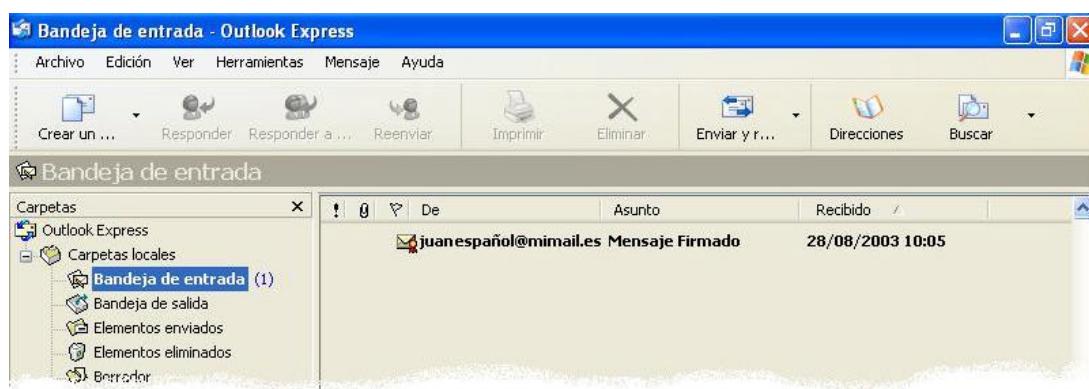


Figura 116: Cliente de correo en el que se muestra el mensaje firmado.



Si abrimos el mensaje firmado aparecerá una pantalla previa en la que *Outlook Express* nos indica que el mensaje ha sido firmado digitalmente. Tras pulsar el botón de “Continuar”, se usará el certificado para comprobar la autenticidad de la firma. Si puede verificar la firma recibida, el mensaje aparecerá normalmente. Si no, nos advertirá que no pudo ser verificada, aunque nos mostrará el texto del mensaje.

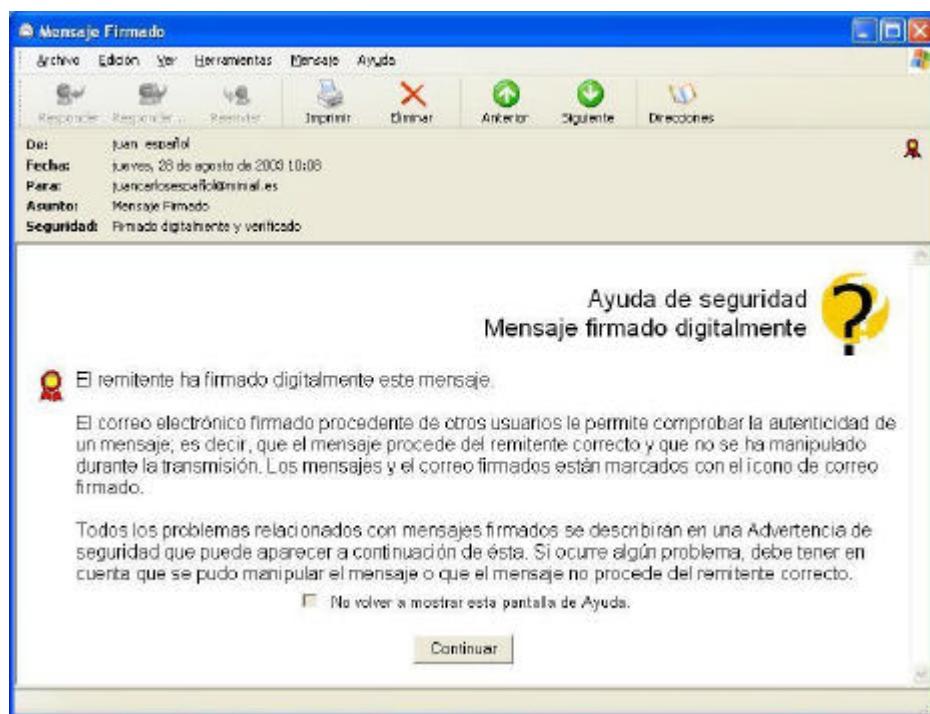


Figura 117: Aviso de correo FIRMADO.



#### 14.1.3 Cifrado y descifrado de mensajes.

Todo lo anterior era referente a la firma digital. Ahora comenzaremos con el **cifrado** y el **descifrado** de mensajes. Sabemos que para poder cifrar un mensaje debemos utilizar la clave pública del receptor. Esa clave pública se envía junto con el certificado, por lo que hasta que no lo tengamos no podremos enviarle un mensaje cifrado a ese usuario.

Una manera de obtener el certificado del receptor es recibir previamente un mensaje firmado por él y que lo incluya. De esta manera al añadirse a nuestra libreta de contactos, quedará reflejado el certificado asociado a ese usuario y que se usará para las operaciones criptográficas que lo requieran.

Cuando queramos cifrar un mensaje actuaremos normalmente, pero antes de enviarlo pulsaremos el botón de **Cifrar**, o bien lo indicaremos desde el menú de **Herramientas** del mensaje.

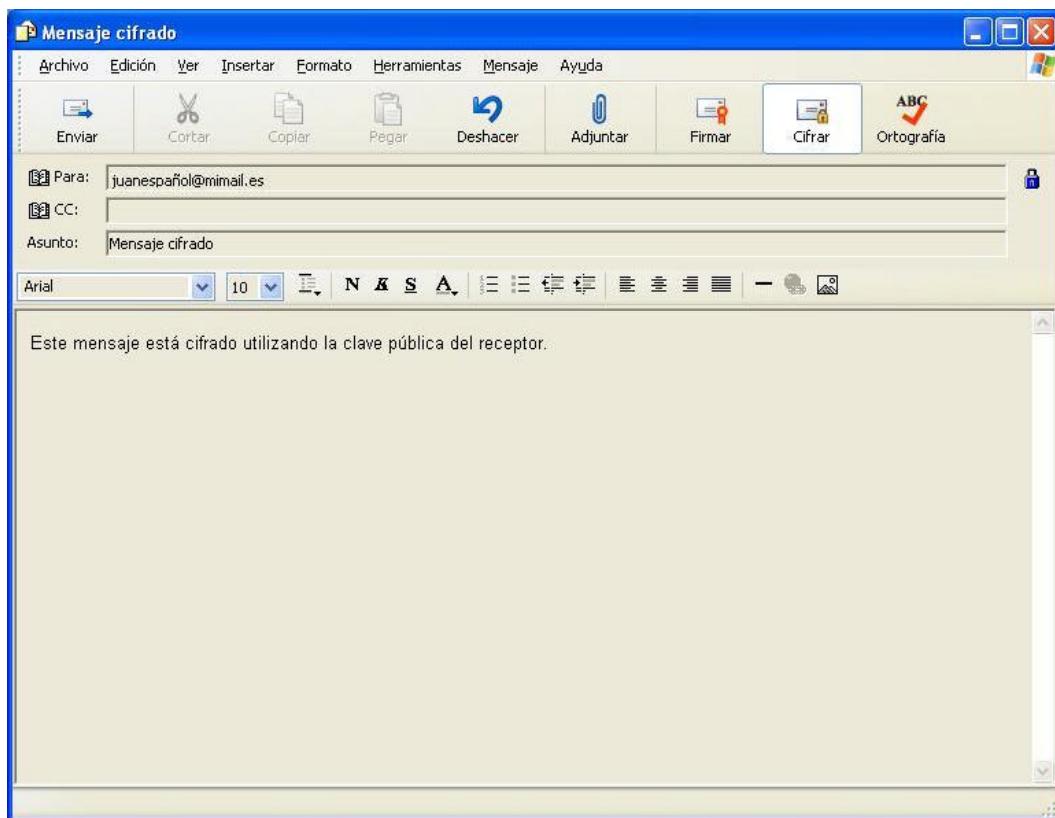


Figura 118: Mensaje marcado para cifrar.

En el mensaje aparecerá un pequeño ícono de un *candado* en la parte derecha que indica que al enviar se va a realizar el cifrado del mensaje. Al contrario que con la firma



digital, ahora no es necesario tener insertada nuestra tarjeta inteligente ya que la clave que se va a usar es la del certificado del receptor.

Cuando el receptor del mensaje reciba el correo cifrado, le aparecerá marcado con el icono correspondiente.

