Cifrado de datos

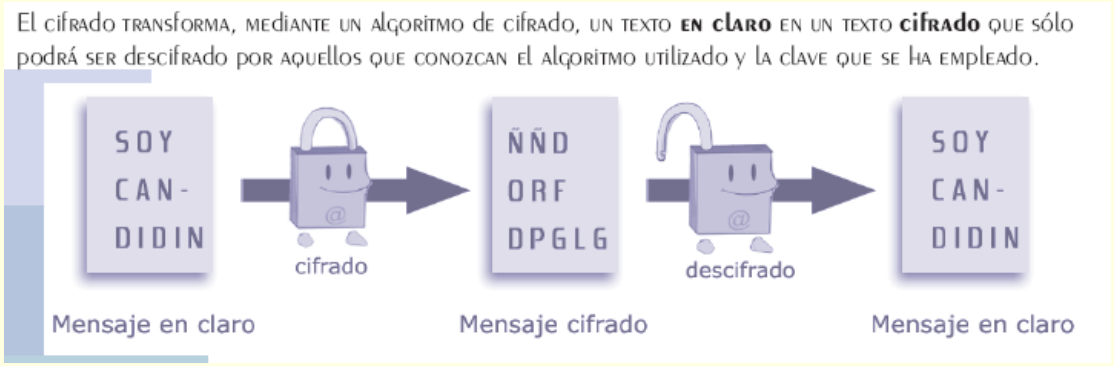
Esconder las cosas de valor

Para obtener la Confianza de las partes

- Autenticación
  - Confianza en la identidad de todas las entidades.
- Confidencialidad
  - Confianza en la privacidad de la información.
- Integridad
  - Confianza en que los datos no sean modificados.
- No repudio
  - Confianza en que las partes no se desdigan.
- Adicionalmente
  - La Fecha y la Hora Cierta de la Firma “Secure Time Stamp” en la que se ha generado, y se ha recibido el documento.
  - Disponibilidad legítima de servicios e información.

Criptografía

- El conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido
  - Es el arte de escribir en clave
  - Protege la información del acceso de quien no está autorizado a conocerla
- La criptografía oculta datos
  - Cifrado: ocultación de datos
  - Descifrado: liberación de datos
- Elementos:
  - clave y algoritmos



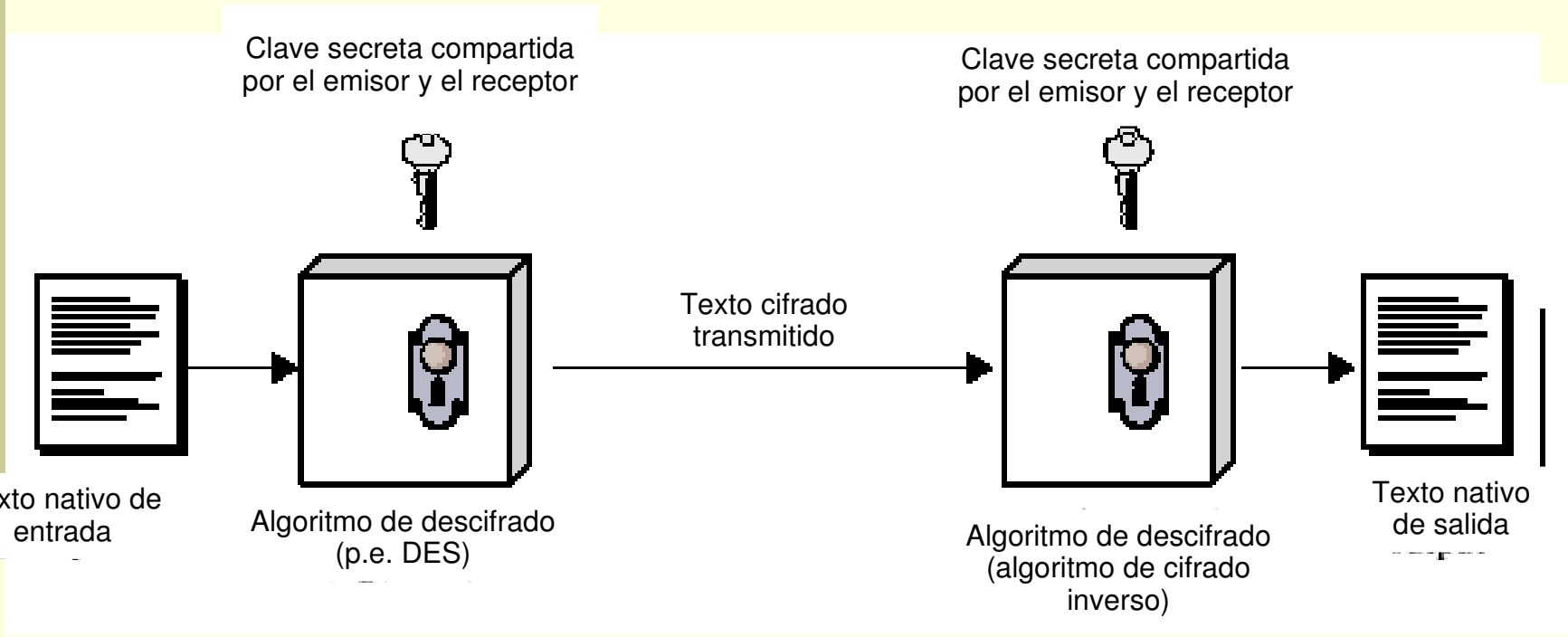
Clases de Criptografía

- Criptografía de clave privada
- Funciones resumen o hash
- Criptografía de clave pública

Criptografía de clave privada o simétrica

- Se basa en el uso de una única llave entre las partes implicadas, el remitente y el receptor.
  - La información se cifra con una clave privada que tienen tanto el remitente como el receptor
  - Utiliza la misma clave para cifrado y descifrado
  - Muy rápidos, adecuados para cifrar grandes volúmenes de datos
  - Ejemplos:
    - DES, Triple DES, DESX: aplicaciones bancarias, EFS
    - IDEA: PGP
    - RC4, RC5: SSL
    - AES: Rijndael
    - Blowfish, CAST, SAFER,...
  - Problemas:
    - Número y gestión de clave

Cifrado convencional



Ingredientes

- Texto nativo
- Algoritmo de cifrado
- Clave secreta
- Texto cifrado
- Algoritmo de descifrado

Requisitos de seguridad

- Algoritmo de cifrado robusto:
  - Incluso si conoce el algoritmo, no debería ser capaz de descifrar el texto o describir la clave.
  - Incluso si posee un determinado número de textos cifrados junto con los textos nativos que produce cada texto.
- El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura.
- Una vez que se conoce la clave, todas las comunicaciones que utilicen esta clave pueden ser leídas.

