JCCM*: Java Card Certificate Management

Mª Celeste Campo Vázquez, Arturo García Ares, Andrés Marín López, Ignacio Díaz Asenjo, Carlos Delgado Kloos, Carlos García Rubio, Peter T. Breuer

Universidad Carlos III de Madrid. Avd. Universidad 30 28911 Leganés
<eticket@it.uc3m.es>

Resumen El estándar PKCS #11 define una interfaz que ofrece a las aplicaciones una visión lógica común de los dispositivos criptográficos: dispositivos con capacidad de almacenamiento, proceso y, específicamente, capaces de proteger de manera efectiva los objetos sensibles (claves de cifrado) almacenados. Los desarrollos que se han realizado hasta la actualidad de módulos PKCS #11 con tarjetas inteligentes recortan la semántica definida por el estándar para adaptarla a la que ofrece el fabricante en cada tarjeta.
Este artículo describe el trabajo desarrollado para obtener una implementación de PKCS #11 que emplea una tarjeta inteligente programable mediante tecnología Java Card como dispositivo criptográfico. El hecho de poder incluir código ejecutable en la tarjeta inteligente nos permite trasladar parte de la inteligencia de la implementación del estándar a la tarjeta, resultando en una mayor flexibilidad e independencia del dispositivo. El resultado de implementar PKCS #11 es una biblioteca; es necesario disponer de una aplicación que haga uso de ella para disfrutar de los servicios ofrecidos: en concreto, hemos hecho uso de Netscape como aplicación tipo. Ello nos permite utilizar nuestro módulo PKCS #11 para navegación segura, cifrado y firma de correo electrónico.

1 Introducción

El número de usuarios con acceso a Internet sigue creciendo, y este incremento en el número de usuarios lleva consigo necesidades crecientes en materia de seguridad. Cada vez hay más sitios con páginas seguras y nuevos procedimientos de compra, por lo que los usuarios demandan navegación segura, cifrado, firma de correo electrónico, etc.

Los navegadores más populares (Microsoft Explorer, Netscape, Opera, etc.) incluyen habilidades criptográficas que los usuarios empiezan a utilizar incluso antes de comprender muy bien su funcionamiento e implicaciones. Estas habilidades dependen de la utilización de certificados digitales ([X.509]) que establecen un mecanismo para comprobar la identidad de un usuario o de un sitio, para dar fe de que un usuario ha firmado un mensaje y garantizar la integridad del mismo, o bien para proteger una clave de sesión mediante la cual cifrar un mensaje. Estos certificados encapsulan distintas claves, entre ellas la más importante

* Este trabajo ha sido desarrollado dentro del proyecto E-TICKET CYCYT Nº2FD1997-1269-C02-01(TEL)

es la clave privada. Los navegadores citados anteriormente permiten el almacenamiento cifrado en disco mediante una clave simétrica que también almacenan en el disco. Este es el eslabón más débil de la cadena, y que define la seguridad del sistema. El problema es recursivo y de difícil solución, y hay que pensar en nuevas opciones, como las tarjetas inteligentes.

Las tarjetas actuales son dispositivos inviolables (*tamper-proof*)[1] y además tienen una considerable capacidad de cómputo y almacenamiento. Las tarjetas inteligentes se integran de forma natural con las aplicaciones que utilizamos, por ejemplo nuestro navegador favorito, mediante el uso de [PKCS#11], que explicamos en la sección 2. PKCS #11 define un interfaz que proporciona a las aplicaciones que desean utilizar servicios criptográficos una visión lógica común de los dispositivos capaces de ofrecer dichos servicios: dispositivos con capacidad de almacenamiento, proceso, y específicamente, capaces de proteger de manera efectiva los elementos sensibles (claves de cifrado) almacenados. Las aplicaciones que utilizamos suelen utilizar este API (por ejemplo, la NSL de Netscape sigue este estándar).

La alternativa más segura es utilizar módulos que implementen PKCS #11 para las aplicaciones que lo admitan, y utilizar tarjetas inteligentes para compartir la gestión y para almacenar de forma segura claves y certificados. Sin embargo, los desarrollos que se han realizado hasta la actualidad de módulos PKCS #11 ([SMARTSIGN], [GPKPKCS#11], [SLBCBPKCS#11]) con tarjetas inteligentes emplean tarjetas no programables o bien no utilizan la facilidad de programación de las tarjetas que sí son programables. Estas implementaciones se limitan a adaptar la funcionalidad criptográfica predefinida en las tarjetas a la visión lógica que debe ofrecer un módulo PKCS #11, recortando la semántica definida por el estándar para adaptarla a la que ofrece el fabricante en cada tarjeta.

Nuestro sistema, Java Card Certificate Management (JCCM), emplea una tarjeta inteligente programable mediante tecnología Java Card como dispositivo criptográfico, trasladando parte de la implementación del estándar PKCS #11 a la tarjeta, resultando en una mayor flexibilidad, e independencia del dispositivo. JCCM se compone de dos piezas complementarias:

- Una biblioteca de enlace dinámico (DLL) que sirve de interfaz entre la tarjeta inteligente y la biblioteca de seguridad (NSL) de Netscape –el agente de usuario.
- Un *cardlet* (programa residente en la tarjeta inteligente escrito acorde con la especificación Java Card) que implementa las funciones requeridas.

[1] La inviolabilidad de la tarjeta se entiende a efectos prácticos en la relación coste/beneficio del ataque. Si dispusieramos de un número ilimitado de medios físicos, podríamos comprometer la seguridad de una tarjeta moderna. En [USENIX 99] se describen una serie de sofisticados ataques químicos y físicos, y las sencillas, pero efectivas, contramedidas adoptadas por los fabricantes. El artículo concluye asertando la dificultad de que todavía hay ataques muy difíciles de parar (ataques con herramientas sofisticadas basadas en haces de iones de Galio) mientras que las tarjetas no dispongan de una fuente de alimentación propia.