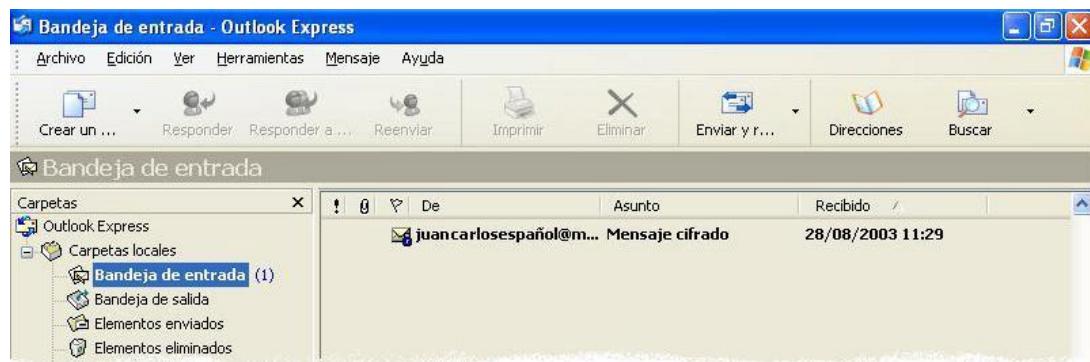


Figura 119: Cliente de correo en el que se muestra el mensaje cifrado.

Cuando se abra el mensaje nos aparecerá una advertencia indicándonos que ese mensaje está cifrado.

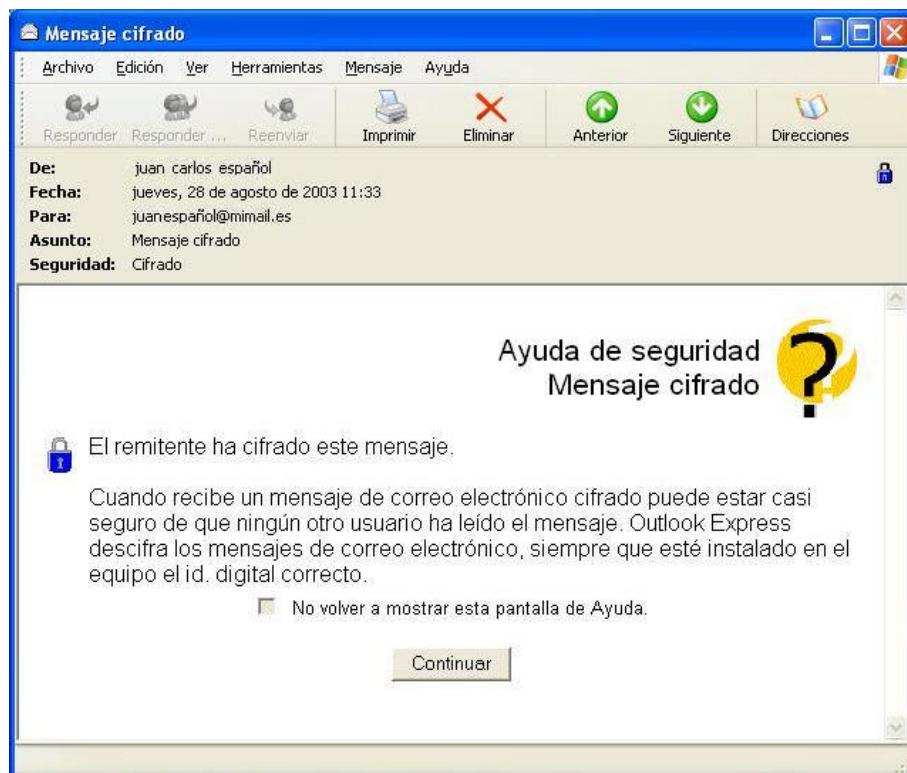


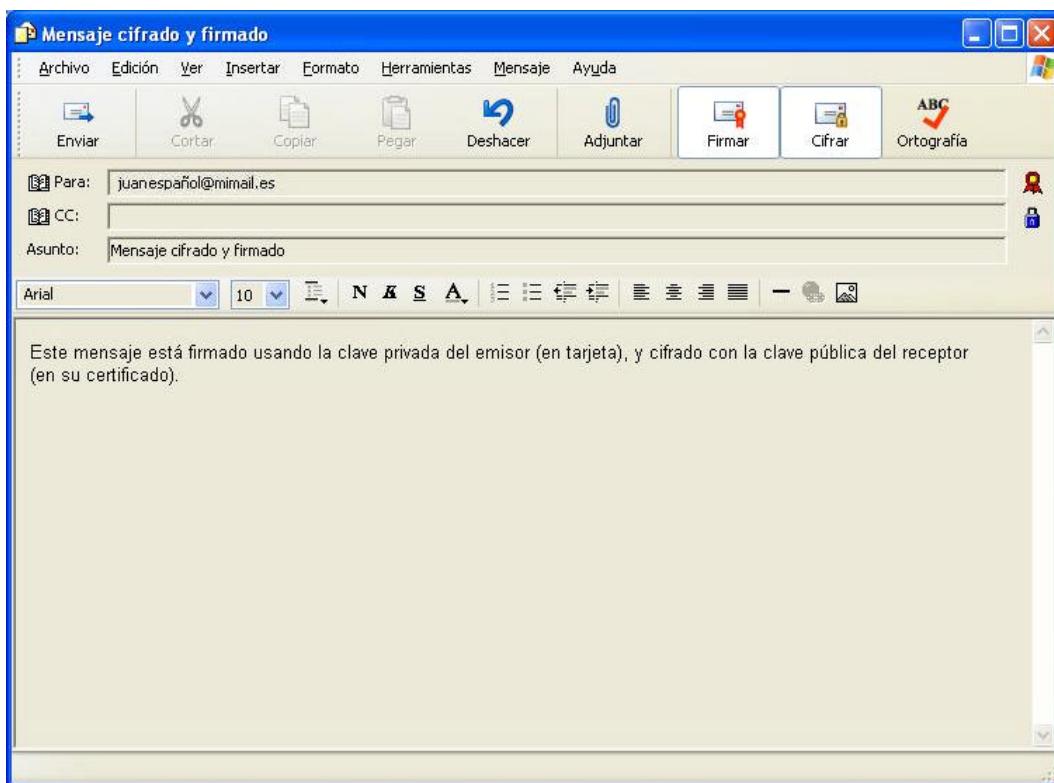
Figura 120: Aviso de correo CIFRADO.

Para poder abrirlo necesitaremos nuestra tarjeta FNMT-RCM en la que se encuentra nuestra **clave privada**, necesaria para descifrar el mensaje. Si no estuviera insertada,

aparecería una ventana solicitando la tarjeta cuyo número de serie corresponda con la asociada al certificado.

Cuando queramos enviar un correo que esté a la vez **cifrado y firmado** realizaremos las mismas operaciones descritas anteriormente. Al realizarse una operación de firma digital y otra de cifrado, será necesario tener insertada la tarjeta con nuestra clave privada y además tener instalado el certificado del receptor del mensaje.

Antes de enviar el correo pulsaremos los botones de **Firmar** y **Cifrar**, mostrándose en este caso los iconos de las dos operaciones.



**Figura 121:** Mensaje cifrado y firmado digitalmente.

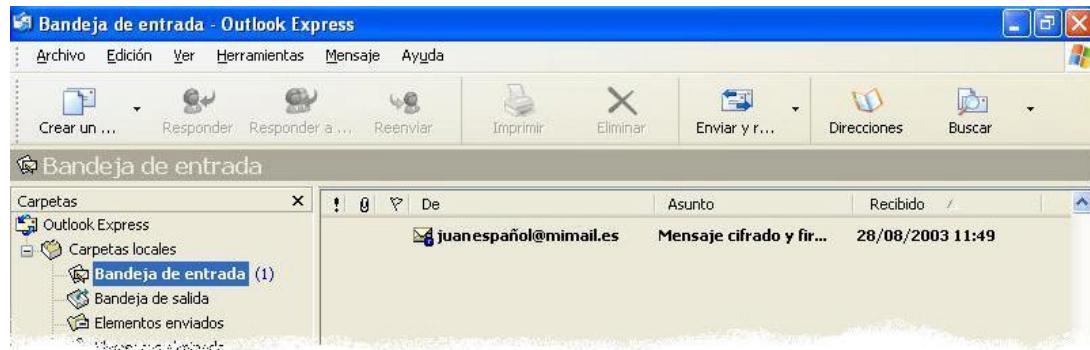
A continuación se intentará acceder a la tarjeta para firmar el mensaje. Si no estuviera insertada en el lector o la tarjeta actual no fuese la que está asociada al certificado instalado, aparecerá una ventana informándonos del error y solicitando aquella cuyo número de serie coincida con el indicado.





