Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Infraestructura de clave pública

Presentación

Daniel F. García

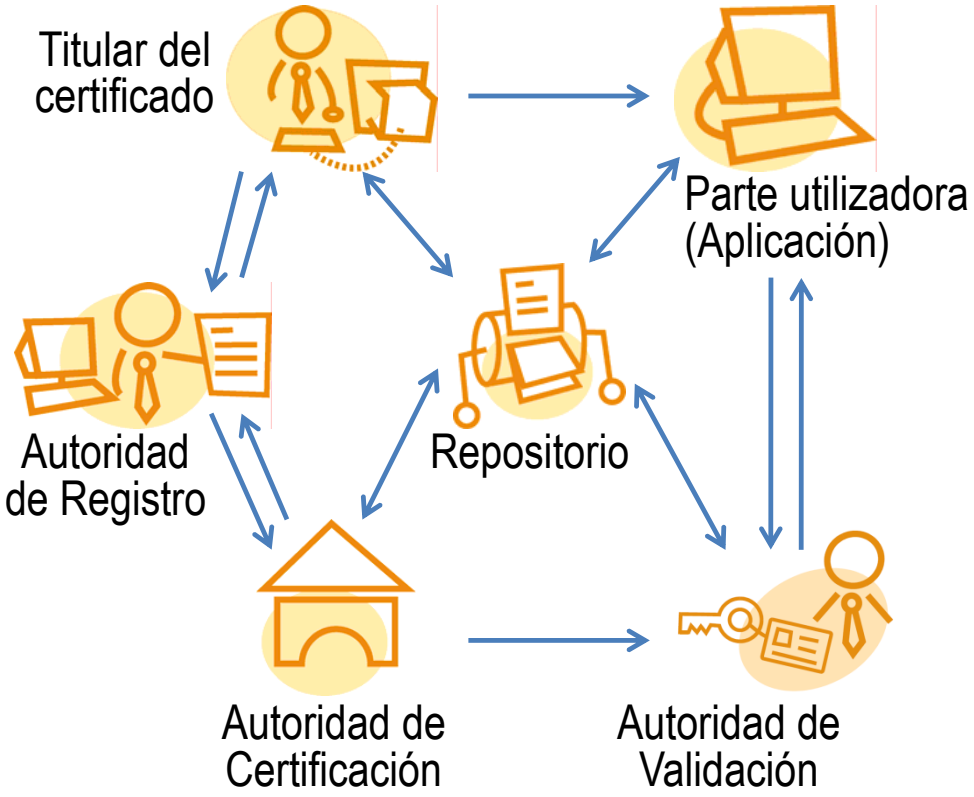
Infraestructura de clave pública (PKI)

En inglés se denomina "**Public Key Infrastructure**" y se abrevia como **PKI**

Definición

El hardware, software, personas, políticas y procedimientos necesarios para: crear, gestionar, almacenar, distribuir y revocar certificados digitales

Componentes



Titular del certificado

Entidades finales /Usuarios /Suscriptores

Autoridad de Registro

Autoriza la asociación entre una clave pública y el titular de un certificado

Autoridad de Certificación

Gestiona los Certificados

Repositorios (Directorios)

Almacenan y distribuyen certificados con sus estados: expirado, revocado, etc.

Parte Utilizadora

Verifican certificados y firmas

Autoridad de Validación

Suministra información en tiempo real acerca del estado de un certificado

PKI: Autoridad de Certificación

Entidad fiable, encargada de garantizar de forma unívoca y segura la identidad asociada a una clave pública

Recibe y procesa **peticiones** de certificados de los usuarios finales

Consulta con una Autoridad de Registro para determinar si **acepta o rehúsa** la petición de certificado

Emite el certificado

Gestiona **Listas de Revocación** de Certificados (CRLs)

Renueva certificados

Proporciona:

- Servicios de backup y archivo seguro de claves de cifrado
- Infraestructura de seguridad para la confianza, políticas de operación segura, información de auditoría

PKI: Autoridad de Registro

Gestiona el registro de usuarios y
sus peticiones de certificación/revocación,
así como los certificados respuesta a dichas peticiones

Indica a la Autoridad de Certificación si debe emitir un certificado o NO

Autoriza la **ASOCIACIÓN** entre una clave pública y el titular de un certificado