En este artículo describimos la implementación del API definida por RSA Laboratories en el estándar PKCS #11 versión 2.10, con el objetivo de permitir al usuario de Netscape beneficiarse del uso de tarjetas inteligentes como almacén seguro de certificados y claves de cifrado para su empleo en navegación segura, cifrado y firma de correo electrónico basada en el algoritmo RSA.

La estructura de este artículo es la siguiente: en primer lugar hacemos una breve introducción a las tecnologías directamente involucradas: PKCS #11 (sección 2), la arquitectura de seguridad de Netscape (sección 3) y las tarjetas inteligentes (sección 4). A continuación se describe la arquitectura de JCCM en la sección 5, y finalmente terminamos con unas conclusiones.

2 El estándar PKCS #11

PKCS #11 es uno más del creciente grupo de estándares PKCS, acrónimo de Public-Key Cryptography Standards (estándares de criptografía de clave pública) y publicados por RSA Labs. Estos estándares abarcan aspectos del sistema que acabamos de esbozar tales como:

- Definición de los algoritmos criptográficos (tanto de clave pública como de clave simétrica) y algoritmos de apoyo.
- Procedimientos para aplicar los algoritmos criptográficos a flujos de bytes y para producir firmas digitales.
- Definición de tipos de datos (certificados, claves, ...) y sus correspondientes sintaxis de transferencia o formatos de representación binaria.
- Procedimiento para efectuar transacciones HTTP seguras
- Definición de formatos para transmisión de correo electrónico cifrado e inclusión de firma digital.
- Interfaz de programación para aplicaciones (API) que permite hacer uso de los algoritmos, procedimientos y tipos de datos.

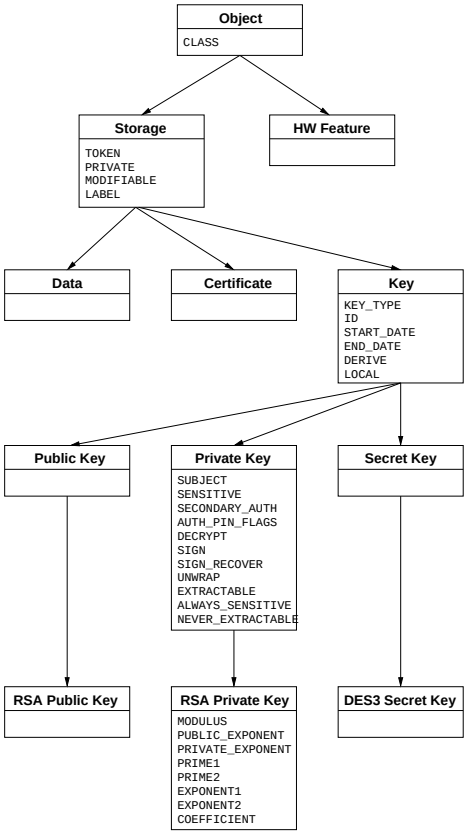

Figura1. Jerarquía parcial de objetos de Cryptoki y detalle de atributos de clases participantes en la jerarquía de RSA Private Key

La biblioteca descrita por el estándar PKCS #11 recibe el nombre de Cryptoki, abreviatura de "cryptographic token interface". A lo largo de este artículo utilizaremos el término "el estándar" para referirnos al estándar PKCS #11, y Cryptoki para referirnos a la biblioteca definida por el estándar.

Cryptoki aisla a la aplicación de los detalles del dispositivo criptográfico. En terminología de Cryptoki, estos dispositivos se llaman *tokens*. Los tokens portátiles (p.e. una tarjeta inteligente) se insertan en su correspondiente *slot*, nombre asignado por Cryptoki para la abstracción del terminal lector. Un token almacena *objetos* y es capaz de ejecutar *primitivas criptográficas* empleando esos objetos, posiblemente tras un paso inicial de autenticación del usuario/aplicación al token mediante la presentación de un PIN. Toda comunicación con el token se efectúa dentro del contexto de una *sesión*, que representa un canal de comunicación establecido con un token presente en un slot.

Todas estas abstracciones son soportadas mediante las funciones y estructuras de datos definidas por el estándar. Estas funciones (ver tabla 1) pertenecen a varios grupos:

- Funciones de propósito general: Inicialización y obtención de información general acerca de la biblioteca.
- Funciones de gestión de slots y tokens: Permiten obtener información acerca de los slots presentes en el sistema, el estado de presencia o ausencia de un token en cada slot, capacidades de los tokens presentes y establecimiento de PINs.
- Funciones de gestión de sesiones: Apertura y cierre de sesiones, obtención de información acerca de la sesión y autenticación al token mediante la presentación de un PIN.
- Funciones de gestión de objetos: Permiten crear, buscar y obtener objetos.
- Funciones criptográficas: Permiten ejecutar primitivas criptográficas de las siguientes categorías: cifrado y descifrado de flujos de bytes, firmado y verificación de firmas y generación, importación y exportación de claves, entre otras.

Un objeto es una lista de parejas atributo/valor. Todos los posibles objetos están perfectamente definidos en el estándar mediante la lista de atributos que lo componen y el tipo de cada atributo. Se emplea una pseudo-orientación a objetos para definir los distintos tipos de objetos, de manera que se definen tipos básicos de los cuales derivan tipos especializados que incorporan todos los atributos de los tipos base y añaden atributos propios (ver fig. 1). Los principales tipos de objetos son "Certificate" y "Key" pero también existen los tipos "HW Feature", empleado para describir capacidades especiales de los tokens, y "Data" que se utiliza para almacenar un objeto binario sin interpretar.

