SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.2.1.MF0489_3. Capítulo 2
Parte 1
Infraestructura de clave pública

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Con la aparición de la criptografía de clave pública en 1976, surgen las infraestructuras de clave pública (habitualmente referidas como PKI, del inglés Public Key Infrastructure), cuya misión es gestionar el ciclo de vida de los certificados de clave pública.

2. COMPONENTES DE UNA PKI

En una infraestructura de clave pública (en adelante, PKI) figuran todas las entidades que se relacionan, de alguna manera, con la gestión de certificados de clave pública.

La norma que regula la existencia de estas entidades y su modelo de relaciones es la ITU-T X.509.

2.1. ENTIDADES PARTICIPANTES

La entidad que emite un certificado de clave pública se denomina **Autoridad de Certificación** (en adelante **CA**, del inglés **Certification Authority**).

Acredita o certifica la identidad de una determinada entidad.

Existen dos atributos que la identifican: su nombre y su clave pública.

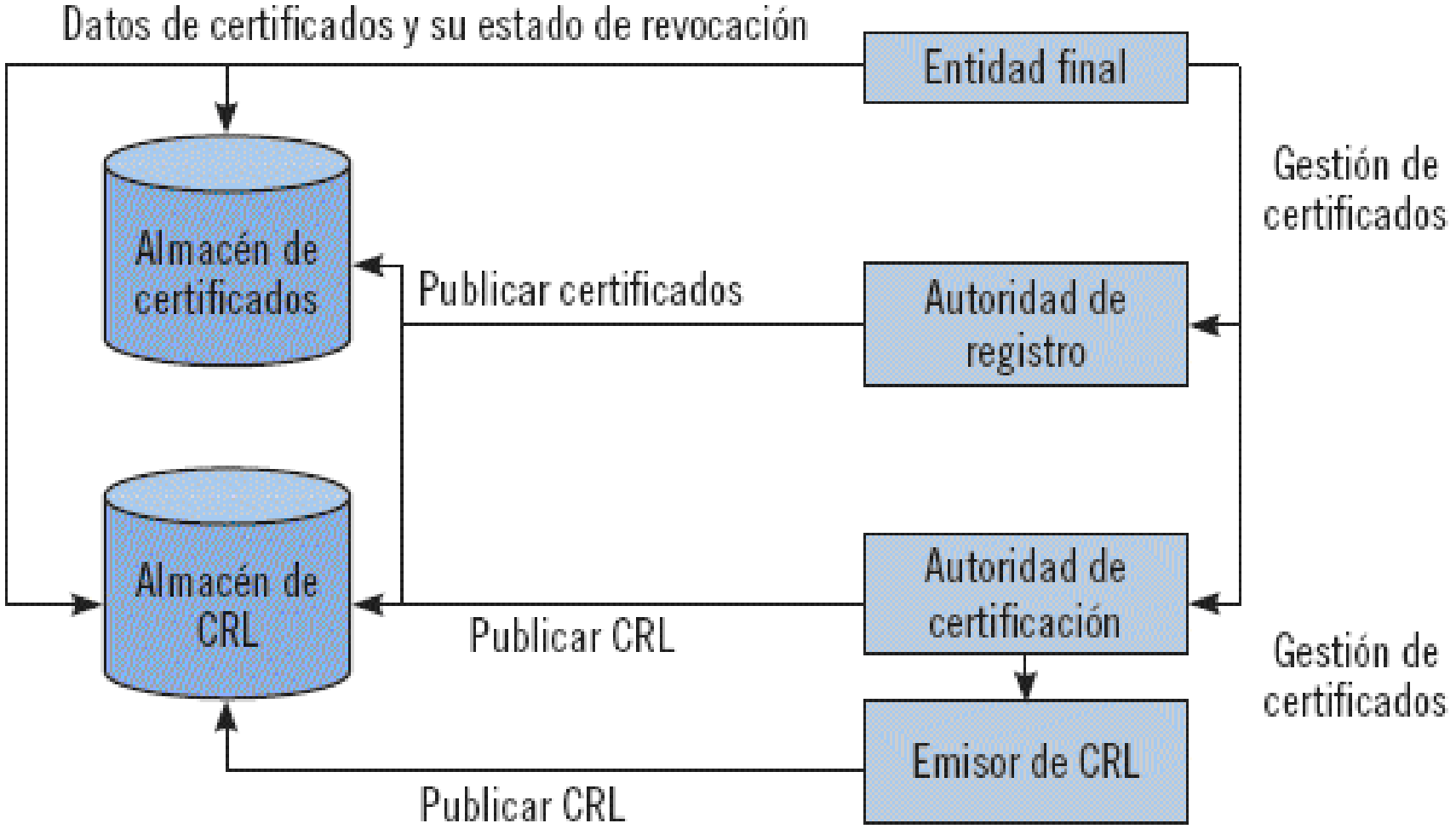
2.1. ENTIDADES PARTICIPANTES

Una CA realiza cuatro funciones fundamentales:

- Emitir certificados
- Mantener información actualizada sobre el estado de los certificados y emitir listas de certificados revocados
- Hacer públicos estos datos para que los usuarios puedan emplearlos en sus servicios de seguridad
- Mantener un archivo histórico sobre el estado de aquellos certificados que ya están caducados

2.1. ENTIDADES PARTICIPANTES

Elementos de una infraestructura de clave pública (PKI) [Adaptado de RFC 5280]



2.2. MODELO DE RELACIONES

Las autoridades en una PKI se relacionan habitualmente de manera jerárquica.

En el modelo jerárquico, se establece una CA raíz en la que se deposita toda la confianza.

Por debajo de esta CA pueden existir una o varias CA subordinadas, las cuales tienen la potestad de emitir y gestionar certificados digitales.

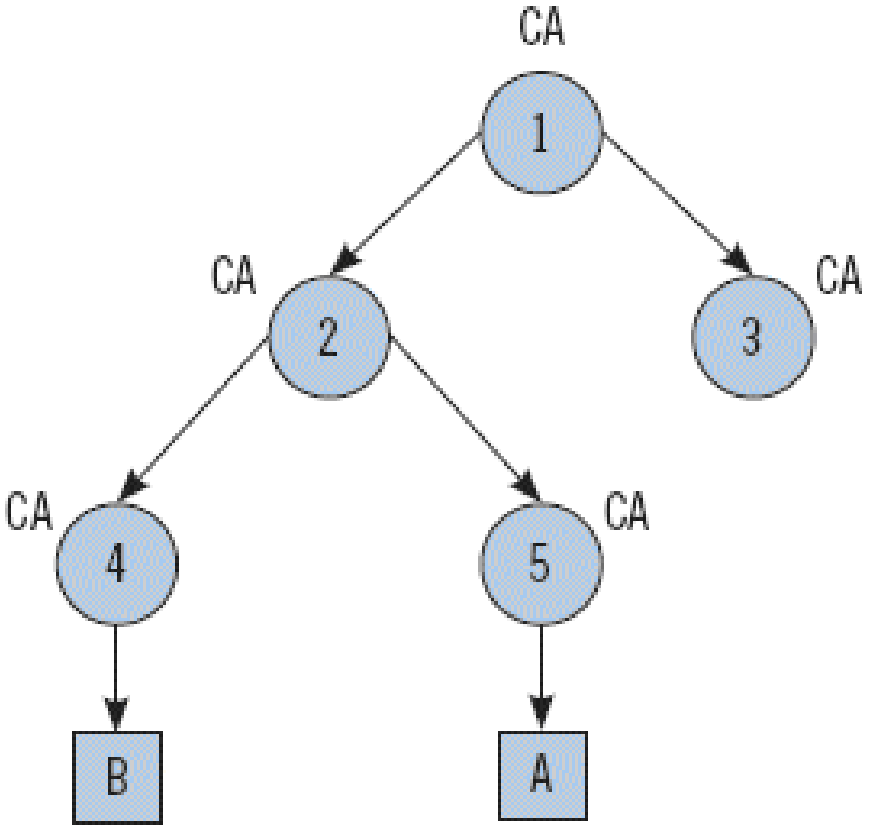
2.2. MODELO DE RELACIONES

2.3. ARQUITECTURAS DE UNA PKI

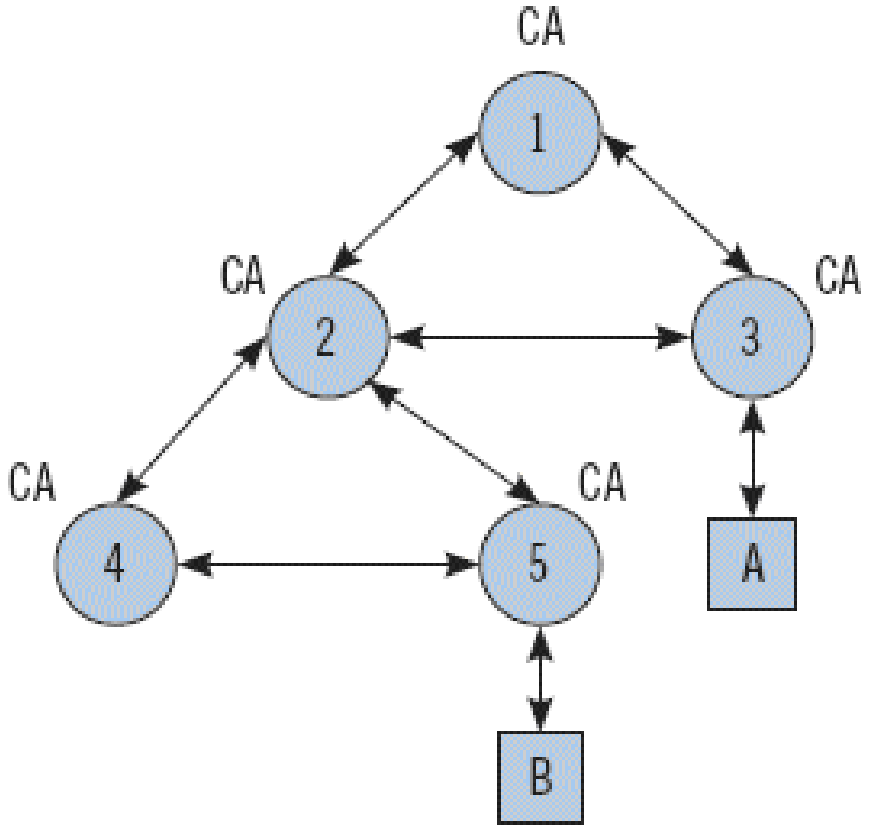
Tradicionalmente se puede distinguir, además de la arquitectura jerárquica introducida anteriormente, la arquitectura en red (mesh).

Además, para conseguir conectar dos PKI que están en distintas empresas entre las que se desea establecer un vínculo, se desarrolla la arquitectura de puente (bridge).

