8636 Criptografía y Seguridad Informática

.UBAfiuba
FACULTAD DE INGENIERÍA

Infraestructura de Clave Pública PKI

Ing Hugo Pagola

Administración de claves publicas

(key management)

La administración de claves públicas asegura la autenticidad de las afirmaciones "esta clave pública me pertenece" mediante infraestructuras confiables, como las Autoridades Certificantes. Estas validan y certifican que una clave pública está vinculada a una entidad específica, evitando suplantación

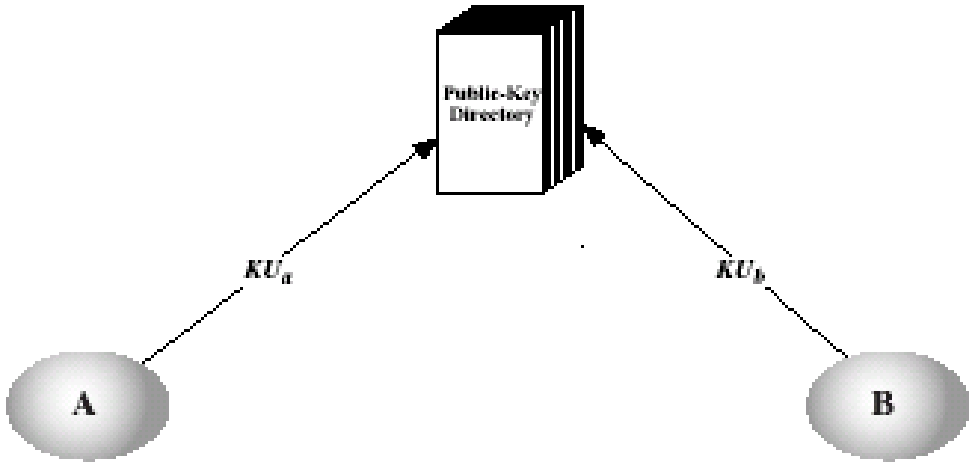
Anuncio publico

- Los usuarios distribuyen sus claves
  - ej. Incorporar las claves PGP al enviar claves PGP.
- Debilidad
  - Cualquiera puede enviar un email haciéndose pasar por otro

Directorio Publico

- Las claves se registran en un directorio publico
- Debe ser confiable y cumplir con:
  - Tener entradas {nombre, clave publica}
  - Los usuarios se deben registrar de forma segura
  - Los participantes deben poder hacer un ABM de sus entradas
  - Debe ser publico
  - Debe poder ser accedido electrónicamente
- NO ES ESCALABLE
- Único punto de falla

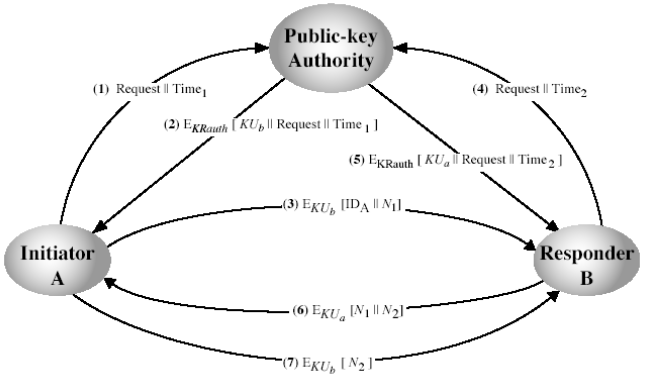
https://pgp.mit.edu/



Autoridad de claves publicas

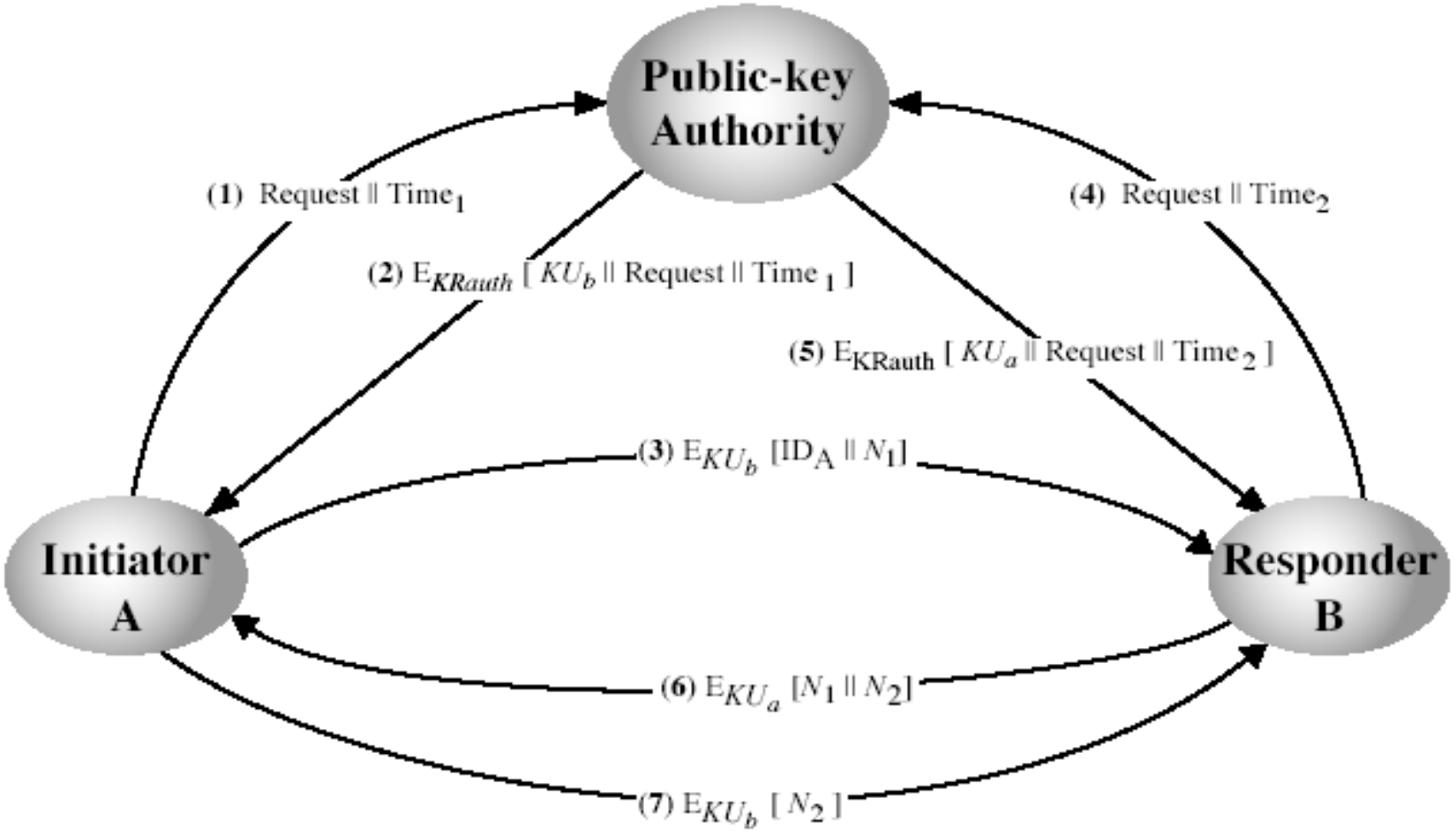
(Public-Key Authority)

- Mejora la seguridad validando las claves que retorna el directorio (mediante firma digital)
- Requiere que los usuarios conozcan la clave publica de la autoridad
- Los usuarios consultan con la autoridad para obtener la clave
  - Requiere acceso en línea con la autoridad

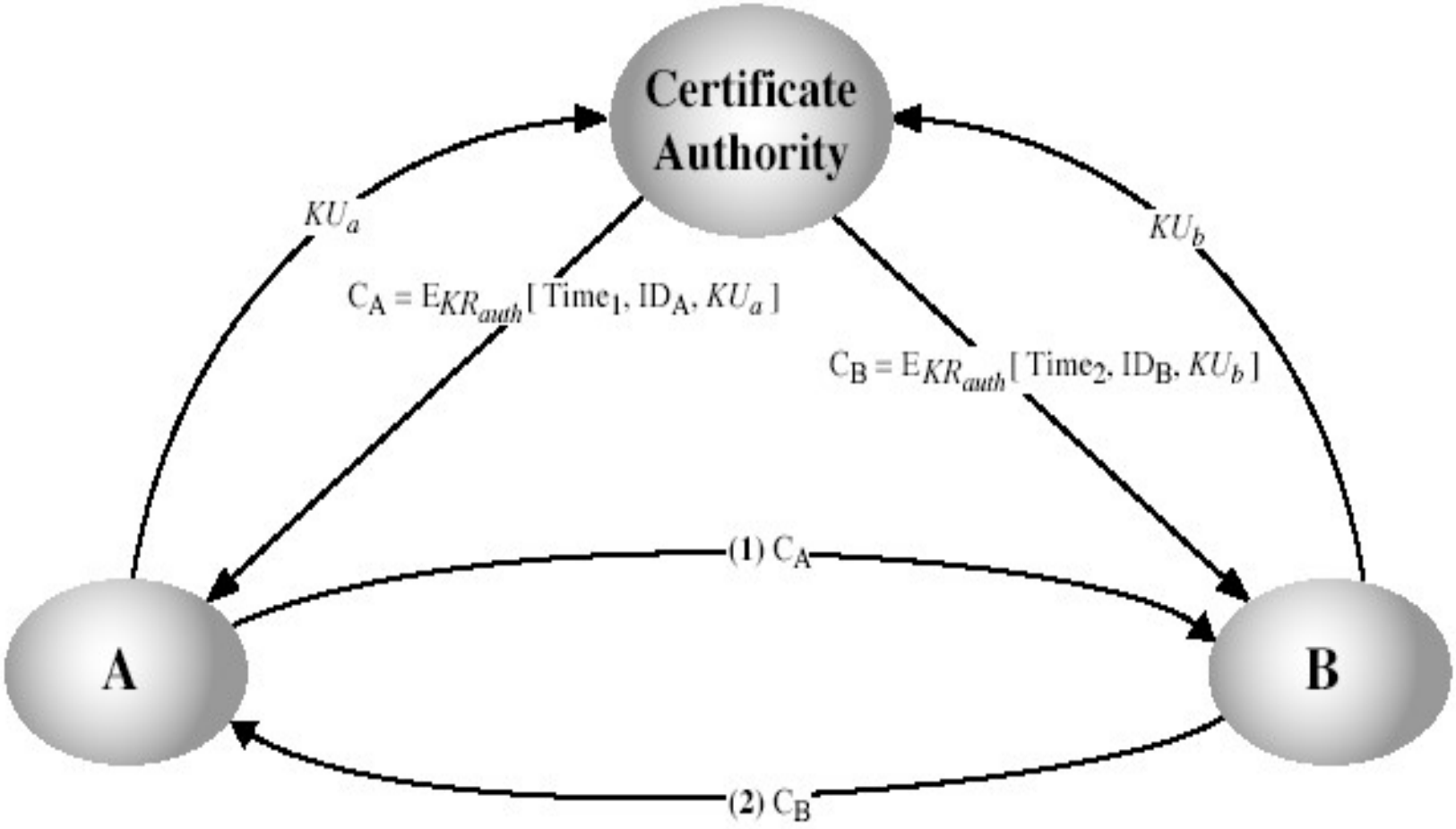


Autoridad de claves publicas

(Public-Key Authority)



Autoridad Certificante



Certificados: Autoridad Certificante

- Permiten el intercambio de claves sin el acceso en línea con la autoridad PKI

- Certificado

  - Es un archivo que contiene registros firmado por la autoridad certificante.
  - Contiene la identidad, Numero de serie, periodo de validez, derechos de uso, etc.
  - Puede ser verificado por cualquiera que conozca la clave publica de la autoridad

Infraestructura de clave publica PKI

Los componentes, roles y procesos fundamentales de una infraestructura de clave pública (PKI) son pilares esenciales para establecer y mantener la confianza en la seguridad cibernética.

PKI

Combinación de hardware y software, políticas y procedimientos

- Registrar, Validar Personas y entidades.
- Crear, manejar, guardar, distribuir y revocar Certificados Digitales.

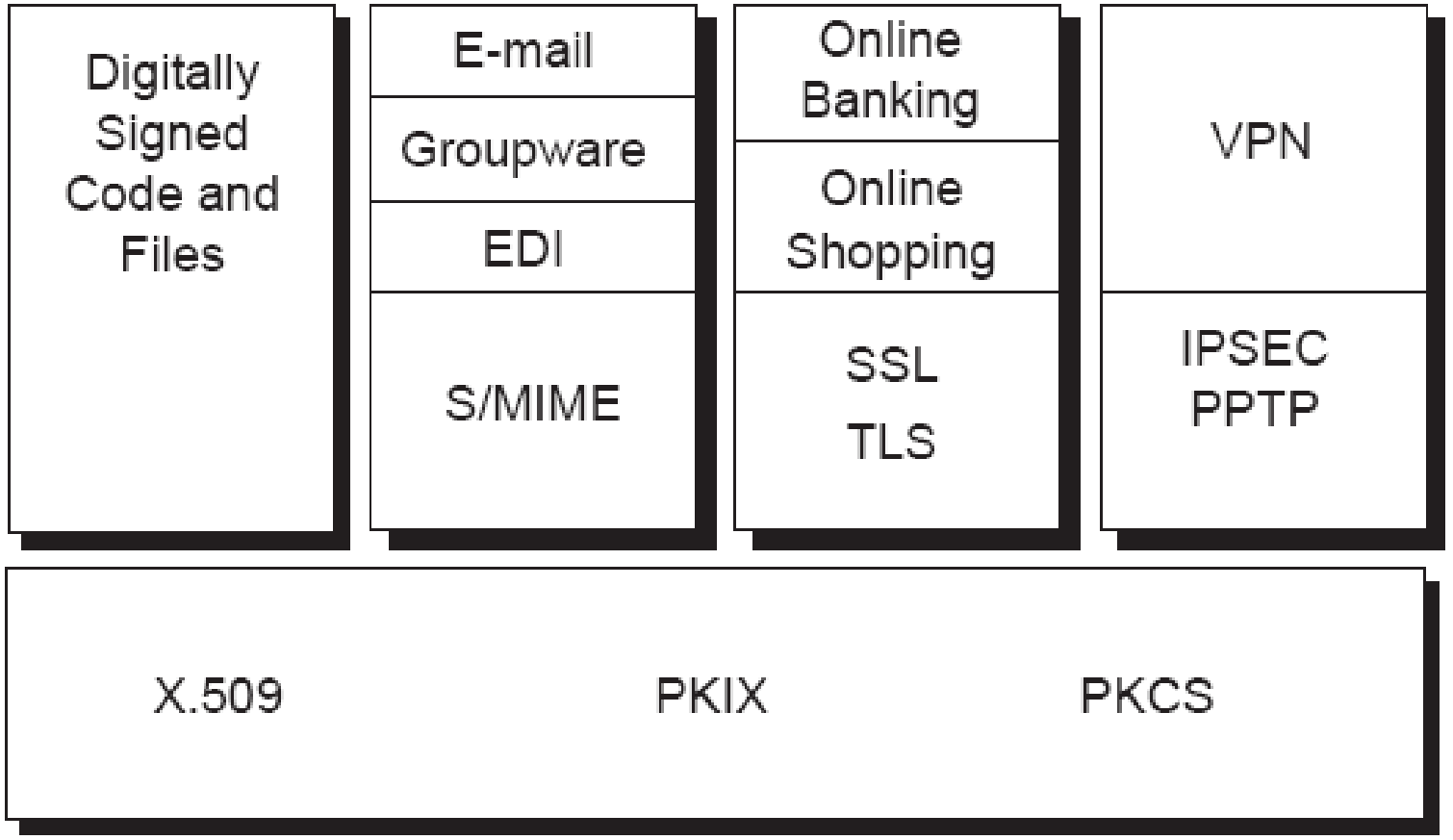
Asegurar la identidad de los participantes en un intercambio de datos usando criptografía de clave pública.

