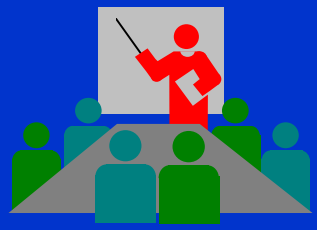
Capítulo 17
Certificados Digitales y Estándar PKCS

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 21 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

¿Qué son los certificados digitales?

- Un certificado digital es un documento que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado por una Autoridad de Certificación (AC).
- Como emisor y receptor confiarán en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública está firmada por dicha autoridad.
- Una de las certificaciones más usadas y un estándar en la actualidad en infraestructuras de clave pública PKIs (Public-Key Infrastructure) es X.509.

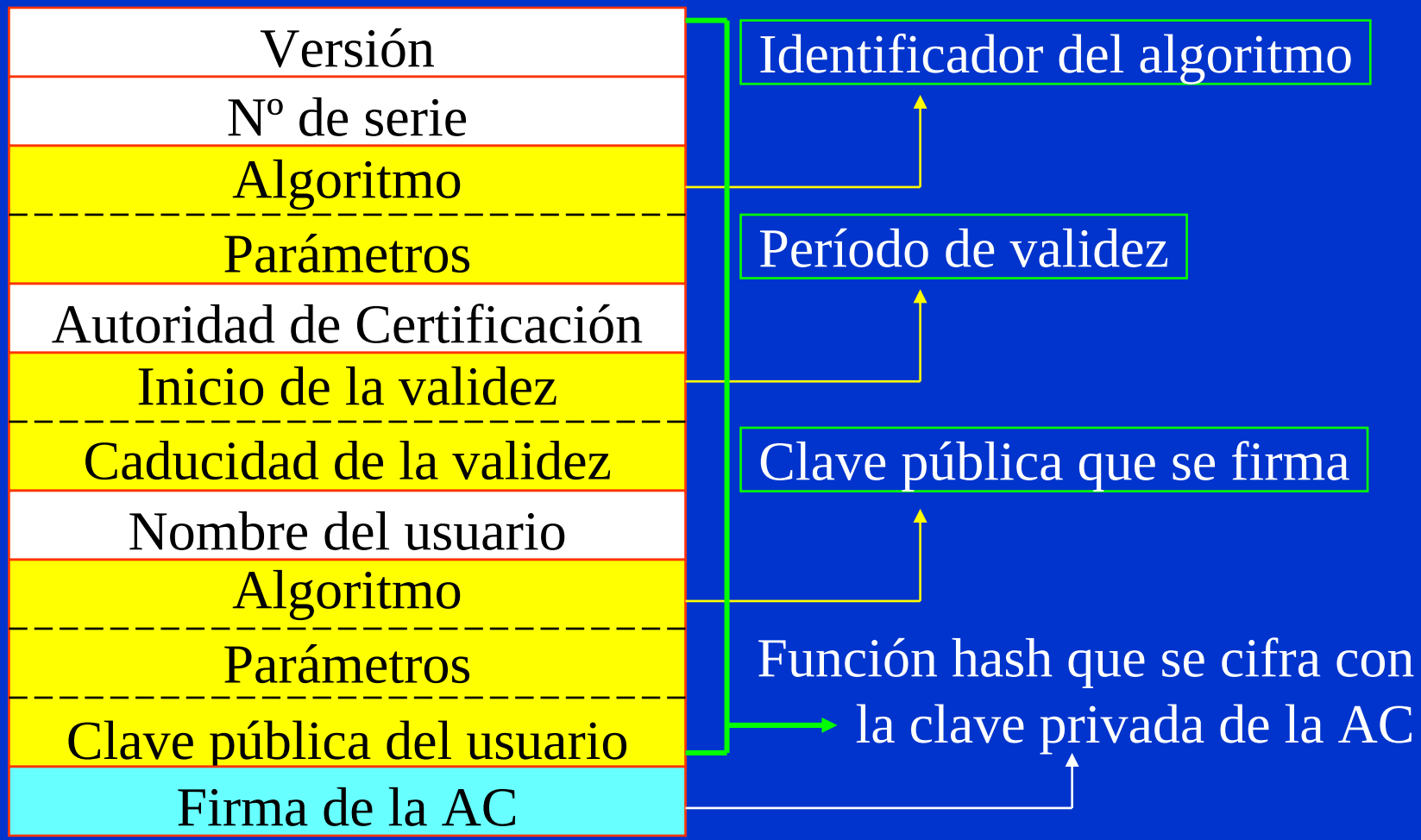
http://www.ietf.org/html.charters/pkix-charter.html