Los objetos más importantes son los de tipo clave ("Key"). Todas las funciones criptográficas requieren o generan objetos de este tipo. Como queda reflejado en la fig. 1, el tipo clave se especializa en clave pública ("Public Key"), privada ("Private Key") y secreta ("Secret Key"). A su vez, cada uno de estos tipos se especializa en tipos concretos de claves dependiendo del algoritmo de cifrado con

Funciones de propósito general	**Funciones de gestión de slots y tokens**	**Funciones criptográficas**
C_Initialize	C_GetSlotList	C_EncryptInit
C_Finalize	C_GetSlotInfo	C_Encrypt
C_GetInfo	C_GetTokenInfo	C_DecryptInit
Funciones de gestión de objetos	C_GetMechanismList	C_Decrypt
	C_SetPIN	C_SignInit
C_CreateObject	**Funciones de gestión de sesiones**	C_Sign
C_CopyObject		C_VerifyInit
C_DestroyObject	C_OpenSession	C_Verify
C_GetAttributeValue	C_CloseSession	C_DigestInit
C_SetAttributeValue	C_CloseAllSessions	C_Digest
C_FindObjectsInit	C_GetSessionInfo	C_GenerateKey
C_FindObjects	C_Login	C_GenerateKeyPair
C_FindObjectsFinal	C_Logout	C_WrapKey
		C_UnwrapKey

Tabla1. Muestra representativa de funciones de Cryptoki

el que deban ser utilizadas. En la fig. 1 se han incluido todos los atributos de los objetos que forman parte del tipo concreto "RSA Private Key".

Cryptoki identifica diversos algoritmos de cifrado (*mecanismos*), y da libertad a las implementaciones sobre cuales deben estar soportadas. Cada mecanismo tiene asignado un identificador, opera sobre unos tipos concretos de objetos y puede o no requerir ciertos parámetros propios. Por ejemplo, en la fig. 1 se muestra una relación de todos los atributos que forman un objeto de tipo clave privada RSA, incluyendo los atributos de las clases base. Cryptoki adapta la representación física a esta visión lógica. A continuación se describen los pasos que deberá realizar una aplicación que desee utilizar una clave privada RSA almacenada en un token para efectuar una operación de firma digital. La secuencia de llamadas a funciones de Cryptoki necesaria para generar una firma termina en:

```
C_SignInit(...);
C_Sign(...);
```

Los prototipos respectivos de estas funciones son:

```
CK_RV S_SignInit(
  CK_SESSION_HANDLE hSession,
  CK_MECHANISM_PTR pMechanism,
  CK_OBJECT_HANDLE hKey);
CK_RV C_Sign(
  CK_SESSION_HANDLE hSession,
  CK_BYTE_PTR pData,
  CK_ULONG ulDataLen,
  CK_BYTE_PTR pSignature,
  CK_ULONG_PTR pulSignatureLen);
```

No nos detendremos a explicar en detalle los tipos de datos involucrados, pues su nombre es suficientemente descriptivo; los aspectos a destacar son:

- El primer parámetro de las dos funciones es un manejador (*handle*) de sesión. Este manejador habrá sido obtenido previamente por la aplicación mediante la correspondiente llamada a `C_OpenSession()`.
- La operación de firma se inicia con una llamada a `C_SignInit()`. Esta función recibe, además del manejador de sesión, una especificación del algoritmo a emplear (parámetro `pMechanism`) y el manejador del objeto de tipo clave que habrá de emplearse para efectuar la operación. Este manejador habrá sido obtenido previamente por la aplicación mediante la secuencia de llamadas

```
C_FindObjectsInit(...);
C_FindObjects(...);
C_FindObjectsFinal(...);
```

- Una vez establecidos los parámetros de la operación de firma, se realiza la operación en sí. La llamada a `C_Sign()` acepta un puntero a los datos a firmar (`pData`), la longitud de los mismos (`ulDataLen`), el buffer donde se depositará el resultado de la operación (`pSignature`) y la longitud de este buffer (`pulSignatureLen`).

3 Netscape y PKCS #11

Netscape incorpora una arquitectura de seguridad que permite tráfico HTTP seguro y gestionar correo cifrado y firmado. Esta arquitectura de seguridad, conocida como "Netscape Security Library" (NSL), hace uso de las primitivas presentes en PKCS #11 para ofrecer la funcionalidad de alto nivel a la que nos referimos. Netscape se distribuye con un módulo PKCS #11 interno que constituye una implementación bastante completa del estándar: incluye tanto los mecanismos basados en RSA como algunos mecanismos de clave simétrica. Este módulo PKCS #11 interno ofrece una visión lógica del propio ordenador como dispositivo criptográfico: utiliza el sistema de archivos como almacenamiento persistente para almacenar los objetos de Cryptoki y la capacidad de proceso de la CPU para efectuar las operaciones de cifrado. Gracias a este módulo interno Netscape es plenamente capaz de ofrecer las capacidades mencionadas, pero adolece de un problema: la utilización del sistema de archivos del ordenador para almacenar certificados y claves rompe la premisa inicial de almacenamiento seguro de datos sensibles. La solución adoptada por Netscape es permitir la incorporación de módulos PKCS #11 externos que sirvan de interfaz a hardware criptográfico especializado, como es el caso de nuestro módulo. Otra peculiaridad de la NSL es que permite la presencia simultánea de varios módulos PKCS #11: nuestro módulo puede coexistir con el módulo interno, por lo que no es necesario implementar los mecanismos ya soportados por este módulo; en particular, no se implementan mecanismos orientados al cifrado de datos (clave simétrica) pues la velocidad de transferencia de datos entre el ordenador y la tarjeta la hace inapropiada para el cifrado de volúmenes arbitrarios de datos.

A continuación se analiza una traza de todas las llamadas efectuadas por Netscape a nuestra biblioteca para emitir un correo firmado, incluyendo todas las llamadas desde el arranque de la aplicación. La traza ha sido simplificada eliminando todas las entradas salvo la correspondiente a la salida de cada función de Cryptoki.