Usos de la tecnología PKI

La tecnología PKI se utiliza para:

- Autenticación de usuarios y sistemas
- Cifrado de datos
- Firma digital de documentos, codigo...
- Comunicaciones seguras (TLS, VPN) y
- Garantía de no repudio

PKI y Algunos estándares y aplicaciones



Servicio de Autenticación X.509

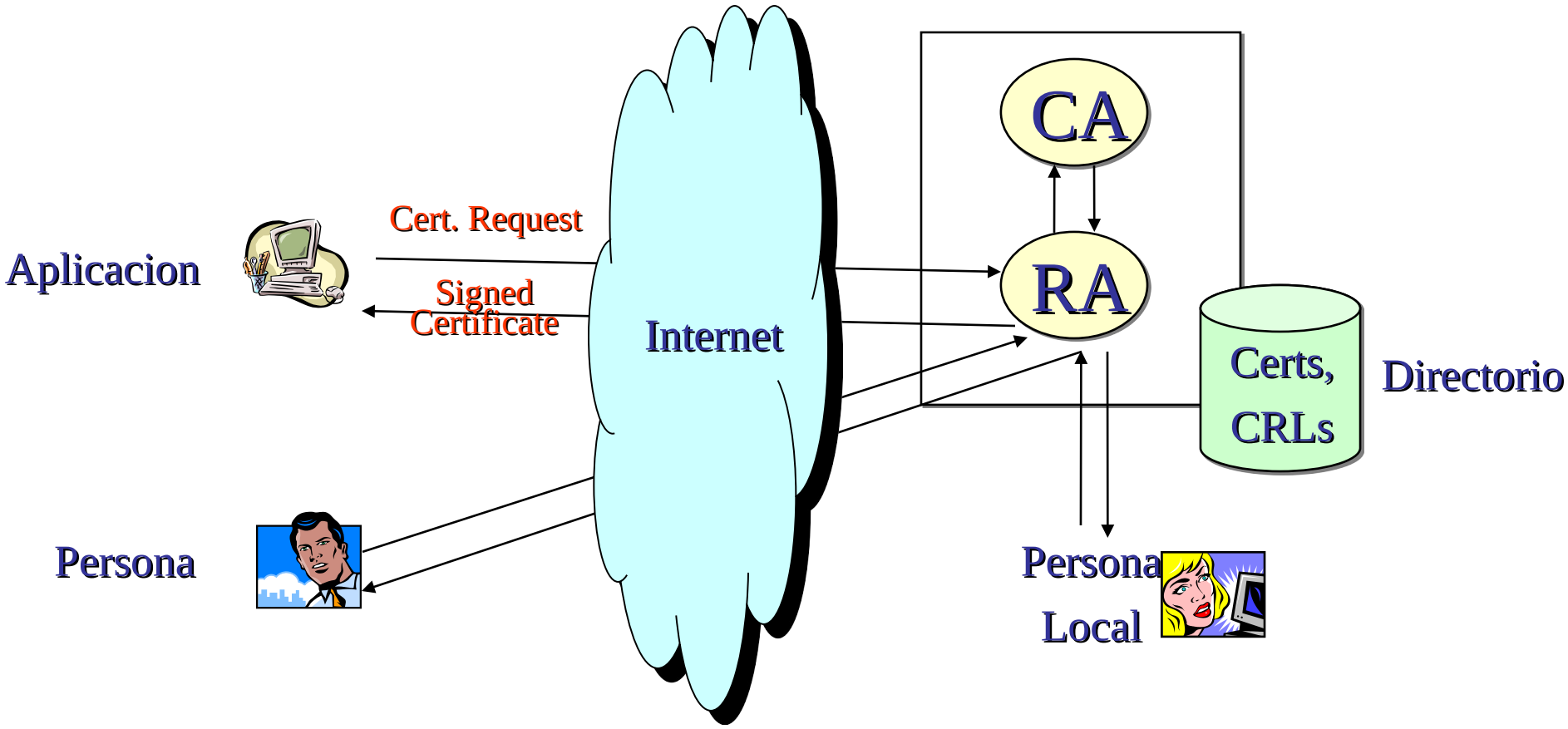
- **CCITT X.500**: Parte de la norma que define un marco para servicios de directorio y autenticación.
- **Servidores Distribuidos y Seguridad**: Incluye servidores distribuidos y una base de seguridad.
- **Claves Públicas**: El directorio contiene claves públicas de los usuarios firmadas por la autoridad certificante.
- **Protocolos de Autenticación**: Se definen protocolos para autenticación, algoritmo recomendando RSA y ECC.

PKIX (Public Key Infrastructure X.509)

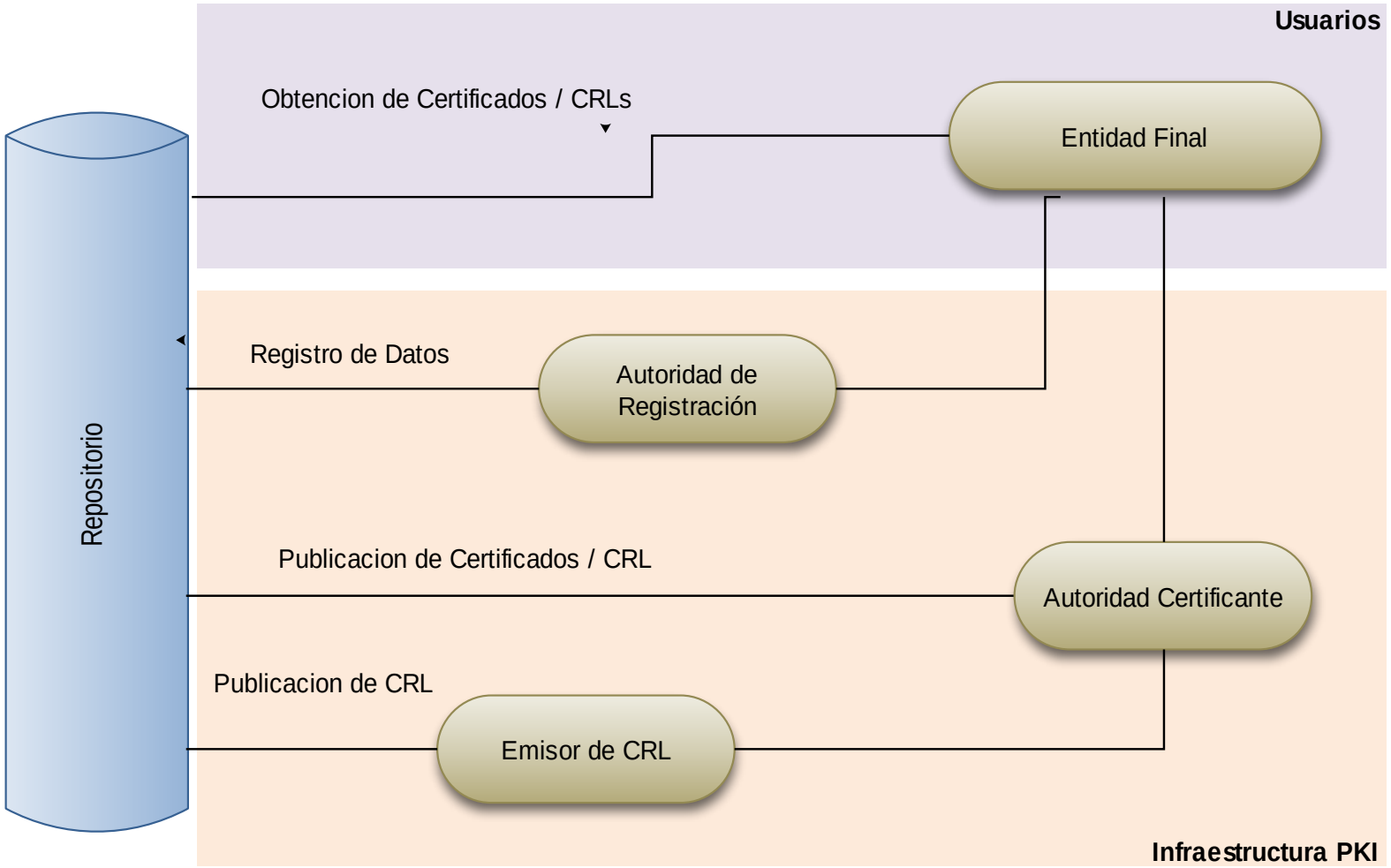
- **Infraestructura de Clave Pública (PKI)**: Basada en los certificados X.509.
- **Estándares PKIX (IETF)**: El grupo de trabajo PKIX del IETF ha desarrollado estos estándares clave:
  - RFC 4210: Protocolo de Gestión de Certificados (CMP).
  - RFC 3647: Marco de Políticas de Certificación y Prácticas.
  - RFC 5280: Perfil de Certificados y CRL.
  - RFC 6960: Perfil para Verificación del Estado de Certificados (OCSP).
  - RFC 3161: Protocolo de Sello de Tiempo.

http://datatracker.ietf.org/wg/pkix/charter/

Modelo Simple de un PKI



Arquitectura de PKIX



CA Autoridad Certificante

Las Autoridades Certificantes son entidades de confianza que emiten certificados digitales

Validan la autenticidad según políticas de certificación establecidas

CA Autoridad Certificante

emiten certificados y dan fe de la veracidad de la información incluida en los mismos

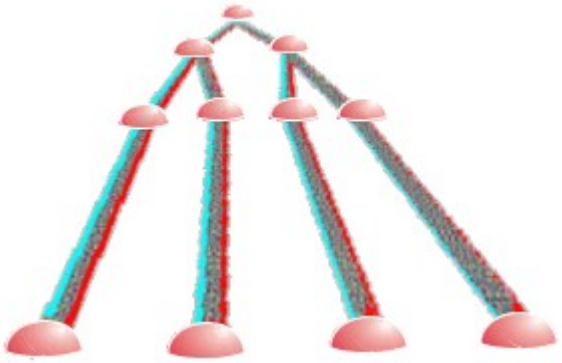
Emite certificados digitales según su política de certificación (CP = Certificate Policy).

- Reglas que indican la aplicabilidad de un certificado digital a una comunidad y/o a una clase de aplicaciones con requerimientos de seguridad en común.
- Incluyen la definición de un perfil de certificados.

CA Autoridad Certificante

Existen dos tipos de CAs en una jerarquía de certificación:

- **CA raíz (RootCA)**: La primera es la que emite certificados a otras CAs y la que cuyo certificado ha sido autofirmado.
- **CA subordinada (SubCA)**: Emite certificados de entidad final y cuyo certificado ha sido firmado digitalmente por la CA raíz.



- El certificado raiz es autofirmado
- Las sub-cas son certificadas por la raiz
- Cada CA tiene su CRL (lista de anulación)

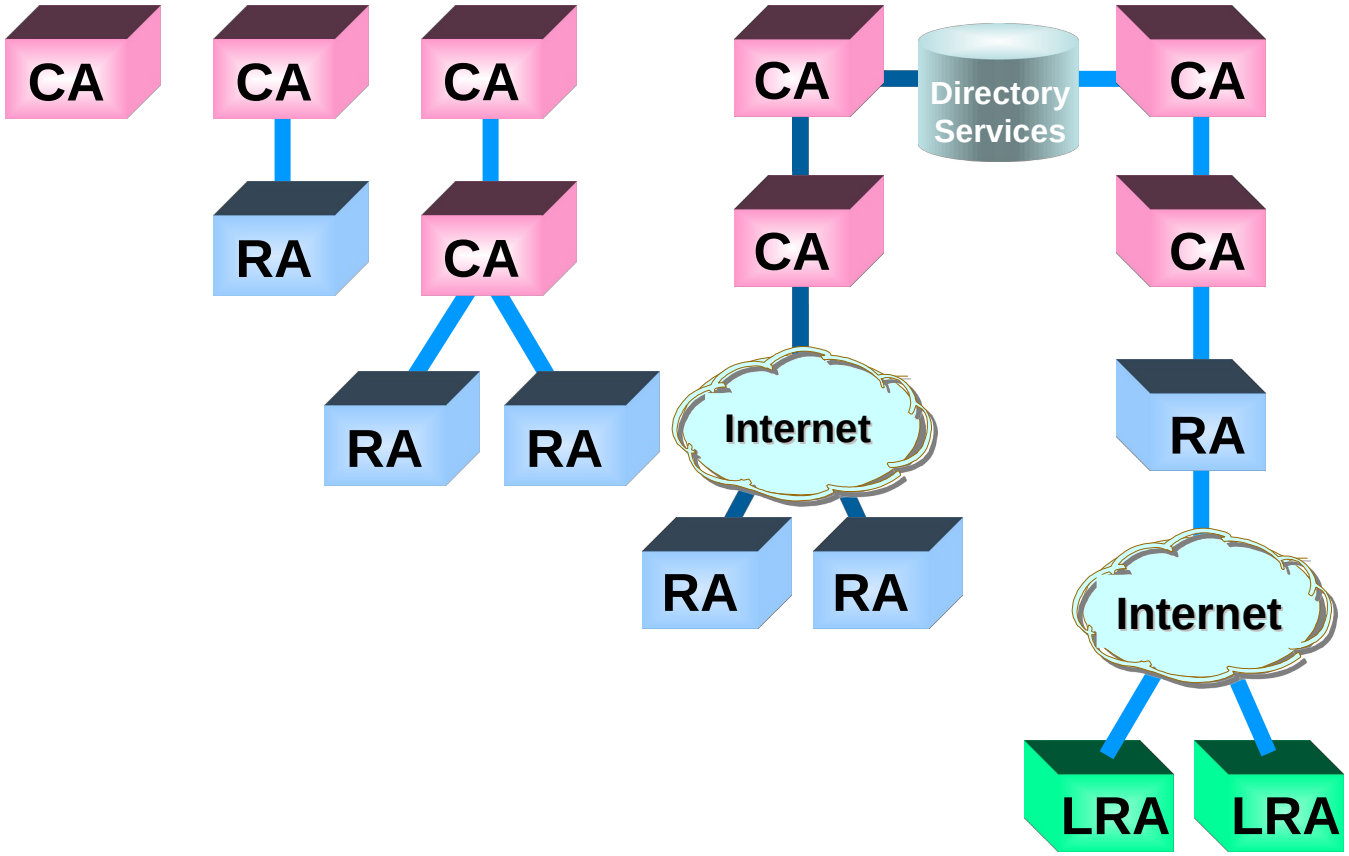
RA Autoridad de Registro

- **Autoridad de Registro (RA)**: Elemento opcional de PKIX para realizar tareas administrativas.

- **Tareas Principales:**
  - Registro de entidades finales.
  - Revocación de certificados.
  - Gestión de datos de la entidad final.

- **Jerarquía:** Puede haber una o más autoridades de registro, que pueden ser internas o externas a la jerarquía de certificación.

Cadenas de Certificación

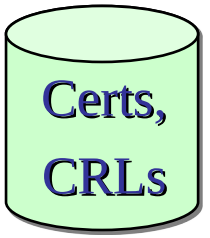


PKIX Términos

- **Entidad Final:**
  - Son los usuarios en una PKI (Infraestructura de Clave Pública).
  - Su identidad se muestra en el campo que indica al propietario del certificado X.509.
- **Emisor CRL:**
  - Cmponente opcional sobre el que se delega la emisión de Listas de Revocación de Certificados (CRLs).
  - A veces integrado como servicio en la CA.

PKIX Términos

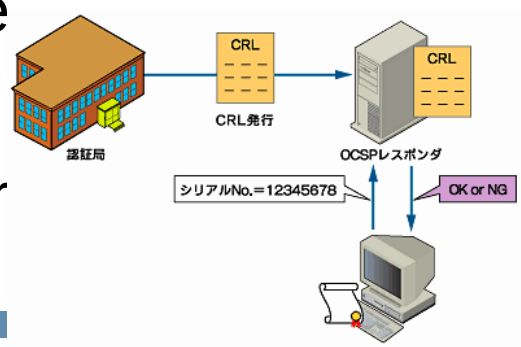
- **Repositorio**: almacena información de la PKI.
- **Incluye**:
  - **Almacén de Certificados emitidos**.
  - **Almacén de CRLs**: Listas de revocación.
  - **Método de Acceso**: Permite a las entidades finales obtener la información, normalmente a través de LDAP.
- **Típicamente utiliza:**
  - Directorio X.500, DAP o LDAP.



