Curso de bastionado de redes y sistemas

areaproject

2.3.Certificados digitales, gestión de una PKI

Certificado Digital

- ✓ El certificado Digital de un usuario es un documento digital que contienen nuestros datos identificativos autenticados por una entidad ya sea un organismo oficial o alguien que acredite que somos quien decimos ser.
- ✓ Confirman nuestra identidad de manera digital.
- ✓ La clave pública se almacena dentro del certificado y la clave privada será objeto de almacenamiento y custodia por la entidad.
- ✓ Podemos realizar gestiones por ejemplo con la seguridad social, agencia tributaria, registros mercantiles…

Certificado Digital

- ✓ Se pueden emplear para:
  - Firmar correos electrónicos o documentos.
  - Cifrar un mensaje.
- Tipos de certificados:
  - Clase 1, para usuarios y destinado al correo electrónico
  - Clase 2, para organizaciones. Comprobación de identidad
  - Clase 3, para servidores y firmas de programas.
  - Clase 4, trámites online entre empresas.
  - Clase 5, para empresas privadas y de seguridad del gobierno.

Elementos de los certificados digitales

- ✓ Principalmente hay dos tipos de certificados
  - Certificados X.509 emitidos por CA
  - Certificados PGP (Pretty Good Privacy)

- ✓ Características comunes
  - Número de serie
  - Nombre de la entidad emisora
  - Periodo de validez
  - Propietario del certificado
  - Clave pública del propietario del certificado

Infraestructura de clave pública (PKI)

- ✓ ¿Cómo asegurar que la clave pública realmente pertenece al otro interlocutor?
- ✓ Necesidad de gestionar el ciclo de vida de las claves públicas.

Componentes de una PKI

- ✓ Figuran las entidades que se relacionan con la gestión de los certificados de clave pública.
- ✓ Regulado por la norma ITU X.509
- ✓ Las entidades de una PKI
  - Emiten certificados.
  - Renuevan certificados.
  - Verifican y emplean certificados.
  - Revocan certificados.
  - Relación entre ellas.

Entidades participantes de una PKI. CA

- ✓ Las entidades participantes de una PKI se llaman Certificate Authority (CA).
- ✓ Emiten certificados. Actúan como notarios.
- ✓ Acreditan e identifican a una entidad.
- ✓ Realizan funciones de autenticación.
- ✓ Tienen dos atributos principales:
  - Nombre de la CA.
  - Clave pública de la CA.

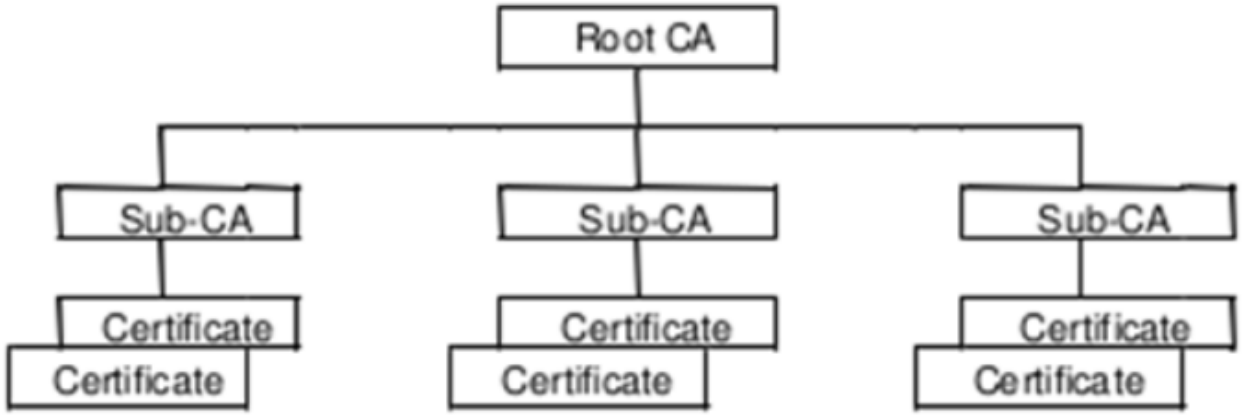
Funciones de una CA

- ✓ Emitir certificados PKC (Public Key Certificate).
- ✓ Mantener actualizada la información sobre los certificados.
- ✓ Emitir y publicar listas de certificados revocados CRL.
- ✓ Mantener histórico del estado de certificados caducados.
- ✓ Un PKC se puede emitir:
  - Personal.
  - Otras CA, cadena de certificación.

