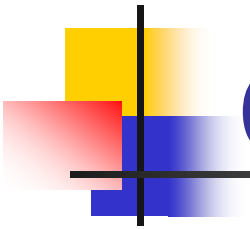
# Bloque II
# Sistemas de autenticación

**Firma digital y certificados digitales**

Seguridad en Redes de Comunicaciones

María Dolores Cano Baños



# Contenidos

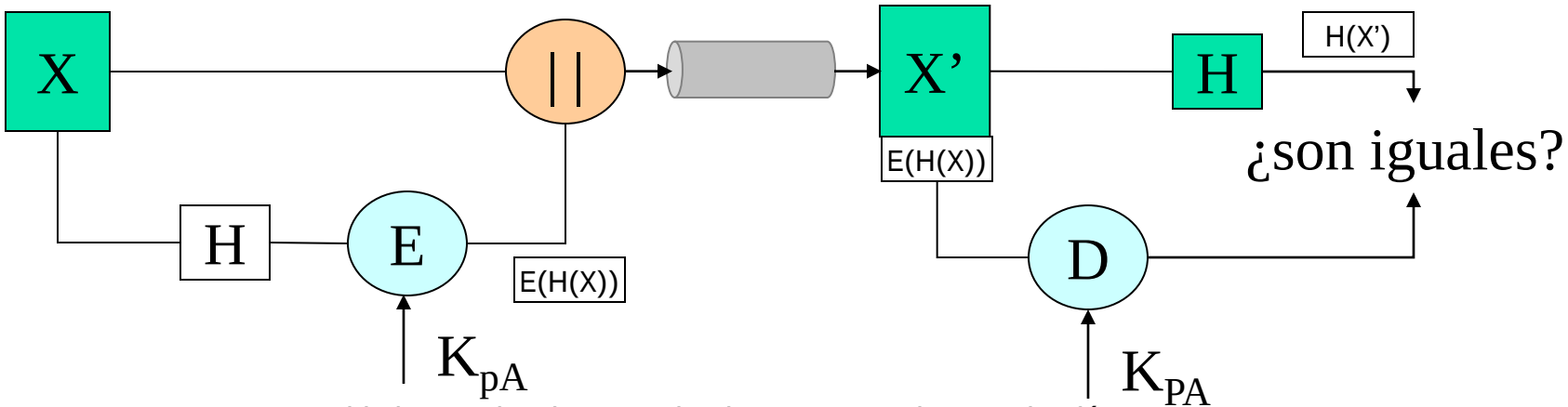
# Firma digital

- Criptografía de clave pública (asimétrica)

- La FIRMA DIGITAL debe tener las siguiente propiedades:
  - Poder verificar autor, fecha y hora de la firma
  - Poder autenticar el contenido del mensaje a la hora en la que se firmó
  - Debe estar verificada por un tercero para evitar disputas

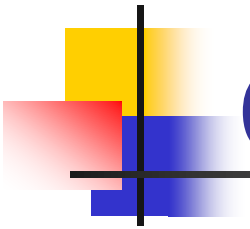
# Firma digital

- Cualquier FIRMA DIGITAL:
  - Firma ≡ patrón de bits dependientes del mensaje firmado
  - Utilizará información única del emisor para evitar denegación y falsificación
  - Sencilla de crear
  - Sencilla de reconocer y verificar
  - Falsificarla debe ser computacionalmente no factible



# Firma Digital

- Firma Digital Directa
  - Sólo intervienen los dos comunicantes
  - Destino conoce clave pública de emisor
  - Firmamos mensaje completo ó hash del mensaje con $K_p$ emisor
  - Problema: seguridad de la clave secreta
- Firma Digital Arbitrada
  - Una tercera entidad actúa como árbitro
  - Funcionamiento general: todos los mensajes pasan por el árbitro que comprueba la validez de origen y contenido
  - Confiabilidad total en el árbitro