Puede intervenir en la gestión del ciclo de vida de un certificado

- Revocación
- Expiración
- Renovación (extensión del periodo de validez del certificado, respetando el par de claves)
- Reemisión del par claves del usuario
- Actualización de datos del certificado

PKI: Repositorios/Directorios

Los Repositorios/Directorios proporcionan almacenamiento y un mecanismo de distribución para los Certificados y las Listas de Revocación

Cuando la AC emite un Certificado o una Lista de Revocación

- Lo envía al Repositorio/Directorio
- También lo guarda en su base de datos local

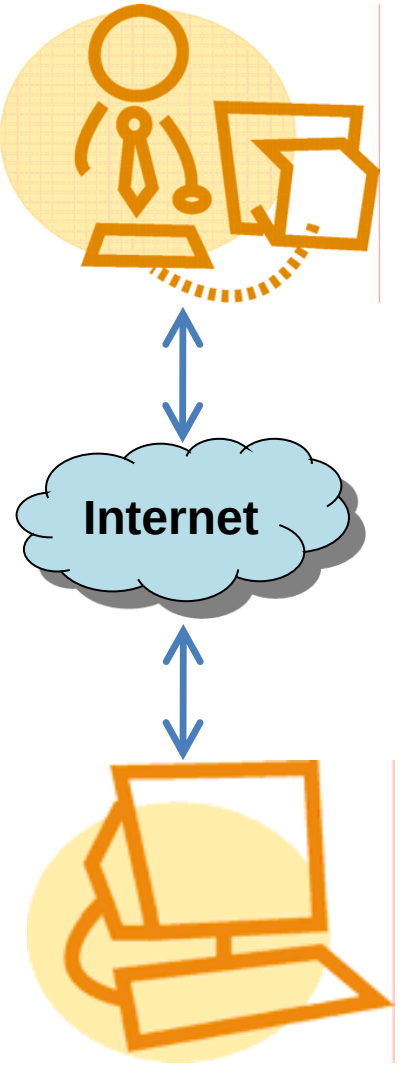
La AC utiliza el protocolo LDAP (Light-weight Directory Access Protocol) para acceder a los directorios

El usuario puede obtener certificados de otros usuarios y comprobar el estado de los mismos

PKI: Titulares de certificados y Partes utilizadoras

Titulares de certificados

- Entidades finales
- Usuarios finales
- Suscriptores



Partes utilizadoras

Una vez la entidad final tiene un certificado…

Hay partes que confían en el certificado para comunicarse y realizar transacciones con sus suscriptores

Las partes utilizadoras verifican los certificados, las firmas electrónicas y las rutas de certificación

PKI: Autoridad de Validación

Suministra información online (en tiempo real) acerca del estado de un certificado

La AV suele proporcionar **dos** servicios de validación:

1. Permitir la descarga de Listas de Revocación de Certificados para que el usuario las interprete él mismo

2. Mediante el protocolo **OCSP** (***O**nline **C**ertificate **S**tatus **P**rotocol*)

   Los usuarios y las aplicaciones que deseen obtener el estado de un certificado sólo tienen que realizar una petición OCSP contra la AV para obtener su estado

La AC actualiza la información de la AV cada vez que modifica el estado de un certificado → a diferencia de las Listas de Revocación, se dispone de información en tiempo real

PKI: Autoridad de Sellado de Tiempos (Opcional)

Permite firmar documentos con sellos de tiempos, de manera que permite obtener una prueba de que un determinado dato existía en una fecha concreta

RFC-3161 Internet X.509 PKI - Time-Stamp Protocol (TSP) Agosto 2001
https://datatracker.ietf.org/doc/pdf/rfc3161.pdf RFC-5816 Update Marzo 2010

