SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.2.2.MF0489_3. Capítulo 2
Parte 2
Infraestructura de clave pública

JOSÉ PABLO HERNÁNDEZ

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

Razones de revocación de un certificado según X.509:

- Inespecífica, ninguna razón se señala.
- La clave privada asociada al certificado es comprometida.
- La clave privada de la CA que emitió certificados es comprometida.
- El propietario del certificado rompe el vínculo con el emisor del certificado y o no tiene derecho de acceso al mismo o no lo necesita.
- Otro certificado reemplaza a uno existente.
- La CA que emitió un certificado deja de ser operable.
- Un certificado se mantiene a la espera de alguna acción. En este estado se considera revocado hasta el momento en que sea activado y nuevamente válido.

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

El uso de los certificados implica la verificación de los mismos, para lo cual, además de verificar su fecha de expiración, la firma de las CA correspondientes, etc., es imprescindible verificar si es o no un certificado revocado.

La verificación se realiza verificando la existencia del certificado concreto en una lista, conocida como lista de certificados revocados (del inglés Certificate Revocation List, CRL) en la que, como su propio nombre indica, se almacenan todos los certificados que han sido revocados, identificados por su número de serie.

5.1. FORMATO DE UNA LISTA DE REVOCACIÓN DE CERTIFICADOS

La CRL X.509 está compuesta por los siguientes campos:

- **Algoritmo de firma**
- **Valor de la firma**
- **Nombre emisor**
- **Día de emisión**
- **Día emisión nueva lista**
- **Lista de certificados revocados**
- **Extensiones**

5.2. CONCEPTO DE DELTA CRL

La CRL se publica periódicamente. Este modo de funcionamiento introduce un problema práctico de máxima importancia: cómo difundir, en el intervalo entre dos CRL, los certificados que quedan revocados.

Para paliar esta situación se definieron las Delta CRL o, lo que es lo mismo, fragmentos reducidos de CRL que contienen los certificados revocados desde la última lista publicada.

5.3. ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

OCSP, definido en la RFC 2560, es un protocolo también utilizado en la revocación de los certificados X.509, el cual se desarrolló como alternativa a las CRL.

El propósito de OCSP es facilitar la verificación en línea de los certificados evitando posibles fallos en el proceso de revocación debido a CRL desactualizadas.

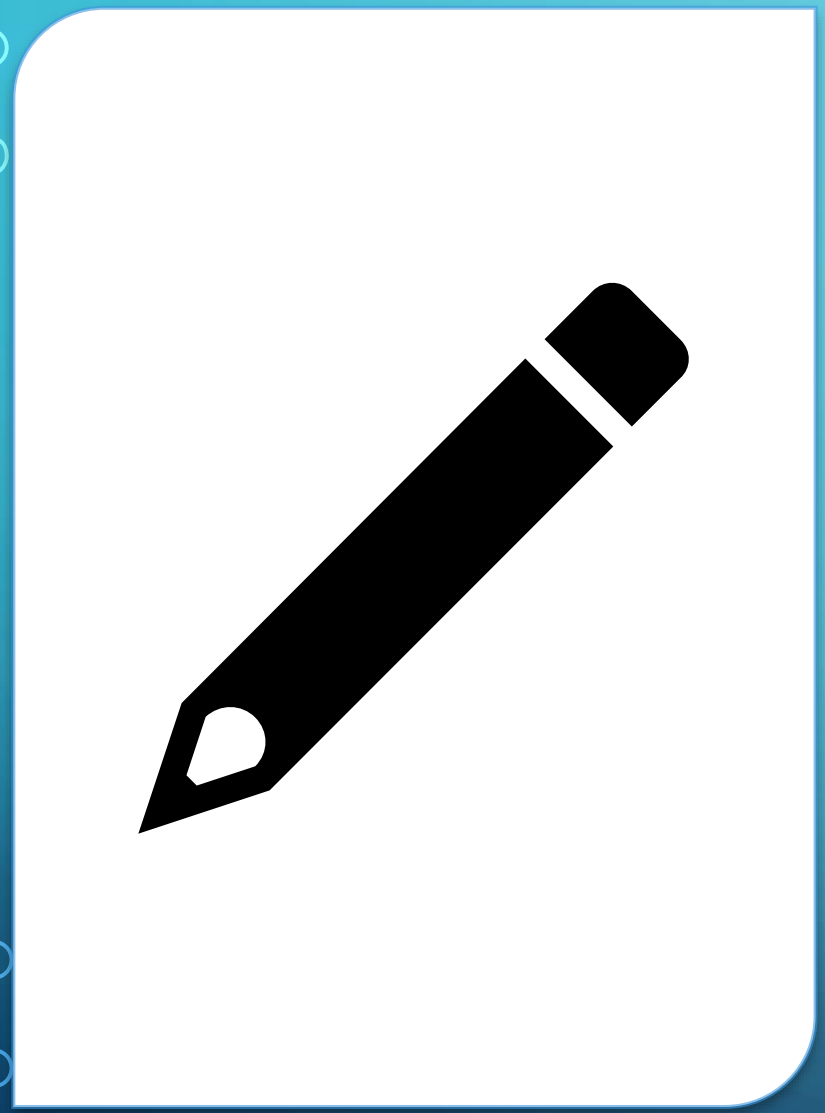
5.3. ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