- ✓ Los certificados emitidos se firman con la clave privada de la CA.

Estructura de una PKI

- ✓ Modelos jerárquico, en red y puente.
- ✓ Existe una CA raíz, en la que se deposita toda la confianza.
- ✓ Por debajo de la CA raíz se disponen otras CA subordinadas que puede emitir y gestionar certificados.

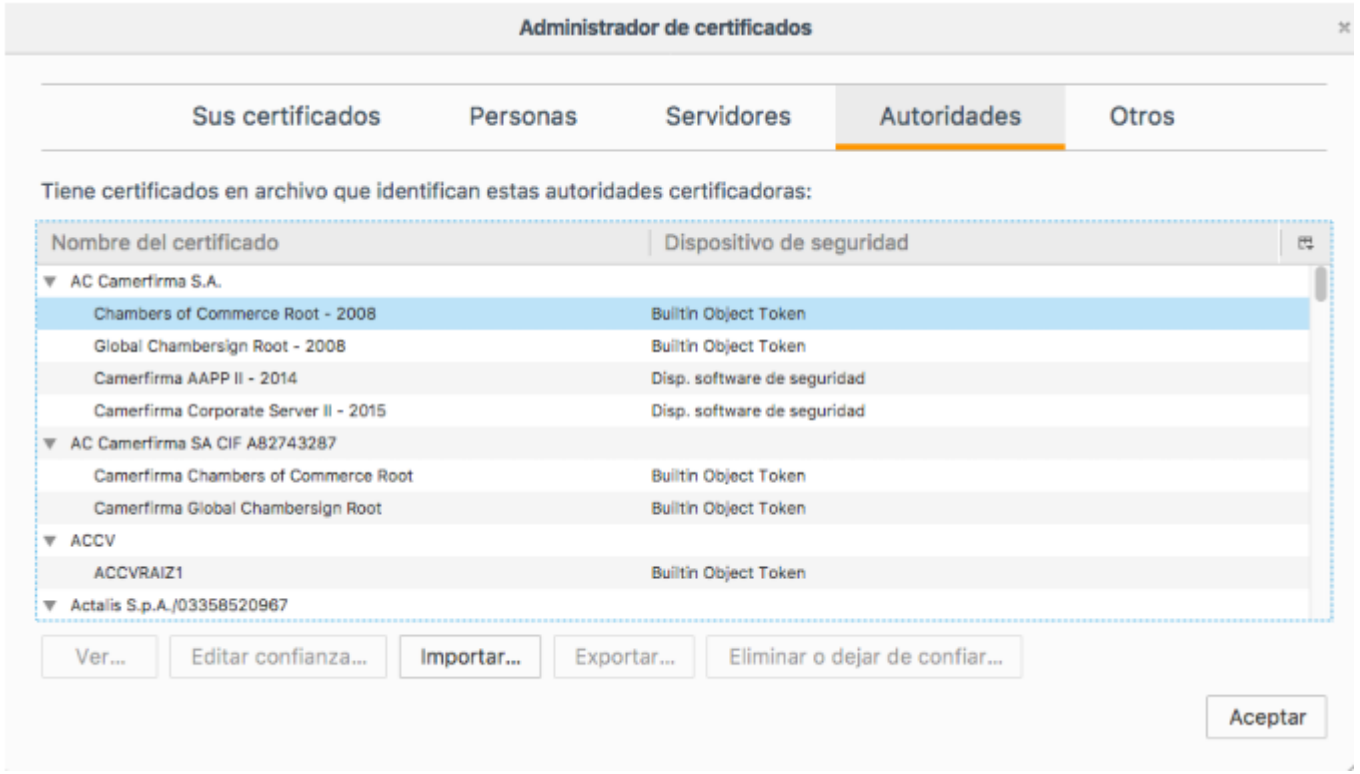


Validación de una cadena de certificación

- ✓ Determinar si un certificado de una entidad final ha sido emitido por una CA de confianza.
- ✓ El primer certificado de la cadena pertenece a una CA de confianza o ha sido emitido por ella (autofirmado).
- ✓ Para las CA intermedias
  - Una CA avala a la siguiente.
  - Todos los certificados intermedios emitidos son válidos.
- ✓ El último certificado de la cadena es el de la entidad final.