Certificado digital X.509

- X.509 está basado en criptografía asimétrica y firma digital.
- En X.509 se define un framework (una capa de abstracción) para suministrar servicios de autenticación a los usuarios del directorio X.500.
- La autenticación se realiza mediante el uso de certificados.

  - Un certificado contiene: el nombre de la AC, el nombre del usuario, la clave pública del usuario y cualquier otra información como puede ser un un indicador de tiempo o *timestamp*.
  - El certificado se cifra con la clave privada de la AC.
  - Todos los usuarios poseen la clave pública de la AC.

Formato del certificado digital X.509



Campos del certificado digital X.509

- V: Versión del certificado (actualmente V3).
- SN: Número de serie.
- AI: identificador del algoritmo de firma que sirve para identificar el algoritmo usado para firmar el paquete X.509.
- CA: Autoridad certificadora.
- T_A: Periodo de validez.
- A: Propietario de la clave pública que se está firmando.
- P: Clave pública más identificador de algoritmo utilizado y más parámetros si son necesarios.
- Y{I}:Firma digital de Y por I usando la clave privada de la unidad certificadora.

CA<<A>> = CA { V, SN, AI, CA, T_A, A, AP }

Y<<X>> es el certificado del usuario X expedido por la autoridad certificadora Y.

Autoridades de Certificación

Autoridad de Certificación es un ente u organismo que, de acuerdo con unas políticas y algoritmos, certificará -por ejemplo- claves públicas de usuarios o servidores.

El usuario A enviará al usuario B su certificado (la clave pública firmada por AC) y éste comprobará con esa autoridad su autenticidad. Lo mismo en sentido contrario.

Elementos de una AC

El sistema de autenticación debe tener:

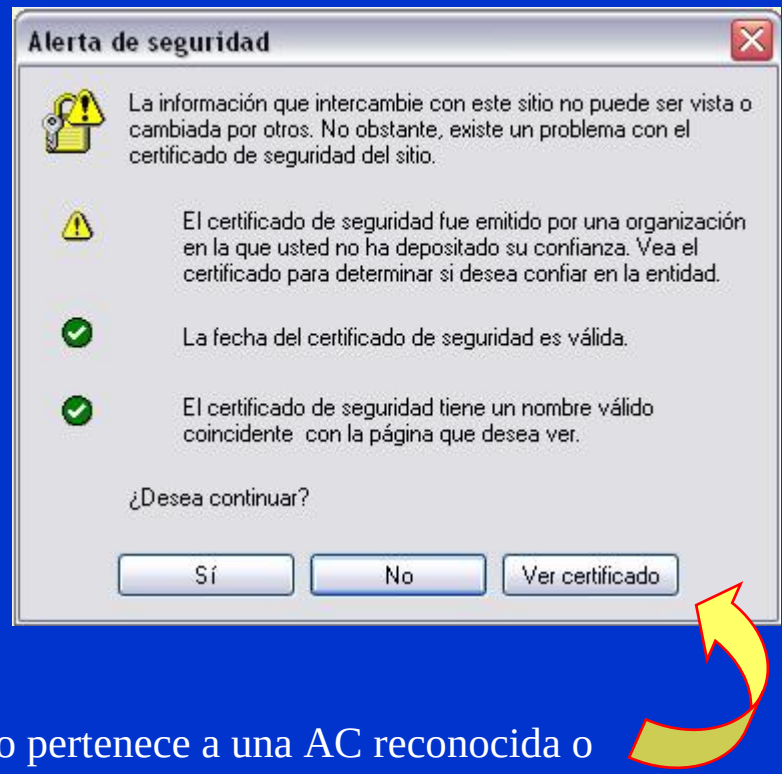
- Una política de certificación.
- Un certificado de la CA.
- Los certificados de los usuarios (X.509).
- Los protocolos de autenticación, gestión y obtención de certificados:
  - Se obtienen de bases de datos (directorio X.500).
  - O bien directamente del usuario en tiempo de conexión (WWW con SSL).

