Certificados Digitales y PKI

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://homepage.cem.itesm.mx/rogomez

Criptosistemas de llave pública

Continuación

Deberias checar tu email mas seguido.
Hace 3 semanas que te despedi...

Algunos problemas de la criptografía de llave pública

Lámina 3 Dr. Roberto Gómez C

Solicitando una llave pública

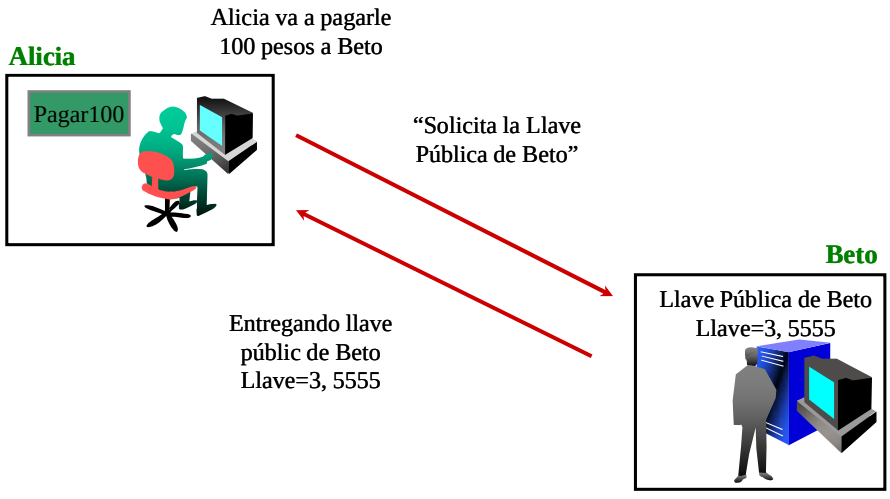


Lámina 4 Dr. Roberto Gómez C

El ataque "Man in the Middle" (MIM)

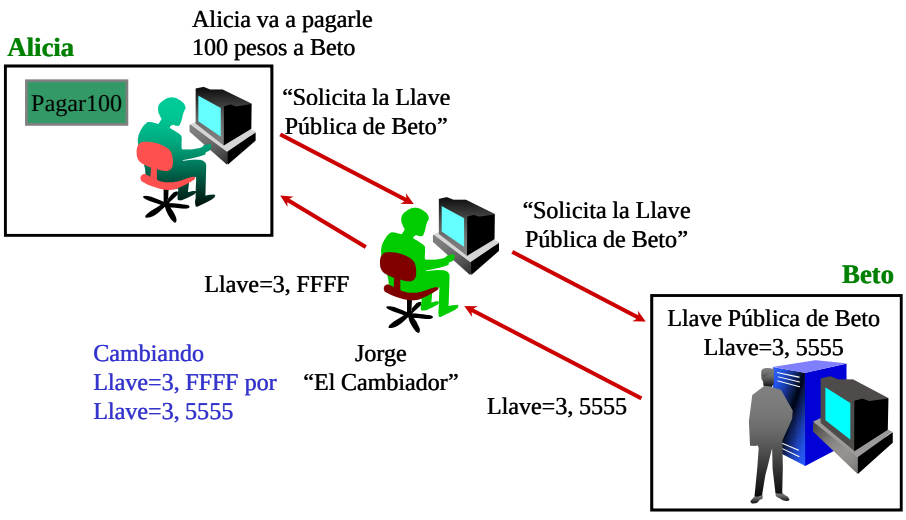


Lámina 5 Dr. Roberto Gómez C

Ese momento desafortunado cuando 2 cybernautas se encuentran cara a cara

Lámina 6 Dr. Roberto Gómez C

Comentarios acerca del MIM

- Problema: intercambio de llaves públicas.
- Peligro inminente: “Man-in-the-middle Attack”.
- Es vital que la llave pública que se esta usando en realidad pertenezca a la persona que se desea y no a un extraño.

Lámina 7 Dr. Roberto Gómez C

Solución al MIM

- Solución:
  - Intercambio de llaves públicas firmadas digitalmente con la llave privada de una 3a persona.
  - 3a. persona de confianza que de a conocer su llave pública.
- Uso de un certificado digital que certifique que la llave pertenece en realidad a la persona.

Lámina 8 Dr. Roberto Gómez C

Certificado Digital

- Paquete emitido por una autoridad certificadora (CA), que:
  - contiene una llave pública
  - identifica al dueño de la llave,
  - especifica la vigencia del certificado e
  - incluye la firma digital de la CA.
- Propósito: mostrar que una llave pública pertenece en verdad a una persona.
- Contiene cuando menos un nombre, una llave pública y una firma digital calculada a partir de los dos primeros.
- La interoperabilidad entre sistemas de distintos fabricantes se logra a través del estándar público X.509
  - gobierna el formato y el contenido de los certificados digitales.

Lámina 9 Dr. Roberto Gómez C

Observaciones certificados digitales

- Estar seguros que la información de certificación ha sido atestada por otra persona o identidad
- La firma no atesta la autenticidad de todo el certificado, sólo asegura que la información de identificación corresponde a la llave pública

Lámina 10 Dr. Roberto Gómez C

Autoridad Certificadora.

- Un organismo interno confiable o tercera parte también confiable que respalda (vouches) la identidad de un dispositivo o individuo, mediante la emisión de un certificado y la llave privada correspondiente.
- Se responsabiliza por la gente a la cual emitió el certificado:
  - Compañía a sus empleados
  - Universidad a sus estudiantes
  - CA Pública (Verisign) a sus clientes

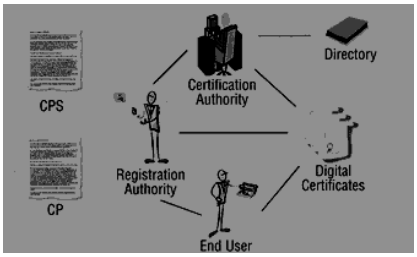


Lámina 11 Dr. Roberto Gómez C

Certification Practice Statement

- La autoridad Certificadora opera de acuerdo con una Declaración de Prácticas de Certificación “Certification Practice Statement (CPS)”
- La CPS explica:
  - Como la CA emite certificados
  - Como la CA verifica la identidad de los poseedores de los certificados
  - Como la CA mantiene la información segura
  - Responsabilidades de la CA y de sus Clientes

Lámina 12 Dr. Roberto Gómez C

¿Qué confiamos que debe hacer la CA?

- La CA debe mantener confidencial la llave privada utilizada para firmar los certificados durante el período de validez
- La CA NO debe asignar a diferentes certificados el mismo número de serie
- La CA debe asegurar que toda la información en un certificado es correcta
- Mantener actualizada la Lista de Certificados Revocados “Certificate Revocation List (CRL)”

Lámina 13 Dr. Roberto Gómez C

Revocación

- Las CAs necesitan alguna forma de revocar los certificados
- Propuesta: listas de revocación de certificados CRL (Certificate Revocation List)
- Idealmente una CA emite una CRL a intervalos regulares.
- Además de listar los certificados revocados, la CRL especifica durante cuanto tiempo es válida esta lista y cuando obtener la siguiente.

Lámina 14 Dr. Roberto Gómez C

Causas revocación

- Baja solicitada por el usuario.
- Baja por exposición de llaves.
- Baja por finalización del periodo de vida del certificado.
- Baja por abandono de la organización.
- Baja por orden superior (mal uso del Certificado).

Lámina 15 Dr. Roberto Gómez C

El contenido de un Certificado Digital

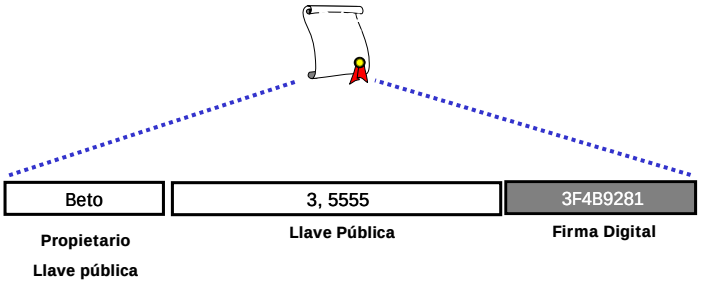


Lámina 16 Dr. Roberto Gómez C

Ejemplo Certificado Digital

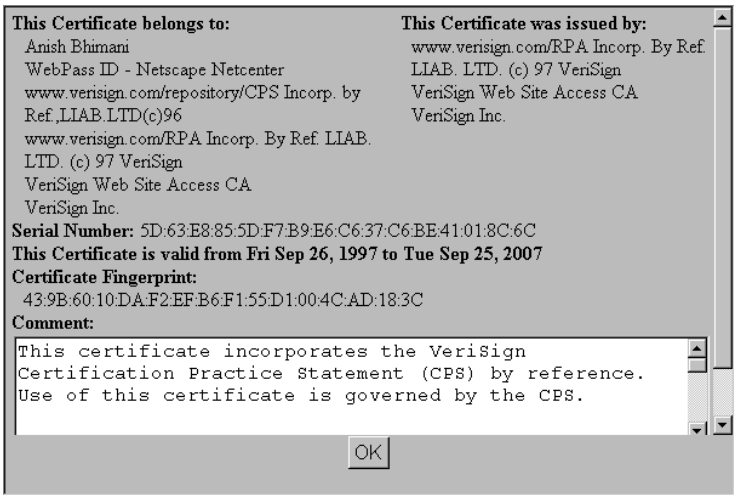


Lámina 17 Dr. Roberto Gómez C

La generación de un certificado digital

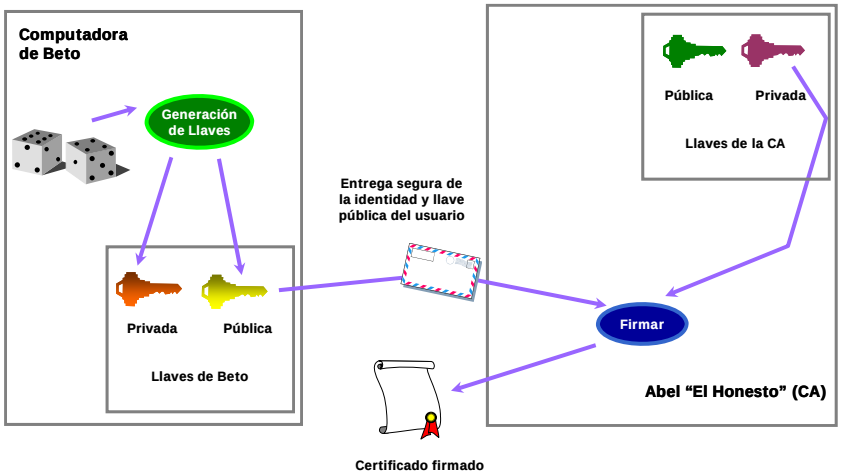


Lámina 18 Dr. Roberto Gómez C

La validación de un certificado digital

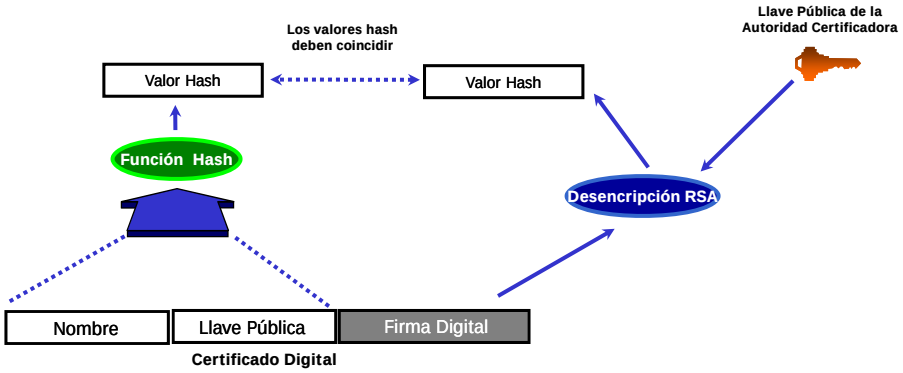


Lámina 19 Dr. Roberto Gómez C

¿Cómo funciona todo?