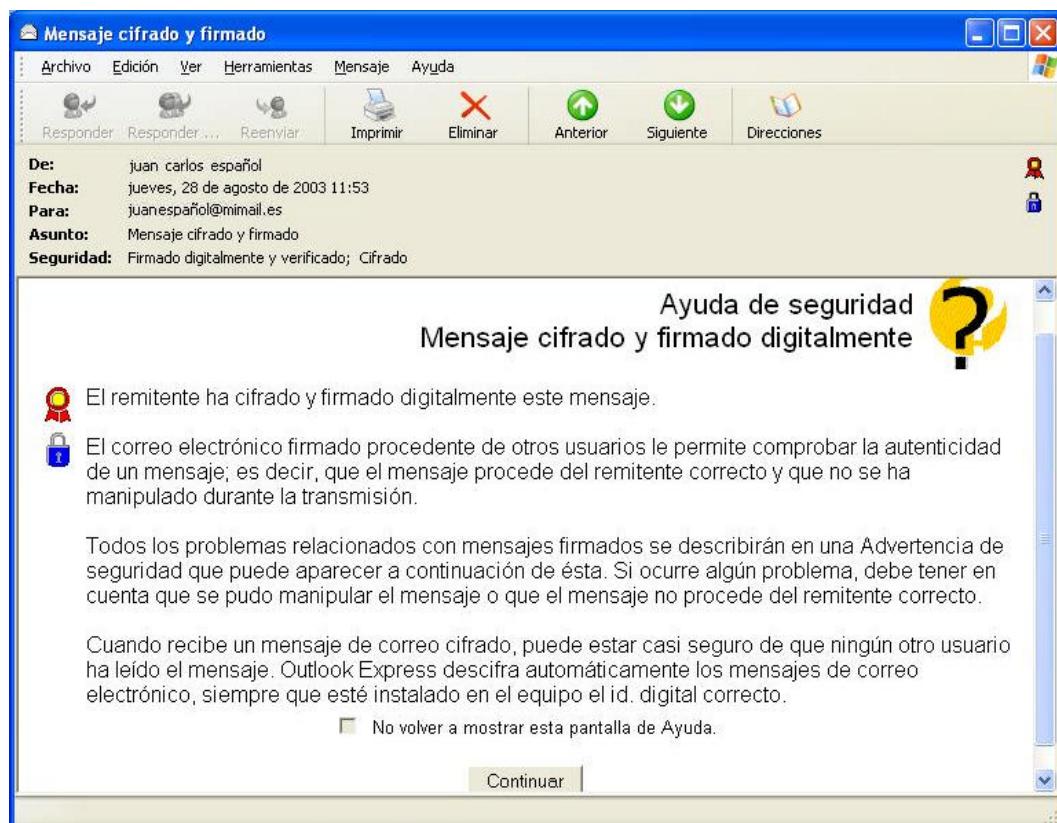
**Figura 122:** Solicitud de tarjeta con número de serie determinado.

Al recibir el mensaje veremos que el ícono que aparece junto a él es solamente el de *cifrado*. Esto es debido a que el descifrado es la primera operación que se llevará a cabo, para después proceder con la verificación de la firma digital.



**Figura 123:** Cliente de correo con mensaje cifrado y firmado.

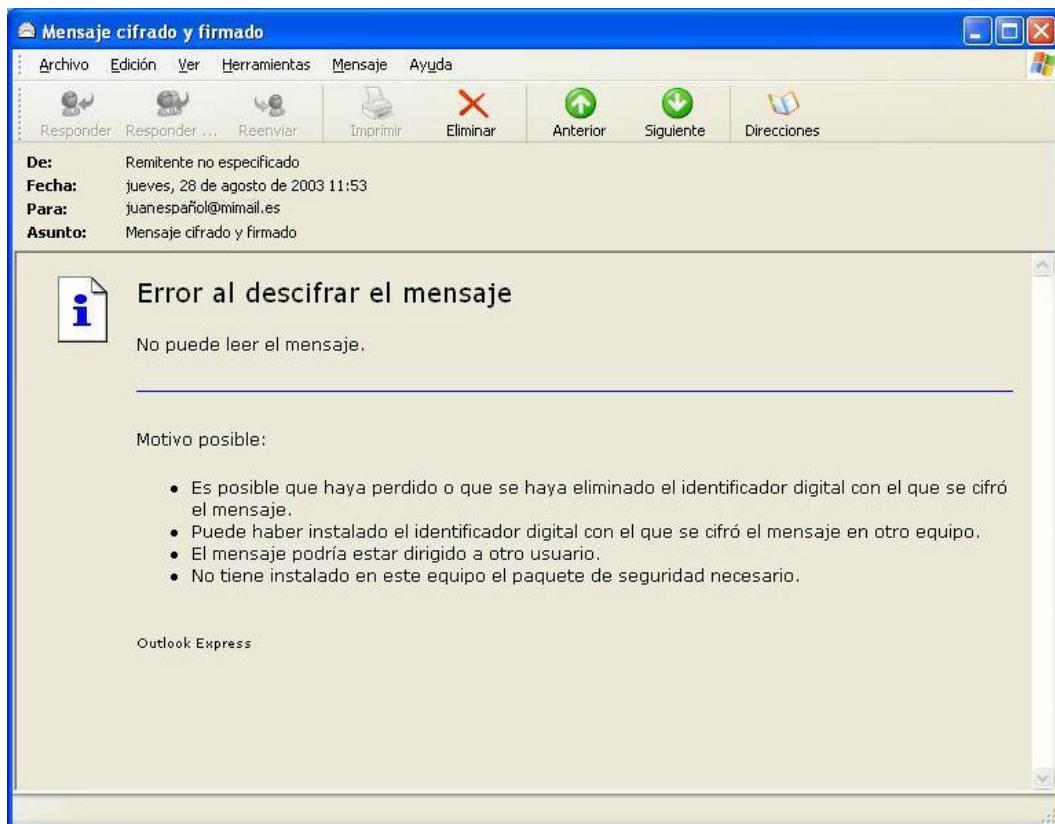
A la hora de abrir un correo que esté cifrado y firmado, el mensaje que aparecerá es similar a los anteriores, informándonos del estado del correo.



**Figura 124:** Aviso de correo CIFRADO y FIRMADO.



Para abrirlo necesitaremos nuestra tarjeta FNMT-RCM con nuestro certificado almacenado para descifrar el mensaje, además del certificado del emisor para poder verificar su firma digital.



**Figura 125:** Error al descifrar el mensaje.



## 14.2 Correo seguro con Netscape Messenger.

El cliente de correo **Netscape Messenger** también nos permite utilizar correo seguro entre usuarios, soportando tareas de cifrado, firma digital, verificación, etc. Seguramente la mayor diferencia que existe entre este cliente de correo y el de Microsoft es en la librería sobre la que basan dichas operaciones para realizarlas sobre dispositivos tales como tarjetas inteligentes. Mientras Outlook utiliza **CryptoAPI**, Messenger usa **PKCS#11**. Esto no implica que sean incompatibles, ni mucho menos, ambos sistemas. El correo cifrado y/o firmado con uno de ellos podrá ser descifrado y/o verificado con cualquiera de los dos sistemas.

Hemos indicado en apartados anteriores que la librería PKCS#11 de la FNMT-RCM es **pkcs12gk.dll**. Esta librería deberá estar convenientemente instalada como módulo criptográfico en el sistema para que nos dé acceso a la tarjeta FNMT-RCM (para su instalación, ver apartado de *Netscape* dentro del *Gestor de aplicaciones*).

### 14.2.1 Añadiendo un certificado a la cuenta.

Con la librería PKCS#11 instalada (ver apartado **10.1.2**) deberemos configurar las opciones del *Messenger* para que asocie a nuestra cuenta el certificado digital que nosotros queramos utilizar. Al igual que ocurría con Outlook Express, es necesario que la dirección de e-mail contenida en el certificado se corresponda con aquella que vamos a usar ahora.

Para configurar estas opciones deberemos pulsar el botón de ‘**Security**’ que aparece en el propio mensaje o desde el navegador Netscape Navigator.



Figura 126: Configuración de seguridad desde la ventana de mensajes.

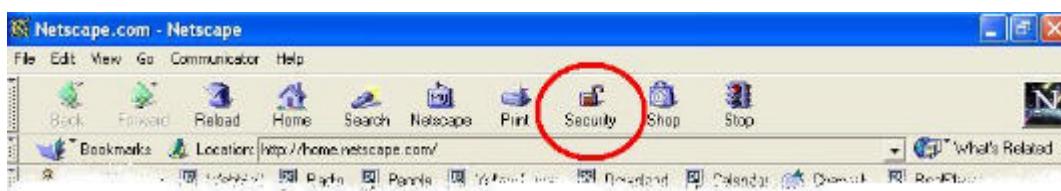


Figura 127: Configuración de seguridad desde Netscape Navigator.



En esa pantalla, dentro de **Messenger**, seleccionaremos las opciones de envío y el certificado que queremos usar con nuestra cuenta.

