UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

Seguridad Informática

Capítulo 8: Infraestructura de Clave Pública (PKI)

Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2005-2006)

Javier Jarauta Sánchez
José María Sierra
Rafael Palacios Hielscher

Tema 12: Infraestructuras de Clave Pública-PKI

- Introducción
- Certificados digitales: el estándar X.509
- Autoridades de Certificación
- Autoridades de Registro
- Arquitectura de las PKI. Jerarquías
- Tipos de certificados digitales
- Almacenamiento de los certificados
- Fabricantes existentes en el mercado
- Aplicaciones y ejemplos reales de PKI

Conceptos Básicos

La identidad en el mundo real...

En el mundo real un pasaporte (1) demuestra **QUIENES SOMOS**

Los pasaportes son emitidos por una autoridad en cada país.

La emisión por parte de una Autoridad confiable hacen que el pasaporte y la persona sean de confianza

1: No en todos los países existe la figura del DNI

...y en el mundo digital

Certificados digitales

En el mundo digital un certificado representa la identidad de una persona, una máquina,...

...es emitido por una Autoridad de Certificación (e.g. DNIe, FNMT en la que se confía para este fin.

Autoridades de Certificación

El certificado son los datos públicos de la persona (identidad, clave pública y otros,...) firmados por la Autoridad de Certificación.

La firma en el mundo real...

En el mundo real la firma demuestra nuestro acuerdo o autoría de un documento o proceso

La firma está ligada a cada persona y el DNI o pasaporte permiten demostrarlo y comprobar la firma

...y en el mundo digital

- Usamos nuestra clave **privada** para firmar datos.
- Dado que sólo nosotros podemos acceder y usar la clave privada (mediante PIN), esto demuestra nuestra intervención en el proceso.
- No se firma todo el documento sino que se realiza un resumen matemático primero.
- La firma digital, realizada en las condiciones técnicas y administrativas es inquebrantable.
- La ley de firma electrónica 59/2003 da validez legal y regula la firma electrónica

Tarjetas inteligentes

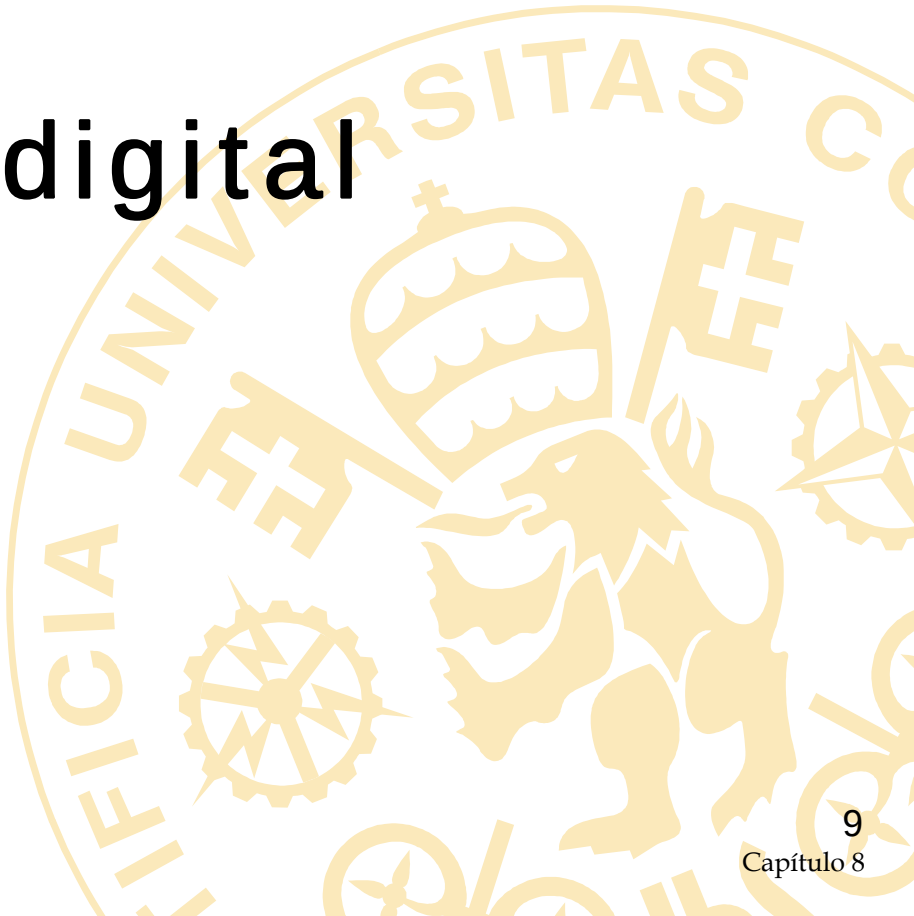
La parte privada de nuestra clave es un elemento que nunca debe ser expuesto.

El medio más seguro de asegurar la parte privada, y por tanto que nuestra identidad digital no pueda ser comprometida, es el uso de **tarjetas inteligentes**

La tarjeta inteligente genera internamente las claves y no permite que sean extraídas por ningún medio

Y realiza los procesos de firma y verificación internamente.