# Contenidos

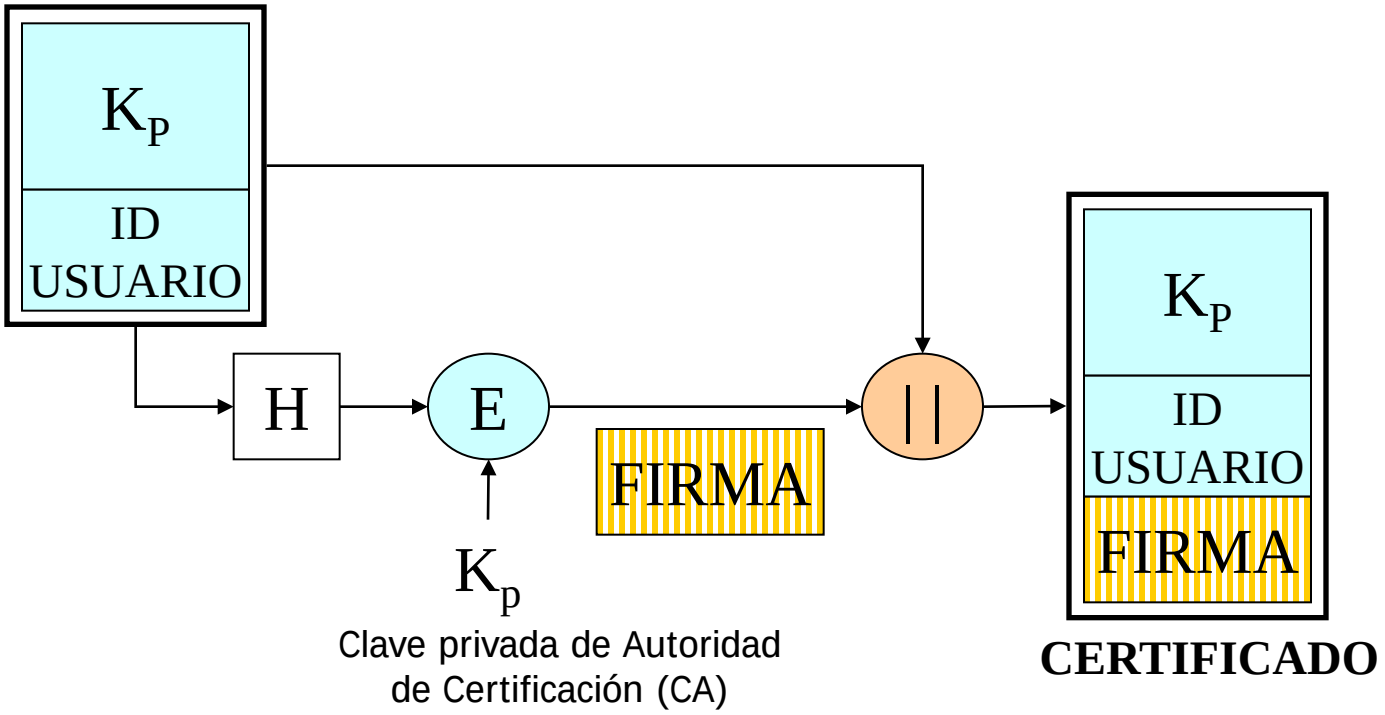
3.1 Introducción

3.2 Firma digital ✓

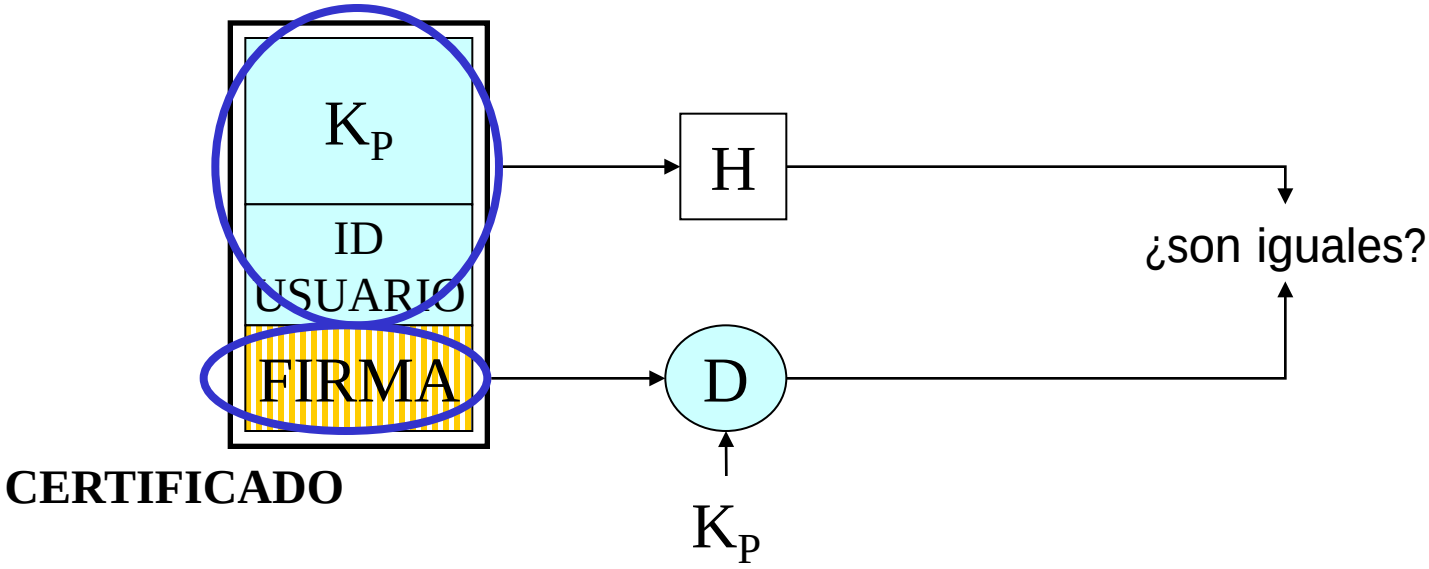
3.3 Certificados

# Certificados

- Las claves públicas han de ser “públicas” ⇨ ¿problema de suplantación?
  - Solución: certificados de clave pública