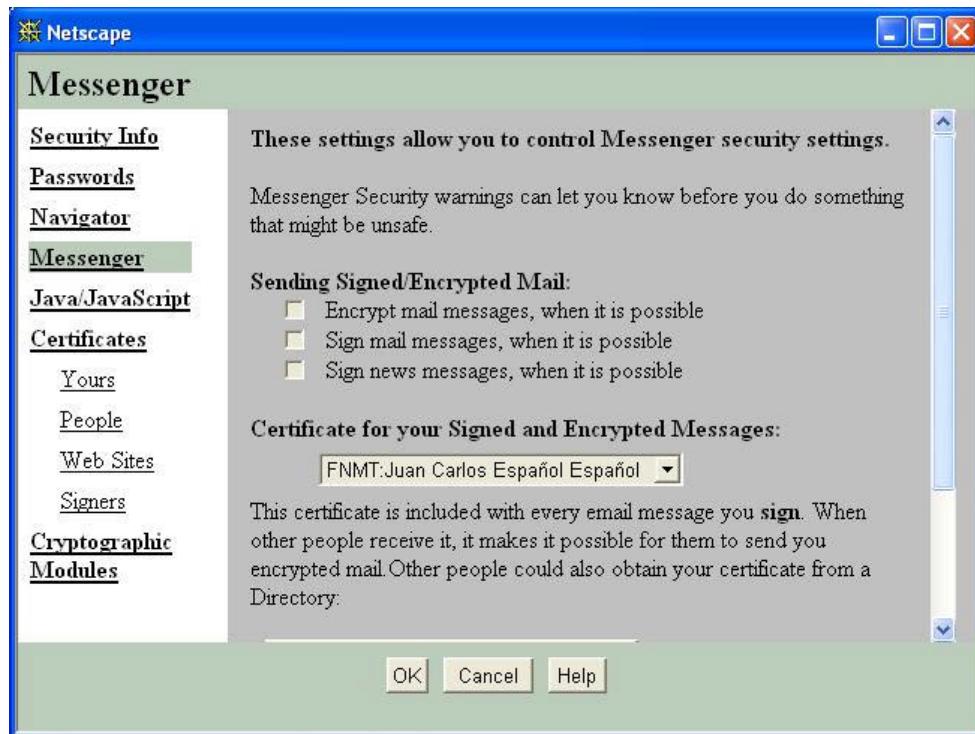


Figura 128: Selección del certificado a usar.



#### 14.2.2 Firma y verificación de mensajes.

En cuanto al interfaz de Netscape Messenger es similar al de Microsoft Outlook Express, y la forma de operar será también muy parecida.

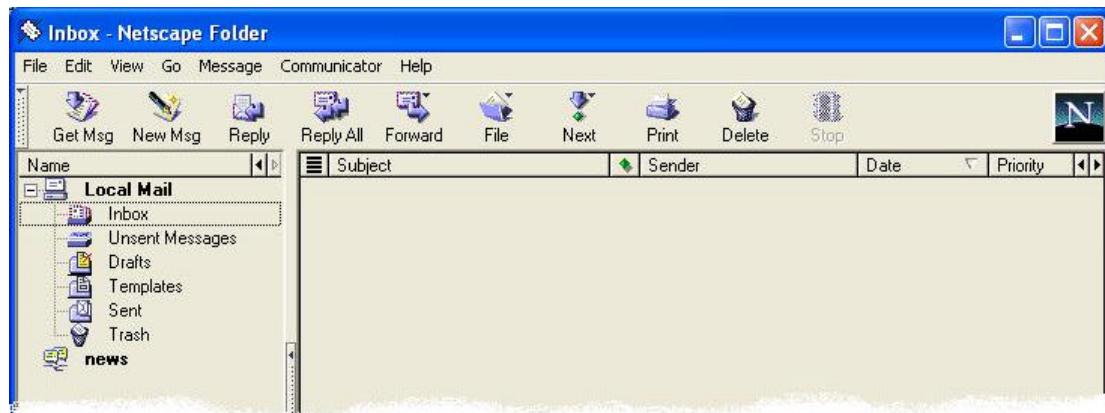


Figura 129: Interfaz de Netscape Communicator.

Cuando escribamos un mensaje que queramos que sea **firmado**, deberemos seleccionar la solapa de “**Opciones de envío de mensajes**”, situada en la parte izquierda de la pantalla. Entonces aparecerán una serie de opciones de envío, donde podremos indicar si queremos cifrar, firmar digitalmente, etc.

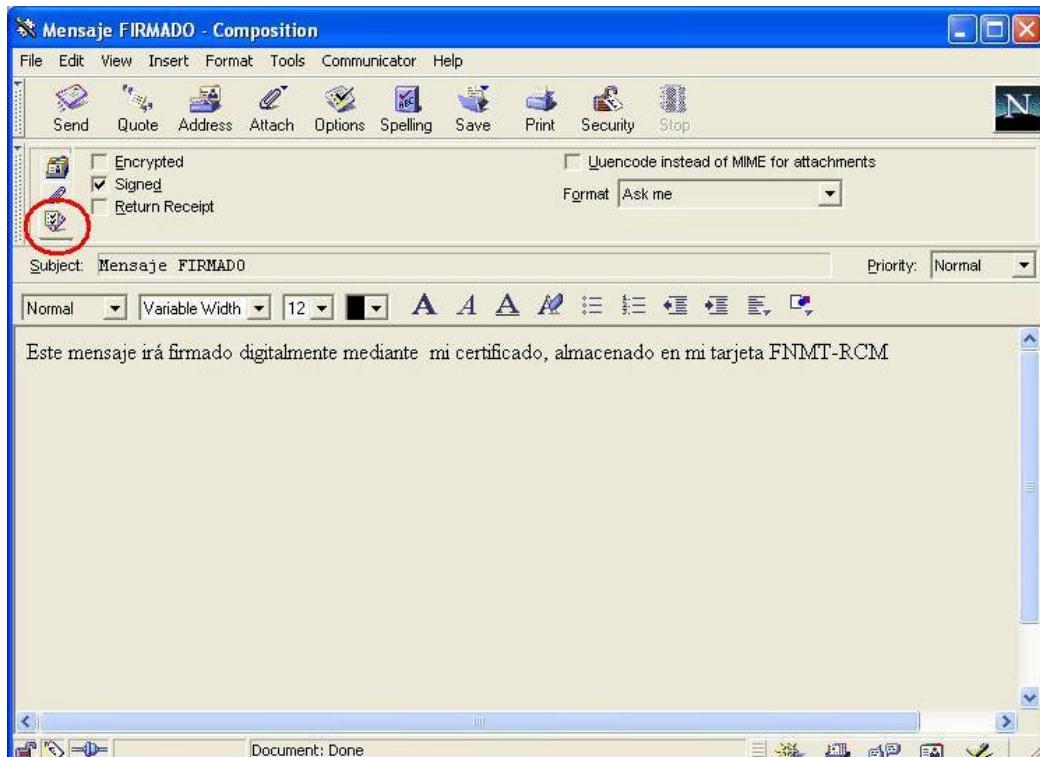


Figura 130: Opciones de envío para correo seguro.



Si ya tenemos configurado el sistema para que utilice un certificado en tarjeta FNMT-RCM, cuando envíemos el mensaje la aplicación nos pedirá que introduzcamos el PIN de la tarjeta. Al contrario de lo que sucedía con Outlook Express, en Messenger sólo nos pedirá el PIN una vez, quedando validadas las operaciones posteriores con tarjeta hasta que se cierre la aplicación o hasta que se extraiga la tarjeta del lector.



Figura 131: Ventana de solicitud del PIN de la tarjeta.

En caso de no introducir correctamente el PIN o no tener acceso a la tarjeta, Netscape Messenger nos mostrará un mensaje de error en el que nos informará de que no ha sido posible enviar el mensaje firmado. Esto, como sabemos, es debido a que al no habernos autenticado en la tarjeta no podemos acceder al uso de sus claves.



Figura 132: Información sobre seguridad del mensaje.

Cuando recibamos un mensaje firmado y lo abramos, el cliente de correo nos informará si ese mensaje está cifrado, firmado o ambas cosas a la vez. Podemos verlo rápidamente observando los iconos que aparecerán en la parte derecha del correo.