- *Líneas 1 a 10*: Funciones de inicialización de biblioteca y obtención de información básica. Son llamadas al arrancar Netscape antes de que iniciemos cualquier operación. El token estaba presente en el lector (es lo que Netscape determina al llamar a la función `C_GetSlotInfo()`), es por ello que se obtiene información acerca del token presente y sus capacidades mediante las llamadas a `C_GetTokenInfo()` y `C_GetMechanismList()`. Por último, se inicia una sesión con el token.

```
 1 Mar  2 12:06:20: C_GetFunctionList Returns (CKR_OK) 0x0
 2 Mar  2 12:06:20: C_Initialize Returns (CKR_OK) 0x0
 3 Mar  2 12:06:20: C_GetInfo Returns (CKR_OK) 0x0
 4 Mar  2 12:06:20: C_GetSlotList Returns (CKR_OK) 0x0
 5 Mar  2 12:06:20: C_GetSlotList Returns (CKR_OK) 0x0
 6 Mar  2 12:06:21: C_GetSlotInfo Returns (CKR_OK) 0x0
 7 Mar  2 12:06:21: C_GetTokenInfo Returns (CKR_OK) 0x0
 8 Mar  2 12:06:21: C_GetMechanismList Returns (CKR_OK) 0x0
 9 Mar  2 12:06:21: C_GetMechanismList Returns (CKR_OK) 0x0
10 Mar  2 12:06:21: C_OpenSession Returns (CKR_OK) 0x0
```

- *Líneas 11 a 14*: Si nos fijamos en los instantes de traza asociados a cada línea, veremos que transcurren 32s entre la línea 10 y la 11; corresponden al tiempo transcurrido en escribir el mensaje de correo electrónico que dió lugar a esta traza y pulsar el botón de enviar. Estas líneas corresponden a la solicitud del PIN por parte de Netscape y la correspondiente llamada a `C_Login()`. El tiempo transcurrido entre las líneas 13 y 14 corresponde a la introducción del PIN en el cuadro de diálogo.

```
11 Mar  2 12:06:53: C_GetSlotInfo Returns (CKR_OK) 0x0
12 Mar  2 12:06:53: C_GetSessionInfo Returns (CKR_OK) 0x0
13 Mar  2 12:06:53: C_GetSessionInfo Returns (CKR_OK) 0x0
14 Mar  2 12:06:57: C_Login Returns (CKR_OK) 0x0
```

- *Líneas 15 a 66*: El resto de la traza corresponde a las llamadas efectuadas por Netscape a nuestro módulo para realizar la operación de firma. Las dos últimas corresponden a la realización de la firma en sí. El tiempo empleado en efectuar esta operación (líneas 65 a 66) es de tan sólo 2s, mientras que el tiempo total empleado para la firma (líneas 15 a 66) es de 26s. Esos 24s restantes se emplean en búsquedas de certificados y claves en el token y en transferencias de los mismos al ordenador; éstas son, por tanto, las culpables de que la operación tarde tanto.

```
15 Mar  2 12:06:59: C_FindObjectsInit Returns (CKR_OK) 0x0
16 Mar  2 12:06:59: C_FindObjects Returns (CKR_OK) 0x0
17 Mar  2 12:06:59: C_FindObjectsFinal Returns (CKR_OK) 0x0
18 Mar  2 12:07:00: C_FindObjectsInit Returns (CKR_OK) 0x0
19 Mar  2 12:07:00: C_FindObjects Returns (CKR_OK) 0x0
20 Mar  2 12:07:00: C_FindObjectsFinal Returns (CKR_OK) 0x0
21 Mar  2 12:07:07: C_GetAttributeValue Returns (CKR_OK) 0x0
22 Mar  2 12:07:07: C_GetAttributeValue Returns (CKR_OK) 0x0
```

```
23 Mar  2 12:07:08: C_GetSessionInfo Returns (CKR_OK) 0x0
24 Mar  2 12:07:08: C_GetAttributeValue Returns (CKR_OK) 0x0
25 Mar  2 12:07:08: C_GetAttributeValue Returns (CKR_OK) 0x0
26 Mar  2 12:07:12: C_FindObjectsInit Returns (CKR_OK) 0x0
26 Mar  2 12:07:12: C_FindObjects Returns (CKR_OK) 0x0
27 Mar  2 12:07:12: C_FindObjectsFinal Returns (CKR_OK) 0x0
28 Mar  2 12:07:12: C_GetMechanismList Returns (CKR_OK) 0x0
29 Mar  2 12:07:12: C_GetMechanismList Returns (CKR_OK) 0x0
30 Mar  2 12:07:16: C_FindObjectsInit Returns (CKR_OK) 0x0
31 Mar  2 12:07:16: C_FindObjects Returns (CKR_OK) 0x0
32 Mar  2 12:07:16: C_FindObjectsFinal Returns (CKR_OK) 0x0
33 Mar  2 12:07:17: C_GetAttributeValue Returns (CKR_OK) 0x0
34 Mar  2 12:07:17: C_GetAttributeValue Returns (CKR_OK) 0x0
35 Mar  2 12:07:17: C_GetSessionInfo Returns (CKR_OK) 0x0
36 Mar  2 12:07:17: C_GetAttributeValue Returns (CKR_OK) 0x0
37 Mar  2 12:07:17: C_GetAttributeValue Returns (CKR_OK) 0x0
38 Mar  2 12:07:18: C_FindObjectsInit Returns (CKR_OK) 0x0
39 Mar  2 12:07:18: C_FindObjects Returns (CKR_OK) 0x0
40 Mar  2 12:07:18: C_FindObjectsFinal Returns (CKR_OK) 0x0
41 Mar  2 12:07:18: C_GetSlotInfo Returns (CKR_OK) 0x0
42 Mar  2 12:07:18: C_GetSessionInfo Returns (CKR_OK) 0x0
43 Mar  2 12:07:18: C_GetSessionInfo Returns (CKR_OK) 0x0
44 Mar  2 12:07:18: C_FindObjectsInit Returns (CKR_OK) 0x0
45 Mar  2 12:07:18: C_FindObjects Returns (CKR_OK) 0x0
46 Mar  2 12:07:18: C_FindObjectsFinal Returns (CKR_OK) 0x0
47 Mar  2 12:07:18: C_GetAttributeValue Returns (CKR_OK) 0x0
48 Mar  2 12:07:19: C_GetAttributeValue Returns (CKR_OK) 0x0
49 Mar  2 12:07:19: C_GetSessionInfo Returns (CKR_OK) 0x0
50 Mar  2 12:07:19: C_GetAttributeValue Returns (CKR_OK) 0x0
51 Mar  2 12:07:19: C_GetAttributeValue Returns (CKR_OK) 0x0
52 Mar  2 12:07:19: C_FindObjectsInit Returns (CKR_OK) 0x0
53 Mar  2 12:07:19: C_FindObjects Returns (CKR_OK) 0x0
54 Mar  2 12:07:19: C_FindObjectsFinal Returns (CKR_OK) 0x0
55 Mar  2 12:07:19: C_GetSessionInfo Returns (CKR_OK) 0x0
56 Mar  2 12:07:20: C_GetAttributeValue Returns (CKR_OK) 0x0
57 Mar  2 12:07:20: C_GetAttributeValue Returns (CKR_OK) 0x0
58 Mar  2 12:07:20: C_FindObjectsInit Returns (CKR_OK) 0x0
59 Mar  2 12:07:20: C_FindObjects Returns (CKR_OK) 0x0
60 Mar  2 12:07:20: C_FindObjectsFinal Returns (CKR_OK) 0x0
61 Mar  2 12:07:22: C_GetAttributeValue Returns (CKR_OK) 0x0
62 Mar  2 12:07:23: C_GetAttributeValue Returns (CKR_OK) 0x0
63 Mar  2 12:07:23: C_GetAttributeValue Returns (CKR_OK) 0x0
64 Mar  2 12:07:23: C_GetSessionInfo Returns (CKR_OK) 0x0
65 Mar  2 12:07:23: C_SignInit Returns (CKR_OK) 0x0
66 Mar  2 12:07:25: C_Sign Returns (CKR_OK) 0x0
```