# Certificados



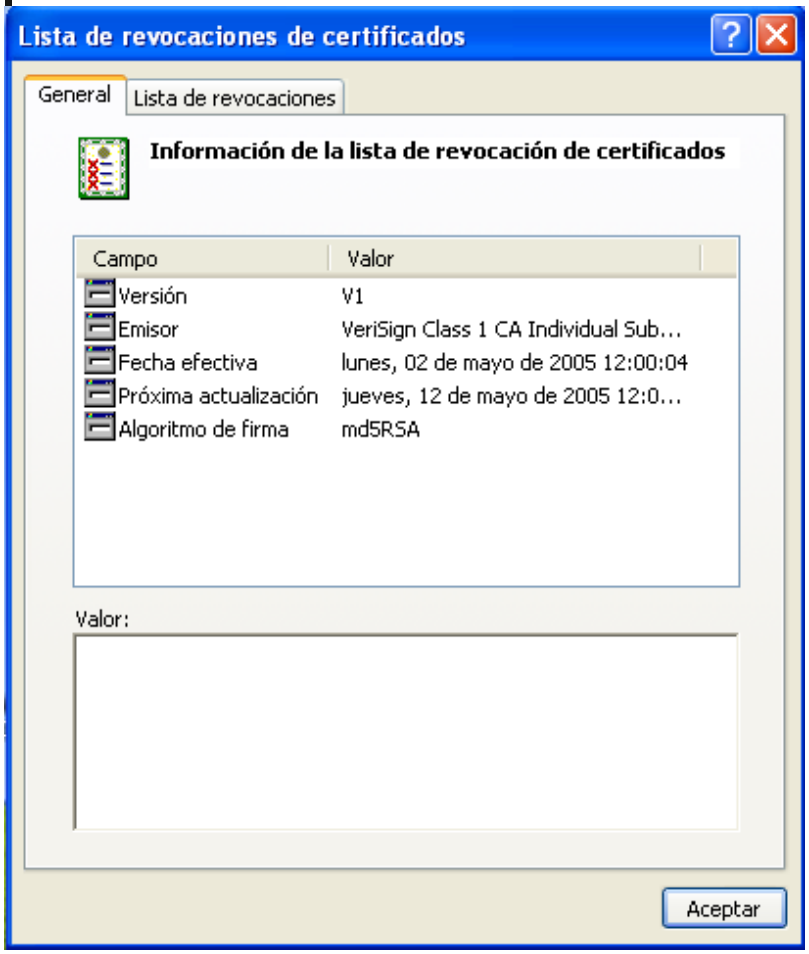
# Certificados

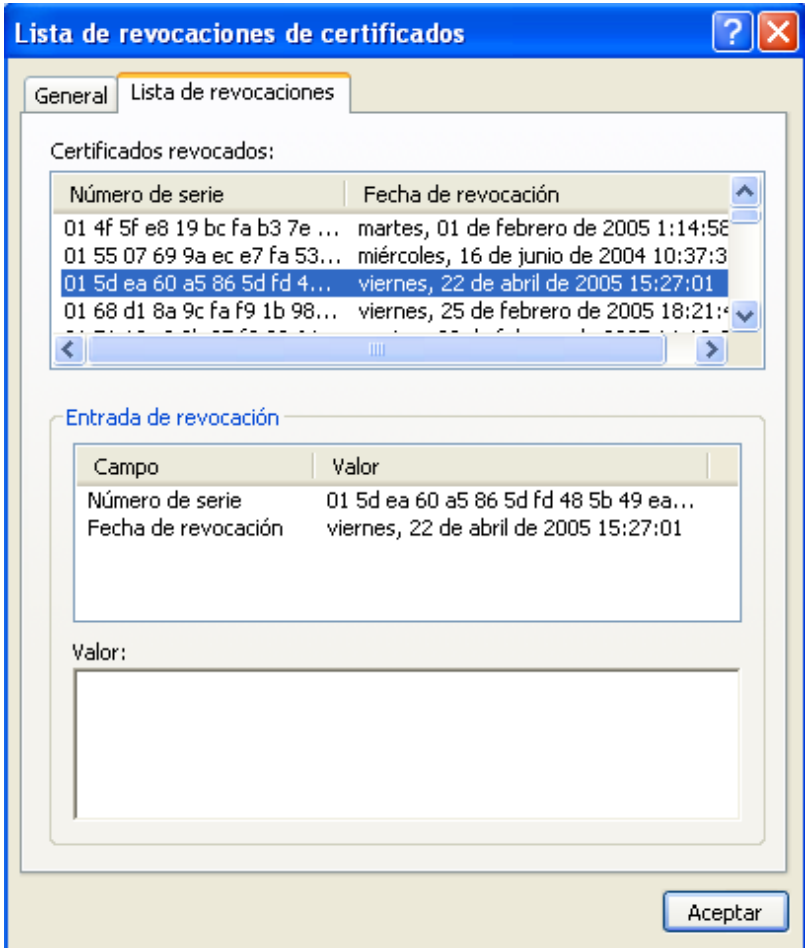
- Servicio ofrecido por las CA
  - CA interna, certificar a sus propios empleados, puestos y niveles de autoridad
  - CA externa de empleados, empresa contrata a otra para certificar a sus empleados
  - CA externa de clientes, empresa contrata a otra para que certifique a sus clientes
  - **CA confiable de terceros**, compañía o gobierno opera una CA que relaciona claves públicas con nombres legales de individuos o empresas

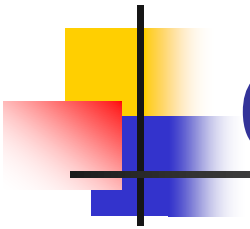
# Certificados

- Revocación de certificados:
  - Clave privada de usuario comprometida
  - CA emite certificado a entidad incorrecta
  - El usuario cambia de CA
  - Violación de la seguridad de la CA
- **Lista de revocación de certificados** (CRL, Certification Revocation List)
  - Ejemplo: http://crl.verisign.com/