Algunas características de diseño de la AC

- Deberá definirse una política de certificación
  - Ambito de actuación y estructura
  - Relaciones con otras ACs
- Deberá definirse el procedimiento de certificación para la emisión de certificados:
  - Verificación on-line
  - Verificación presencial
- Deberá generarse una Lista de Certificados Revocados

Funcionamiento de una AC

- Puesta en marcha de la AC:
  - Generará su par de claves.
  - Protegerá la clave privada con una *passphrase*.
  - Generará el certificado de la propia AC.
- Distribución del certificado de la AC:
  - A través del directorio X.500.
  - Por medio de páginas Web.
- Podrá certificar a servidores y a clientes.



Si el certificado digital X.509 de un servidor no pertenece a una AC reconocida o instalada en su programa cliente, aparecerá una pantalla similar a la que se muestra.

Certificado de email X.509 de Verisign (1)

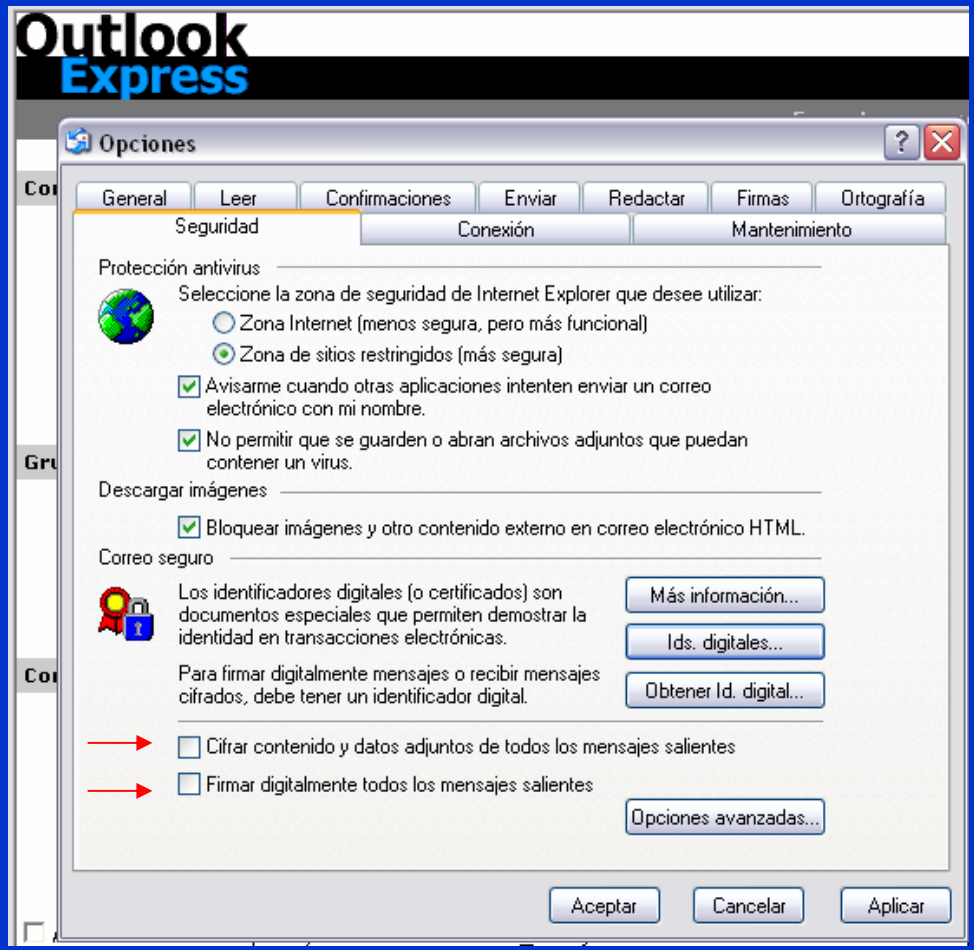
- Paso 1
  - Acceda a la web segura indicada abajo y seleccione navegador.
  - Introduzca su nombre, dirección de correo y password.
  - Indique que desea un certificado de prueba gratis por 60 días.
  - Seleccione el nivel de seguridad que desea para el acceso a su clave privada; es recomendable elegir el valor alto.
  - Pulse el botón aceptar.
- Paso 2
  - Observará el mensaje "*You should receive an e-mail from the Digital ID Center within the hour at the e-mail address you entered in the enrollment form. It will contain instructions for installing the Digital ID*" y en menos de 10 minutos recibirá un email para seguir los pasos 3 y 4.
- Pasos 3 y 4 en próxima diapositiva.