La comunicación entre cliente y servidor se compone de un par de mensajes:

- **Solicitud**
- **Respuesta**

Ejemplo.

SE DISPONE DE UN SISTEMA DE APRENDIZAJE ONLINE EN EL QUE LOS USUARIOS DE LA UNIVERSIDAD DE ARAGÓN, LOS CUALES TIENEN LAS CREDENCIALES DE ACCESO ADECUADAS, PUEDEN REGISTRARSE Y BAJARSE EL MATERIAL ASOCIADO A CADA UNA DE LAS ASIGNATURAS EN LAS QUE ESTÁN MATRICULADOS. EL CONTENIDO DE CADA ASIGNATURA ES ACTUALIZADO DIARIA O SEMANALMENTE PARA QUE LOS ALUMNOS ACCEDAN A ELLA. EL SISTEMA OFRECE A LOS USUARIOS LA POSIBILIDAD DE DESCARGARSE TODA LA INFORMACIÓN RELATIVA A CADA UNA DE LAS ASIGNATURAS, ASÍ COMO DE ENVIAR MENSAJES INSTANTÁNEOS ENTRE LOS USUARIOS DE LAS ASIGNATURAS Y EL PROFESOR DE LAS MISMAS. TENIENDO EN CUENTA TODO LO COMENTADO Y SABIENDO QUE LOS USUARIOS HACEN USO DE UN CERTIFICADO CADA VEZ QUE SE REGISTRAN EN EL SISTEMA, ASÍ COMO ASUMIENDO QUE SE DISPONE DE UN ÚNICO SERVIDOR OCSP EN EL QUE TODOS LOS USUARIOS CONFÍAN, INDIQUE LAS VENTAJAS E INCONVENIENTES DE APLICAR UNA CRL U OCSP.



Ejemplo. Solución.

DADO QUE EL SISTEMA PROPORCIONADO DISPONE DE INFORMACIÓN DE TODAS LAS ASIGNATURAS EN LAS QUE UN ALUMNO ESTÁ MATRICULADO, ES ESPERABLE QUE LOS USUARIOS ACCEDAN AL SISTEMA CON MUCHA FRECUENCIA. POR EJEMPLO, ES POSIBLE QUE ACCEDAN DIARIAMENTE O INCLUSO CON UNA FRECUENCIA MAYOR. POR TANTO, ESTE HECHO PODRÍA HACER PENSAR EN LA UTILIDAD DE CRL. SI LAS VERIFICACIONES SE HACEN SOBRE UNA CRL SE EVITA SOBRECARGAR AL SERVIDOR OCSP CON MUCHAS PETICIONES. SIN EMBARGO, JUSTO POR ESA MISMA SITUACIÓN, ES DECIR, POR LA GRAN CANTIDAD DE ACCESOS QUE SE ESPERAN, ES IMPORTANTE REALIZAR UNA VERIFICACIÓN EN LÍNEA DE LOS CERTIFICADOS. POR EJEMPLO, SI UN USUARIO ACCEDE DIARIAMENTE, O N VECES AL DÍA AL SISTEMA, SE HA DE GARANTIZAR QUE SU CERTIFICADO ES VÁLIDO EN TODO MOMENTO, SIENDO DESEABLE EL USO DE OCSP.

6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)

La solicitud de firma de un certificado (del inglés Certificate Signing Request, CSR), es un formato para realizar la solicitud de certificados, definidos en el estándar PKCS#10/RFC 2986.

6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

Las infraestructuras de gestión de privilegios, habitualmente referidas por sus siglas en inglés PMI (de Privilege Management Infrastructure), permiten administrar de manera eficaz los permisos o acciones que una determinada entidad está autorizada a realizar.

El mecanismo con el que se instrumenta la concesión de privilegios son los certificados de atributos.

