Si no tienes tu certificado digital en tu tarjeta chip es porque no quieres

(Módulos PKCS#11)

Rafael Calzada Pradas

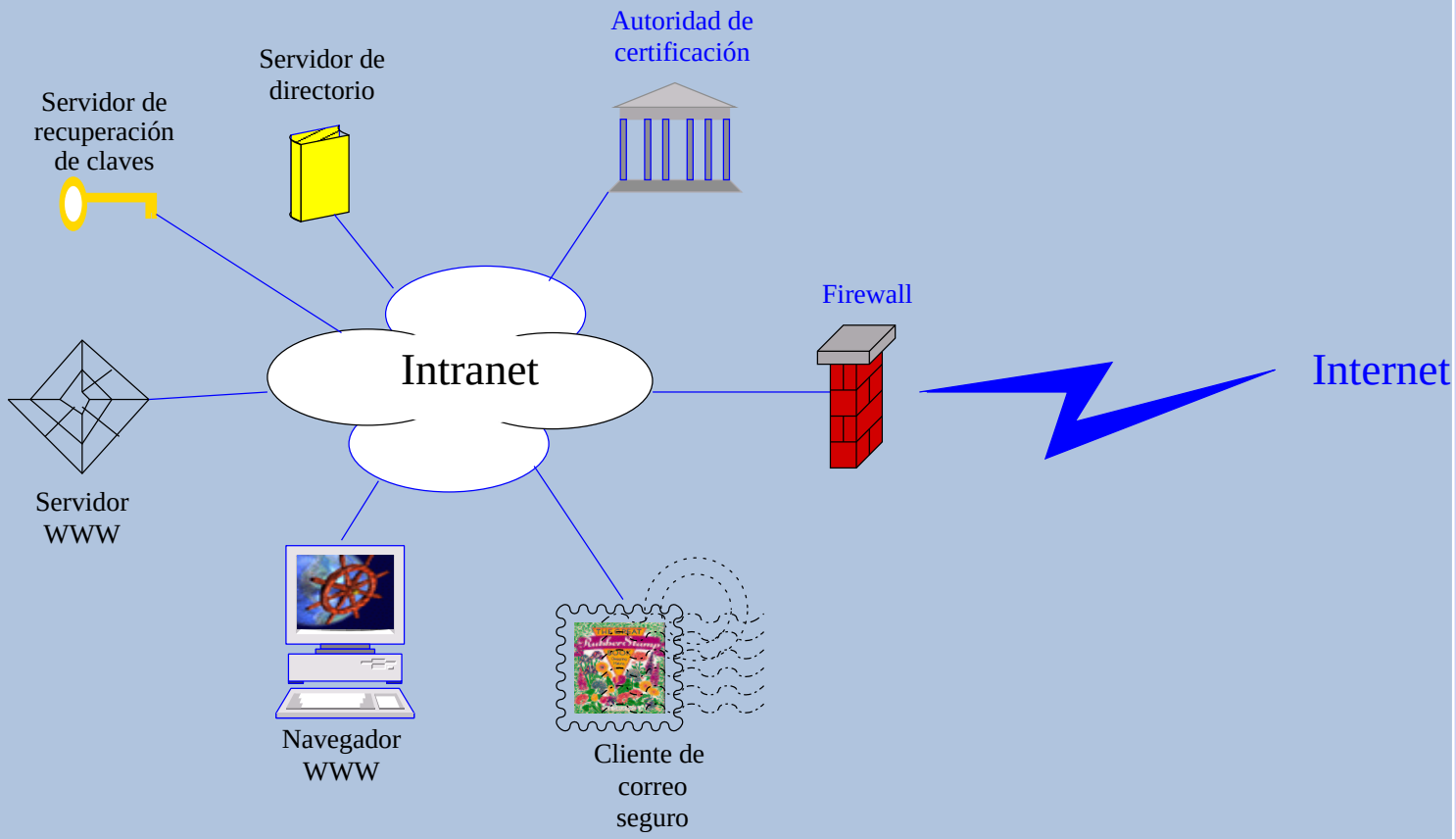
Objetivo

- Desmitificar los módulos PKCS#11
- Fomentar la utilización de tarjertas-chip para almacenar certificados.