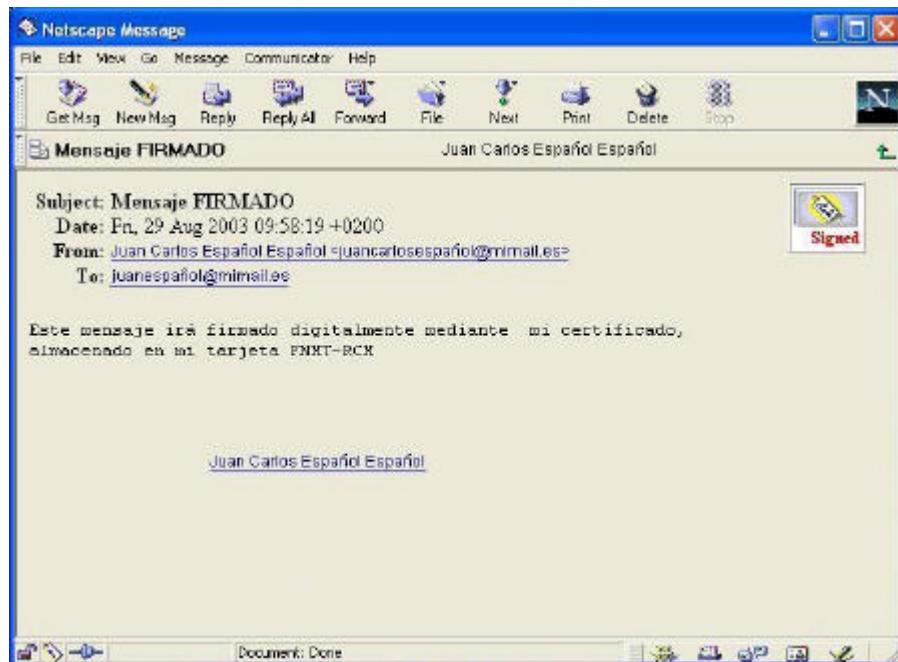


Figura 133: Información sobre seguridad del mensaje.

En la figura anterior podemos observar el ícono que indica que el mensaje está firmado (**Signed**). En caso de que también estuviese cifrado (**Encrypted**), aparecería otro ícono similar junto a él, avisándonos de ello.

Esos íconos nos darán acceso a la pantalla de seguridad, en la que nos informará si la firma ha podido ser verificada, el formato de cifrado que se utilizó, etc.

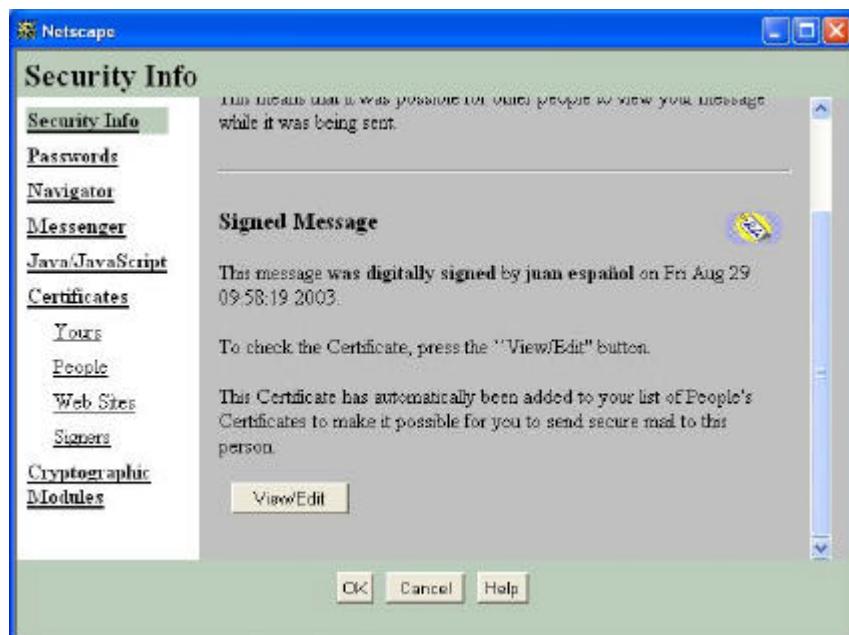


Figura 134: Información sobre seguridad del mensaje.



#### 14.2.3 Cifrado y descifrado de mensajes.

Para los mensajes **cifrados** deberemos seguir el mismo procedimiento. Desde la ventana de creación del nuevo mensaje, en las opciones de envío marcaremos **Cifrado (Encrypted)**.

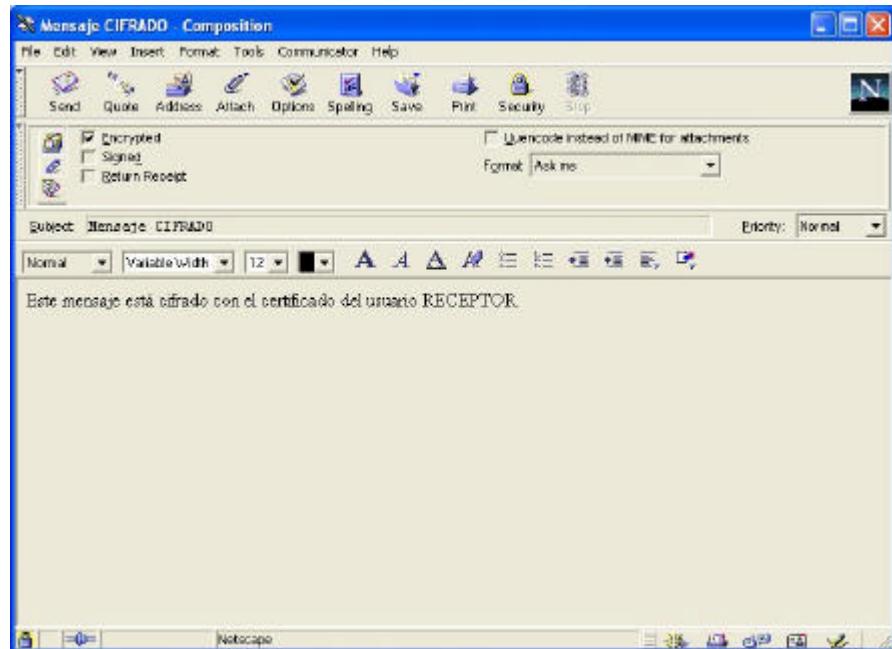


Figura 135: Mensaje cifrado.

Al abrir el mensaje comprobaremos que aparece el ícono informándonos de que había sido cifrado y que nos permite acceder a la información sobre él.

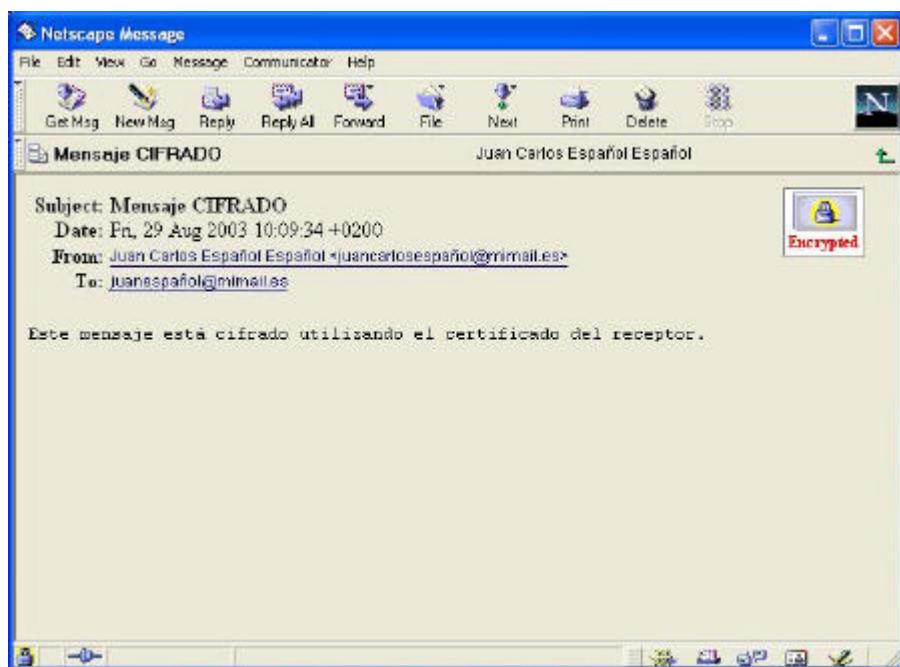


Figura 136: Mensaje cifrado recibido por el cliente de correo.