https://digitalid.verisign.com/client/enroll.htm

Certificado de email X.509 de Verisign (2)

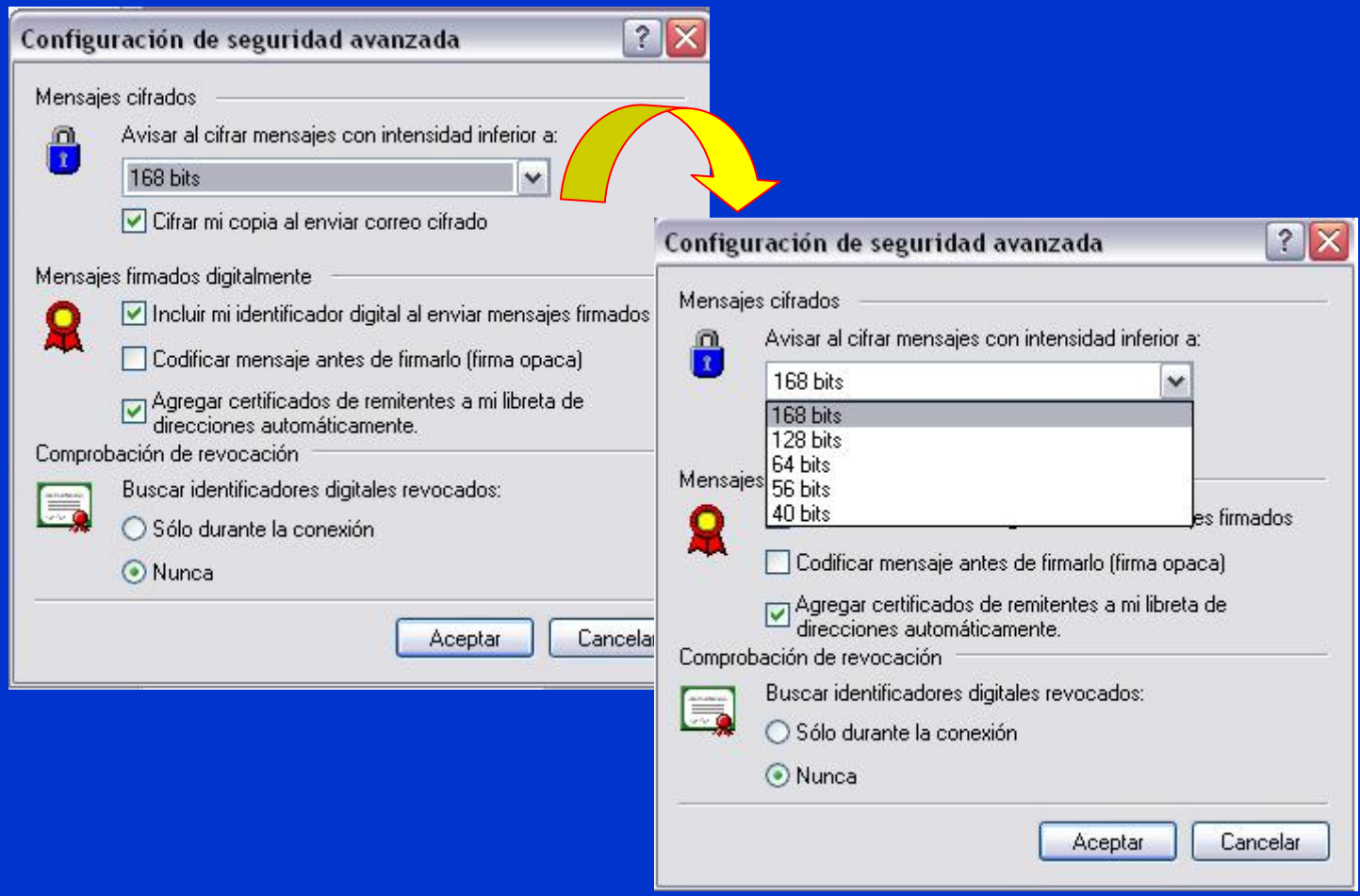
- Paso 3
  - Use el *Personal Identification Number* (PIN) que le envían por correo que será parecido a éste 5cd472bd311f89eb25f2511ce5e86b31 y péguelo en la página de *VeriSign's secure Digital ID Center* que se indica: https://digitalid.verisign.com/enrollment/mspickup.htm
  - Pulse el botón de Submit para instalar el certificado en su computador.
- Paso 4
  - El Digital ID^{SM} ha sido generado con éxito y con los siguientes datos:
    - Organization = VeriSign, Inc.
    - Organizational Unit = VeriSign Trust Network
    - Organizational Unit = www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD©98
    - Organizational Unit = Persona Not Validated
    - Organizational Unit = Digital ID Class 1 – Microsoft
    - Common Name = Jorge Ramio
    - Email Address = jramio@eui.upm.e
  - SPulsamos el botón Instalar