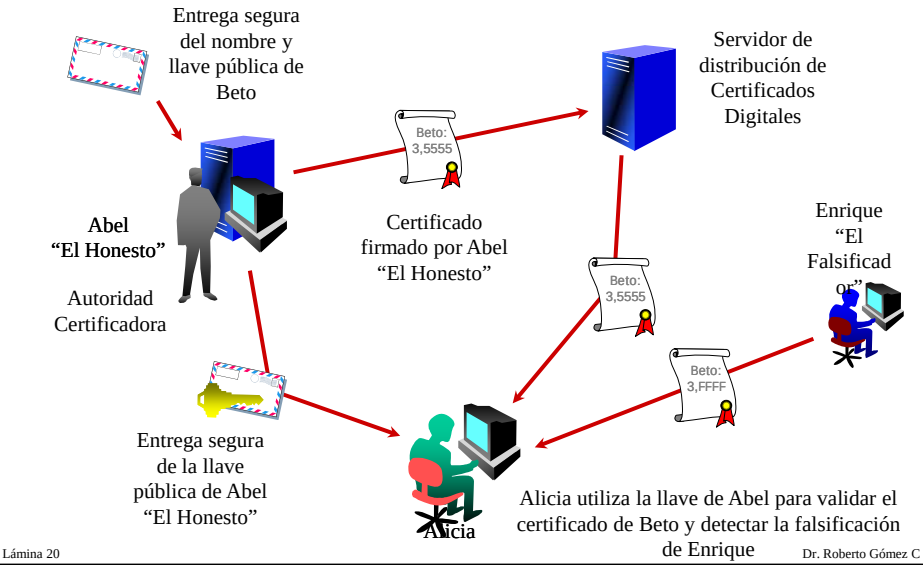


Lámina 20 Dr. Roberto Gómez C

Ejemplo certificado en una página

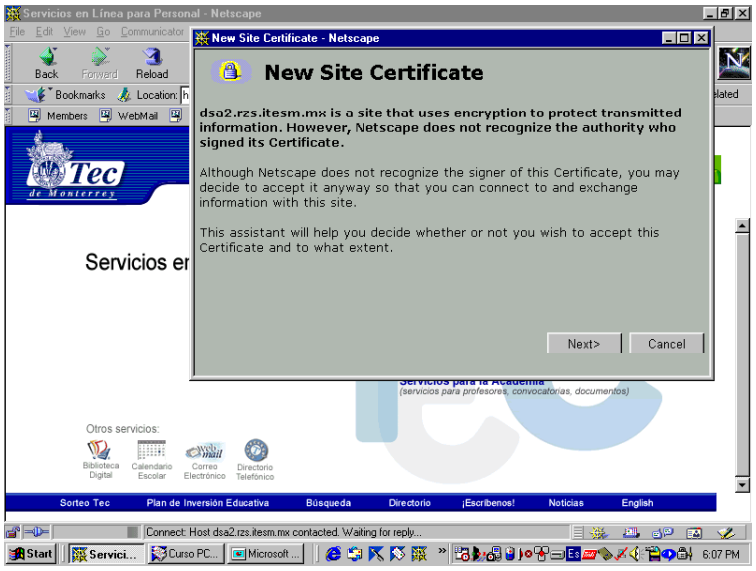


Lámina 21 Dr. Roberto Gómez C

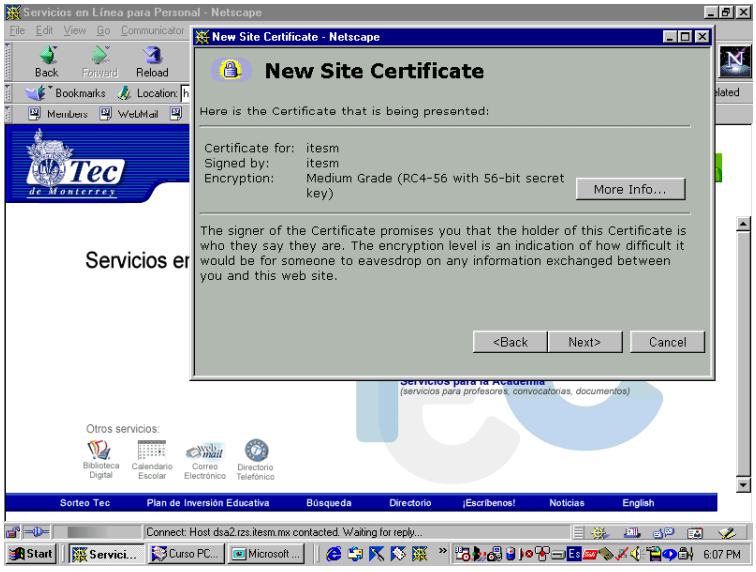


Lámina 22 Dr. Roberto Gómez C

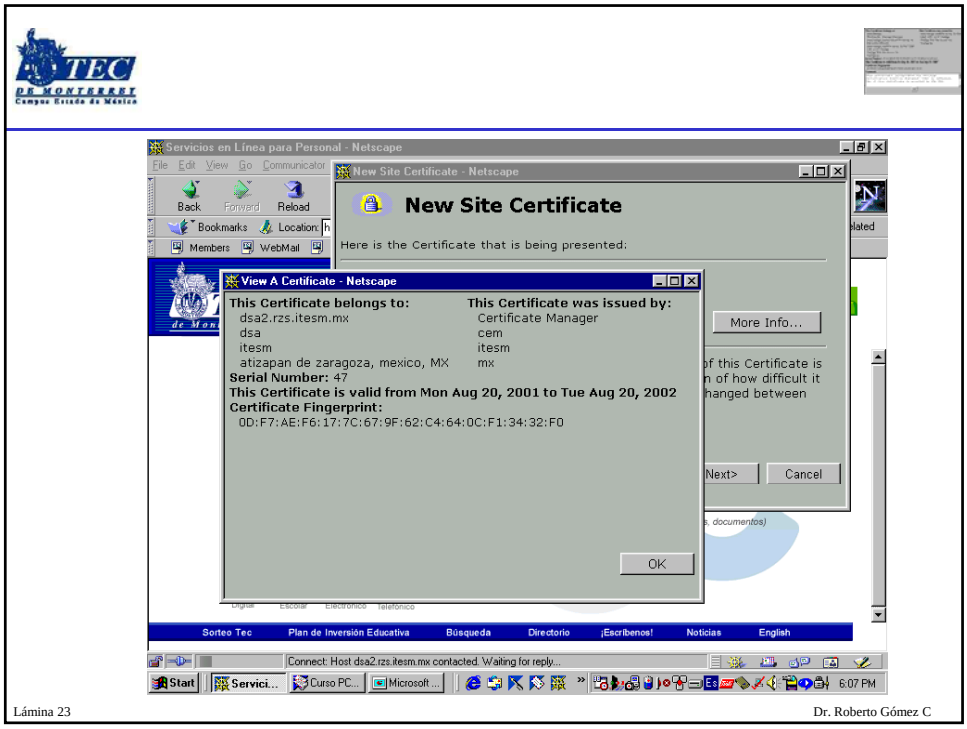


Lámina 23 Dr. Roberto Gómez C

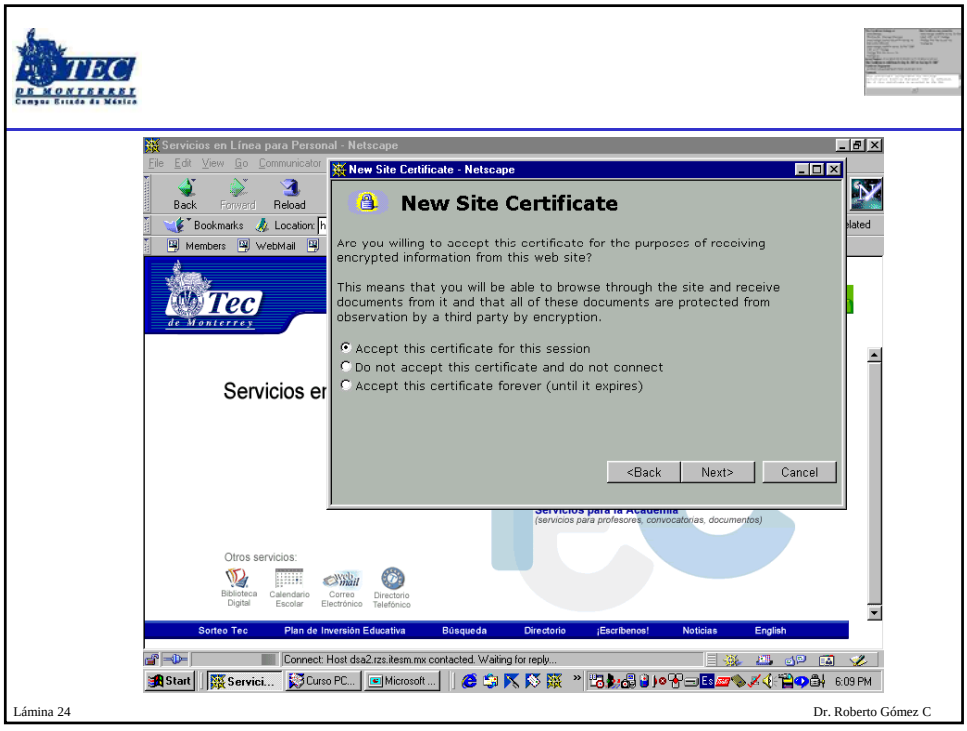


Lámina 24 Dr. Roberto Gómez C

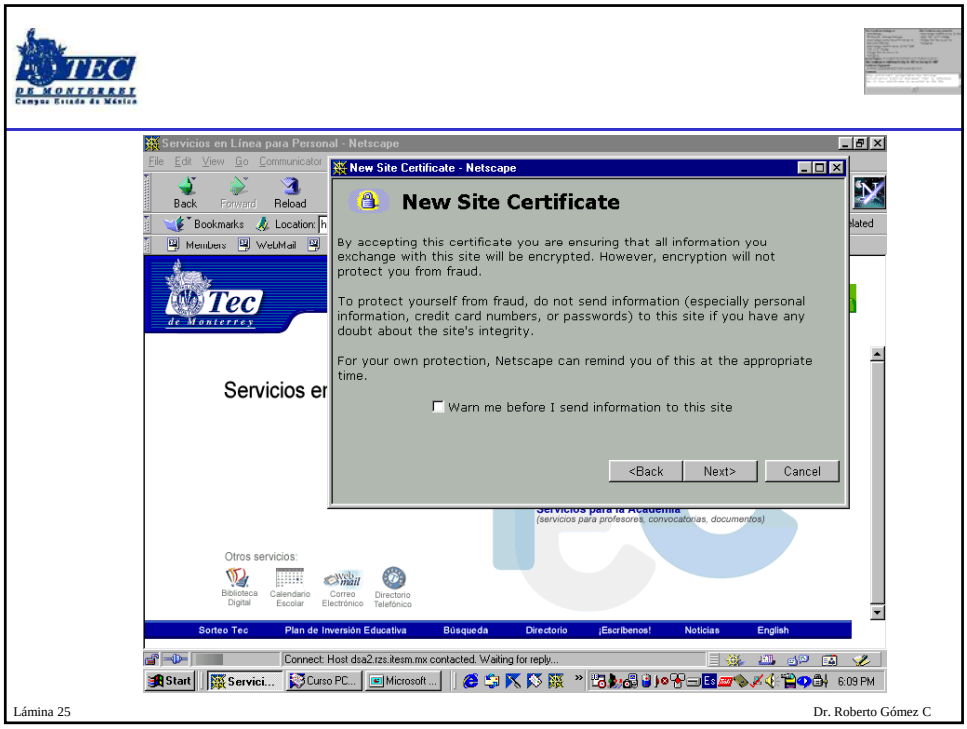


Lámina 25 Dr. Roberto Gómez C

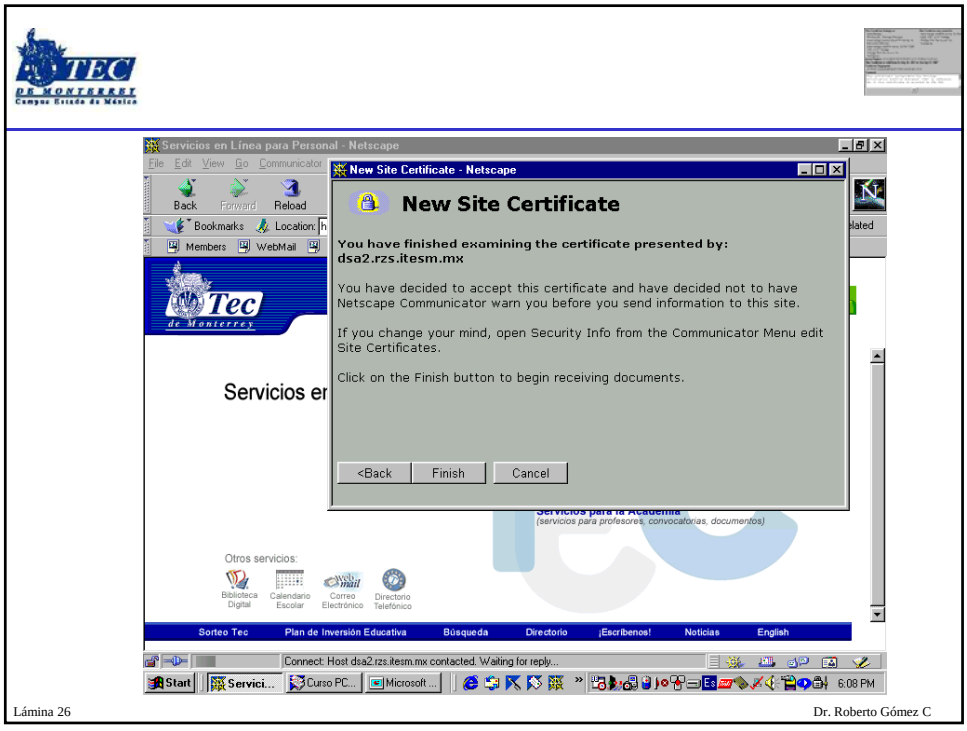
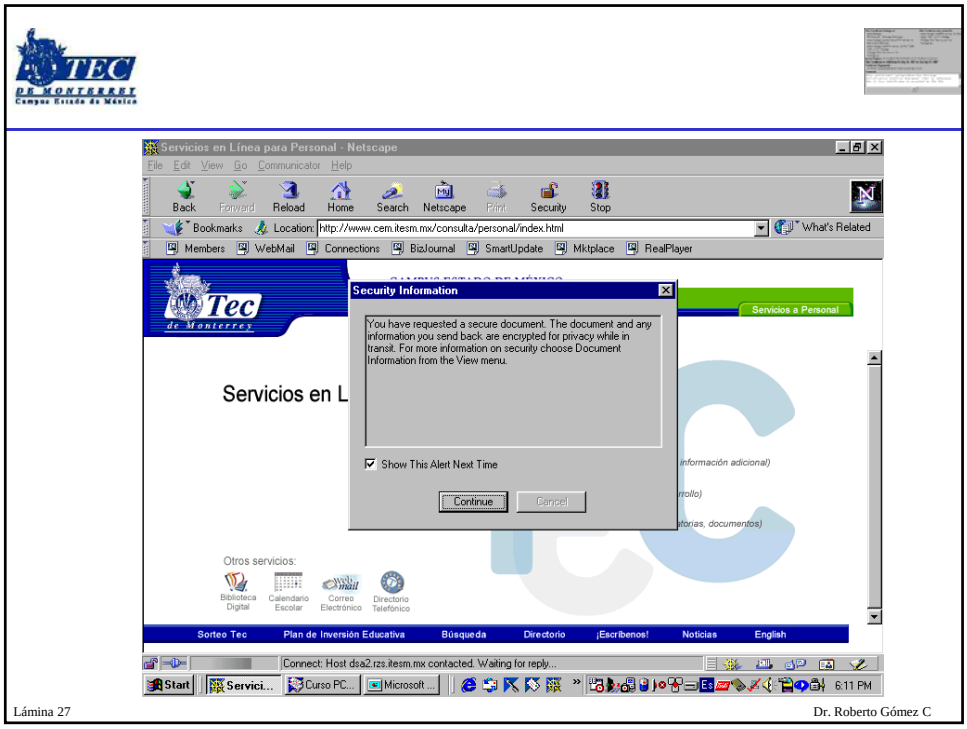
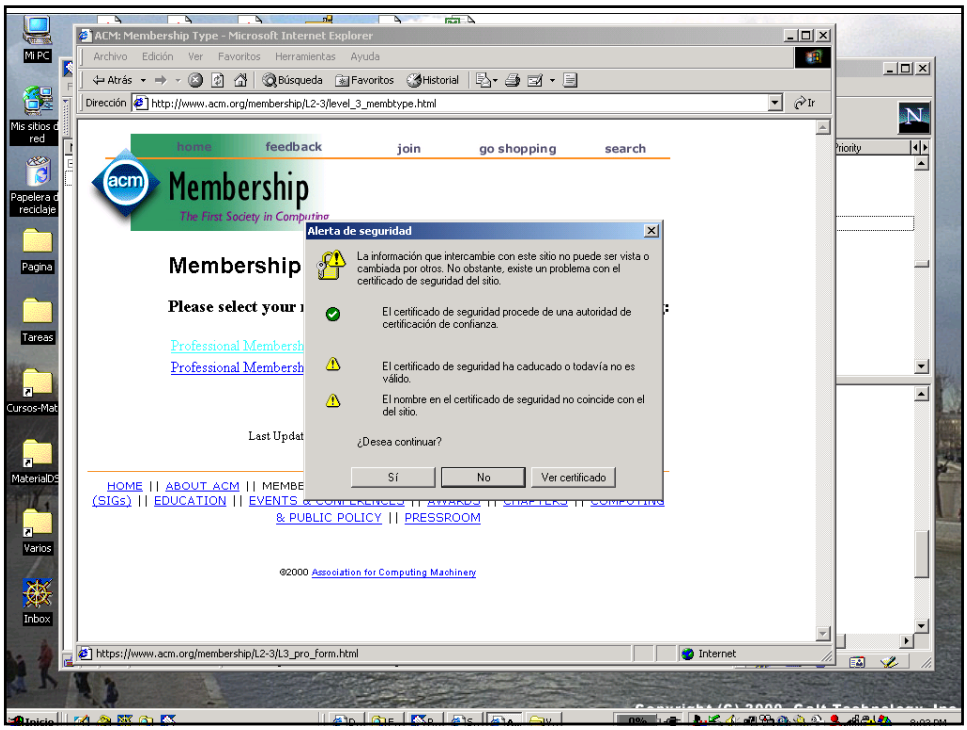


Lámina 26 Dr. Roberto Gómez C


Servicios en Línea para Personal - Netscape
Security Information
You have requested a secure document. The document and any information you send back are encrypted for privacy while in transit. For more information on security choose Document Information from the View menu.
Show This Alert Next Time
Continue
Cancel
Servicios en L
Servicios a Personal
Otros servicios:
Sorteo Tec
Plan de Inversión Educativa
Búsqueda
Directorio
¡Escríbenos!
Noticias
English
Lámina 27
Dr. Roberto Gómez C


ACM: Membership Type - Microsoft Internet Explorer
http://www.acm.org/membership/L2-3/level_3_membtype.html
home
feedback
join
go shopping
search
Membership
The First Society in Computing
Alerta de seguridad
La información que intercambie con este sitio no puede ser vista o cambiada por otros. No obstante, existe un problema con el certificado de seguridad del sitio.
El certificado de seguridad procede de una autoridad de certificación de confianza.
El certificado de seguridad ha caducado o todavía no es válido.
El nombre en el certificado de seguridad no coincide con el del sitio.
¿Desea continuar?
Sí
No
Ver certificado
Please select your
Professional Membersh
Professional Membersh
Last Updat
HOME || ABOUT ACM || MEMBE
(SIGs) || EDUCATION || EVENTS & CONFERENCES || AWARDS || CHAPTERS || COMPUTING & PUBLIC POLICY || PRESSROOM
©2000 Association for Computing Machinery
https://www.acm.org/membership/L2-3/L3_pro_form.html
Internet

Tipos Certificados Digitales (i)

- Certificado Personal
  - certifica identidad y posesión llave pública de un individuo
  - un servidor lo puede requerir para establecer una conexión segura, cliente envía su certificado
- Certificado de Servidor