7.1. ENTIDADES PARTICIPANTES

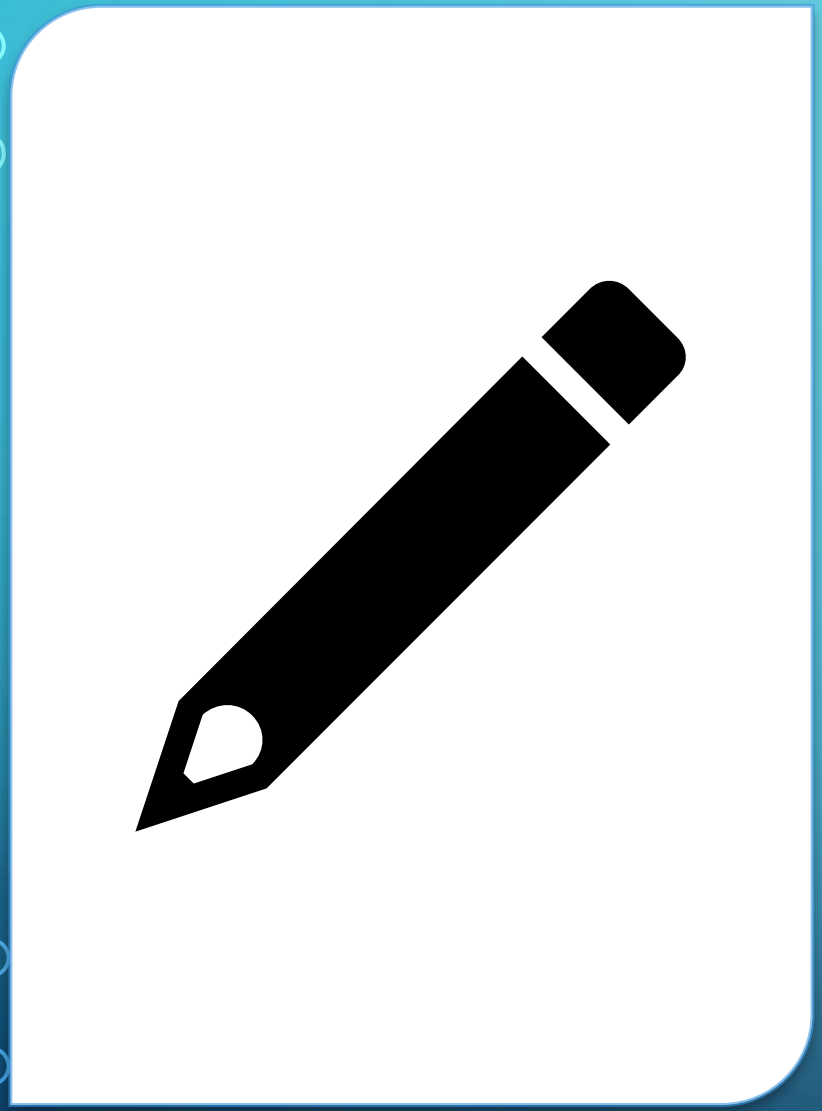
De acuerdo a la norma X.509:

- **Fuente de Autoridad (más conocida por su acrónimo en inglés Source Of Authority, SOA).**
- **El titular del certificado puede tener la capacidad para transferir el privilegio: AA y PH.**
- **El verificador (en inglés, Privilege Verifier) comprueba la validez y vigencia del certificado.**
- **Lista de Certificados de Atributos Revocados (comúnmente ACRL, del inglés Attribute Certificate Revocation List).**

7.2. PROCESO DE VERIFICACIÓN DE PRIVILEGIOS

El proceso de verificación comprende las siguientes acciones:

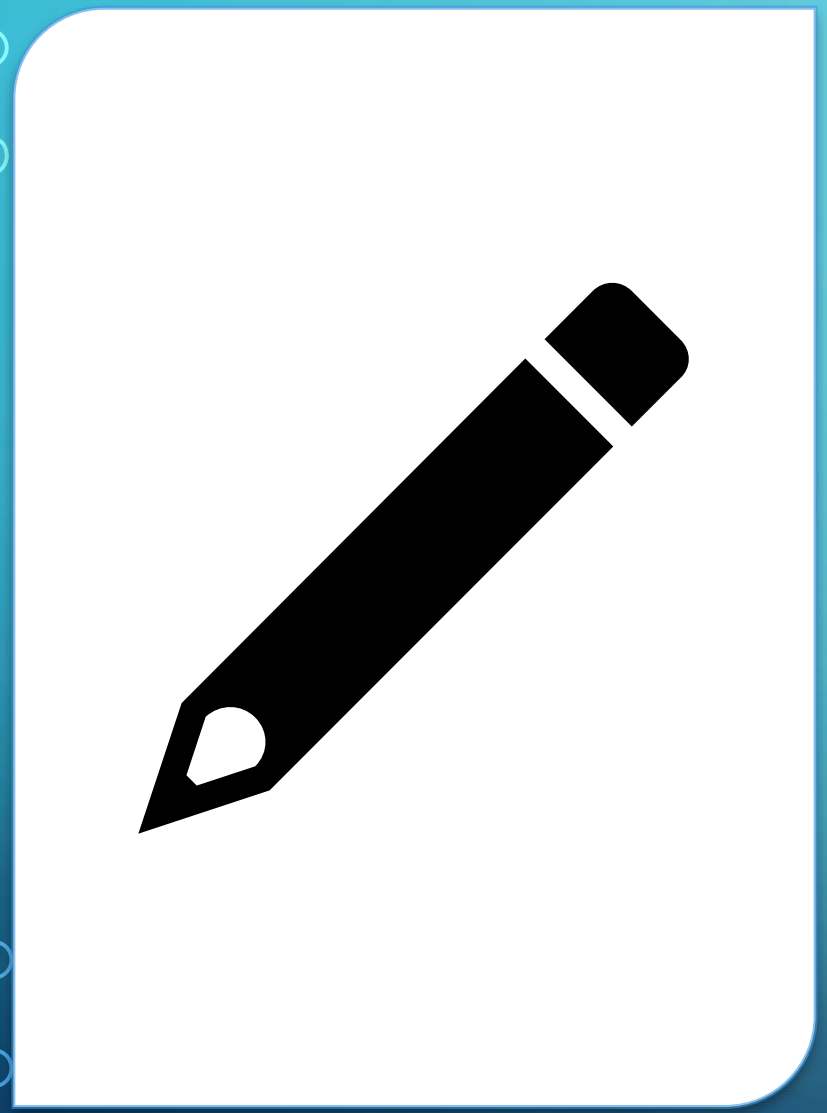
- El propietario del privilegio solicita realizar una determinada acción sobre un recurso.
- El verificador comprueba que los atributos (privilegios) del solicitante se ajustan a los necesarios para realizar la acción.
- El verificador establece ahora la vigencia del certificado de atributos, para lo que efectúa dos acciones principales:
  - Comprobar la validez de la cadena de certificación.
  - Comprobar si el certificado está revocado de acuerdo a la lista de certificados de atributos revocados publicada por la SOA.



Ejemplo.

JUAN DISPONE DE UN CERTIFICADO DE CLAVE PÚBLICA. UN DÍA A JUAN LE ROBAN SU ORDENADOR, CON TAL MALA SUERTE QUE EN ÉL SE ENCONTRABAN TANTO SU CERTIFICADO COMO LA CLAVE PRIVADA ASOCIADA. ¿QUÉ TIENE QUE HACER JUAN? ¿QUÉ ELEMENTO SE VE AFECTADO Y CÓMO AFECTA DICHO CAMBIO? ADEMÁS, EL DÍA DEL ROBO JUAN TENÍA QUE ENVIAR AL DIRECTOR DE LA EMPRESA EN LA QUE TRABAJABA UNA PROPUESTA DE UN PROYECTO DE GRAN ENVERGADURA. DADA LA RELEVANCIA DEL PROYECTO, JUAN TENÍA QUE ENVIAR LA PROPUESTA FIRMADA Y CIFRADA.

¿QUÉ PASOS TUVO QUE REALIZAR JUAN PARA CONSEGUIR ENVIAR EL DOCUMENTO FIRMADO Y CIFRADO?



Ejemplo. Solución.

UNA VEZ QUE JUAN IDENTIFICA QUE SU CLAVE PRIVADA, PUEDE ESTAR COMPROMETIDA, HA DE REALIZAR LA REVOCACIÓN DEL CERTIFICADO, LO CUAL TIENE UN EFECTO DIRECTO EN LA LISTA DE REVOCACIÓN DE CERTIFICADOS. EL CERTIFICADO QUE JUAN HA REVOCADO SERÁ INCLUIDO EN LA LISTA.

POR OTRO LADO, PARA ENVIAR LA PROPUESTA FIRMADA Y CIFRADA NECESITA UN NUEVO CERTIFICADO. EL PROCESO COMIENZA REALIZANDO UNA SOLICITUD DE CERTIFICADO A UNA AC O UNA AR DELEGADA. POSTERIORMENTE, CREA UN PAR DE CLAVES (PÚBLICO Y PRIVADA) Y PREPARA LA SOLICITUD DEL CERTIFICADO. LA SOLICITUD ES FIRMADA Y CONTIENE EL NOMBRE, JUAN, LA CLAVE PÚBLICA CREADA Y EL ALGORITMO DE FIRMA (ADEMÁS DE OTROS POSIBLES ATRIBUTOS). POSTERIORMENTE, LA SOLICITUD ES ENVIADA A UNA CA O AR DELEGADA, LA CUAL VERIFICARÁN SU IDENTIDAD, ASÍ COMO LA FIRMA, Y EN CASO DE SER VÁLIDO, LA SOLICITUD SERÁ ENVIADA A LA CA CORRESPONDIENTE PARA QUE CREE EL CERTIFICADO. FINALMENTE, CUANDO JUAN DISPONGA DEL CERTIFICADO, UNA VEZ QUE ESTÉ CONVENIENTEMENTE INSTALADO EN SU NUEVO ORDENADOR, HACIENDO USO DEL PROGRAMA CONVENIENTE (EJ. MICROSOFT WORD O ADOBE ACROBAT) PODRÁ REALIZAR TANTO LA FIRMA COMO EL CIFRADO DEL DOCUMENTO.

