Iniciación a PKI (Public Key Infraestructure)

29 de marzo de 2007

INDICE

Criterios de Seguridad según B.O.E. 26-6-2003

Autenticación

• Identifica a las entidades implicadas en una transacción y **garantiza** que estas entidades son lo que dicen ser (emisor y receptor). También conocida como “Autenticación fuerte”. Necesita del establecimiento de un **Círculo de Confianza** y de una infraestructura de Certificación (PKI) que lo mantenga y lo gestione.

Integridad

• Garantía de que una información, o un conjunto de datos en general, no es modificado en el transcurso de la comunicación desde el generador al receptor.

No repudio

• Garantía de que el emisor es el autor de la transacción que ha sido firmada.

Confidencialidad

• Capacidad de mantener la información fuera del alcance de usuarios no autorizados. Para ello se utiliza el protocolo estándar Secure Socket Layer (SSL), que mediante técnicas criptográficas oculta el contenido de la información que viaja a través de la Red.

Firma Electrónica con Certificados X.509 v3

Cifrado

- Proceso mediante el cual una determinada información se ofusca por medio de un algoritmo determinado, haciendo uso de una clave conocida.

Tipos de claves

Claves Simétricas

- Permiten cifrar y descifrar datos utilizando la misma clave.
- Se utilizan longitudes de clave cortas: 8, 16, 24 bits.

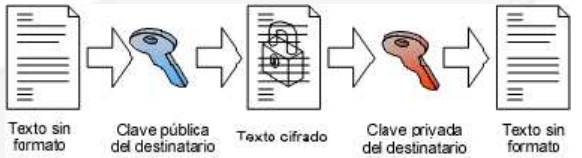
Claves Asimétricas

- Son claves complementarias. Solamente pueden ser generadas una a partir de la otra.
- Lo cifrado con una sólo puede descifrarse con su complementaria.
- Las claves se denominan respectivamente, pública y privada.
- La clave pública puede difundirse.
- La clave privada debe ser custodiada por su propietario.
- Longitudes de clave a partir de 512 bits.

Tipos de cifrado

- **Cifrado simétrico (ej: 3DES, AES)**
  - Proceso eficiente
  - Misma clave para todo el proceso
  - Emisor y receptor deben conocer la clave

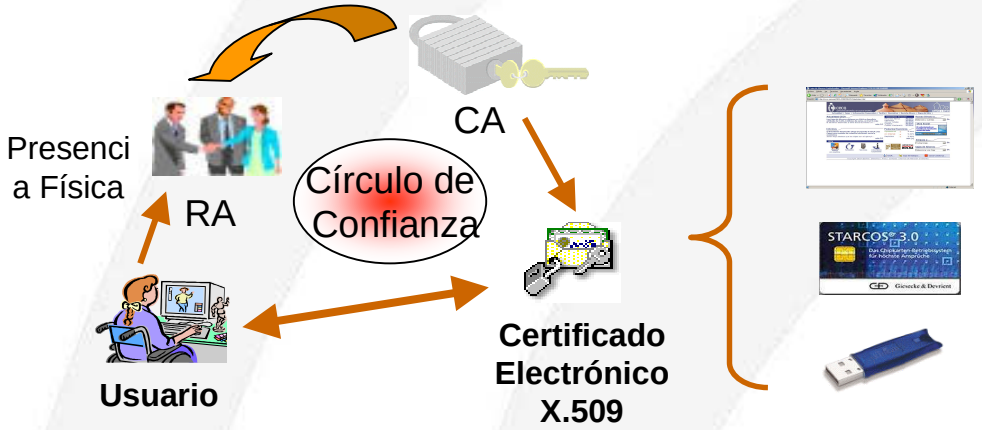
- **Cifrado asimétrico (ej: DSA, RSA)**
  - Proceso costoso
  - Intervienen claves asimétricas
  - La clave privada no se intercambia