Índice

1. Arquitectura de PKI

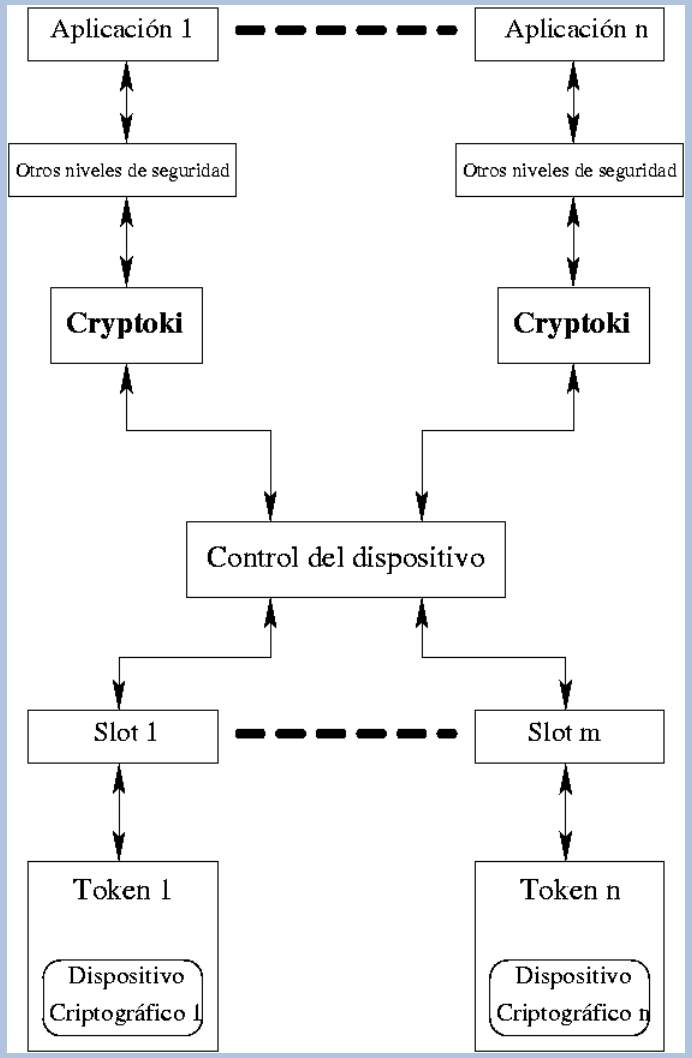
Arquitectura de PKI



2. Módulo PKCS#11

¿Qué es un módulo PKCS#11?

- Librería dinámica que cumple el estándar RSA PKCS#11.
- Interfaz común entre:
  - Aplicaciones (Navegadores, etc)
  - Tokens (Dispositivos que almacenan claves).
- No es obligatorio implementar todas las funcionalidades.
  - Solo es necesario Cifrado y Creación de claves RSA.
- La librería puede implementar las funcionalidades que no implemente el Token.