Ataques al cifrado convencional

- Criptoanálisis:
  - Se basa en la naturaleza del algoritmo más algún conocimiento de las características generales del texto nativo.
  - Intento de deducir un texto nativo o la clave.
- Fuerza bruta:
  - Intentar cada clave posible hasta que se obtenga una traducción inteligible del texto nativo.

Criptografía de clave pública o asimétrica

- Está basada en el uso de dos claves por cada entidad, dos claves separadas pero relacionadas (asimétrica)
  - Una pública y otra privada
    - La privada sólo es conocida por su propietario
      - Debe permanecer en secreto y bajo el control del usuario
    - La pública puede y debe ser conocida por todo el mundo
- Dichas llaves se caracterizan por que:
  - Son diferentes,
  - Están matemáticamente asociadas
  - No se puede obtener la llave privada a partir de la pública.
  - Cada llave únicamente puede descifrar lo que la otra ha cifrado, por tanto;
    - a.- con la llave pública del suscriptor, cualquiera puede cifrar un mensaje, que solo puede ser descifrado por la llave privada del suscriptor, se logra la confidencialidad.
    - b.- con la llave pública del suscriptor, cualquiera puede descifrar un mensaje, y así verificar la identidad del documento que ha sido cifrado por el suscriptor usando su llave privada.

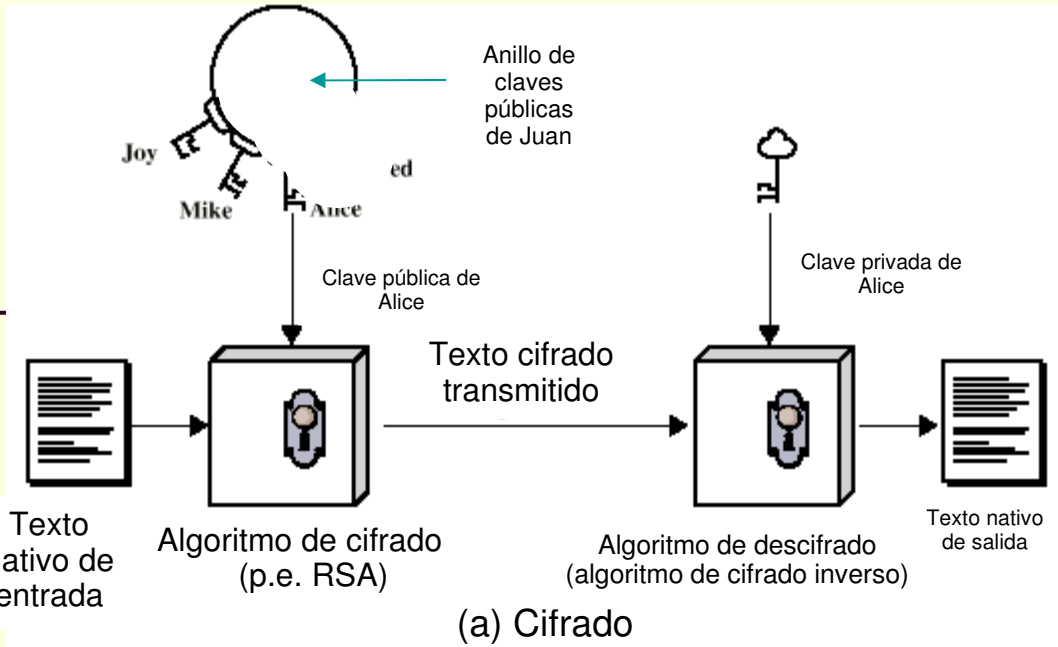
Cifrado de clave pública

- **El suscriptor** puede establecer la integridad y el origen (autoría) de la información (datos) que envía a otro participante, firmando digitalmente dicha información, cifrándola con su llave privada.
- **Quien recibe la información** puede usar la llave pública asociada del suscriptor para validar que proviene del suscriptor (tenedor de la llave privada), y verificar la integridad de la información.
- Más lentos, adecuados para:
  - Autenticación
  - Distribución de claves de sesión
  - Firmas digitales
- Ejemplos:
  - RSA, Diffie-Hellman, ElGamal, Algoritmos de curva elíptica

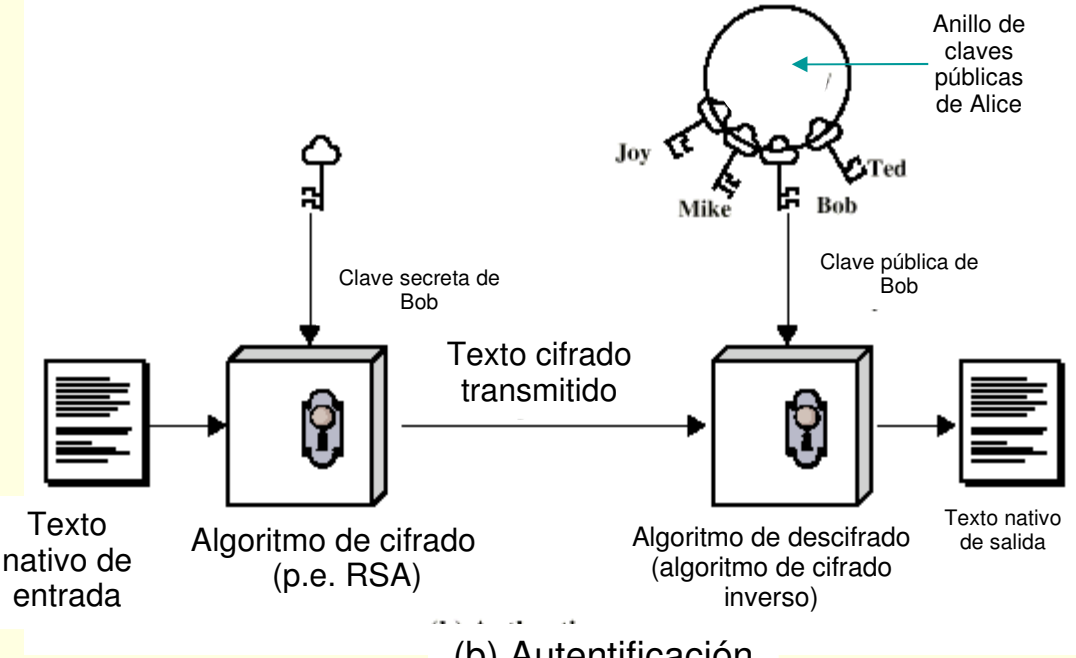
Ingredientes

- Texto nativo.
- Algoritmo de cifrado.
- Clave pública y privada.
- Texto cifrado.
- Algoritmo de descifrado

Cifrado Clave Pública



(a) Cifrado



(b) Autentificación

Técnica de Cifrado de Clave Pública

- Una clave se hace pública:
  - Se usa para el cifrado.
- Otra clave se mantiene privada:
  - Se usa para el descifrado.
- No es factible determinar la clave de descifrado dadas la clave de cifrado y el algoritmo.
- Cualquiera de las claves se puede usar para cifrar, la otra para descifrar.

