IFCT0109. SEGURIDAD INFORMÁTICA

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

UD02

APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

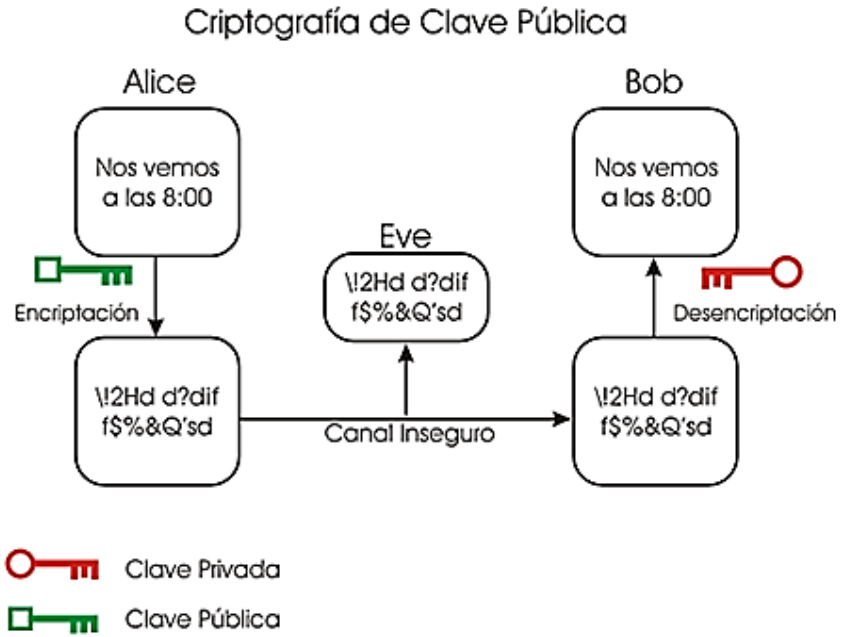
CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

1. INTRODUCCIÓN

LA APARICIÓN DE LA **CRIPTOGRAFÍA DE CLAVE PÚBLICA** EN 1976 SUPUSO EL NACIMIENTO DE UN NUEVO PARADIGMA EN EL ASEGURAMIENTO DE LAS COMUNICACIONES.

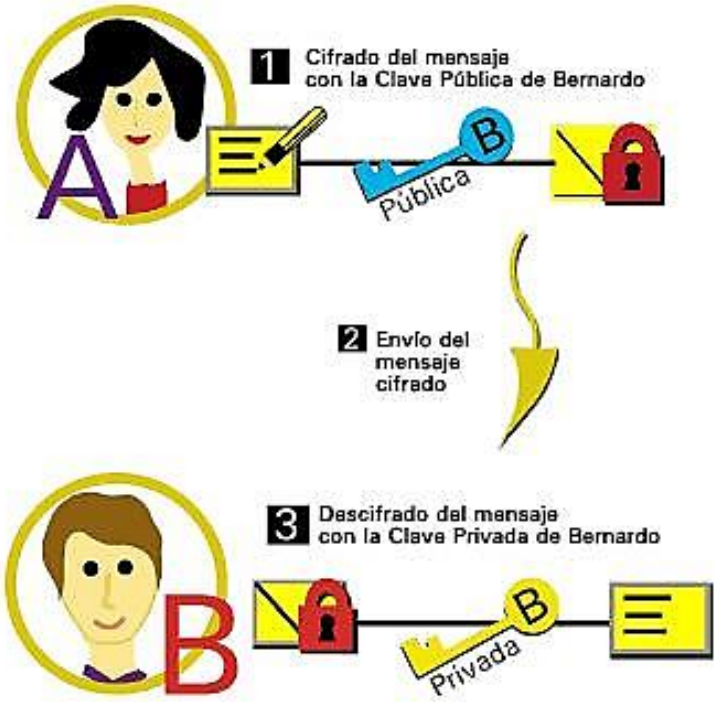
*YA **NO ERA NECESARIO DISPONER DE UNA CLAVE COMPARTIDA*** ENTRE LOS COMUNICANTES, SINO QUE **ERA SUFICIENTE CON CONOCER LA CLAVE PÚBLICA DEL OTRO** INTERLOCUTOR.



1. INTRODUCCIÓN

LA PREGUNTA QUE SURGÍA A RAÍZ DE ESTA CUESTIÓN ERA: **¿CÓMO ASEGURAR QUE LA CLAVE PÚBLICA REALMENTE PERTENECÍA AL OTRO INTERLOCUTOR?**

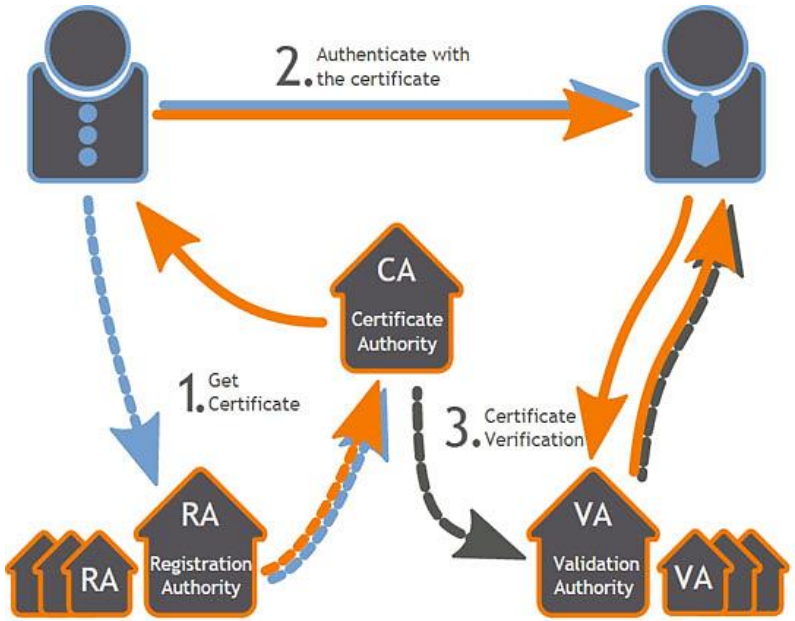
ERA NECESARIO **ESTABLECER UN VÍNCULO VERIFICABLE** DE FORMA ELECTRÓNICA **ENTRE LA IDENTIDAD DE LA PERSONA Y SU CLAVE PÚBLICA** ASOCIADA.



1. INTRODUCCIÓN

EN ESTE CONTEXTO SURGEN LAS **INFRAESTRUCTURAS DE CLAVE PÚBLICA** (**PKI, PUBLIC KEY INFRASTRUCTURE**), CUYA **MISIÓN** ES **GESTIONAR EL CICLO DE VIDA DE LOS CERTIFICADOS DE CLAVE PÚBLICA**, QUE SON DOCUMENTOS QUE VINCULAN UNA IDENTIDAD Y SU CLAVE PÚBLICA.

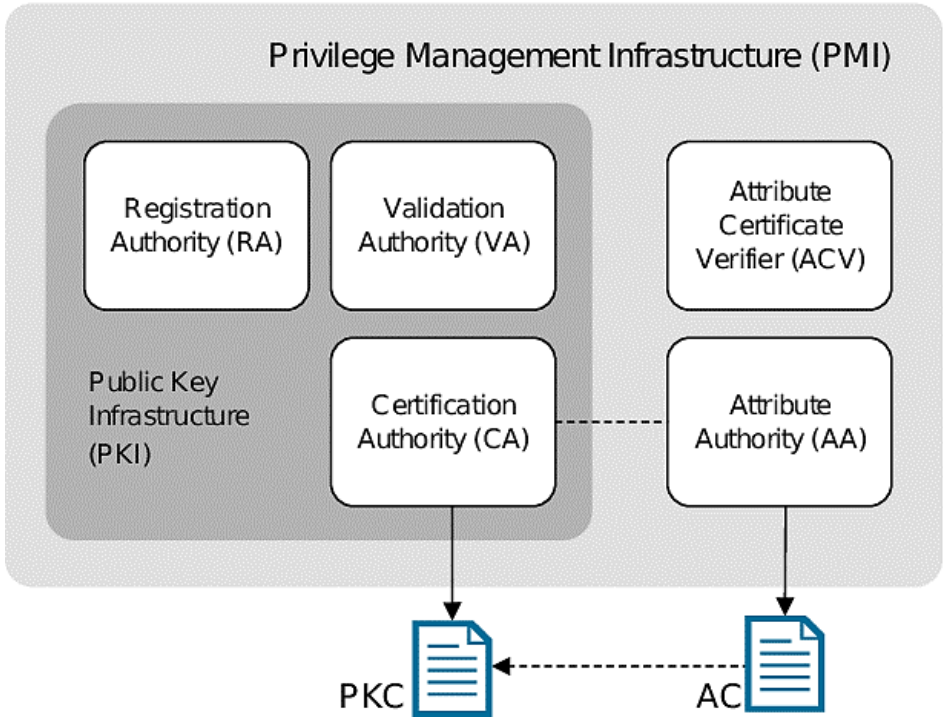
SE PRESENTAN EN PROFUNDIDAD LAS INFRAESTRUCTURAS DE CLAVE PÚBLICA Y SUS CERTIFICADOS ASOCIADOS.



1. INTRODUCCIÓN

EN EL TERRENO ELECTRÓNICO **NO SÓLO ES IMPORTANTE AUTENTICAR, SINO TAMBIÉN COMPROBAR SI SE TIENEN PRIVILEGIOS SUFICIENTES** PARA REALIZAR UNA ACCIÓN.

SE INTRODUCEN TAMBIÉN LAS **INFRAESTRUCTURAS DE GESTIÓN DE PRIVILEGIOS** (**PMI, PRIVILEGE MANAGEMENT INFRASTRUCTURE**), QUE SE ENCARGAN DE INSTRUMENTAR LA CONCESIÓN, VERIFICACIÓN Y REVOCACIÓN DE PRIVILEGIOS A UNA ENTIDAD.



CONTENIDOS

1. INTRODUCCIÓN
2. **IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES**
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

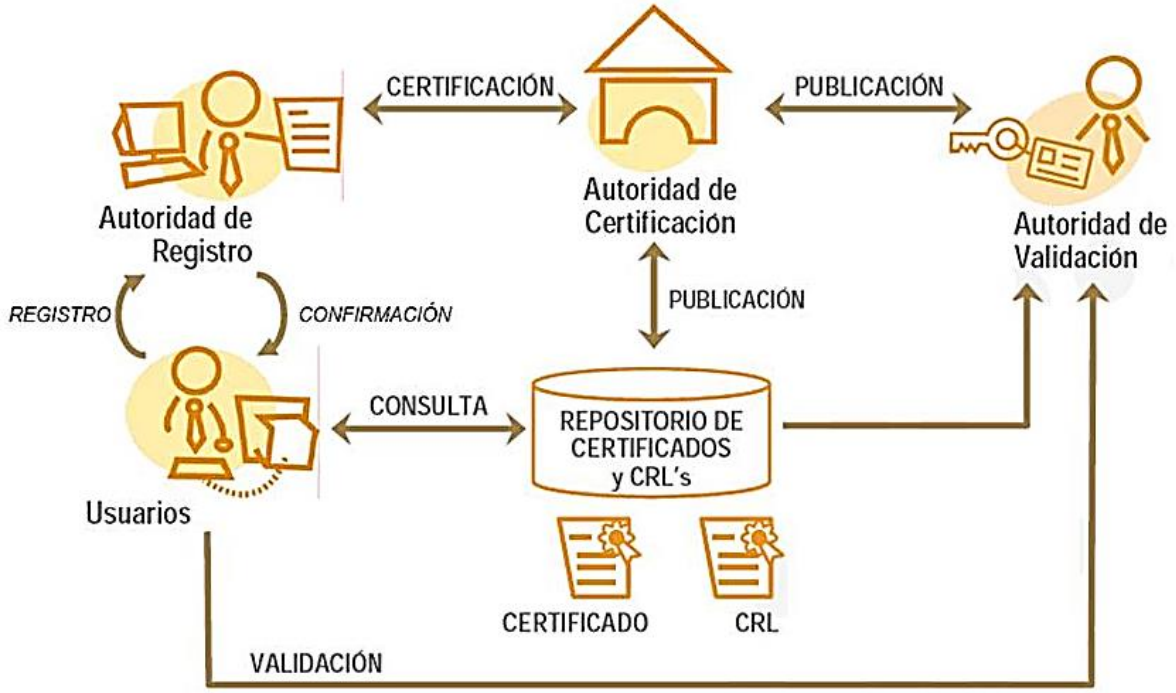
EN UNA **INFRAESTRUCTURA DE CLAVE PÚBLICA** (**PKI**) FIGURAN TODAS LAS ENTIDADES QUE SE RELACIONAN, DE ALGUNA MANERA, CON LA GESTIÓN DE CERTIFICADOS DE CLAVE PÚBLICA.

LAS NORMAS QUE LO REGULAN SON:

- **REGLAMENTO (UE) Nº 910/2014** DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 23 DE JULIO DE 2014 RELATIVO A LA *IDENTIFICACIÓN ELECTRÓNICA Y LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS* EN EL MERCADO INTERIOR
- **LEY 6/2020, DE 11 DE NOVIEMBRE**, REGULADORA DE *DETERMINADOS ASPECTOS DE LOS SERVICIOS ELECTRÓNICOS DE CONFIANZA*.

2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

MÁS ALLÁ DEL TITULAR DEL CERTIFICADO, **EXISTE UN** AMPLIO **CONJUNTO DE AUTORIDADES** QUE PARTICIPAN EN LA **EMISIÓN, RENOVACIÓN, VERIFICACIÓN (USO) Y REVOCACIÓN** DEL MISMO.

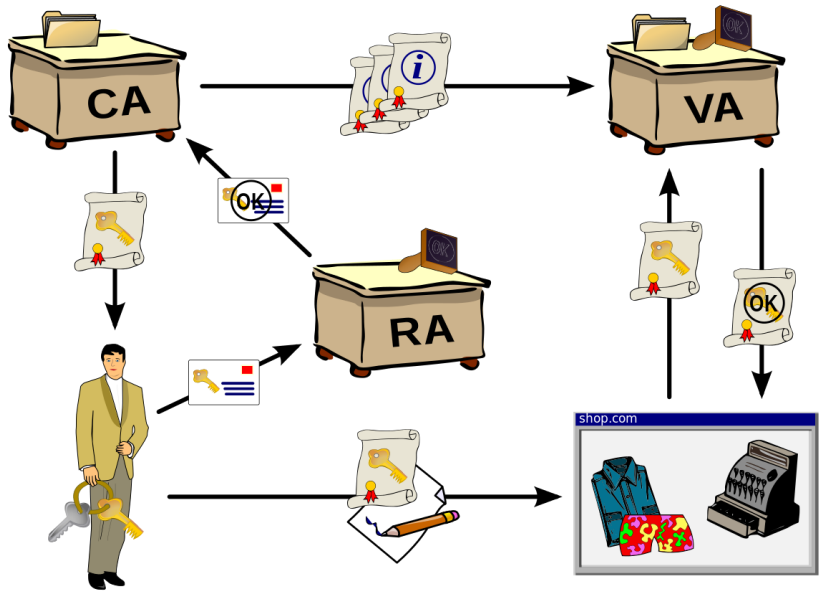


2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

INFRAESTRUCTURA DE CLAVE PÚBLICA

- CA: AUTORIDAD DE CERTIFICACIÓN
- VA: AUTORIDAD DE VALIDACIÓN
- RA: AUTORIDAD DE REGISTRO



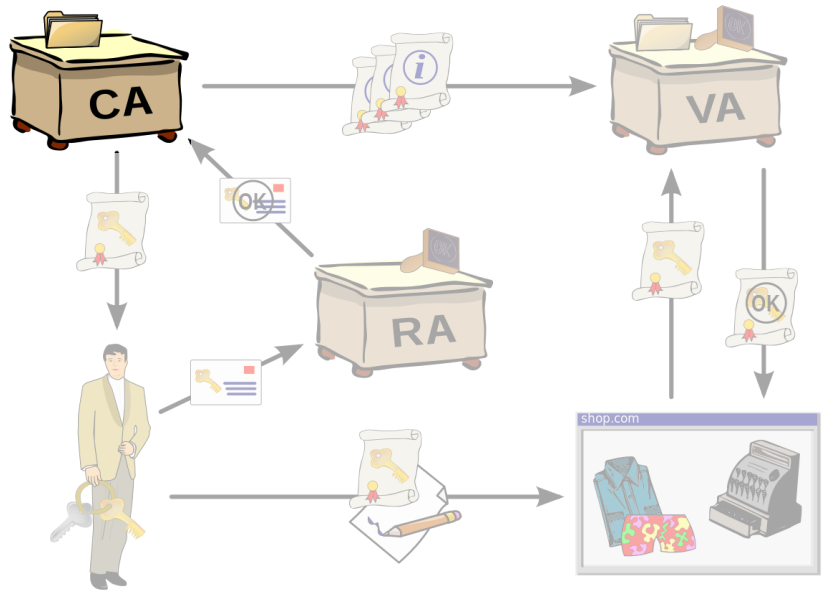
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

LA ENTIDAD QUE **EMITE UN CERTIFICADO DE CLAVE PÚBLICA** SE DENOMINA:

AUTORIDAD DE CERTIFICACIÓN (CA)

SUS FUNCIONES SON SIMILARES A LAS DE UN NOTARIO, EN TANTO QUE ACREDITA O CERTIFICA LA IDENTIDAD DE UNA DETERMINADA ENTIDAD.