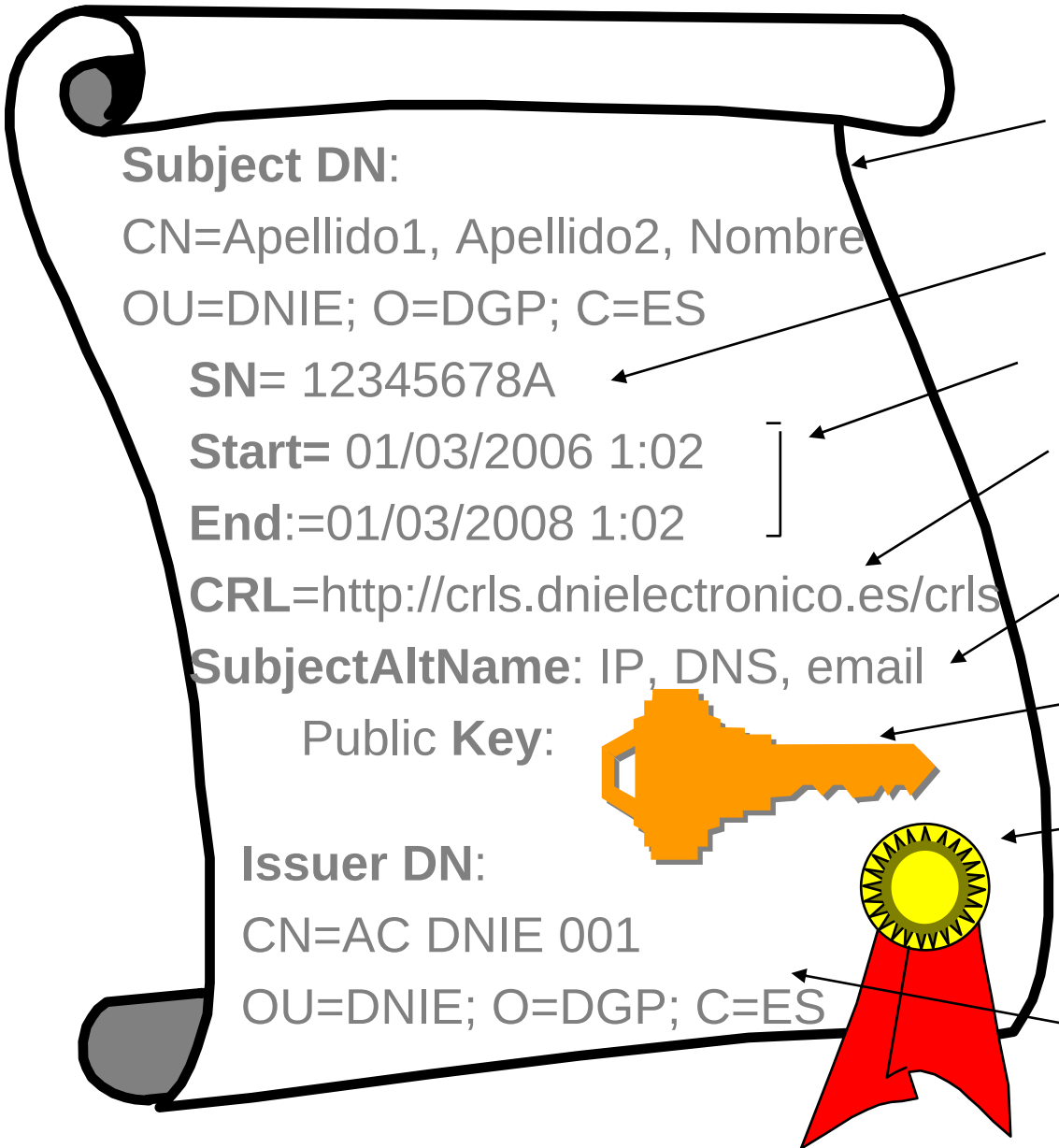
El certificado digital X.509v3



Definiciones

- AC: Autoridad de Certificación
- AR: Autoridad de Registro
- AV: Autoridad de Validación
- DN: Distinguished Name – Nombre distintivo. Identificación unívoca
- CN: commonName – Nombre común
- GN: guivenName – Nombre
- SN : surName - Apellido
- O: Organización
- OU: Unidad organizativa
- C: Country
- CRL: Certificate Revocation List – Certificados revocados

Certificados digitales (X.509.v3)



Nombre único del poseedor

Número de serie

Periodo de validéz

Información para publicar la posible revocación

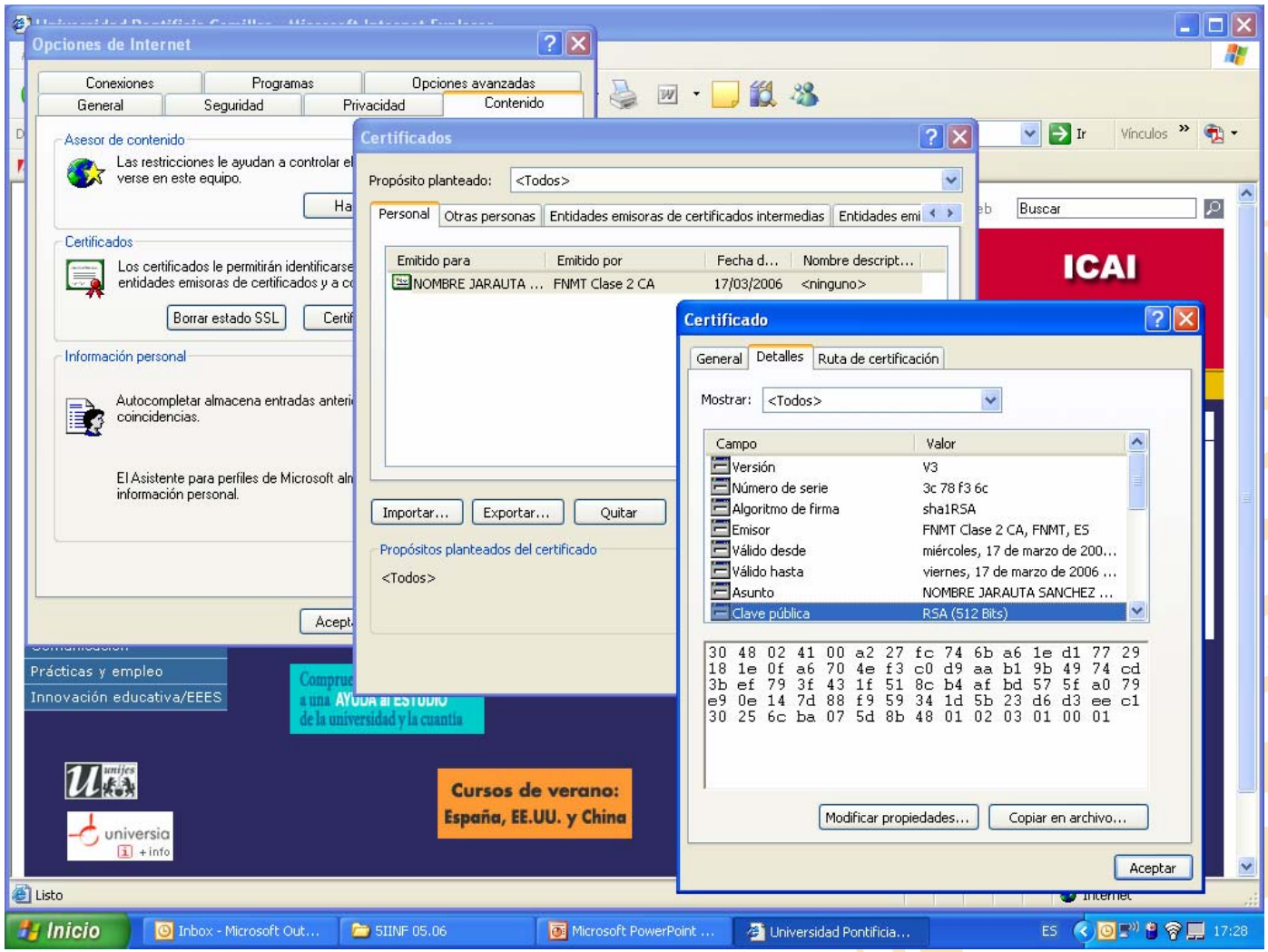
Posibles ‘alias’