# Certificados





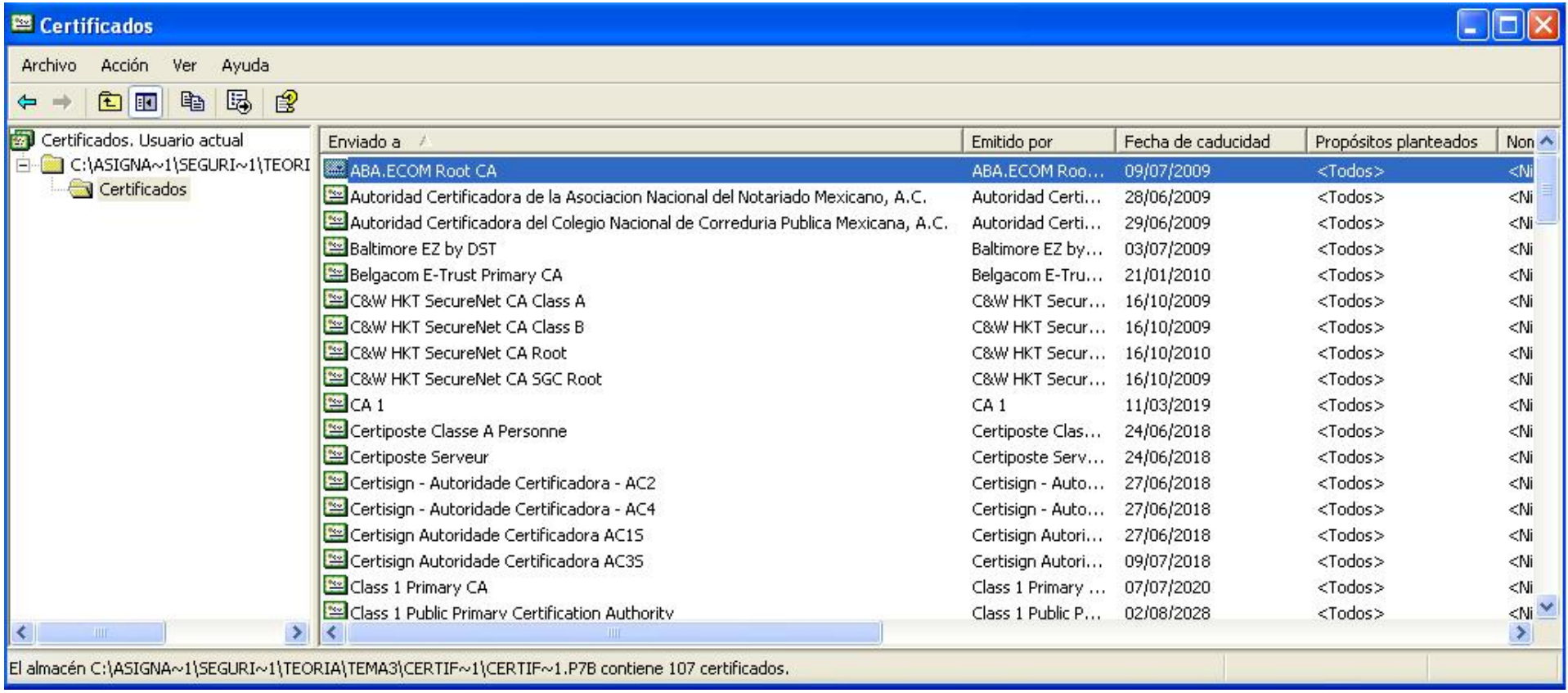
# Certificados

- Certificados de autoridades certificadoras
- Certificados de servidores
- Certificados personales
- Certificados de editor de software