2.3. ARQUITECTURAS DE UNA PKI

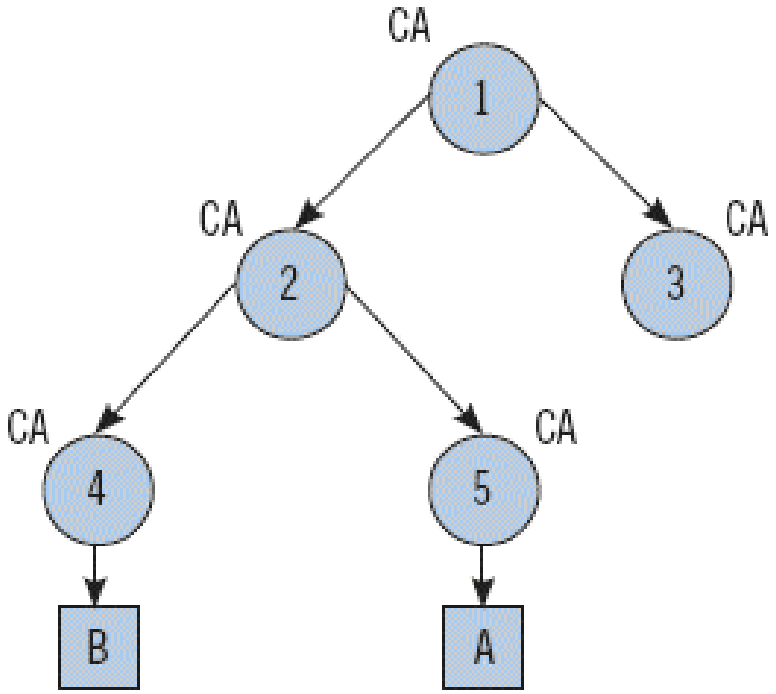


a) Jerarquía

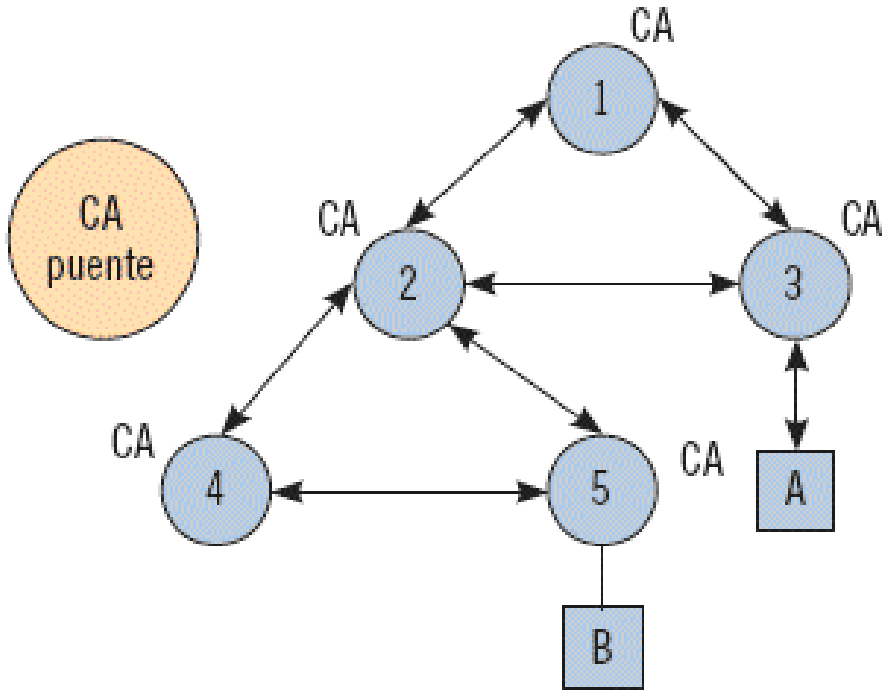


b) Red

2.3. ARQUITECTURAS DE UNA PKI

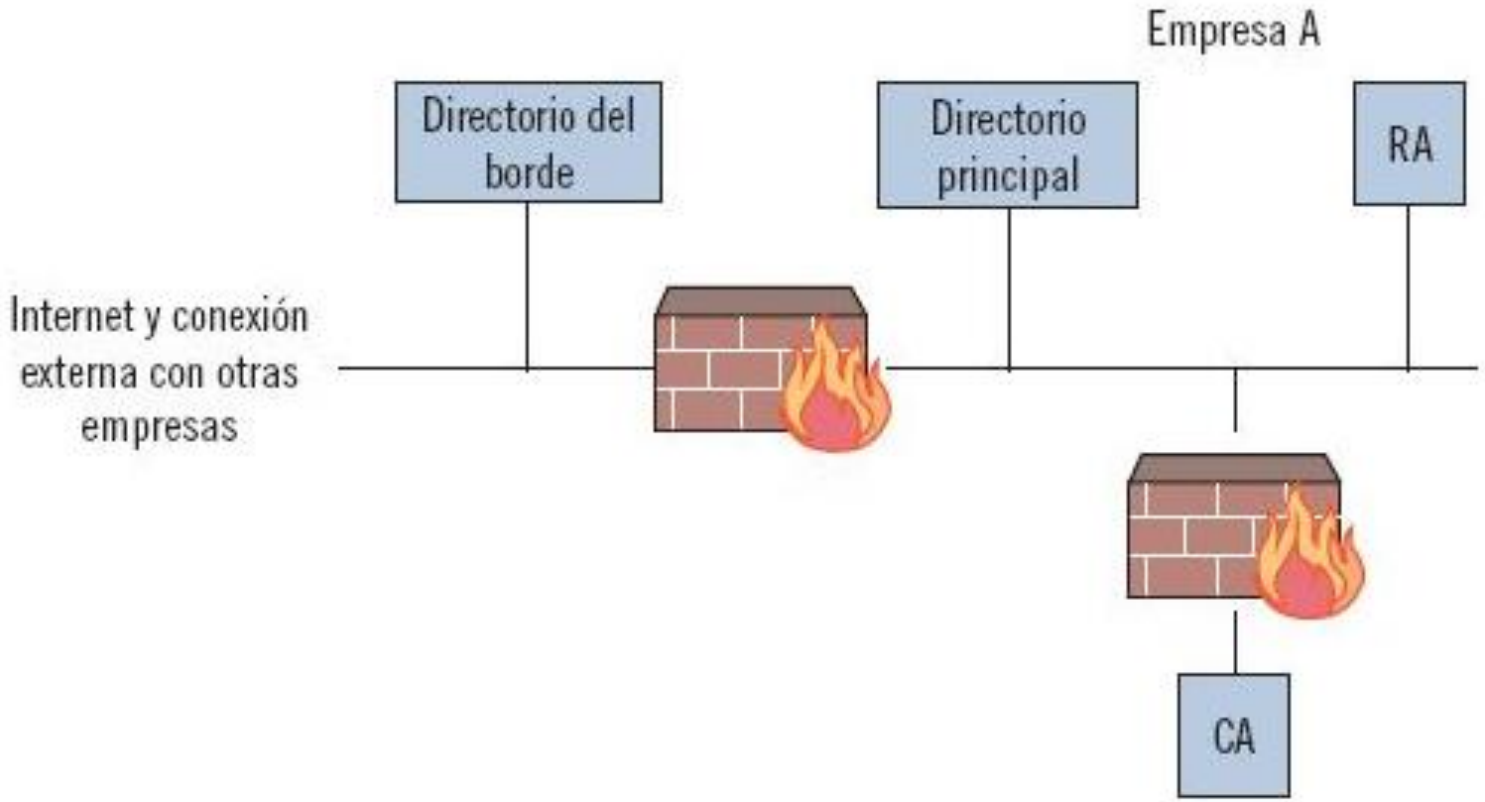


a) Jerarquía



b) Red

2.3. ARQUITECTURAS DE UNA PKI



3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

La CA se encarga de la gestión del ciclo de vida de los certificados que expide.

Dentro de ese ciclo de vida se identifican una serie de funciones de gestión.

3.1. FUNCIONES DE GESTIÓN