Hay que hacer constar que sólo se incurre en esta penalización la primera vez que se utiliza el certificado y la clave privada asociada; la generación de una firma digital para un nuevo mensaje consume únicamente 6s.

4 Tarjetas inteligentes y Java Card

Una tarjeta inteligente contiene un pequeño ordenador que consta de un microprocesador, memoria volátil (RAM) y memoria persistente (EEPROM). Las

capacidades típicas de estos elementos son: microprocesador de 8 bits a 4MHz, RAM de 512 bytes, 32Kb de EEPROM y 16Kb de ROM. Los contactos presentes en la superficie de la tarjeta aportan la tensión de alimentación, la señal de reloj y un canal de comunicación serie (a 9600bps[2]). Estos contactos son gobernados por el terminal lector en el que esté insertada la tarjeta, por lo tanto el microprocesador sólo estará activo cuando la tarjeta esté insertada en un terminal. Extraer la tarjeta del terminal tiene el mismo efecto que apagar un ordenador: se interrumpe la actividad de la CPU y se pierde el contenido de la RAM, pero el almacenamiento persistente permanece; en un ordenador este almacenamiento persistente está constituido por dispositivos magnéticos (discos duros), mientras que en una tarjeta inteligente es la memoria EEPROM. Otra característica importante de este tipo de memoria es su relativamente corta esperanza de vida, unos 100000 ciclos de escritura, y su elevado tiempo de acceso para ciclos de escritura, del orden de 10ms.

La tarjeta inteligente es un dispositivo pasivo: recibe un comando proveniente del ordenador a través del terminal en el que esté insertada, lo procesa, genera una respuesta que es devuelta al ordenador y espera el siguiente comando. Estos comandos se denominan APDUs (Application Protocol Data Unit) y su estructura está definida en [ISO/IEC 7816-4]. Existen dos tipos de APDU, las que codifican un comando enviado por el ordenador y las que codifican la respuesta generada por la tarjeta.

Existen tarjetas no programables, que aceptan un juego de comandos predefinido, y tarjetas programables capaces de incorporar dinámicamente a su memoria persistente programas provenientes del exterior y enriquecer así el conjunto de comandos que son capaces de ejecutar. Una de las tecnologías de tarjetas programables es Java Card. Una Java Card es una tarjeta inteligente capaz de incorporar y ejecutar programas escritos en un subconjunto del lenguaje de programación Java. Las principales limitaciones son:

- Independencia de la plataforma: las aplicaciones Java Card pueden ejecutarse sobre cualquier tarjeta acorde a la especificación, independientemente del fabricante de la misma.
- Multiaplicación: varias aplicaciones pueden ejecutarse en la misma tarjeta. Tanto la descarga como ejecución de estas aplicaciones se realiza con restricciones de seguridad.
- Descarga de aplicaciones despues de su uso: los usuarios finales podrán actualizar las aplicaciones que tienen en sus tarjetas, para adaptarlas a sus necesidades.
- Utilización del lenguaje Java, lo que permite desarrollar aplicaciones con un lenguaje de alto nivel orientado a objetos.
- Compatible con estándares sobre tarjetas inteligentes: Es compatible con otros estándares desarrollados para tarjetas inteligentes como el ISO 7816.