La clave pública

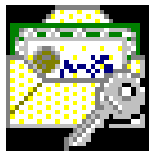
Firma de la Autoridad de Certificación

Nombre de la AC emisora

Estructura detallada

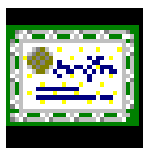


Almacen y formato de certificados



Fichero P12 FNMT JJS.pfx

Almacén PKCS#12 con Clave Privada
(.pfx; .p12)



Certificado FNMT C2 JJS.cer

Certificado Público
(.cer)

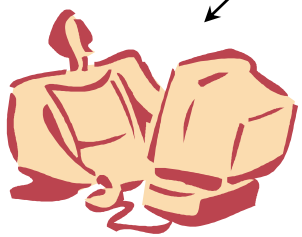
Como se establece la confianza

- ¿Cómo se obtienen las claves públicas?
- ¿Cómo se sabe que la entidad con la que te estás comunicando es quien dice ser?
  - Si se puede confiar en ella
  - Si no se ha retirado la confianza en ella
- Terceras Partes Confiables (TTP – Trusted Third Party)
- Prestadores de Servicios de Certificación (PSC)

Terceras partes confiables (TTP)

Autoridad de Certificación

confianza *confianza*



Alicía **Benito**

Confianza a través de la AC

Elementos del sistema

Alicia

Credenciales &
Clave Pública

Autoridad de
Registro

Certificados

CRLs

Directorio

Benito

Autoridad de
Certificación

Autoridad de
Validación

Aplicación

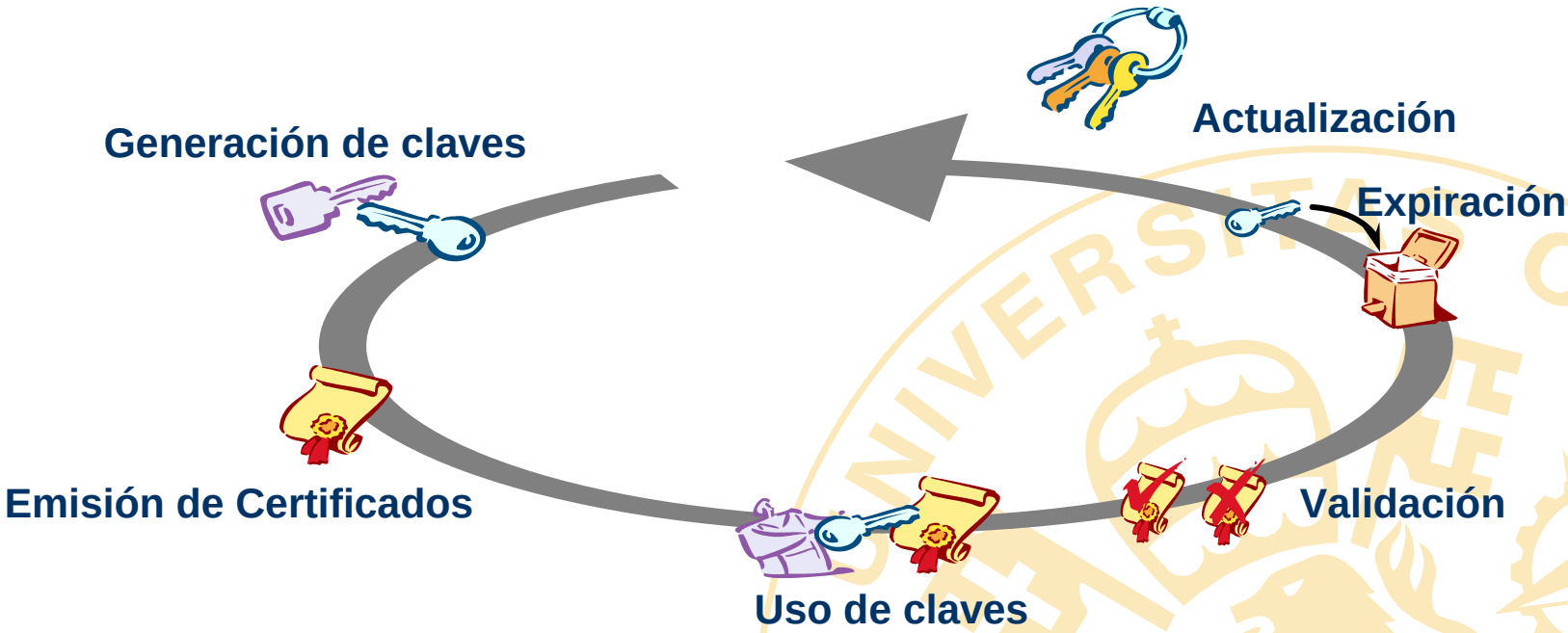
¿es válido el certificado?