# Certificados

**CERTIFICADO DE AUTORIDAD CERTIFICADORA**

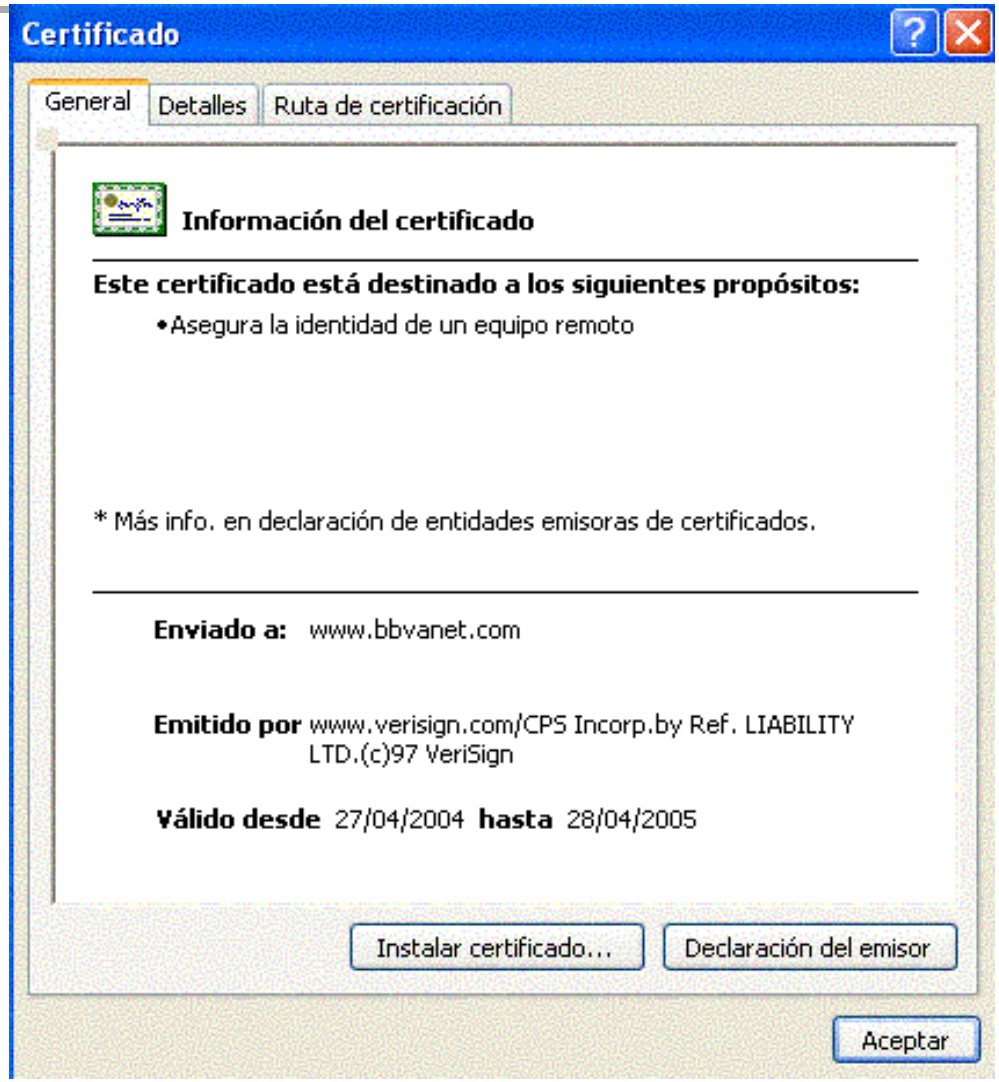
- Nombre y clave pública de la CA
- Pueden ser autofirmados
- PKI (Public Key Infrastructure)