  - identidad y posesión llave pública de un servidor
  - servidor presenta su certificado para establecer comunicación segura con otras entidades de la red

Lámina 29 Dr. Roberto Gómez C

Tipos Certificados Digitales (ii)

- Certificado de Correo Seguro
  - identidad y llave pública de un usuario de correo electrónico.
  - usado para verificar identidad usuario, encriptar, desencriptar y firmar mensajes de correo electrónico.
- Certificado de Autoridad Certificadora
  - Se pueden certificar entre sí al expedirse un documento digital que certifique su identidad y la posesión de la llave que utiliza para firmar los certificados que expiden.

Lámina 30 Dr. Roberto Gómez C

Tipos Certificados Digitales (iii)

- Certificados de fabricante de software
  - Sistemas no pueden garantizar que el código firmado se pueda ejecutar con seguridad, pero si pueden informar al usuario acerca de si el fabricante participa en la infraestructura de compañías y entidades emisoras de certificados de confianza.
  - Estos certificados se utilizan para firmar el software que se distribuye por Internet.

Lámina 31 Dr. Roberto Gómez C

El formato X.509

- El estándar base es el ITU-T X.509
  - Alineado con el ISO/IEC 9594-8
- Forma parte del servicio de directorios X.500 (UIT-T)
- Debe contener información tanto de la entidad que lo solicitó como de la Autoridad Certificadora que lo expidió.
- Define un entorno de trabajo para provisión de servicio de autenticación:
  - Formato de certificado.
  - Protocolo de autenticación basado en clave pública.

Lámina 32 Dr. Roberto Gómez C

Elementos estándar X.509

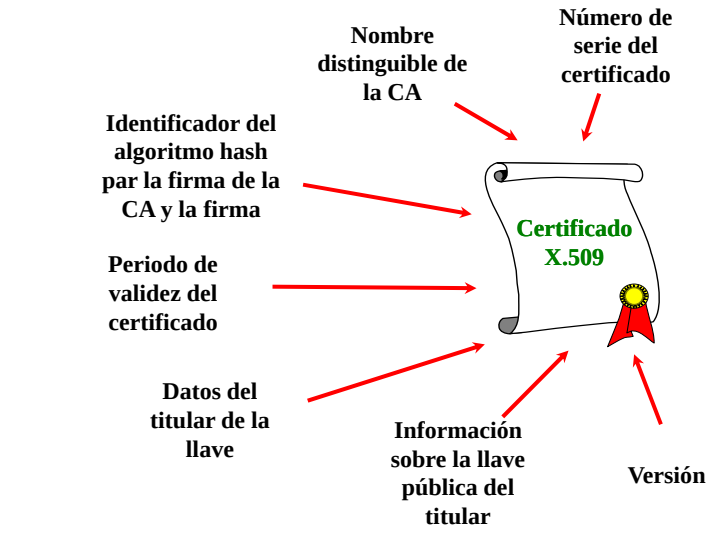


Lámina 33 Dr. Roberto Gómez C

Versiones formato X.509

- Versión 1:
  - Fecha: 1988
  - Base del estándar
- Versión 2
  - Fecha: 1992
  - Añade flexibilidad en los nombres.
- Versión 3
  - Fecha: 1993
  - Añade extensiones

Lámina 34 Dr. Roberto Gómez C

Certificado X.509 y ASN.1

- Especificado en un lenguaje conocido como Abstract Syntax One (ASN.1)
  - Estandarizado en las recomendaciones X.680-X.683.ASN.1
- ASN.1 es usado para la especificación ITU-T e ISP (y otros estándares) de comunicaciones.
- Propósito de ASN.1 es contar con un lenguaje estandarizado e independiente de plataformas, que permita expresar una estructura de datos.
- Acompañado por un conjunto de reglas conocido como reglas de codificación.