El lenguaje Java Card es una versión reducida del lenguaje Java. Las principales limitaciones son:

[2] El estándar [ISO/IEC 7816-3] permite una velocidad de hasta 115Kbps

- Los paquetes accesibles a una aplicación Java Card no son los mismos que los accesibles a una aplicación Java. En concreto, el paquete java.lang carece las clases `Thread` y `String` y la clase `Object` está muy simplificada.
- Limitaciones en la máquina virtual: No existe recolector de basura; todo objeto es instanciado en memoria persistente y permanece en ella hasta que se elimine el cardlet de la tarjeta. Esta es, como veremos más adelante, la diferencia más chocante respecto al lenguaje Java y la que más influencia el diseño de una aplicación Java Card. Los tipos primitivos soportados se limitan a los permitidos por la aritmética entera de 16 bits de que son capaces los procesadores de las tarjetas inteligentes, lo que reduce el conjunto de tipos a `byte`, `short` y `boolean`.

5 Arquitectura de JCCM

Los desarrollos que se han realizado hasta la actualidad de módulos PKCS #11 con tarjetas inteligentes emplean tarjetas no programables o bien no utilizan la facilidad de programación de las tarjetas que sí son programables. Estas implementaciones se limitan a adaptar la funcionalidad criptográfica predefinida en las tarjetas a la visión lógica que debe ofrecer un módulo PKCS #11. La semántica definida por el estándar se recorta para adaptarla a la que ofrece la tarjeta para la que se realiza la implementación, que además queda ligada a una tarjeta de un determinado fabricante.

La característica distintiva de nuestro desarrollo es la implementación por parte del cardlet presente en la tarjeta de parte de la funcionalidad definida en el estándar PKCS #11. Los objetos se almacenan en la tarjeta con los mismos atributos definidos en el estándar, y es el propio cardlet quien procesa las operaciones de gestión de objetos de Cryptoki, soportando así el almacenamiento de cualquier tipo de objeto e implementando la semántica completa de búsqueda, copia, creación y borrado.

En los siguientes apartados se explican las diferentes partes de que consta la aplicación Java Card desarrollada en este proyecto.

5.1 Gestión de memoria dinámica en tarjetas Java Card

La memoria en una tarjeta inteligente es un recurso limitado y es una de las restricciones más importantes a tener en cuenta cuando se realizan aplicaciones para este tipo de sistemas. Para almacenar datos de forma persistente en una tarjeta inteligente, es necesario que residan en memoria EEPROM. El estándar [ISO/IEC 7816-4] definió para ello una estructura de sistema de ficheros similar a la que tenemos en un ordenador y estandarizó APDUs para poder gestionarla. Las primeras versiones de Java Card, hasta la 2.0, imitaban este modelo de gestión de la memoria persistente: existían clases que replicaban la funcionalidad de las APDUs de acceso a ficheros definidas por ISO y que trataban de imitar el modelo de *streams* de Java. A partir de la versión 2.1 se abandonó este modelo de acceso a memoria persistente para sustituirlo por el método nativo

en Java de instanciación de objetos: para disponer de un bloque de bytes en el almacenamiento persistente se instancia un objeto de la clase deseada; el acceso estructurado a la EEPROM, a través de los miembros del objeto instanciado, es así más directo que el efectuado a través de streams. Cuando en Java Card se habla de almacenamiento persistente no se bromea; los objetos instanciados no serán destruidos ni tampoco será liberado el espacio que ocupen por ningún recolector de basura, pues el estándar Java Card no contempla esta facilidad. Por lo tanto, todo objeto instanciado permanecerá durante la vida del cardlet: hasta que éste sea eliminado de la tarjeta.

Las funciones de Cryptoki permiten la creación dinámica de objetos y nosotros deseábamos que nuestra implementación no limitase esa flexibilidad. Podíamos haber diseñado una implementación capaz de almacenar un número predeterminado de objetos Cryptoki, p.e. un certificado X.509 y una clave privada RSA, pero eso limitaba la funcionalidad de nuestra implementación y por lo tanto las aplicaciones potenciales que podrían beneficiarse de ella. Topamos con el problema de desarrollar un cardlet capaz de crear, destruir y modificar dinámicamente un número indeterminado de objetos en un esquema de asignación de memoria que nunca libera los bloques asignados. La solución a este problema consiste en desarrollar un módulo de asignación de memoria dinámica que ofrezca funcionalidad similar a las tradicionales `malloc()` y `free()` de la biblioteca estándar del lenguaje C. La asignación de bloques se hace sobre un array de bytes Java cuyo tamaño se especifica en tiempo de compilación y que es reservado en memoria persistente en el instante de instalación del cardlet en la tarjeta.

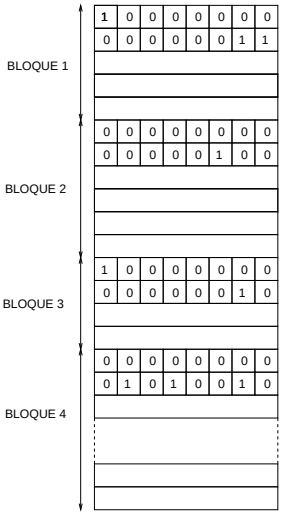

Figura2. Formato de los bloques en memoria

Se ha adoptado un sencillo esquema para gestionar los bloques libres y ocupados: todo bloque tiene una cabecera de dos bytes para la gestión de la memoria y el resto disponible para almacenar datos. La cabecera puede considerarse como una palabra de dos bytes, primero el byte de mayor peso, en la que el bit más a la izquierda es un indicador de si el bloque está libre (0) u ocupado (1) y los 15 bits restantes indican el tamaño del bloque en bytes excluyendo la cabecera. Por tanto, el tamaño máximo de bloque y de memoria dinámica que podemos manejar con este esquema es de 2^{15} bytes (32Kb), suficiente para abarcar toda la memoria persistente disponible en tarjetas inteligentes de tecnología actual.

