



Infraestructuras de Clave Pública

José María Sierra



1



Introducción



2

Necesidad de una PKI

- Ventajas de la criptografía de clave pública
 - Solo puede utilizarse si se cumplen determinadas condiciones
 - Claves privadas protegidas
 - Claves públicas inequívocamente asociadas a una identidad
 - Intervención de entidades confiables
 - “confianza”
-

3

Protección claves privadas

- Almacenamiento cifrado en el disco duro
 - pgp, netscape
 - Almacenamiento cifrado en un disquete
 - Almacenamiento en un dispositivo “smart”
 - Tarjeta inteligente “smart card”
-

4

Protección claves privadas

- El proceso de firma digital debe protegerse:
 - Evitando que la clave privada salga del dispositivo que la contiene.
 - Capacidad de procesamiento en las smart cards
 - Tiempo de almacenamiento en la RAM
 - Caballos de Troya.

5

Necesidad de certificados

- Autoridad de Certificación
 - Entidad intermediaria y confiable que emite y administra los certificados
 - Garantiza la asociación entre una clave pública y una identidad.
 - Debe verificar los datos incorporados en el certificado.
 - Problemas asociados a lo difuso de las relaciones de confianza

6

Necesidad de certificados


- Información que debe contener un certificado
 - La identidad de un usuario y su clave pública
 - Un número de serie
 - Periodo de validez
 - La identidad de quién emite el certificado
 - La firma digital de las informaciones contenidas en el certificado.
-

7

Certificados X509

8

Certificados X.509v3

- Se trata de una recomendación de la ITU (International Telecommunication Union) 
 - La X.509 establece servicios de autenticación a los usuarios de directorios en sistemas abiertos
 - Autenticación simple
 - Autenticación fuerte
 - Procedimientos
 - Gestión de claves y certificados
-

9

Certificados X509v3

- Su sintaxis se define usando ASN.1 (Abstract Syntax Notation One)
 - Los campos están expresados en notación DN (Distinguished Name)
 - Están formados por atributos
 - Country (C)
 - Organization (O)
 - Common Name (CN)
 - ...
-

10

Certificados X.509v3

- Formato de un certificado X.509v3

- *versión*
- *nº de serie*
- *Identificación*
 - creador del certificado
 - poseedor del certificado
- *Periodo de validez*
 - NO antes de ...
 - NO después de ...

- *Descripción*
- *Clave pública*
- *Algoritmos utilizados*
 - Parámetros si fueron necesarios
- *Firma Digital*
 - Realizada sobre todo el contenido del certificado

11

Certificados X509v3

- Las versiones 1 y 2 de X.509 son deficientes en varios aspectos cuando se usan para sistemas a gran escala
- Puede ocurrir que el sujeto de un certificado tenga diferentes claves públicas para diferentes propósitos
- Algunas aplicaciones necesitan identificar usuarios mediante nombres específicos para la aplicación
- Surgen las extensiones para dotar de flexibilidad a los certificados
 - Información sobre claves
 - Información sobre el sujeto y el emisor
 - Restricciones de certificación
 - ...

12



Autoridades de Certificación

13



Autoridades de Certificación

- Se trata de una entidad que certifica claves públicas de acuerdo a una política
 - Política de certificación
 - Diversos tipos de certificados
 - Su mayor valor es la confianza, ya que técnicamente no son sustanciales
 - Los certificados pueden incluir otras informaciones que también sean certificadas
-

14



Autoridades de Certificación

- **Funcionamiento básico**
 - Puesta en marcha
 - Par de claves pública y privada de la AC
 - Distribución
 - Publicación del certificado de la AC
 - Recepción de solicitudes de firma
 - Protocolo de recepción de solicitudes
 - Comprobación de la asociación identidad – clave pública
 - Política de certificación
 - Firma digital de las solicitudes
 - Creación del certificado

15

Autoridades de Certificación

- **Certificación de la clave pública de la AC**
 - Esta certificación es indispensable
 - En ella se basan toda la seguridad de los certificados
 - Descarga por Internet
 - No está exenta de amenazas
 - Instalación o verificación manual
 - Está muy condicionada por la dimensión de la organización
 - Certificación por parte de otra AC
 - Integración directa en las aplicaciones que utilizan los certificados.