Lámina 35 Dr. Roberto Gómez C

Especificación X.509

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

 TBSCertificate  ::=  SEQUENCE  {
     version         [0]  EXPLICIT Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version shall be v2 or v3
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version shall be v2 or v3
     extensions      [3]  EXPLICIT Extensions OPTIONAL
                          -- If present, version shall be v3
     }

 Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
```

Lámina 36 Dr. Roberto Gómez C

Especificación X.509

```
CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
    notBefore      Time,
    notAfter       Time }

Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime    GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
    algorithm           AlgorithmIdentifier,
    subjectPublicKey    BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING  }
```

Lámina 37 Dr. Roberto Gómez C

Campos de la versión 1

- V (version): Versión del certificado.
- SN: Número de serie. (para los CRL)
- AI (signature): identificador del algoritmo de firma que sirve única y exclusivamente para identificar el algoritmo usado para firmar el paquete X.509.
- CA (issuer): Autoridad certificadora (nombre en formato X.500).
- TA (validity) : Periodo de validez.
- A (subject): 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 (con clave privada de una unidad certificadora).

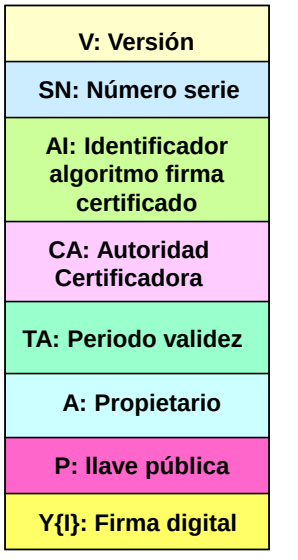


Lámina 38 Dr. Roberto Gómez C

Ejemplo X.509 v1

Ejemplo: **Una CA identifica a un certificado por su Serial Number**

SEQUENCE {

toBeSigned: SEQUENCE {
version: 0 (v1)
serialNumber: 75657
signature: pkcs1-sha1WithRsaSignature
issuer: CN=root, O=UOC, C=ES
validity: SEQUENCE {
notBefore: [utcTime] "000907164714Z"
notAfter: [utcTime] "100907164632Z“
}
subject: CN=Name Surname1, OU=Development, O=Empresa1, C=ES
subjectPublicKeyInfo: "AF3FD31ABEE4C1F743D ... 0BD8F8DF7"
}

DN : Distinguished Name
•CN : *Common Name* (nombre común)
•OU : *Organizational Unit* (departamento)
•O : *Organization* (organización)
•C : *Country* (país)

Periodo de validación

Incluye otra secuencia ASN.1 codificada en DER

signatureAlgorithm: pkcs1-sha1WithRsaSignature
signature: "56A376E029E97824 ... DFB19FBFAF“
}

Firma digital con la clave privada de la CA emisora

Lámina 39 Dr. Roberto Gómez C

Contenido de un certificado

```
Data:
    Version: 1 (0x0)
    Serial Number: 18 (0x12)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ES, ST=Madrid, L=Madrid, O=Lexus, OU=TI, CN=Lexus Certificate Server
    Validity
        Not Before: Jan  7 13:02:39 2000 GMT
        Not After : Jan  6 13:02:39 2001 GMT
    Subject: C=ES, L=Madrid, O=Lexus, OU=Ventas, CN=Javier Gallego/Email=jgallego@lexus.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (512 bit)
            Modulus (512 bit):
                00:98:59:ab:d9:7e:a3:40:21:60:ee:54:a5:a4:54:
                d2:29:fd:50:82:c1:28:05:25:0a:6b:aa:61:aa:e0:
                19:3b:d7:5e:18:f2:14:60:ed:58:f6:87:eb:4c:61:
                fc:9e:ed:9d:b2:19:d4:73:25:cc:d4:63:88:54:f4:
                49:2a:ba:ce:7b
            Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        7a:df:8a:aa:b5:23:5b:c6:ff:f3:02:73:65:bb:0f:05:7a:fd:
        f4:68:ee:b9:fe:92:72:53:bb:f2:31:9e:38:92:69:b3:04:22:
        d7:be:f5:18:42:7a:c0:9b:e2:1e:04:a4:66:02:80:76:79:0e:
        f6:c3:7e:25:2d:ec:00:01:fb:f7
```

Lámina 40 Dr. Roberto Gómez C

Segundo ejemplo certificado X.509

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            04:60:00:00:02
        Signature Algorithm: md2WithRSAEncryption
        Issuer: C=US, O=CREN/Corp for Research and Educational
Networking, OU=Education and Research Client CA
        Validity
            Not Before: Nov 17 00:00:00 1999 GMT
            Not After : Nov 17 00:00:00 2003 GMT
        Subject: C=US, O=CREN/Corp for Research and Educational
Networking, OU=Education and Research Client CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:96:f8:ea:aa:de:bc:33:74:ce:02:54:ef:1a:c7:
                    9d:0b:93:28:f3:59:e5:36:9b:a4:05:df:79:fd:99:
                    71:66:2c:90:1d:9c:d9:44:df:b9:ca:d9:e5:dd:f1:
                    69:03:dc:4a:e3:ba:ea:7d:68:84:7a:78:e8:b6:b7:
                    8e:94:ac:af:93:1e:05:81:0b:25:a0:72:ff:9e:0c:
                    24:9f:e3:bb:95:d4:40:82:c0:ff:d6:80:f2:ff:a4:
                    d6:20:be:09:bd:ec:44:59:74:ff:6f:5d:7a:69:3d:
                    d0:38:1e:33:17:be:d2:f7:ec:a7:e8:a9:05:ae:ba:
                    0b:98:85:3e:25:7e:92:e0:6f:25:32:a1:05:1f:7b:
                    54:01:3c:28:09:58:d8:7a:83:ed:aa:18:33:5a:14:
                    df:da:d5:d0:fe:d8:c2:17:16:fc:a7:16:af:de:c7:
                    06:f0:07:62:de:26:7b:bb:44:c8:02:ad:99:e4:d7:
                    f4:ff:1a:9f:51:d2:cd:9f:91:82:88:ae:f5:93:18:
                    5e:ec:37:1a:06:5c:62:1e:cf:9c:dd:5a:3f:23:8e:
                    e8:c3:59:05:5a:09:0e:9c:8c:08:c5:ad:55:fc:13:
                    b3:bb:38:08:45:f2:36:8e:f8:5a:3c:ba:96:45:38:
                    82:da:95:87:35:f8:2a:9a:75:1f:de:34:3d:27:0c:
                    6c:39
                Exponent: 65537 (0x10001)
    Signature Algorithm: md2WithRSAEncryption
```


Segundo ejemplo certificado X.509

```
                Exponent: 65537 (0x10001)
    Signature Algorithm: md2WithRSAEncryption
        1c:50:cf:82:d0:27:fc:a2:86:f1:c6:dd:b2:d1:f2:56:dc:c9:
        a0:4f:cc:0b:10:5c:25:c7:fc:25:60:ab:06:3d:55:44:3e:97:
        bb:62:8c:33:f6:80:c4:0d:72:41:47:ea:dc:e2:bf:d9:3e:83:
        c4:07:ac:25:b0:86:f5:d5:0f:63:fc:8b:0e:de:89:d5:c3:31:
        9f:cb:ba:71:9b:00:1d:67:64:94:2d:5f:93:59:93:27:d0:d2:
        8a:10:f2:83:e0:b4:00:f6:36:5f:67:86:3f:bb:ef:55:d6:44:
        41:01:fc:5c:66:5a:fa:64:b6:6f:9e:c5:c1:86:31:3f:37:53:
        fa:fc:57:01:94:02:bd:2d:4d:90:49:00:14:06:54:c3:75:d3:
        53:14:a2:10:e6:12:37:ee:bb:97:32:ff:ad:e5:b3:58:25:5d:
        40:9b:ed:3e:5c:79:f3:15:3f:d1:a7:bb:87:68:6a:0b:70:c3:
        19:54:46:84:d7:d7:76:9c:b3:79:92:a8:25:63:70:dc:ca:b5:
        b7:1b:96:34:c8:12:52:cb:fa:a6:16:c4:a6:0f:98:51:2f:44:
        90:5f:ea:74:4e:97:5a:82:33:84:20:51:70:04:bd:65:ae:97:
        0f:f0:c0:fa:91:00:07:e1:ec:2f:d9:bc:7c:f3:3a:02:ca:27:
        56:ec:67:22
-----BEGIN CERTIFICATE-----
MIIDYDCCAkgCBQRqAAACMA0GCSqGSIb3DQEBAqUAMHQxCzAJBqNVBAYTAlVTMTow
OAYDVQQKExFDUkVOL0NvcnAgZm9yIFJlc2VhcmNoIGFuZCBFZHVjYXRpb25hbCBO
ZXR3b3JraW5nMSkwJwYDVQQLEyBFZHVjYXRpb24gYW5kIFJlc2VhcmNoIENsaWVu
dCBDQTAeFw05OTExMTcwMDAwMDBaFw0wMzExMTcwMDAwMDBaMHQxCzAJBqNVBAYT
AlVTMTowOAYDVQQKExFDUkVOL0NvcnAgZm9yIFJlc2VhcmNoIGFuZCBFZHVjYXRp
b25hbCBOZXR3b3JraW5nMSkwJwYDVQQLEyBFZHVjYXRpb24gYW5kIFJlc2VhcmNo
IENsaWVudCBDQTCCASIwDQYJKoZIhvcNAQEBDQADggEPADCCAQoCggEBAJb46qre
wDN0zqJ07xHnQuYKPWZ5TshpAXfof2ZcWYakH2c2UTfucrZ5d3zaQPcSuO66nIo
hHp46La3jpSzr5MeBYKLJaBy/54MJJ/juSXUQILA/9aAB+k1iC+Cb3sRF10/29d
emk90DgeMze+0wfsp+ipBa66C5iFPiV+kuBwJTKhBR97VAE8KA1Y2HqD7aoYM1oU
39rV0P7YwhcW/KcWr97HBwAHYt4ae7tEwAKtmeTX9P8an1HSzZ+Rqoiu9ZMYXuw3
CqZcYh7PnNiaPyOO6MWZBVoJDpyMCMWtWfwTs7s4CEXyNo74Wjy6lkU4qtqVhzX4
Kpp1H940PScMbDkCAwEAATANBqqhkiG9w0BAQIFAAOCAQEAH1DPqtAn/KKC8cbd
stHyVtzpqE/MixhcJcf8JWirhj1VRD6Xu2KMM/aAxA1yQUfq3OK/2T6DxAesJbCG
9dUPY/yLDt6J1cMxn8u6cZsAHWdk1C1fk1mTJ9DSihDyg8C2APY2X2eGP7jPYdZE
QQH8XGZa+mSZb57FwYYxPzdT+vxXAZQCwS1NkEkAFAZUw3XTUxSiEMYSN8671zL/
xeWzWCVdQJvtPlx59xU/0ae7h2hqC3DDGVRGhNfXdp6zeZKoJWWw3OqltxuWNMqS
Usv6phbEpg+YUS9EkF/qdEyXWoIzhCBRcAS9Za6Xj/jA+pEIB+HsL9m8fPM6Ason
VuxnIq==
-----END CERTIFICATE-----
```

Tomado de http://www.cren.net/crenca/crencapages/docs/sample.html

Campos de la versión 2

- Se añaden dos campos de identificadores
  - **Id. único emisor**: identifica la CA de forma única si su nombre X.500 ha sido reutilizado por otras entidades (poco utilizado).
  - **Id. único sujeto**: identifica al sujeto de forma única si su nombre X.500 ha sido reutilizado por otras entidades (poco utilizado).

V: Versión
SN: Número serie
AI: Identificador algo-ritmo firma certificado
CA Autoridad Certificadora
TA: Periodo validez
A: Propietario
P: llave pública
Id. único emisor
Id. único sujeto
Y{I}: Firma digital

Lámina 43 Dr. Roberto Gómez C

X.509 v3

- Versiones anteriores no se adaptan a todos los requisitos que solicitan las aplicaciones actuales:
  - Campo de identificación de sujeto y emisor es demasiado corto y no se adapta a algunas aplicaciones que se identifican con URL o e-mail.
  - Necesario añadir información de políticas de seguridad para poder ser utilizado por aplicaciones como IPSec.
  - Necesario acotar el daño producido por un CA defectuoso o malicioso.
  - Necesario distinguir diferentes claves usadas por un mismo usuario e instantes de tiempo distintos (gestión del ciclo de vida de la clave).

Lámina 44 Dr. Roberto Gómez C

Características del X.509 v3

- Versión 3 propone introducir estas nuevas capacidades en forma de extensiones opcionales en vez de campos fijos:
- Tres categorías de extensiones:
  - Información de políticas y claves.
  - Atributos de emisor y sujeto.
  - Restricciones del certificado.