Certificado X.509 en Outlook Express



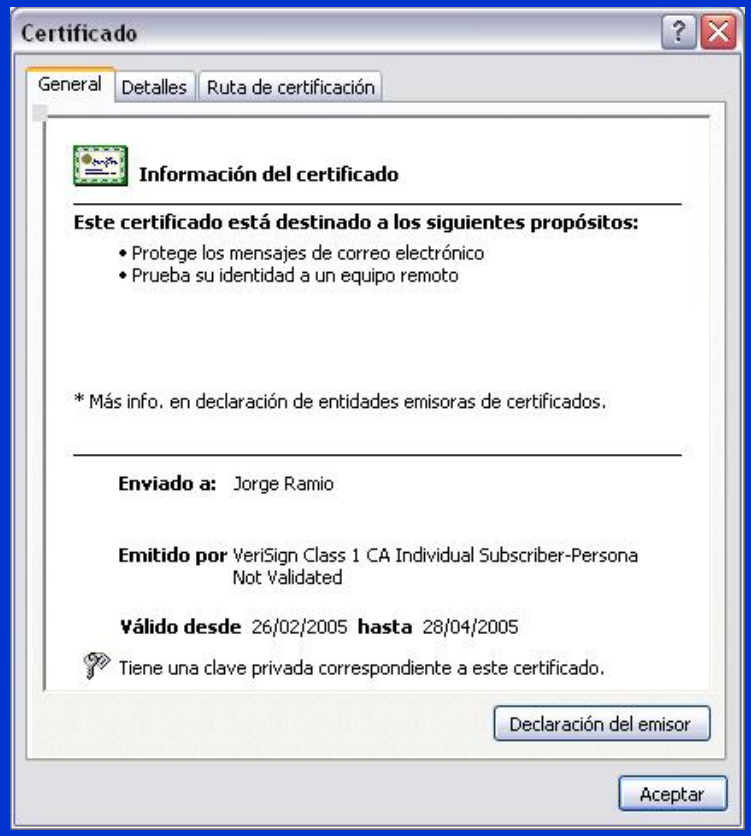
- Abra Outlook Express.
- Seleccione Herramientas - Opciones - Seguridad.
- Puede seleccionar que todos sus mensajes salientes vayan cifrados.
- Puede seleccionar que todos sus mensajes salientes vayan firmados digitalmente.
- Para mayor información vaya a Opciones Avanzadas.