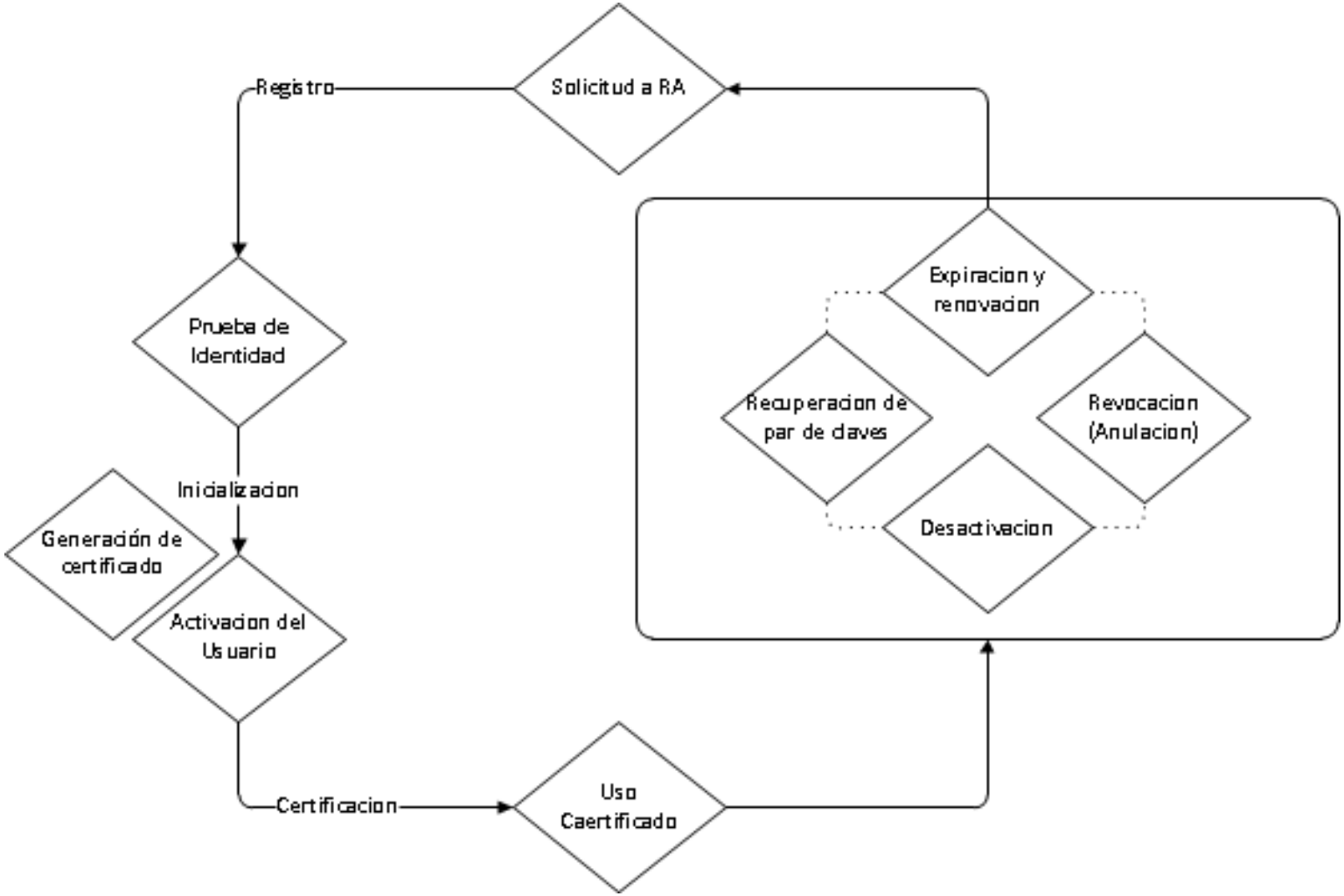
Directorio

PKIX Términos

- **Autoridad de Validación (VA):** Proporciona información sobre la validez de certificados digitales.
- **Funciones**:
  - Informa sobre los certificados anulados.
  - Usa el protocolo OCSP para la validación, aunque no está en la arquitectura PKIX.
  - A menudo, este servicio es ofrecido por la CA.
- **Recomendación**:
  - Se sugiere que la VA sea independiente
  - Separar la validación de la vigencia
  - De la información de identidad del titular



Principales procesos



PKIX funciones de gestión

- **Registro**:
  - Proceso en el que una entidad final registra sus datos en una CA o a través de una RA.

- **Inicialización**:
  - La entidad final se inicializa con su clave pública y la información de la CA en la que se registró.
  - Esta información se usará en la validación de certificados.

- **Certificación**:
  - La CA certifica que una clave pública pertenece a una entidad final, devolviendo el certificado al cliente o almacenándolo en un repositorio.

PKIX funciones de gestión

- **Pedido de Anulación (Revocación):** Una persona autorizada informa a la CA de un suceso anormal y solicita la revocación del certificado de una entidad final.

- **Razones comunes:**
  - Compromiso de la clave privada.
  - Cambio de nombre de la entidad.
  - Finalización del uso previsto.
  - Error en los datos del certificado.
  - No cumplir con las políticas de uso.

PKIX funciones de gestión

Recuperación del Par de Claves:

- Permite que las entidades finales recuperen sus claves a través de una entidad autorizada que las resguarda. Normalmente, es la CA que emitió el certificado.
- Sin embargo, si se pierde la clave de desencriptación, los datos cifrados no se pueden recuperar.

- **No se recomienda implementar: Esto podría exponer información sensible a quienes puedan acceder a la clave de desencriptación.**

http://pki.jgm.gov.ar/docs/Manual_de_Procedimientos_ACONTIv2.0.pdf

Prácticas y políticas de certificación

Las prácticas y políticas de certificación en el marco de la infraestructura de clave pública (PKI) son fundamentales para garantizar la seguridad y confianza en el mundo digital.

Obligación Prestadores de PKI

Los prestadores de servicios de certificación están obligados a:

- ***Efectuar una supervisión y gestión permanente*** de los certificados electrónicos que expiden
- ***Documentar los procedimientos y prácticas*** que desarrollen a fin de cumplir con esta gestión.
- Este documento ***debe estar disponible al público*** de manera fácilmente accesible.

RFC 3647 Certificate Policy and Certification Practices Framework

Política de Certificación

Declaración de las prácticas que emplea para emitir y gestionar certificados

- Existe una política por cada tipo de certificado emitido

- Servidor Seguro TLS
- Firma de Código
- Persona Vinculada

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

Política de Certificación

Ejemplo de PC de Persona Vinculada

- **Objetivo**: Establecer reglas de emisión y uso de certificados.
- **Verificación de la Identidad**: Verificada: Identidad de empleado verificada a través de documentos de identificación oficiales.
- **Vigencia del Certificado**: 1 año.
- **Uso Permitido**: Autenticación de empleados en la red interna y firma de documentos.

Declaración Prácticas de Certificación

En este documento se especifican:

- **Condiciones aplicables**: Solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos.
- **Obligaciones del prestador**: Gestión de los datos de creación de firma y de certificados electrónicos.
- **Medidas de seguridad** técnicas y organizativas de la empresa,
- **Perfiles**: Los tipos de perfiles que existen
- **Servicios de validación de certificados disponibles**. (OCSP / CRL)

Declaración Prácticas de Certificación

- **Objetivo**: Detalles técnicos y procedimientos para implementar la CP.
- **Proceso de Solicitud**: Empleados deben completar un formulario de solicitud, que se verifica por el Departamento de Recursos Humanos.
- **Generación de Claves**: RSA de 2048 bits para firmar y cifrar.
- **Revocación de Certificados**: Se revocan si el empleado se retira o en caso de compromiso.

Prácticas y Políticas de Certificación

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 Prácticas y políticas de custodia y recuperación de claves

La tarjeta soporte del DNI es un dispositivo cualificado de creación de firma electrónica certificado EAL4+ aumentado con AVA_VAN.5. Los datos de creación de firma (las claves privadas) se generan dentro de la tarjeta y no pueden ser exportadas en ningún caso.

No se efectúa por tanto archivo de la clave privada de los certificados. ok

Por otro lado, en el ámbito del certificado de firma centralizada, la clave privada que se genera quedará custodiada por la DGP, teniendo en cuenta que el acceso a esta clave será realizado por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del ciudadano. ???

En este sentido, el acceso a dicha clave sólo puede ser efectuado por el titular de la misma mediante Cl@ve permanente siendo necesario introducir un código de usuario (DNI/NIE), una contraseña tan sólo conocida por el ciudadano, y no almacenada en los sistemas de DGP, y un segundo factor de autenticación.

https://www.dnielectronico.es/PDFs/Politicas_de_certificacion_v2.11.pdf (2022)

En línea con la mención anterior, en el apartado cuarto del anexo II del Reglamento (UE) 910/2014 se establece que, sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma

únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

5.11 Depósito y recuperación de claves

5.11.1 Política y prácticas de depósito y recuperación de claves

ASI-GCABA no presta servicios de depósito y recuperación de claves.

5.11.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

https://pki-gcba.buenosaires.gob.ar/assets/PKI-PO-005-Politica-DPC-V1.2.pdf (2022)

Certificados Digitales

Los certificados digitales, respaldados por autoridades de confianza, son elementos esenciales de la infraestructura PKI, permitiendo comunicaciones seguras.

- **Datos de Identidad**: Contiene el nombre y la clave pública de un usuario, firmada por la Autoridad Certificante (AC).
- **Confianza**: Tanto el emisor como el receptor deben confiar en la AC.
- **Autenticación**: El usuario se autentica mostrando su certificado.

https://www.ietf.org/proceedings/64/pkix.html

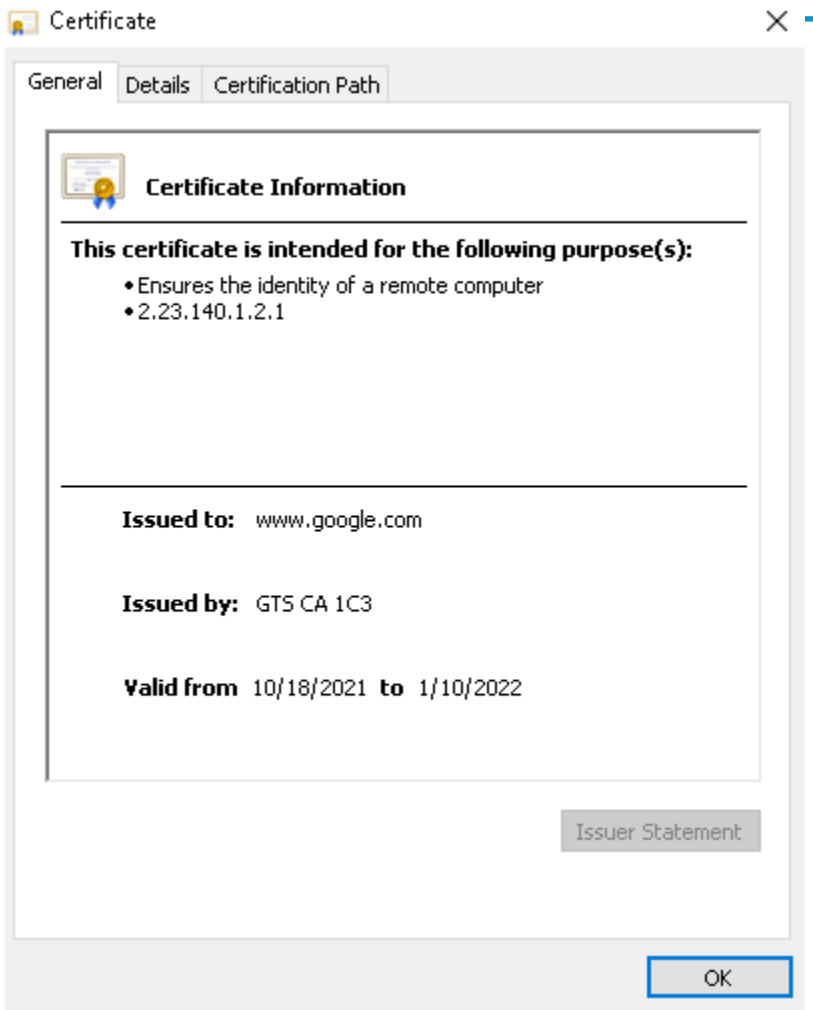
Certificados X.509

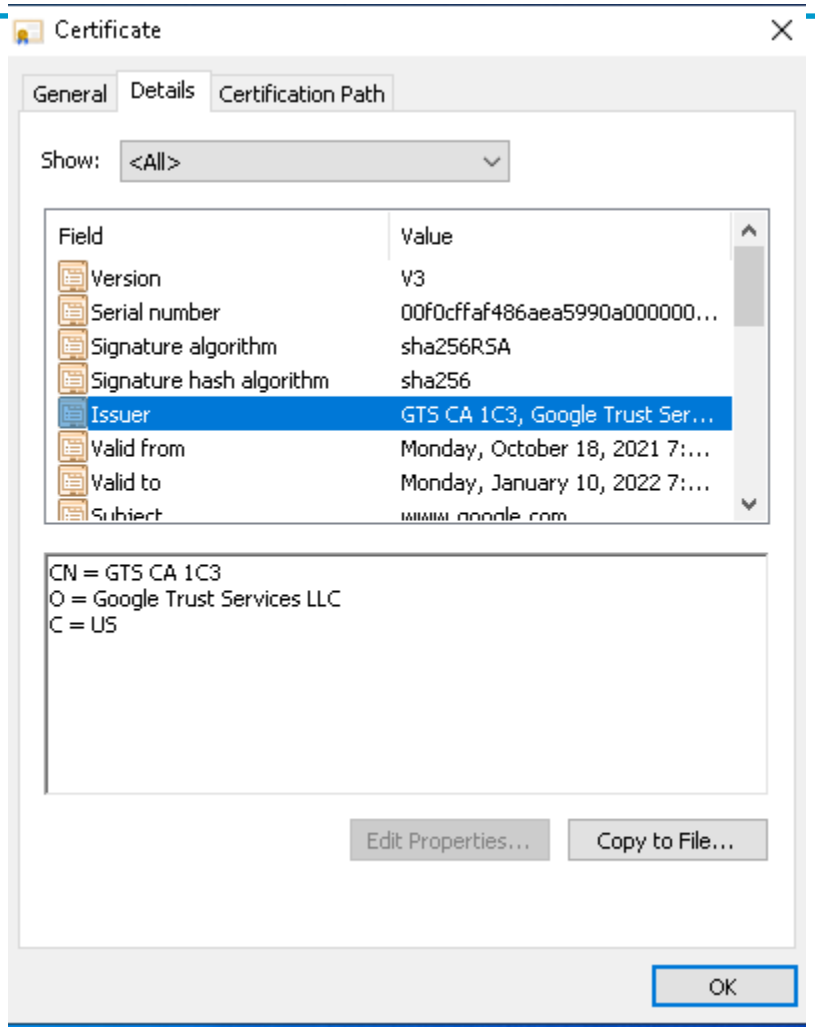
Incluye:

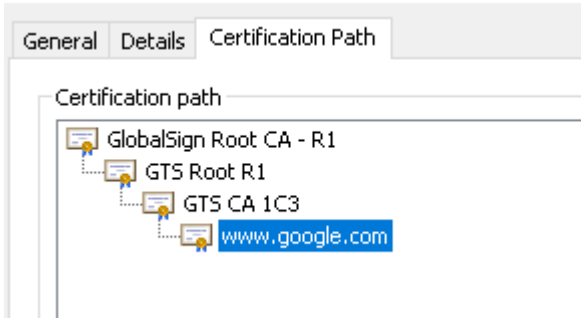
- versión (1, 2, or 3)
- Numero de Serie para identificar el Certificado (Unico en el CA)
- Identificación del Algoritmo de Firma
- Nombre X.500 de la CA
- Periodo de validez del certificado
  - (Desde - Hasta)
- Identificación X500 del Dueño del certificado.(subject X.500 name)
- Información de la clave publica (algoritmo, parámetros, clave)
- issuer unique identifier (v2+)
- subject unique identifier (v2+)
- extension fields (v3)
- Firma del Hash de todos los parametros