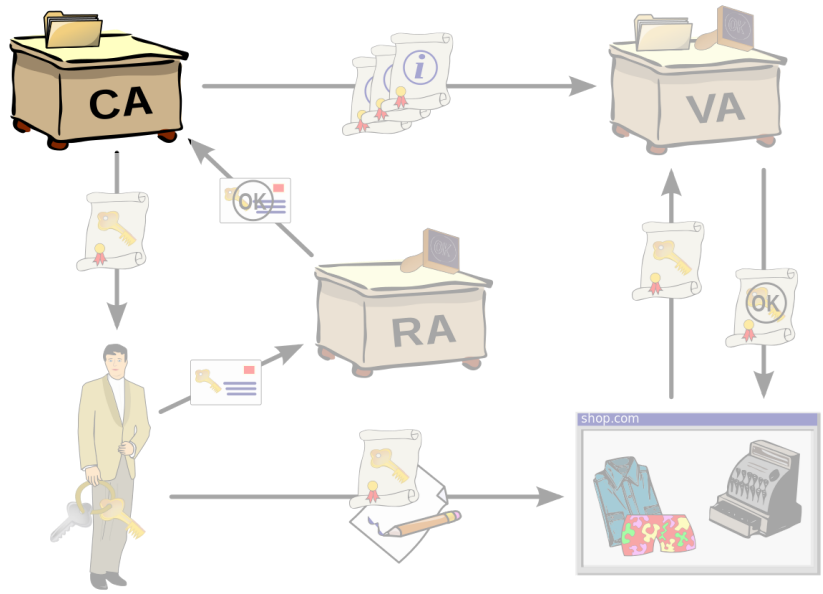
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

ESTA CUESTIÓN **ES CLAVE PARA LA AUTENTICACIÓN**, LA CUAL ES FUNDAMENTAL PARA UNA PARTE IMPORTANTE DE LOS INTERCAMBIOS DE DATOS QUE SE PRODUCEN EN INTERNET.

EXISTEN DOS **ATRIBUTOS QUE LA IDENTIFICAN**:

- **SU NOMBRE**
- **SU CLAVE PÚBLICA**



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

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.

UNA CUESTIÓN IMPORTANTE ES QUE, DADO QUE LOS CERTIFICADOS SON FIRMADOS UTILIZANDO LA CLAVE PRIVADA DE LA **CA**, DICHA CLAVE ES FUNDAMENTAL PARA GARANTIZAR LA SEGURIDAD DEL PROCESO

2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

LOS CERTIFICADOS DE CLAVE PÚBLICA (**PKC, PUBLIC KEY CERTIFICATE**) **SIRVEN PARA QUE LA CA ACREDITE QUE LA ENTIDAD A LA QUE SE REFIERE EL CERTIFICADO CONOCE LA CLAVE PRIVADA ASOCIADA A LA PÚBLICA** QUE FIGURA EN DICHO DOCUMENTO.

SI LA **CA** INCLUYE INFORMACIÓN ADICIONAL EN EL **PKC**, TAMBIÉN SE ACREDITA QUE DICHOS DATOS SE RELACIONAN CON EL SUJETO DEL CERTIFICADO.

LOS **PKC** SE PUEDEN EMITIR PARA UN USUARIO FINAL, O BIEN PARA OTRAS **CA** (**CADENAS DE CERTIFICACIÓN**).

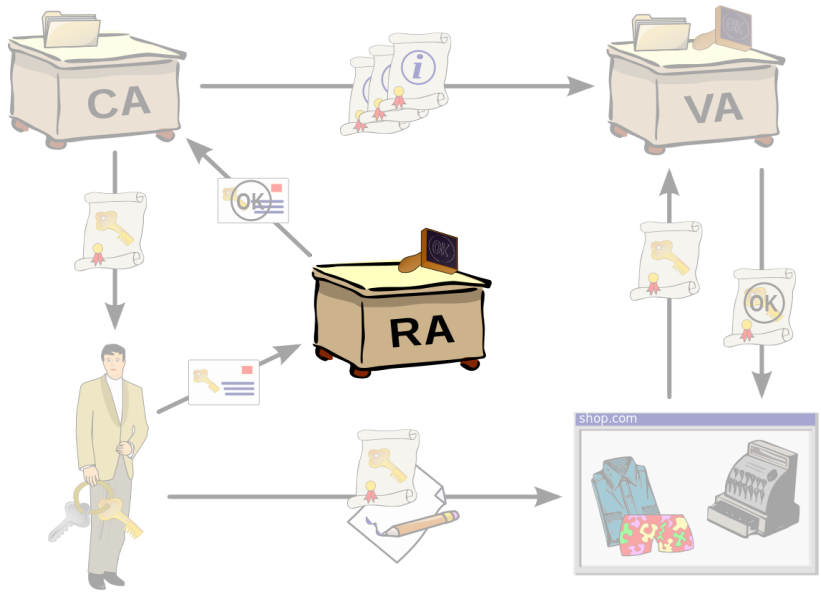
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

PARA EL **PROCESO DE EMISIÓN**, LAS **CA** DEBEN **VERIFICAR LA IDENTIDAD DE LA ENTIDAD FINAL**.

LAS **CA** PUEDEN DELEGAR ESTA TAREA A UNA **AUTORIDAD DE REGISTRO (AR)**.

ES IMPORTANTE TENER EN CUENTA QUE **LA AR DEBE VERIFICAR NO SOLO LA IDENTIDAD, SINO TAMBIÉN LOS DATOS QUE FIGUREN EN EL CERTIFICADO.**



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

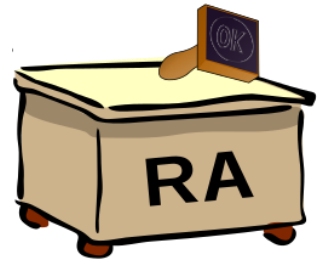
ENTIDADES PARTICIPANTES

LA GESTIÓN DE UNA **AR** LA REALIZA UNA ÚNICA PERSONA (POR EJEMPLO, UN FUNCIONARIO PÚBLICO).

PARA REFLEJAR QUE LA **AR** HA VERIFICADO LOS DATOS, HABITUALMENTE ÉSTA FIRMA UNA CONSTANCIA.

LA **CA** VERIFICA DICHA FIRMA PARA TENER CONSTANCIA DE ESTE HECHO.

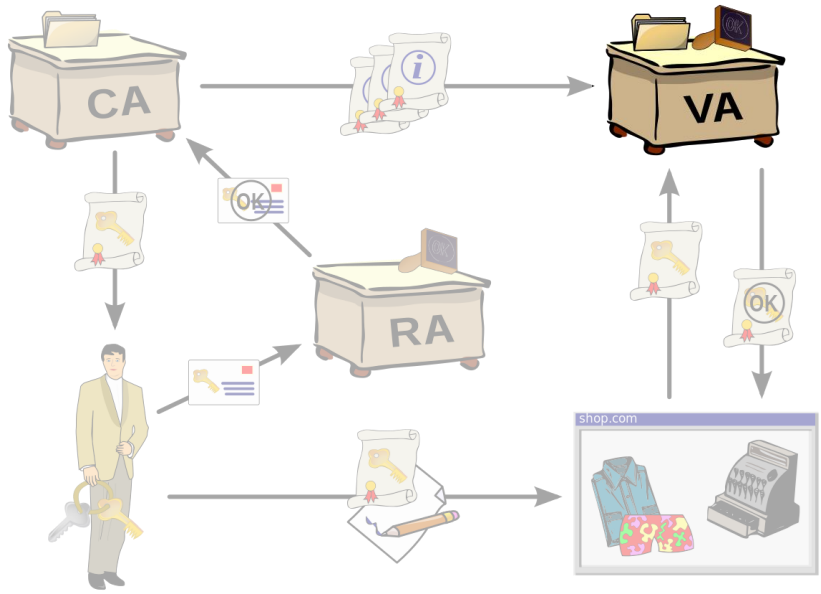
LA CUSTODIA DE LA CLAVE PRIVADA DE LA **AR** ES FUNDAMENTAL PARA GARANTIZAR LA SEGURIDAD.



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

LA **AUTORIDAD DE VALIDACIÓN** (AV) ES AQUEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN QUE **ASEGURA LA AUTENTICIDAD, VALIDEZ E INTEGRIDAD DE LAS TRANSACCIONES** MÁS CRÍTICAS, COMO AQUELLAS DE TRANSFERENCIA DE VALORES, COMPRA, VENTA A TRAVÉS DE LA RED.



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

AV ES UNA AUTORIDAD DE CERTIFICACIÓN (**AC**) NEUTRAL **PARA CHEQUEO DE LA VALIDEZ DE LOS CERTIFICADOS DIGITALES** SEGÚN NORMA **X509V3** EN SISTEMAS QUE UTILIZAN **PKI** EN CORPORACIONES, BANCOS O DEPENDENCIAS GUBERNAMENTALES.

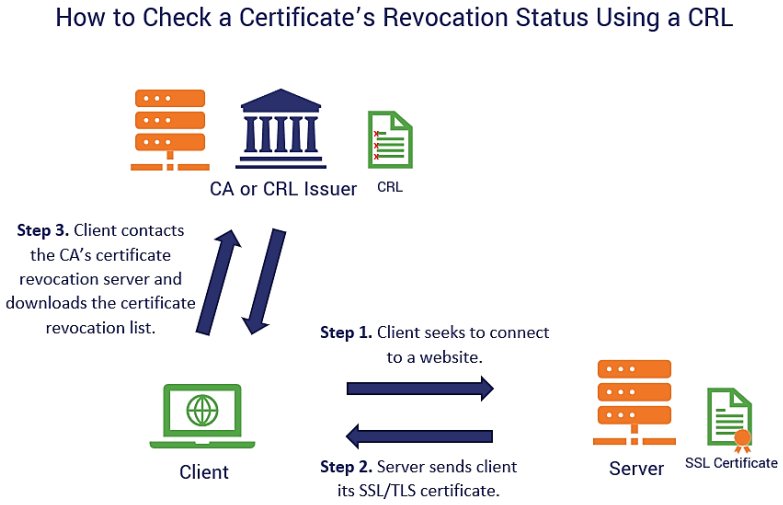
LA **AV** ES EL COMPONENTE QUE **TIENE COMO TAREA SUMINISTRAR INFORMACIÓN SOBRE LA VIGENCIA DE LOS CERTIFICADOS ELECTRÓNICOS** QUE, A SU VEZ, HAYAN SIDO REGISTRADOS POR UNA **AR** Y CERTIFICADOS POR LA **AC**.

2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

ACERCA DE **LA REVOCACIÓN**, SE DISTINGUE POR SU IMPORTANCIA EL **EMISOR DE LISTAS DE CERTIFICADOS REVOCADOS** (**CRL ISSUER**).

TANTO LAS TAREAS DE LA AUTORIDAD DE REGISTRO COMO DE LA EMISIÓN DE **CRL**, PUEDEN SER REALIZADAS POR LA PROPIA **CA**.



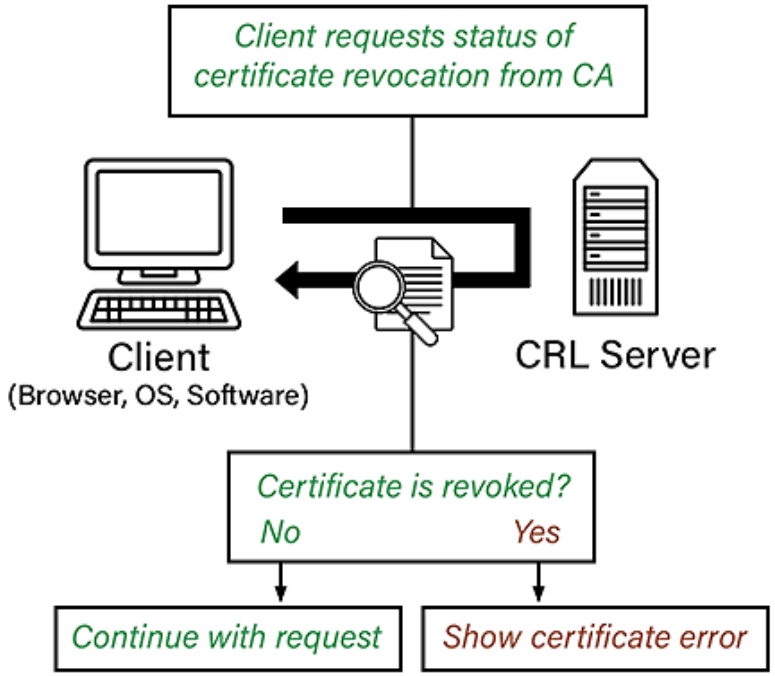
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

PARA DIFUNDIR LOS CERTIFICADOS DE CLAVE PÚBLICA Y LAS LISTAS DE CERTIFICADOS REVOCADOS, SE IDENTIFICA **UN REPOSITORIO** DENTRO DE LA ARQUITECTURA.

LOS REPOSITORIOS **DEBEN SER INTEROPERABLES**.

CUALQUIER PERSONA PUEDE CONSULTAR LOS REPOSITORIOS DE CUALQUIER **CA**, PUESTO QUE TODAS **HACEN USO DE UN PROTOCOLO DE COMUNICACIÓN COMÚN**.



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ENTIDADES PARTICIPANTES

ADEMÁS DE LOS REPOSITORIOS, HABITUALMENTE **SE DISTINGUEN EN LAS PKI LOS ARCHIVOS**. ESTOS **TIENEN COMO MISIÓN SERVIR DE ALMACÉN HISTÓRICO CONFIABLE**.

SE ENCARGAN DE **GARANTIZAR LA CUSTODIA DE LA INFORMACIÓN DURANTE LARGO TIEMPO**, ASEGURANDO QUE ESTA NO HA SIDO MODIFICADA DESDE QUE SE INTRODUJO.

GRACIAS A ESTO, ES POSIBLE CONSEGUIR UNA DOBLE FINALIDAD. POR UN LADO, SE PERMITE **RESOLVER DISPUTAS QUE TENGAN QUE VER CON CERTIFICADOS QUE YA CADUCARON**. POR OTRO, SE HACE POSIBLE **VERIFICAR FIRMAS REALIZADAS EN EL PASADO**.

2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

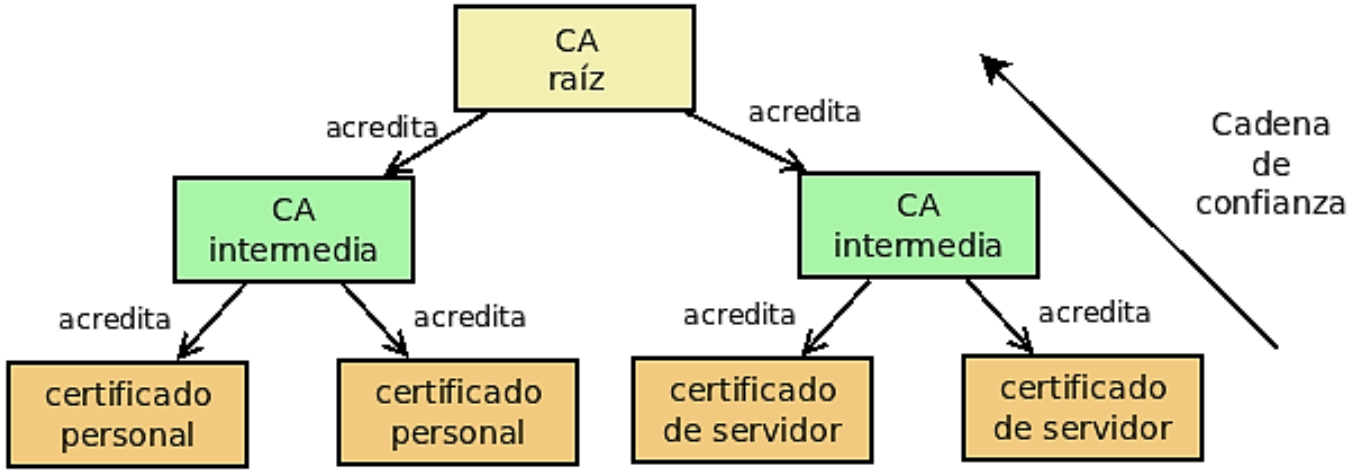
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

MODELO DE RELACIONES

LAS AUTORIDADES EN UNA **PKI SE RELACIONAN DE MANERA JERÁRQUICA**.

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.