16

Autoridades de Certificación

- Cuestiones a tener en cuenta
 - Posibles tipos de AC
 - Dependiendo de las necesidades de las organizaciones
 - Jerarquías de confianza
 - Para facilitar la gestión de las AC's
 - Listas de revocación de certificados (CRL)
 - Certificados que dejan de ser válidos antes de caducar
 - Certificación de la clave pública de la AC

17

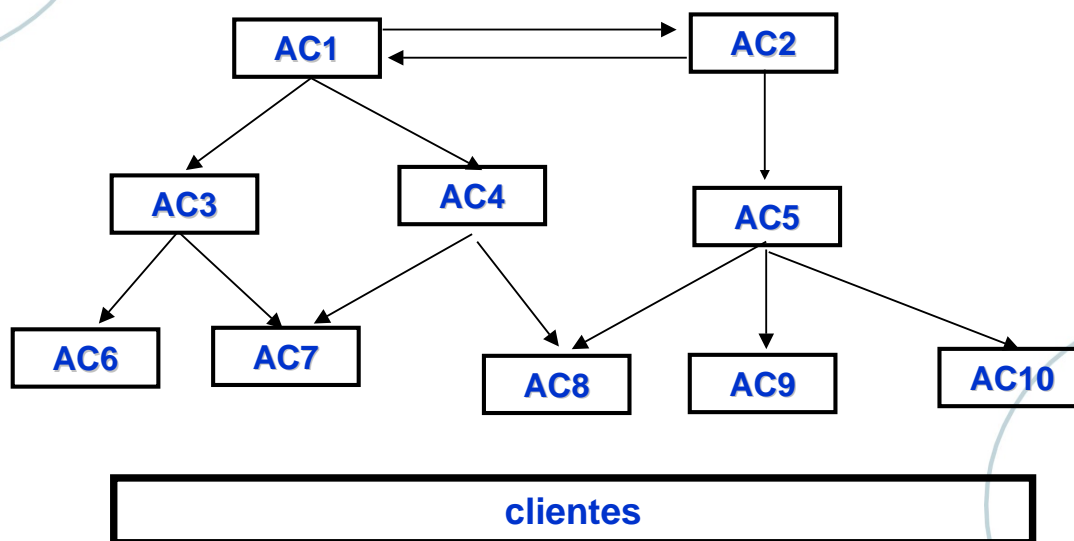
Autoridades de Certificación

- Tipos de autoridades de certificación
 - AC interna
 - AC ext. certificadora de empleados
 - AC ext. certificadora de clientes
 - AC tipo Tercera Parte Confiable
- Tipos de certificados
 - Certificados de usuarios
 - Certificados de servidores
 - Certificados de AC

18

Autoridades de Certificación

Jerarquía de autoridades de Certificación



19

Autoridades de Certificación

Listas de Revocación de Certificados (Certificate Revocation Lists, CRL)

- Causas
 - sustracción, errores, cambios de derechos, ruptura de la CA
- Problemas
 - CRL's de gran longitud
 - Existe un intervalo de posible fraude
 - Comprobación on-line de certificados
- Para verificar una firma de un documento, el usuario no sólo ha de verificar el certificado y su validez, sino que también ha de adquirir la versión más reciente de la CRL y confirmar que el número de serie del certificado no está en tal CRL

20

Autoridades de Certificación

- Contenido de una lista CRL
 - Versión
 - Algoritmo de Firma
 - Emisor
 - Actualización Presente
 - Siguiete Actualización
 - N° Serie Certificado
 - Fecha Revocación
 - Extensiones Locales
 - Extensiones Globales
-

21

Autoridades de certificación

- Problemas asociados a las CRL
 - 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
-

22

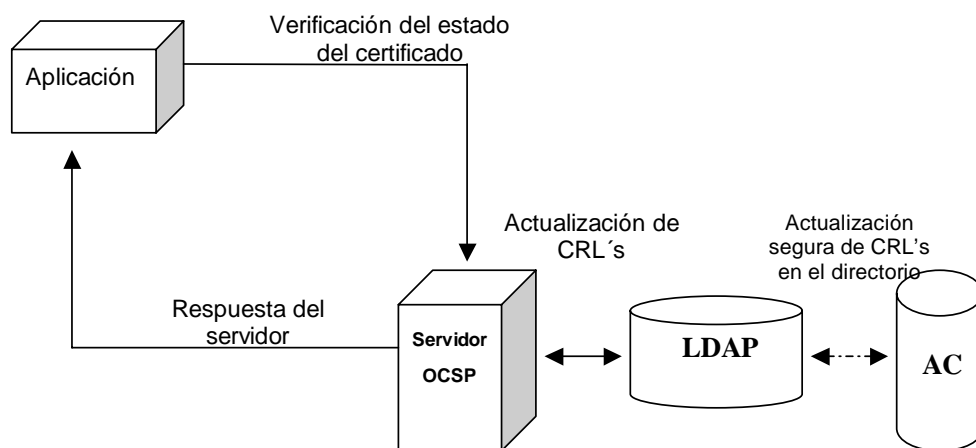
Autoridades de Certificación

- Servidor OSCP
- El Online Certificate Status Protocol
- Confirmación online del estado de un certificado
- La CA debe poner a disposición de todos los usuarios potenciales un servicio seguro online de alta disponibilidad