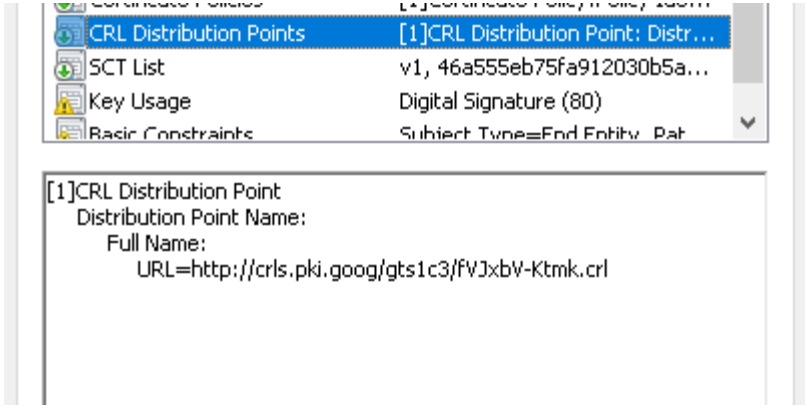
Version	
Numero de Serie	
Identificador del Algoritmo	Algoritmo
	Parametros
dn del Emisor	
Periodo de Validez	Desde
	Hasta
dn del Dueño (subject)	
Informacion de la clave publica	Algoritmo
	Parametros
	Clave
Identificador unico del emisor	
Identificador unico del subject	
Extensiones	
FIRMA	algoritmo
	Parametros

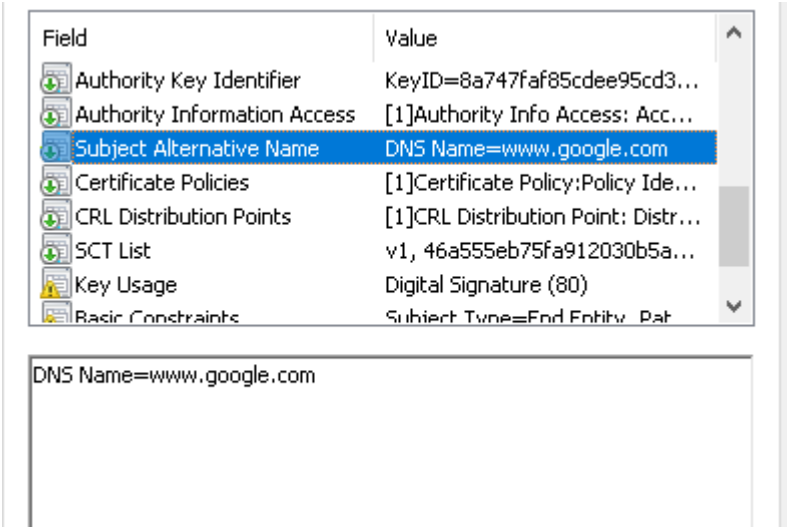
•La notación CA<<A>> indica que el certificado de A esta expedido o firmado por CA


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer
•2.23.140.1.2.1
Issued to: www.google.com
Issued by: GTS CA 1C3
Valid from 10/18/2021 to 1/10/2022
Issuer Statement
OK


Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
00f0cffaf486aea5990a000000...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
GTS CA 1C3, Google Trust Ser...
Valid from
Monday, October 18, 2021 7:...
Valid to
Monday, January 10, 2022 7:...
Subject
www.google.com
CN = GTS CA 1C3
O = Google Trust Services LLC
C = US
Edit Properties...
Copy to File...
OK


General
Details
Certification Path
Certification path
GlobalSign Root CA - R1
GTS Root R1
GTS CA 1C3
www.google.com


CRL Distribution Points
[1]CRL Distribution Point: Distr...
SCT List
v1, 46a555eb75fa912030b5a...
Key Usage
Digital Signature (80)
[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.crl


Field
Value
Authority Key Identifier
KeyID=8a747faf85cdee95cd3...
Authority Information Access
[1]Authority Info Access: Acc...
Subject Alternative Name
DNS Name=www.google.com
Certificate Policies
[1]Certificate Policy:Policy Ide...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
SCT List
v1, 46a555eb75fa912030b5a...
Key Usage
Digital Signature (80)
DNS Name=www.google.com

Certificado X.509 v3: extensiones

Extensiones más comunes:

SubjectAltName: Nombre alternativo del titular (web o e-mail del titular)

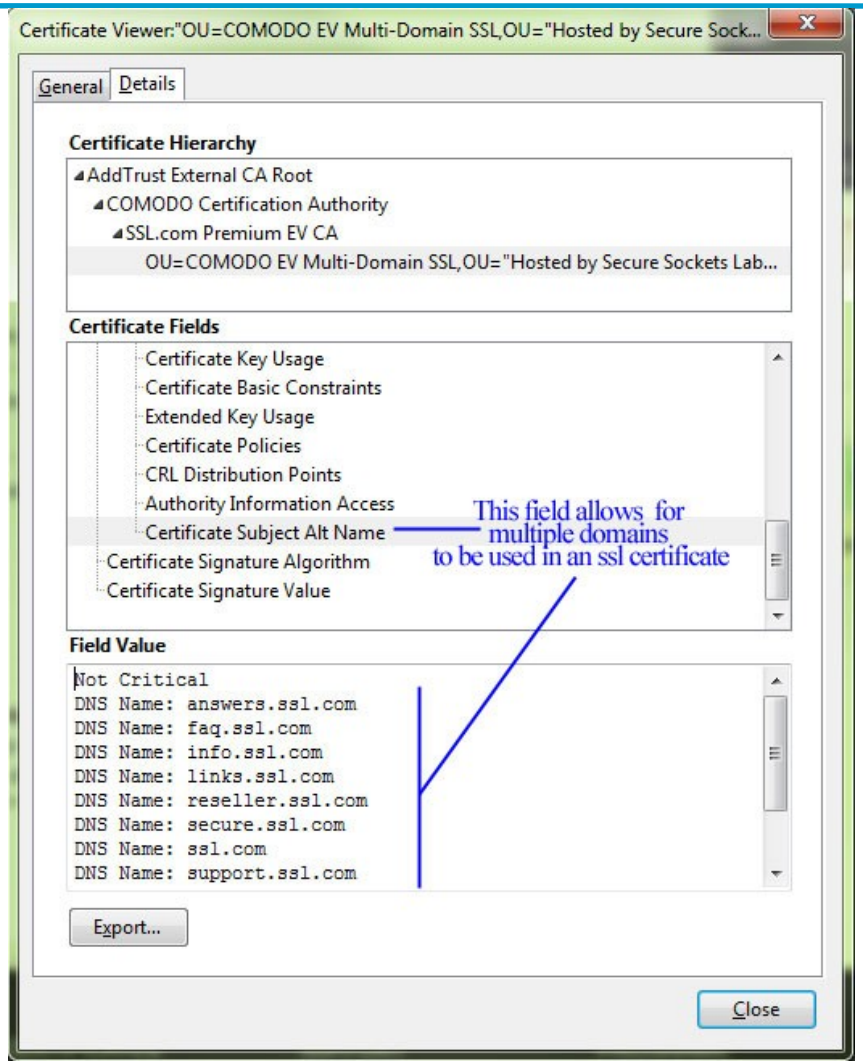
keyUsage (crítico): Indica el uso que se debe hacer de ese certificado, por ejemplo si es para firmar, cifrar, firmar CRL's, etc...

ExtendedKeyUsage (crítico): Similar al anterior.

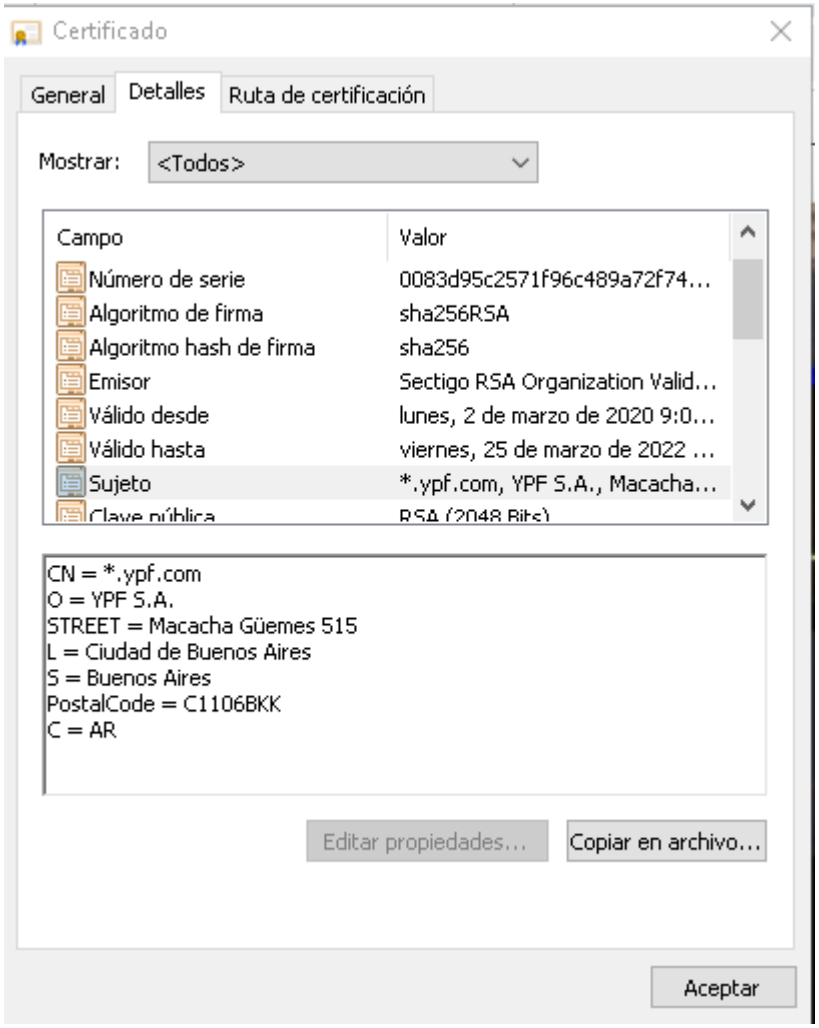
crlDistributionPoints (crítico): Identifica los puntos donde se podrá acceder a las CRL's para comprobar si el certificado ha sido revocado.

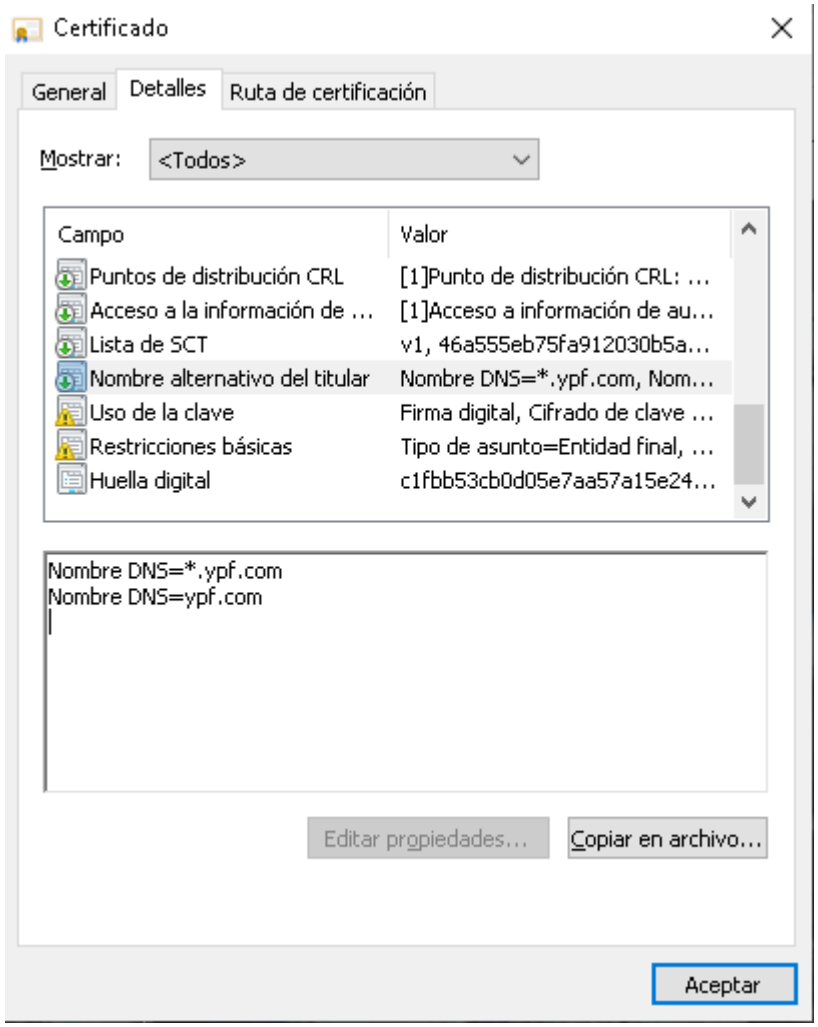
basicContraints (crítico): Indica si el certificado proviene de una CA o no. En caso afirmativo, indica si es raiz o no.

SubjectAltName



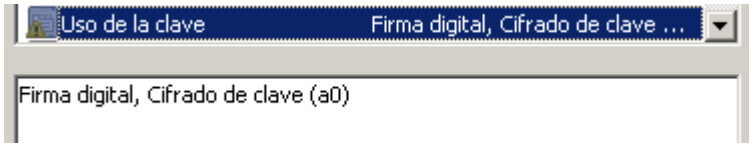
wildcard


Certificado
General
Detalles
Ruta de certificación
Mostrar:
<Todos>
Campo
Valor
Número de serie
0083d95c2571f96c489a72f74...
Algoritmo de firma
sha256RSA
Algoritmo hash de firma
sha256
Emisor
Sectigo RSA Organization Valid...
Válido desde
lunes, 2 de marzo de 2020 9:0...
Válido hasta
viernes, 25 de marzo de 2022 ...
Sujeto
*.ypf.com, YPF S.A., Macacha...
Clave pública
RSA (2048 Bits)
CN = *.ypf.com
O = YPF S.A.
STREET = Macacha Güemes 515
L = Ciudad de Buenos Aires
S = Buenos Aires
PostalCode = C1106BKK
C = AR
Editar propiedades...
Copiar en archivo...
Aceptar


Certificado
General
Detalles
Ruta de certificación
Mostrar:
<Todos>
Campo
Valor
Puntos de distribución CRL
[1]Punto de distribución CRL: ...
Acceso a la información de ...
[1]Acceso a información de au...
Lista de SCT
v1, 46a555eb75fa912030b5a...
Nombre alternativo del titular
Nombre DNS=*.ypf.com, Nom...
Uso de la clave
Firma digital, Cifrado de clave ...
Restricciones básicas
Tipo de asunto=Entidad final, ...
Huella digital
c1fbb53cb0d05e7aa57a15e24...
Nombre DNS=*.ypf.com
Nombre DNS=ypf.com
Editar propiedades...
Copiar en archivo...
Aceptar

KeyUsage ::=BIT STRING

{ digitalSignature (0),
nonRepudiation (1),
keyEncipherment (2),
dataEncipherment (3),
keyAgreement (4),
keyCertSign (5),
cRLSign (6),
encipherOnly (7),
decipherOnly (8)
}



- **digitalSignature** se usara para firma digital en autenticación de partes o autenticación de origen.
- **nonRepudiation** se usara para garantizar el no repudio. Una tercera parte confiable debera mediar.
- **keyEncipherment** Se usara para cifrado de claves
- **dataEncipherment** Se usara para cifrado de datos
- **keyAgreement**: El certificado sera usado para un algoritmo de intercambio de claves. Ej Diffie-Hellman
- **keyCertSign** se usara para verificar claves publicas (CA)

- **id-kp-serverAuth:** Autenticación Server TLS
  - *Keyusage: digitalSignature, keyEncipherment o keyAgreement*
- **id-kp-clientAuth:** Autenticacion cliente TLS
  - *Keyusage: digitalSignature, keyEncipherment o keyAgreement*
- **id-kp-codeSigning:** Firma de codigo ejecutable.
  - *Keyusage: digitalSignature*
- **id-kp-emailProtection** Proteccion E-mail
  - *Keyusag: digitalSignature, nonRepudiation, y/o (keyEncipherment o keyAgreement)*
- **id-kp-timeStamping:** Fechado de un Hash
  - *KeyUsage: digitalSignature y/o nonRepudiation*
- **id-kp-OCSPSigning** -- Firma de respuestas OCSP
  - *KeyUsage: digitalSignature y/o nonRepudiation*

Extensiones de archivo de certificados

.CER	Certificado codificado en CER, algunas veces es una secuencia de certificados
.DER	Certificado codificado en DER
.PEM	Certificado codificado en Base64 encerrado entre "-----BEGIN CERTIFICATE-----“ y "-----END CERTIFICATE-----"
.P7B .P7C	Estructura PKCS#7 SignedData sin datos, solo certificado(s) o CRL(s) Usado para Firmar y/o cifrar mensajes.
.P12 .PFX	PKCS#12, puede contener certificados y claves privadas (protegido con clave)

http://www.rsa.com/rsalabs/node.asp?id=2124

Certificados de la Autoridad de Certificación

- **Certificado CA RAIZ**: El emisor de una CA es el mismo que el receptor, campos Issuer y Subject respectivamente, se dice que que el certificado es auto-firmado.