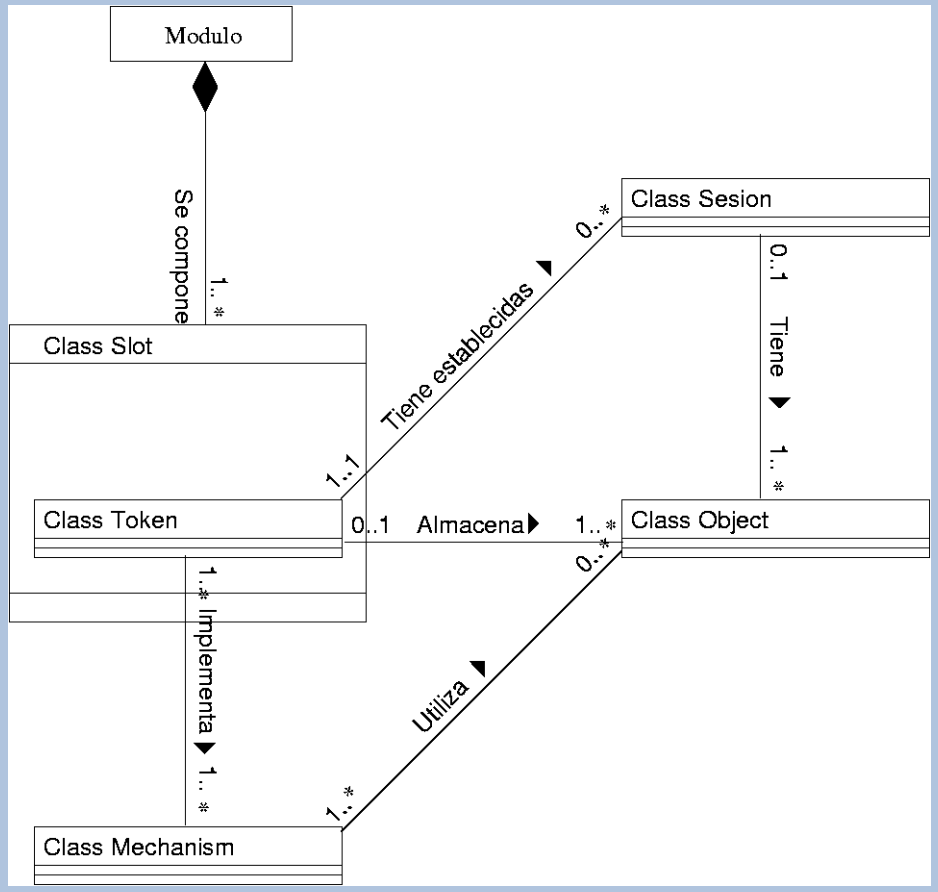
Por qué desarrollar un módulo cuanto Netscape ya tiene uno

- Aumentar la seguridad:
  - Hace falta poseer algo físico (tarjeta) y algo lógico (el PIN).
  - Dificultad para replicar tarjetas.
- Aceptadas por los usuarios.
  - No las prestan *alegremente*.
- Proporcionadas por las entidades financieras.
  - Tienen un coste asequible.

Finalmente, no es tan difícil.