Lámina 45 Dr. Roberto Gómez C

Esquema X.509 v3

- Extensiones
  - Conjunto de una o varias extensiones

V: Versión
SN: Número serie
AI: Identificador algo-ritmo firma certificado
CA Autoridad Certificadora
TA: Periodo validez
A: Propietario
P: llave pública
Id. único emisor
Id. único sujeto
Extensiones
Y{I}: Firma digital

Lámina 46 Dr. Roberto Gómez C

Formato listas de revocación de certificados

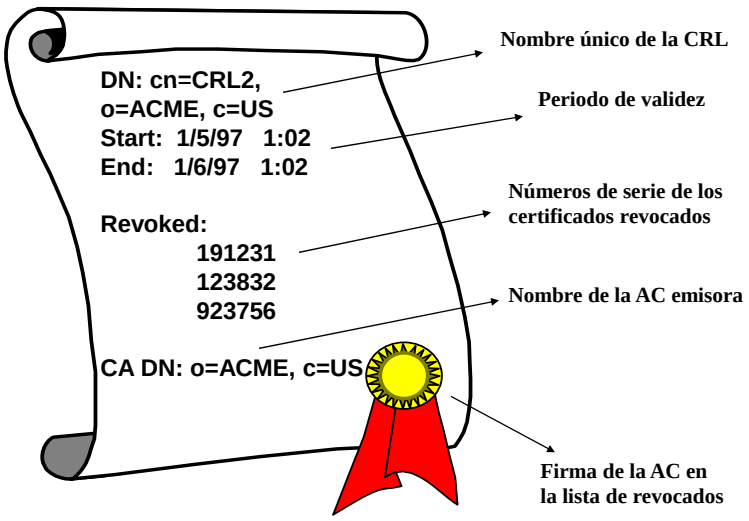


Lámina 47 Dr. Roberto Gómez C

Campos de una CRL

version	version 2
signature algorithm	
issuer x.500 name	la autoridad de certificación
this update	
next update (optional)	
certificate {user, time, extensions}	123.456.789.0, 28/12/1999, comprometida
certificate {user, time, extensions}	
certificate {user, time, extensions}	
extension {type, criticality, value}	CRL number: 313
extension {type, criticality, value}	
extension {type, criticality, value}	
CA digital signature	

Lámina 48 Dr. Roberto Gómez C

Estructura de una CRL

- Las CRL's disponen de un formato ASN.1
- Contienen una lista de números de serie de certificados revocados por la CA.

```
Ejemplo de CRL:
CRL: SEQUENCE {
                    toBeSigned: SEQUENCE {
                    version: 1 (v2)
                    signature: pkcs1-sha1WithRsaSignature
                    issuer: CN=root, O=UOC, C=es
                    thisUpdate: [utcTime] "000830165749Z"
                    nextUpdate: [utcTime] "000930165749Z"
                    revokedCertificates: SEQUENCE OF { revokedCertificate }
                    crlExtensions: SEQUENCE OF { extension }
                    }
          signatureAlgorithm: pkcs1-sha1WithRsaSignature
          signature: "56A376E029E97824 ... DFB19FBFAF"
          }
```

Lámina 49 Dr. Roberto Gómez C

Verificando los certificados

- Dos formas de verificar si un certificado es válido o no.
  - Listas de revocación CRL
    - Modelo pull: verificador baja la CRL de la CA cuando lo necesita
    - Modelo push: una vez que la CA actualiza la CRL, la información es enviada al verificador
  - Online Certificate Status Protocol (OCSP)

Lámina 50 Dr. Roberto Gómez C

Problemas asociados a las CRLs

- Metodos PULL
  - Periodicidad en la publicación de la CRL
    - Periodo de granularidad
  - Gran tamaño de las listas
    - Delta CRLs
    - Incremento de los puntos de distribución
    - Periodo de validez de los certificados
    - Reducción de los certificados Revocados
- Métodos PUSH
  - Establecimiento de canales seguros
  - Sobrecarga del tráfico
  - Métodos distribuidos de actualización

Lámina 51 Dr. Roberto Gómez C

Protocolo de estado de certificado en línea (OCSP)

- Proporciona información más adecuada y reciente
- Cuenta con una rápida aceptación
- CAs delegan a *responders* el proporcionar información de revocaciones
- No requiere CRLs: ahorra tráfico y CPU
- CRLs contienen información sensible
- Funcionamiento: el OCSP *client* envía petición de estado al OCSP *responder* y suspende su aceptación hasta recibir respuesta

Lámina 52 Dr. Roberto Gómez C

Online Certificate Status

- Los clientes ya no tienen que manejar el status

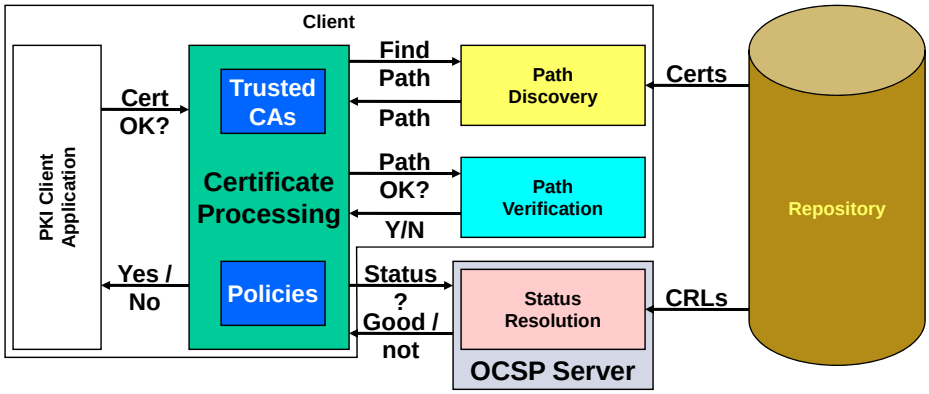


Lámina 53 Dr. Roberto Gómez C

Primera generación OCSP

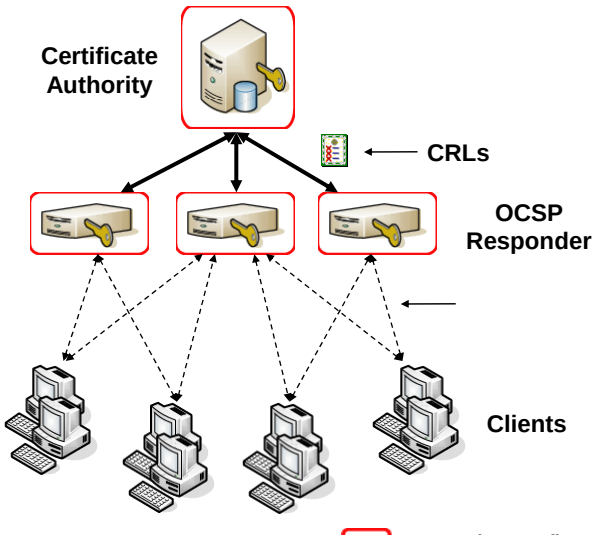
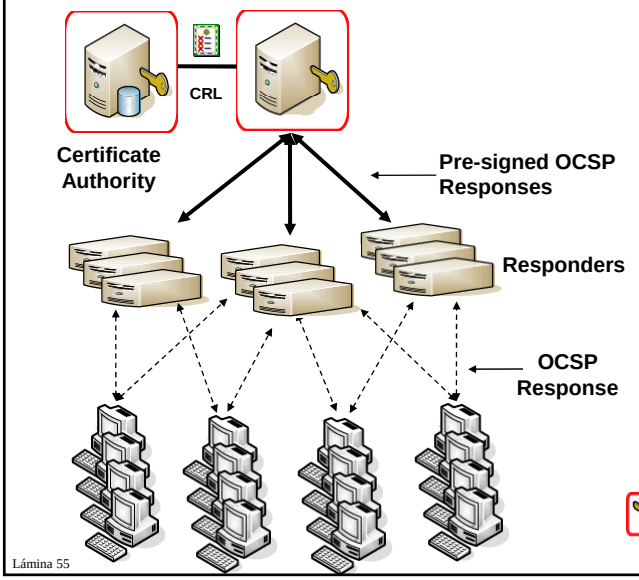


Lámina 54 Dr. Roberto Gómez C

OCSP distribuido



Principio:
Separar las funciones de seguridad de las de distribución

Lámina 55 Dr. Roberto Gómez C

Protocolo de estado de certificado en línea (OCSP)

- Proporciona información más adecuada y reciente
- RFC 2560
- Cuenta con una rápida aceptación
- CAs delegan a *responders* el proporcionar información de revocaciones
- No requiere CRLs: ahorra tráfico y CPU
- CRLs contienen información sensible
- Funcionamiento: el OCSP *client* envía petición de estado al OCSP *responder* y suspende su aceptación hasta recibir respuesta

Lámina 56 Dr. Roberto Gómez C

Online Certificate Status

- Los clientes ya no tienen que manejar el status

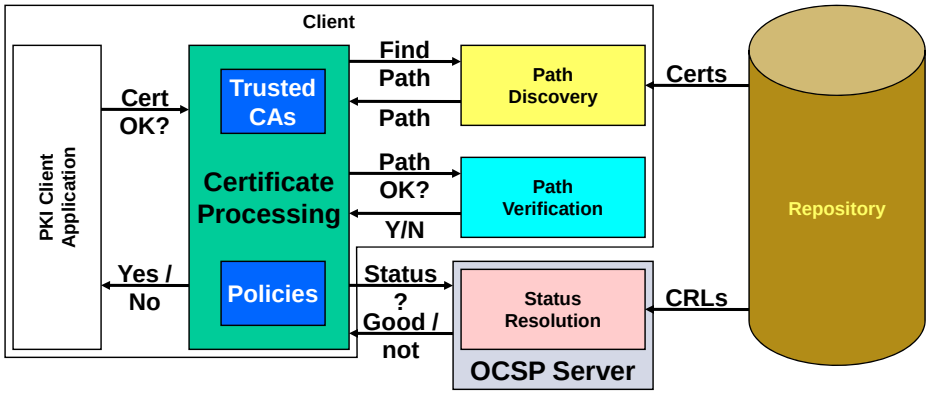


Lámina 57 Dr. Roberto Gómez C

Primera generación OCSP

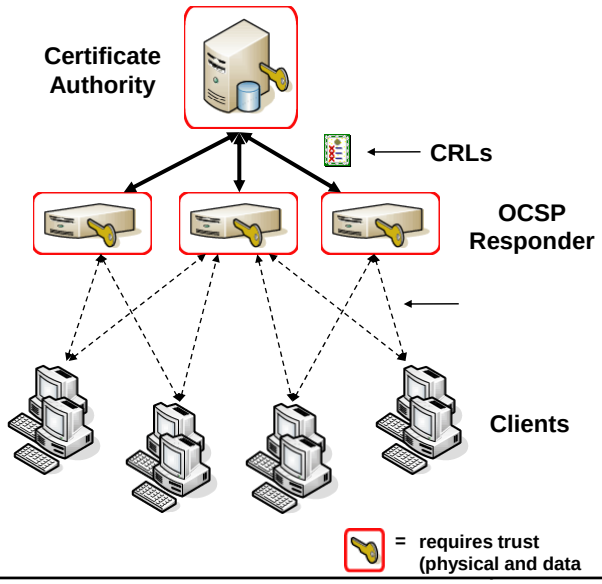
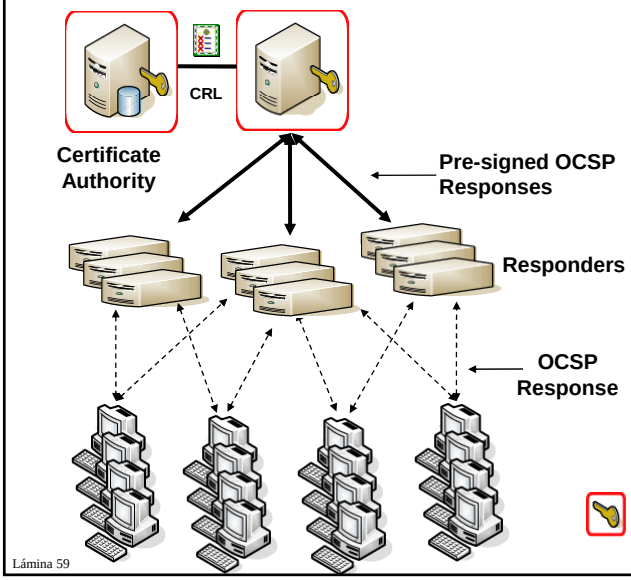


Lámina 58 Dr. Roberto Gómez C

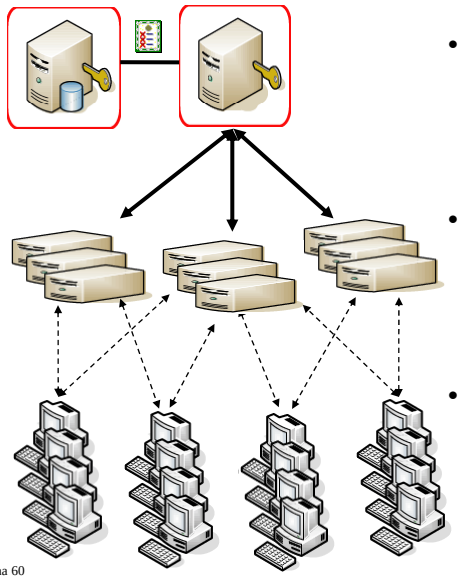
OCSP distribuido



Principio:
Separar las funciones de seguridad de las de distribución

Lámina 59 Dr. Roberto Gómez C

Características OCSP distribuido



- Seguridad
  - Firmado de llave fuera de línea
  - Ninguna llave en los servidores en línea
    - Responders no pueden mentir
- Desempeño
  - Más de 1000 pets/seg cada una:
    - No RSA a tiempo real
    - Simple búsqueda en tabla
    - 10-100 ms por petición
- Costo (aprox USD)
  - Servidor: $3K
  - Admon: $3-5K / año

Lámina 60 Dr. Roberto Gómez C

Infraestructura de llave pública (PKI)

Una infraestructura de llave pública (PKI) es la arquitectura, organización, tecnología, prácticas, políticas y procedimientos que en conjunto soportan la implantación y operación de un sistema criptográfico de llave pública basado en certificados.