La norma X.509 establece 7 funciones de gestión que tienen lugar en las relaciones entre una entidad final (por ejemplo, un usuario) y la CA.

3.1. FUNCIONES DE GESTIÓN

Registro: constituye el primer acercamiento de la entidad a la CA.

Esencialmente, permite que esta se identifique frente a la CA.

De acuerdo a la descripción presentada anteriormente, esto puede realizarse directamente o a través de una entidad intermedia, tal como la Autoridad de Registro (AR).

3.1. FUNCIONES DE GESTIÓN

Certificación: en la que se emite el certificado de clave pública que acredita que la clave pública pertenece a la entidad correspondiente.

Dicho certificado puede enviarse directamente a la entidad final interesada, o puede ponerse a disposición de los usuarios en el repositorio mencionado anteriormente.

3.1. FUNCIONES DE GESTIÓN

Operaciones relacionadas con el mantenimiento del par de claves de la entidad final:

- **Copia de respaldo del par de claves.**
- **Actualización del par de claves.**

3.1. FUNCIONES DE GESTIÓN

Revocación de la clave:

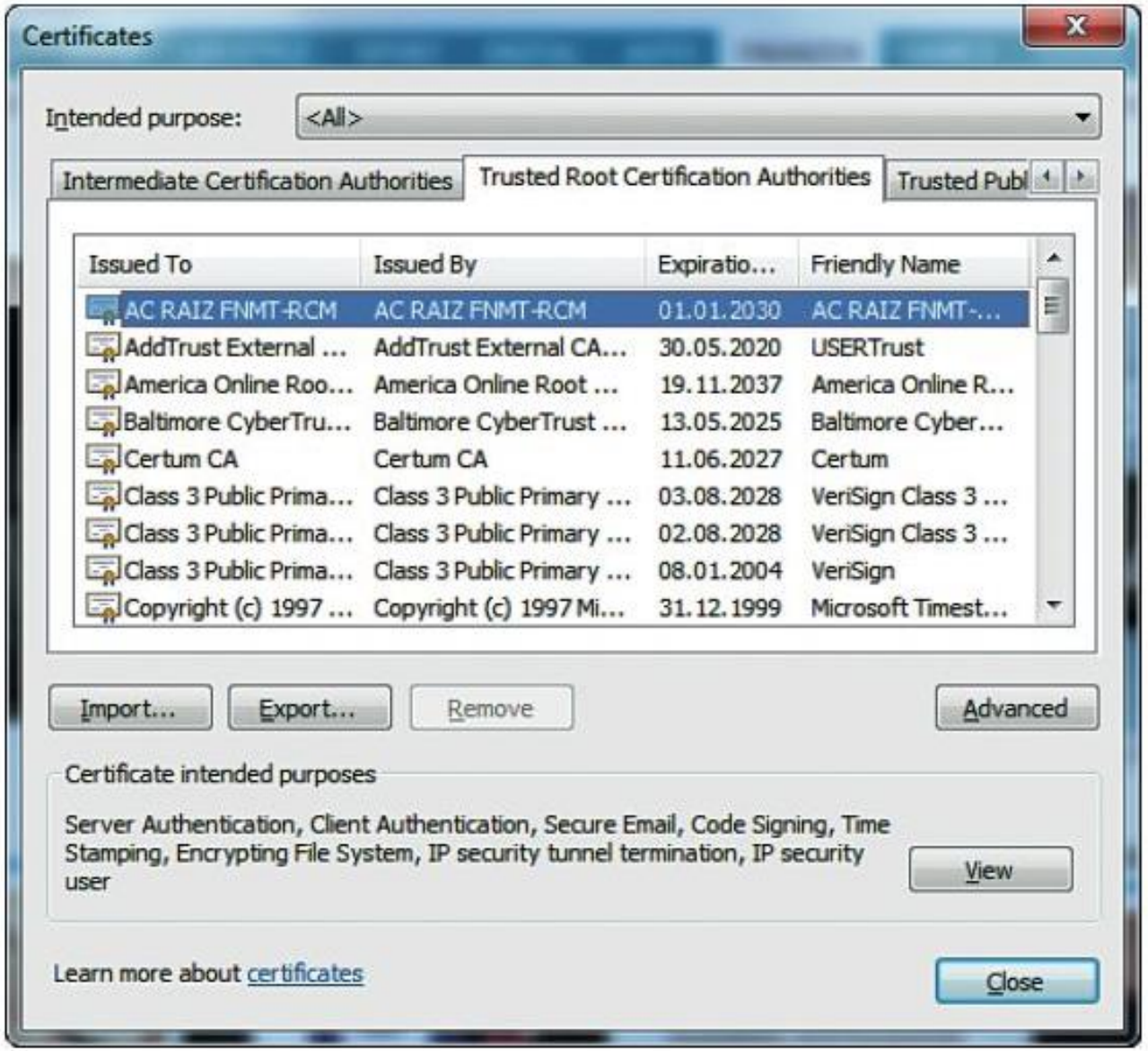
Tiene la misión de reducir los efectos de un posible ataque o pérdida de una clave.