7.3. APLICACIÓN DE PMI PARA EL CONTROL DE ACCESO

Una de las aplicaciones más habituales de los PMI es en los sistemas de control de acceso.

Uno de los modelos clásicos de control de acceso es el modelo discrecional (DAC, del inglés Discretionary Access Control), en el que la asignación de privilegios a personas y recursos se hace de forma particularizada.

7.4. COMPARACIÓN CON RESPECTO A UNA PKI

- Se centran en la gestión de certificados.
- Concepto de jerarquía de entidades.
- Gestión de la revocación.

8. CERTIFICADOS DE ATRIBUTOS

Una vez conocido el concepto de CA, este apartado presenta los campos que contiene, así como sus usos más habituales y las diferencias con respecto a los certificados digitales.

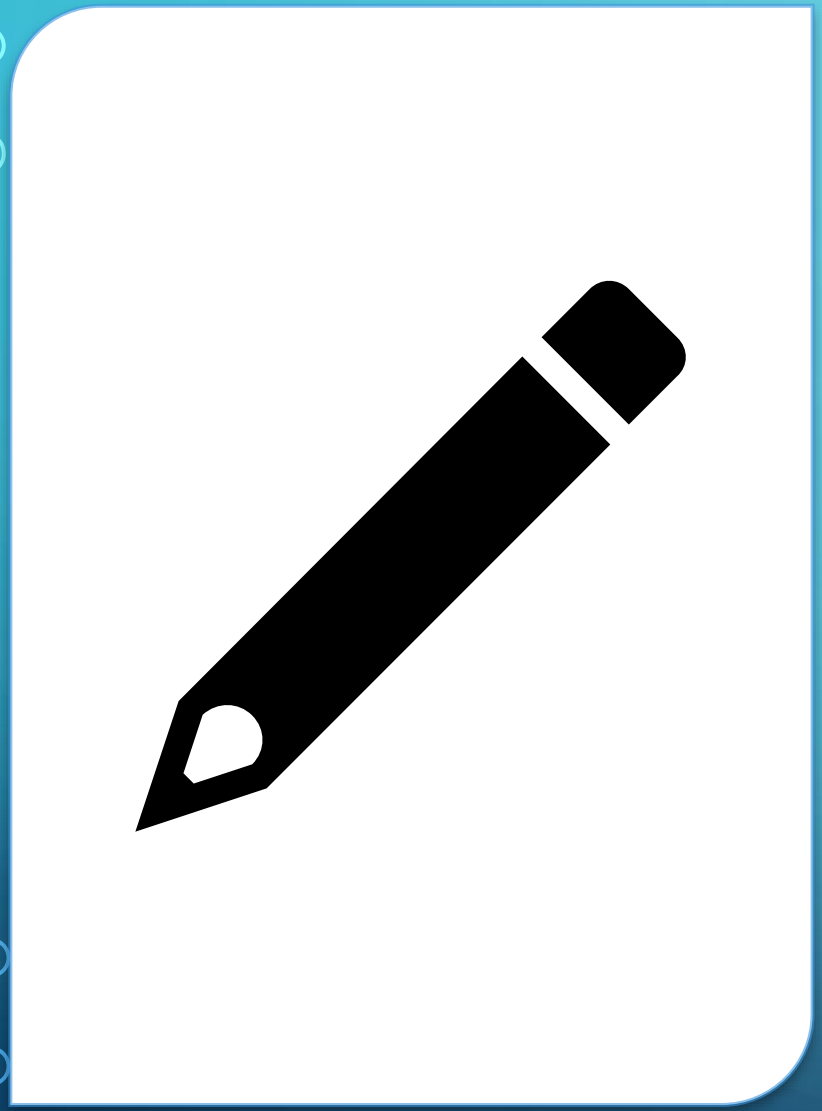
8.1. CAMPOS DE LOS CERTIFICADOS DE ATRIBUTOS

- Versión.
- Propietario (holder.
- Nombre del emisor.
- Algoritmo de firma.
- Firma.
- Número de serie.
- Periodo de validez.
- Atributos:
  - Identificador único del emisor.
  - Extensiones.