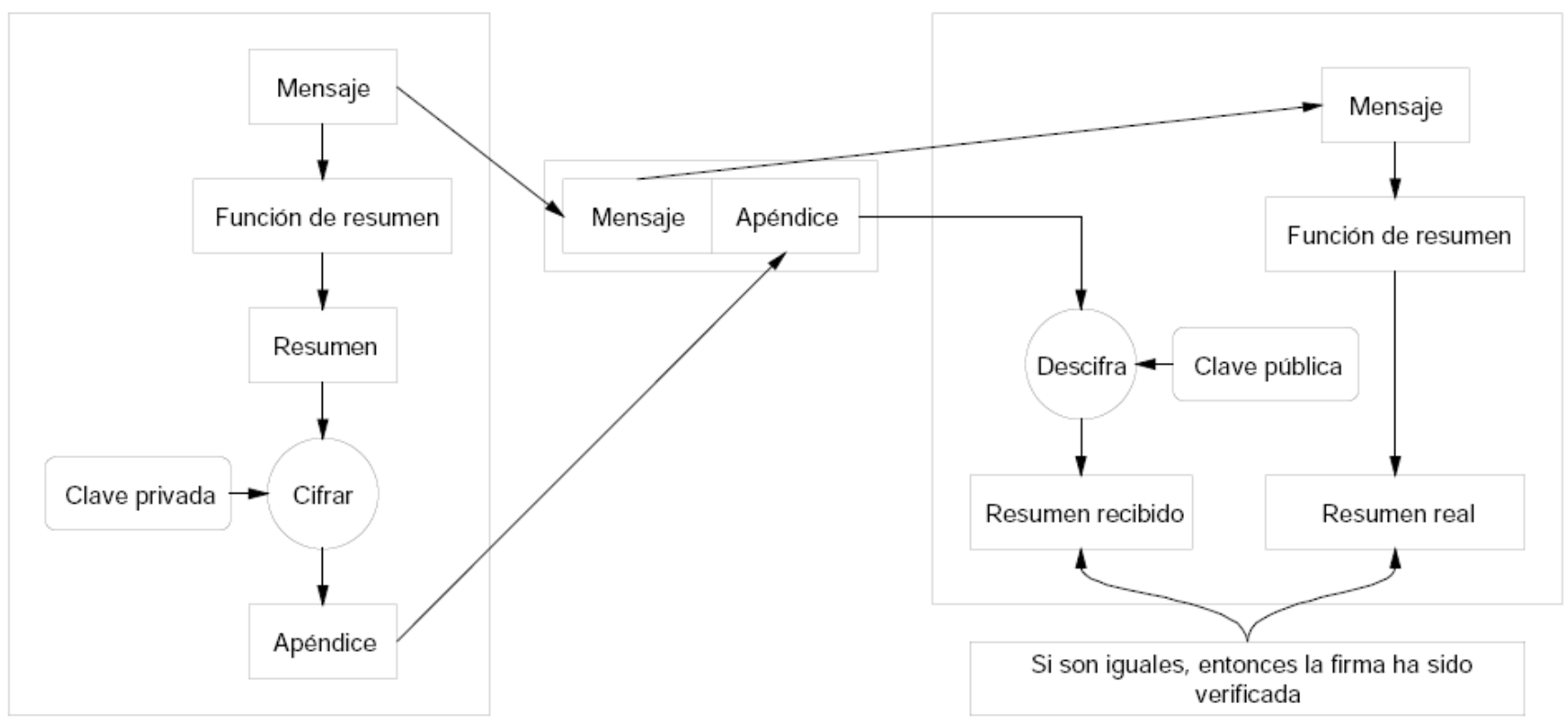
Pasos

- Cada usuario genera un par de claves.
- Cada usuario publica la clave pública.
- Para enviar un mensaje al usuario, se cifra el mensaje utilizando la clave pública.
- El usuario descifra el mensaje utilizando su clave privada.