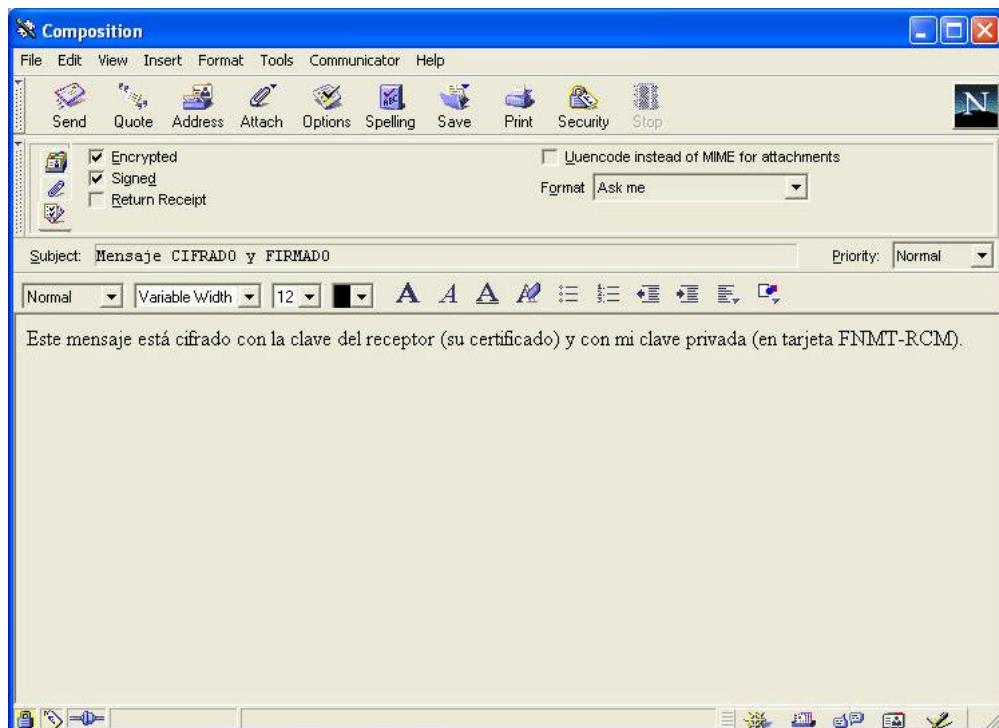


Al igual que ocurría con los correos firmados, si pulsamos el icono de cifrado, aparecerá la ventana de seguridad, explicándonos la operación de cifrado del mensaje.



**Figura 137:** Información sobre seguridad del mensaje.

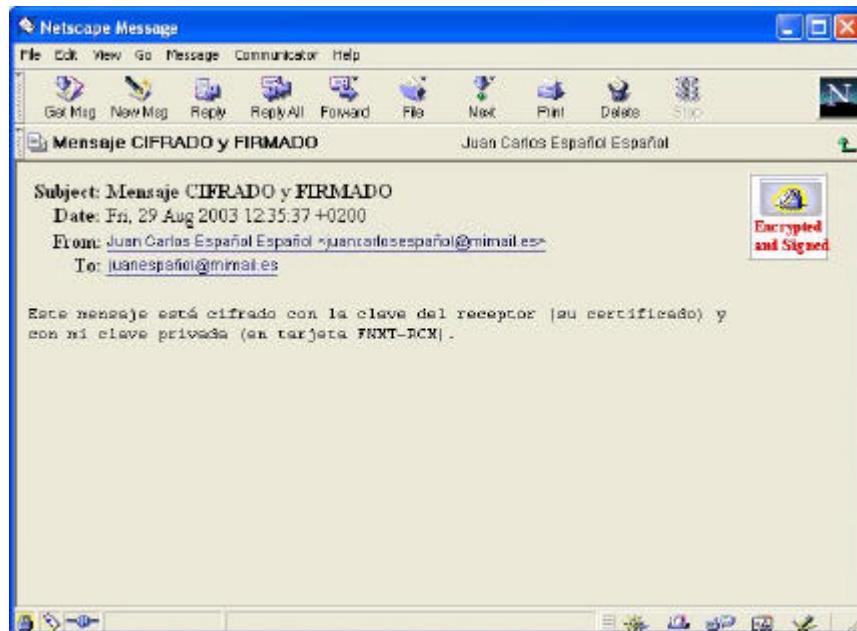
Una vez comentadas cómo serían las operaciones de firma y de cifrado, sólo queda indicar que también es posible realizar ambas cosas sobre un mismo correo. Bastará con indicarlo en las opciones de envío.



**Figura 138:** Mensaje cifrado y firmado.

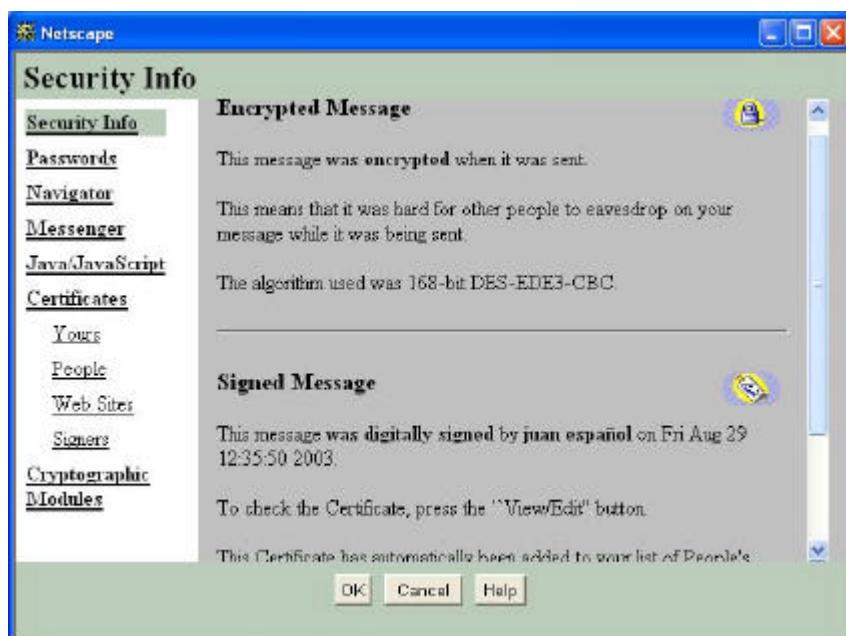


Al recibir un mensaje cifrado y firmado digitalmente, la pantalla que se nos muestra será similar a la que aparece a continuación.



**Figura 139:** Información sobre seguridad del mensaje.

Si pulsamos sobre el ícono de información de seguridad, aparecerá de nuevo la ventana de información correspondiente al mensaje recibido.



**Figura 140:** Información sobre seguridad del mensaje.



## Capítulo 15

### *Conexión segura*





## 15 CONEXIÓN SEGURA.

Otra de las funcionalidades que presentan las librerías **CeresCsp.dll** y **pkcsv2gk.dll** es que permiten la comunicación segura entre cliente-servidor. Para ello se utilizan protocolos de comunicación, tales como SSL, que permiten establecer un canal de comunicación seguro entre equipos.

En los siguientes apartados vamos a explicar brevemente la forma de conexión en los distintos navegadores.

### 15.1 Conexión segura en Microsoft Internet Explorer.

A lo largo de todo el documento hemos visto que para que un certificado almacenado en la tarjeta FNMT-RCM sea accesible a las aplicaciones de Microsoft, debe estar también instalado en el sistema.

Cuando una aplicación Web requiera una conexión segura, pasará el control al navegador, quien nos mostrará la ventana de certificados instalados, donde podremos seleccionar aquel con el que queremos conectarnos.

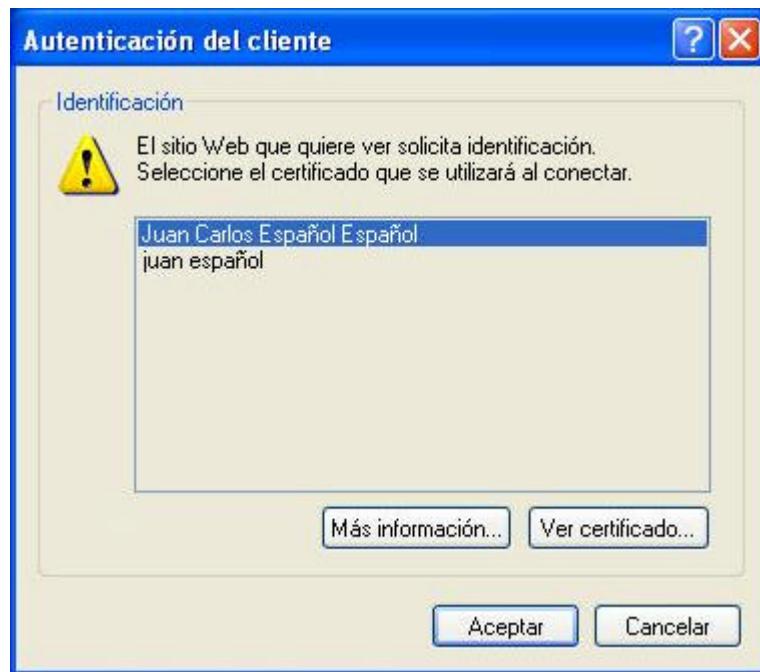


Figura 141: Selección del certificado a utilizar.



Después, el navegador comprobará si ese certificado está en software o si por el contrario está asociado a alguna tarjeta inteligente. En este último caso nos pedirá que introduzcamos la tarjeta con el **número de serie** correspondiente.



Figura 142: Solicitud de tarjeta inteligente.