8.1. CAMPOS DE LOS CERTIFICADOS DE ATRIBUTOS

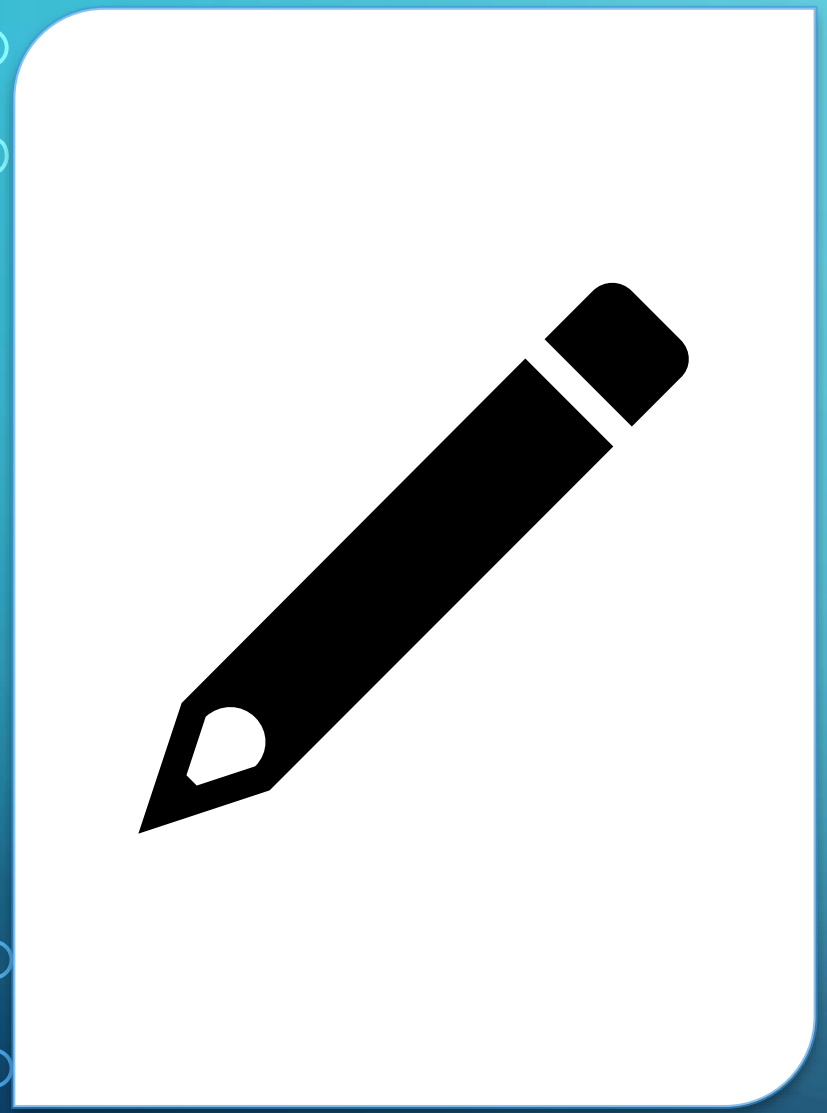
Tipos de atributos:

- **Servicio de autenticación de la información.**
- **Identidad de acceso.**
- **Identidad de cobro (charging identity).**
- **Grupo.**
- **Rol.**
- **Autorización (clearance).**



Ejemplo.

MARÍA TERESA ES DESIGNADA PERITA JUDICIAL EN UN CASO DE CORRUPCIÓN POLÍTICA, DONDE TAMBIÉN ACTÚAN LOS ACUSADOS Y EL JUEZ. COMO LOS DATOS QUE SE MANEJAN EN LA INVESTIGACIÓN SON SECRETOS, ES NECESARIO ESTABLECER UN MODELO DE CONTROL DE ACCESO ADECUADO. LOS RECURSOS CONSIDERADOS SON LA CAUSA DE IMPUTACIÓN (PÚBLICA), LOS INFORMES PERICIALES (CREADOS POR LOS PERITOS) Y LA SENTENCIA JUDICIAL (ESCRITA POR EL JUEZ). EMPLEANDO EL MODELO MULTINIVEL, DETERMINE QUÉ CERTIFICADOS DE ATRIBUTOS DEBEN EMITIRSE, Y CON QUÉ PERMISOS (LECTURA O ESCRITURA).



Ejemplo. Solución.

SE IDENTIFICAN TRES NIVELES DE INFORMACIÓN: “PÚBLICO” (LA CAUSA DE IMPUTACIÓN), “INTERMEDIO” (LOS INFORMES PERICIALES) Y “CONFIDENCIAL” (LA SENTENCIA).