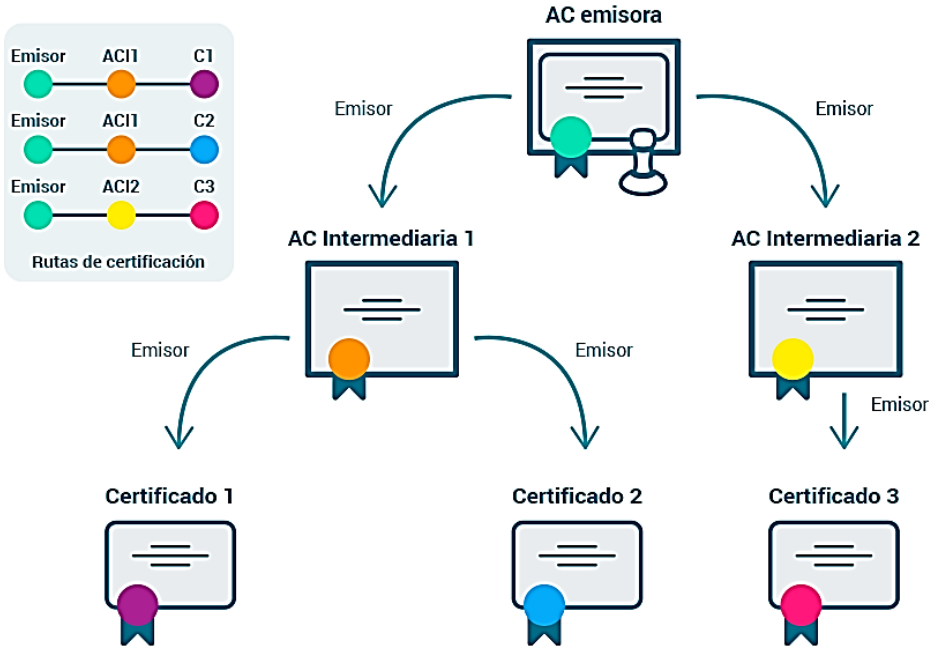


2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

MODELO DE RELACIONES

GRACIAS A LA EXISTENCIA DE **AC INTERMEDIAS** APARECE EL CONCEPTO DE **CADENAS DE CERTIFICACIÓN**.

ASÍ, EL CERTIFICADO DE UNA ENTIDAD FINAL PUEDE SER EMITIDO POR UNA **AC** INTERMEDIA (**AC2**), QUE DEPENDE DE OTRA **CA** INTERMEDIA (**AC1**) QUE ES SUBORDINADA A SU VEZ DE LA **AC RAÍZ**.

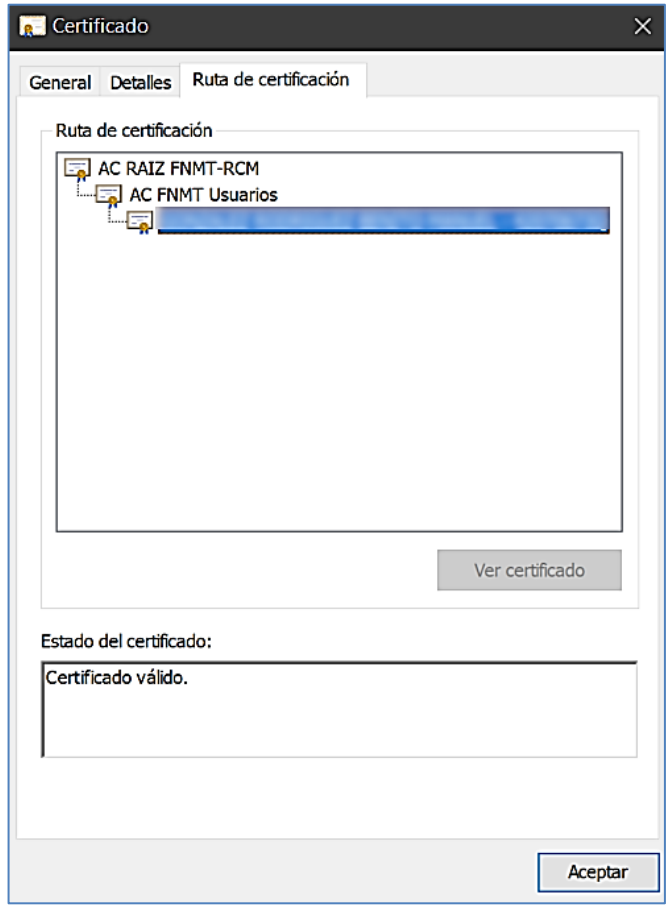


2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

MODELO DE RELACIONES

LA SIGUIENTE IMAGEN REPRESENTA ESTA SITUACIÓN A MODO DE EJEMPLO, EN LA QUE SE OBSERVA QUE EL CERTIFICADO DE UN USUARIO ES EMITIDO POR LA AUTORIDAD **AC FNMT USUARIOS** ES SUBORDINADA DE **AC RAIZ FNMT RCM**.

LAS CADENAS DE CERTIFICACIÓN PERMITEN LLEVAR AL MUNDO REAL LAS PKI, DADO QUE LA GESTIÓN DE LOS CERTIFICADOS DE UNA ENTIDAD PUEDE SER DISTRIBUIDA ENTRE VARIAS **CA** INTERMEDIAS O SUBORDINADAS.



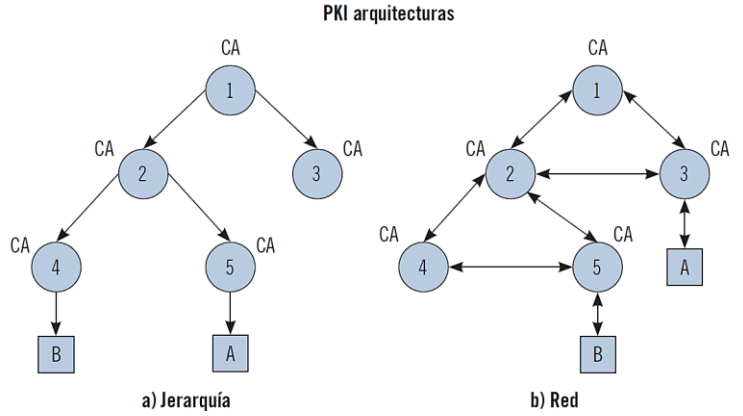
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

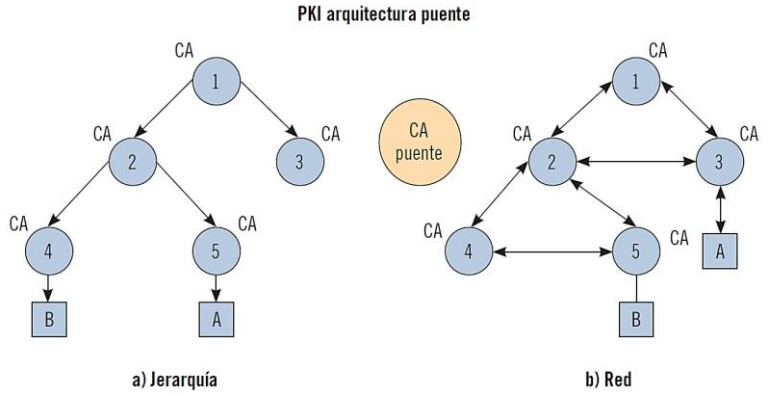
ARQUITECTURAS DE UNA PKI

UNO DE LOS RETOS PRÁCTICOS DE LAS **PKI** ES SU APLICACIÓN EN UNA EMPRESA.

SE PUEDE DISTINGUIR, ADEMÁS DE LA **ARQUITECTURA JERÁRQUICA**, LA **ARQUITECTURA EN RED**.

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**).





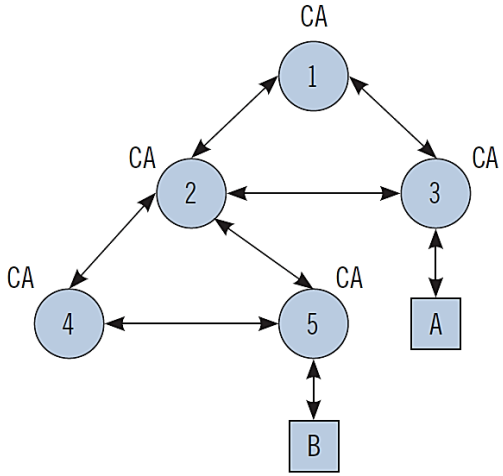
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ARQUITECTURAS DE UNA PKI

RED

LAS CA SE VERIFICAN INDEPENDIENTE **UNAS A OTRAS**, DANDO COMO RESULTADO UNA RED DE CONFIANZA ENTRE LAS **CA** CERCANAS.

UNA ENTIDAD FINAL CONOCE LA CLAVE PÚBLICA DE LA **CA** GENERALMENTE MÁS CERCANA Y VERIFICA LA CADENA DE CERTIFICACIÓN EN BASE A LAS **CA** DE CONFIANZA.

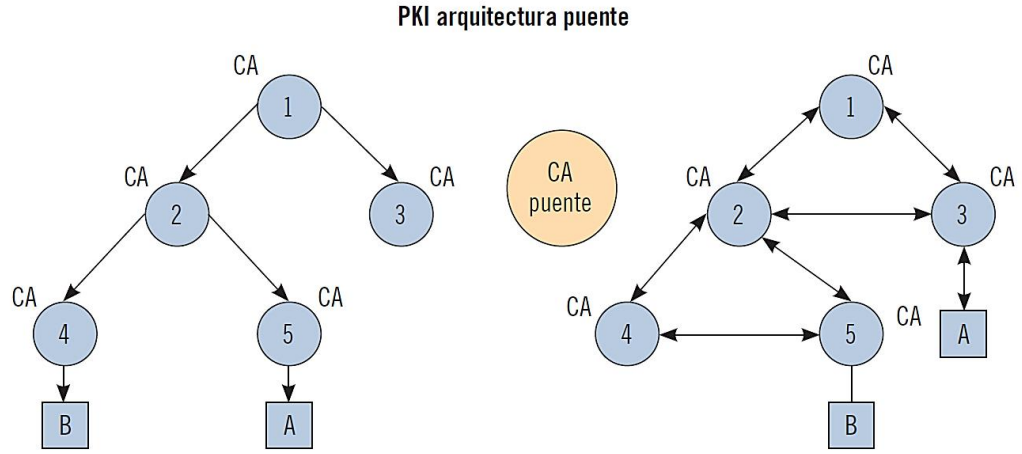


2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ARQUITECTURAS DE UNA PKI

PUENTE

ESTE TIPO FUE DISEÑADO PARA CONECTAR LAS **PKI** DE DOS EMPRESAS CON INDEPENDENCIA DEL TIPO DE ARQUITECTURA. PARA ELLO, SE INTRODUCE UNA NUEVA **CA**, DENOMINADA **CA PUENTE**, CUYA FUNCIÓN ES **ESTABLECER RELACIONES ENTRE LAS PKI** DE LAS EMPRESAS CORRESPONDIENTES.



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ARQUITECTURAS DE UNA PKI

PUENTE

UNA **CA PUENTE** *ESTABLECE RELACIONES ENTRE DIFERENTES PKI*. ESTAS RELACIONES PUEDEN UTILIZARSE PARA **ESTABLECER UN PUENTE DE CONFIANZA ENTRE LAS ENTIDADES FINALES** DE LAS EMPRESAS ASOCIADAS.

SI LA ARQUITECTURA MODO PUENTE ES **EN JERARQUÍA**, LA **CA** PUENTE ESTABLECERÁ UNA RELACIÓN CON LA **CA** RAÍZ.

SI LA ARQUITECTURA ES **DE RED**, LA **CA** PUENTE SOLO ESTABLECERÁ UNA RELACIÓN CON UNA DE LAS **CA** DE LA RED.

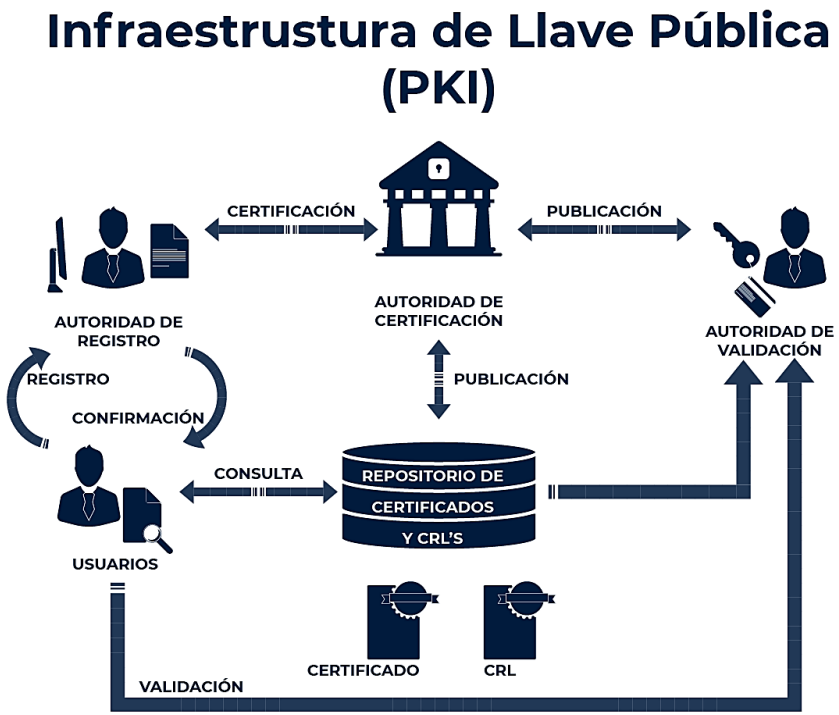
LA **CA** QUE ESTABLECE RELACIÓN CON LA **CA** PUENTE RECIBE EL NOMBRE DE **CA PRINCIPAL**.

2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ARQUITECTURAS DE UNA PKI

HAY MÚLTIPLES FORMAS DE **CREAR UNA ARQUITECTURA FÍSICA DE PKI**, SIENDO RECOMENDABLE **QUE LOS COMPONENTES DE LA PKI SE IMPLANTEN EN SISTEMAS SEPARADOS**.

SE ACONSEJA PUES QUE LA **CA**, LA **RA** Y **LOS REPOSITORIOS** SE ENCUENTREN **EN SISTEMAS INDEPENDIENTES**, CONSIGUIENDO QUE LOS DATOS SENSIBLES SE SITÚEN DETRÁS DEL CORTAFUEGOS DE LA EMPRESA.