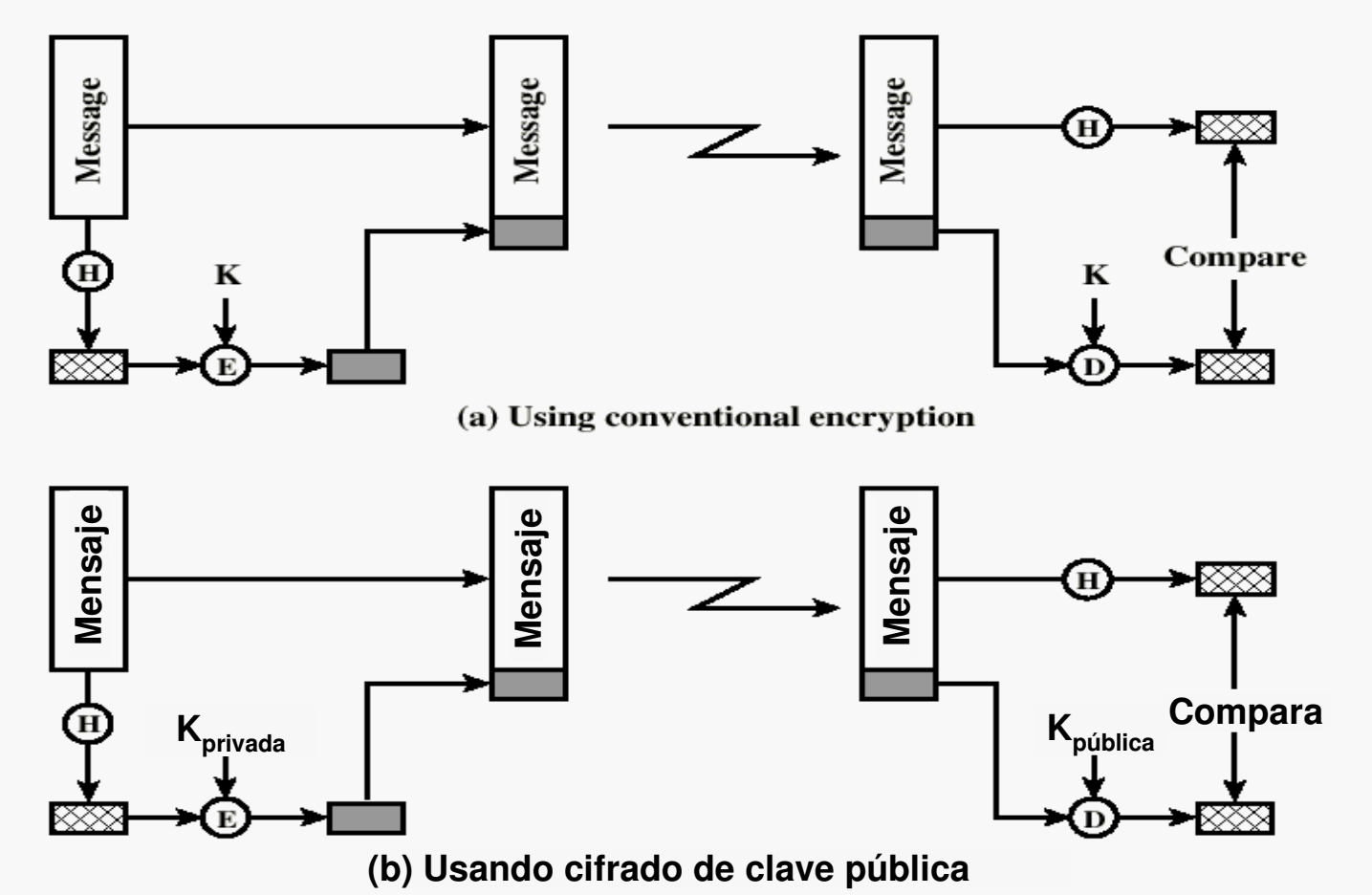
Funciones resumen o hash

- Transforman mensajes de longitud arbitraria en mensajes de longitud fija.
  - No se puede recobrar a partir del resumen(Message Digest)
  - Es completamente diferente si cambia un solo bit de el mensaje original.
  - Función con determinados requisitos.
  - Ejemplos:
    - MD4, MD5, SHA, SHA-1, SHA-256, RIPEMD-160

Firma digital



Enfoque típico de firma digital



Infraestructuras de Clave Pública (ICPs o PKIs, Public Key Infrastructures).

- El modelo basado en Terceras Partes Confiables
- Definiciones:
  - Es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.
  - El hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados.
  - una infraestructura de clave pública, es el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de la red de una empresa, extranet oInternet.

Algunos de los servicios del PKI

- Registro de claves:
  - Emisión de un nuevo certificado para una clave pública.
- Revocación de certificados:
  - Cancelación de un certificado.
- Selección de claves:
  - Publicación de la clave pública
- Evaluación de la confianza:
  - Determinación sobre si un certificado es válido
- Recuperación de claves:
  - Posibilitación de recuperar las claves de un usuario.
- La norma es:
  - Internet Certificate and CRL Profile RFC 3280
  - http:\\www.ietf.org


Autoridad de Registro
Parte Utilizadora (aplicación)
Internet
Autoridad de Certificación
Repositorio
Titular del Certificado

PKI: componentes

- Las ICPs están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:·
  - Autoridades de Certificación (CAs)
    - Gestión de Certificados ·
  - Autoridades de Registro (RAs)
    - Autoriza la asociación entre una clave pública y el titular de un certificado
  - Entidades finales /Usuarios /Suscriptores (a quien se pretende identificar)
    - Son los titulares de los Certificados
  - Los repositorios (Directorios)
    - Almacenan y distribuyen certificados y estados: expirado, revocado, etc.
  - Autoridad de Validación
    - Suministra información de forma online (en tiempo real) acerca del estado de un certificado
  - Emisores de CRLs.
  - Otras Terceras Partes Confiables como por ejemplo
    - Las Autoridades de Fechado Digital.
    - Las partes utilizadoras
      - Verifican certificados y firmas

Infraestructura de Clave Pública (PKI)

Autoridad de Certificación

- Entidad fiable, encargada de garantizar de forma unívoca y segura la identidad asociada a una clave pública
- Representan la fuente de credibilidad de la infraestructura de llave pública.
  - Son quienes emiten los certificados, firmándolos digitalmente con su llave privada.
  - Certifican que la llave pública asignada en un certificado a una entidad final, corresponde realmente a dicha entidad final.
  - Recibe y procesa peticiones de certificados de los usuarios finales
  - Consulta con una Autoridad de Registro para determinar si acepta o rehúsa la petición de certificado
  - Emite el certificado
  - Gestiona Listas de Revocación de Certificados (CRLs)
  - Renueva certificados
- Proporciona:
  - Servicios de backup y archivo seguro de claves de cifrado
  - Infraestructura de seguridad, para la confianza, políticas de operación segura, información de auditoría.
- Nomenclatura CNI: Entidad de Certificación (EC)

Autoridad de Registro

- Realiza el proceso de registro de las entidades finales por encargo de la autoridad de certificación.
- Valida los atributos del sujeto que solicita el certificado
- Gestiona el registro de usuarios y sus peticiones de certificación/revocación, así como los certificados respuesta a dichas peticiones
- Indica a la CA si debe emitir un certificado
- Autoriza la ASOCIACIÓN entre una clave pública y el titular de un certificado
- Gestión del ciclo de vida de un certificado:
  - Revocación
  - Expiración
  - Renovación (extensión periodo validez del certificado, respetando el plan de claves)
  - Reemisión del par claves del usuario
  - Actualización de datos del certificado
- Nomenclatura CNI: Entidad de Registro (ER)

Repositorios

- Permite guardar información sobre PKI, como puedan ser
  - Certificados, y
  - CRLs para su acceso por parte de las entidades finales o de sus delegados.
- Tienen por finalidad que la entidad final obtenga la confirmación sobre:
  - El estatus de revocación de los certificados de otros usuarios, y
  - La validación del “Certification Path”, o cadena de certificados.