Creación de una estampa de tiempo

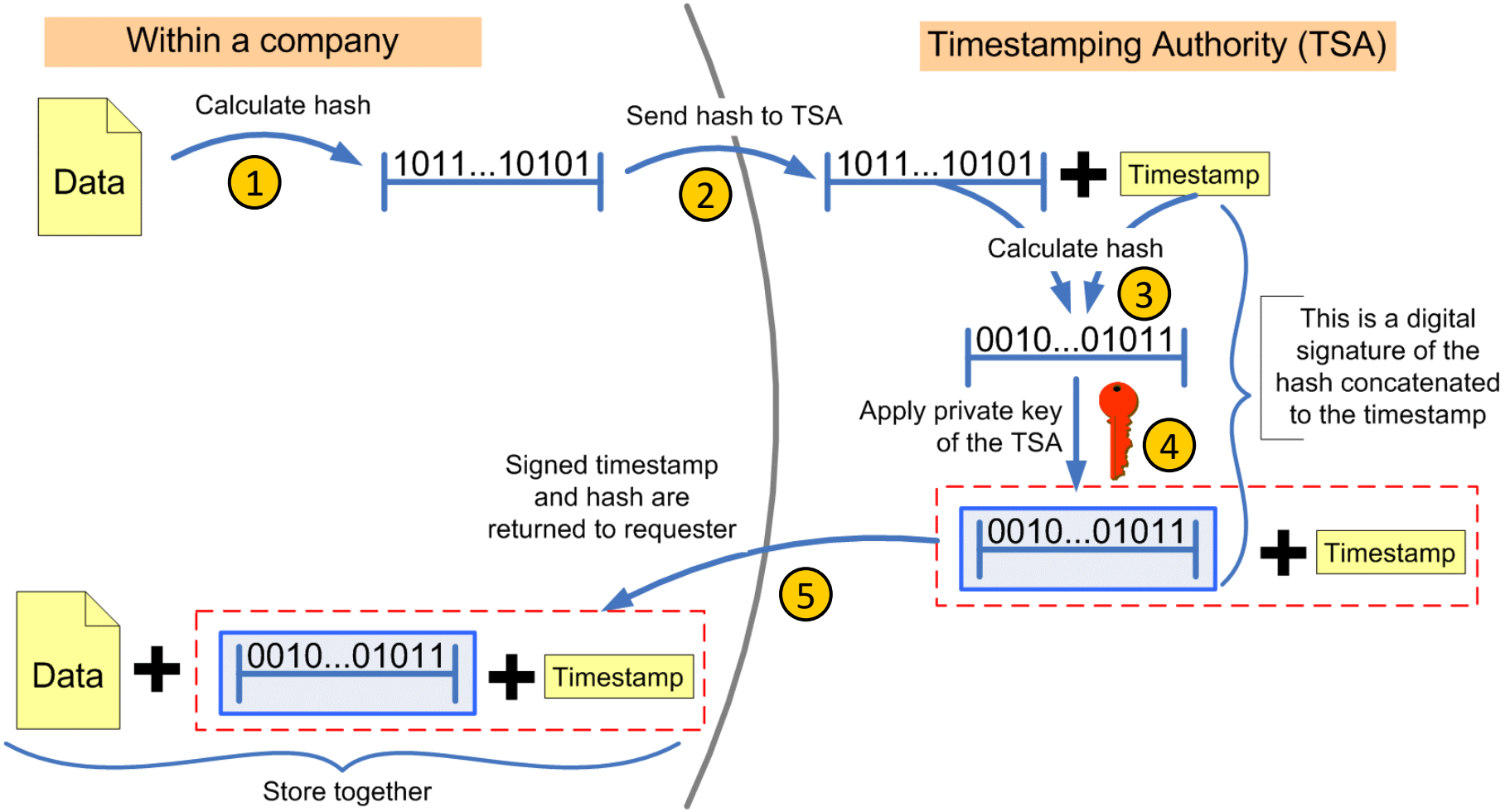
1. El usuario obtiene un Resumen (Hash) del documento
2. Envía el hash a la TSA (Time Stamping Authority)
3. La TSA concatena una estampa de tiempo con el hash y calcula el hash de la concatenación
4. Este hash es firmado digitalmente (cifrado) con la clave privada de la TSA
5. El hash firmado +la estampa de tiempo se envían al usuario que los almacena con el documento

Comprobación de una estampa de tiempo

1. El usuario obtiene el Hash del documento y lo concatena con la estampa de tiempo de la TSA
2. El usuario calcula el Hash de la concatenación → hA
3. Se verifica el hash firmado digitalmente (descifra) con la clave pública de la TSA → hB