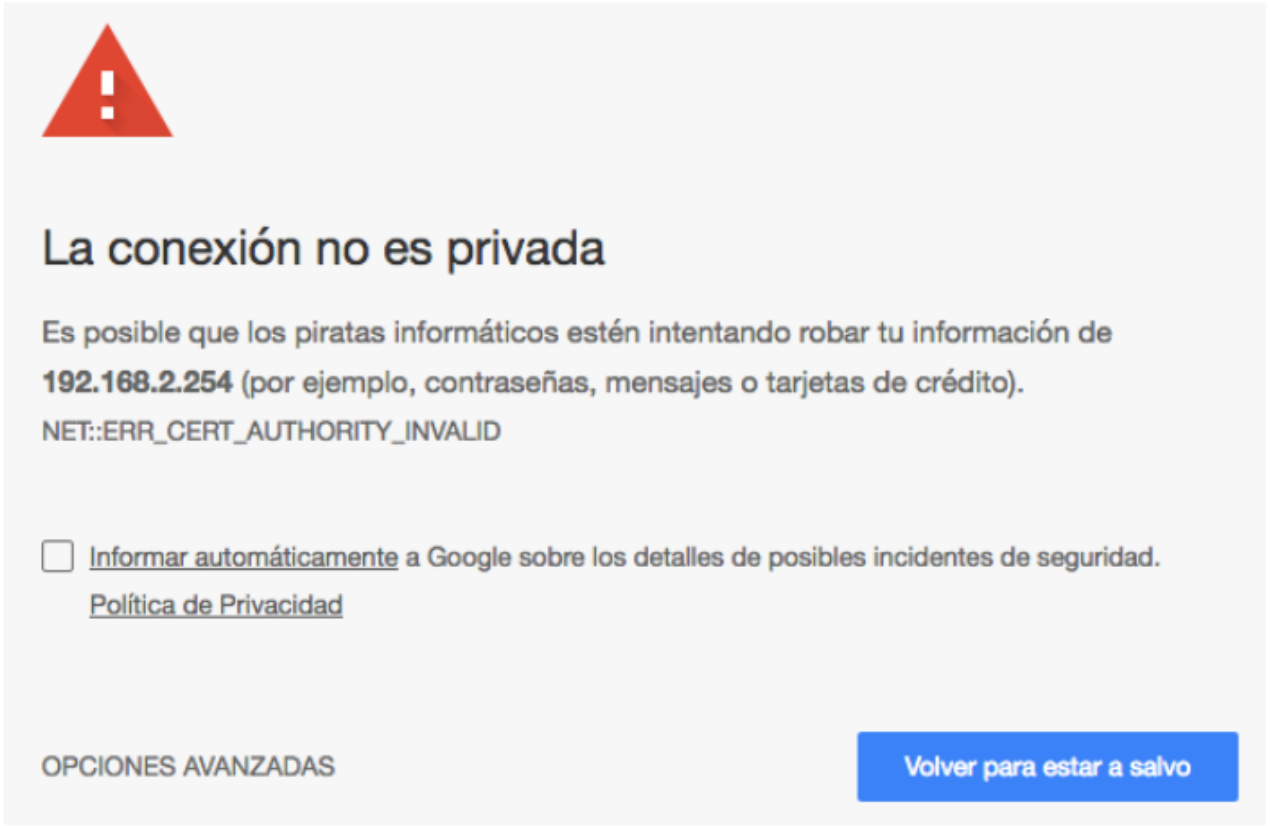
Validación en los navegadores

- ✓ Cuando navegamos por sitios web empleando https el navegador valida los certificados por que tiene instalados los certificados de CA raíz de confianza.