Una vez introducida la tarjeta correcta en el lector, la aplicación pasará a realizar las operaciones necesarias para establecer la comunicación segura. Para ello utilizará las claves almacenadas en la tarjeta FNMT-RCM, así que de nuevo nos solicitará el PIN.



Figura 143: Petición de PIN.

En caso de no autenticarnos contra la tarjeta o que el certificado no esté correctamente instalado en la misma, el navegador no será capaz de establecer la conexión y mostrará un mensaje de error informándonos de ello. Si la conexión se realiza correctamente, en la barra de estado inferior del navegador aparecerá un ícono de un pequeño candado que indica que hay establecida una conexión segura.



Figura 144: Ícono de conexión segura en Explorer.



Si la conexión se realiza correctamente, en la barra de estado inferior del navegador aparecerá un icono de un pequeño candado que indica que hay establecida una conexión segura.

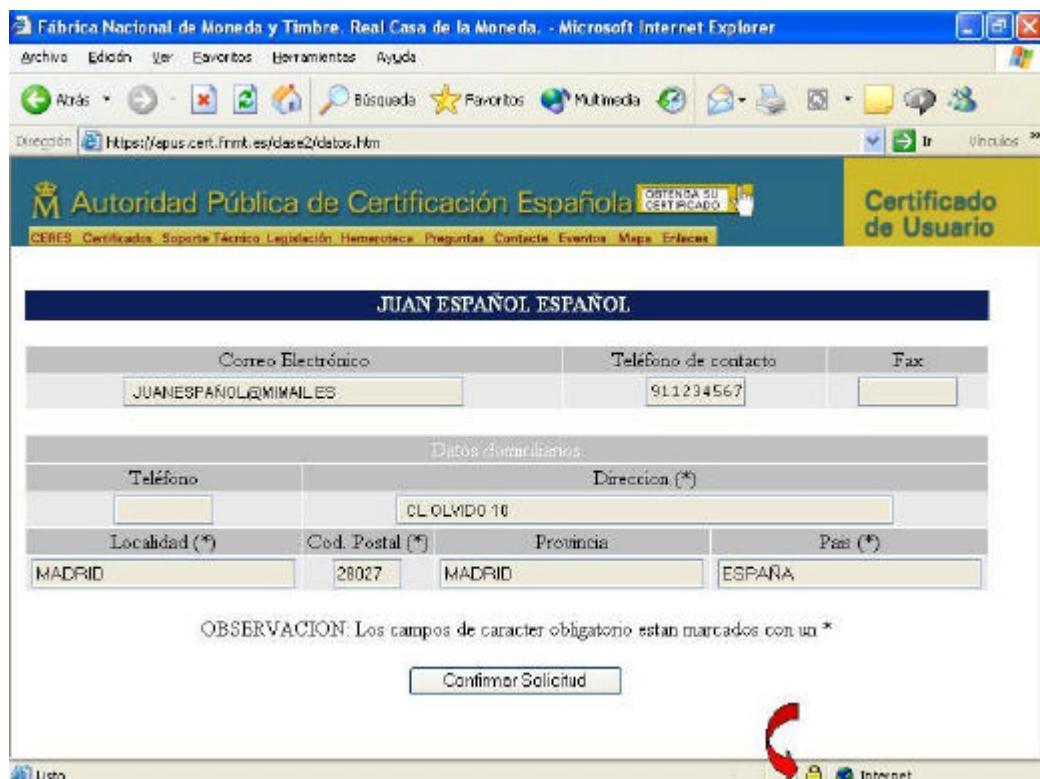


Figura 145: Comprobación de la conexión segura en Explorer.



## 15.2 Conexión segura en Netscape Navigator.

La librería utilizada en este caso será de nuevo **pkcsv2gk.dll**. Básicamente la conexión segura en este navegador sigue el mismo patrón que con Microsoft. Cuando la aplicación requiera una comunicación segura, deberá acceder a la tarjeta obtener los posibles certificados reconocidos por esa autoridad de certificación y con los que podremos conectarnos. Para ello nos solicitará el **PIN** de la tarjeta insertada en el lector del equipo.



Figura 146: Petición de PIN.

A diferencia de como funciona Microsoft, los certificados en Netscape no tienen que estar instalados en el sistema, sino que basta con que estén almacenados en la tarjeta. Cuando haya leído todos los que se encuentren en la tarjeta, nos mostrará una ventana en la que seleccionar el certificado que queremos utilizar para dicha conexión de entre todos los posibles.

La ventana será similar a la que se aparece en la siguiente figura.



Figura 147: Selección de certificado a utilizar para la conexión segura.



Una vez indicado el certificado que queremos utilizar para la conexión, se realizarán las operaciones necesarias para ello. En caso de que ocurriese algún problema, el navegador nos advertiría y mostraría un mensaje de error.

Si se realiza la conexión correctamente, podremos observar un icono de un pequeño candado en la parte inferior de la pantalla del navegador.



Figura 148: Icono de conexión segura en Explorer.

Así se mostrará gráficamente en pantalla la conexión segura establecida.

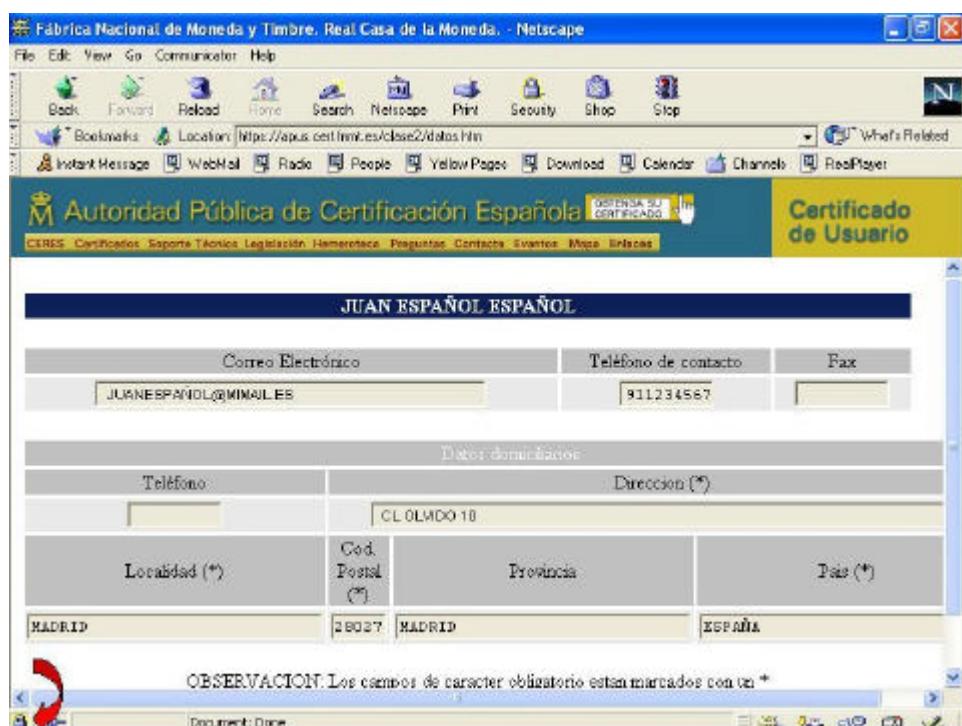


Figura 149: Comprobación de la conexión segura en Netscape.



## Capítulo 16

### *Windows Log-on*





## 16 WINDOWS LOGON

El sistema operativo *Windows* desde su versión **Windows 2000** soporta el inicio de sesión utilizando tarjeta inteligente y un certificado digital con unas determinadas características. La tarjeta FNMT-RCM soporta este tipo de arranque del sistema.

Al iniciar una nueva sesión, el sistema operativo nos muestra una ventana en la que nos indica las acciones que podemos realizar para arrancarla. Si pulsamos **Ctrl+Alt+Supr** se mostrará el habitual cuadro de identificación de usuario, dominio y contraseña. En cambio, si insertamos la tarjeta aparecerá una ventana en la que se nos solicitará que introduzcamos su PIN.

Para conseguir *logon* con tarjeta debemos estar en posesión de un certificado emitido por **Active Directory** de Microsoft. Si tuviésemos más de un certificado en la tarjeta se comprobaría si su certificado por defecto permite realizar el *logon*. En caso de que no sea así, se mostrará una ventana en la que deberemos seleccionar el certificado con el que autenticarnos. Una vez validado el usuario, se iniciará la sesión normalmente.

Al solicitar este tipo de arranque con tarjeta aparece la duda de saber qué ocurre cuando ésta es extraída. Es decir, si el equipo debe quedar bloqueado, si la sesión debe cerrarse, si no debe ocurrir nada, etc. Estas acciones posteriores a la extracción de la tarjeta son configurables. Para modificarlo debemos acudir al **Panel de Control** y seleccionar **Herramientas Administrativas**.