- **Certificado CS Subordinada**: Su certificado firmado por una CA de nivel superior.

- Solicitud del Cliente:
  - El cliente genera un par de claves (pública y privada) y envía una solicitud a la CA usando **PKCS #10.**
  - La CA valida y responde con un certificado, utilizando **PKCS #6.**
- Solicitud a través de la CA:
  - El cliente solicita un certificado a la CA, que genera el par de claves.
  - La CA envía al cliente un archivo protegido con una contraseña mediante **PKCS #12** para asegurar la clave privada.

PKCS#10. Entorno de uso

Petición de Certificado PKCS#10

CA

Certificado PKCS#6

Certificado X.509

.UBAfiuba
FACULTAD DE INGENIERÍA

Laboratorio PKI

En este laboratorio PKI, exploraremos la creación de una autoridad certificante con XCA y configuraremos un servidor web Apache para habilitar un sitio web seguro.

Laboratorio PKI

- Utilizar la PKI XCA para armar una autoridad certificante
- Obtener el certificado de un servidor web apache
- Iniciar en el apache un sitio protegido.
- Por favor respetar los nombres de los campos ya que la CA se usara en el lab de TLS

Otros PKCS

Pkcs12 contenedor criptográfico

PKCS7 para firma digital y sobre electrónico.

PKCS#12. Entorno de uso

Petición de Claves

CA

PKCS#12

Certificado X.509

PKCS#12. Introducción

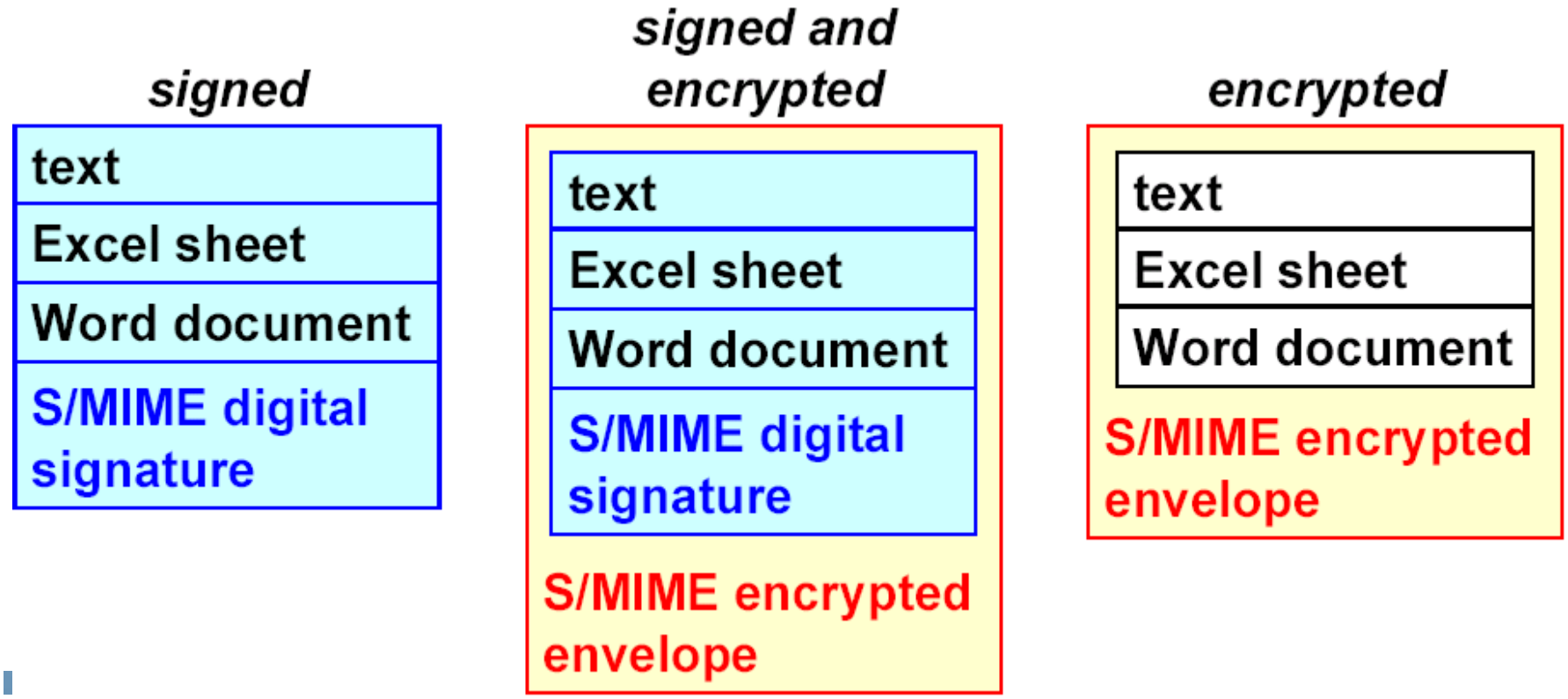
- Describe una sintaxis de transferencia de información personal:
  - Claves privadas
  - Certificados
  - Cualquier tipo de información secreta
  - Extensiones
- Las máquinas,aplicaciones y navegadores que soportan esta norma permiten importar, exportar y emplear un conjunto de información con un identificador personal.
- Soporte de la información personal que se transfiere.

PKCS #7: Contenedores de datos

- **PKCS #7:** Contenedores de datos no estructurados.
- Usos:
  - Datos firmados no incluidos. (No contiene los datos que firma)
  - Datos firmados incluidos.
  - Datos cifrados.
  - Datos cifrados y firmados.
  - Cadenas de certificación.
  - Certificados individuales. (por ejemplo que responden a una petición de certificación).

S/MIME

- Basado en PKCS#7
- Definido inicialmente para proteger e-mail



S/MIME : Ejemplo


```
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=sha1;
boundary="-----aaaaa"
-----aaaaa
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
Hello!
-----aaaaa
Content-Type: application/x-pkcs7-signature
Content-Transfer-Encoding: base64
MIIN2QasDDSdwe/625dBxgdhdsf76rHfrJe65a4f
fvVSW2Q1eD+SfDs543Sdwe6+25dBxfdER0eDsrs5
-----aaaaa
```

Anulación de Certificados

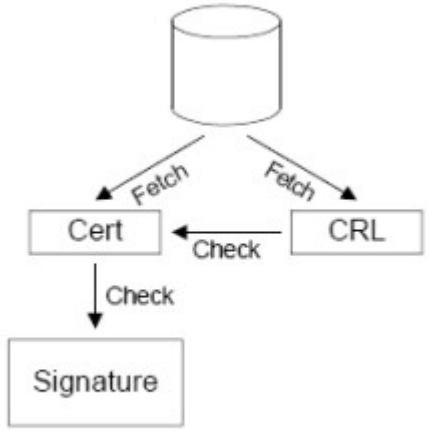
La anulación de certificados en la PKI es esencial para asegurar que las partes confíen en la actualidad y validez de los certificados digitales

Anulación de Certificados

- Tienen un periodo de Validez
- Se puede necesitar anular, Ej:
  1. Clave privada comprometida
  2. El usuario no sera mas certificado por la CA
  3. La CA esta comprometida
- La CA Mantiene una lista de certificados Anulados
  - Certificate Revocation List (CRL)
  - OCSP
- Los sistemas deben verificar la CRL

CRL

- Constituyen un medio para verificar el estado de validez de un certificado digital.
- Las AC están obligadas a publicar permanentemente la CRL, que tiene un período de validez.
- Lista firmada de números de serie certificados revocados.



CRL

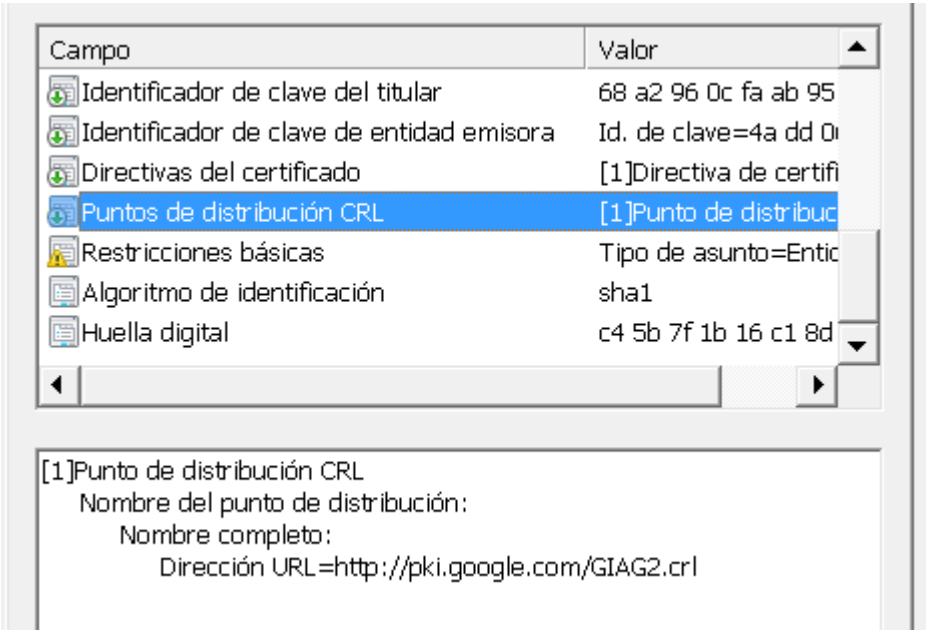
- Cuando un tercero desea comprobar la validez de un certificado debe:
  - Descargar una CRL actualizada desde los servidores de la misma autoridad de certificación que emitió el certificado en cuestión.
  - A continuación comprueba la autenticidad de la lista gracias a la firma digital de la autoridad de certificación.
  - Después debe comprobar que el número de serie del certificado cuestionado está en la lista. En caso afirmativo, no se debe aceptar el certificado como válido.

Validar un certificado con CRL

Cuando un tercero desea comprobar la validez de un certificado debe:

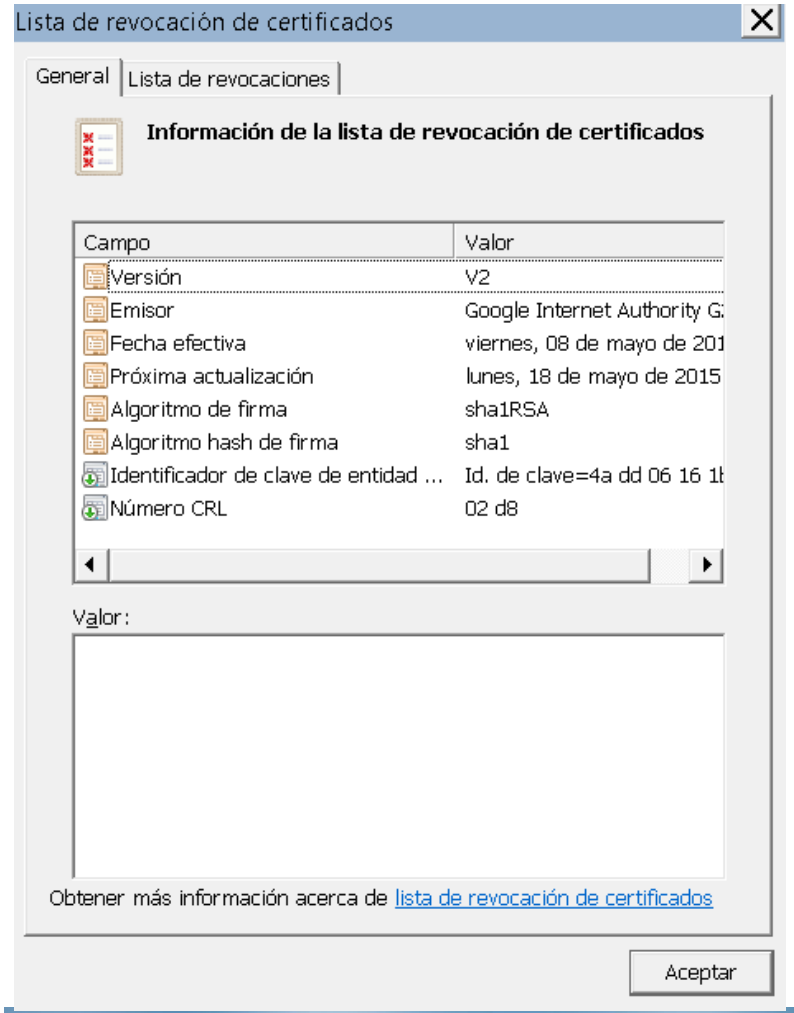
- Descargar la CRL actualizada desde la CA del certificado.
- Comprobar la firmade la lista.
- Comprobar si el número de serie del certificado cuestionado está en la lista.

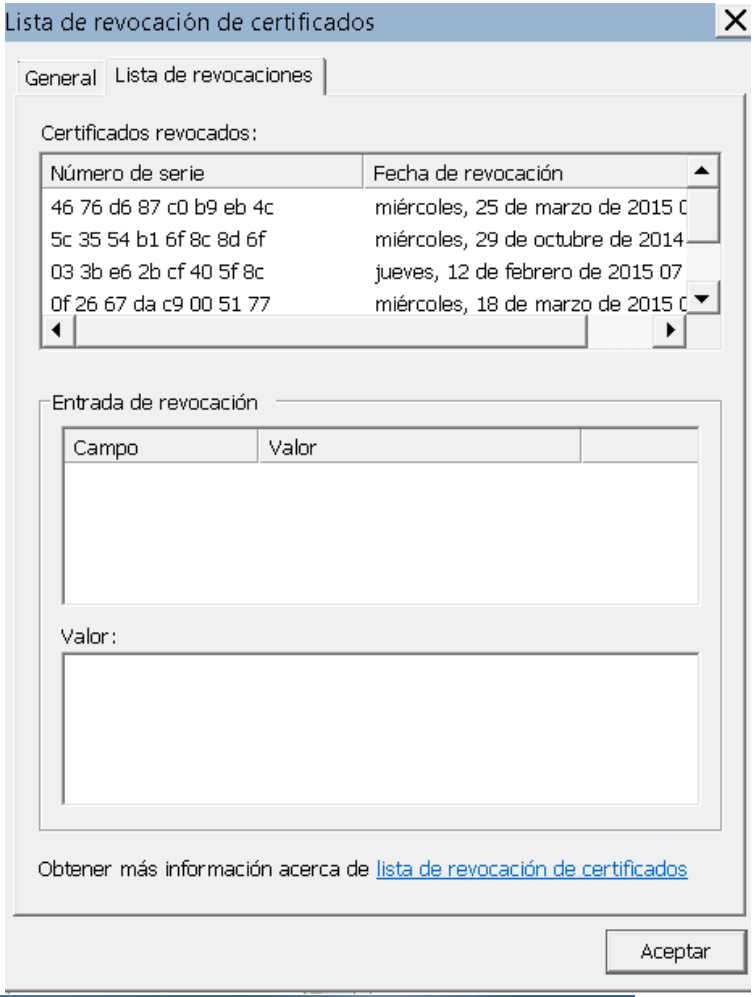
CRL


Campo
Valor
Identificador de clave del titular
68 a2 96 0c fa ab 95
Identificador de clave de entidad emisora
Id. de clave=4a dd 0
Directivas del certificado
[1]Directiva de certifi
Puntos de distribución CRL
[1]Punto de distribuc
Restricciones básicas
Tipo de asunto=Entic
Algoritmo de identificación
sha1
Huella digital
c4 5b 7f 1b 16 c1 8d
[1]Punto de distribución CRL
Nombre del punto de distribución:
Nombre completo:
Dirección URL=http://pki.google.com/GIAG2.crl