Titulares de certificados

- Entidades finales
- Usuarios finales
- Suscriptores
- Ejemplo:
  - Un servidor web es una ‘Entidad Final’ cuando obtiene un certificado y lo utiliza para probar su identidad en la red

Autoridad de Validación (VA)

- Suministra información de forma online acerca del estado de un certificado.
- La VA suele proporcionar dos servicios de validación:
  - El tradicional, permitiendo la descarga de CRLs para que el usuario las interprete él mismo, o a través del protocolo OCSP (Online Certification Status Protocol).
  - Los usuarios y las aplicaciones que deseen obtener el estado de un certificado, sólo tienen que realizar una petición OCSP contra la VA para obtener dicho estado.
- La CA actualiza la información de la VA cada vez que se modifica el estado de un certificado, con lo que, a diferencia de las CRLs, se dispone de información en tiempo real.
- Nomenclatura CNI: Entidad de Validación (EV)

Emisores de CRLs o “Certificate Revocation List Issuers”

- Los emisores de Listas de Revocación de Certificados actúan en nombre de la Autoridad de Certificación, siendo de carácter opcional aunque sumamente convenientes.
- Son listas de los Certificados que han dejado de ser válidos y por tanto en los que no se puede confiar.
- Los Certificados son revocados en los casos en los cuales:
  - a) la llave privada se vea comprometida,
  - b) hayan cambiado los atributos del certificado.

Procedimiento de la Certificación:

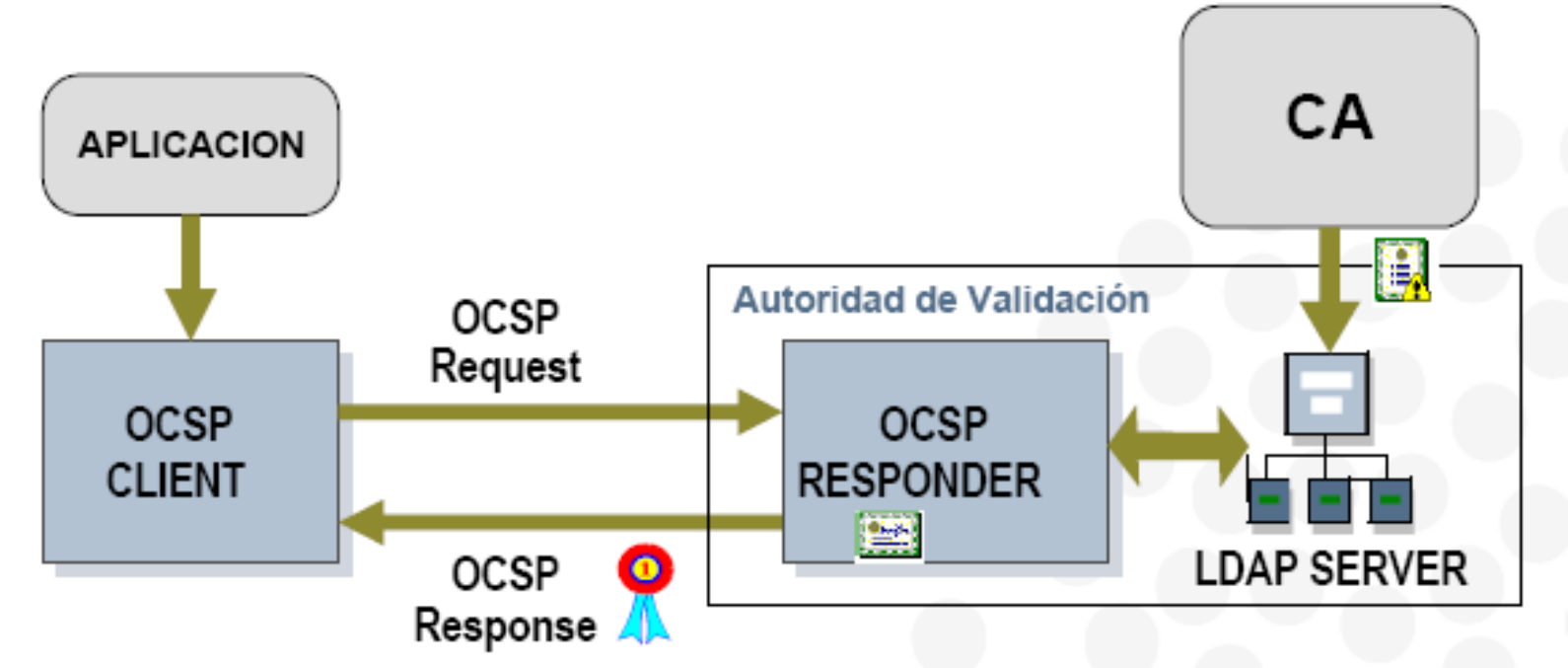
- 1º Solicitud a la Autoridad de Certificación de un certificado por parte de la Entidad Final, a través de la Autoridad de Registro, con el objeto de que la Autoridad de Certificación garantice la identidad de la entidad final.
- 2º La Autoridad de Certificación comprueba que cada usuario es quien dice ser y que la clave pública que inscriba en el certificado realmente le pertenece.
- 3º El Certificado de la entidad final se firma digitalmente, cifrándolo con la llave privada de la Autoridad de Certificación.
- 4º A su vez la autoridad de certificación es certificada por otra/s Autoridad/es de Certificación.
- 5º Dicho certificado se distribuye globalmente, es decir, al mayor numero de destinatarios posibles.

Métodos de Registro

- Registro Presencial
  - El usuario se persona a Autoridad de Registro, y le entrega toda la documentación que requiera.
  - Si la Autoridad de Registro aprueba la solicitud, pasa los datos a la Autoridad de Certificación para que emita el certificado.
  - Una vez emitido, la Autoridad de Registro suministra en certificado al usuario

OCSP: Online Certificate Status Protocol

- Protocolo que permite el acceder al estado del certificado de manera online
- IETF RFC 2560



Aspectos a garantizar por el modulo PKI

- Autoría:
  - Autenticación de la identidad del suscriptor.
    - i. Suscriptor:
      - Firma el documento con su llave privada, estableciendo la autoría al ser él el único que puede utilizar su llave privada.
    - ii. Verificador:
      - Verificación de la firma utilizando el certificado público del suscriptor.
- Confidencialidad:
  - Autenticación de la identidad del portador y verificador.
    - i. Suscriptor:
      - Cifra el documento con la llave pública del verificador.
    - ii. Verificador:
      - Descifra el documento con su llave privada.