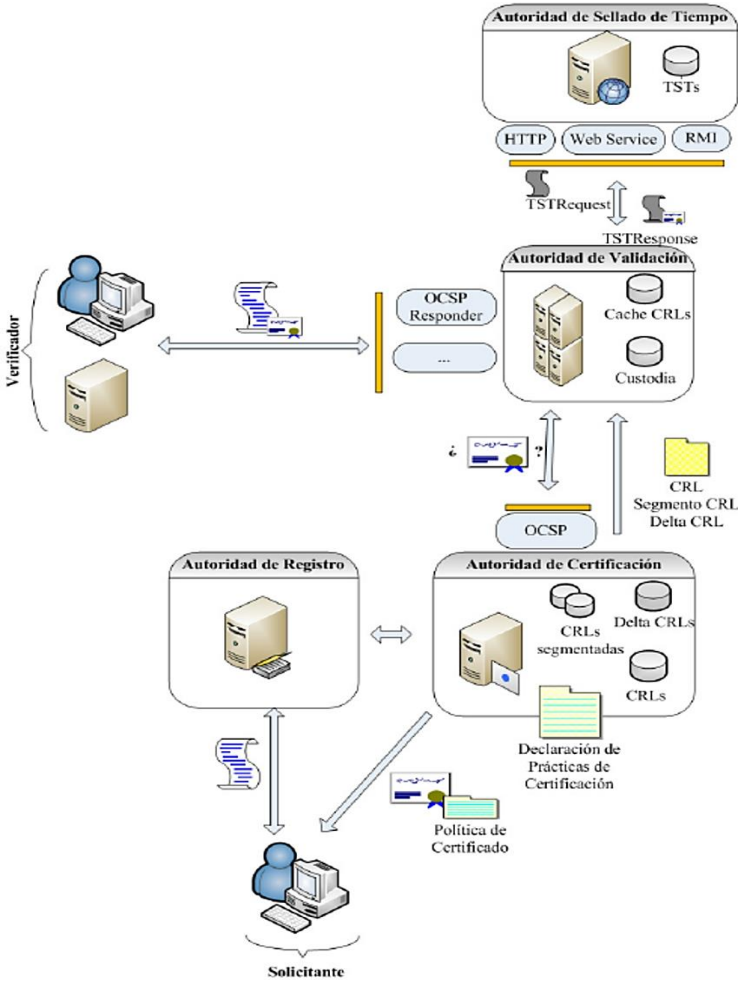


2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ARQUITECTURAS DE UNA PKI

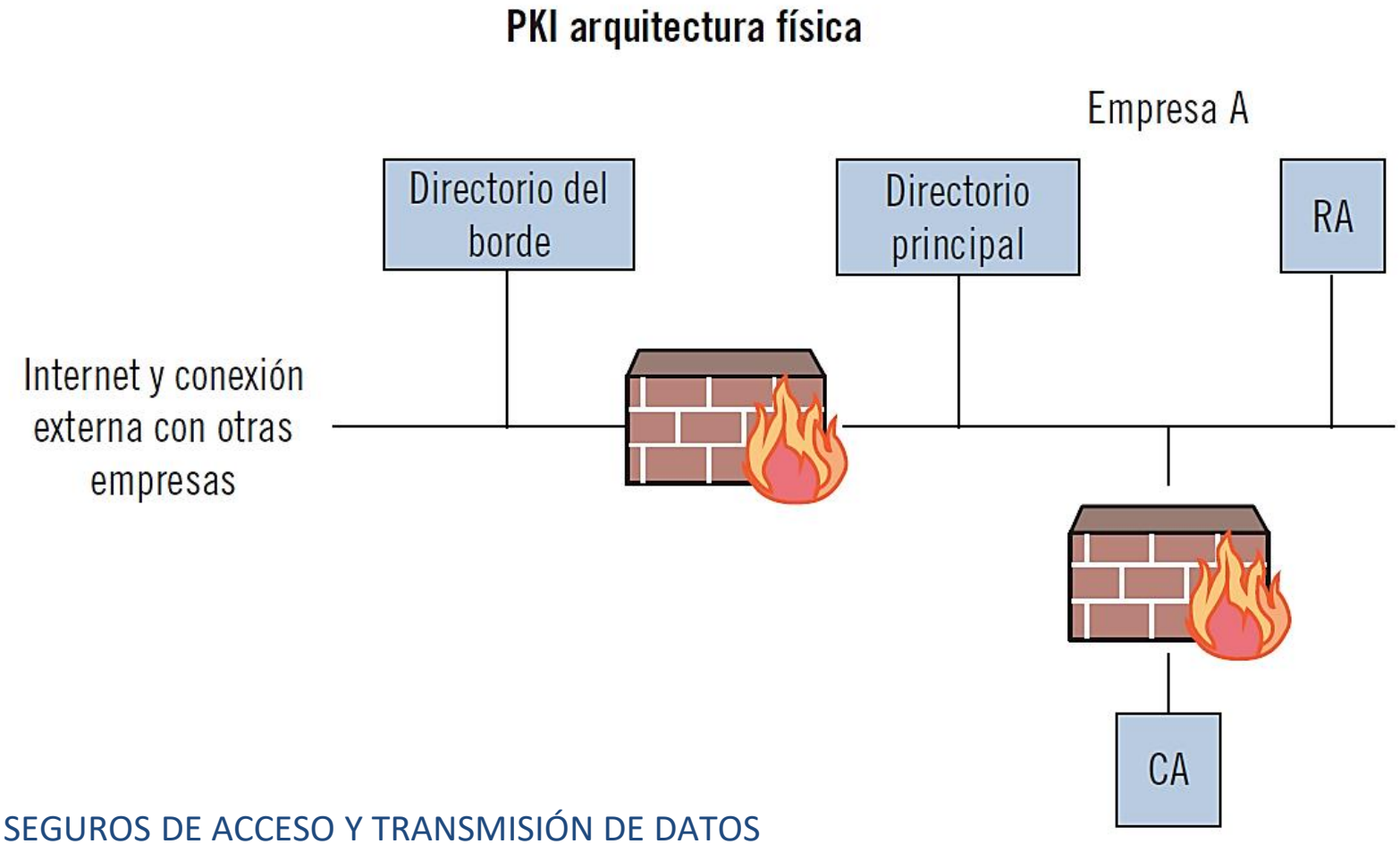
EN CONCRETO, LA **PROTECCIÓN DEL SISTEMA** DE LAS **CA** ES MUY IMPORTANTE PORQUE **SI** ESTE **RESULTA COMPROMETIDO EL SISTEMA** SERÍA SUSCEPTIBLE DE ATAQUES Y **HABRÍA QUE VOLVER A CREAR TODOS LOS CERTIFICADOS** AFECTADOS.

POR ELLO, EL SISTEMA DE **CA** HA DE LOCALIZARSE **DETRÁS DEL CORTAFUEGOS**, EL CUAL, ADEMÁS, HA DE **PERMITIR LA COMUNICACIÓN ENTRE TODOS LOS SISTEMAS** QUE PARTICIPEN.



2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

ARQUITECTURAS DE UNA PKI



CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. **AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS**
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

LA AUTORIDAD DE CERTIFICACIÓN (**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**, QUE SE INTRODUCEN A CONTINUACIÓN.

POSTERIORMENTE, Y DADO QUE LA **CA** PUEDE FORMAR PARTE DE UNA CADENA DE CERTIFICACIÓN, SE PRESENTA EL PROCESO DE VALIDAR LA MISMA.

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

FUNCIONES DE GESTIÓN

HAY 7 **FUNCIONES DE GESTIÓN** EN LAS **RELACIONES ENTRE UN USUARIO Y LA CA**:

- **EL REGISTRO**
- **LA OPERACIÓN DE INICIALIZACIÓN**
- **LA CERTIFICACIÓN**
- **COPIA DE RESPALDO**
- **ACTUALIZAR EL PAR DE CLAVES**
- **REVOCACIÓN DE LA CLAVE**
- **LA CERTIFICACIÓN CRUZADA**

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

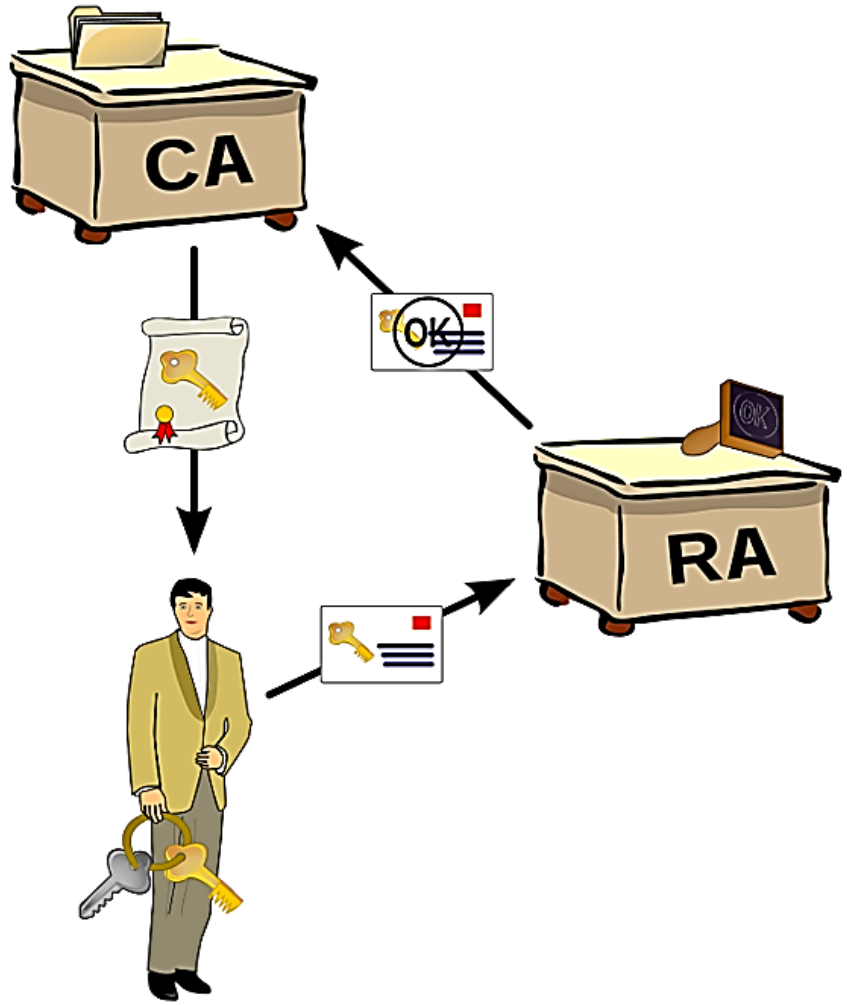
FUNCIONES DE GESTIÓN

EL 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. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

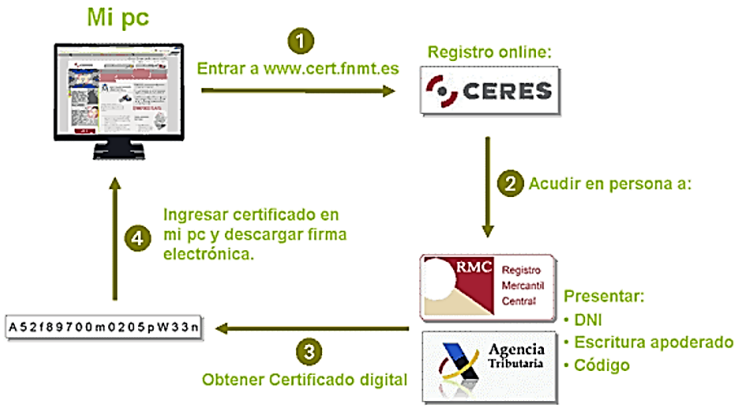
FUNCIONES DE GESTIÓN

LA OPERACIÓN DE INICIALIZACIÓN

ES FUNDAMENTAL PARA QUE LA ENTIDAD FINAL PUEDA SER CAPAZ DE VERIFICAR LOS CERTIFICADOS RECIBIDOS.

EN LA INICIALIZACIÓN, **LA ENTIDAD FINAL RECIBE SU PAR DE CLAVES PÚBLICA-PRIVADA**.

ESTE PAR PUEDE NO SER ÚNICO Y QUE, DE HECHO, ES HABITUAL CONTAR CON MÁS DE UN PAR (PARA AUTENTICACIÓN Y OTRO PARA FIRMA).



3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

FUNCIONES DE GESTIÓN

LA CERTIFICACIÓN

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 UN REPOSITORIO.**

COPIA DE RESPALDO

DEBE EXISTIR UNA **FUNCIÓN QUE PERMITA REALIZAR UNA COPIA DE RESPALDO** DE DICHO PAR, A FIN DE QUE EL USUARIO PUEDA RECUPERARLA EN CASO DE PÉRDIDA (POR EJEMPLO, SI SE PIERDE UN PENDRIVE EN EL QUE SE HABÍA ALMACENADO ESTE MATERIAL).

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

FUNCIONES DE GESTIÓN

ACTUALIZAR EL PAR DE CLAVES

ESTA FUNCIÓN **ES CONVENIENTE** POR UN DOBLE MOTIVO.

EL PRIMERO ES **DIFICULTAR LOS ATAQUES** QUE PRETENDAN ADIVINAR O AVERIGUAR LA CLAVE PRIVADA DE LA ENTIDAD EN JUEGO.

EL SEGUNDO ES **LIMITAR EL POSIBLE IMPACTO** QUE ESE ATAQUE PUDIERA TENER: AL RENOVAR EL PAR DE CLAVES, LAS OPERACIONES SIGUIENTES HARÁN USO DE ESTE NUEVO PAR.

DE ESTA MANERA, UNA FIRMA ELECTRÓNICA REALIZADA CON EL PAR ANTIGUO CARECERÍA DE VALIDEZ.

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

FUNCIONES DE GESTIÓN

REVOCACIÓN DE LA CLAVE

CON LA MISIÓN DE **REDUCIR LOS EFECTOS DE UN POSIBLE ATAQUE O PÉRDIDA DE UNA CLAVE**, SURGE LA OPERACIÓN DE REVOCACIÓN DE LA CLAVE, **CUANDO EL PROPIETARIO DE UN CERTIFICADO CONSIDERA QUE ESTE YA NO ES VÁLIDO**.

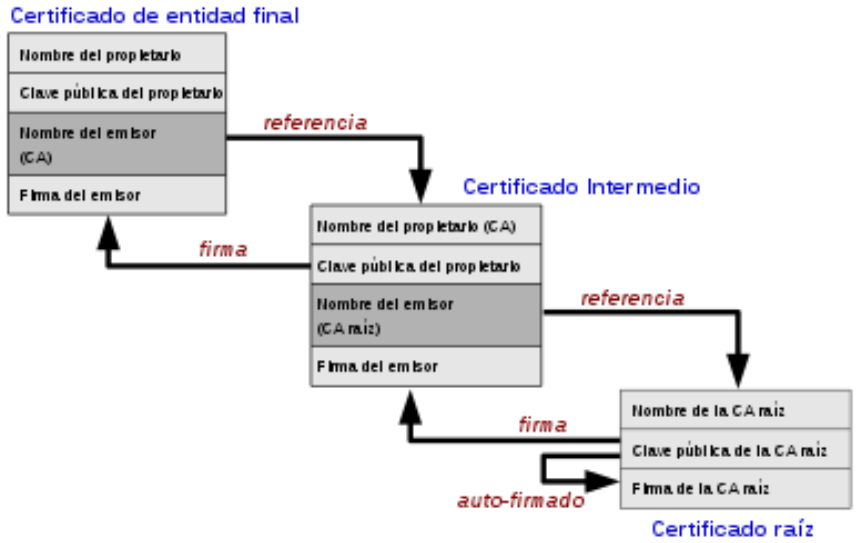
LA CERTIFICACIÓN CRUZADA

ES LA 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. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

VALIDACIÓN DE UNA CADENA DE CERTIFICACIÓN

EL PROCESO DE **VALIDACIÓN DE UNA CADENA DE CERTIFICACIÓN** *TIENE POR OBJETIVO DETERMINAR SI UN CERTIFICADO DE UNA ENTIDAD FINAL HA SIDO EMITIDO, DIRECTA O INDIRECTAMENTE, POR UNA* ***CA*** *DE CONFIANZA.*



3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

VALIDACIÓN DE UNA CADENA DE CERTIFICACIÓN

EL PROCESO **PERSIGUE COMPROBAR** QUE:

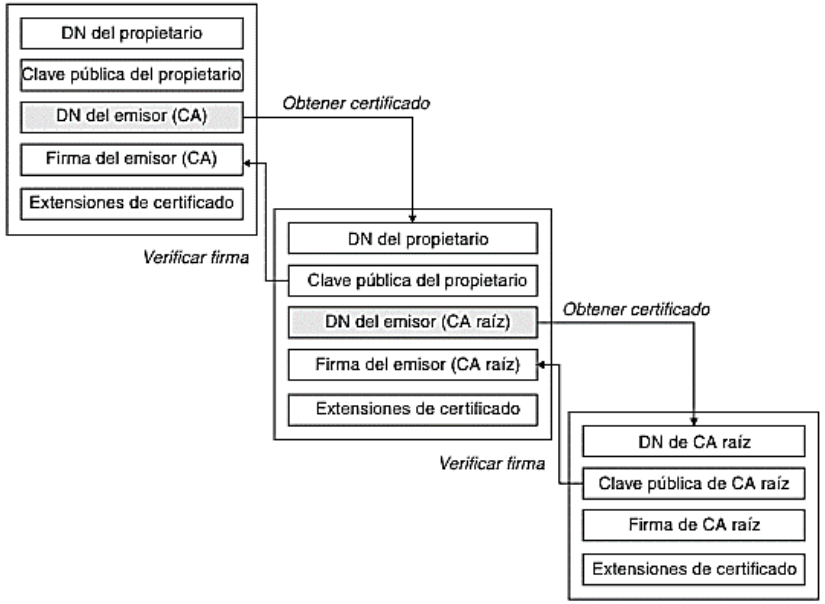
- EL PRIMER CERTIFICADO DE LA CADENA PERTENECE A UNA **CA** DE CONFIANZA O HA SIDO EMITIDO POR ELLA.
- PARA CADA UNO DE LOS CERTIFICADOS INTERMEDIOS, SE CUMPLE QUE:
  - LA ENTIDAD QUE FIGURA COMO SUJETO DE UN CERTIFICADO ES LA QUE EMITE EL CERTIFICADO SIGUIENTE.
  - TODOS LOS CERTIFICADOS EN JUEGO ERAN VÁLIDOS EN EL MOMENTO DE SU UTILIZACIÓN.
- EL ÚLTIMO CERTIFICADO DE LA CADENA ES EL DE LA ENTIDAD FINAL QUE PARTICIPA EN EL PROCESO.
- A LO LARGO DE LA CADENA NO PUEDEN PRODUCIRSE CICLOS (UN MISMO CERTIFICADO NO PUEDE APARECER MÁS DE UNA VEZ).