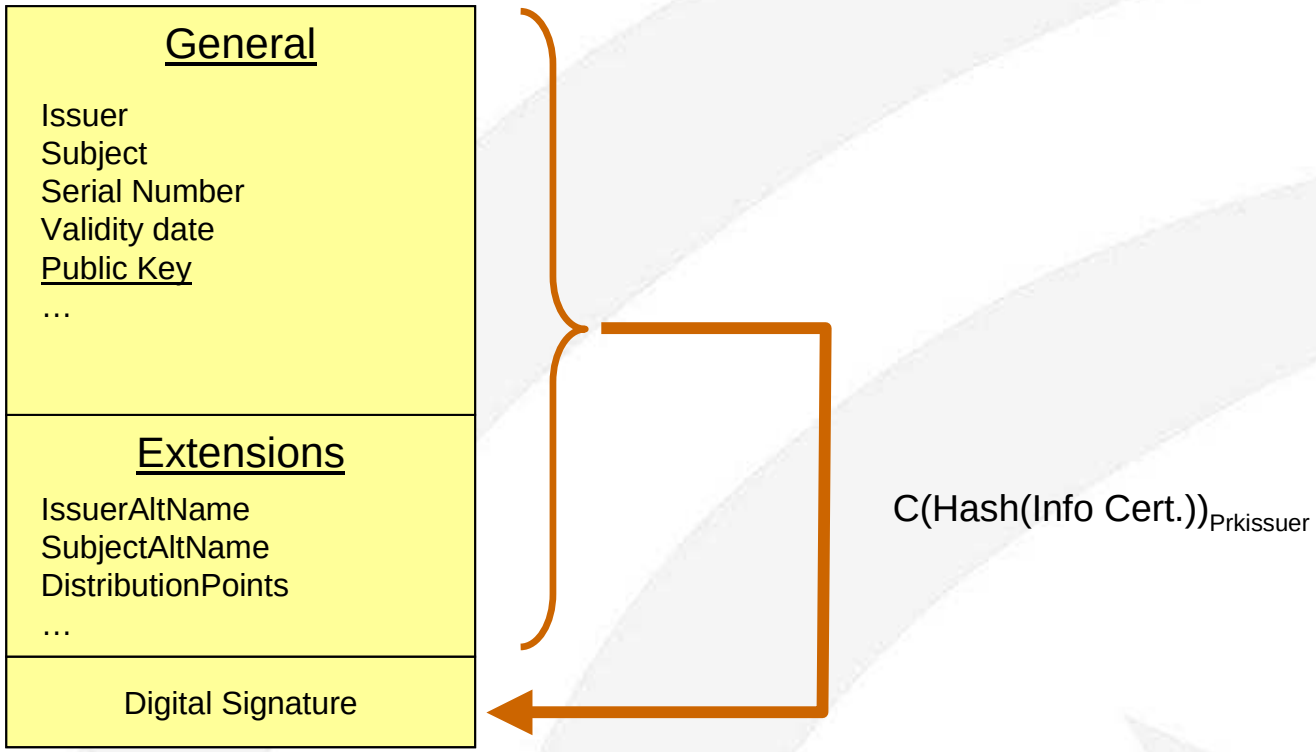
- **Cifrado híbrido (ej: SSL)**
  - Aúna las ventajas de ambos
  - Eficiencia y seguridad

Un paso más, los certificados digitales

- Componentes basados en sistemas de clave pública que identifican de manera telemática a una persona física o jurídica.
- Son emitidos por Entidades de Certificación (CA) que garantizan la identidad de responsable del certificado. Para ello delegan en Autoridades de Registro (RA).
- Contienen información del responsable y su clave pública.
- Los certificados y claves privadas pueden almacenarse en dispositivos software (keystores) o hardware (HSM, SmartCards, token USB, etc.)



Estructura de un certificado digital X.509v3



Autenticación

• El sistema de autenticación envía un dato generado por él mismo al sujeto que se autentica.

• El sujeto cifra con su clave privada el dato y lo envía junto con su certificado digital al sistema de autenticación.