PKI´s son 80% políticas y 20% tecnología

Lámina 61 Dr. Roberto Gómez C

Componentes de una PKI

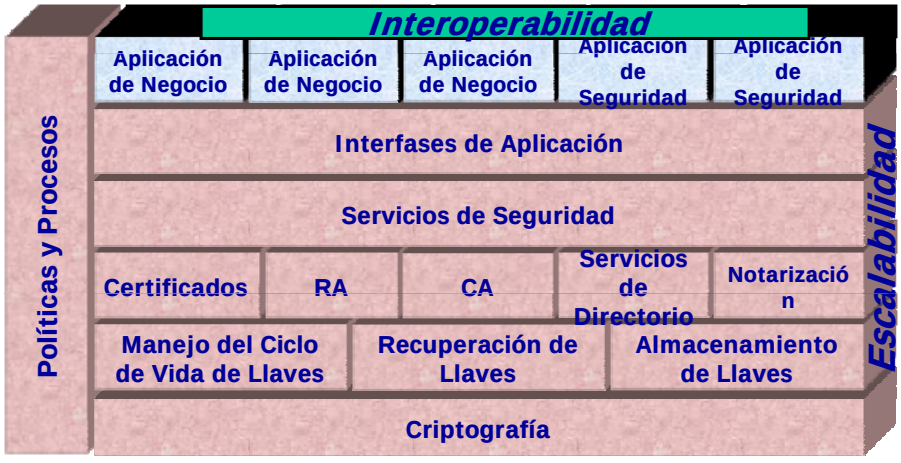


Lámina 62 Dr. Roberto Gómez C

Componentes y funciones de una PKI

- Autoridad certificadora
- Certificados digitales
- Autoridad de validación
- Repositorio de certificados
- Autoridad de registro

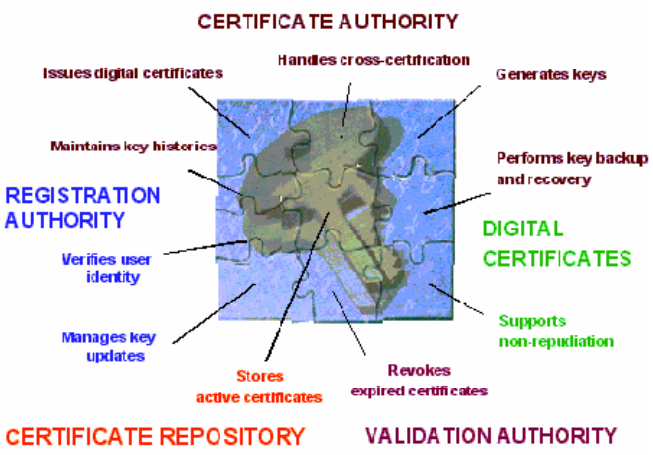


Lámina 63 Dr. Roberto Gómez C

Estructura General de una PKI

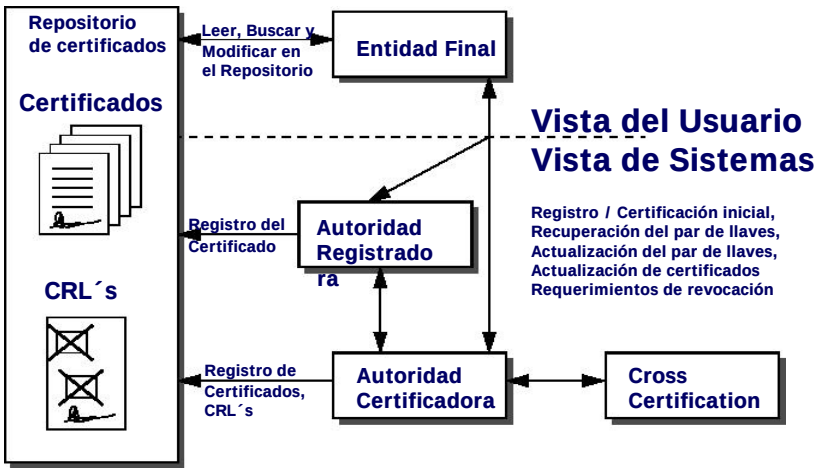


Lámina 64 Dr. Roberto Gómez C

Repositorio

- X.500 & DAP
  - lo clásico, que iba a ser el directorio universal y ha resultado excesivo e inviable
- LDAP [rfc 2587]
  - nace como una forma económica de que clientes ligeros (PC) accedan a directorios x.500
  - modelo de información jerarquizada, asociando atributos con los nodos
  - se presta de forma natural a ser un servicio de directorio distribuible y coordinable y, por tanto, a almacenar certificados y CRL
- HTTP & FTP [rfc 2585]
  - soluciones ad-hoc

Lámina 65 Dr. Roberto Gómez C

Autoridades de registro

- Son los responsables de verificar los datos que se añadirán al certificado como verificar el nombre del titular, ... de acuerdo con una política de certificación.
- Cada CA tiene una o más RAs que le proporcionan peticiones de certificado.
- La RA será la encargada de enviar la petición de certificados a la CA una vez las comprobaciones sean correctas.
- Los certificados podrán ser publicados en un servicio de directorios como puede ser LDAP y donde todo el mundo pueda acceder a él.

Lámina 66 Dr. Roberto Gómez C

Los modelos de confianza

- La entidad “A” confía en la entidad “B” cuando “A” supone y asume que “B” se comportará exactamente como “A” espera.
  - Jerárquico
    - Basado en la relación Superior / Subordinado
    - Actualmente es la regla en ambiente de web
    - Mientras mas cercano al nivel root se comprometa una llave mayor será el impacto para la organización
  - Distribuido
    - Es una red distribuida basada en una certificación cruzada “Cross Certification”
    - Mas flexible tanto en ambientes intra/inter organizacionales
  - “La mayoria de los proveedores soportan uno o el otro, pero pocos soportan ambos”

Lámina 67 Dr. Roberto Gómez C

CA Centralizada

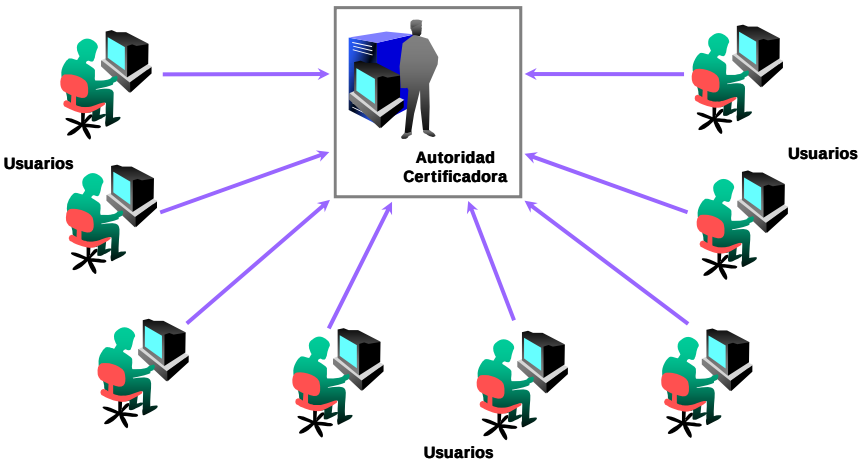


Lámina 68 Dr. Roberto Gómez C

CA Jerárquica

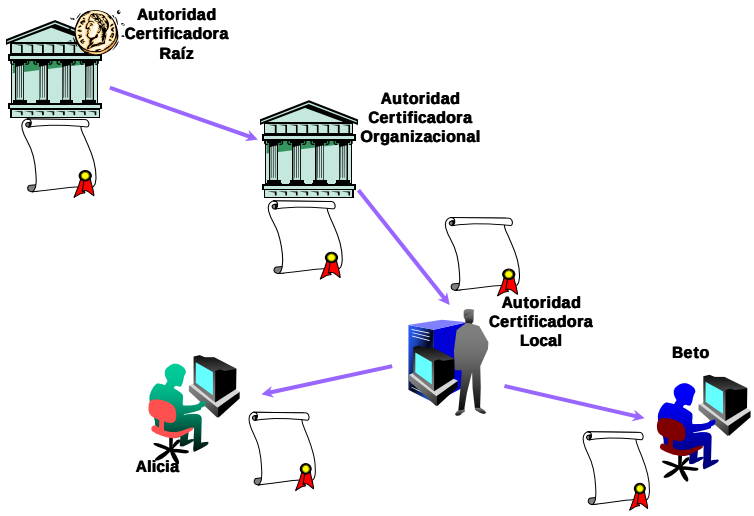


Lámina 69 Dr. Roberto Gómez C

"Web of Trust" de PGP

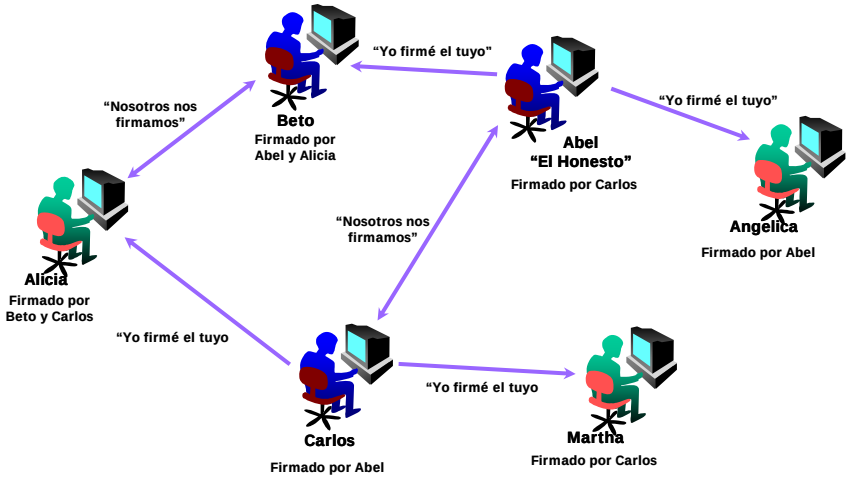


Lámina 70 Dr. Roberto Gómez C

Un caso práctico en México

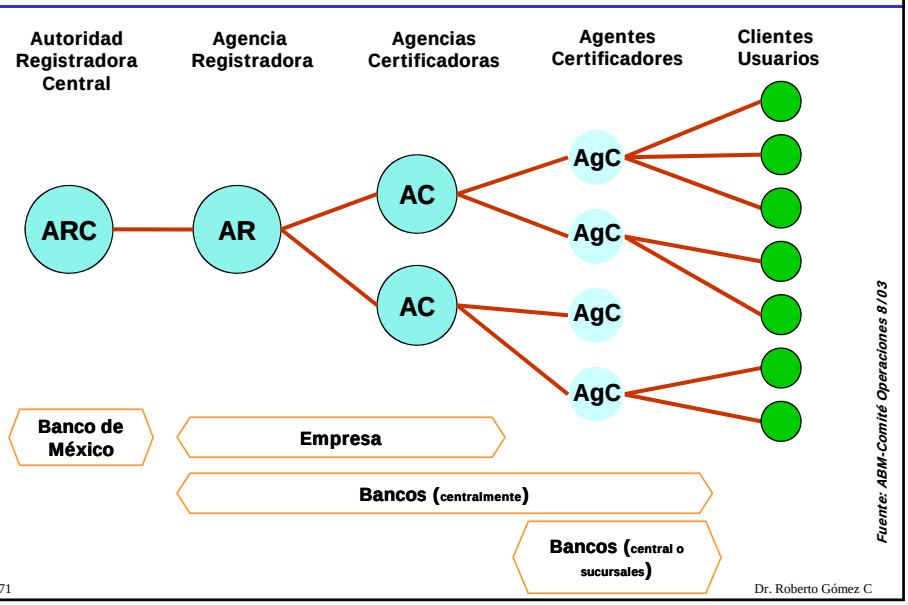


Lámina 71 Dr. Roberto Gómez C

Construcción y validación de paths de certificados

- Cadena de certificados, donde el emisor del primer certificado es un punto confianza y el sujeto del último certificado es la entidad final.
  - El último certificado es el que va a ser validado
- Construcción del path
  - Construir la cadena de certificados
- La validación del path es el proceso de verificar el path creado
  - Verificación criptográfica de cada firma en un certificado

Lámina 72 Dr. Roberto Gómez C

¿Qué es descubrimiento de una ruta (path discovery)?