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

VALIDACIÓN DE UNA CADENA DE CERTIFICACIÓN

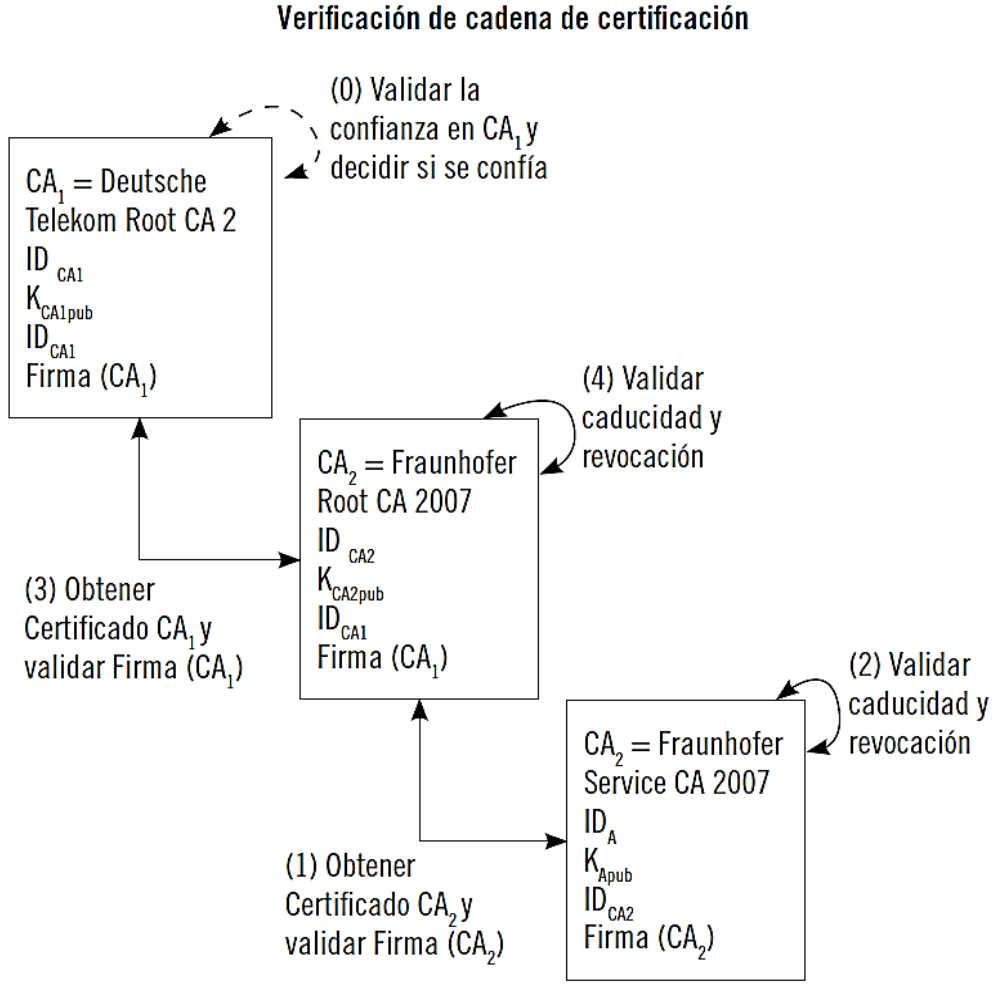
A LO LARGO DE LA **COMPROBACIÓN SE VERIFICA LA FIRMA ELECTRÓNICA DE CADA UNO DE LOS CERTIFICADOS**.

ADEMÁS, SE COMPRUEBA QUE LA POLÍTICA DE CADA UNO DE LOS CERTIFICADOS ES COHERENTE CON LA DE LOS DEMÁS Y CON EL USO PREVISTO EN LA ACCIÓN QUE DIO INICIO AL PROCESO DE VERIFICACIÓN.



3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

VALIDACIÓN DE UNA CADENA DE CERTIFICACIÓN



EN RELACIÓN CON EL EJEMPLO PRESENTADO ANTERIORMENTE, EN LA SIGUIENTE IMAGEN SE MUESTRA LA CADENA DE CERTIFICACIÓN DE LA AUTORIDAD “FRAUNHOFER SERVICE CA 2007”, LA CUAL ES SUBORDINADA DE “FRAUNHOFER ROOT CA 2007” Y ESTA, A SU VEZ, DE “DEUTSCHE TELEKOM ROOT CA 2”.

COMO SE PUEDE COMPROBAR EN LA IMAGEN, EL PROCESO CONSISTE, PRINCIPALMENTE, EN VERIFICAR LA FIRMA DE CADA UNO DE LOS CERTIFICADOS QUE APARECEN EN LA CADENA, ASÍ COMO LA CADUCIDAD Y REVOCACIÓN DE LOS MISMOS.

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

COMO PARTE DE LA NAVEGACIÓN POR INTERNET, **LOS NAVEGADORES REALIZAN DE MANERA AUTOMÁTICA LA VALIDACIÓN DE LOS CERTIFICADOS**.

ESTO OCURRE, POR EJEMPLO, CUANDO SE INGRESA EN UNA PÁGINA UTILIZANDO EL PROTOCOLO **HTTPS.**

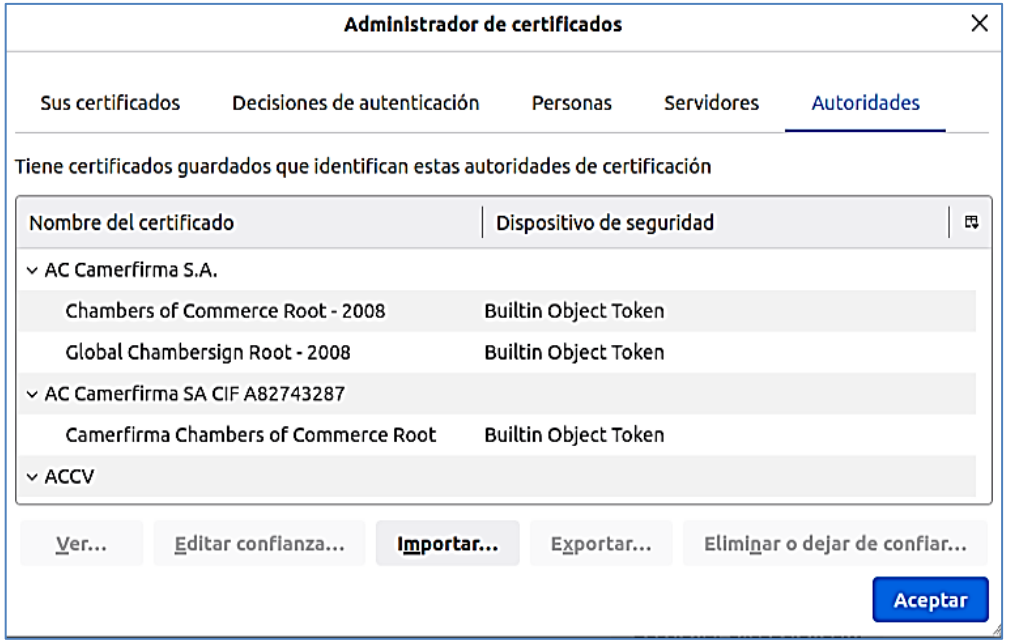
GRACIAS A ESTA VALIDACIÓN, **EL USUARIO QUE NAVEGA PUEDE TENER LA GARANTÍA DE QUE SE ESTÁ CONECTANDO A LA PÁGINA LEGÍTIMA** Y NO A UNA COPIA MANIPULADA.

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

PARA QUE ESTA VALIDACIÓN SE PUEDA REALIZAR DE MANERA AUTOMÁTICA, **EL NAVEGADOR DEBE CONOCER CUÁLES SON LAS CA RAÍZ QUE SON CONFIABLES**.

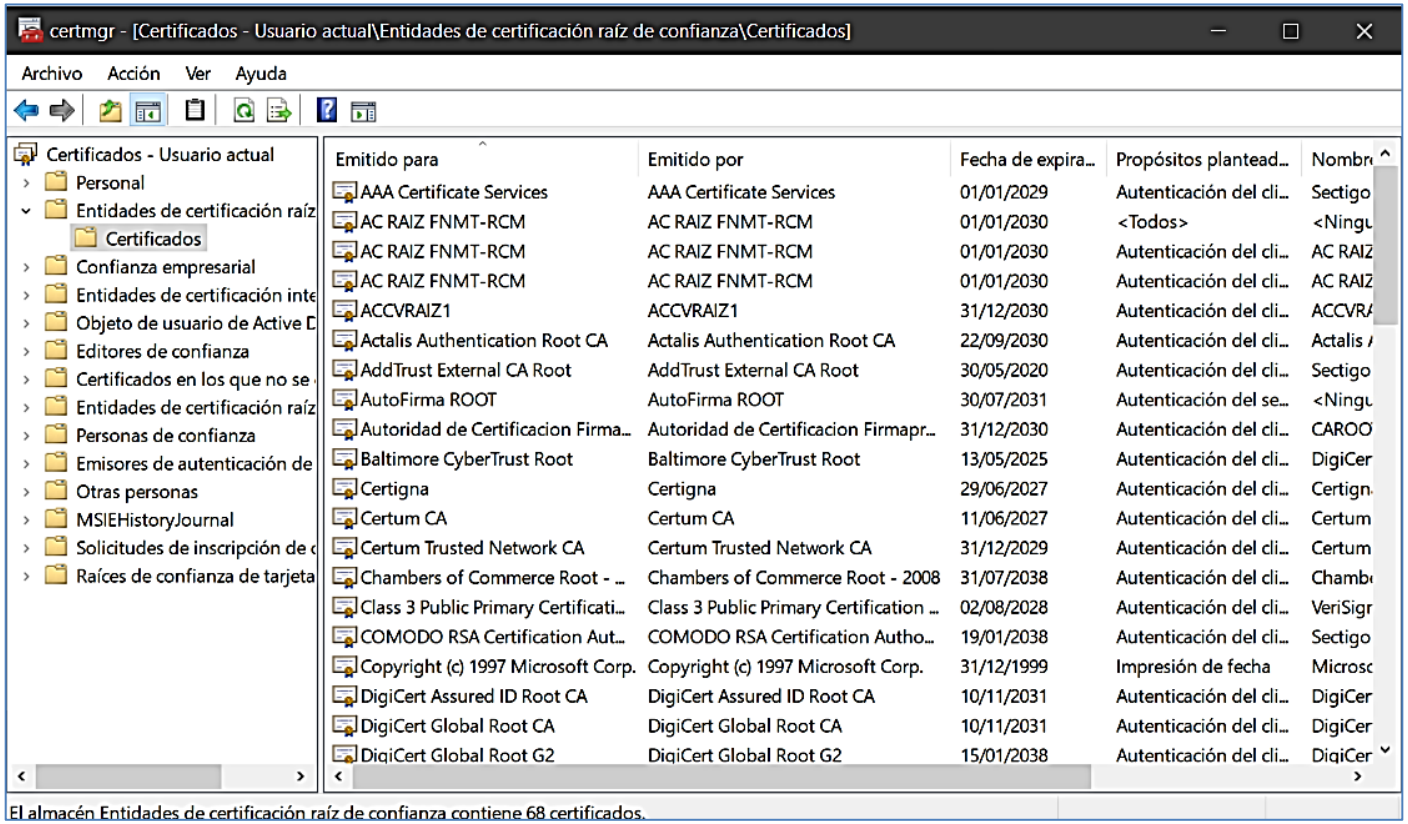
PARA ELLO, **LOS NAVEGADORES INCORPORAN EN SU INTERIOR UN GESTOR DE CERTIFICADOS** EN EL QUE VIENEN PREINSTALADOS LOS CERTIFICADOS DE AQUELLAS **CA** QUE SE CONSIDERAN CONFIABLES.



3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

LA SIGUIENTE IMAGEN MUESTRA EL **ADMINISTRADOR DE CERTIFICADOS DE USUARIO DE WINDOWS:**



3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

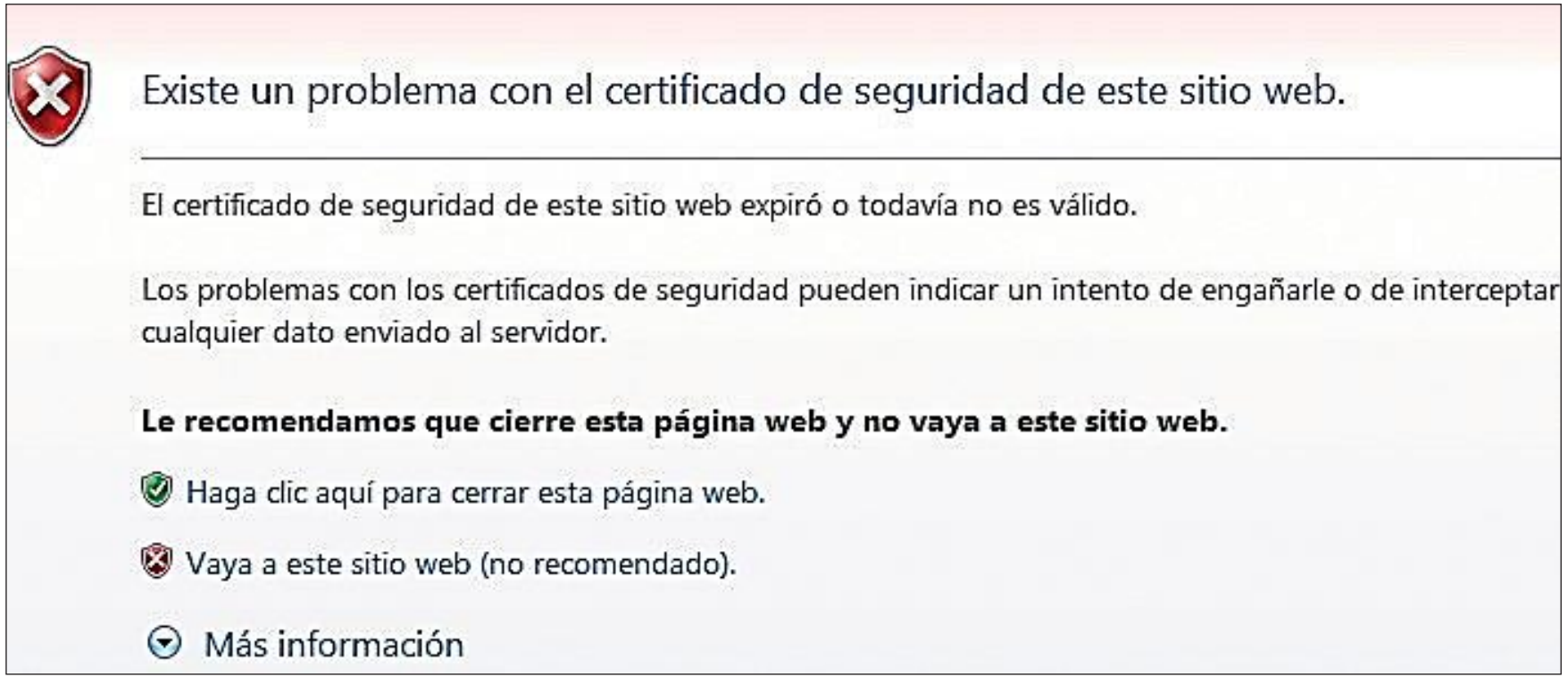
EN EL CASO DE QUE UNA PÁGINA UTILICE **UN CERTIFICADO QUE NO HAYA SIDO EMITIDO POR UNA CA RAÍZ DE CONFIANZA, EL NAVEGADOR MOSTRARÁ UN AVISO**:

ESTE TIPO DE AVISOS SON FUNDAMENTALES PARA **EVITAR ATAQUES TIPO PHISING**, TALES COMO AQUELLOS QUE REPLICAN LA PÁGINA DE UN BANCO Y EMPLEAN INGENIERÍA SOCIAL PARA ENGAÑAR AL USUARIO.