3.1. FUNCIONES DE GESTIÓN

Certificación cruzada:

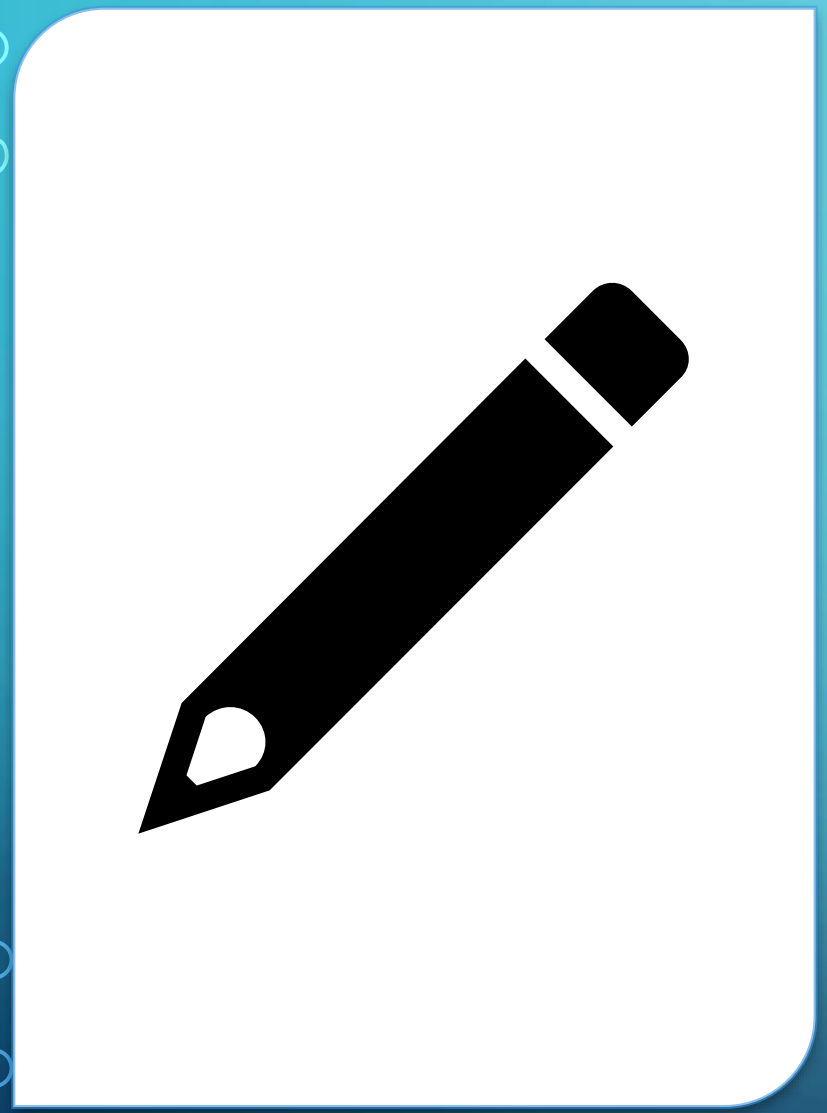
Posibilidad de que una CA pueda emitir un certificado para otra CA que le permita a la segunda emitir certificados que sean válidos también para la primera.