Validación en los navegadores

- ✓ Cuando no se puede verificar el certificado



Lista de certificados revocados

- ✓ Cuando un certificado caduca o el usuario ya no lo necesita, se revoca.
- ✓ Razones:
  - Clave privada comprometida.
  - Clave privada de la CA emisora comprometida.
  - Pérdida de derechos de uso del certificado.
  - Reemplazado por otro certificado.
  - Certificado revocado temporalmente.
- ✓ Las CA mantienen una lista de certificados revocados (CRL) y son responsables de mantener la lista.
- ✓ Un certificado se verifica contra la lista para detectar su validez.

Online Certificate Status Protocol (OCSP)

- ✓ Es un protocolo de X.509 para la revocación de certificados.
- ✓ Facilita la verificación en línea de los certificados debido a CRL desactualizadas.
- ✓ Acciones:
  - Un cliente OCSP solicita a un servidor OCSP información sobre un certificado.
  - El servidor OCSP responde al cliente sobre el estado del certificado.

ADCS- Active Directory Certificate Services

- ✓ Nos evitaría tener que utilizar un tercero para realizar la autenticación, realizando esta comprobación internamente en nuestro sistema.

- ✓ Permite realizar una infraestructura de clave publica (PKI) y proporcionar criptografía de clave publica, certificados digitales y firma electrónica para nuestra organización.

ADCS- Active Directory Certificate Services

✓ Ventajas

- Permite trabajar simultáneamente con Active Directory.
- Mantiene las políticas de grupo y asistentes de AD.
- Automatizaremos la gestión de certificados.
- Instalación automática de certificados.

ADCS- Active Directory Certificate Services

- ✓ Desventajas

  - La CA que crearemos no será reconocida frente a otras entidades oficiales.
  - Tiempo de configuración para su realización y gasto de hardware.

Tendríamos que valorar si queremos realizar esta función o la externalizaremos a un tercero que se encargue de ello

2.4.Aplicación de firma digital

Aplicación de la firma digital

- ✓ La firma digital es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico.

- ✓ Las funciones básicas son:

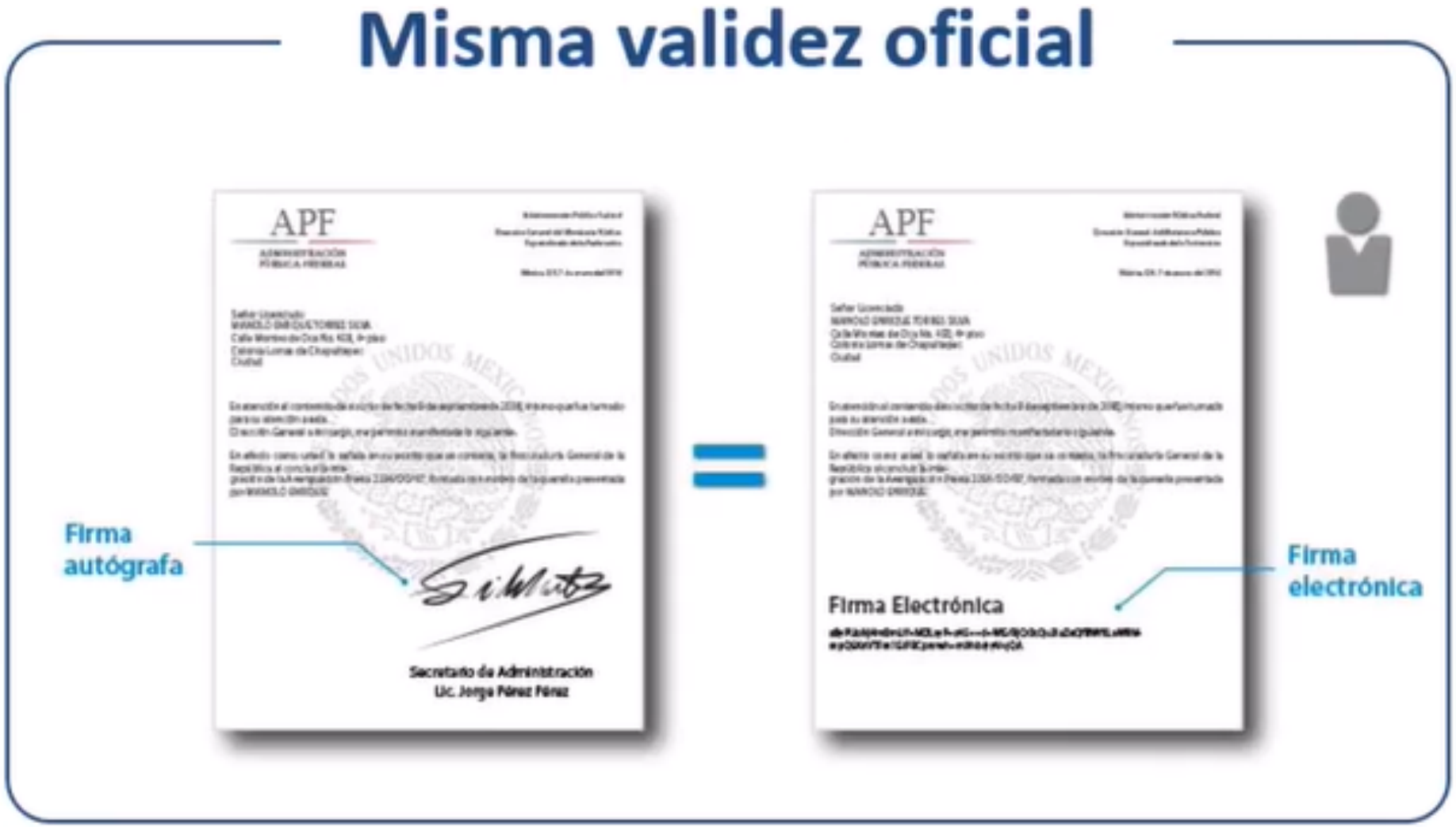
  - Identificar al firmante de manera inequívoca.
  - Asegurar la integridad del documento firmado, el documento es igual al original y no se ha modificado.
  - Asegurar el no repudio del documento firmado dado a que los datos para firmar son únicos y exclusivos del firmante.