- ¿Existe una ruta (path)?
  - De algo en lo que yo confío
  - Al subscriptor del certificado
  - Sin certificados revocados
  - ¿Qué satisfaga todas las políticas/limitaciones?

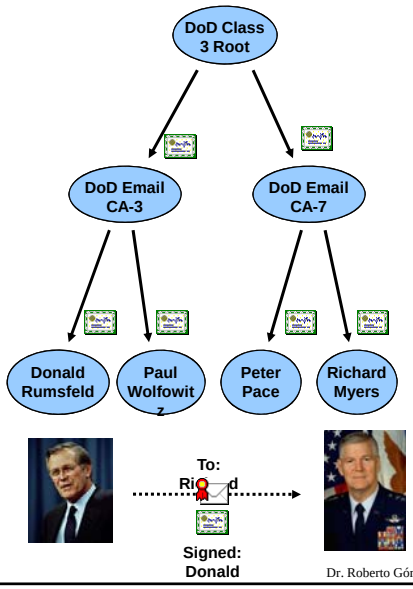


Lámina 73 Dr. Roberto Gómez C

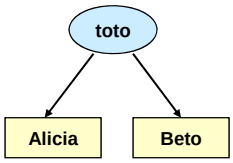
Path de certificados

- Aplicación dentro PKI debe verificar un certificado antes de usar la llave pública dentro de este para una operación criptográfica.
- No es posible confiar en la llave, a menos que exista una cadena de certificados.
- Aplicación inicializada para reconocer paths que inician con una o más autoridades certificadoras
  - Estas CAs se conocen como puntos de confianza
- Primer paso para usar certificado es construir un path de certificación entre el certificado y una de las puntos de confianza.

Lámina 74 Dr. Roberto Gómez C

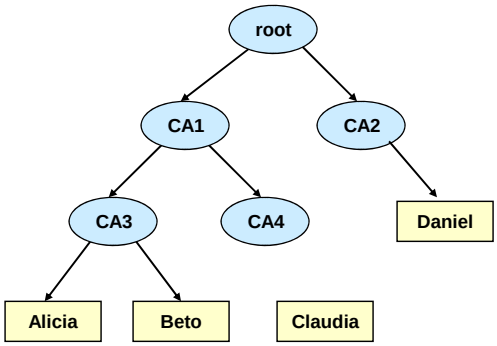
Ejemplo construcción del path

- Arquitectura simple
  - Un solo certificado
  - Solo es necesario un certificado para conectar el punto de confianza con el negocio



Alicia: [(toto → Alicia)]
Beto: [(toto → Beto)]

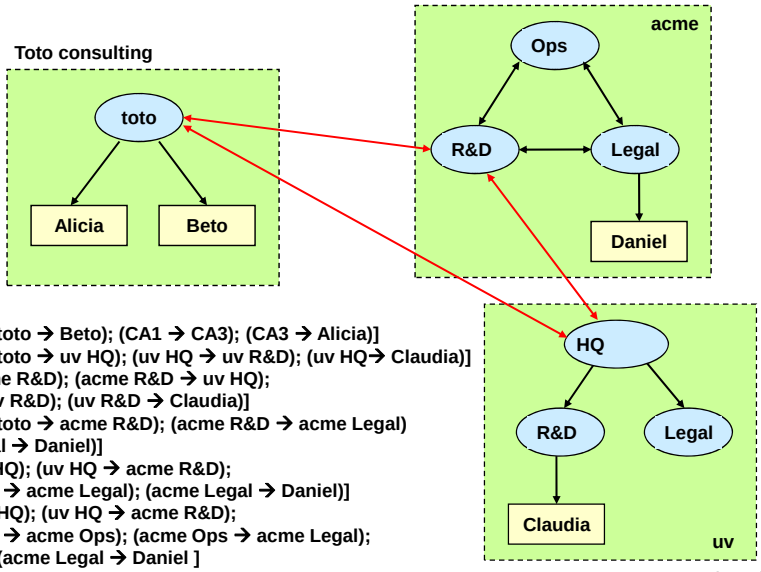
- Jerarquías
  - Se empieza en raíz y se termina en entidad final



Alicia: [(root → CA1); (CA1 → CA3); (CA3 → Alicia)]
Beto: [(root → CA1); (CA1 → CA3); (CA3 → Beto)]
Claudia: [(root → CA1); (CA1 → CA4); (CA4 → Claudia)]
Daniel: [(root → CA2); (CA2 → Daniel)]

Lámina 75 Dr. Roberto Gómez C

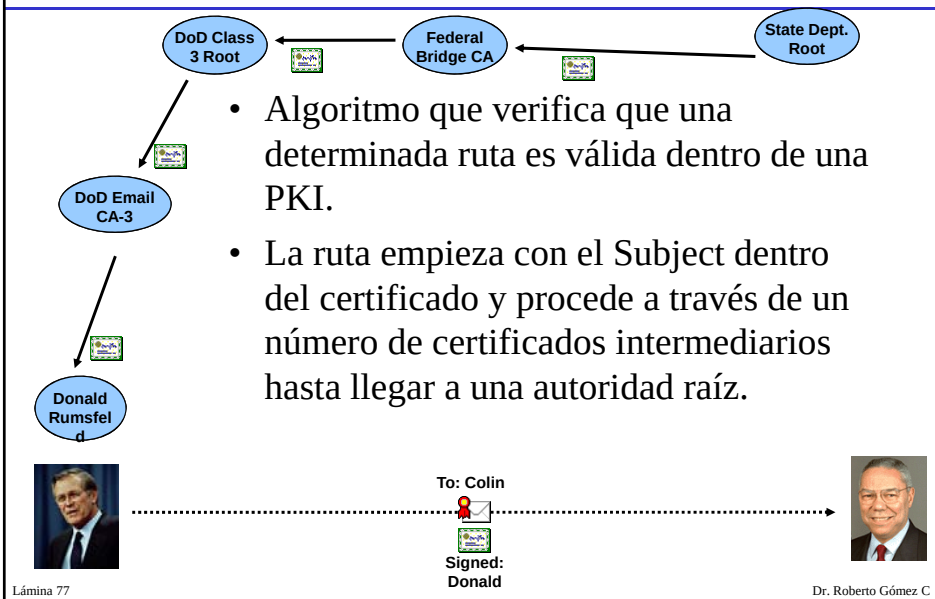
¿Y en el caso de un cross site?



Alicia: [(toto → Beto); (CA1 → CA3); (CA3 → Alicia)]
Claudia: [(toto → uv HQ); (uv HQ → uv R&D); (uv HQ→ Claudia)]
[(toto → acme R&D); (acme R&D → uv HQ);
(uv HQ→ uv R&D); (uv R&D → Claudia)]
Daniel: [(toto → acme R&D); (acme R&D → acme Legal)
(acme Legal → Daniel)]
[(toto → uv HQ); (uv HQ → acme R&D);
(acme R&D → acme Legal); (acme Legal → Daniel)]
[(toto → uv HQ); (uv HQ → acme R&D);
(acme R&D → acme Ops); (acme Ops → acme Legal);
(acme Legal → Daniel]

Lámina 76 Dr. Roberto Gómez C

Algoritmo de validación de ruta a un certificado



- Algoritmo que verifica que una determinada ruta es válida dentro de una PKI.
- La ruta empieza con el Subject dentro del certificado y procede a través de un número de certificados intermediarios hasta llegar a una autoridad raíz.

Lámina 77 Dr. Roberto Gómez C

Validación del path de certificados

- Para ser válida, la secuencia de certificados debe satisfacer
  - Un punto de confianza emitió el primer certificado
  - El último certificado fue emitido por la entidad final de interés y contiene la llave pública de interés
  - Los nombres del sujeto y del emisor forman una cadena
    - Para todos los certificados de la secuencia excepto el primero y el último, el nombre del emisor coincide con el nombre del sujeto en el certificado anterior y el nombre del sujeto coincide con el nombre del emisor del certificado subsecuente.
  - El certificado no ha expirado

Lámina 78 Dr. Roberto Gómez C

Pasos en la validación del path

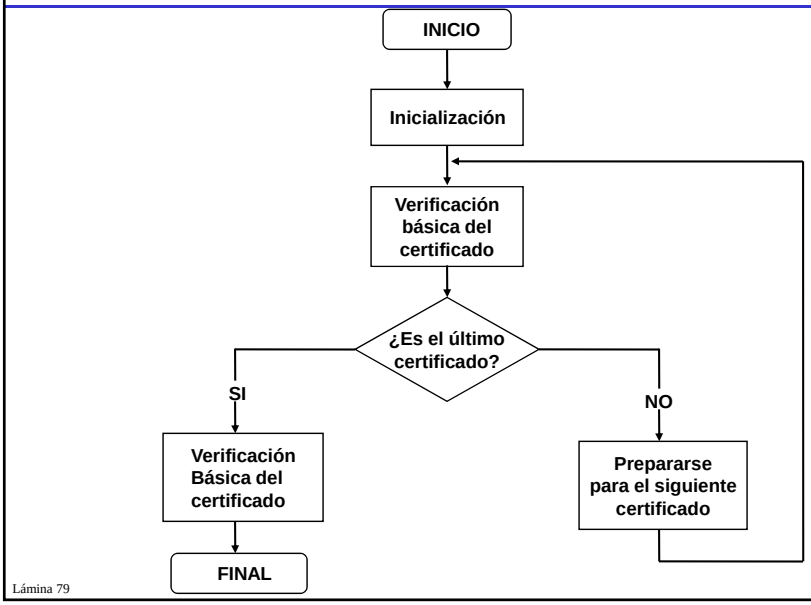


Lámina 79 Dr. Roberto Gómez C

PKI tradicional

- Clientes llevan a cabo todo el trabajo

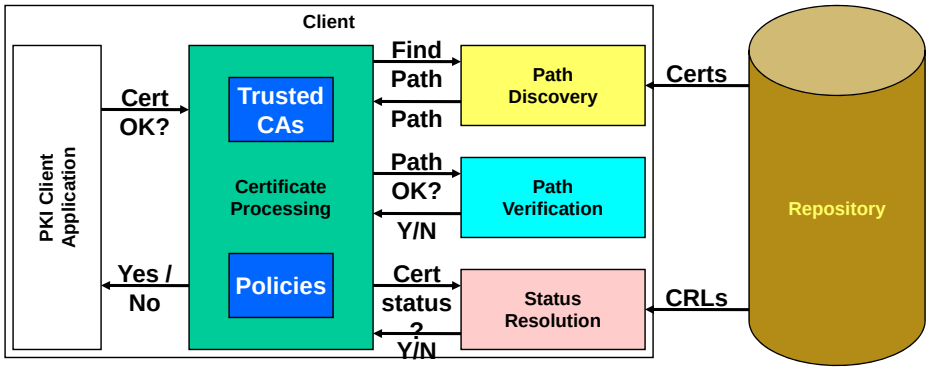


Lámina 80 Dr. Roberto Gómez C

Delegated Path Validation

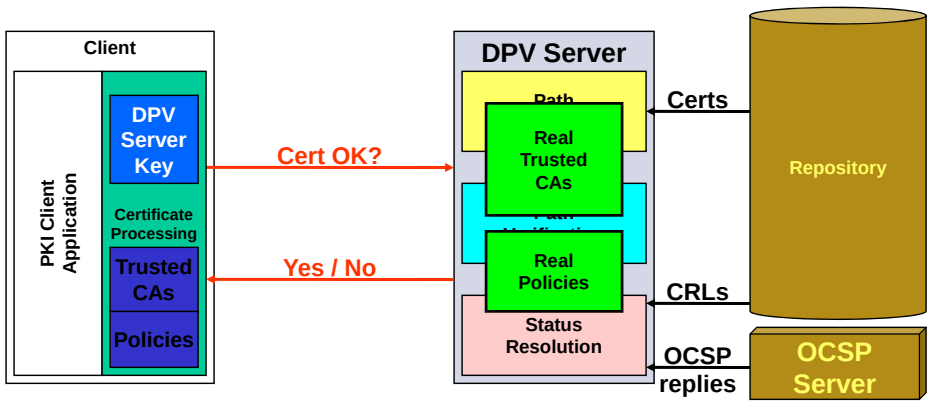


Lámina 81 Dr. Roberto Gómez C

Status regresado por el DPV

- De acuerdo a la política de validación, el status de la respuesta puede ser:
  - El certificado es válido
  - El certificado es inválido
  - El servidor no puede determinar la validez del certificado (i.e. no se puede construir la ruta).
  - La validez no pudo determinarse debido a un error