Aspectos a garantizar por el modulo PKI (II)

- Integridad:
  - Tiene por objeto garantizar que el contenido del documento está inalterado.
    - i. A través del cifrado simétrico y de la coincidencia del “message digest” o“hash”, obtenido mediante el descifrado de dicho “message digest” o “hash” con la llave privada, y la pública del suscriptor.
- No Repudio:
  - Consiste en garantizar que el suscriptor no pueda negar haber firmado un documento.
    - i. Se logra manteniendo un par de llaves de cifrado / descifrado en manos de la Autoridad de Certificación, además del par de llaves de firma en manos del suscriptor.

¿Qué es un certificado?

- ¿Como garantizar la identidad de las partes?
  - Cualquiera puede generar un par de claves y pretender que su clave pública es la de otra persona
- Un certificado en un documento emitido y firmado por la Autoridad de Certificación que confirman la identidad de una persona física o jurídica, vinculada con una llave pública asociada a la llave privada.
- Tienen dos objetivos:
  - 1- Que la llave pública del suscriptor pueda ser accesible por los verificadores o participes interesados en validar y verificar la firma digital del suscriptor.
  - 2- Que los participes puedan confiar en que la llave pública que recibe el verificador sea realmente la del suscriptor.
- Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

Tipos de certificados:

- Según a quién se le emitan
  - Personales
  - Servidor
  - Software
  - Entidades jurídicas

Clases de certificados

- Certificados de Clase 1:
  - Son emitidos únicamente a individuos.
  - No se verifica la identidad de éstos y por tanto no permite autentificarla.
  - Confirman que el nombre o seudónimo y el sujeto del certificado forman un nombre de sujeto inequívoco.
- Certificados de Clase 2:
  - Son emitidos únicamente a individuos, y
  - Confirman que la información proporcionada por el Suscriptor no entra en conflicto con la información de las bases de datos fiables propiedad de una EE (Entidad de Emisión) o una ERL (Entidad de Registro Local), incluida la identidad del sujeto y otros datos del Suscriptor.
  - a) Certificados de Clase 2 no reconocidos (Clase 2 tipo 1),
    - Usados para transaciones de bajo riesgo como servicios de suscripción de la Sociedad de la Información.
  - b) Certificados de Clase 2 reconocidos (Clase 2 tipo 2),
    - Pueden ser usados como soporte de firmas electrónicas legalmente reconocidas, obtienen una razonable seguridad de la identidad del Suscriptor, comparando automáticamente el nombre del solicitante, dirección y otra información personal contenida en la solicitud de certificado, con la información contenida en las bases de datos propiedad de la EE o ERL.

Clase de certificador (II)

- Certificados de Clase 3, se emiten a:
  - Individuos:
    - Requiere la presentación de evidencias probatorias de la identidad de la identidad del sujeto, personándose ante una Entidad de Registro Local (ERL) o su delegado, como puede ser un notario público.
  - Organizaciones:
    - Se emiten a individuos con capacidad de firma dentro de una organización, probada esta capacidad de firma por evidencia notarial, y de la propia organización a través de organizaciones empresariales que confirmen su identidad.

¿Qué es un certificado raíz?

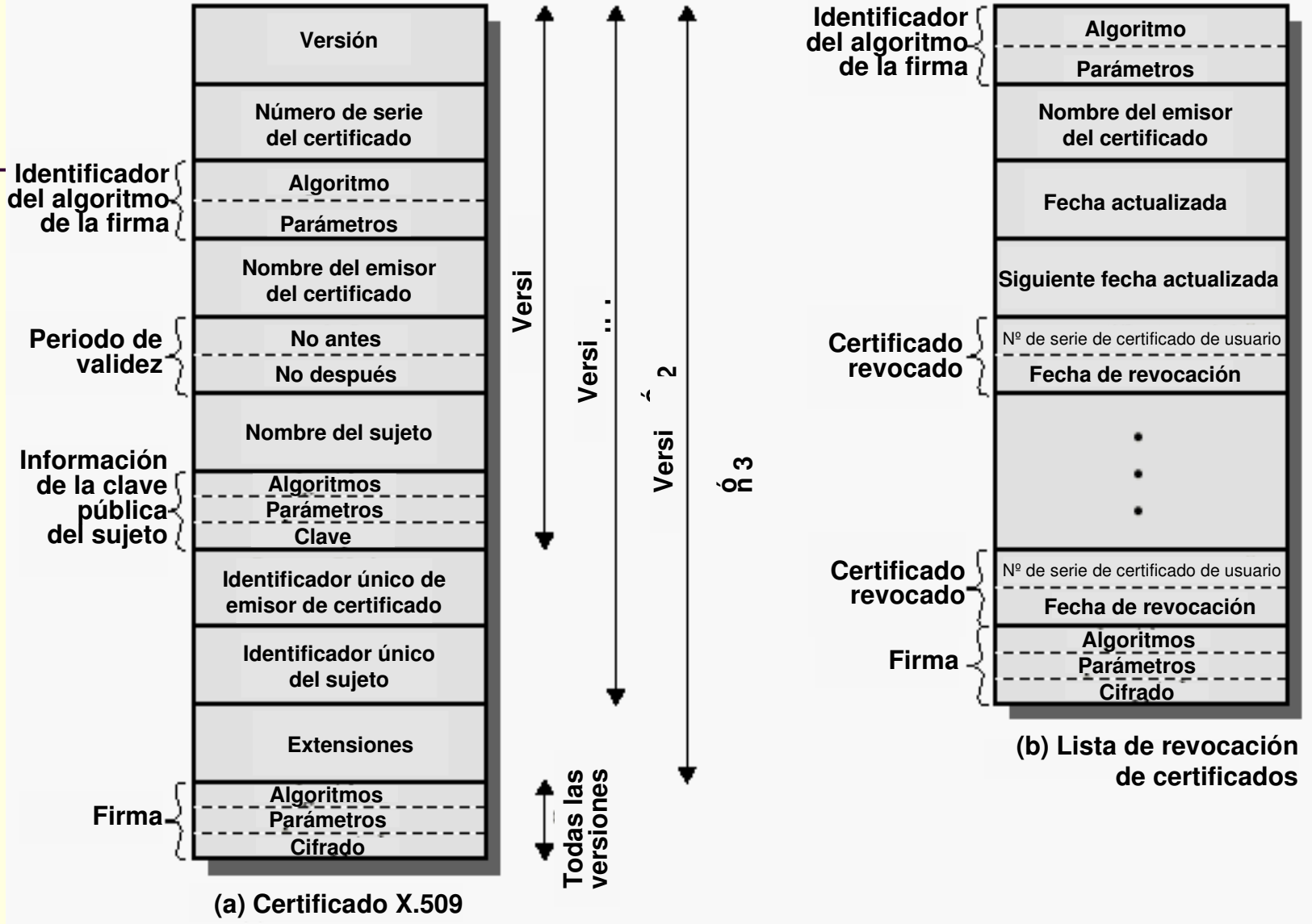
- Un certificado raíz es un certificado emitido por la Autoridad de Certificación para sí misma.
- En este certificado consta la clave pública de la Autoridad de Certificación y por tanto será necesario para comprobar la autenticidad de cualquier certificado emitido por ella.
- Es el certificado origen de la cadena de confianza.
- Entidades raices
  - Verisign: Class 3 Public Primary Certification Authority – G2;Verisign, inc.; US “Verisign Trust Network”.
  - Global Sign: GlobalSign WTLS CA; GlobalSign nv-s.
  - CybrTrust; Baltimore; IE ; Baltimore CyberTrust Mobile Root.
  - Entrust; Entrust.net WAP CA © 1999; Limited liability. Www.entrust.net/-wap cps;