LOS IMPUTADOS DEBEN TENER UN CERTIFICADO DE ATRIBUTOS QUE LES PERMITA LEER EN EL NIVEL “PÚBLICO”.

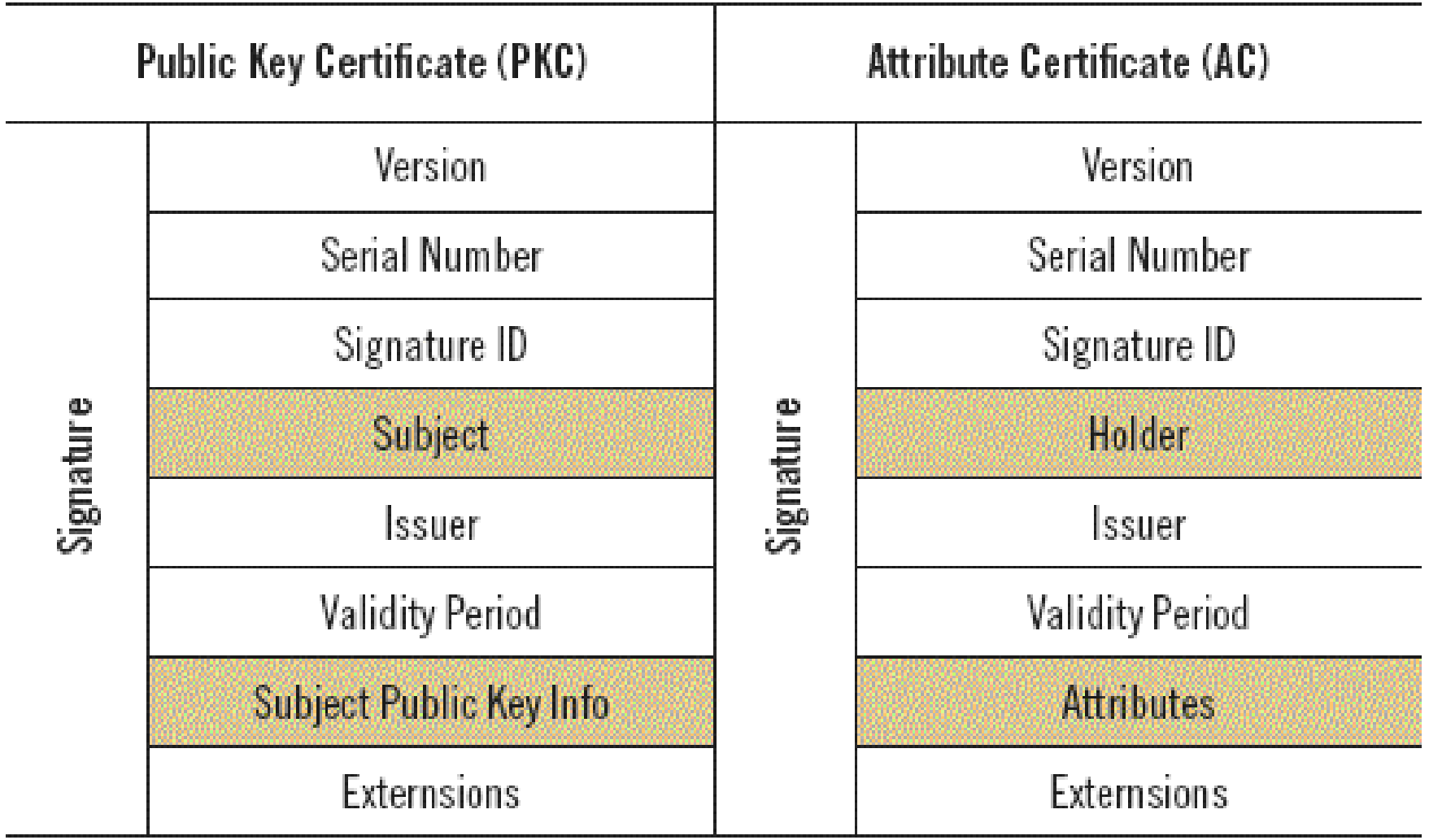
Mª TERESA DEBE PODER ACCEDER TANTO AL NIVEL “PÚBLICO” (PARA LECTURA) COMO AL NIVEL “INTERMEDIO” (PARA LECTURA Y ESCRITURA).

FINALMENTE, EL JUEZ DEBE PODER ACCEDER TANTO AL NIVEL “PÚBLICO” (PARA LECTURA Y ESCRITURA), COMO AL “INTERMEDIO” (PARA LECTURA) Y AL “CONFIDENCIAL” (PARA LECTURA Y ESCRITURA).

8.2. USOS HABITUALES DE LOS CERTIFICADOS DE ATRIBUTOS

Los certificados de atributos se pueden utilizar en gran variedad de servicios, entre los que se incluyen el control de acceso, la autenticación en el origen y el no repudio.