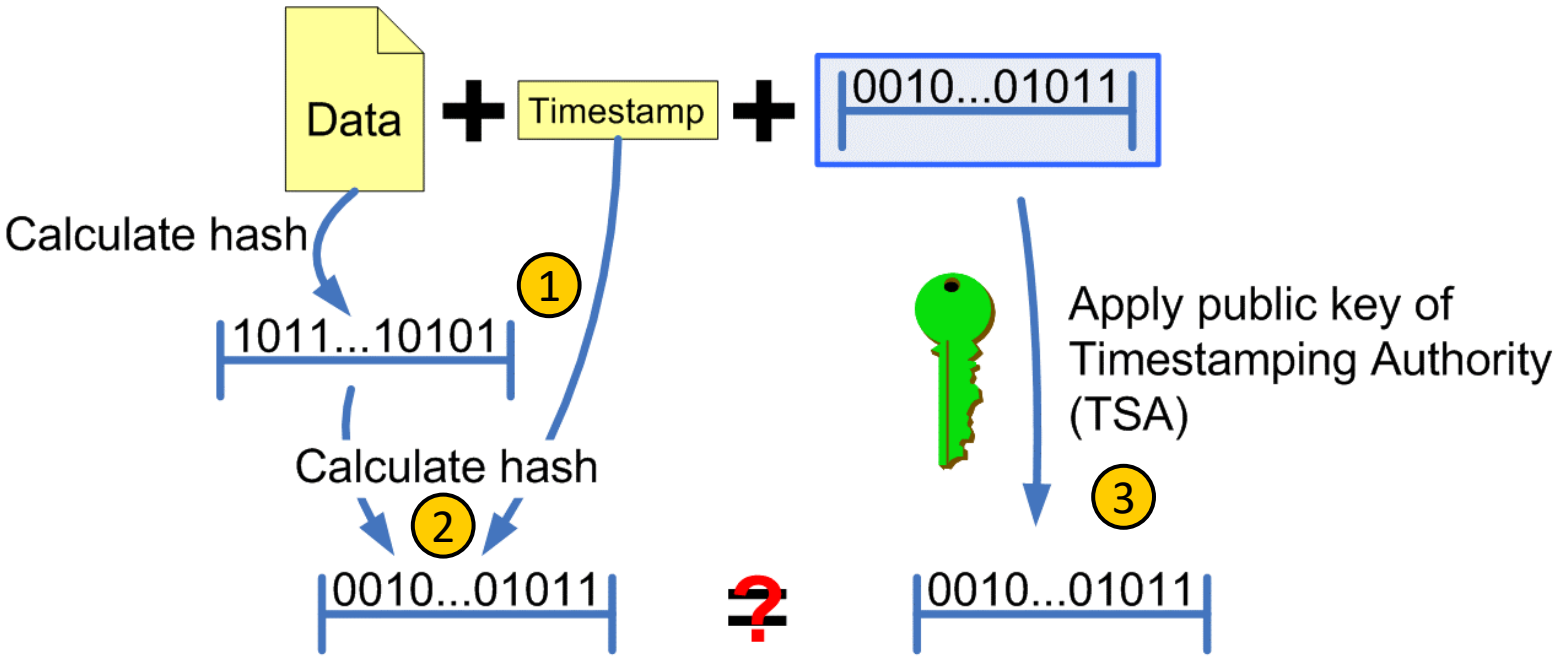
Si hA == hB el documento no ha sido alterado respecto al de la estampa de tiempo

Creación de una estampa de tiempo



E { H[H(Data) + tStamp)] }

Comprobación de una estampa de tiempo



H[H(Data) + tStamp)]

D (E { H[H(Data) + tStamp)] })

Estándares de PKI (X.509 de ITU)

1988 **ITU-T X.509** (11-1988) **Cer X.509 V1**
ISO/IEC 9594-8:1990 Edition 1

1993 **ITU-T X.509** (11-1993) **Cer X.509 V2**
ISO/IEC 9594-8:1995 Edition 2 **CRL V1**

1997 **ITU-T X.509** (08-1997) **Cer X.509 V3**
ISO/IEC 9594-8:1998 Edition 3

2000 **ITU-T X.509** (03-2000) **CRL V2**
ISO/IEC 9594-8:2001 Edition 4

2005 **ITU-T X.509** (08-2005)
ISO/IEC 9594-8:2005 Edition 5

2008 **ITU-T X.509** (11-2008)
ISO/IEC 9594-8:2008 Edition 6

2012 **ITU-T X.509** (10-2012)
ISO/IEC 9594-8:2014 Edition 7

2016 **ITU-T X.509** (10-2016)
ISO/IEC 9594-8:2017 Edition 8

2019 **ITU-T X.509** (10-2019)
ISO/IEC 9594-8:2020 Edition 9

X.509 es un estándar de PKI de la ITU
ITU = International Telecommunication Union