Ejemplo CRL

http://pki.google.com/GIAG2.crl

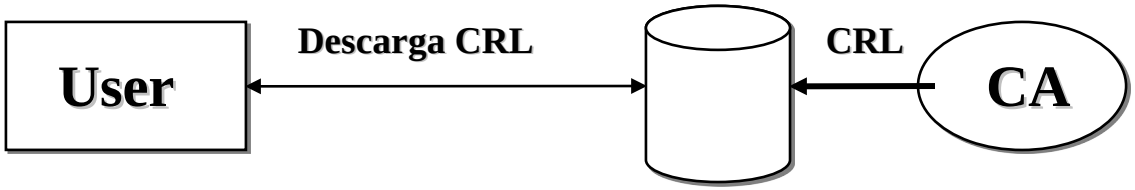




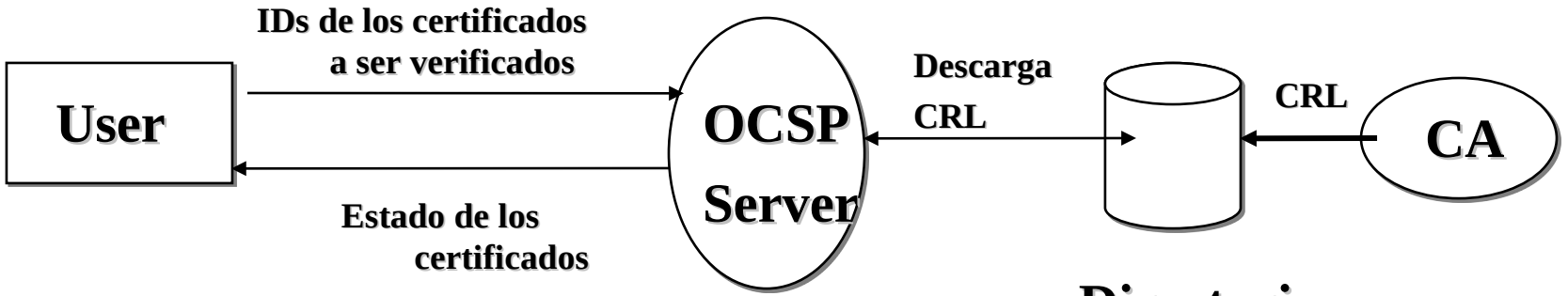
Online Certificate Status Protocol

- Alternativa a los CRL
- Servicio definido por IETF/PKIX para verificar si un certificado fue anulado o suspendido.
- Requiere Alta Disponibilidad del Servicio OCSP
- Hay tres estados posibles: “good”, “revoked” y “unknown”.

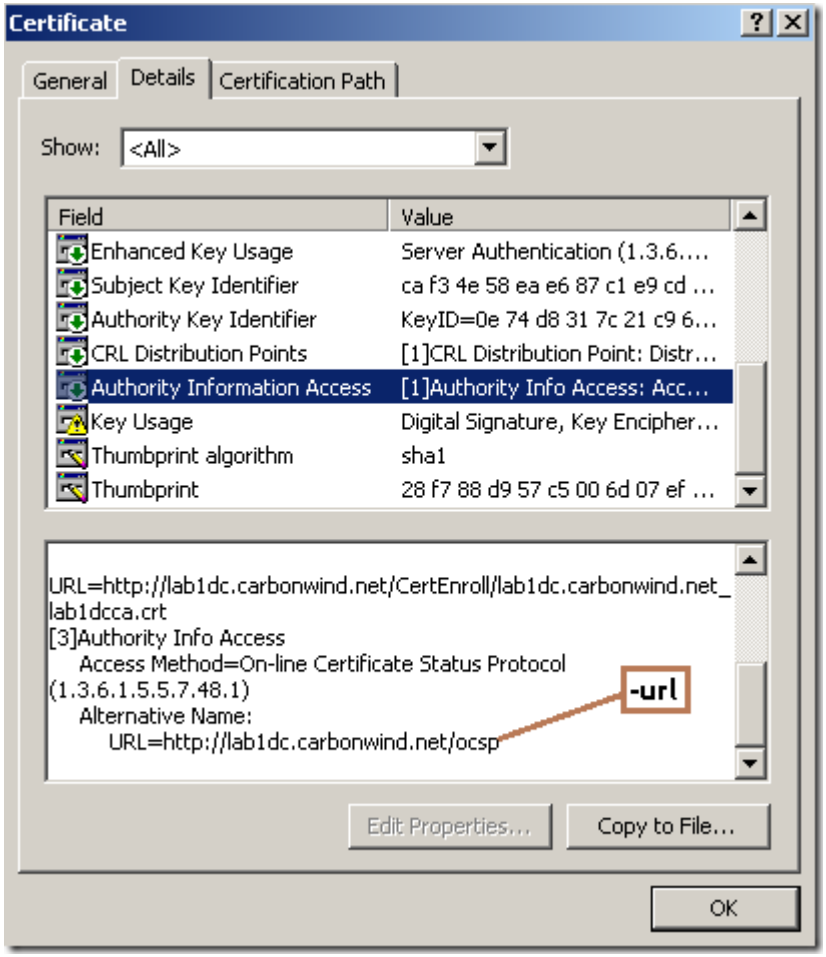
Comparación de CRL y OCSP



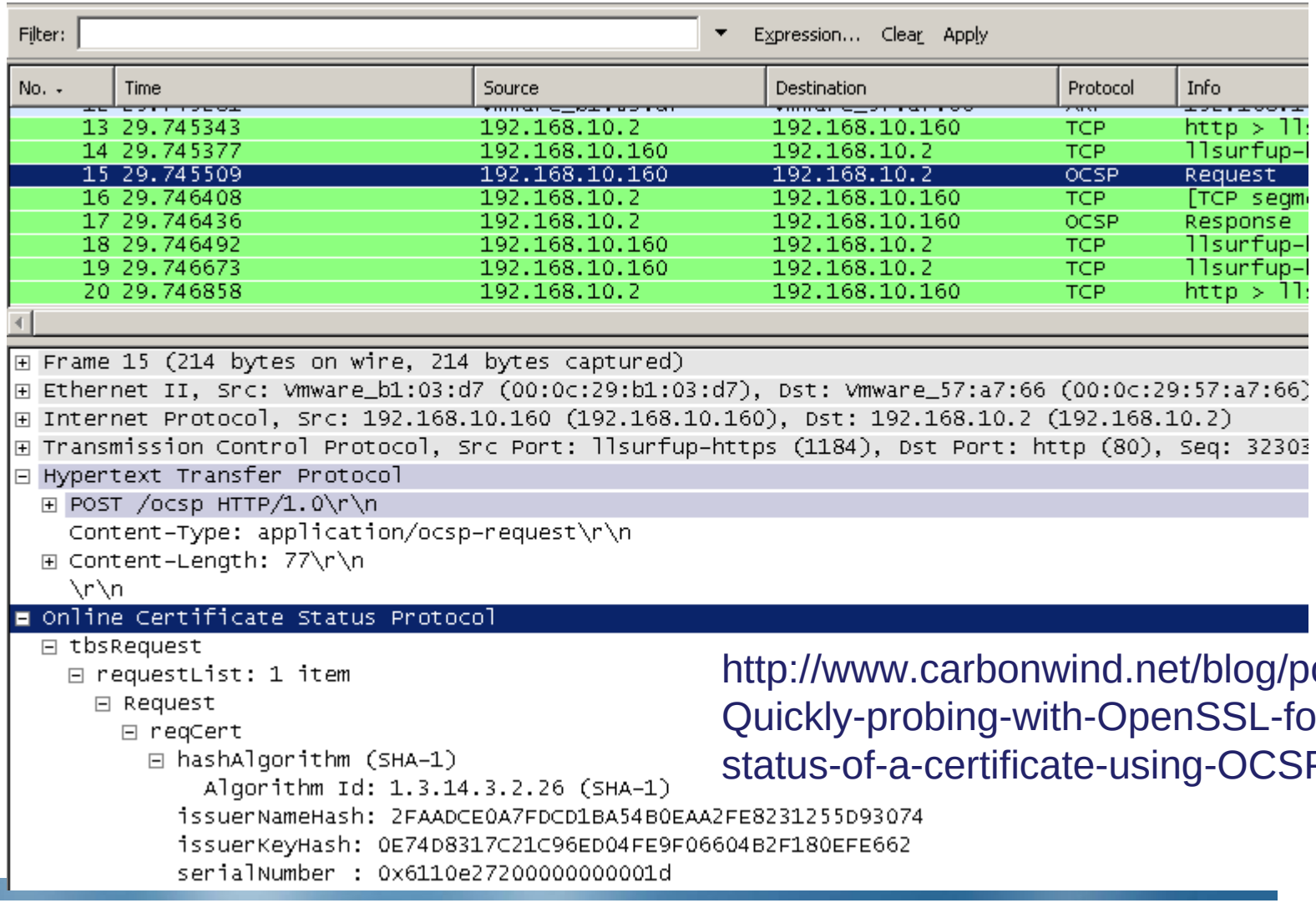
CRL



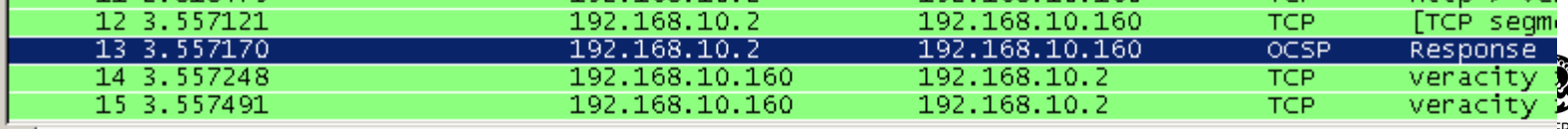
OCSP


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Enhanced Key Usage
Server Authentication (1.3.6....
Subject Key Identifier
ca f3 4e 58 ea e6 87 c1 e9 cd ...
Authority Key Identifier
KeyID=0e 74 d8 31 7c 21 c9 6...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Authority Information Access
[1]Authority Info Access: Acc...
Key Usage
Digital Signature, Key Encipher...
Thumbprint algorithm
sha1
Thumbprint
28 f7 88 d9 57 c5 00 6d 07 ef ...
URL=http://lab1dc.carbonwind.net/CertEnroll/lab1dc.carbonwind.net_lab1dcca.crt
[3]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://lab1dc.carbonwind.net/ocsp
-url
Edit Properties...
Copy to File...
OK

Request OCSP



http://www.carbonwind.net/blog/post/Quickly-probing-with-OpenSSL-for-the-status-of-a-certificate-using-OCSP.aspx



12 3.557121	192.168.10.2	192.168.10.160	TCP	[TCP segm
13 3.557170	192.168.10.2	192.168.10.160	OCSP	Response
14 3.557248	192.168.10.160	192.168.10.2	TCP	veracity
15 3.557491	192.168.10.160	192.168.10.2	TCP	veracity

```
⊞ Frame 13 (444 bytes on wire, 444 bytes captured)
⊞ Ethernet II, Src: Vmware_57:a7:66 (00:0c:29:57:a7:66), Dst: Vmware_b1:03:d7 (00:0c:29:b1:03:d7)
⊞ Internet Protocol, Src: 192.168.10.2 (192.168.10.2), Dst: 192.168.10.160 (192.168.10.160)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: veracity (1062), Seq: 55826138, A
⊞ [Reassembled TCP Segments (1850 bytes): #12(1460), #13(390)]
⊞ Hypertext Transfer Protocol
⊟ Online Certificate Status Protocol
    responseStatus: successful (0)
  ⊟ responseBytes
      ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
    ⊟ BasicOCSPResponse
      ⊟ tbsResponseData
        ⊟ responderID: byKey (2)
            byKey: 1D28CB0F46CF6B1EE250123254E5665A25C59217
          producedAt: 2009-10-03 08:19:42 (UTC)
        ⊟ responses: 1 item
          ⊟ SingleResponse
            ⊟ certID
              ⊟ hashAlgorithm (SHA-1)
                  Algorithm Id: 1.3.14.3.2.26 (SHA-1)
                issuerNameHash: 2FAADCE0A7FDCD1BA54B0EAA2FE8231255D93074
                issuerKeyHash: 0E74D8317C21C96ED04FE9F06604B2F180EFE662
                serialNumber : 0x6110e27200000000001d
            ⊟ certStatus: revoked (1)
              ⊟ revoked
                  revocationTime: 2009-10-01 13:28:00 (UTC)
                  revocationReason: certificateHold (6)
              thisUpdate: 2009-10-03 07:56:24 (UTC)
              nextUpdate: 2009-10-03 18:16:24 (UTC)
            ⊞ singleExtensions: 1 item
      ⊞ signatureAlgorithm (shaWithRSAEncryption)
        Padding: 0
        signature: 7FA4419F7912656C0E2D980ED91AA57A72872F0C32776275...
      ⊟ certs: 1 item
        ⊟ Certificate ()
          ⊞ signedCertificate
          ⊞ algorithmIdentifier (shaWithRSAEncryption)
```

Certificados “Extended Validation”

- **Identificación Legal**: Confirmar que el sitio web es controlado por una entidad jurídica específica, cuya información (nombre, dirección, jurisdicción y otros datos) está en el certificado

- **Prevención del Phishing**: Dificultar la suplantación de identidad asegurando la autenticidad de los sitios web..

- **Construcción de Confianza**: Generar confianza en los usuarios mostrando una barra verde en el navegador, que indica una conexión segura y certificada.

La CA emitirá certificados EV a organizaciones que cumplan estos criterios:

- **Tipos de Organización**: Incluye agencias gubernamentales, corporaciones, sociedades generales y asociaciones no incorporadas.

- **Documentación Requerida**:
  - Número de registro.
  - Fecha de registro o incorporación.
  - Dirección registrada o la del agente autorizado.ga

Comparación con Certificados normales

In a nutshell, here's the difference between EV and DV SSL:

Features	Extended validation SSL	Domain validation SSL
Validation level	Most strict	Lowest
Verification method	CA verifies ownership, physical location, organization information and legal existence of the organization	CA verified the organization has authority over the domain in question
Verification mode	Documents needed for identification	Through email
Duration	Few weeks	Minutes to a few hours
Expense	Most expensive – high human involvements	Minimal – no human involvement
Indication	A green address bar with the name of the organization	HTTPS connection

https://www.knownhost.com/blog/difference-domain-validation-extended-validation/

Algunas problemáticas y riesgos al usar PKI

El uso de la Infraestructura de Clave Pública (PKI) es esencial para la seguridad, pero no está exento de riesgos si no se la implementa de la manera correcta.

Problematicas

- **Autenticación de Usuario:**
  - Al emitir un certificado, ¿cómo se verifica y autentica al usuario remoto?
- **Autenticación de CA:**
  - ¿Cómo se garantiza una distribución segura de las Root CA?
  - ¿Son seguras las prácticas de certificación?
- **Listas de Revocación de Certificados (CRL):**
  - Obtener las listas CRL a tiempo presenta problemas a gran escala.
  - A menudo, la infraestructura opera sin un sistema de revocación efectivo.

https://www.schneier.com/academic/archives/2000/01/ten_risks_of_pki_wha.html

Problematicas

- **Calidad de la Clave Privada:**
  - **No hay garantía sobre la calidad de la clave usada para cifrar la privada.**
- **Seguridad del Servidor:**
  - **Algunos servidores almacenan claves privadas en texto claro o de forma fácilmente accesible.**

https://www.schneier.com/academic/archives/2000/01/ten_risks_of_pki_wha.html

.UBAfiuba
FACULTAD DE INGENIERÍA

Firma Digital

Limitaciones de Documentos Digitales

- **Autoría No Verificable**: No se puede identificar con certeza quién creó un documento digital.
- **Fácilmente Alterable**: Los documentos digitales pueden modificarse sin dejar evidencia de los cambios.
- **Desconocimiento del Autor**: El autor puede negar su creación.
- **No Verificable**: No se puede confirmar la autoría ante terceros.