3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

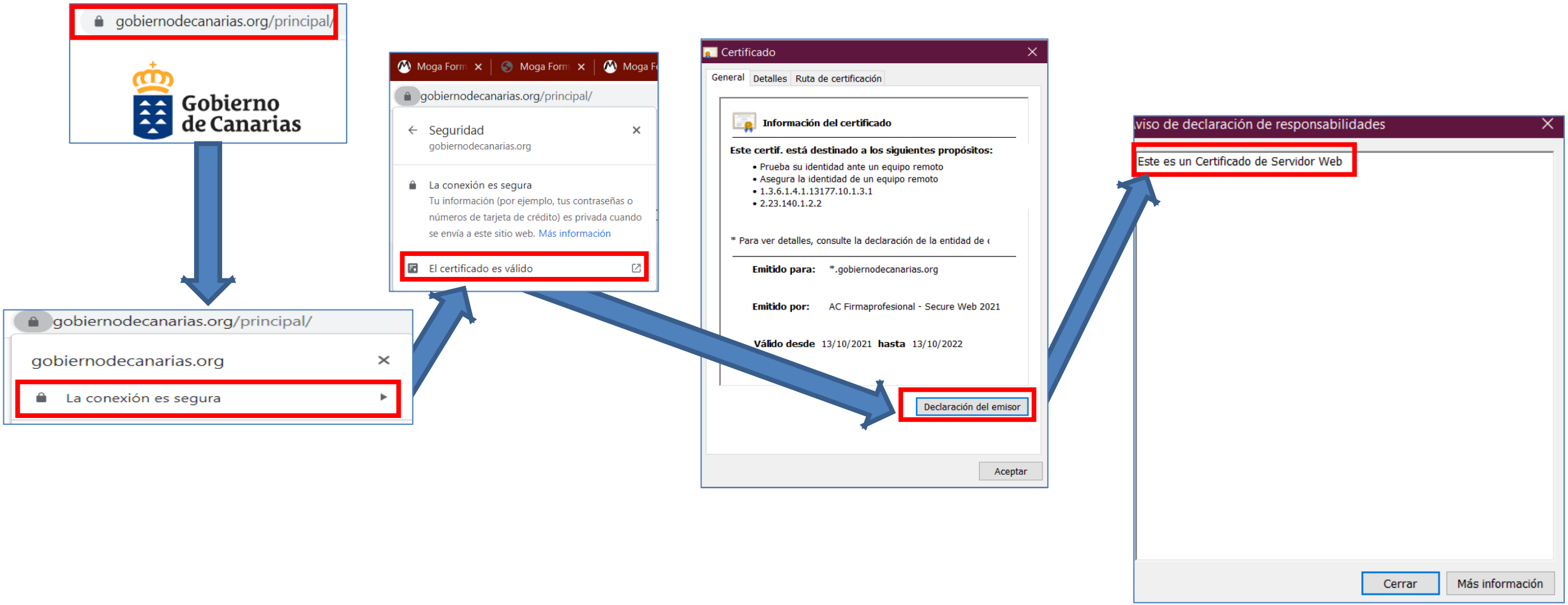
ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

SI EL **CERTIFICADO NO** ES **VÁLIDO O** YA **HA EXPIRADO**, EL NAVEGADOR TAMBIÉN **MUESTRA** HABITUALMENTE **UN MENSAJE**:



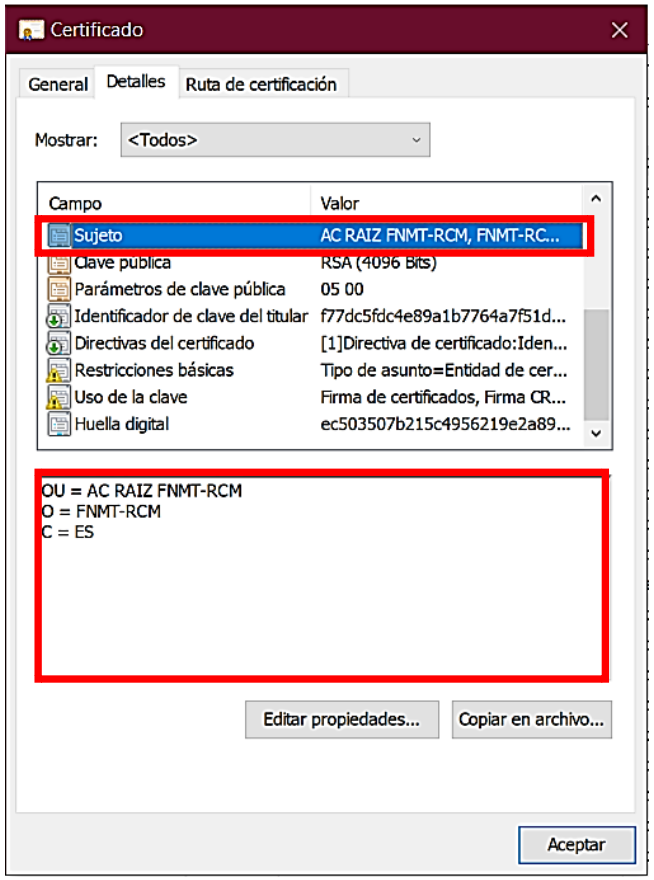
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

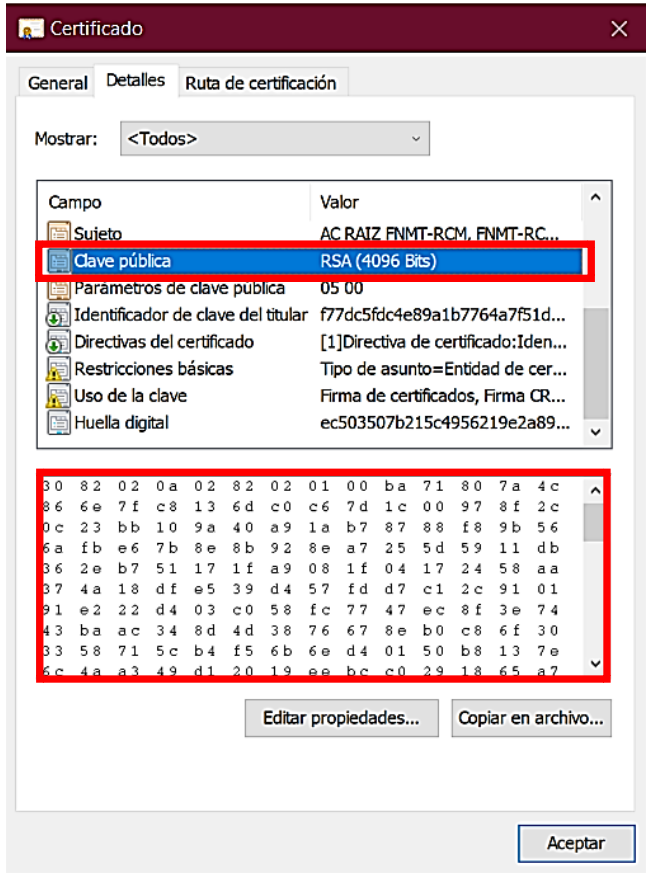
ASPECTOS PRÁCTICOS: VALIDACIÓN EN LOS NAVEGADORES

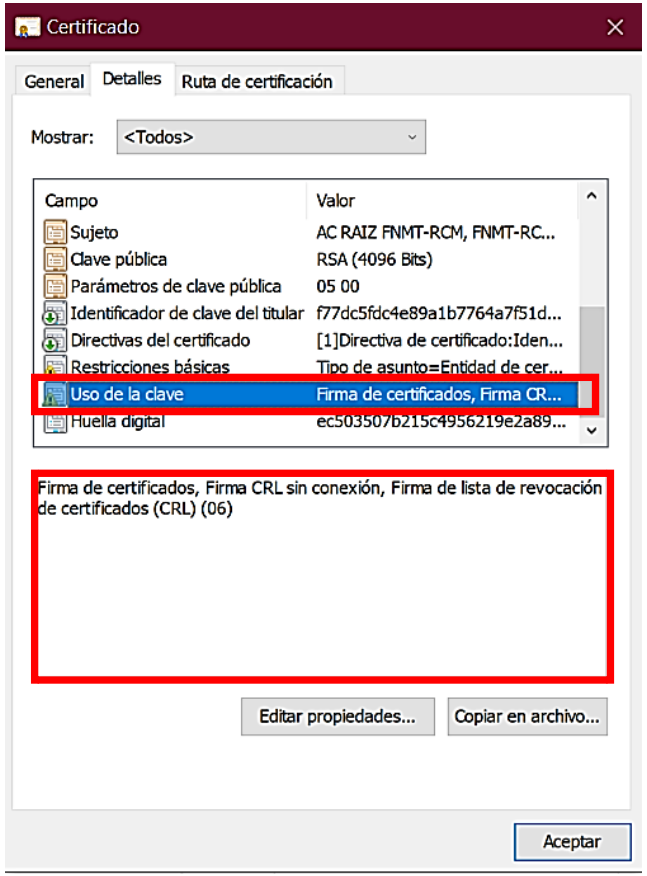


3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

CERTIFICADO DE AUTORIDAD DE CERTIFICACIÓN







CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. **POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)**
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

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

SE DESCRIBEN LOS CONCEPTOS DE **POLÍTICA DE CERTIFICACIÓN** (**CP CERTIFICATION POLICY**) Y **DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN** (**CERTIFICATION POLICY STATEMENT, CPS**), PRESENTÁNDOSE EN ESTE APARTADO TANTO LA DEFINICIÓN DE CADA UNO DE ESTOS CONCEPTOS COMO LAS DIFERENCIAS ENTRE AMBOS.

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

POLÍTICA DE CERTIFICACIÓN

CONSIDERANDO QUE UN CERTIFICADO ES EMITIDO POR UNA DETERMINADA **CA**, VINCULANDO A UN USUARIO CON UN PAR DE CLAVES, **HAY QUE DETERMINAR EL GRADO CON EL QUE EL USUARIO PUEDE CONFIAR EN EL CERTIFICADO OBTENIDO.**

ESTE PROCESO HA DE SER REALIZADO POR EL PROPIO USUARIO O ALGUNA ENTIDAD QUE CONTROLE EL MODO EN EL QUE LOS USUARIOS O SUS APLICACIONES HACEN USO DE LOS CERTIFICADOS.

MUCHOS PUEDEN SER LOS CERTIFICADOS UTILIZADOS, ASÍ COMO LAS APLICACIONES Y OBJETIVOS DE CADA UNO DE ELLOS.

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

POLÍTICA DE CERTIFICACIÓN

SE DISTINGUEN UN PAR DE CATEGORÍAS:

- LAS **CP** QUE INDICAN LA **APLICACIÓN DE UN CERTIFICADO EN UNA COMUNIDAD CONCRETA**, ENFOCADAS A ESTABLECER LOS REQUISITOS PARA EL USO DE LOS CERTIFICADOS Y PARA LOS MIEMBROS DE LA COMUNIDAD QUE HACE USO DE ELLOS.
- LAS **CP** QUE INDICAN LA **APLICACIÓN DE UN CERTIFICADO A UN TIPO DE APLICACIÓN** CON UNOS OBJETIVOS COMUNES DE SEGURIDAD, CUYO PROPÓSITO ES IDENTIFICAR EL CONJUNTO DE APLICACIONES Y LOS USOS DE LOS CERTIFICADOS Y ESTABLECER LOS NIVELES DE SEGURIDAD EN CADA CASO, LOS CUALES SE DIVIDEN EN TIPOS O CLASES.

  ADEMÁS, ESTA ÚLTIMA CATEGORÍA ESTABLECE LOS REQUISITOS QUE LA PKI HA DE CUMPLIR EN LAS APLICACIONES Y USOS IDENTIFICADOS.

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

POLÍTICA DE CERTIFICACIÓN

LOS CERTIFICADOS PROPORCIONADOS EN UNA PKI TIENEN UN PROPÓSITO CONCRETO, POR ESTAR VINCULADOS A UNA DETERMINADA APLICACIÓN, Y POR ELLO ES IMPORTANTE EL ESTABLECIMIENTO DE UNA **CP** QUE INDIQUE LOS USOS DE LOS CERTIFICADOS EXPEDIDOS.

LAS **CP** SE IDENTIFICAN CON UN **IDENTIFICADOR DE OBJETO** (**OBJECT IDENTIFIER, OI**). DICHO IDENTIFICADOR PUEDE SER REGISTRADO Y ASOCIADO CON UNA ORGANIZACIÓN EN CONCRETO, SIENDO LA ENTIDAD QUE REALIZA EL REGISTRO LA QUE PUEDE PUBLICAR EL TEXTO DE LAS **CP**.

CADA CERTIFICADO ESTÁ ASOCIADO A UNA O MÚLTIPLES **CP**, INDICÁNDOSE ESTE HECHO DENTRO DEL CAMPO "**POLÍTICAS DEL CERTIFICADO**"

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

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)

LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ES UN DOCUMENTO ELABORADO POR UNA AUTORIDAD DE CERTIFICACIÓN QUE **RECOGE O REGULA LA PRESTACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN POR PARTE DE DICHA AUTORIDAD DE CERTIFICACIÓN EN SU CONDICIÓN DE PRESTADOR DE SERVICIOS DE CERTIFICACIÓN**.

SE REGULA, ENTRE OTRAS COSAS, LA GESTIÓN DE LOS DATOS DE CREACIÓN Y VERIFICACIÓN DE FIRMA Y DE LOS CERTIFICADOS, LAS CONDICIONES APLICABLES A LA SOLICITUD, EXPEDICIÓN, USO, SUSPENSIÓN Y EXTINCIÓN DE LA VIGENCIA DE LOS CERTIFICADOS.

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

DIFERENCIAS ENTRE POLÍTICA DE CERTIFICACIÓN Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

LAS DIFERENCIAS SE PUEDEN RESUMIR:

- **EL OBJETIVO DE LA CP ES ESTABLECER QUÉ DEBEN HACER LOS PARTICIPANTES**. EN CAMBIO**, LA CPS DETERMINA CÓMO UNA CA IMPLEMENTAN LOS PROCEDIMIENTOS Y CONTROLES** PARA SATISFACER LOS REQUISITOS ESTABLECIDOS POR LA **CP**.
- 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.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. **LISTA DE CERTIFICADOS REVOCADOS (CRL)**
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

CUANDO EL PROPIETARIO DE UN CERTIFICADO CONSIDERA QUE ESTE YA NO ES VÁLIDO, PUEDE LLEVAR A CABO LA **REVOCACIÓN** DEL MISMO. LAS **RAZONES DE REVOCACIÓN** DE UN CERTIFICADO SON NUMEROSAS:

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

LAS **RAZONES** DE REVOCACIÓN DE UN CERTIFICADO SON NUMEROSAS:

- 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)

LA **EMISIÓN DE LAS CRL PUEDE REALIZARSE** TANTO **POR LA CA** COMO **POR OTRA ENTIDAD DELEGADA.**

CUANDO UN SISTEMA HACE USO DE UN CERTIFICADO, EN EL PROCESO DE VERIFICACIÓN SE GARANTIZA QUE EL NÚMERO DE SERIE DEL CERTIFICADO A UTILIZAR NO SE ENCUENTRA EN LA **CRL**.

LAS CRL SE ACTUALIZAN PERIÓDICAMENTE (CADA HORA, DÍA O SEMANA), CONSIGUIENDO VERIFICACIONES SOBRE LISTAS LO SUFICIENTEMENTE ACTUALIZADAS.

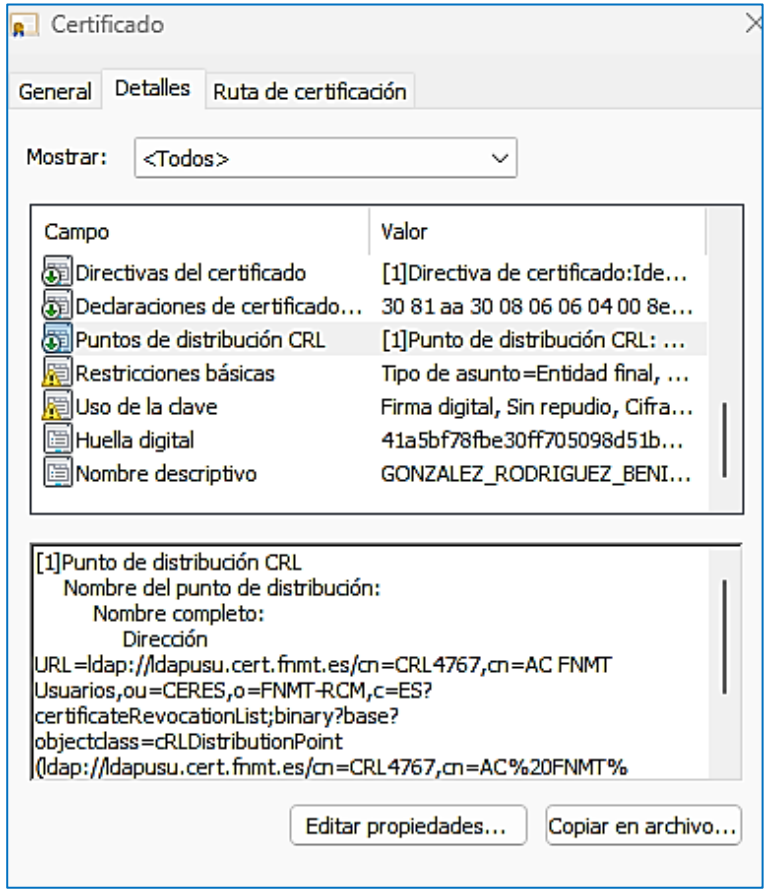
ES IMPORTANTE CONSIDERAR QUE **EN LA CRL SE MANTENDRÁ LA IDENTIFICACIÓN DE LOS CERTIFICADOS REVOCADOS HASTA QUE ESTOS EXPIREN**.

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

HAY QUE DESTACAR QUE **LA PERIODICIDAD DE ACTUALIZACIÓN DE CRL ES MUY IMPORTANTE.** DE NO SER MUY FRECUENTE ES POSIBLE CONSIDERAR VÁLIDOS CERTIFICADOS QUE DEBERÍAN SER REVOCADOS.

UNA EXTENSIÓN DENTRO DE LOS CERTIFICADOS (**CRLDISTRIBUTIONPOINT**) PERMITE **INDICAR LOS PUNTOS DE DISTRIBUCIÓN DE CRL**.

ASÍ, ES POSIBLE CONOCER DÓNDE OBTENER LA **CRL** QUE INFORMA DEL ESTADO DE REVOCACIÓN DEL CERTIFICADO ASOCIADO.



5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

FORMATO DE UNA LISTA DE REVOCACIÓN DE CERTIFICADOS

LA **CRL ESTÁ COMPUESTA POR LOS SIGUIENTES CAMPOS**:

- **ALGORITMO DE FIRMA:** ALGORITMO UTILIZADO PARA FIRMAR LA LISTA
- **VALOR DE LA FIRMA:** FIRMA DE LA LISTA
- **NOMBRE EMISOR:** NOMBRE DE LA ENTIDAD EMISORA DE CRL
- **DÍA DE EMISIÓN:** DÍA EN EL QUE SE REALIZA LA EMISIÓN DE LA CRL
- **DÍA EMISIÓN NUEVA LISTA:** DÍA DE EMISIÓN DE LA NUEVA CRL
- **LISTA DE CERTIFICADOS REVOCADOS:** Nº. SERIE Y FECHA DE REVOCACIÓN.
- **EXTENSIONES:** CAMPOS OPCIONALES.