Opciones Avanzadas del certificado X.509

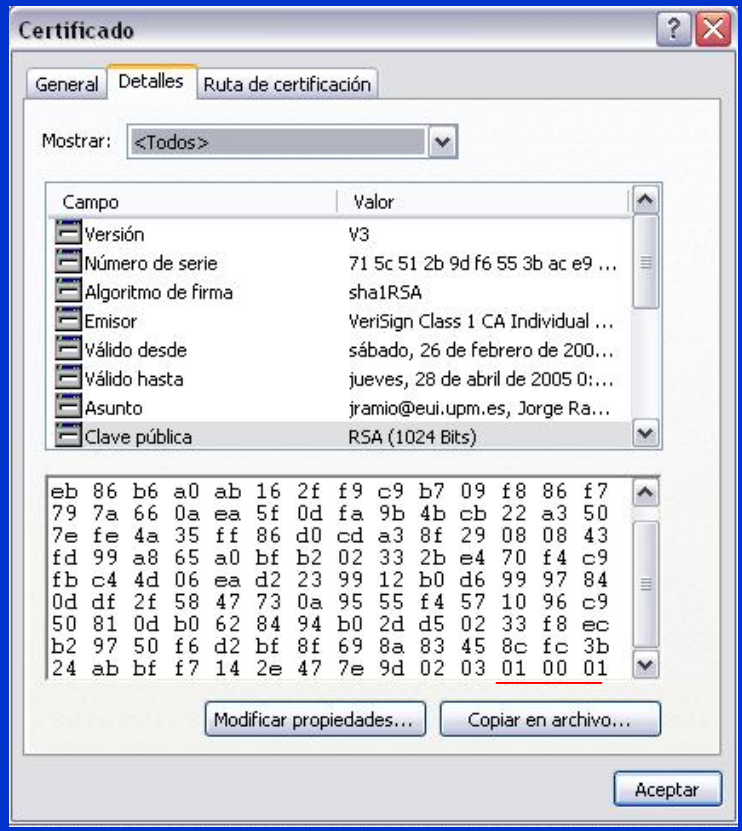


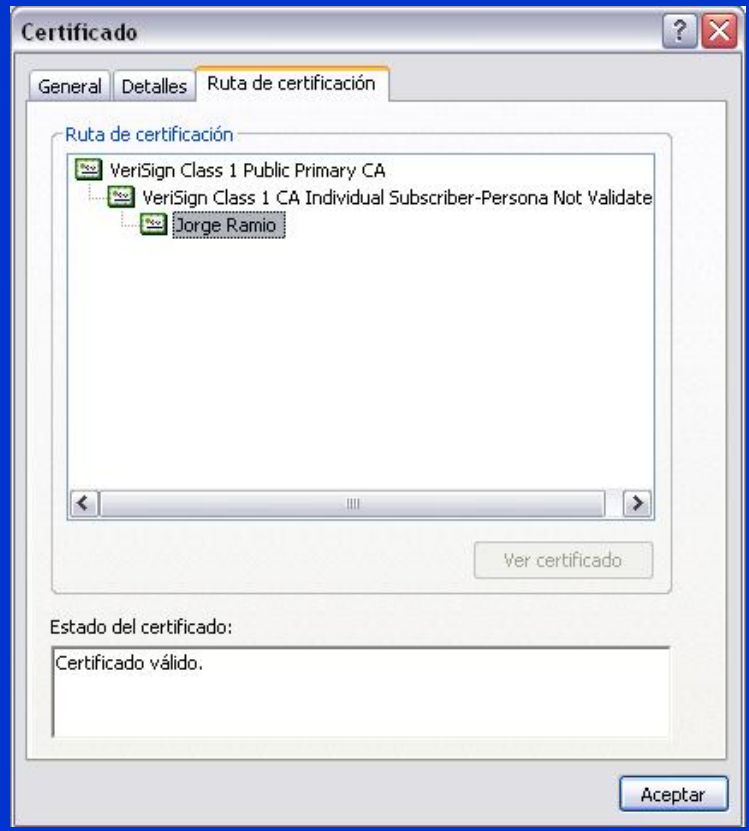
Características del certificado X.509 (1)

Si pulsamos en Ids. Digitales, podemos observar nuestro certificado.



Características del certificado X.509 (2)





Observe en la clave pública RSA el valor e = 010001

Estándar PKCS

- PKCS: Public-Key Cryptography Standards, son un conjunto de especificaciones técnicas desarrolladas por Netscape, RSA y otros desarrolladores de informática cuyo objeto es uniformizar las técnicas y protocolos de la criptografía pública.
- Publicación de la primera versión 1.0 se hace en el año 1991.
- PKCS forma parte de distintos estándares de hecho como ANSI PKIX, X9, SET, S/MIME y SSL.
- A la fecha existen 14 documentos con títulos genéricos que van desde PKCS #1 a PKCS #15.
- El de mayor trascendencia podría ser PKCS #11 llamado CRYPTOKI.
- Mantendremos los títulos originales en su versión en inglés de RSA Security Inc. Public-Key Cryptography Standards PCKS.