Firma Digital: Requerimientos

- **Autenticidad del Autor:** Atribuir el documento de forma fehaciente al autor.
- **Integridad del Contenido**: Asegurar que el documento no ha sido modificado tras ser firmado.
- **No Repudio**: Garantizar que el remitente no pueda negar la existencia o autoría del mensaje.
- **Verificabilidad**: Asegurar que el documento puede ser verificado por terceros.

Firma Digital

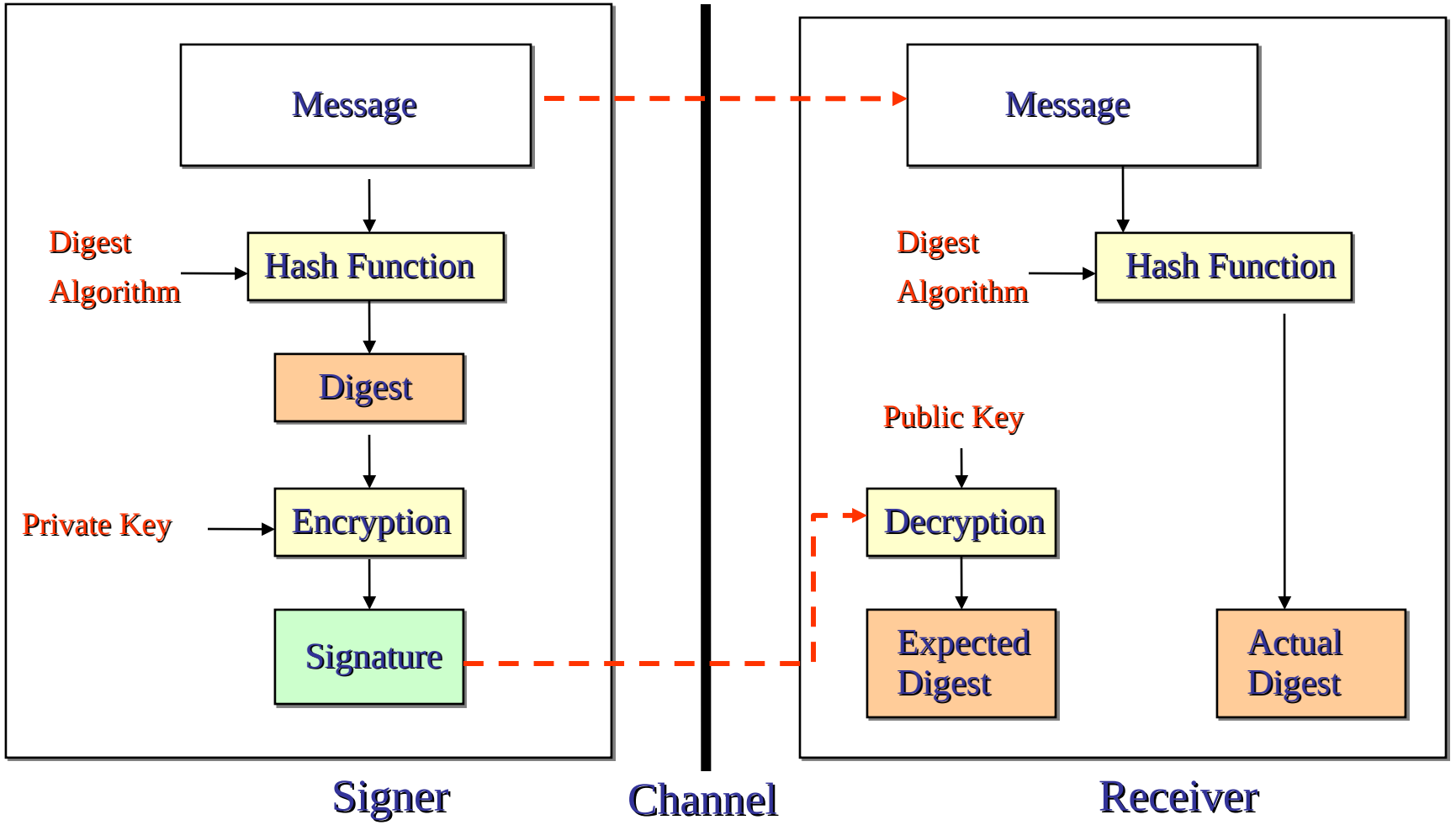
Uso:

- **Identificación del Firmante**: Confirma la identidad de la persona que firma el documento.
- Integridad del Contenido: Verifica que el contenido no ha sido alterado.

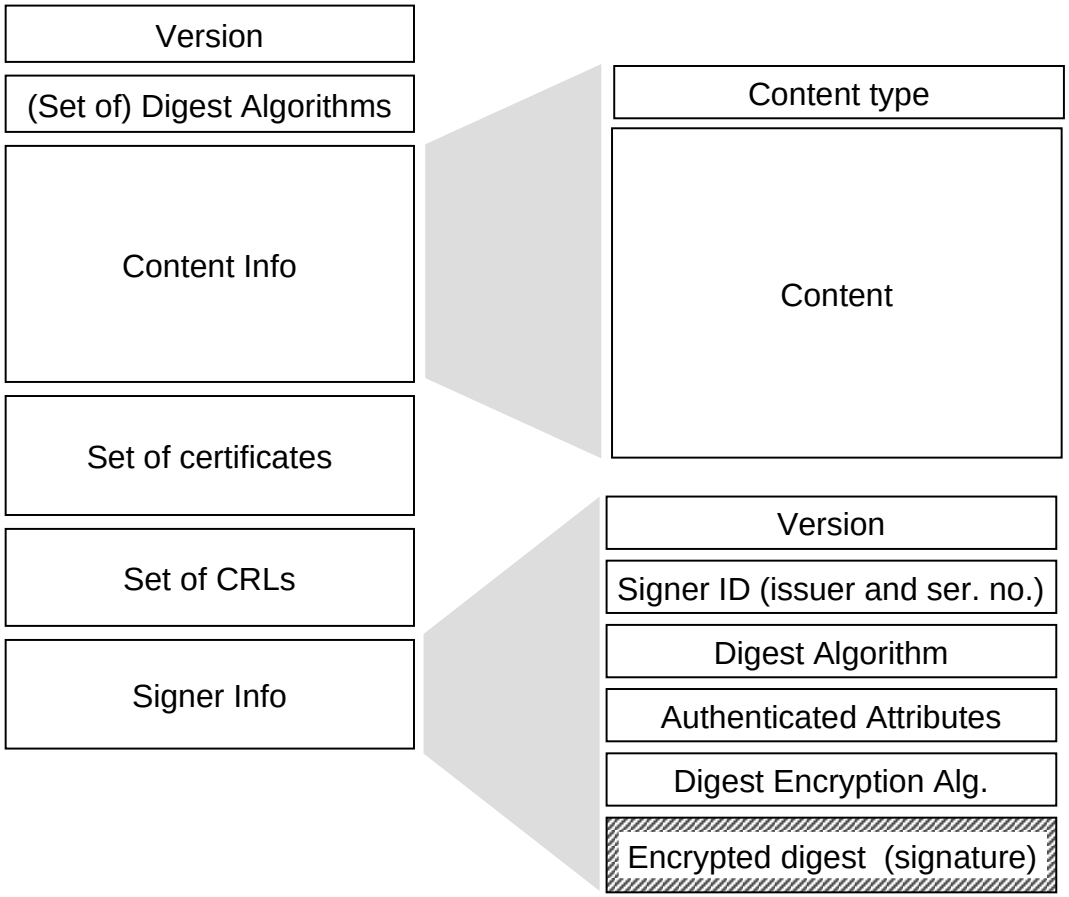
Requisitos:

- **Propiedad Exclusiva**: Debe pertenecer únicamente al titular.
- **Control Total**: Estar bajo su control absoluto.
- **Verificable**: Permitir la verificación de la firma.
- **Evidencia de Alteración**: Debe indicar si el documento ha sido modificado.

Firma Digital: Diagrama



Firma Digital: PKCS7 “signed data”



http://www.hit.bme.hu/~buttyan/courses/BMEVIHI9367/PGP_SMIME.ppt

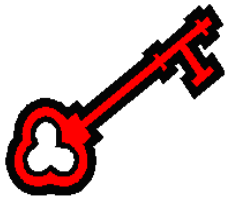
Firma Digital: S/MIME : Ejemplo


```
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=sha1;
boundary="-----aaaaa"
-----aaaaa
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
Hello!
-----aaaaa
Content-Type: application/x-pkcs7-signature
Content-Transfer-Encoding: base64
MIIN2QasDDSdwe/625dBxgdhdsf76rHfrJe65a4f
fvVSW2Q1eD+SfDs543Sdwe6+25dBxfdER0eDsrs5
-----aaaaa
```

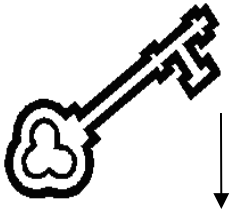
Sobre Digital

El sobre digital garantiza la seguridad de datos en tránsito.

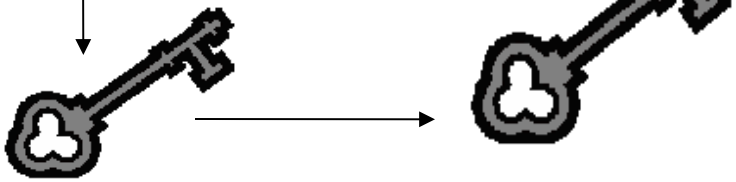
Sobre Digital



Mensaje → Clave Simétrica → Mensaje Cifrado → Sobre Digital

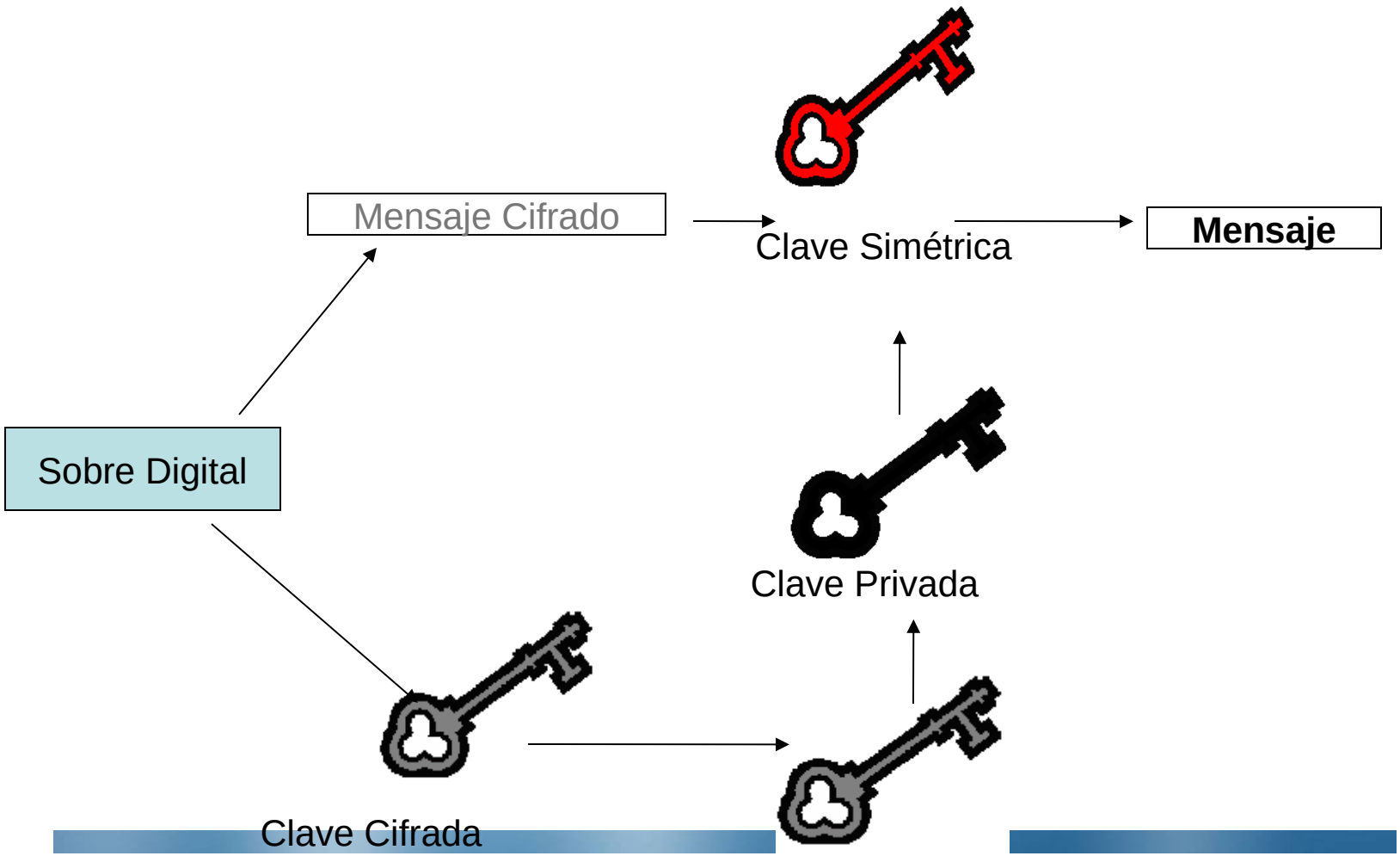


Publica del destino

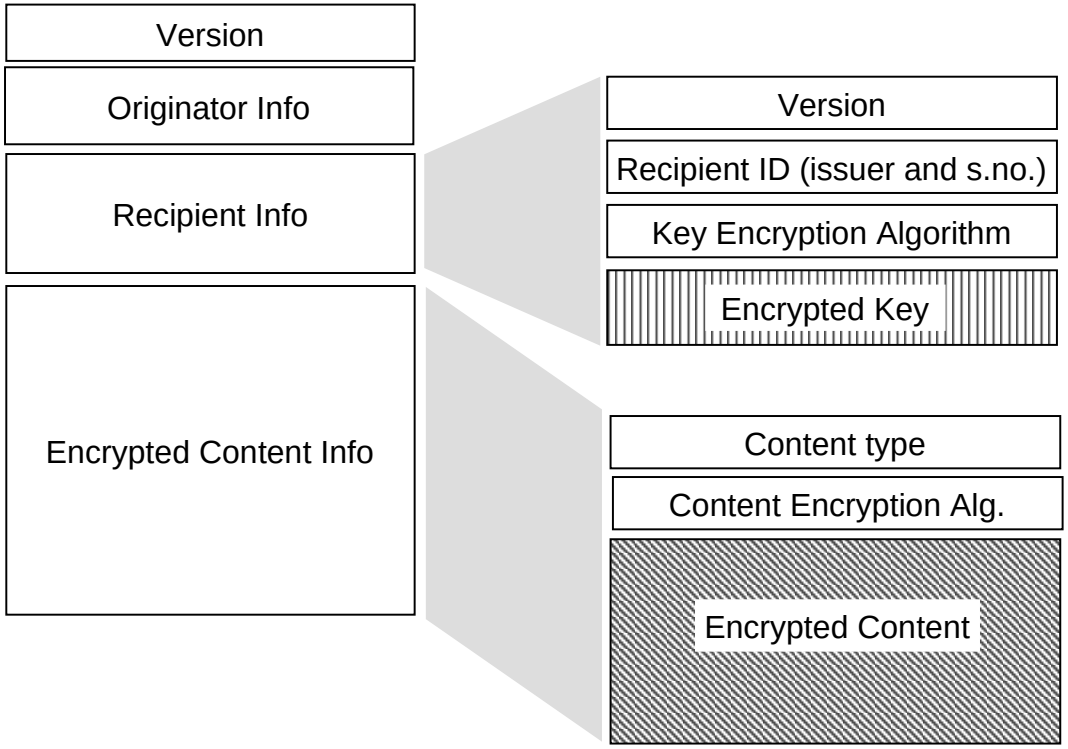


Clave Cifrada

Sobre Digital



PKCS7 “enveloped data”