¿Qué información contiene un certificado ?

- **Nombre habitual del propietario de la clave de firma**
- **Identificador único del propietario**
- **Clave pública correspondiente a la clave privada de firma**
- **Identificación de los algoritmos de clave pública**
- **Número del certificado**
- **Nombre de la Entidad Certificadora**
- **Limitaciones de aplicación de las claves**
- **Capacidad de representación por terceras partes**
- **Fecha y hora de emisión y aceptación del certificado**
- **Fecha y hora de expiración del certificado**
- **Firma de la Autoridad Pública de Certificación como emisora del certificado**
- **Versión de la DPC bajo la cual se haya emitido el certificado**

Certificado X.509v3 contiene:

Versión del certificado	Versión 3
Núm. de serie del certificado	*Generado por la CA, único*
Algoritmo de firma del certif.	sha1withRSAEncryption
Nombre X.500 del emisor	c=ES, o=Empresa, cn= Autoridad de Certificación
Periodo de validez	desde dd/mm/aa hasta dd'/mm'/aa'
Nombre X.500 del sujeto	c=ES, o=Empresa, cn=José Pérez
Clave pública del sujeto	AC:46:90:6D:F9:.....
Uso de la clave	Firma digital, cifrado de clave
Uso de la clave mejorado	Autenticación en W2000
Identificador claves CA	Identifica el par de claves utilizado para firmar el certificado
Identificador claves usuario	Identifica el par de claves asociado a la clave pub. en el certif.
Punto de distribución CRLs	HTTP://servidor/ruta/nombre.crl (publicación en web)
Firma de la AC	Firma del certificado por la CA


Versión
Número de serie del certificado
Identificador del algoritmo de la firma
Algoritmo
Parámetros
Nombre del emisor del certificado
Periodo de validez
No antes
No después
Nombre del sujeto
Información de la clave pública del sujeto
Algoritmos
Parámetros
Clave
Identificador único de emisor de certificado
Identificador único del sujeto
Extensiones
Firma
Algoritmos
Parámetros
Cifrado
Versi
Versi
Versi
ó n 3
Todas las versiones
(a) Certificado X.509
Identificador del algoritmo de la firma
Algoritmo
Parámetros
Nombre del emisor del certificado
Fecha actualizada
Siguiente fecha actualizada
Certificado revocado
Nº de serie de certificado de usuario
Fecha de revocación
Certificado revocado
Nº de serie de certificado de usuario
Fecha de revocación
Firma
Algoritmos
Parámetros
Cifrado
(b) Lista de revocación de certificados

Estados de los Certificados Electrónicos

- Emisión (válido)
  - Inicio de su vigencia
- Caducado :
  - Por Finalización(expiración) del periodo de validez
  - Requiere la renovación del certificado
- Revocación de certificados:
  - La clave privada asociada al certificado se ha visto comprometida (extravío, robo, copia...)
  - Cambio de datos asociados al certificado
  - Puede ser revocado por la CA o por el propio titular
  - CRLs:
    - Listas firmadas por la CA incluyendo referencias a certificados revocados por ella.
- Suspensión de certificados:
  - Revocación temporal
  - Mismas actuaciones que revocación, salvo que es reversible.

Tipos de soporte para los certificados

- Fichero en disco duro
- Fichero en diskette
- Tarjeta TIBC
- Tarjeta criptográfica
- Token USB

Identificación personal: tarjeta inteligente

- Una llave muy segura
  - Algo que se posee
  - No duplicable e inviolable
- Además protegida por PIN secreto y/o biometría
  - Algo que se conoce y/o se es.
- Portabilidad total
  - Claves y certificados grabados en la tarjeta
- Firma electrónica avanzada
  - Según la normativa vigente

Tarjetas y chip criptográficos

- El chip criptográfico contiene un microprocesador que realiza las operaciones criptográficas con la clave privada. La clave nunca se expone al exterior.
- Doble seguridad: posesión de la tarjeta y PIN de acceso (o mecanismos biométrico).
- Puede ser multipropósito:
  - Tarjeta de identificación gráfica.
  - Tarjeta de control de acceso/horario mediante banda magnética o chip de radiofrecuencia.
  - Tarjeta monedero.
  - Tarjeta generadora de contraseñas de un solo uso (OTP).
- Se precisa de un middleware (CSP) específico para utilizar la tarjeta, así como de un lector (USB, integrado en teclado o PCMCIA)
- El número de certificados que se pueden cargar depende del perfil de certificado, de la capacidad del chip y del espacio que se reserve para los certificados.
  - Chip de 32 KB: 3 a 5 certificados tipo
  - Chip de 64 KB: de 6 a 10 certificados tipo

Otros tipos

- Token USB:
  - al igual que las tarjetas criptográficas sirven de almacén de claves/certificados y realizan las operaciones criptográficas en su interior.
  - Ventajas: no precisan de lector (sólo puerto USB), reducido tamaño.
  - Inconveniente: no sirven como tarjeta de identificación, monedero, de acceso.
- Chip de radiofrecuencia (p. ej. Mifare):
  - El chip criptográfico puede ser de acceso por radiofrecuencia (sin contacto).
    - Ventajas:
      - se reduce el desgaste físico, no es necesaria la introducción de la tarjeta.
    - Inconveniente:
      - las operaciones criptográficas son lentas, lo que exige mantener la proximidad un tiempo significativo
  - En la práctica el chip de radiofrecuencia se usa para control de acceso físico y horario.
  - El lector lee el número de serie del chip o un código almacenado y lo compara con su base de datos de acceso.