3.3. ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES



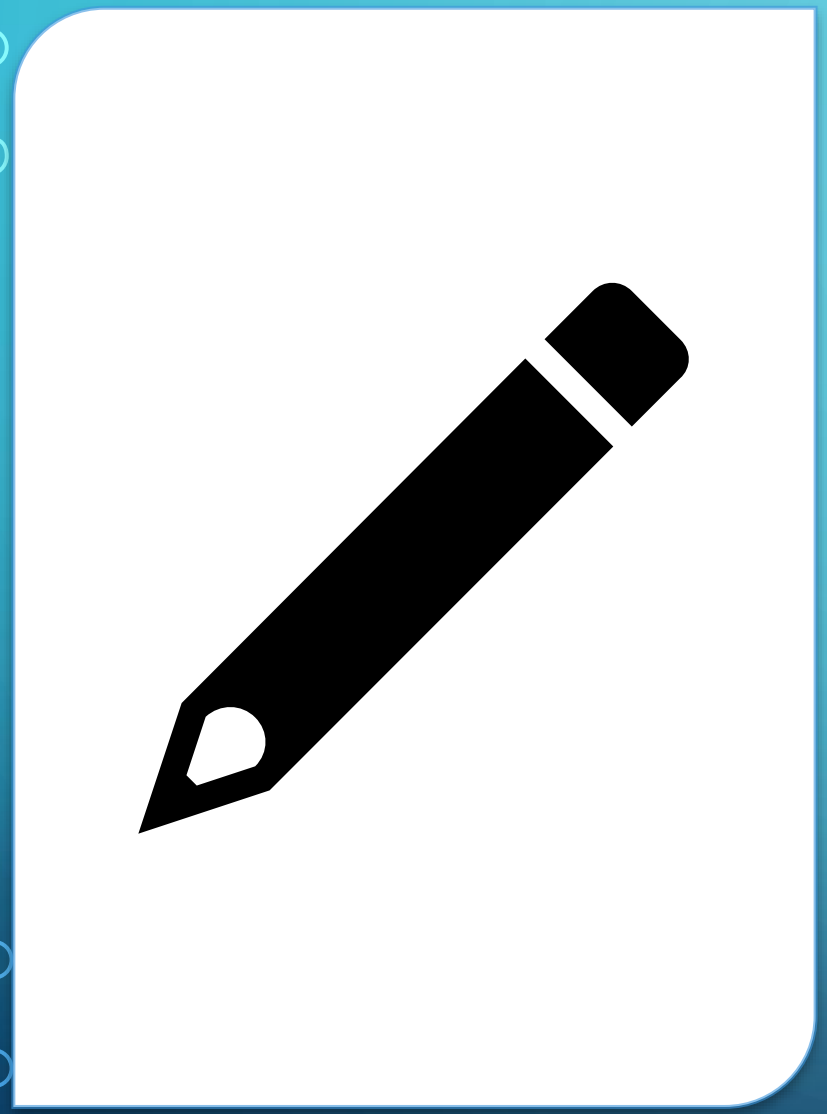
3.3. ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

3.3. ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES



Ejemplo.

MARIVÍ Y JOSÉ LUIS SON ASESORES DE SEGURIDAD LÓGICA DE UNA EMPRESA DE COMERCIO ELECTRÓNICO. DADO EL CRECIENTE NÚMERO DE CASOS DE FRAUDE ELECTRÓNICO, NECESITAN INCORPORAR UN MECANISMO QUE ASEGURE LA IDENTIDAD. SIN EMBARGO, CADA UNO TIENE UNA PROPUESTA DISTINTA. MARIVÍ OPINA QUE, PARA EVITAR QUE LOS CLIENTES ACCEDAN A PÁGINAS FALSAS, ES NECESARIO IMPLANTAR UNA PKI EN LA EMPRESA, DE FORMA QUE LA PÁGINA WEB TENGA UN CERTIFICADO EMITIDO POR ESA PKI. POR SU PARTE, JOSÉ LUIS CREE QUE ES IMPRESCINDIBLE QUE LOS USUARIOS SE AUTENTIQUEN UTILIZANDO UN CERTIFICADO Y, DADO QUE NO ES MUY HABITUAL QUE LOS CIUDADANOS TENGAN UNO, PLANTEA QUE PUEDAN SER CERTIFICADOS AUTO-FIRMADOS. CADA UNO IDENTIFICA PROBLEMAS EN LA ALTERNATIVA DEL OTRO. ¿PODRÍA INDICAR CUÁLES SON?