Que es una PKI

Infraestructura de clave pública - PKI

- Para organizar correctamente la criptografía, los certificados, las AC, ... de una manera gestionable, flexible y segura, el sistema utilizado es la Infraestructura de Clave Pública – PKI
- La PKI es la Infraestructura que da los servicios de seguridad a la organización utilizando criptografía de clave pública
- Conceptos como AC, AR, renovación de certs automática, recuperación de claves, revocación, cross-certs, no-repudio... Son parte esencial de la PKI
- Hay componentes adicionales al software PKI que son necesarios para el funcionamiento de todo el sistema de confianza

Ciclo de vida de los certificados



Componentes de un sistema PKI

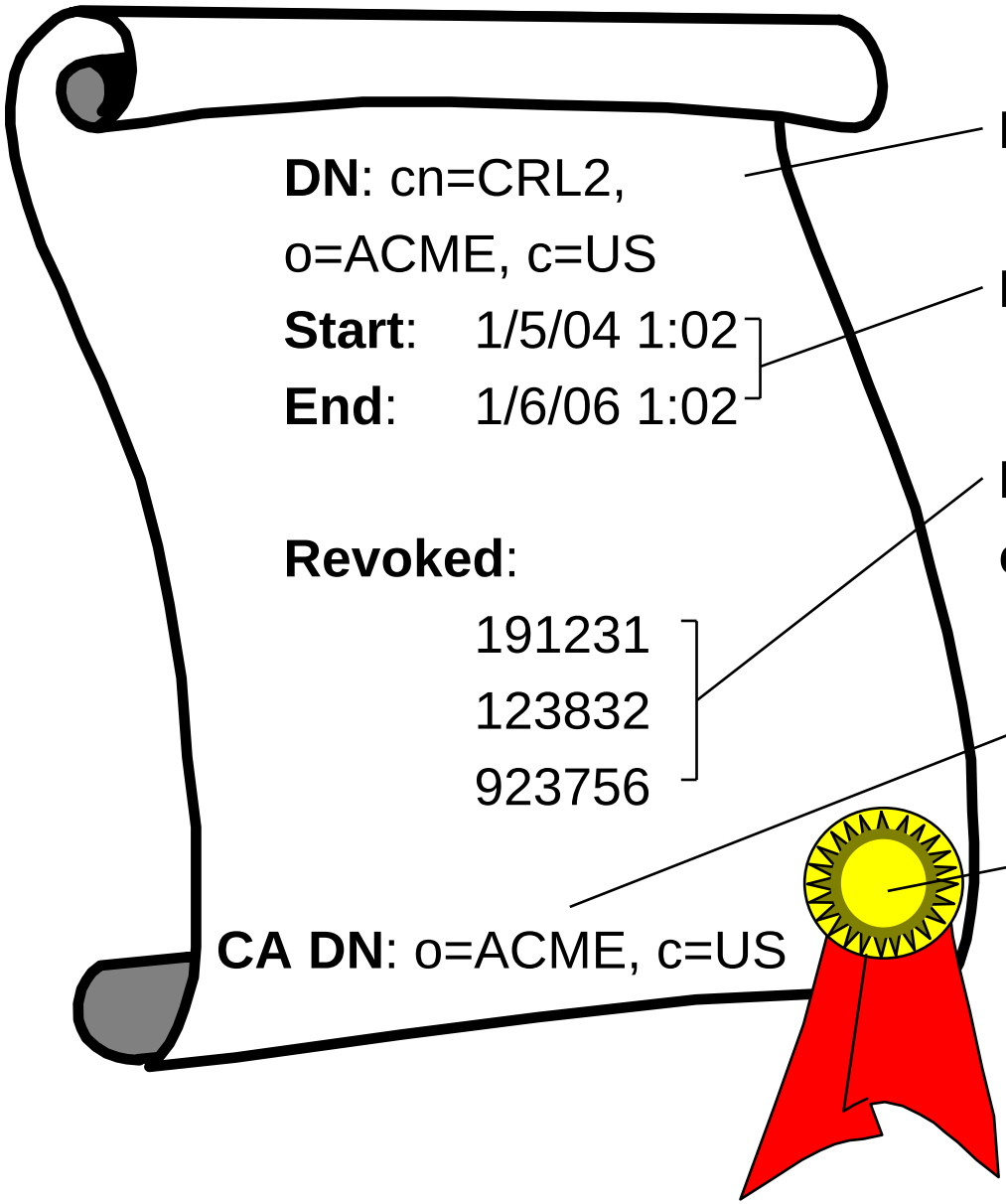
- Autoridad de Certificación (AC)
  - Se encarga de emitir los certificados
- Autoridad de Registro (RA)
  - Se encarga de registrar a los usuarios
- Autoridad de Validación (VA)
  - Se encarga de validar los certificados on-line
- Autoridad de Sellado de Tiempos (TSA)
  - Se encarga de sellar fecha y hora de transacciones
- Directorio de certificados (LDAP)
  - Se encarga de almacenar los certificados
- Hardware criptográfico (HSM)
- Tarjetas Criptográficas (TI)

Tipos de certificados

- Certificados Web para Navegador
- Certificados para VPN
- Certificados de doble o triple pareja de claves
- Certificados cualificados (autenticación y firma)
- Certificados de roaming
- Certificados de atributos

Otros conceptos asociados

¿Qué es y que contiene una CRL[1]?



Nombre único de la CRL

Periodo de validez

Números de serie de los certificados revocados

Nombre de la AC emisora

Firma de la AC en la lista de revocados

[1] Lista de Certificados Revocados

El concepto de varias parejas de claves (varios certificados)

- Un certificado (un par de claves) para firmar y garantizar el no repudio
  - La clave privada bajo control exclusivo del usuario
- Otro certificado (otro par de claves) para cifrar la información almacenada y garantizar su recuperación
  - Se hace backup de la clave privada de cifrado
- Para certificados cualificados (tercer par de claves)
  - Para autenticación del usuario

Otros conceptos (1)

- Declaración de Prácticas y Políticas de Certificación (DPC – CP/CPS)
  - RFC 3647. Documento donde se detalla la estructura, ámbito de uso y características de los certificados emitidos.
  - Reglas de relación entre el Prestador y usuarios
- Certificados cualificados
  - RFC 3039. Certificados separados para Autenticación, Firma y Cifrado
- Dispositivo seguro de creación de firma
  - Sistema que garantice la seguridad de la firma

Otros conceptos (2)

- Certificados (firma) electrónica avanzada
- Certificados (firma) electrónica reconocida
  - Generados por un dispositivo seguro de creación de firma
  - Certificados (firma) avanzada
  - Emitidos por un Prestador de Servicios de Certificación reconocido
  - Cumplimiento de la ley 59/2003
- Jerarquía de confianza
  - Conjunto de AC que mantienen relaciones de confianza entre sí. Raiz y Subordinadas
- Dispositivo seguro de creación de firma
  - Sistema que garantice la seguridad de la firma

Aplicaciones que requieren una PKI

- Aplicaciones Internet
- Correo electrónico
- Comercio electrónico
- EDI
- Acceso Remoto y teletrabajo
- Redes Privadas Virtuales
- Seguridad en la Intranet
- Seguridad en el puesto de Trabajo
- ERP’s
- Secure Single Sing-On
- Y más...