Régimen Jurídico Aplicable

- ✓ La base legal de la Firma electrónica está recogida en la Ley 59/2003 de Firma Electrónica y se desarrolla en más profundidad en la sección Base legal de las Firmas.

- ✓ La sección también explora, bajo qué circunstancias la ley equipara la firma electrónica a la firma manuscrita.

Régimen Jurídico Aplicable



Régimen Jurídico Aplicable

- ✓ A escala europea:
  - Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
  - 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 y por la que se deroga la Directiva 1999/93/CE.

Régimen Jurídico Aplicable

- ✓ La legislación en vigor más destacada sobre la firma electrónica a escala europea y estatal es la siguiente.

  - Ley 34/2002, de 11 Julio, de servicios de la sociedad de la información y de comercio electrónico.
  - Ley 59/2003, de 19 de Diciembre, de firma electrónica.
  - Ley 56/2007, de 28 de Diciembre, de Medidas de Impulso de la Sociedad de la Información.

Tipos de Firma

- ✓ Desde el punto de vista legal define la firma electrónica a través de tres tipos:
  - Firma electrónica general.
  - Firma electrónica avanzada.
  - Firma electrónica reconocida.

- ✓ Desde el punto de vista técnico:
  - Firma básica.
  - Firma fechada.
  - Firma validada o firma completa.