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

CONCEPTO DE DELTA CRL

LA **CRL SE PUBLICA PERIÓDICAMENTE**. ESTO 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. LISTA DE CERTIFICADOS REVOCADOS (CRL)

CONCEPTO DE DELTA CRL

LA **DELTA CRL** REDUCE EL PERIODO DE INCERTIDUMBRE.

ESTO INTRODUCE UNA MAYOR SOBRECARGA EN LA AUTORIDAD, QUE VE ASÍ INCREMENTADA LA FRECUENCIA CON LA QUE PUBLICAR ESTA INFORMACIÓN.

SE TRATA DE UN MECANISMO QUE DEBE CALIBRARSE ADECUADAMENTE PARA COMPENSAR LOS BENEFICIOS CON EL ESFUERZO NECESARIO.

LAS **DELTA CRL** SUPONEN UNA REDUCCIÓN DEL PROBLEMA PLANTEADO, PERO **NO PROPORCIONAN UNA INMEDIATEZ COMPLETA**.

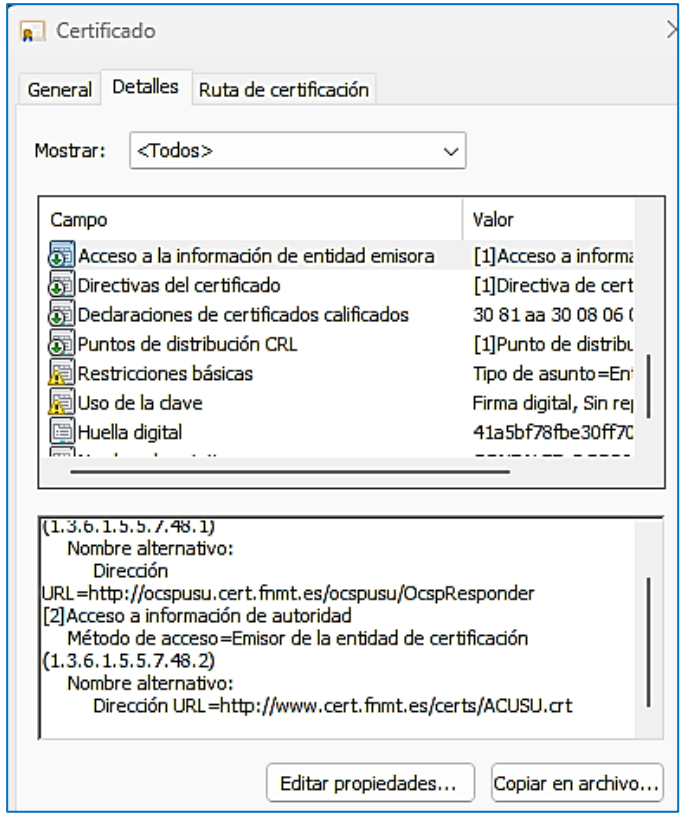
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

ES UN PROTOCOLO DESARROLLADO 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.

OCSP ESPECIFICA LOS DATOS QUE NECESITA INTERCAMBIAR UNA APLICACIÓN CON UN SERVIDOR **OCSP** PARA CONOCER EL ESTADO DE UN DETERMINADO CERTIFICADO.



5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

LA COMUNICACIÓN SE COMPONE DE UN PAR DE MENSAJES:

- **SOLICITUD**

  SE REALIZA DESDE UN CLIENTE **OCSP** A UN SERVIDOR **OCSP** Y CONTIENE LA VERSIÓN DEL PROTOCOLO, EL SERVICIO SOLICITADO, EL IDENTIFICADOR DEL CERTIFICADO DEL CUAL SE DESEA CONOCER EL ESTADO Y, OPCIONALMENTE, EXTENSIONES.

- **RESPUESTA**

  EL SERVIDOR **OCSP** RESPONDE AL CLIENTE **OCSP**. HAY MÚLTIPLES TIPOS DE RESPUESTA. TODAS LAS RESPUESTAS HAN DE SER FIRMADAS POR EL SERVIDOR **OCSP**.

5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

EL PROTOCOLO **OCSP** PROPORCIONA INFORMACIÓN ACTUALIZADA.

LA UTILIZACIÓN DE **OCSP** ELIMINA LA NECESIDAD DE PROCESAR **CRL** Y, AL CONTENER MENOR INFORMACIÓN QUE UNA TÍPICA **CRL**, ES POSIBLE HACER UN USO MÁS EFICIENTE DE LOS RECURSOS TANTO EN CLIENTE COMO EN SERVIDOR.

OCSP NO SE INTERCAMBIA INFORMACIÓN CONSIDERADA SENSIBLE, LA CUAL SÍ SE INTERCAMBIA EN LAS **CRL**.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. **FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)**
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

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

UNA SOLICITUD DE FIRMA DE CERTIFICADO (**CSR**) CONSTITUYE UNO DE LOS PRIMEROS PASOS HACIA LA OBTENCIÓN DE UN CERTIFICADO **SSL/TLS**.

LA **CSR**, QUE SE GENERA EN EL MISMO SERVIDOR EN EL QUE POSTERIORMENTE SE INSTALARÁ EL CERTIFICADO, CONTIENE LA INFORMACIÓN (P. EJ., NOMBRE COMÚN, ORGANIZACIÓN, PAÍS) QUE LA **CA** UTILIZARÁ PARA CREAR EL CERTIFICADO.

TAMBIÉN CONTIENE LA CLAVE PÚBLICA QUE SE INCLUIRÁ EN EL CERTIFICADO, Y SE FIRMA CON LA CORRESPONDIENTE CLAVE PRIVADA.

LAS **CSR** SE USAN PARA PROPORCIONAR A LAS **CA** TODA LA INFORMACIÓN NECESARIA PARA LA EMISIÓN DE CERTIFICADOS, EVITANDO PROPORCIONAR LA CLAVE PRIVADA DEL SOLICITANTE.

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

SE PUEDEN DISTINGUIR LAS **FASES**:

1. **EL USUARIO CONSTRUYE UNA SOLICITUD** DEL **CSR**, LA CUAL ESTÁ COMPUESTA POR TRES GRANDES CAMPOS DE INFORMACIÓN:
   - INFORMACIÓN DE SOLICITUD DEL CERTIFICADO. ESTA INFORMACIÓN CONTIENE:
     - VERSIÓN DE LA SOLICITUD
     - NOMBRE DEL SOLICITANTE
     - CLAVE PÚBLICA DEL SOLICITANTE
     - OTROS ATRIBUTOS QUE PROPORCIONAN INFORMACIÓN ADICIONAL SOBRE EL SOLICITANTE
   - FIRMA DE LA SOLICITUD
   - ALGORITMO UTILIZADO PARA REALIZAR LA FIRMA.

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

2. **EL SOLICITANTE FIRMA LA SOLICITUD** (CON SU CLAVE PRIVADA).
3. **LA SOLICITUD, LA FIRMA Y EL ALGORITMO DE FIRMA SON ENVIADOS A LA CA**, LA CUAL COMPLETA LA PETICIÓN AUTENTICANDO AL SOLICITANTE Y VERIFICANDO LA FIRMA REALIZADA.
4. **SE CONSTRUYE UN CERTIFICADO DE CLAVE PÚBLICA CON TODOS LOS CAMPOS** (NOMBRE DEL SOLICITANTE Y SU CLAVE PÚBLICA, EL NOMBRE DE LA **CA** EMISORA, EL NÚMERO DE SERIE DE LA **CA**, EL PERIODO DE VALIDEZ DEL CERTIFICADO Y EL ALGORITMO DE FIRMA).

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. **INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)**
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

LAS INFRAESTRUCTURAS DE GESTIÓN DE PRIVILEGIO (**PMI, PRIVILEGE MANAGEMENT INFRASTRUCTURE**), **PERMITEN ADMINISTRAR DE MANERA EFICAZ LOS PERMISOS O ACCIONES** QUE UNA DETERMINADA ENTIDAD ESTÁ AUTORIZADA A REALIZAR

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

A CONTINUACIÓN, SE PRESENTAN LAS DISTINTAS ENTIDADES QUE PARTICIPAN EN UNA **PMI.**

POSTERIORMENTE, SE DESCRIBE EL PROCESO POR EL QUE SE VERIFICAN LOS PRIVILEGIOS ESGRIMIDOS.

EN TERCER LUGAR, SE DETALLA CÓMO SE APLICA ESTE CONCEPTO EN EL TERRENO DEL CONTROL DE ACCESO.

FINALMENTE, SE SEÑALAN LAS DIFERENCIAS ENTRE ESTA INFRAESTRUCTURA Y UNA DE CLAVE PÚBLICA (**PKI**).

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

ENTIDADES PARTICIPANTES

UNA **PMI** SE COMPONE DE DIVERSAS ENTIDADES. DEBE TENERSE EN CUENTA QUE EXISTEN DIFERENTES FASES DENTRO DEL CICLO DE VIDA DE UN **CERTIFICADO DE ATRIBUTOS**:

EMISIÓN, VERIFICACIÓN Y REVOCACIÓN

EN CADA UNA DE ELLAS, UN GRUPO DISTINTO DE ENTIDADES PARTICIPAN EN DIVERSO GRADO.

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

ENTIDADES PARTICIPANTES

LA **EMISIÓN DE LOS CERTIFICADOS** CORRE A CARGO DE LA **FUENTE DE AUTORIDAD** (**SOA, SOURCE OF AUTHORITY**).

ESTA ENTIDAD EMITE LOS CERTIFICADOS ESPECIFICANDO QUÉ PRIVILEGIO SE CONCEDE AL TITULAR DEL MISMO. DICHO PRIVILEGIO O PERMISO SE ESPECIFICA A TRAVÉS DE UNO O VARIOS ATRIBUTOS.

EL TITULAR DEL CERTIFICADO PUEDE TENER LA CAPACIDAD PARA **TRANSFERIR EL PRIVILEGIO**.

EN FUNCIÓN DE ESTO, SURGEN DOS TIPOS DE ENTIDADES QUE PUEDEN SER TITULARES: **AUTORIDAD DE ATRIBUTOS** (**AA, ATTRIBUTE AUTHORITY**) Y **PROPIETARIO DEL PRIVILEGIO** (**PH, PRIVILEGE HOLDER**).

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

ENTIDADES PARTICIPANTES

LA **VERIFICACIÓN DEL CERTIFICADO** TIENE HABITUALMENTE LUGAR CUANDO EL TITULAR DEL PRIVILEGIO DESEA EJERCERLO.

ES EL CASO, POR EJEMPLO, DEL ACCESO A UN RECURSO ELECTRÓNICO DESDE UN EQUIPO CORPORATIVO: EL TITULAR DEBE ACREDITAR QUE ESTÁ AUTORIZADO A CONSULTAR DICHO RECURSO.

EN ESE MOMENTO, EL VERIFICADOR (**PRIVILEGE VERIFIER**) COMPRUEBA LA VALIDEZ Y VIGENCIA DEL CERTIFICADO DE ATRIBUTOS QUE REFLEJA LA EXISTENCIA DEL PRIVILEGIO.

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

ENTIDADES PARTICIPANTES

LA COMPROBACIÓN DE LA VALIDEZ CONLLEVA TAMBIÉN LA **REVISIÓN DEL ESTADO DEL CERTIFICADO**. LOS CERTIFICADOS DE ATRIBUTOS PUEDEN SER VÁLIDOS, ESTAR CADUCADOS O SER REVOCADOS.

PARA HACER EFECTIVA LA REVOCACIÓN ES NECESARIA LA PARTICIPACIÓN DE LA **SOA**, QUIEN EMITE LA CORRESPONDIENTE REVOCACIÓN. ESTA QUEDA INCLUIDA EN LA **LISTA DE CERTIFICADOS DE ATRIBUTOS REVOCADOS** (**ACRL, ATTRIBUTE CERTIFICATE REVOCATION LIST**).

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

PROCESO DE VERIFICACIÓN DE PRIVILEGIOS

EL **PROCESO DE VERIFICACIÓN** COMPRENDE LAS SIGUIENTES ACCIONES:

1. EL PROPIETARIO DEL PRIVILEGIO SOLICITA REALIZAR UNA DETERMINADA ACCIÓN SOBRE UN RECURSO.
2. EL **VERIFICADOR** COMPRUEBA QUE LOS ATRIBUTOS (PRIVILEGIOS) DEL SOLICITANTE SE AJUSTAN A LOS NECESARIOS PARA REALIZAR LA ACCIÓN. PARA ELLO, TOMA EN CONSIDERACIÓN LOS DATOS DEL CERTIFICADO, EL RECURSO SOLICITADO Y, EVENTUALMENTE, OTROS PARÁMETROS DEL CONTEXTO (POR EJEMPLO, LA FECHA Y HORA EN QUE SE PRODUCE LA SOLICITUD). EN CASO DE QUE NO SE AJUSTE A LO ESTABLECIDO, DENIEGA EL PERMISO.

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

PROCESO DE VERIFICACIÓN DE PRIVILEGIOS

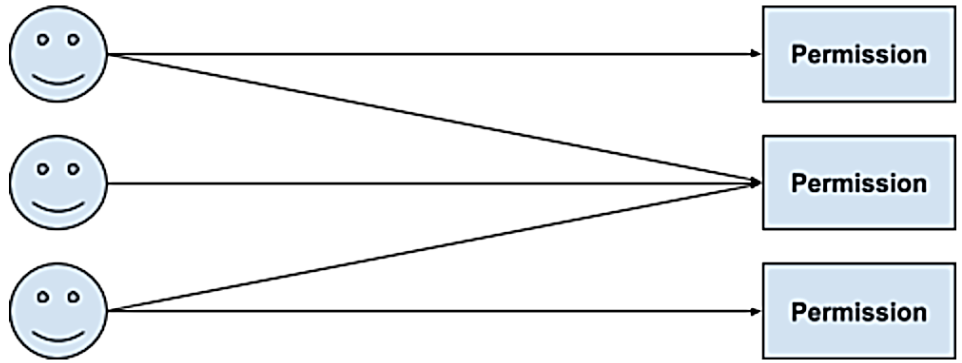
3. EL **VERIFICADOR** ESTABLECE AHORA LA VIGENCIA DEL CERTIFICADO DE ATRIBUTOS, PARA LO QUE EFECTÚA DOS ACCIONES PRINCIPALES:
   A. **COMPROBAR LA VALIDEZ DE LA CADENA DE CERTIFICACIÓN**, ESTABLECIENDO SI LA FIRMA DEL CERTIFICADO DE ATRIBUTOS ES CORRECTA Y SI CORRESPONDE A UNA AUTORIDAD CORRECTAMENTE AUTENTICADA Y CONFIABLE.
   B. **COMPROBAR SI EL CERTIFICADO ESTÁ REVOCADO** DE ACUERDO A LA LISTA DE CERTIFICADOS DE ATRIBUTOS REVOCADOS PUBLICADA POR LA **SOA**.

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

APLICACIÓN DE PMI PARA EL CONTROL DE ACCESO

UNA DE LAS APLICACIONES DE LOS **PMI** ES EN LOS **SISTEMAS DE CONTROL DE ACCESO**. SE ENCARGAN DE CONTROLAR QUIÉN PUEDE ACCEDER A QUÉ RECURSOS Y CON QUÉ FINES.

UN MODELO ES EL **MODELO DISCRECIONAL** (**DAC, DISCRETIONARY ACCESS CONTROL**), EN EL QUE LA ASIGNACIÓN DE PRIVILEGIOS A PERSONAS Y RECURSOS SE HACE DE FORMA PARTICULARIZADA.



7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

APLICACIÓN DE PMI PARA EL CONTROL DE ACCESO

OTRO MODELO DE CONTROL DE ACCESO, MÁS EFICAZ EN SU GESTIÓN QUE EL DAC ANTERIORMENTE INTRODUCIDO, ES EL **SISTEMA DE ACCESO MULTINIVEL**.

ESTE TIPO DE SISTEMAS SON AMPLIAMENTE UTILIZADOS **EN ENTORNOS DONDE EXISTEN DIFERENTES NIVELES DE CONFIDENCIALIDAD DE LA INFORMACIÓN**, COMO PUEDEN SER LOS ÁMBITOS DE LOS CUERPOS DE SEGURIDAD. EN ESTOS SISTEMAS SE ASOCIA A CADA RECURSO CON UNA ETIQUETA (POR EJEMPLO, “CONFIDENCIAL”, “ALTO SECRETO”).

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

APLICACIÓN DE PMI PARA EL CONTROL DE ACCESO

FINALMENTE, EN LOS ÚLTIMOS TIEMPOS SE ESTÁ GENERALIZANDO EL **CONTROL DE ACCESO BASADO EN ROLES** (**RBAC, ROLE-BASED ACCESS CONTROL**).