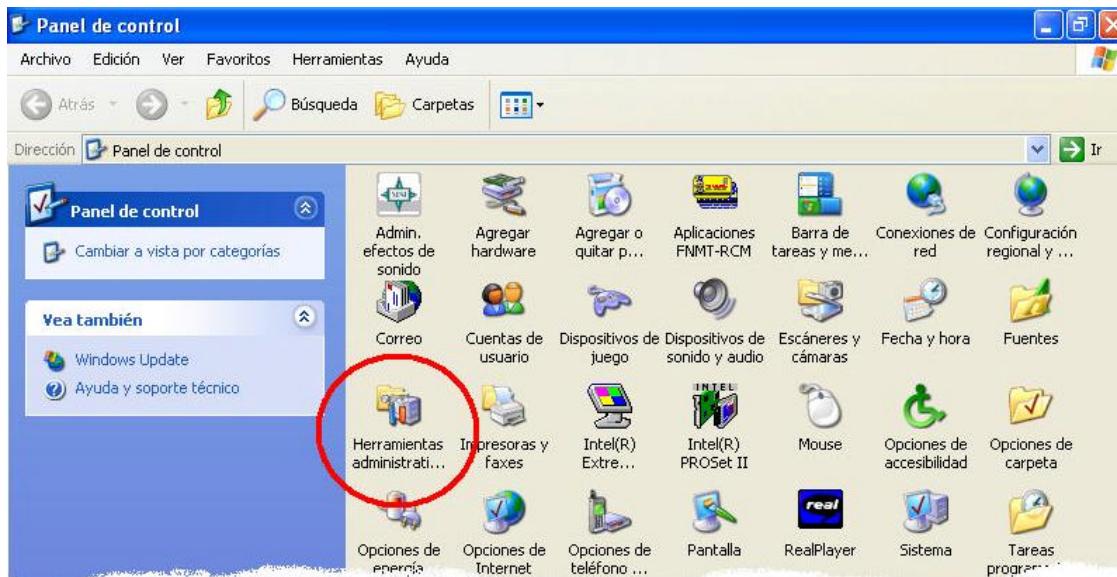


Figura 150: Panel de control.

Cuando se abra la ventana de las herramientas administrativas aparecerán una serie de opciones de configuración. La que nos interesa en este caso es la de: '**Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente**'. En la siguiente figura podemos ver la pantalla de configuración que debemos modificar.

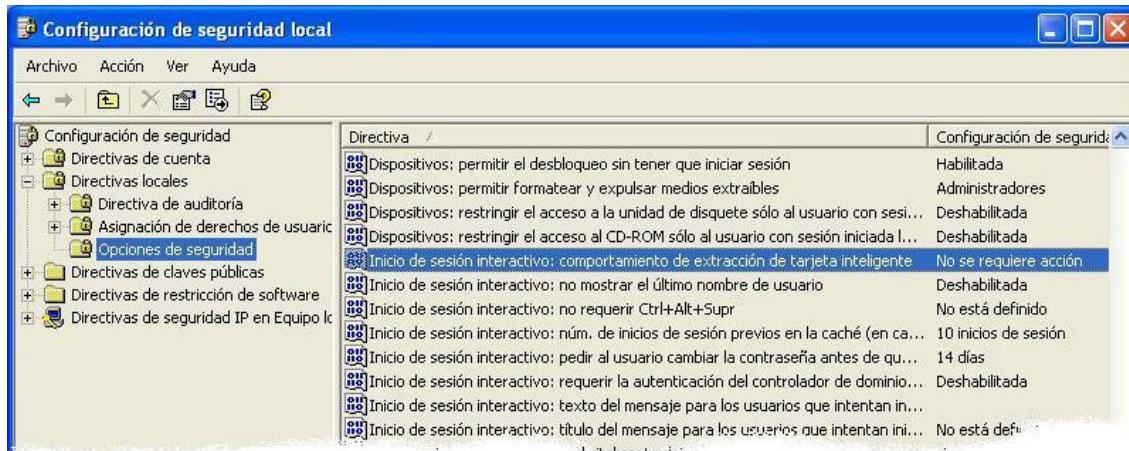


Figura 151: Opciones de configuración.

Aquí podremos indicar qué acción queremos que se lleve a cabo al extraer la tarjeta con la que hicimos *logon*. Estas opciones, como vemos en la figura inferior, son tres:

- no ejecutar **ninguna** acción,
- **bloquear** la estación de trabajo,
- forzar el **reinicio** de la sesión,

En la siguiente figura vemos cómo podemos seleccionar entre las tres.

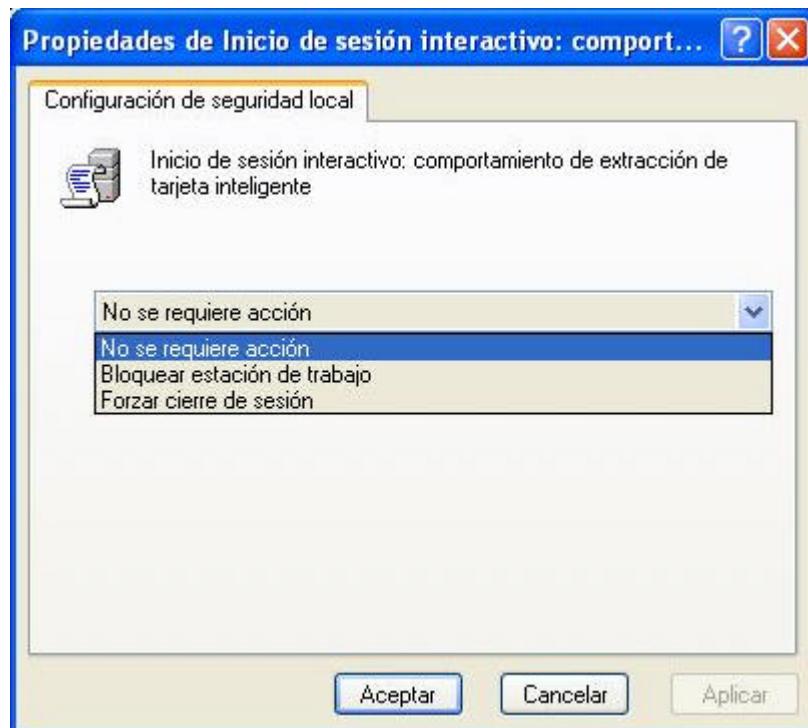


Figura 152: Acción a ejecutar en caso de extraer la tarjeta.



## 16.1 Selección de certificado por defecto.

A la hora de realizar *logon* con tarjeta en *Windows 2000*, *Windows NT* o *Windows XP*, el certificado que se utilizará para la autenticación será el propio de Microsoft. La aplicación **ccmng.exe** permite seleccionar el certificado que queremos establecer por defecto en la tarjeta FNMT-RCM. De esta manera evitaremos tener que seleccionarlo para el *logon* cada vez que queramos iniciar una sesión.

Cuando ejecutemos esta aplicación aparecerá una ventana solicitándonos que insertemos la tarjeta en el lector.



Figura 153: Solicitud de inserción de tarjeta.

En cualquier caso la aplicación continúa con la ejecución normal, solicitándonos el PIN de la tarjeta.



Figura 154: Solicitud del PIN de tarjeta.

Una vez tecleado el PIN, la aplicación comprobará si la tarjeta está insertada en el lector. En caso de no sea así, se nos mostrará una ventana de error y la aplicación se detendrá.



Figura 155: Información sobre seguridad del mensaje.



Si hemos introducido el PIN correctamente, aparecerá en pantalla una última ventana que nos permitirá seleccionar qué certificado queremos dejar por defecto en la tarjeta. Simplemente debemos pulsar en el que hayamos elegido y pulsar el botón de “Aceptar”.



Figura 156: Selección de certificado por defecto.

Una vez hecho esto, el certificado seleccionado quedará asignado como certificado por defecto para la tarjeta.



## Capítulo 17

### *Versiones de navegadores válidas*





## **17 VERSIONES DE NAVEGADORES VÁLIDAS.**

Las versiones de navegadores válidas para el correcto funcionamiento de los certificados digitales de la FNMT-RCM son las siguientes:

### **MICROSOFT**

Microsoft Internet Explorer versión 4 o posterior sobre Win 32 (Windows 95 - Windows 98 - Windows NT - Windows 2000 - Windows Me).

Los usuarios de Microsoft Internet Explorer cuyo Nombre o Apellidos contengan la letra "Ñ", deberán solicitar su certificado con la [Versión 5.0 de IE](#).

### **NETSCAPE**

Netscape Navigator versión 4.06 o posterior, a excepción de la versión 4.60, versiones 6.0 y posteriores, que actúe sobre un Sistema Operativo de al menos 32 bits.