Procedimientos

Generación de certificados

1. En la tarjeta del usuario (o en el PC) se genera un par de claves Cpub y Cpriv
2. La Cpriv se protege con un PIN y nunca sale de la tarjeta (o almacén de software seguro)
3. Se envía la Cpub a la AC (PKCS#10) solicitando un cetificado
4. La AR verifica la identidad del usuario y proporciona a la AC dichos datos junto con su aprobación
5. La AC junta la Cpub, los datos del usuario, y sus políticas y los firma con su Cpriv(AC) para formar el certificado digital
6. La AC envía el certificado al usuario (PKCS#7) y se carga en la tarjeta (o almacén Sw)

Revocación y Validación de Certificados

- REVOCACIÓN

1. Si el usuario pierde el PIN, la tarjeta o cree que ha sido comprometido, solicita a la AC que revoque su cert.
2. La AC emite cada cierto tiempo (minutos, horas, días) una lista de certificados revocados (CRL)
3. Cualquier aplicación que quiera utilizar el certificado se deberá ir a la CRL para verificar que no está revocado

- VALIDACIÓN

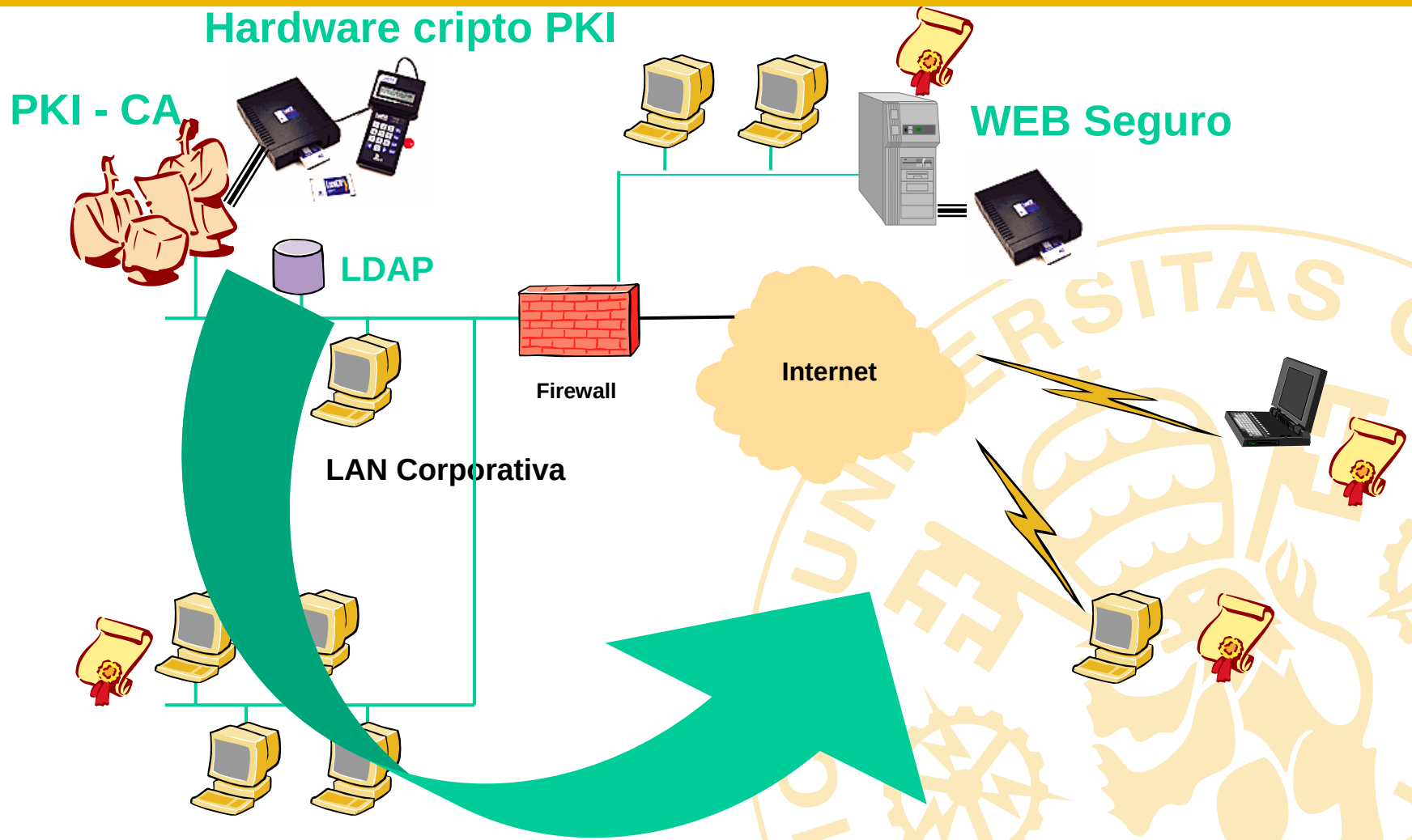
1. Las Autoridades de Validación AV (suele haber varias) llegan a acuerdos con la AC para que les pase las CRL. Cuanto más actualizada mejor
2. Cuando una aplicación quiere saber el estado del certificado en tiempo real, lo solicita a la AV. Se utiliza el protocolo OCSP

Hardware criptográfico Y tarjetas

Tipos de dispositivos HW

- **Equipos de generación y almacenamiento de claves**
  - Generación de ruido pseudoaleatorio o totalmente aleatorio
  - Comprobaciones de primalidad y claves débiles
  - Almacenamiento seguro (anti-tamper) de claves privadas (root-key)
- **Tarjetas inteligentes con procesamiento**
  - Generación segura de pareja de claves publica y privada
  - Almacenamiento seguro de la clave privada
  - Proceso de firma o cifrado realizado en la tarjeta