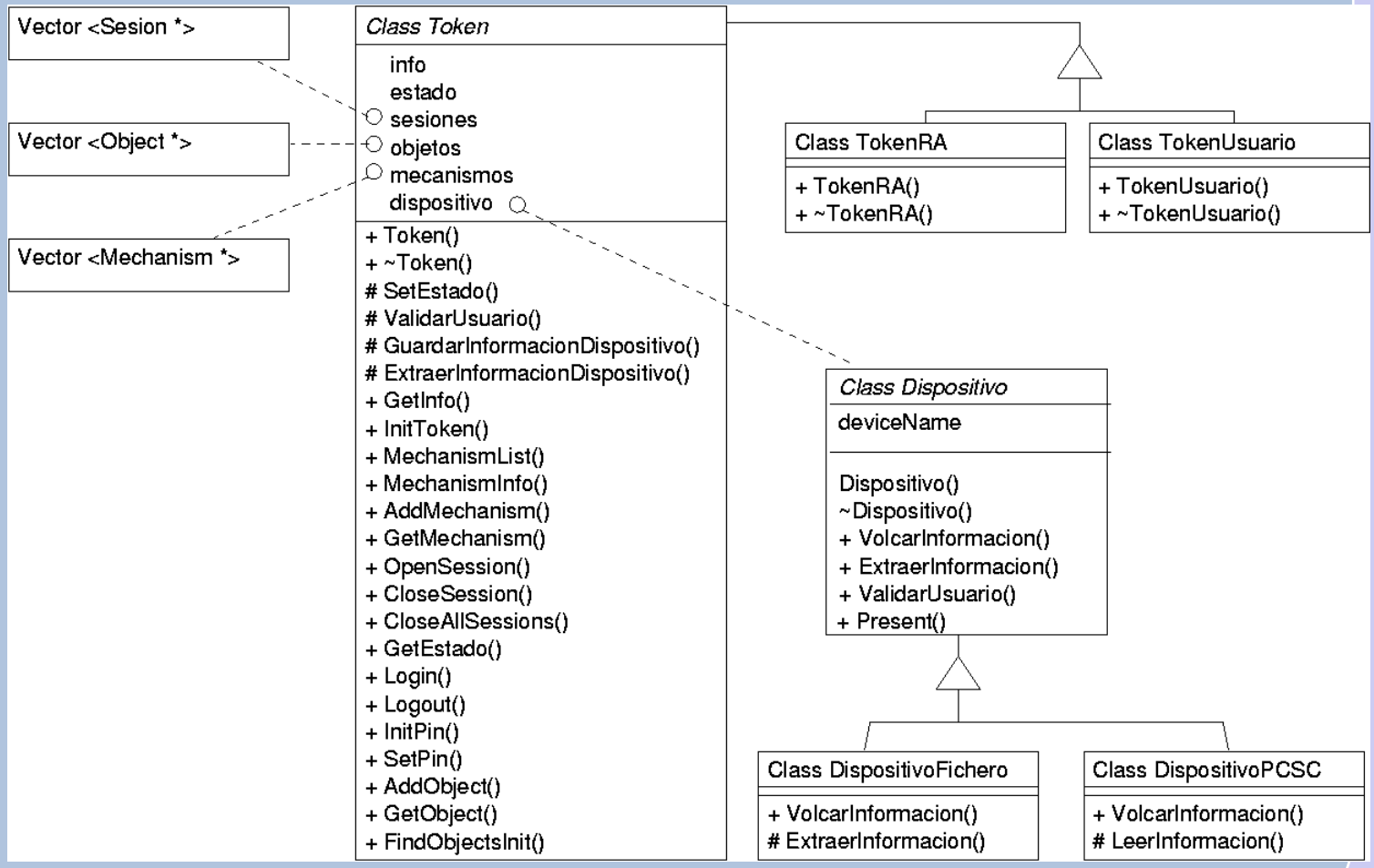
El módulo UC3M-PKCS#11

- Permite tener varios Slots.
- Cada Slot tiene un Token.
- Cada Token tiene un Dispositivo asociado.
- Utiliza OpenSSL para op. criptográficas.
- Emplea PCSC para comunicación con los lectores.
- Por ahora solo disponible para Netscape/Windows.



El módulo UC3M-PKCS#11

- Solo es necesario retocar DispostivoPCSC.
- DispostivoFichero, para realizar pruebas.



Futuros desarrollos

- Sistemas operativos
  - Linux
- Entorno Microsoft
  - Cryptographic Service Provider (CSP)
  - Utilizado por Internet Explorer, Outlook, etc

Aplicaciones de acompañamiento

- Cambio de PIN.
- Copia de Seguridad de la clave asociada al Certificado.
- Acceso a Claves/Certificados no válidos.
- Otras aplicaciones:
  - Cifrado de ficheros.

3. ¿Cómo crear un módulo PKCS#11?

¿Qué necesito para empezar?

- Un ordenador para dedicación exclusiva de la CA.
- Programa de gestión de la CA y RA.
  - OpenCA (gratis).
  - Sun ONE Certificate Server (Comercial)
- Entorno de desarrollo:
  - Windows: Visual C++
  - Linux: gcc
  - JDK.
- Módulo PKCS#11
  - UC3M-PKCS11 (disponible en breve).
  - UMPKCS11 (ya disponible)
  - gpkcs11 (¿Abandonado?)

Ya tengo el software. . . y ahora

- Familiarizarse con el Módulo.
  - Pruebas con DispositivoFichero.
- Pedir información a la entidad financiera:
  - Reservar espacio en la tarjeta (3 o 4 KB).
  - Operaciones de lectura/escritura en la tarjeta.
  - Validación del titular de la tarjeta (PIN).
  - Cambio de PIN.
- Afiliarse al proyecto IRIS-PCA.

Referencias

- Estándar PKCS#11, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11
- Proyecto SCTI-UC3M, http://nuberu.uc3m.es/~rafa/proyecto.html
- UMPKCS11, http://sourceforge.net/projects/umpkcs11
- OpenCA, http://www.openca.org
- PC/SC, http://www.pcscworkgroup.com/