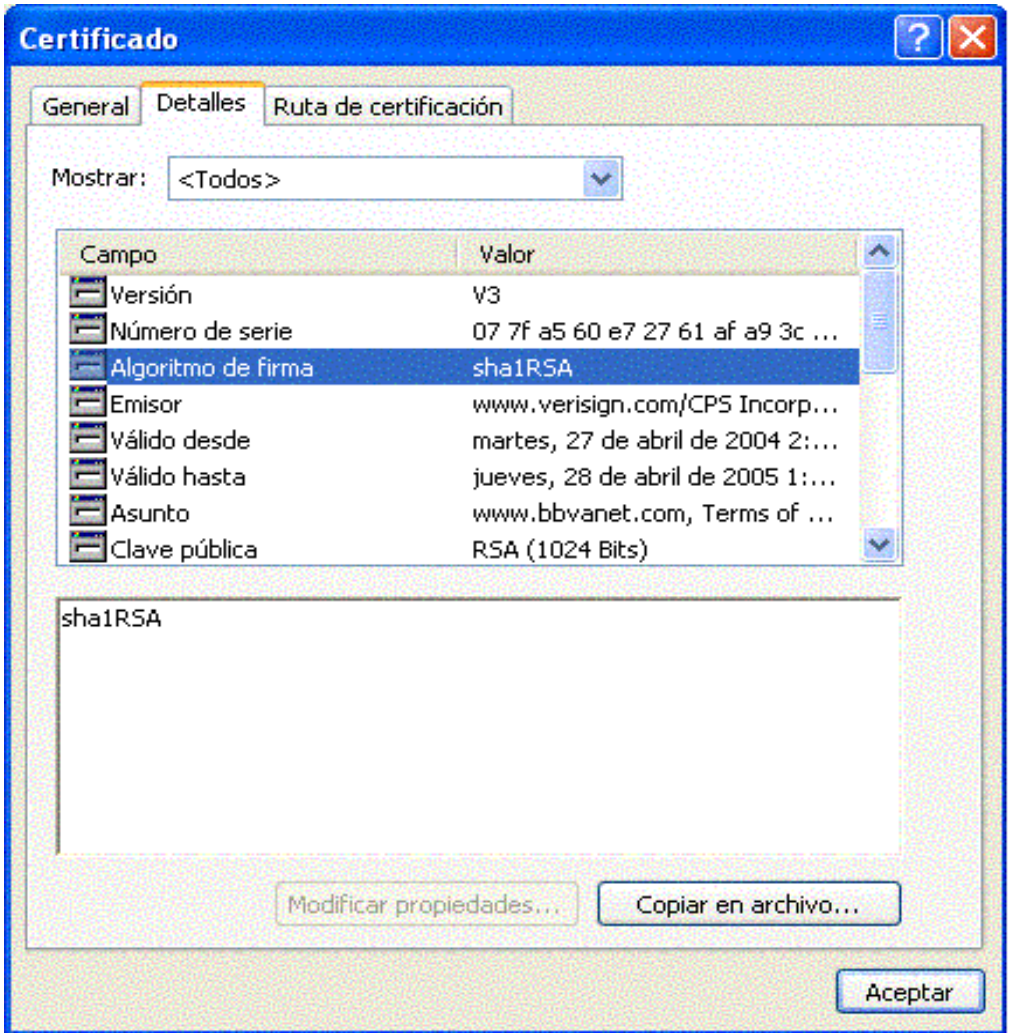
# Certificados

**CERTIFICADO DE SERVIDOR**

- Cada servidor SSL -> un certificado de servidor SSL
- Debe contener:
  - longitud de clave firmada
  - nº serie del certificado
  - algoritmo de firma
  - nombre del servidor
- Ejemplo