Ejemplo. Solución.

AMBAS PROPUESTAS TIENEN UN MISMO PUNTO DÉBIL: LA CONFIANZA EN LA CA QUE EMITE EL CERTIFICADO.

LA PROPUESTA DE MARIVÍ ESTÁ BIEN ENCAMINADA EN TANTO QUE LA SUPLANTACIÓN ES UNA DE LAS PRINCIPALES AMENAZAS DEL COMERCIO ELECTRÓNICO. NO OBSTANTE, SI LA PKI ES LA PROPIA EMPRESA, NO FIGURARÁ ENTRE LAS CA DE CONFIANZA QUE VIENEN PRE-INSTALADAS EN LOS NAVEGADORES. ESTO CAUSARÁ QUE LOS USUARIOS OBSERVEN MENSAJES DE ADVERTENCIA Y POSIBLEMENTE RECELEN DE LA PÁGINA WEB.

POR SU PARTE, LA PROPUESTA DE JOSÉ LUIS TIENE COMO DEFECTO QUE SI LOS CERTIFICADOS SON AUTO-FIRMADOS, SERÁN CREADOS POR LOS PROPIOS USUARIOS. EN OTRAS PALABRAS, CADA USUARIO SE CONVIERTE EN SU PROPIA PKI. EL PROBLEMA NUEVAMENTE ES QUE NO EXISTE CONFIANZA EN LA PKI: NADIE ASEGURA QUE EXISTA UNA VINCULACIÓN ENTRE LA CLAVE PÚBLICA Y LA IDENTIDAD QUE APARECE EN EL CERTIFICADO.

4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)

En base a la RFC 3647, de carácter informativo, se describen los conceptos de

- **Política de Certificación (en adelante CP del inglés Certification Policy, CP)**
- **Declaración de Prácticas de Certificación (del inglés Certification Policy Statement, CPS**

4.1. POLÍTICA DE CERTIFICACIÓN

En el estándar X.509 una CP se define como "un conjunto de reglas que indican la aplicación de un certificado en una comunidad y / o en un tipo de aplicación con objetivos comunes de seguridad".

Dos categorías:

- **CP que indican la aplicación de un certificado en una comunidad concreta.**
- **CP que indican la aplicación de un certificado a un tipo de aplicación con unos objetivos comunes de seguridad.**

4.2. DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

CPS se define como "declaración de las prácticas que una CA ha de realizar a la hora de expedir certificados".

La CPS establece las prácticas en base al ciclo de vida de los servicios con los que se asocie, incluyendo la emisión, la revocación y la renovación de certificados.

4.3. DIFERENCIAS ENTRE CP Y CPS

- El objetivo de la CP es establecer qué deben hacer los participantes. En cambio, la CPS determina cómo una CA y sus participantes, en un determinado dominio, implementan los procedimientos y controles para satisfacer los requisitos establecidos por la CP.

- CP sirve para transmitir mínimas guías de operación a seguir por PKI que son compatibles (interoperables) entre sí. Por tanto, una CP es generalmente aplicable a múltiples CA, organizaciones o dominios. Por el contrario, una CPS es aplicable a una única CA u organización, la cual no es generalmente utilizada para facilitar interoperabilidad.

- Una CPS generalmente incluye más detalle que una CP y especifica cómo las CA han de satisfacer los requisitos establecidos en una o varias CP bajo los cuales emiten los certificados.

4.4. PROVISIONES: POLÍTICA DE CERTIFICACIÓN Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

La norma RFC 3647, establece el contenido de un conjunto de provisiones :

- **Introducción.**
- **Publicación y repositorio.**
- **Identificación y autenticación.**
- **Ciclo de vida de los certificados, requisitos operaciones.**
- **Facilidades, gestión y controles de operación.**
- **Controles técnicos de seguridad.**
- **Perfiles de certificado, CRL y OCSP.**
- **Auditoría de cumplimiento.**
- **Otros asuntos legales y de negocio.**