• El sistema de autenticación descifra el dato con la clave pública del sujeto y lo compara con el dato original.

• Se verifica el certificado para comprobar su validez.

• Ej. SSL con autenticación mutua.

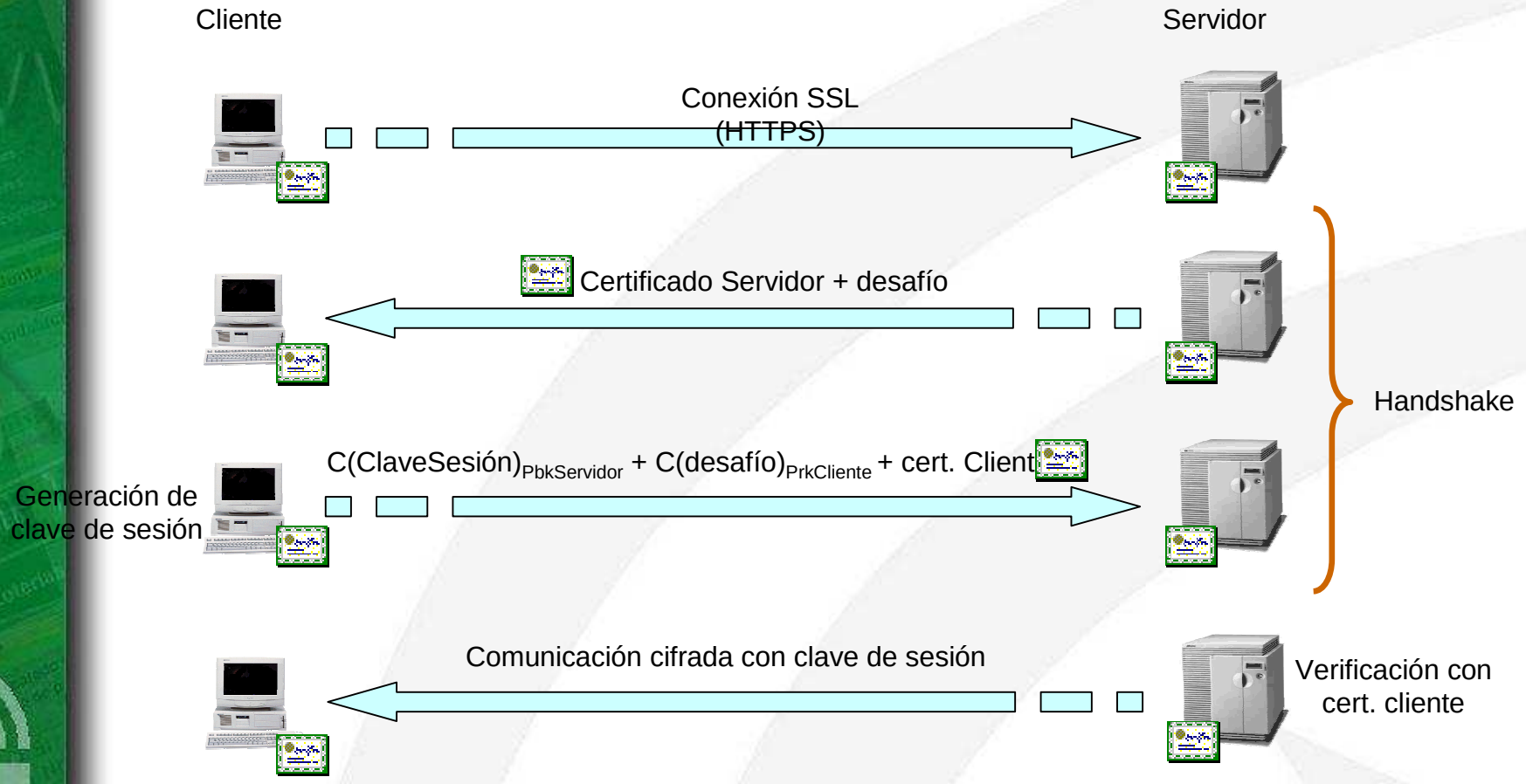
Firma digital

• Se obtiene un resúmen de los datos a firmar, y se procede a la firma del mismo con la clave privada del firmante.