GRACIAS A LOS ROLES, ES POSIBLE OTORGAR UNA SERIE DE PRIVILEGIOS A TODOS LOS SUJETOS QUE DISPONGAN DE ÉL. UNA VENTAJA ADICIONAL ES QUE EXISTEN VARIANTES DE RBAC EN LAS QUE ES POSIBLE CONSTRUIR JERARQUÍAS DE ROLES, DE FORMA QUE SE FACILITE LA GESTIÓN DE LOS PRIVILEGIOS ASOCIADOS.

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

COMPARACIÓN CON RESPECTO A UNA PKI

TENIENDO EN CUENTA QUE TANTO LA **PKI** COMO LA **PMI** ESTÁN DEFINIDAS DENTRO DE LA NORMA **X.509**, ES RAZONABLE PENSAR QUE EXISTEN ANALOGÍAS SUSTANCIALES ENTRE AMBAS ESTRUCTURAS.

- TANTO **PKI** COMO **PMI SE CENTRAN EN LA GESTIÓN DE CERTIFICADOS**: MIENTRAS QUE LOS CERTIFICADOS DE CLAVE PÚBLICA LIGAN A UNA ENTIDAD CON DICHA CLAVE, LOS DE ATRIBUTOS RELACIONAN AL TITULAR CON CIERTAS PROPIEDADES.

7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

COMPARACIÓN CON RESPECTO A UNA PKI

- RESPECTO AL **CONCEPTO DE JERARQUÍA DE ENTIDADES**:
  - EN UNA **PKI**, EXISTE UNA **AUTORIDAD RAÍZ CA** Y UNA O VARIAS AUTORIDADES SUBORDINADAS
  - EN PMI, EL **SOA** EJERCE DE **AUTORIDAD RAÍZ** MIENTRAS QUE LAS AUTORIDADES DE ATRIBUTOS **AA** PUEDEN EMITIR CERTIFICADOS PARA DELEGAR SUS PRIVILEGIOS A UN TERCERO.
- EN AMBAS ESTRUCTURAS EXISTE UN MECANISMO SIMILAR PARA LA GESTIÓN DE LA REVOCACIÓN. EN UNA **PKI** LOS CERTIFICADOS SE INCLUYEN EN UNA **CRL**, EN LA **PMI** LO HACEN EN UNA **ACRL**.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. **CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES**
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

CAMPOS DE LOS CERTIFICADOS DE ATRIBUTOS

LOS **CA** ESTÁN COMPUESTOS POR LOS SIGUIENTES CAMPOS:

- **VERSIÓN:** VERSIÓN DEL CERTIFICADO.
- **PROPIETARIO** (**HOLDER**): ES UNA SECUENCIA CUYO PROPÓSITO ES LA IDENTIFICACIÓN DEL PROPIETARIO.
- **NOMBRE DEL EMISOR: SOA** EMISORA DE LOS CERTIFICADOS DE ATRIBUTOS.
- **ALGORITMO DE FIRMA**: ALGORITMO UTILIZADO PARA FIRMAR EL CERTIFICADO.
- **FIRMA**: FIRMA DEL CERTIFICADO, LA CUAL ES REALIZADA POR LA **SOA** EMISORA.
- **NÚMERO DE SERIE**: NÚMERO ENTERO POSITIVO.
- **PERIODO DE VALIDEZ**: FECHA DE INICIO Y FECHA DE FIN.
- **ATRIBUTOS**: PROPORCIONAN INFORMACIÓN SOBRE EL PROPIETARIO DEL CERTIFICADO. ADEMÁS, SI EL CERTIFICADO SE UTILIZA PARA AUTORIZACIÓN, ESTE CAMPO INCLUIRÁ UN CONJUNTO DE PRIVILEGIOS.

8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

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**
- **EL NO REPUDIO**.

8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

USOS HABITUALES DE LOS CERTIFICADOS DE ATRIBUTOS

CONTROL DE ACCESO

EN MUCHOS CONTEXTOS, BASTA CON MOSTRAR LA PERTENENCIA A UN DETERMINADO ROL O GRUPO. ESTOS ESQUEMAS DE ACCESO SE CONOCEN CON EL NOMBRE DE ***CONTROL DE ACCESO BASADO EN ROLES*.**

CUANDO SE SOLICITA ACCESO CON UN **CERTIFICADO DE ATRIBUTOS**, SE HA DE DETERMINAR QUE EL PROPIETARIO DEL CERTIFICADO ES EL QUE HA REALIZADO LA SOLICITUD.

8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

USOS HABITUALES DE LOS CERTIFICADOS DE ATRIBUTOS

AUTENTICACIÓN EN ORIGEN Y NO REPUDIO

LA FIRMA DIGITAL ES UNO DE LOS MECANISMOS ESENCIALES PARA AUTENTICAR A LA ENTIDAD ORIGEN Y EVITAR EL NO REPUDIO EN EMISIÓN, LOS ATRIBUTOS CONTENIDOS EN EL CERTIFICADO PROPORCIONAN INFORMACIÓN ADICIONAL SOBRE LA ENTIDAD QUE REALIZA LA FIRMA, ES DECIR, EL PROPIETARIO DEL CERTIFICADO.

POR TANTO, ESTA INFORMACIÓN PUEDE SER UTILIZADA PARA ASEGURAR QUE EL PROPIETARIO PUEDE REALIZAR LA FIRMA DE UNOS DETERMINADOS DATOS.

8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

CERTIFICADOS DIGITALES FRENTE A CERTIFICADOS DE ATRIBUTOS

LOS **CERTIFICADOS DIGITALES** VINCULAN A UN INDIVIDUO CON UNA CLAVE PÚBLICA MANTENIÉNDOSE EN SECRETO LA CLAVE PRIVADA ASOCIADA.

EN CAMBIO, LOS **CERTIFICADOS DE ATRIBUTOS** VINCULAN UN CONJUNTO DE ATRIBUTOS BIEN CON UN INDIVIDUO O CON EL IDENTIFICADOR DE UN CERTIFICADO DIGITAL, EL CUAL ES UN PKC.

8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

CERTIFICADOS DIGITALES FRENTE A CERTIFICADOS DE ATRIBUTOS

	Public Key Certificate (PKC)		Attribute Certificate (AC)
Signature	Version	Signature	Version
	Serial Number		Serial Number
	Signature ID		Signature ID
	Subject		Holder
	Issuer		Issuer
	Validity Period		Validity Period
	Subject Public Key Info		Attributes
	Externsions		Externsions

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. **APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI**

9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

LAS APLICACIONES FUNDAMENTALES DE LAS PKI SON:

- **LA AUTENTICACIÓN**
- **LA FIRMA ELECTRÓNICA**
- **EL CIFRADO**

9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

USO DE PKI PARA AUTENTICACIÓN

LA **AUTENTICACIÓN** SE UTILIZA EN MUCHOS TIPOS DE APLICACIONES PARA TENER CONSTANCIA DE QUIÉN ES LA ENTIDAD QUE ESTÁ INTENTANDO HACER USO DE ELLA. CON FRECUENCIA, ESTÁ BASADA EN NOMBRES DE USUARIOS Y CONTRASEÑAS.

LA PKI ES UNA ALTERNATIVA MÁS SEGURA EN LA QUE LA AUTENTICACIÓN SE PRODUCE PROBANDO LA POSESIÓN DE UNA CLAVE PRIVADA EN LUGAR DE UNA CONTRASEÑA.

UN EJEMPLO TÍPICO DE AUTENTICACIÓN ES LA UTILIZACIÓN DEL PROTOCOLO SSL.

9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

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.

ALGUNOS DE LOS EJEMPLOS MÁS TÍPICOS DE FIRMA DIGITAL SON LA FIRMA DE DOCUMENTOS (UTILIZANDO PROGRAMAS COMO MICROSOFT OFFICE O ADOBE READER), O LA FIRMA DE FORMULARIOS ELECTRÓNICOS (COMO LOS UTILIZADOS EN LA ADMINISTRACIÓN PÚBLICA ELECTRÓNICA).

9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

USO DE PKI EN FIRMA

UNA CUESTIÓN CRÍTICA EN EL ÁMBITO DE LAS FIRMAS ES ASEGURAR SU VALIDEZ A LO LARGO DEL TIEMPO. DEBE TENERSE EN CUENTA QUE, **PARA QUE UNA FIRMA SEA VÁLIDA**, ES PRECISO:

1. REALIZAR LA VERIFICACIÓN CRIPTOGRÁFICA DE LA FIRMA, DE ACUERDO AL ALGORITMO SELECCIONADO.
2. VERIFICAR LA CADENA DE CERTIFICACIÓN.

LOS CERTIFICADOS TIENEN DOS FUENTES PRINCIPALES PARA QUEDAR INVALIDADOS: *SU CADUCIDAD O SU REVOCACIÓN*.

SI EL CERTIFICADO DEL FIRMANTE O, EN GENERAL, CUALQUIERA DE LOS CERTIFICADOS DE LA CADENA DE CERTIFICACIÓN, SON INVÁLIDOS CUANDO SE VERIFICA LA FIRMA, LA FIRMA NO SERÁ VÁLIDA.

9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

USO DE PKI EN FIRMA

PARA DAR RESPUESTA A ESTA NECESIDAD HA SURGIDO EL CONCEPTO DE **FIRMA LONGEVA**.

LA FIRMA LONGEVA PERSIGUE MANTENER LA VALIDEZ DE LA FIRMA A LO LARGO DEL TIEMPO.

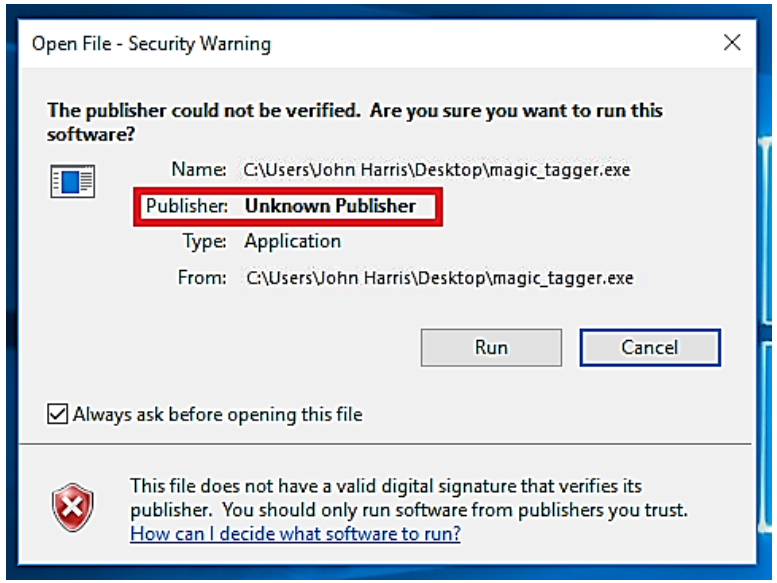
SE PRETENDE CONTRARRESTAR, ADEMÁS, LOS EFECTOS QUE EL PASO DEL TIEMPO PUEDE TENER EN LA SEGURIDAD DE LOS ALGORITMOS (EN LOS QUE SE PUEDEN DESCUBRIR VULNERABILIDADES) O EN LA DISPONIBILIDAD DE LOS MATERIALES (PODRÍA PERDERSE EL CERTIFICADO DE CLAVE PÚBLICA ASOCIADO AL FIRMANTE).

9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

USO DE PKI EN FIRMA

LAS PKI SON TAMBIÉN NECESARIAS PARA LA **FIRMA DEL CÓDIGO FUENTE DE UN PROGRAMA**. GRACIAS A ESTAS FIRMAS, ES POSIBLE ASEGURAR QUE EL CÓDIGO DEL PROGRAMA CUMPLE LAS DOS PROPIEDADES SIGUIENTES:

- NO HA SIDO MANIPULADO DESDE QUE SE CREÓ.
- EL CÓDIGO HA SIDO CREADO, SUPERVISADO O ES RESPONSABILIDAD DE LA ENTIDAD QUE LO FIRMA.

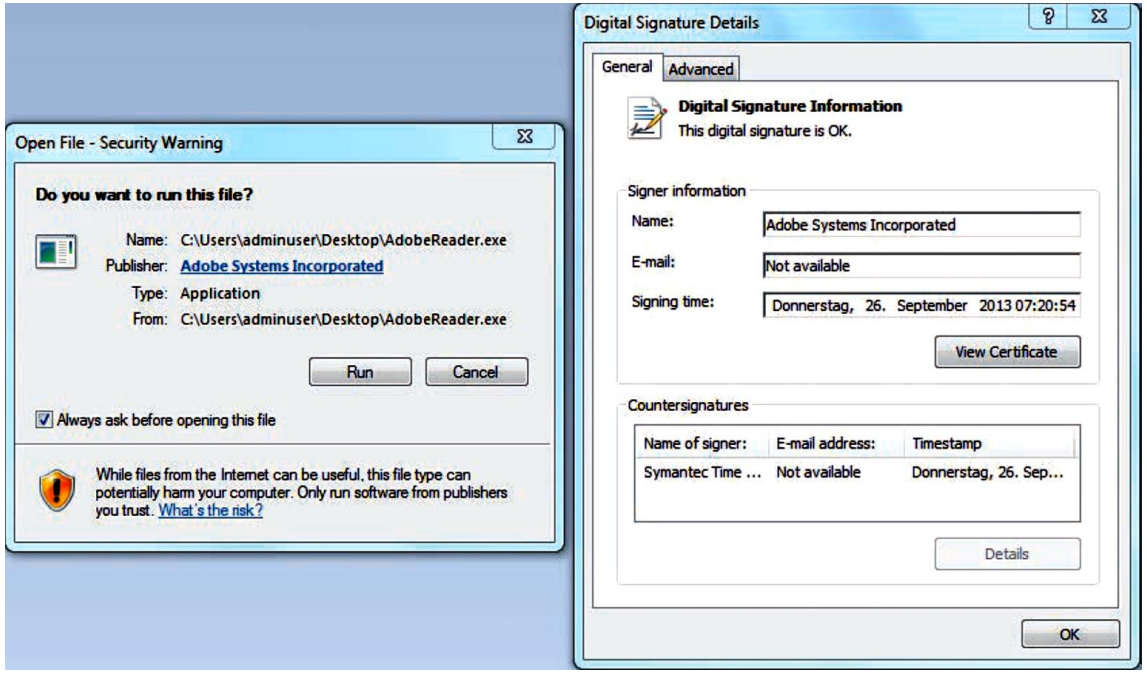


9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

USO DE PKI EN FIRMA

CUANDO EL PROGRAMA ESTÁ CORRECTAMENTE FIRMADO, EL SISTEMA VERIFICA LA FIRMA, INCLUYENDO EL ESTADO DE LOS CERTIFICADOS.

ESTA SITUACIÓN SE REFLEJA EN LA IMAGEN SIGUIENTE.



9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

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.

POR TANTO, LA PRIVACIDAD SE ASEGURA SIEMPRE QUE LA CLAVE PRIVADA SE MANTENGA SECRETA.

EL CIFRADO ES COMÚNMENTE UTILIZADO EN TARJETAS INTELIGENTES PARA ALMACENAR INFORMACIÓN SENSIBLE, EN EL ENVÍO DE CORREOS O EN EL ALMACENAMIENTO DE DATOS DE CARÁCTER CONFIDENCIAL.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

RESUMEN

LAS **INFRAESTRUCTURAS DE CLAVE PÚBLICA** (**PKI**) CONSTITUYEN EL ELEMENTO FUNDAMENTAL QUE PERMITE QUE LOS CERTIFICADOS DIGITALES DE CLAVE PÚBLICA PUEDAN UTILIZARSE DE FORMA MASIVA EN INTERNET.

EN UNA **PKI** PARTICIPAN UNA O VARIAS AUTORIDADES DE CERTIFICACIÓN, RELACIONADAS EN FORMA DE JERARQUÍA O DE RED. PARA QUE LOS USUARIOS PUEDAN DISPONER Y UTILIZAR SUS CERTIFICADOS, ES NECESARIO SOLICITARLOS A TRAVÉS DE PETICIONES **CSR**.

DOS ASPECTOS CLAVE EN LA GESTIÓN DE CERTIFICADOS SON:

- **LA VERIFICACIÓN** DEL MISMO (COMPROBANDO, ENTRE OTRAS CUESTIONES, LA VALIDEZ DE LA CADENA DE CERTIFICACIÓN)
- **LA REVOCACIÓN** (BIEN A TRAVÉS DE LISTAS **CRL** O UTILIZANDO EL PROTOCOLO **OCSP**).

RESUMEN

ASOCIADAS A LAS **PKI** SURGEN LAS **PMI**, O **INFRAESTRUCTURAS DE GESTIÓN DE PRIVILEGIOS**. GRACIAS A ELLAS ES POSIBLE GESTIONAR LOS CERTIFICADOS DE ATRIBUTOS QUE PERMITEN ATESTIGUAR QUE EL PROPIETARIO PUEDE DISFRUTAR DE UN DETERMINADO DERECHO.

LOS CERTIFICADOS DE ATRIBUTOS SON A LOS PRIVILEGIOS LO QUE LOS CERTIFICADOS DE CLAVE PÚBLICA SON A LA IDENTIDAD.

ESTO ES TODO