X.509 es parte del conjunto de estándares X.500
(Que definen los servicios de Directorio)

https://www.itu.int/rec/T-REC-X.509/es

https://www.iso.org/standard/80325.html

El X.509 especifica:

- Formatos y atributos de certificados
- Formatos de listas de revocación
- Alg. para validar la ruta de certificación

En X.509 las descripciones se hacen en ASN.1
(Abstract Syntax Notation 1 Language)

Estándares de PKI (X.509 de IETF)

La IETF tuvo un grupo de trabajo en PKI desde 1995 → Se denomina **PKIX**

https://datatracker.ietf.org/wg/pkix/charter/ El grupo se cerro el 31-Oct-2013

https://datatracker.ietf.org/group/pkix/documents/

Adaptó el rígido estándar X.509 para su utilización en Internet

2001-01	**RFC 3039**	Perfil de Certificado Cualificado X.509	
2004-03	**RFC 3739**	Perfil de Certificado Cualificado X.509	Hace obsoleta la RFC 3039

2002-04	**RFC 3280**	Perfil de Certificado X.509 v3 Perfil de CRL X.509 v2	Hace obsoleta la RFC 2459
2008-05	**RFC 5280**	Perfil de Certificado X.509 v3 Perfil de CRL X.509 v2	Hace obsoleta la RFC 3280
2013-01	**RFC 6818**	**ACTUALIZACIÓN** de la RFC 5280	

Hay muchas mas “secuencias” de RFCs

Solicitud de Certificado con Registro Presencial

1. El usuario se persona en la Autoridad de Registro donde entrega toda la documentación que se le requiere

2. Si la Autoridad de Registro aprueba la solicitud transfiere los datos a la Autoridad de Certificación para que emita el certificado

3. Una vez que el certificado ha sido emitido, la Autoridad de Registro entrega el certificado al usuario

Solicitud de Certificado con Pre-Registro Remoto

1. El usuario realiza un pre-registro en la Autoridad de Certificación
2. El usuario se persona (telemáticamente o personalmente) ante la Autoridad de Registro y le envía toda la documentación que se le requiere
3. Si la Autoridad de Registro aprueba la solicitud transfiere los datos a la Autoridad de Certificación para que emita el certificado
4. Una vez que el certificado ha sido emitido, la Autoridad de Certificación permite al usuario descargarse el certificado

El estándar PKCS#10 de solicitud de certificado

La solicitud de un certificado está estandarizada:
(El mensaje que envía el solicitante a la autoridad certificadora)

PKCS#10 v1.7: Certification Request Syntax Specification 26 Mayo 2000

RFC-2986 Certification Request Syntax Specification v1.7 Noviembre 2000
https://datatracker.ietf.org/doc/pdf/rfc2986.pdf

La solicitud consta de tres partes →
1) Info de la solicitud (*CertificationRequestInfo*)
2) Identificación del algoritmo de firma
3) Firma digital de 1) (*CertificationRequestInfo*)

La entidad solicitante hace:

1) Genera un par de claves (pública / privada)

2) Crea un *CertificationRequestInfo* con
- Nombre distintivo de la entidad
- Clave pública de la entidad
- Atributos (+Info) de la entidad

3) Firma el *CertificationRequestInfo* con la clave privada de la entidad

4) Crea *CertificationRequest* = *CertificationRequestInfo* + ID del Alg. de firma + La firma
El *CertificationRequest* esta definido en ASN.1

Validación de un Certificado 1

La validación de un certificado depende de la estructura de la PKI que lo ha emitido

Estructuras comunes
- Jerárquica (árbol) – Ej. X.509
- Malla (*mesh*) – Ej. PGP (*Pretty Good Privacy*)

Para relacionar 2 PKI
- Certificación cruzada
- Puentes (*bridges*)

La PKI Jerárquica

TODAS las entidades finales y las partes de la PKI que deben confiar en otras usan una UNICA Autoridad de Certificación como su **anclaje de confianza** (*trust anchor*)

En una jerarquía con **múltiples niveles** la AC Raíz certifica a otras ACs intermedias (subordinadas)
Las ACs intermedias certifican a entidades finales y a otras ACs

En esta jerarquía los **certificados se emiten** sólo en una dirección (descendiendo por el árbol)
Una AC nunca certifica a otra AC de un nivel "superior"