Estructura de una PKI



PKI: Hw de gestión cripto

- Dispositivos para generación, gestión y almacenamiento de claves.
  - Generación de las claves simétricas y asimétricas: hardware aleatorio específico o según Anexo C del estándar ANSI X9.17
  - Algoritmos asimétricos: RSA (2048), DH (1024), DSA (1024)
  - Algoritmos simétricos: DES (56), 3DES(168)
  - Funciones Hash: SHA-1(160), MD5(128)
  - Autenticación de mensajes: HMAC-MD5, HAMC-SHA1
  - Almacenamiento seguro en hardware protegido (tamper)
  - Almacenamiento de backup en tarjetas PCMCIA
  - Dispositivos internos o externos con interfaces PCI y SCSI

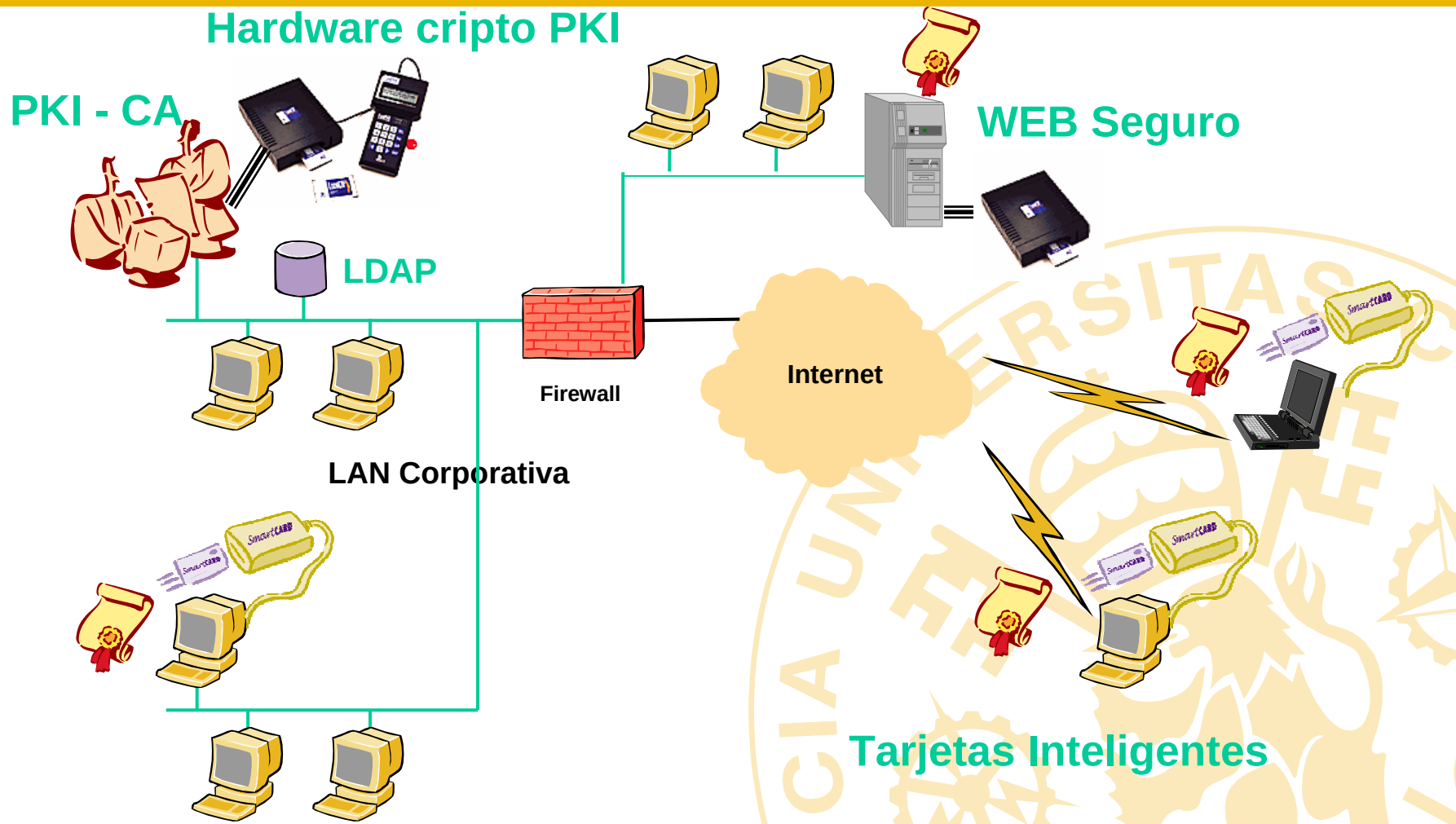
  - Acceso a claves disgregado en múltiples usuarios “M de N”

PKI: Rendimientos RSA-3DES

- Consideraciones sobre rendimientos en dispositivos hardware para RSA y 3DES
  - Una operación RSA de 1024 se realiza en menos 5 ms
  - Chips comerciales trabajan entre 3 Mbps y 64 Mbps con DES
  - ASICs especializados alcanzan hasta 1 Gbps
  - Las últimas implantaciones hard con 3DES alcanzan 23 Mbps

  - IDEA es 6 veces más rápido que 3DES
  - RC5 es 8 veces más rápido que 3DES
  - Blowfish es 12 veces más rápido que 3DES

Tecnología de Tarjetas Inteligentes



Tipos de tarjetas inteligentes

- Tarjetas de memoria
  - No disponen de capacidad de proceso, sino solamente memoria para almacenar información con diferentes tamaños
- Tarjetas criptográficas
  - Disponen de capacidad de proceso, pueden generar claves y realizar cifrado
  - Disponen además de memoria para almacenar certificados y claves (la clave privada nunca sale de la tarjeta)
- Java Cards
  - Además de la capacidad de proceso, disponen de un máquina virtual Java que permite ejecutar applets
- Windows for Smart Cards
  - Respuesta de Miccrosof para poder ejecutar applets