23

Autoridades de Certificación

- Esquema de funcionamiento de servidor OSCP



24



Infraestructura de clave pública

25



Infraestructura de clave pública

- Proporciona el marco que permite la implantación de la clave pública
 - Incluye una Autoridad de Certificación e integra toda su gestión en un sistema de información.
 - Servicios prestados:
 - Emisión de certificados
 - Generación de claves
 - Distribución de certificados
 - Certificación cruzada
 - Salvaguarda de claves
 - Suspensión y revocación de certificados
 - ...
-

26



Infraestructura de clave pública

- Opciones para la Generación del par de claves
- Opciones para la emisión de certificados
- Opciones para la distribución de certificados
- Certificación cruzada
 - Los certificados de usuario incluyen un certificado de otra autoridad de certificación
- Actualización del par de claves
 - Mayor duración de la clave pública
- Utilización de dos pares de claves
 - Confidencialidad y firma digital

27

Infraestructura de clave pública

- En una PKI pueden existir distintos tipos de entidades con funciones determinadas
- Dependiendo del modelo de PKI pueden variar los elementos
- Tipos de entidades
 - Autoridad de Certificación
 - Autoridad de Registro
 - Autoridad Raíz
 - Usuarios finales

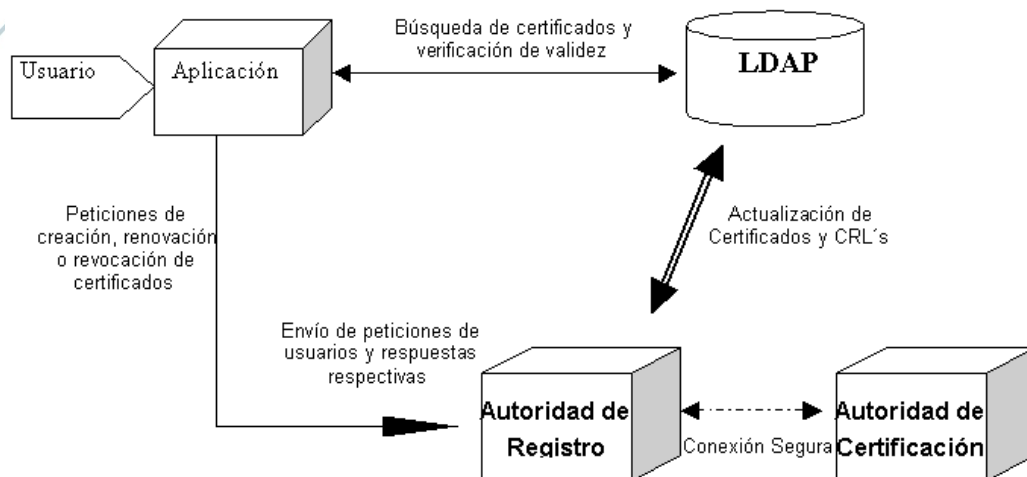
28

Infraestructura de clave pública

- Propiedades deseables en una PKI
 - Requisitos operacionales
 - Compatibilidad e Interoperatividad
 - Transparencia y facilidad de uso
 - Flexibilidad y escalabilidad
 - Requisitos de Seguridad
 - Confidencialidad
 - Integridad
 - Disponibilidad

29

Infraestructura de clave pública



30



Petición de certificados

31



Petición de Certificados

- Pueden ser solicitados mediante email o mediante web.
 - Los navegadores utilizan herramientas para generar las claves.
 - Netscape uses KeyGen
 - Microsoft uses GenerateKeyPair
 - Los servidores envía peticiones PKCS #10 a las CAs.
-

32



Petición de Certificados

- Las peticiones html de los navegadores son diseñadas para cada uno de ellos,
 - Netscape
 - Microsoft
 - Las respuestas con los certificados pueden ser enviadas vía email.
 - Los certificados pueden tener estructuras distintas.
 - PKCS #7
 - Certificados Base 64 encoded
 - Content Info (Netscape)
 - X.509v3
-