• Los datos se envían al receptor junto con la firma y el certificado del firmante.

• El receptor descifra la firma con la clave pública que contiene el certificado del firmante y compara el resúmen con el calculado por el propio receptor a partir de los datos recibidos.

Mecanismo de autenticación mutua con SSL



Firma electrónica

Ley de Firma 59/2003

- **Firma electrónica**: conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- **Firma electrónica avanzada**: firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- **Firma electrónica reconocida**: la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Firma electrónica reconocida ⇔ Firma manuscrita

Firma Electrónica con Certificados X.509 v3

Prestadores de Servicios de Certificación (PSC o CA)

- Son entidades que despliegan y mantienen Entornos de Confianza en ámbitos bien definidos
- Ponen a disposición de sus usuarios herramientas para solicitar la obtención de certificados digitales de forma telemática.
- Gestionan el ciclo de vida de los certificados digitales emitidos.
- Dan servicios de consulta de estado de certificados, Time Stamping, etc.
- Pueden poseer infraestructuras de Autoridad de Registro (RA), o delegar este servicio.
- Definen jerarquías de certificación que permiten dar servicio a sus usuarios.
- Definen sus políticas de funcionamiento en Documentos de Prácticas de Certificación (DPC).
- Ejemplos: FNMT, DGP (eDNI), Firma Profesional, etc.

Servicios de Certificación

•**Consulta de Estado de Certificados (CRLs).** La CA ha de publicar el estado de los certificados (válido, revocado, suspendido) mediante las herramientas y protocolos pertinentes.

- •**CRL (Certificate Revocation List)**
- •**OCSP (Online Certificate Status Protocol)**

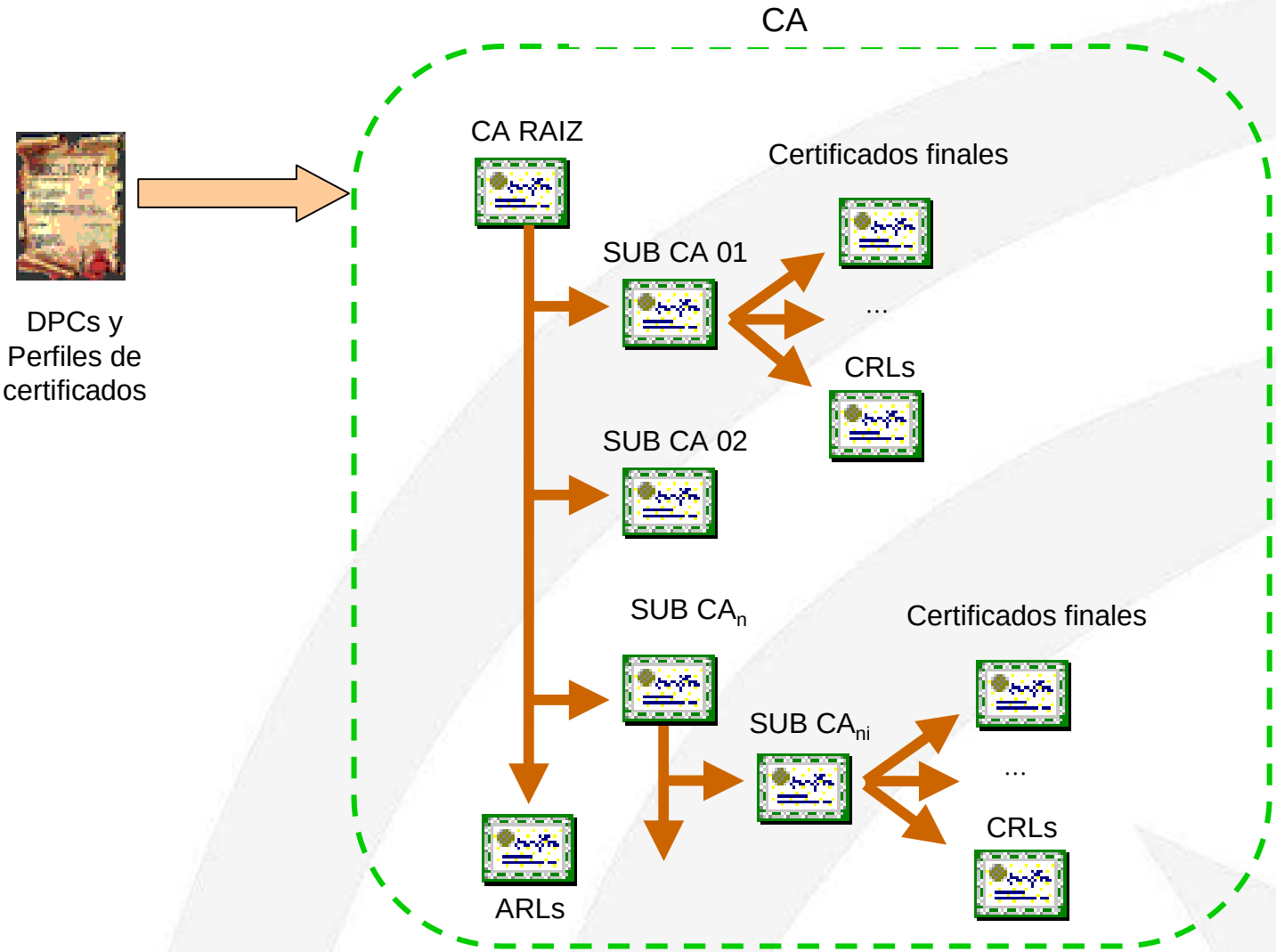
•**TimeStamping**. En toda transacción de firma se ha de constatar el instante de tiempo para que sea válida, y además ese instante de tiempo ha de estar acreditado por un Tercero de Confianza denominado Autoridad de Fechado Digital (TSA).