TI: Almacén y proceso seguro

- Dispositivos para generar y almacenar de forma segura las claves
  - Proporciona autenticación de dos factores (lo que tiene y conoce)
  - Existen tarjetas de memoria, de firma, de generación de claves y criptoprocesadoras completas.
  - Almacenan de forma segura la clave privada de su propietario
  - Almacenan de forma segura el certificado de su propietario
  - Pueden generar la pareja de claves y almacenar la privada
  - Pueden firmar e incluso cifrar
  - Existen modelos con memorias EEPROM de 8k, 16k y 32K
  - Procesan algoritmos simétricos/asimétricos 3DES, RSA, MD5
  - Cumplimiento de estándares ISO 7816, PKCS#11,
  - Lectores con interfaces PC/SC, PCMCIA, diskette
  - Interfaces USB directo sin lector

TI: Rendimientos RSA

- Consideraciones sobre rendimientos en tarjetas inteligentes con RSA
  - La generación de claves RSA de 1024 oscila entre 1,5 y 4 minutos según fabricante y resultado de los test de primalidad
  - Una operación RSA de 1024 se realiza en menos de 1 segundo
  - Es importante asegurarse de la forma de generar las claves
  - El procesamiento criptográfico en las TI, tiene un bajo rendimiento y en la práctica solo se utiliza en circunstancias especiales

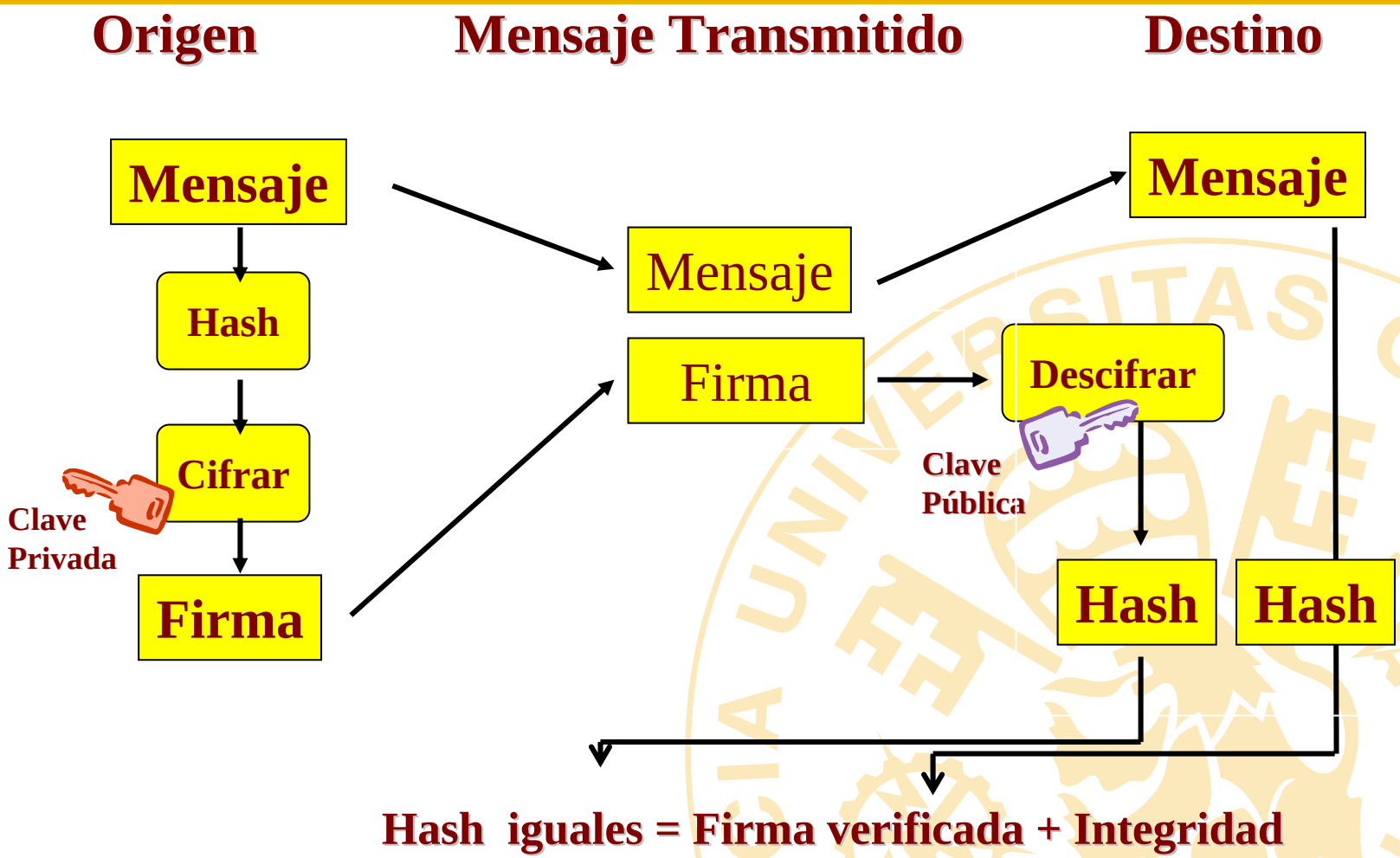
Principales aplicaciones y ejemplos reales

Aplicación: SSL

- SSL - Secure Sockets Layer. Estándar de facto para los navegadores
- Actualmente conocido también como TLS Transport Layer Security
- SSL V2 solo autenticación con certificado del Servidor
- SSL V3 autenticación mutua con certificado del Servidor y del Navegador

- PROCEDIMIENTO
  1. El navegador cliente inicia una sesión https:
  2. El Web Server envía al navegador su certificado
  3. El navegador genera una clave de sesión aleatoria que cifra con la clave pública (certificado) del Web Server
  4. El Server descifra la clave de sesión y la pasa a un algoritmo simétrico (RC4, DES, AES…)
  5. Se establece un túnel cifrado durante la sesión SSL
  6. Si es SSL V2 solicita usuario/password para autenticar al usuario
  7. Si es SSL V3 solicita el certificado de usuario o DNIe