33

PKCS #10 Certificate Request

Webmaster: lusks@cybertrust.gte.com
Phone: (617)455-5270
Server: Netscape-Enterprise/2.0a

Common-name: Server Name
Email: lusks@cybertrust.gte.com
Organization: GTE Network Systems Division
Org-unit: Test Facility
Locality: Needham Heights
State: Massachusetts
Country: US

-----BEGIN NEW CERTIFICATE REQUEST-----

```
MIIBTTCB+AIBADCBIDELMAkGA1UEBhMCVVMxY2h0c2V0dHMxGDAWBgNVBAcTD05lZWRoYW0gSGVpZ2h0czEIMCMGA1UEChMcR1RFIE5ldHdvcm5U3lzdGVtYyBEaXZpc2lvcjEwMBQGA1UECXMNVGVzdCBGYWNpbGI0eTEUMBIGA1UEAxMLU2VydmVylE5hbWUwWjANBgkqhkiG9w0BAQEFAANJADBGAkEACw9hfY68Rr8sNQ2O3JXKZHR7qupgcm2SE/V/WOePf55e6Pjp2FRZrZlcVWjMm5A8LeHErf+UHI2L4bEYxemOwIBA6AAMA0GCSqGSib3DQEBBAUAA0EAZ1i8Q8UmjBMGs0gx0MMW4sGkqJleW619+QHRJLcGq07fXd/NMO2yVHM4Teb5SPDKAZurOHGjOjBmqDshQC/hRA==
```

-----END NEW CERTIFICATE REQUEST-----

34

Certificado

From cmsuser@olca-gte1.cybertrust2.gte.com Fri Nov 1 15:20 EST 1996
X-Authentication-Warning: webserver1.cybertrust2.gte.com: mail set sender to
<cmsuser@olca-gte1.cybertrust2.gte.com> using -f
Date: Fri, 1 Nov 1996 20:18:48 GMT
From: CMS Applications Server user <cmsuser@mail.cybertrust2.gte.com>
To: slusk@swid.ndhm.gtegsc.com
Subject: Certificate

Your certificate request has been generated for reference 8

-----BEGIN CERTIFICATE-----

```
MIIJNAYJKoZIhvcNAQcCoIIJTCCCSECAQEExADALBgkqhkiG9w0BBwGgggkJMIIIB9TCCA  
V4CAQAwDQYJKoZIhvcNAQEEBQAwrTELMaKGA1UEBhMCMVVMxGDAWBgNVBAoTD0dURSBDb3J  
w  
b3JhdGlvbjEcmBoGA1UEAxMTR1RFIEN5YmVyVHJ1c3QgUm9vdDAaFws5NjAyMjMxOTE1Wh  
cLOTkxMjMxMjM1OVowRTELMaKGA1UEBhMCMVVMxGDAWBgNVBAoTD0dURSBDb3Jwb3JhdGl  
vbjEcmBoGA1UEAxMTR1RFIEN5YmVyVHJ1c3QgUm9vdDCBnzANBjGkqhkiG9w0BAQEFAAOBjQ  
LXJldm9rZS5jZ2kwKQYJYIZIAy4QgEHAQEABBAkWF2NnaS1iaW4vY2hY2stcmVuZXcuY2  
dpMDcGCWCGSAGG+EIBDQEBAAQnFIVHVEUgQ3liZXJUCnVzdCBDZXJ0aWZpY2F0ZSBmb3Jl  
U1NMIENBMA0GCsGSIb3DQEBAUA4GBAK+p0RoOHMid+/CyXAPPctSqq/uhsQhWTODVdv  
0HA5b8LB7BcuwPfp0ijsxUUmIrOo9Fe4SrZtthYACiQOFm+qyDK/uYRyG2Mf0Yu0KKnn06  
- Ac0xk6CUiDjZzGC5MJiZHisbKJE7s/aF5V5k6HoeqCnpuWyc/v65J7ufjKAAvwHMMQA=  
-----END CERTIFICATE-----
```

35

Infraestructura de clave pública

- Algunas infraestructuras
 - Comerciales
 - Entrust - www.entrust.com
 - Baltimore - www.baltimore.com
 - SafeLayer - www.safelayer.com
 - Computer Associates www.ca.com
 - Libre distribución
 - OpenCA - www.openca.org