http://www.rsasecurity.com/rsalabs/pkcs/

Documentos del estándar PKCS (2002)

- PKCS #1: RSA Cryptography Standard
- PKCS #2: Incluido ahora en PKCS #1
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #4: Incluido ahora en PKCS #1
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard

PCKS #1 v2.1 del 14 de Junio 2002 (1)

PKCS #1: RSA Cryptography Standard

- Tipos de claves: definición de claves pública y privada.
- Conversión de primitivas: I2OSP (Integer-to-Octet-String primitive) y OS2IP (Octet-String-to-Integer primitive).
- Primitivas criptográficas cifra: RSAEP (RSA encryption primitive) y RSADP (RSA decryption primitive). En este último caso se especifica la operación típica para $n = p*q$ y la operación para $n = r_1*r_2*r_3*...*r_u$.
- Primitivas criptográficas firma: RSASP1 (RSA signature primitive 1) especificando la operación típica para $n = p*q$ y la operación en caso de que $n = r_1*r_2*r_3*...*r_u$ y RSAVP1 (RSA verification primitive 1).
- Esquemas de cifrado: RSAES-OAEP (RSA encryption scheme usando Optimal Asymmetric Encryption Padding). Especificación de las operaciones de cifrado y descifrado.

PCKS #1 v2.1 del 14 de Junio 2002 (2)

- Esquemas de firma con apéndice: RSASSA-PSS (RSA signature scheme with appendix - Probabilistic Signature Scheme). Define la firma y su verificación.
- Métodos de codificación para firmas con apéndices: EMSA-PSS (Encoding Method for Signatures with Appendix - Probabilistic Signature Scheme). Define operaciones de codificación y verificación.
- Sintaxis ASN.1: define los identificadores de objetos ANS.1 para las claves pública y privada RSA, RSAES-OAEP, RSASSA-PSS, etc.
- Técnicas soportadas: algoritmos funciones hash MD2, MD5, SHA-1 y los propuestos SHA-256, SHA-384 y SHA-512 así como funciones de generación de máscaras: MGF1 (Mask Generation Function 1).

☞ La patente de RSA ha expirado en septiembre de 2000 no así el nuevo sistema de cifra RSA con múltiples primos.

Fin del capítulo

Cuestiones y ejercicios

1. ¿Qué es lo que certifica o autentica un certificado digital?
2. Solicitamos un certificado digital a una empresa. ¿Está nuestra clave privada entre los datos que nos solicita para el alta?
3. Si un certificado digital pierde la validez, ¿qué debemos hacer?
4. ¿Por qué una Autoridad de Certificación firma una función hash?
5. Si Ud. fuese una Autoridad de Certificación, ¿qué condición pondría para expedir con seguridad un certificado a un usuario?
6. Una Autoridad de Certificación emite certificados digitales de hasta 1.024 bits y duración un año. Si ella tiene un certificado digital raíz de 2.048 bits, ¿sería lógico plantear una validez de éste por 10 años?
7. ¿Qué es y cuándo se solicita la revocación de un certificado digital?
8. ¿Qué significa que la Autoridad de Certificación deba gestionar una lista de certificados revocados?

Use el portapapeles

Prácticas del tema 17

1. Acceda a un gran almacén de su país que permita realizar compras seguras por Internet. Si no conoce una dirección Web use, por ejemplo, la página http:www.elcorteingles.com en España, ponga algún artículo en el carrito de la compra y comience el proceso necesario para efectuar el pago, sin concluirlo, para abrir una sesión SSL. Observe que al pasar el ratón sobre el candado cerrado de su navegador, aparece SSL 128 bits. ¿Qué significa?
2. Haga doble clic en ese candado y observe todas las características del certificado de ese servidor web.
3. Abra la pestaña de la clave pública RSA y observe los últimos 6 dígitos en hexadecimal 010001. Copie este valor en la calculadora de Windows y luego conviértalo a decimal. Compruebe que este valor es el mismo para otros servidores seguros. ¿Le dice algo este valor?
4. En las propiedades u opciones de su navegador, abra los certificados de distintas Autoridades de Certificación y observe sus características.