Lámina 82 Dr. Roberto Gómez C

Política de validación

- Una política de validación consta de cuatro componentes
  - Requerimientos de la cadena de certificados
  - Requerimiento de revocación
  - Requerimientos específicos al certificado final
  - Un periodo de cautela

Lámina 83 Dr. Roberto Gómez C

El DPV

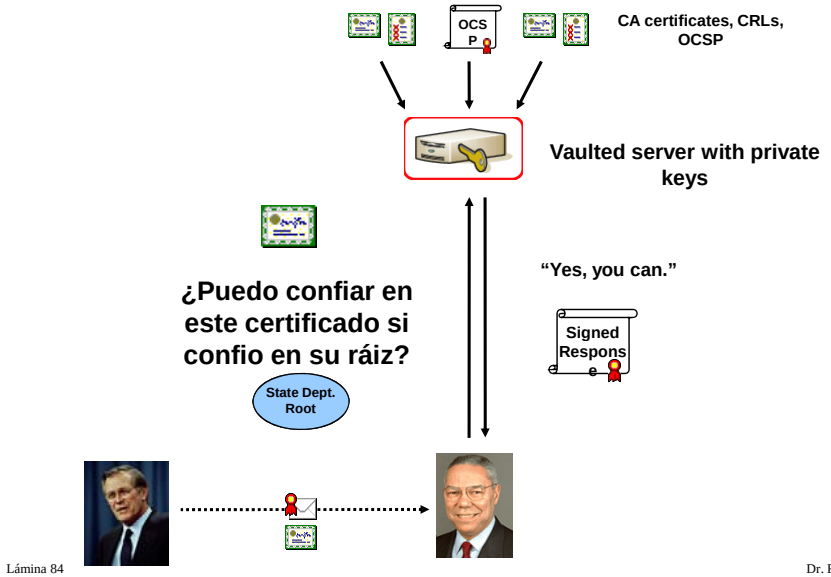
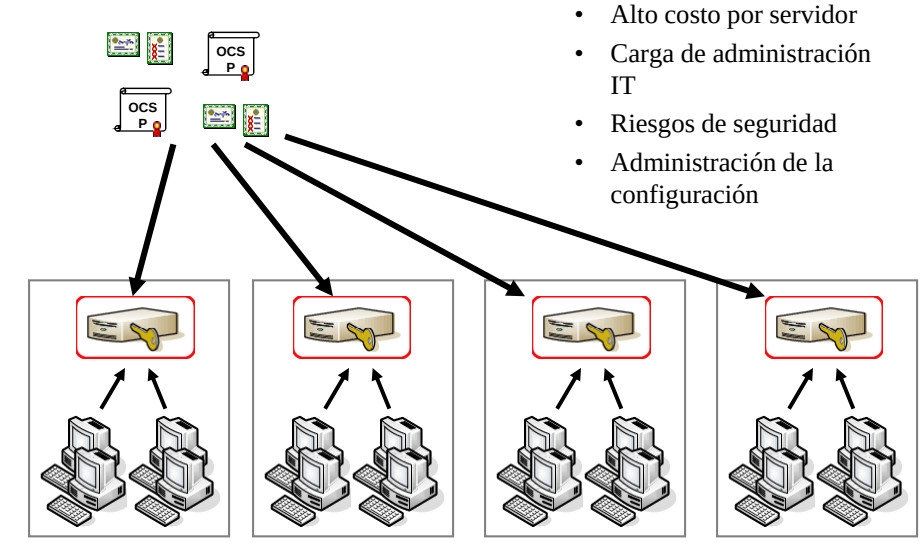


Lámina 84 Dr. Roberto Gómez C

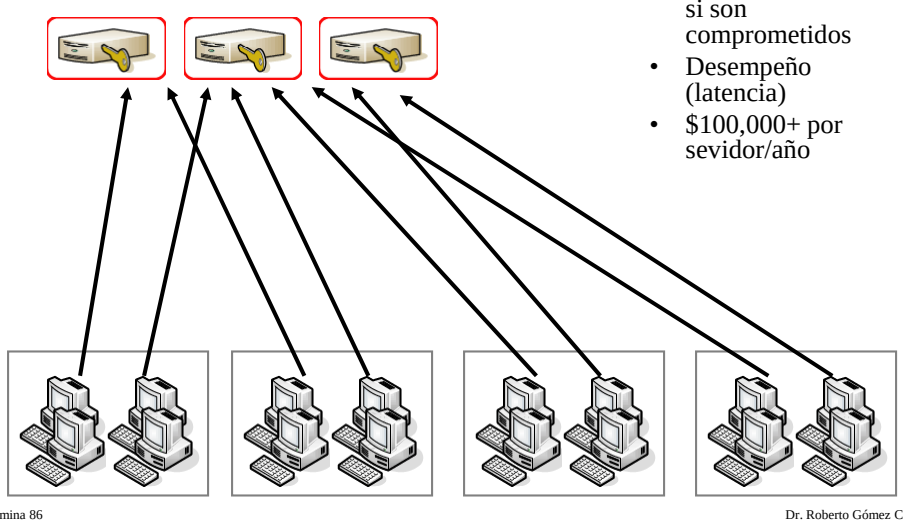
Servidores DPV locales



- Alto costo por servidor
- Carga de administración IT
- Riesgos de seguridad
- Administración de la configuración

Lámina 85 Dr. Roberto Gómez C

Servidores DPV centrales



- Gran impacto si son comprometidos
- Desempeño (latencia)
- $100,000+ por sevidor/año

Lámina 86 Dr. Roberto Gómez C

Delegated Path Discovery

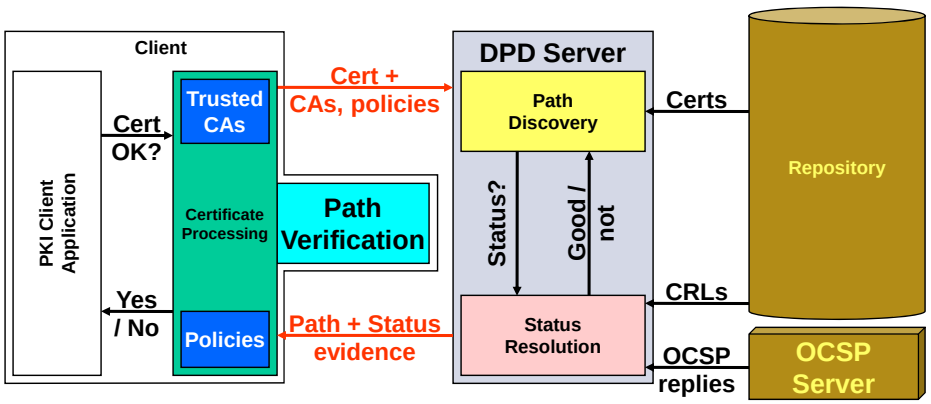


Lámina 87 Dr. Roberto Gómez C

Status regresado por el DPD

- El status de la respuesta puede ser cualquiera de tres opciones
  - Una o más rutas de certificación fueron encontradas de acuerdo a la política de descubrimiento de ruta, con información de revocación parcial o total presente
  - Se pudieron encontrar una o más rutas de certificación de acuerdo a la política de descubrimiento de ruta, sin ninguna información de revocación presente.
  - Ninguna ruta de certificación se pudo encontrar, de acuerdo a la política de descubrimiento de ruta.

Lámina 88 Dr. Roberto Gómez C

La opción DPD

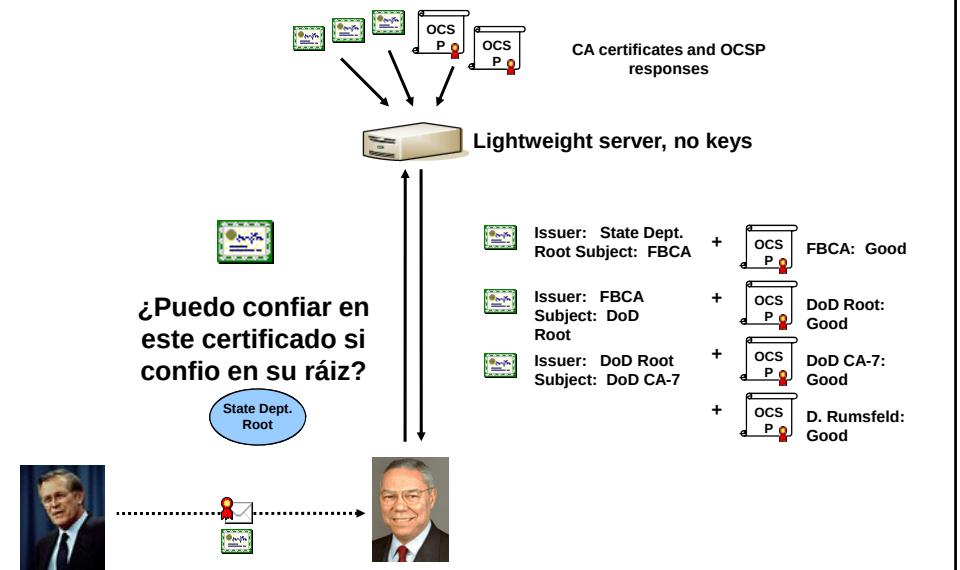


Lámina 89 Dr. Roberto Gómez C

DPD distribuido

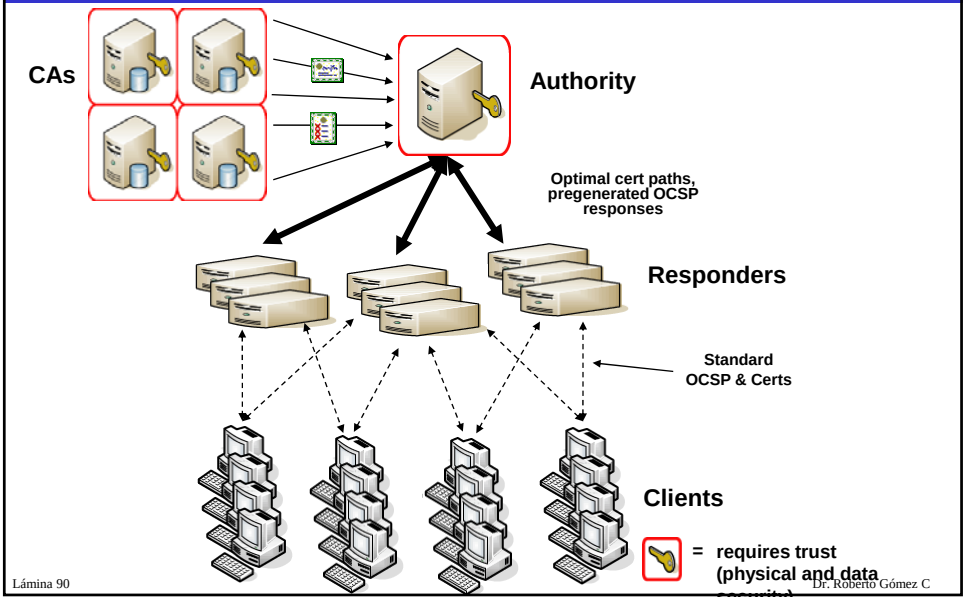


Lámina 90 Dr. Roberto Gómez C

¿Qué se requiere para implementar un demo de PKI ?

Instalación

Configuración

Demo aplicativo

Lámina 91 Dr. Roberto Gómez C

¿Qué se requiere para implementar una PKI operacional?

Soporte de entrenamiento
Administración de token´s
Organización de soporte
Autoridad para autorización de política
CA raiz
Sistemas de respaldo
Procedimientos y Políticas operacionales
Modelo de confianza
Conceptos de operaciones
Auditoría
Estructura del directorio
Proceso de registro
Plan de implementación
Emisión de smart card
CP & CPS
Proceso de Validación
Prueba del sistema
CA´s Operacionales
Responsabilidad legal
Pruebas en operación
Convención de nombres
Cumplimiento regulatorio
Administración de hardware
Administración de llaves
Entrenamiento a operaciones
Business continuity plan
OIDs
Firewalls
Pruebas End-to-end
Procesos de renovación
Procesos de revocación
Políticas y procedimientos de seguridad
Entrenamiento a usuarios
Archiving
OCSP

Lámina 92 Dr. Roberto Gómez C

Una PKI real requiere planeación

"Una PKI operacional de gran escala y misión crítica no es solamente un sistema piloto grande"

Simon Avarne - Head of Baltimore Consultants

Lámina 93 Dr. Roberto Gómez C

Certificados Digitales y PKI

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez

Lámina 94 Dr. Roberto Gómez C