Aplicación: Firma electrónica



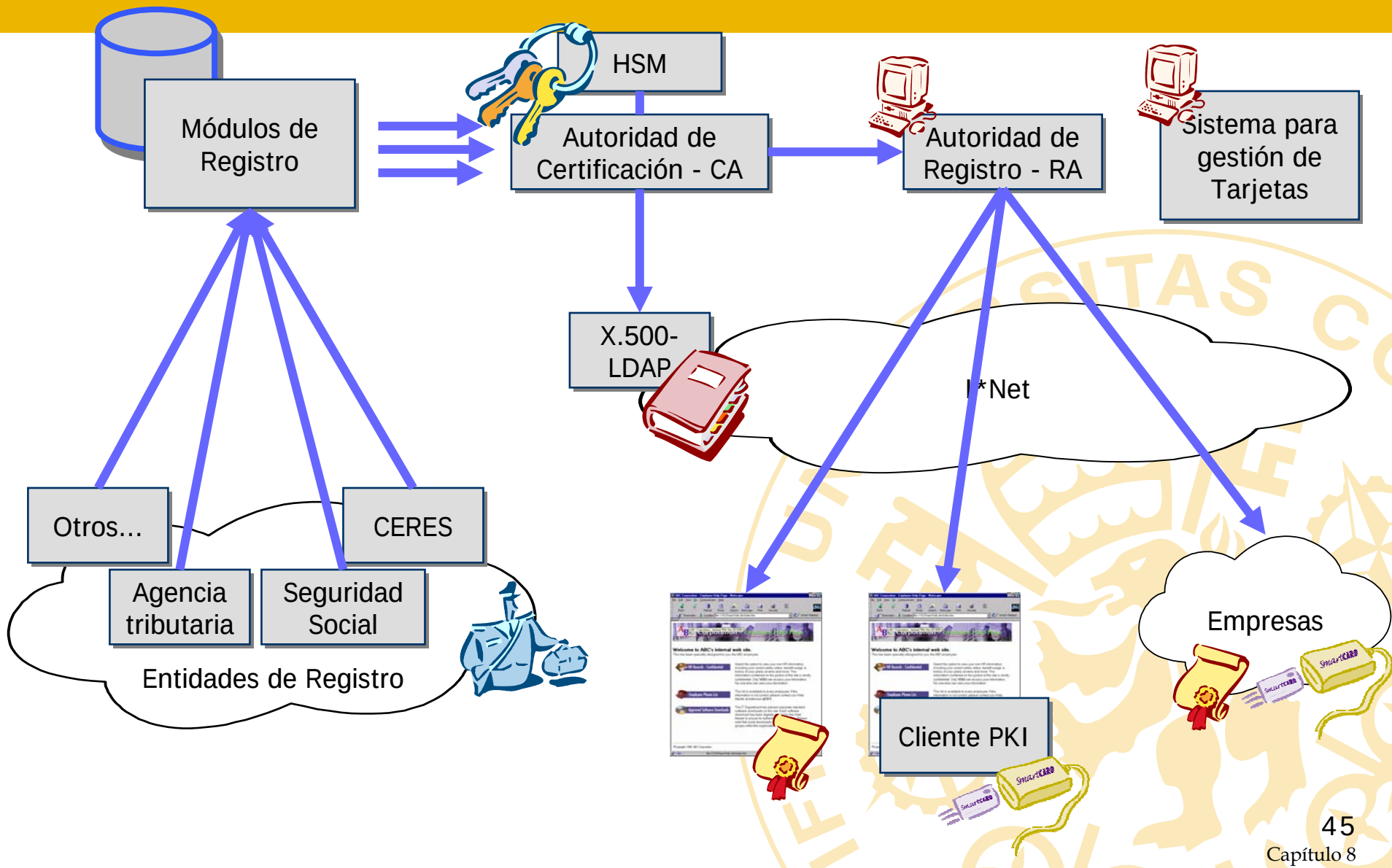
Principales fabricantes

- Entrust: http://www.entrust.com/ Canadiense, el de mayor cuota de mercado. Inventor del concepto PKI
- Safelayer: http://www.safelayer.com/ Fabricante español, con proyección internacional
- Verisign: http://www.verisign.com/ Enfocado a servicios y a certificados para Servidores SSL
- RSA: http://www.rsasecurity.com/ El pionero en la tecnología criptográfica

Autoridades de certificación

- Fabrica Nacional de Moneda y Timbre -CERES (Gobierno) (http://www.cert.fnmt.es)
- Camerfirma - Cámaras de comercio
- FESTE - Notarios y registradores
- CatCert: Cataluña
- Izempe: País Vasco
- Autoridades de Certificación Internas de empresas
- Dirección General de la Policía: DNI Electrónico DNIe (hhtp://www.dnielectronico.es)

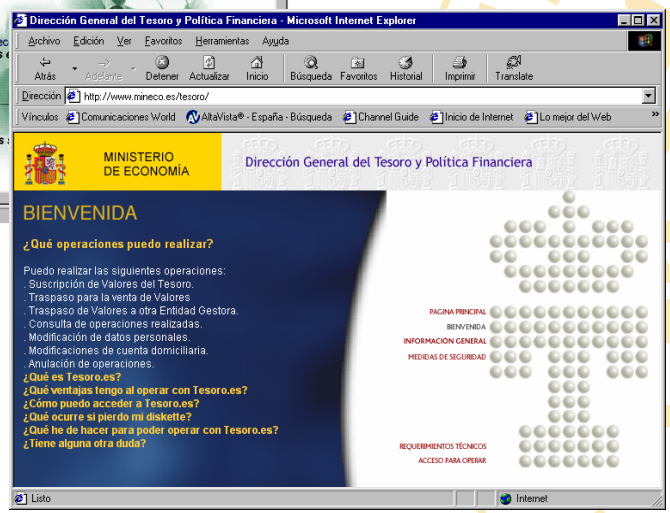
Arquitectura Técnica: FNMT-CERES



Aplicaciones basadas en la CA de FNMT

La Agencia Tributaria se convierte así en la primera Administración Tributaria que lleva a cabo una experiencia de estas características con firma digital de ciudadanos

La SEGURIDAD SOCIAL ofrece mediante su oficina virtual la ventanilla de atención al usuario en Internet a través de la que ciudadanos y empresas pueden realizar consultas y gestiones que venian realizando, de forma presencial, en cualquiera de sus oficinas.



El TESORO PÚBLICO ha desarrollado un servicio para que, con comodidad y sencillez, el ciudadano pueda llevar a cabo la compra, el traspaso y la venta de sus Valores en Internet, además de poder consultar las operaciones realizadas.