# Certificados



# Certificados

CERTIFICADO PERSONAL

- Diseñado para comprobar la identidad de un individuo emitido por una CA
- Beneficios:
  - Eliminar necesidad de recordar login y password
  - Prueba de pertenecer a una organización
  - Comunicaciones cifradas
  - Restringir acceso a sitios web

# Certificados

CERTIFICADO PERSONAL

- A partir de la v.3 de Navigator Netscape e Internet Explorer
  - Creación de claves
  - Obtención de certificados
  - Reto/respuesta
  - Almacenamiento seguro
- En España:
  - Fabrica Nacional de Moneda y Timbre (www.cert.fnmt.es)
  - ANF Autoridad de Certificación (www.anf.es)
  - AC Camerfirma (www.camerfirma.com)
  - Autoridad de Certificación de la Abogacía (www.acabogacia.org)
  - Firma Profesional S.A. (www.firmaprofesional.com)

# Certificados

- **Servicios a los que se puede acceder con un certificado de usuario en España**

**Administración Central**

Agencia Estatal de Administración Tributaria
Comisión del Mercado de las Telecomunicaciones
Instituto de Crédito Oficial
Instituto Nacional de Estadística
Ministerio de Economía
Presidencia de Gobierno
Seguridad Social
Dirección General del Catastro
Dirección General de Costes de Personal y Pensiones Públicas
Ministerio de Trabajo y Asuntos Sociales

**Administración Autonómica**

Comunidad de Madrid
Gobierno de Canarias
Gobierno de Navarra
Gobierno de la Rioja
Junta de Andalucía
Xunta de Galicia

**Administración Local**

Ayuntamiento de Alboraya
Ayuntamiento de Laredo
Ayuntamiento de Catarroja
Ayuntamiento de Madrid
Ayuntamiento de Paterna
Ayuntamiento de Totana
Ayuntamiento de Valencia
Diputación de Barcelona

**Otros**

Asociación de Asesores de Empresa en Internet
Consejo General del Notariado
Gestor de Infraestructuras S.A.
Paradores Nacionales de Turismo
Saniline
SegurosBroker
Sociedad Digital de Autores y Editores

# Certificados

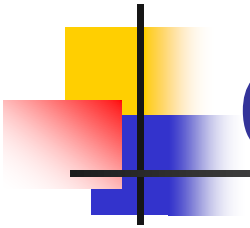
CERTIFICADO PERSONAL

- Cómo solicitarlo de modo gratuito por dos meses:
  1) Ir a https://digitalid.verising.com
  2) Seleccionar PersonalID -> Buy Now -> Enroll Now
  3) Completar el formulario de *enrollment*
     - Nombre y Apellidos
     - Dirección de correo electrónico
  4) Aceptar el acuerdo
  5) Comprobar el correo electrónico, *verisign* enviará un correo con un identificador y la URL de una página web
  6) Ir a la página web indicada e introducir el identificador
  7) El navegador obtendrá el certificado
  8) Para instalarlo seguir las indicaciones del navegador
  9) Comprobación en Internet Explorer: ir a Herramientas -> Opciones de Internet -> Contenido -> Certificados -> Personal