8.3. CERTIFICADOS DIGITALES FRENTE A CERTIFICADOS DE ATRIBUTOS



8.4. MODOS DE USO DE LOS CERTIFICADOS DE ATRIBUTOS

De acuerdo a la RFC 3281, que describe la aplicación de los certificados de atributos para la autorización de entidades, se identifican dos formas en las que se pueden emplear los certificados de atributos:

- **Modelo push**
- **Modelo pull**

9. APLICACIONES DE UNA PKI

Las aplicaciones fundamentales de las PKI son:

- **Autenticación**
- **Firma electrónica**
- **Cifrado**

9.1. USO DE PKI PARA AUTENTICACIÓN

La PKI es una alternativa más segura al par usuario/contraseña, en la que la autenticación se produce probando la posesión de una clave privada en lugar de una contraseña, la cual puede verse comprometida con cierta facilidad.

9.2. USO DE PKI EN FIRMA

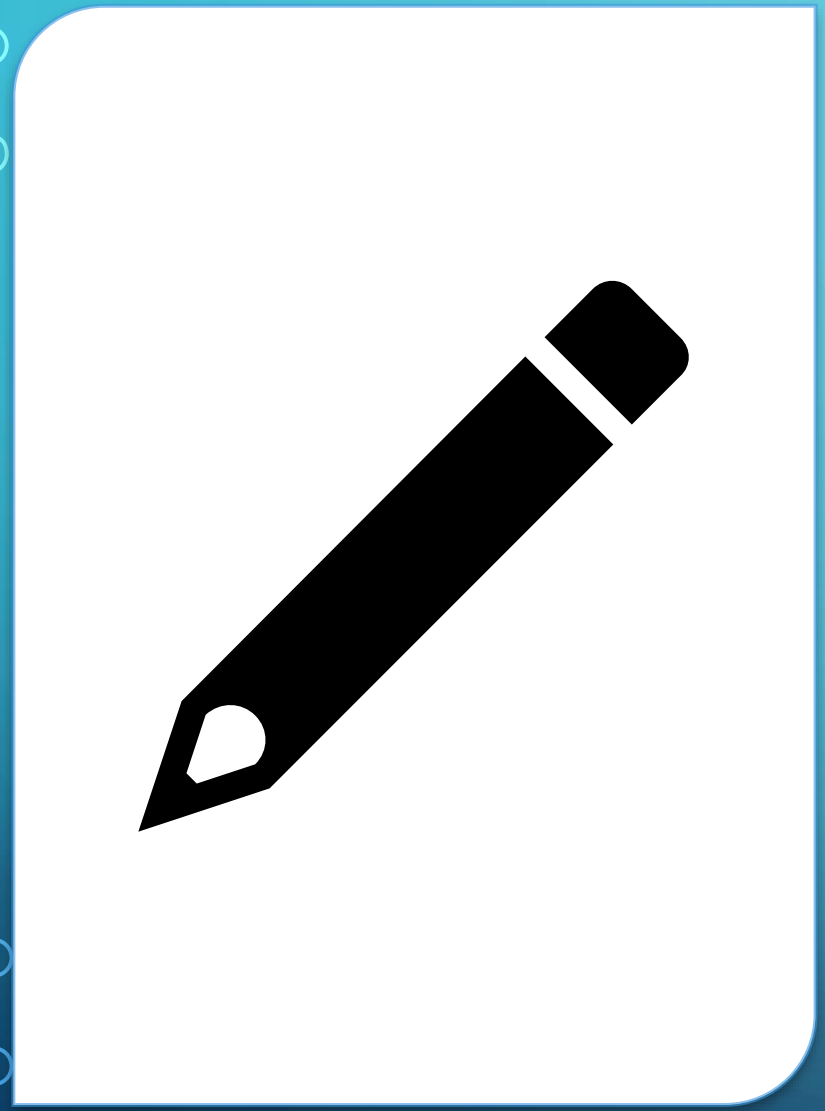
La firma digital es otra de las aplicaciones más frecuentes de las PKI, las cuales se pueden definir como un esquema matemático que permite demostrar la autenticidad de un mensaje digital. En el mundo digital, la firma de documentos (especialmente XML) así como los correos electrónicos, constituyen claros ejemplos de esta aplicación.

9.3. USO DE PKI PARA CIFRADO

La PKI es frecuentemente utilizada para el cifrado de datos.

Cualquier usuario puede cifrar datos pero estos solo podrán ser descifrados por los usuarios que dispongan de las claves de descifrado.

Ejercicios.



4.2.100.1.MF0489_3_EJERCICIOSCAPITULO_2.DOCX