http://www.hit.bme.hu/~buttyan/courses/BMEVIHI9367/PGP_SMIME.ppt

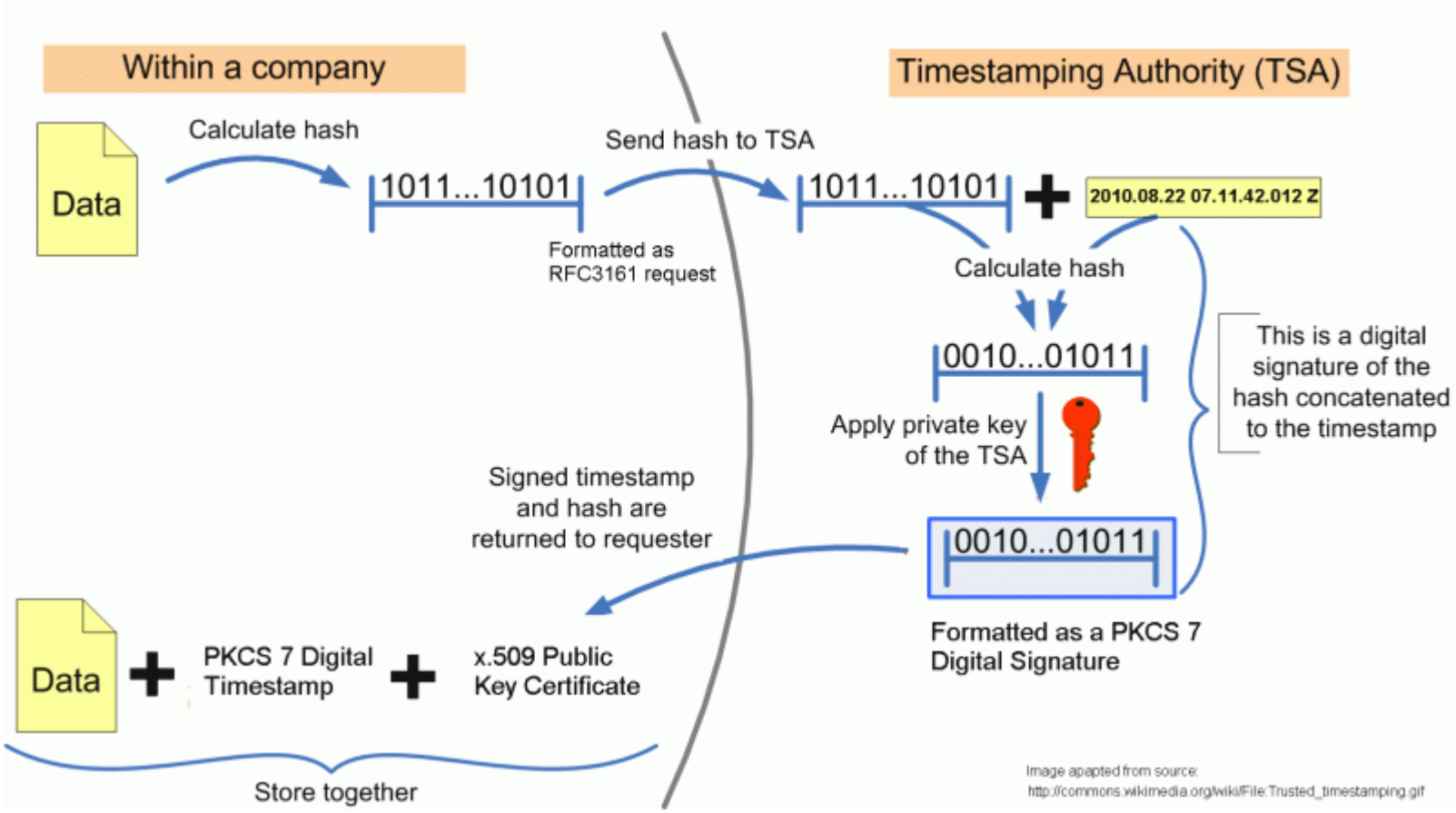
Fechado de Transacciones

El “Time Stamping” es una herramienta esencial para asegurar la trazabilidad temporal y prevenir disputas en la autenticidad de documentos y acciones."

PKI-. Time-Stamping Authority (TSA),

- **Sello Digital de Tiempo**: Emite TST (sellos digitales de tiempo) cuando lo solicitan los usuarios.

- **Gestión TSS**: Administra y controla la infraestructura de todos los servicios de sellado de tiempo (TSS).


Within a company
Timestamping Authority (TSA)
Data
Calculate hash
1011...10101
Formatted as
RFC3161 request
Send hash to TSA
1011...10101
2010.08.22 07.11.42.012 Z
Calculate hash
0010...01011
Apply private key
of the TSA
This is a digital
signature of the
hash concatenated
to the timestamp
Signed timestamp
and hash are
returned to requester
0010...01011
Formatted as a PKCS 7
Digital Signature
Data
PKCS 7 Digital
Timestamp
x.509 Public
Key Certificate
Store together
Image apapted from source:
http://commons.wikimedia.org/wiki/File:Trusted_timestamping.gif

- Firma Electrónica:
  - Están firmados electrónicamente.
  - Se usa un certificado emitido para este propósito
- Exactitud:
  - Los sellos se emiten con una precisión de 1 segundo.
  - Utilizan una fuente de tiempo segura sincronizada con UTC
- Protocolo NTP:
  - NTP en un nivel Stratum 1.

Sellado de Tiempo

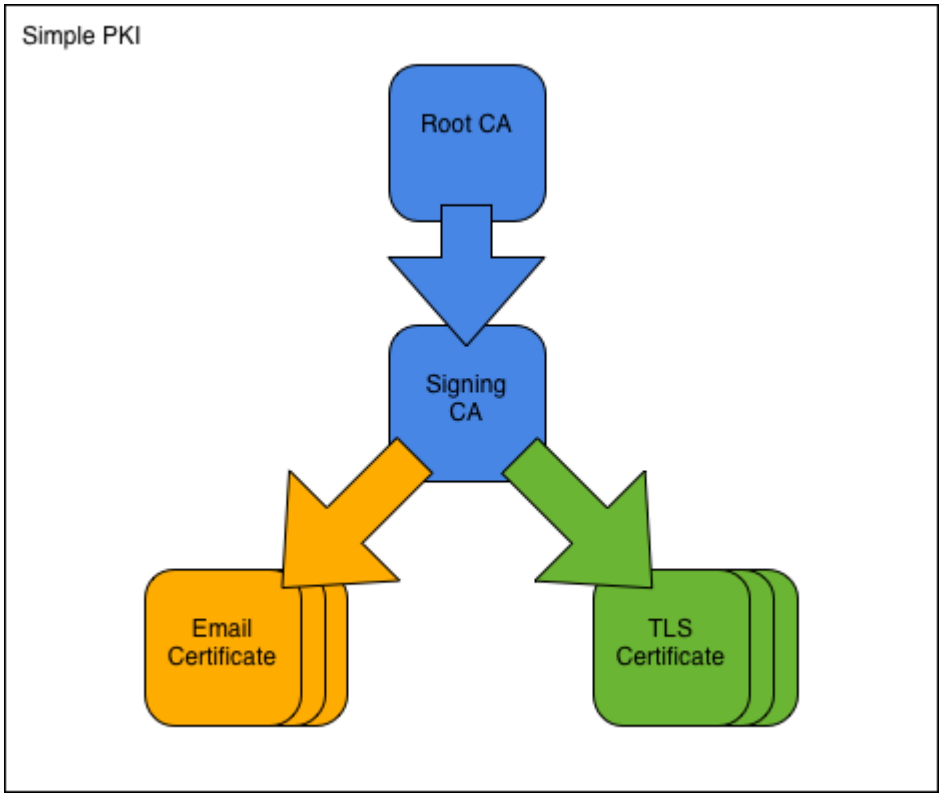
- **Hash Enviado**: El usuario envía a la TSA el hash de un documento (h(D)).
- **Añadir Tiempo**: La TSA añade la marca temporal (t), indicando la fecha y hora de recepción, creando así (h(D), t).
- **Firma Digital**: La TSA firma digitalmente (h(D), t), generando Firma(h(D), t).
- **Envío del Sello**: La TSA devuelve el sello digital de tiempo al usuario.
- **Verificación**: El sello permite probar que el documento D existía en el tiempo t.

Tipos de TST

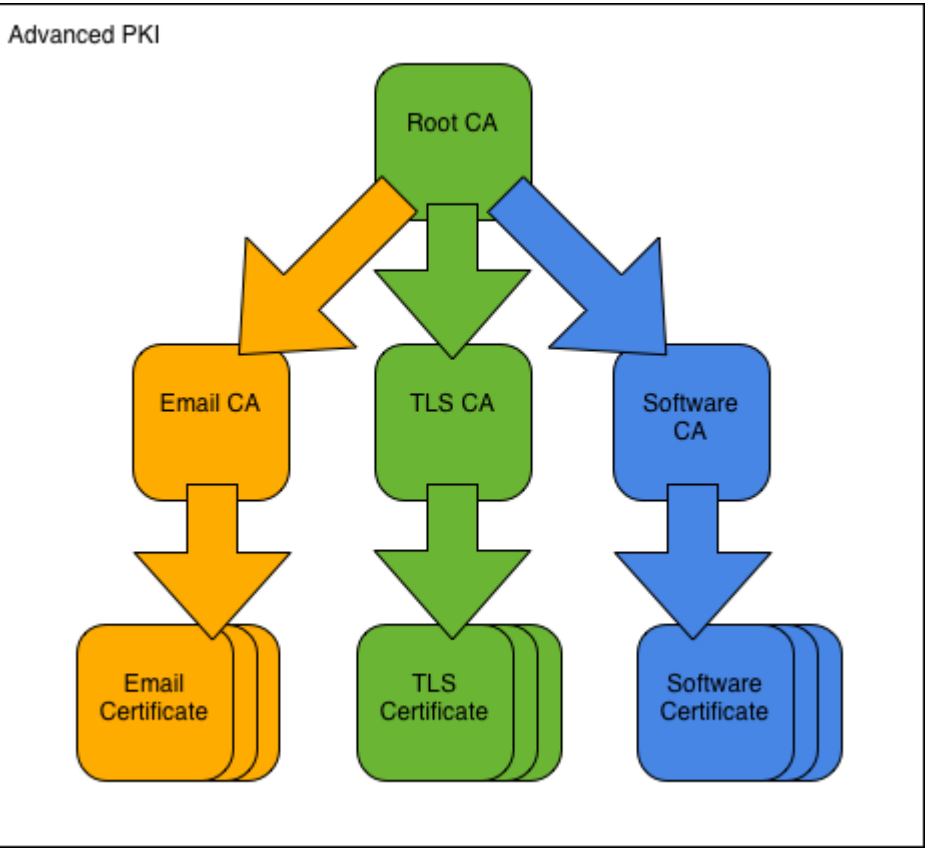
- TST Cliente
  - Emitido a solicitud del usuario.
  - Apoya la generación de firma electrónica.
- TST Servidor
  - Emitido a solicitud del equipo informático.
  - Apoya la generación de firma electrónica .
- TST Auditor
  - Emitido para demostrar la existencia de datos en una fecha determinada

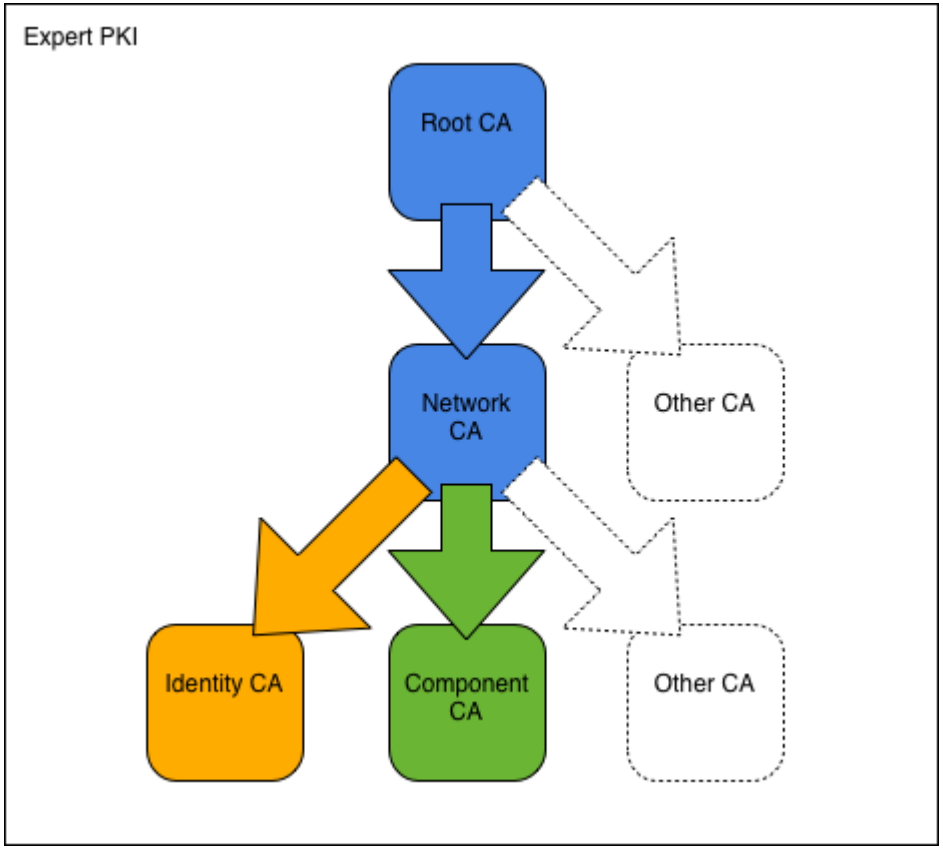
RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol

Ejemplos de Arquitecturas de certificación

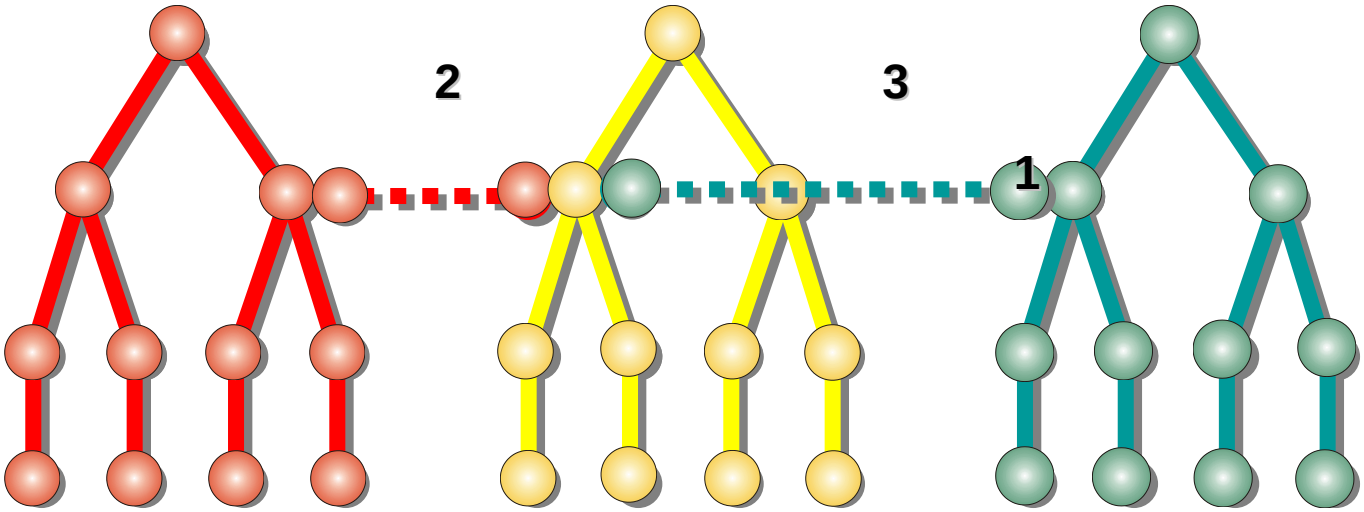


https://pki-tutorial.readthedocs.io/en/latest/


Advanced PKI
Root CA
Email CA
TLS CA
Software CA
Email Certificate
TLS Certificate
Software Certificate


Expert PKI
Root CA
Network CA
Other CA
Identity CA
Component CA
Other CA

Certificación Cruzada



La Certificación Cruzada permite que una persona de una CA pueda reconocer un certificado emitido por otra CA que no reconoce, pero que ha sido certificada por su CA

es necesario que ambas confíen en las políticas de seguridad de la contraparte