# Certificados

CERTIFICADO DE EDITOR DE SOFTWARE

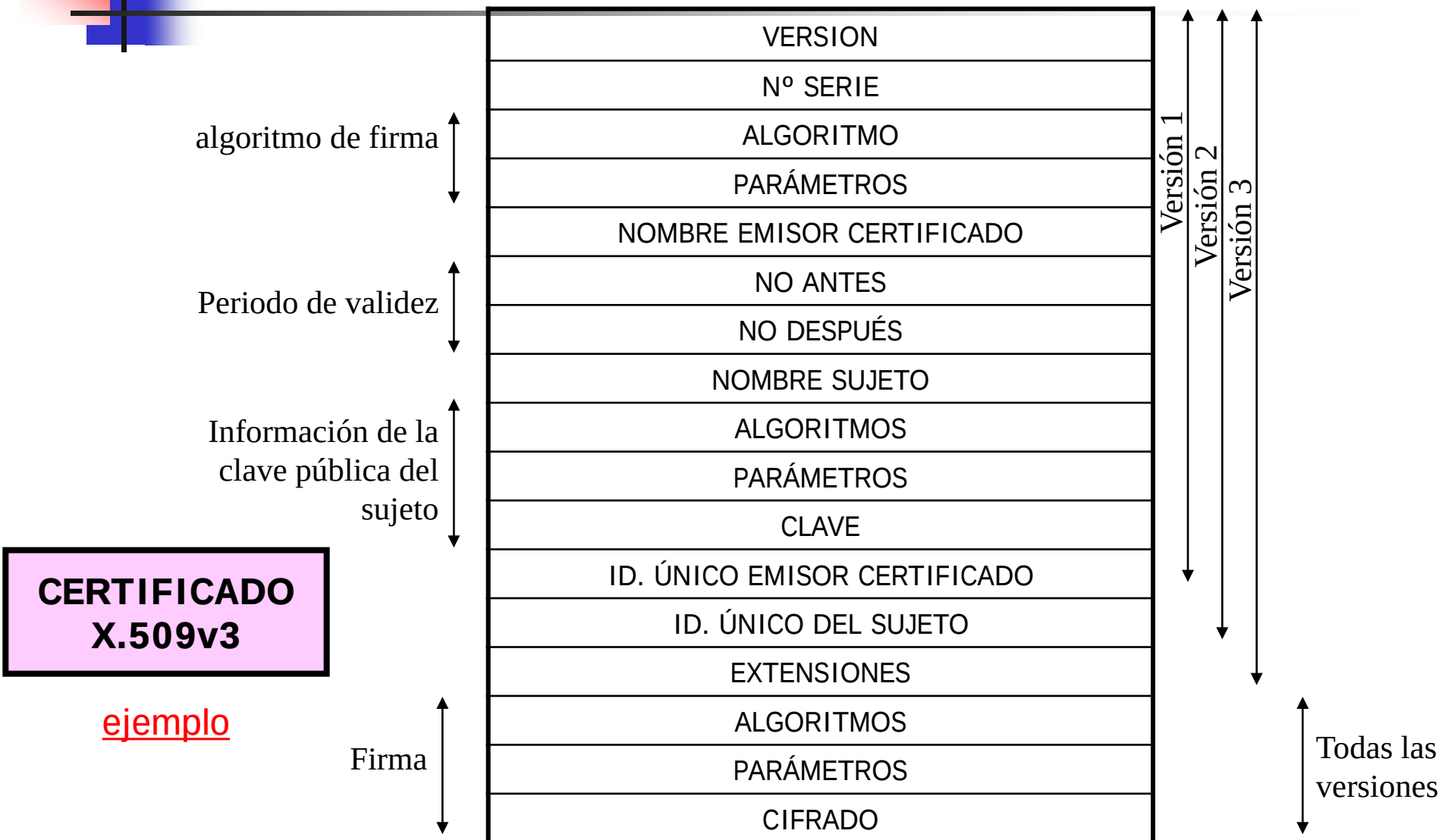
- Firmar programas ejecutables mediante firma electrónica
- Mejora la confiabilidad del software distribuido por Internet
- Propuestas:
  - Authenticode (Microsoft)
  - JAR, formato de archivo java que permite uso de firma digital



# Certificados

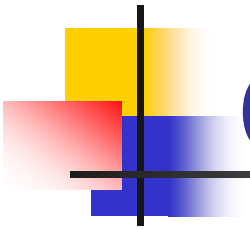
- **Certificado X.509**
  - Parte de la serie de recomendaciones X.500
  - X.509 permite servicio de autenticación
  - Estructura de certificado X.509 empleada en muchos contextos (S/MIME, seguridad IP, SSL/TLS, SET, ...)
  - Versión 3 revisada en 2000

# Certificados




**CERTIFICADO X.509v3**

ejemplo



# Certificados

- Las claves privadas no son personas
- Los nombres distinguidos no son personas
- Existen demasiados nombres de personas iguales
- Los certificados digitales no dicen lo suficiente
- X.509 v.3 no permite la divulgación selectiva
- Los certificados digitales permiten la combinación fácil de datos
- ¿Cuántas CA necesita la sociedad?
- ¿Cómo prestar una clave?
- ¿Existen mejores opciones a las firmas digitales de clave pública?