Cualquier entidad de la PKI que deba confiar en otra entidad de la PKI
¡Debe disponer del certificado de la AC Raíz! → **Anclaje de confianza en el que confían TODOS los elementos de la PKI**

Validación de un Certificado 2

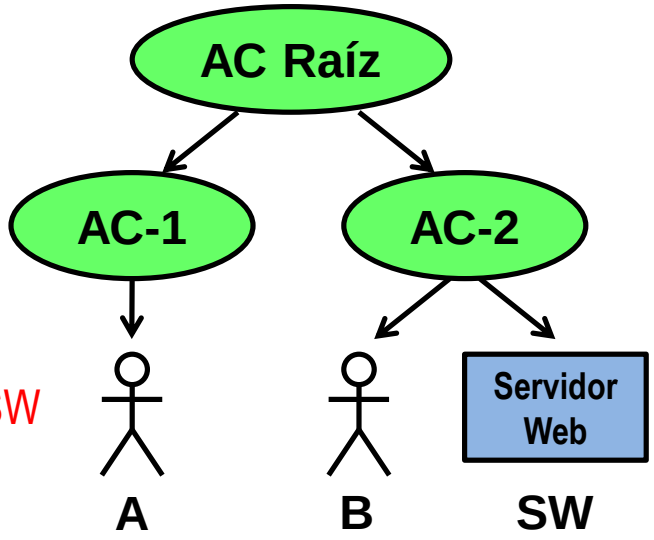
Para validar un certificado hay que hacer 2 operaciones:

1º - Construir una cadena de certificados
2º - Validar la cadena de certificados

Una cadena de certificados es una lista enlazada de los certificados usados para autenticar una entidad

La **cadena comienza** con el certificado de la entidad
Cada cert de la cadena está firmado por la entidad identificada por el siguiente cert de la cadena
La **cadena termina** con el certificado de una AC Raíz (anclaje de confianza)

EJEMPLO:

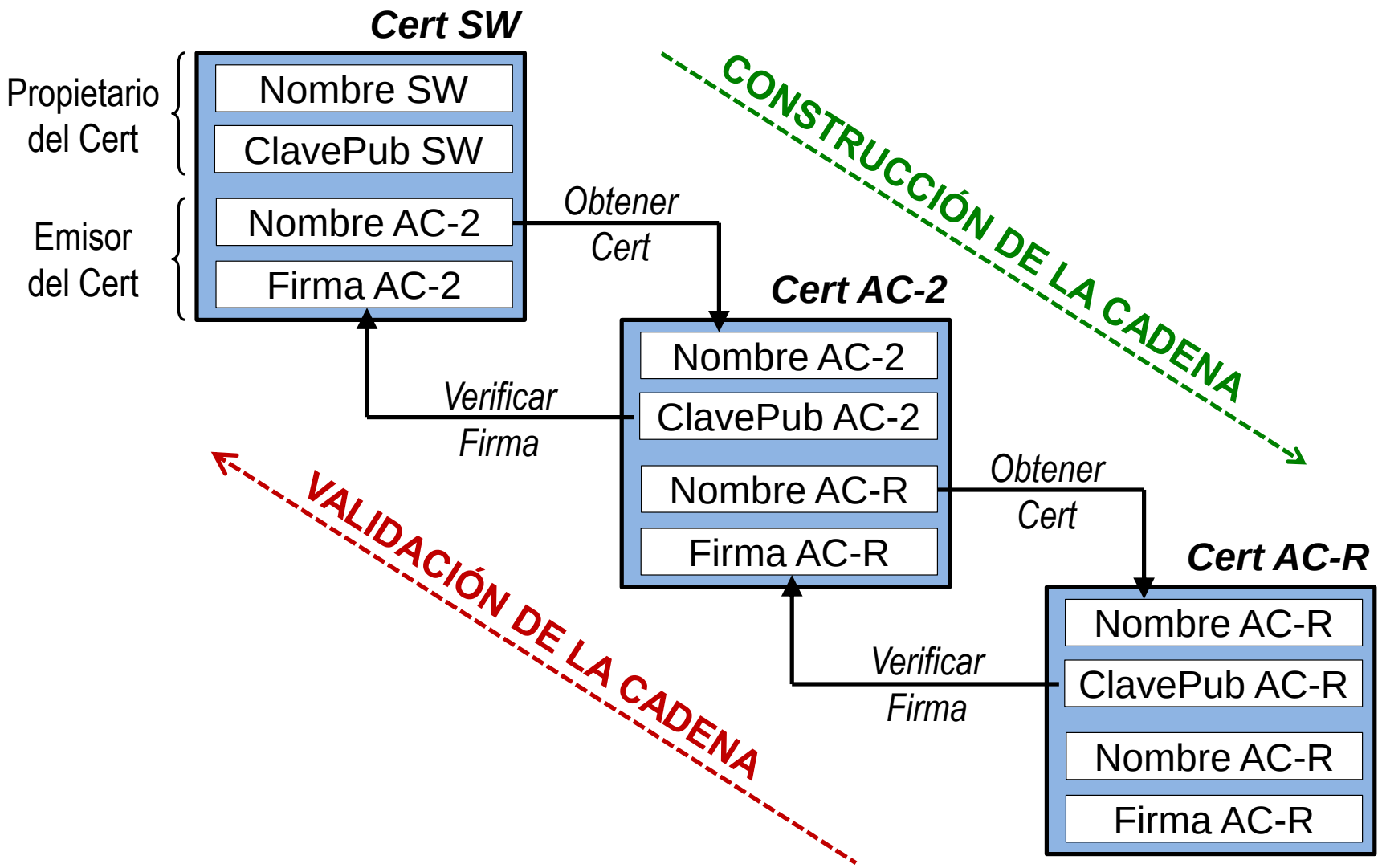


Ej.: A recibe el certificado de SW

Validación de un Certificado 3

Construir y validar la cadena de certificados

Ej.: A recibe el certificado de SW



Validación de un Certificado 4

Para validar cada uno de los certificados de la cadena hay que:

1. Comprobar la firma digital

   Localizar el certificado de la entidad que ha emitido (firmado) el certificado a validar

   Con la clave pública de la entidad firmante se puede verificar la firma del certificado

2. Comprobar la validez temporal

   Comprobar que el instante actual está incluido dentro del período de validez del certificado

3. Comprobar si está revocado

   Hay 2 métodos:

   - Consultar una CRL (*Certificate Revocation List*) disponible a la que se accede mediante un servicio de directorio
   - Hacer una consulta a una Autoridad de Validación sobre el estado del certificado mediante el protocolo OCSP (*Online Certificate Status Protocol*)

4. Comprobar el formato

   Se comprueba si los campos del certificado cumplen el estándar X.509

   También hay que validar las extensiones → Política de validez

El protocolo OCSP (1)

El protocolo OCSP (*Online Certificate Status Protocol*)

OCSP es un estándar de la IETF:

RFC-2560 X.509 Internet PKI - Online Certificate Status Protocol – OCSP Junio 1999

RFC-6960 X.509 Internet PKI - Online Certificate Status Protocol – OCSP Junio 2013

https://datatracker.ietf.org/doc/pdf/rfc6960.pdf

Las Aut. de certificación también suelen operar como Aut. de validación →

→ Proporcionan servicios OCSP

A los servidores OCSP se les suele denominar: ***OCSP Trusted Responders***

https://www.cert.fnmt.es/welcome-ocsp.html

http://ocsp.dnielectronico.es/

Todas las especificaciones de las peticiones y respuestas OCSP están definidas en ASN.1

Petición OCSP:

Versión del protocolo
Identificadores de los certificados a validar
Extensiones opcionales

La firma digital de la petición es opcional (depende de los requisitos de la Aut. de Validación)

El protocolo OCSP (2)

Respuesta OCSP:

Un código de error si
- El mensaje no está bien formado
- El Responder no está preparado para el servicio solicitado
- Falta información necesaria para el servicio solicitado

} Extensiones

Una de las tres respuestas posibles para cada certificado (firmadas digitalmente):

Respuesta bueno “good”:

No hay un certificado con el número de serie enviado que esté en las listas de revocados que utiliza el Responder

El cliente puede hacer comprobaciones adicionales para el certificado

Respuesta revocado “revoked”:

El certificado con el número de serie enviado ha sido revocado ó nunca ha sido emitido ese nº de serie por la autoridad certificadora