En cualquier instante el array estará compuesto por una serie de bloques contiguos libres y ocupados mezclados, dependiendo de la secuencia de asignaciones y liberaciones previa. Inicialmente tenemos un bloque libre que abarca el

array completo. Cada vez que se solicita un bloque se recorren los bloques en secuencia desde el primero (que siempre está en la dirección 0, índice `[0]` en el array) buscando un bloque libre de tamaño suficiente. Cuando ésto ocurre, si el bloque encontrado es de mayor tamaño que el bloque solicitado y suficientemente grande como para poder hacer un nuevo bloque de la parte sobrante, se divide en dos: un fragmento ocupado de tamaño exacto para albergar el tamaño solicitado y el fragmento restante que se marca como libre. Durante este recorrido de búsqueda se fusionan todos los bloques libres contiguos que se vayan encontrando. Si alcanzamos el final del array sin encontrar un bloque suficientemente grande se devuelve la dirección 0, que es una dirección no válida pues por definición apunta a la cabecera del primer bloque. Las clases que solicitan memoria reciben la dirección del campo de datos del bloque, no de la cabecera.

En la figura 2 representamos una posible imagen de la memoria en la que tendríamos cuatro bloques, dos de ellos ocupados (bloque 1 y 3) y dos libres (bloque 2 y 4), el bloque 4 es el que contiene la memoria libre del array sobre la que todavía no se ha realizado ninguna reserva.

5.2 Almacenamiento y gestión de objetos de Cryptoki

En PKCS #11 los objetos están definidos como un array de atributos, donde cada atributo es una estructura de tamaño fijo con tres campos: un tipo de atributo, un puntero al valor y la longitud del valor (fig. 3). Las estructuras empleadas en el cardlet siguen un esquema muy parecido. La estructura empleada para los objetos, es de longitud variable y consta de los siguientes campos:

- Enlace al siguiente objeto, 2 bytes. Todos los objetos PKCS #11 que se crean en la tarjeta se mantienen en una lista enlazada.
- Número de atributos del objeto, 1 byte. Este campo puede deducirse en función del tamaño del bloque en memoria dinámica donde se aloja la estructura y el tamaño de la parte fija, pero se ha optado por incluir el número de atributos en la estructura del objeto porque el ahorro en consumo de memoria que hubiese supuesto su no inclusión es despreciable: típicamente la tarjeta almacenará únicamente dos objetos, un certificado y una clave privada asociada por lo que el ahorro total en este caso sería de 2 bytes.
- Un número variable de estructuras de atributos, tantas como número de atributos tenga el objeto.

La estructura de un atributo consta de los siguientes campos:

- Tipo de atributo, 4 bytes. Es el valor binario definido en el estándar.
- Puntero al valor del atributo, 2 bytes. El campo valor, al ser de tamaño inherentemente variable, se almacena en su propio bloque de memoria dinámica. No almacenamos la longitud del valor en la estructura del atributo para ahorrar memoria. La longitud de este campo se obtiene de la cabecera del bloque de memoria dinámica en el que se aloja.

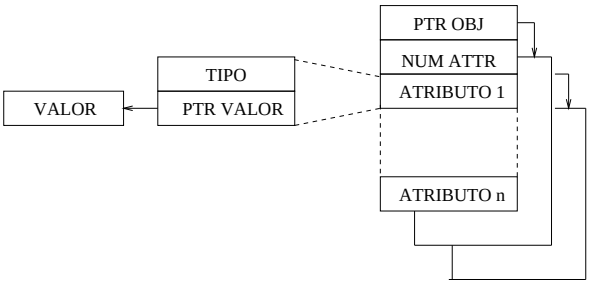

Figura3. Estructura de objetos

El almacenamiento de estas dos estructuras se hace sobre la memoria dinámica descrita en el apartado anterior. Existe una clase Java para ayudar en el manejo de cada una de estas estructuras, son la clase `ObjPatr` para los objetos y la clase `AttrPatr` para los atributos. Estas clases no pueden instanciarse debido al problema de no liberación de memoria mencionado en el apartado 5.1, por lo que únicamente poseen métodos y miembros estáticos. Se utilizan para mapear porciones del array de memoria dinámica sobre la estructura correspondiente y para acceder cómodamente a los distintos campos de cada estructura: poseen métodos para establecer/obtener el valor de cada campo y para liberar toda la memoria dinámica asociada a cada una de estas estructuras. Estas dos clases extienden la clase `Patr`, que aporta los métodos básicos para acceder a campos de tipo multibyte. Antes de emplear una de estas clases para acceder a una estructura alojada en memoria dinámica es necesario establecer primero la dirección inicial de la estructura mediante una llamada a `setAddr(short addr)`, lo que establece la dirección de referencia empleada por todos los métodos que acceden a miembros de una estructura (`get...()`, `set...()`).

6 Implementación del cardlet en tarjetas comerciales

A la hora de implementar un cardlet en tarjetas Java Card, es necesario tener en cuenta las diferencias existentes entre tarjetas y kits de desarrollo Java Card disponibles actualmente. Comentamos a continuación las que más han condicionado nuestro desarrollo:

- Capacidades criptográficas, en tarjetas Java Card además de estar implementado por hardware el algoritmo criptográfico requerido, éste debe de ser accesible a través de una clase Java Card, para que pueda ser utilizado desde el cardlet.
- Descarga de aplicaciones, Java Card no estandariza los procedimientos de descarga de aplicaciones en la tarjeta, por lo que la mayoría de fabricantes implementan sus propios mecanismos, por lo tanto para cada una de las tarjetas comerciales empleadas se deben de desarrollar módulos de descarga específicos.