Uso de la Firma Electrónica

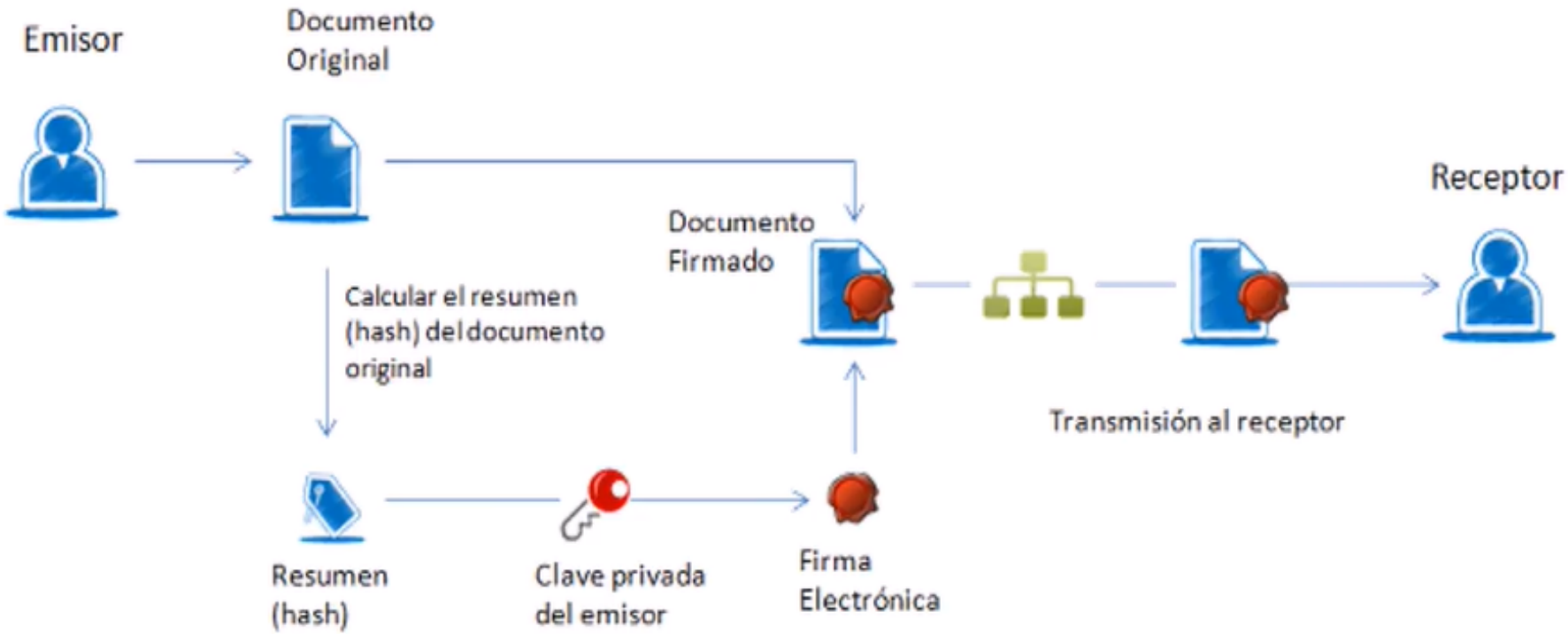
- ✓ Las aplicaciones prácticas de las mismas son:
  - Realización de Declaración de la Renta a través de la red.
  - Firma de documentos única.
  - Firma de documentos por varios firmantes.
  - Cifrado de datos.
  - Firma de contratos.
  - Presentar y liquidar impuestos.

Proceso de la Firma Electrónica

- ✓ Necesitamos tener:
  1. Documento a firmar.
  2. Claves asimétricas vinculadas a nuestra identidad por parte de un tercero de confianza.

- ✓ Necesitamos comprobar:
  1. Que la entidad emisora del certificado es de confianza
  2. El certificado del titular no ha caducado
  3. El certificado del titular ha sido emitido para ese propósito
  4. El certificado del titular no ha sido revocado por su titular

Firma Electrónica Proceso Básico



Comprobación de una Firma Electrónica

- ✓ Necesitamos conocer:

1. El resumen del cifrado (documento firmado).
2. Quien es la Autoridad de Certificación (CA) que emite el certificado.
3. El tipo de función HASH aplicado (SHA-1,SHA-2)
4. El algoritmo de cifrado utilizado (RSA…)
5. El instante en el que se realizó la firma.
6. La vigencia (no renovación) del certificado.

- ✓ Si los códigos hash coinciden, la firma es válida

Ejemplos de firma de documentos

- ✓ Para firmar un documento, salida (documento firmado) entrada (documento a firmar)

  GPG –output doc.sig –sign doc

- ✓ Con un documento con firma digital el usuario puede llevar a cabo dos acciones:
  - Comprobar sólo la firma

    Gpg –verify doc.sig doc

  - Comprobar la firma y recuperar el archivo original

    Gpg –output doc –decrypt doc.sig

Practica

Despliegue de infraestructura de clave pública

areaproject

Curso de bastionado de redes y sistemas