El cliente debe rechazar el certificado

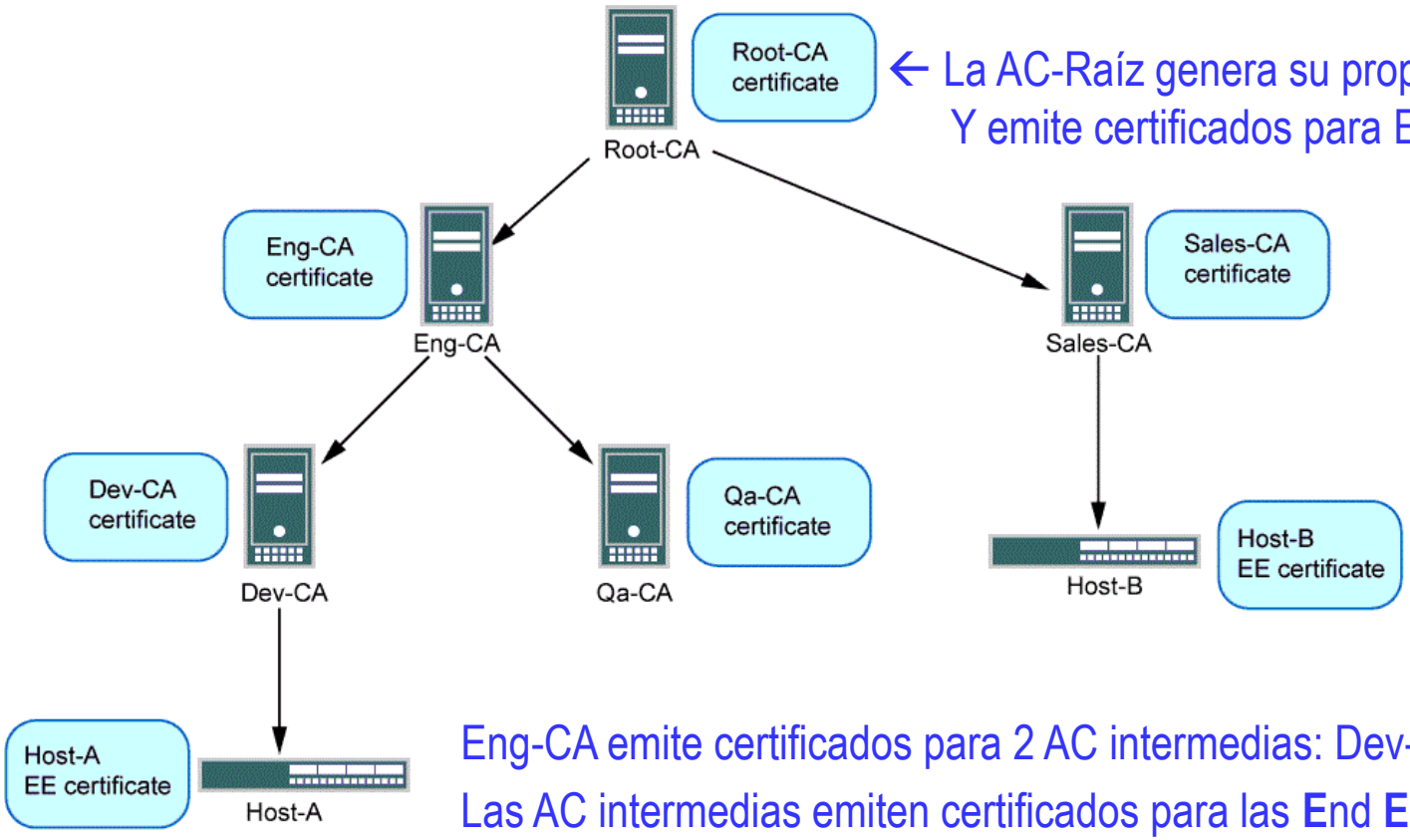
Respuesta desconocido “unknown”:

El Responder no conoce el número de serie del certificado enviado (Típicamente porque el Responder no sirve al emisor del certificado)

El cliente puede utilizar otros Responders o CRLs

Ejercicio

La figura siguiente muestra un diagrama de una PKI basada en el estándar X.509



← La AC-Raíz genera su propio certificado Root-CA
Y emite certificados para Eng-CA y Sales-CA

Eng-CA emite certificados para 2 AC intermedias: Dev-CA y Qa-CA

Las AC intermedias emiten certificados para las **E**nd **E**ntities: Host-A y Host-B

Dibuja la cadena de certificados que necesita el Host-A para validar el certificado del Host-B

Dibuja la cadena de certificados que necesita el Host-B para validar el certificado del Host-A