- Extensiones propietarias al API Java Card, debido a que Java Card es un estándar reciente, los fabricantes incluyen desarrollos propios para aumentar la funcionalidad proporcionada por sus tarjetas, uno de los objetivos que se planteó al realizar la implementación del cardlet fue restringirnos en la medida de lo posible a la especificación del estándar y aumentar la portabilidad de nuestro desarrollo.

Hasta el momento, en este proyecto se han empleado dos kits de desarrollo Java Card para entorno Linux que existen en el mercado:

- **GemXpresso RAD 211is de Gemplus**, [GemXpresso RAD 211 UG], la principal limitación que teniamos con estas tarjetas es que sólo implementan algoritmos de clave simétrica, por lo que el cardlet que se desarrolló en este caso, se limita al almacenamiento de claves y certificados, que se transfieren al ordenador (incluida la clave privada) para realizar las operaciones criptográficas soportadas por nuestra implementación.
- **Cyberflex for Linux Starter's Kit 2.1**, [Cyberflex SDK], se adquirió este kit porque las tarjetas implementan RSA y así podiamos realizar la operación de firma internamente. La principal limitación con la que nos enfrentamos es que las tarjetas son Java Card 2.0 y en esta especificación todavía no se incluía un paquete de seguridad (`javacard.security` en Java Card 2.1). Así, para el acceso desde Java Card a las capacidades criptográficas, es necesario utilizar la extensión proporcionada por Schlumberger `javacardx.crypto`, por lo que la solución desarrollada sólo es válida para este tipo de tarjetas.

7 Conclusiones

La demanda de seguridad en el almacenamiento de claves se puede abordar con éxito mediante el uso de tarjetas inteligentes. En este artículo hemos presentado nuestro sistema de gestión de certificados basado en Java Card (JCCM), que presenta una alternativa flexible a la gestión de certificados de cualquier tipo en tarjetas inteligentes, frente a otros trabajos que emplean tarjetas no programables o bien no utilizan la facilidad de programación. Nuestro enfoque no se limita a adaptar la funcionalidad criptográfica predefinida en las tarjetas a la visión lógica que debe ofrecer un módulo PKCS #11, ni recorta la semántica definida por el estándar para adaptarla a la que ofrece el fabricante en cada tarjeta.

En la actualidad JCCM soporta dos tipos de tarjetas inteligentes: las GemXpresso RAD 211, y las Cyberflex Access de Schlumberger, y está disponible para su uso con Netscape para navegar de forma segura, cifrar y firmar correos.

Los trabajos futuros que estamos abordando en la actualidad son: la integración de JCCM en un módulo PAM (Pluggable Authentication Module), para ampliar el número de aplicaciones seguras; y portar nuestros resultados a las aplicaciones de Microsoft, en Windows 95 y 2000.

Referencias

[ISO/IEC 7816-4] "ISO/IEC 7816-4: Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interchange", ISO/IEC, 1995.

[ISO/IEC 7816-3] "ISO/IEC 7816-3: Integrated circuit(s) cards with contacts. Part 3: Electronic signals and transmission protocols", ISO/IEC, 1997.

[JCADG 2.1] "Java Card Applet Developer's Guide. Java Card Version 2.0", SUN Microsystems, Agosto de 1998.

[JCADG 2.0] 'Java Card Applet Developer's Guide. Java Card Version 2.1", SUN Microsystems, Agosto de 1999.

[GemXpresso RAD 211 UG] "GemXpresso RAD 211 User Guide Version 1.0", Gemplus, Octubre 1999

[GemXpresso RAD 211 CRM] "GemXpresso RAD 211 Card Reference Manual Version 1.0", Gemplus, Octubre 1999

[Cyberflex PG] "Cyberflex Access Developer's Series. Programmer's Guide", Schlumberger, Septiembre 1999.

[Cyberflex SDK] "Cyberflex Access Software Developer's Kit 2 - Release Notes", Schlumberger, Noviembre 1999.

[HTTPS] "HTTP Over TLS", Rescorla, E., IETF RFC 2818, Mayo 2000.

[X.509] "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP". R. Housley, P. Hoffman. IETF RFC 2585, Mayo 1999.

[USENIX 99] "Design Principles for Tamper-Resistant Smartcard Processors" by Oliver Kömmerling, Markus Kuhn, Workshop on Smartcard Technology Proceedings, Chicago, Illinois, USA, Mayo 10-11, 1999

[SC SDK] 'Smart Card Developer's Kit", Scott B. Guthery, Timothy M. Jurgensen. Macmillan Technical Publishg. 1998.ISBN 1-57870-027-2.

[SC APP. DEV. JAVA] 'Smart Card. Application Developement Using Java", Uwe Hansmann, Martin S. Nicklous, Thomas Schack y Frank Seliger, Springer, 2000. ISBN 3-540-65829-7.

[PKCS#11] "PKCS #11 v2.10: Cryptographic Token Interface Standard", RSA Laboratories Inc., Diciembre 1999 (003-903052-210-000-000).

[PKCS#1] "PKCS #1 v2.1: RSA Cryptography Standard", RSA Laboratories Inc.

[PKCS#5] "PKCS #5 v2.0: Password-Based Cryptography Standard", RSA Laboratories Inc.

[PKCS#8] "PKCS #8 v1.2: Private-Key Information Syntax Standard", RSA Laboratories Inc.

[STALL99] 'Cryptography and Network Security: Principles and Practices", Stallings, W., 2ed, Prentice-Hall Inc., 1999

[SMARTSIGN] "Smart Sign", Tommaso Cucinotta, http://sourceforge.net/projects/smartsign

[GPKPKCS#11] "GemSAFE Products", Gemplus, http://www.gemplus.com/products/software/gemsafe/index.html

[SLBCBPKCS#11] "Cyberflex Access SDK", Schlumberger, http://www.cyberflex.com/Products