• **Certificación de RA's.** Formación y acreditación de Autoridades de Registro para la gestión de solicitudes de certificados. Se provee de las herramientas software y hardware necesarias a los registradores.

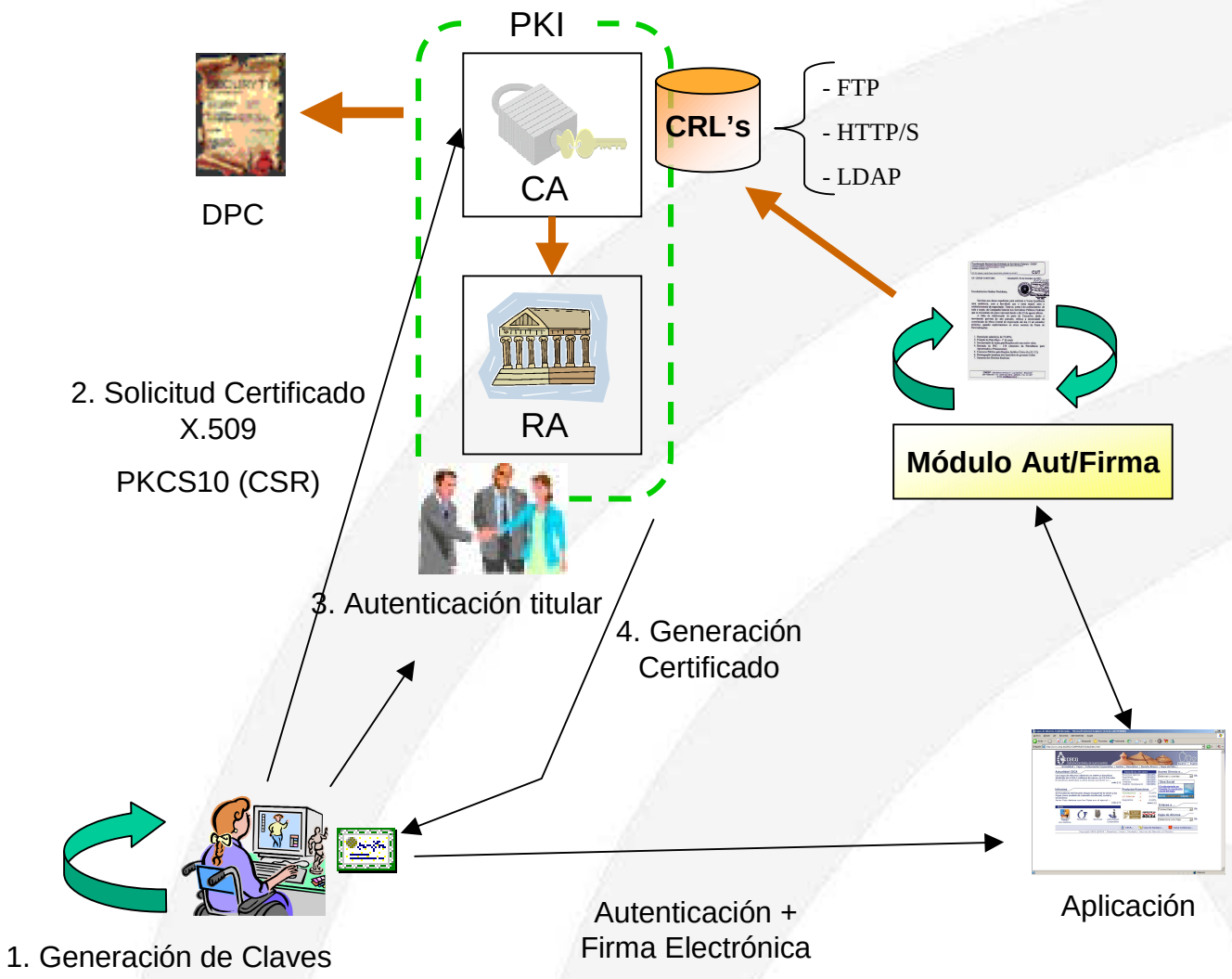
• **Notariado Electrónico**. Almacenamiento y conservación de transacciones de firma en el tiempo proporcionando los métodos de disponibilidad pertinentes (según criterios de seguridad del BOE).

• **Outsourcing.** Suministro de servicios de CA para entidades privadas que lo necesiten. Incluyen un convenio de formación e implantación de RA's exclusivas para estas entidades privadas.

Jerarquías de certificación



Visión global de un sistema PKI



INDICE

I – Conceptos básicos

II – Validación de Certificados Electrónicos

Validación de certificados (I)

¿Qué es la validación de un certificado?

Es la verificación de que el certificado es válido, integro y no ha sido comprometido.

¿Por qué se debe validar un certificado?

Es la forma de garantizar que en el momento de realizar una firma o una autenticación, el receptor del certificado puede confiar en él plenamente.

¿Cómo se lleva a cabo?

- **Validación de integridad del certificado**
  - Cumplimiento del estándar X.509v3
  - Fecha de caducidad.
  - Firma del emisor.
- **Consulta del estado del certificado**
  - Válido.
  - Revocado.
  - Suspendido.
- **Validación de la cadena de certificación**

Según RFC 3280

Validación de certificados (II). Métodos de consulta

- **CRL (Certificate Revocation List)**
  - Listas firmadas que publican los certificados comprometidos.
  - Son emitidas por el PSC emisor de los certificados.
  - Pueden ser completas, segmentadas, indirectas, etc.
  - Pueden ser publicadas por HTTP/S, LDAP, FTP, etc.
  - Tiempo de latencia alto.
- **OCSP (Online Certificate Status Protocol)**
  - Protocolo en línea para consulta de estado de certificados.
  - Es independiente del protocolo de comunicación.
  - Es el método más fiable.

Muchas Gracias