Marco Legal

- Directiva Europea
  - Directiva 1999/93/CE del parlamento europeo y del consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica
- Legislación Española
  - LEY 59/2003, de 19 de diciembre, de firma electrónica (BOE nº 304, 20/12/2003)
- Artículo 1. Objeto.
  - 1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.
- Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones públicas.
  - 1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.(...)
  - 4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Definiciones de la Ley 59/2003

- **Firma electrónica**:
  - Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- **Firma electrónica avanzada**:
  - Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- **Firma electrónica reconocida**:
  - Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- **Prestador de servicios de certificación (PSC):**
  - Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **Certificado electrónico**:
  - Un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- **Certificados reconocidos**:
  - Certificados electrónicos expedidos por un PSC que cumpla los requisitos establecidos la Ley 59/2003 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación.

DNI electrónico, DPC y Órgano supervisor

- Artículo 15. Documento nacional de identidad electrónico.
  - 1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.
  - 2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico (...)
- Artículo 19. Declaración de prácticas de certificación.
  - 1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación (...)
  - 3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación de protección de datos de carácter personal (...)
- Artículo 29. Supervisión y control.
  - 1. El Ministerio de Industria, Turismo y Comercio controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

Requisitos de los PSC

- Requisitos de los Prestadores de Servicios de Certificación
  - No almacenar ni copiar los datos de creación de firma de la persona.
  - Proporcionar al solicitante antes de la expedición del certificado la información mínima que establece la Ley de forma gratuita. (Declaración de Prácticas de Certificación y Políticas de Certificación).
  - Mantener un directorio actualizado de certificados en el que se indiquen los certificados expedidos su vigencia. La integridad del directorio se protegerá mediante mecanismos de seguridad adecuados.
  - Disponer de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.
- Requisitos adicionales de los Prestadores de Servicios de Certificación Reconocidos
  - Disponer de las medidas técnicas y organizativas que garanticen la fiabilidad y seguridad de los servicios (hardware, software, procedimientos de operación y personal empleado).
  - Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años.
  - Constituir un seguro de responsabilidad civil (o garantía mediante aval bancario o seguro de caución) por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

Estándares Europeos

- ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates
- ETSI TS 102 023: Policy requirements for time-stamping authorities
- ETSI TS 101 862: Qualified Certificate profile
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates
- CWA 14167-2 Security Req. for Trustworthy Systems Managing Certificates for Electronic Signatures
- CWA 14172 EESSI Conformity Assessment Guidance (Guía para aplicar los estándares de firmaelectrónica de acuerdo con la iniciativa de estandarización europea)

Estandares

- ITU & ISO
  - ITU-T Recommendation X.509 | ISO/IEC 9594-8:Public-Key and AttributeCertificate Frameworks
  - ISO 17799 Código de buenas prácticas para la Gestión de la Seguridad de la Información
- **Otros**
  - AICPA/CICA **WebTrust Program** for Certification Authorities V 1.0
  - **PKI Assessment Guidelines** – PAG del Information Security Committee (ISC) a Section of Science & Technology Law,American Bar Association.
- Internet Engineering Task Force (IETF) – Request For Comment
  - RFC 3280 Certificate and CertificateRevocation List (CRL) Profile
  - RFC 3739: Qualified Certificates Profile
  - RFC 3647 Certificate Policy and Certification Practices Framework(Obsoletes RFC2527)

Estándares PKCS

- PKCS: Familia de estándares para los sistemas de criptografía de clave pública definidos por los Laboratorios RSA:
  - PKCS#1,#2,#4: RSA Cryptography Standard
  - PKCS#3: Diffie-Hellman Key Agreement Standard
  - PCKS#5: Password-Based Cryptography Standard
  - PKCS#6: Extended-Certificate Syntax Standard
  - PKCS#7: Cryptographic Message Syntax Standard
  - PKCS#8: Private Key Information Syntax Standard
  - PKCS#9: Selected Attibuites Types
  - PKCS#10: Certification Request Syntax Standard
  - PKCS#11: Cryptographic Token Interface Standard
  - PKCS#12: Password Information Exchange Syntax Standard
  - PKCS#13: Elliptic Curve Cryptography Standard

Soluciones PKI

Entrust	Safelayer
Entrust proporciona una tecnología completa PKI que incluye todos los servicios necesarios. **Ventaja**: cubre todos los servicios PKI, tiene mecanismos y formatos propios que facilitan la gestión. **Desventaja**: utiliza algunos formatos propietarios, la solución es más cerrada y sus costes son muy elevados. No está acreditada por el CNI.	**Safelayer** proporciona una tecnología completa PKI que incluye todos los servicios necesarios con una arquitectura abierta. **Ventaja**: cubre todos los servicios PKI, su arquitectura abierta permite soportar cualquier modelo de operación, sus costes son más moderados que los de Entrust. **Desventaja**: su propio carácter abierto exige un trabajo de personalización e integración significativo Está acreditada por el CNI y es la de mayores despliegues en España (FNMT, BdE, Caja Madrid,...).

Proceso de verificación de firma electrónica:

- **Conseguir el certificado del signatario.**
- **Verificar la validez del certificado:**
  - Dentro del período de validez
  - Certificado no revocado
  - Firma electrónica de la CA correcta
- **Verificar la firma digital del hash del mensaje con la clave pública del emisor.**
- **El receptor debe estar en posesión de la clave pública de la CA, con lo que podrá comprobar la firma electrónica de la CA del certificado del emisor.**

Protocolos Estándares

- SSL (*Secure Socket Layer*)
  - Establece un canal seguro de intercambio de información
- SET (*Secure Electronic Transaction*)
  - Además impide la manipulación de la información en los extremos
  - No muy usado en la actualidad (obsoleto)
- EMV (sustituye a SET)
- PGP (*Pretty Good Privac)*
  - Correo electrónico)
- IPsec

SSL *Secure Socket Layer*

- Proporciona:
  - Cifrado de datos
  - Autenticación de servidores
  - Integridad de mensajes
  - Confidencialidad: cifrado de datos
  - Autenticación de cliente (opcional)
  - Durante el transporte, no almacenamiento
- EJEMPLO:
  - Correo electrónico para los alumnos en https://webmerlin.uca.es

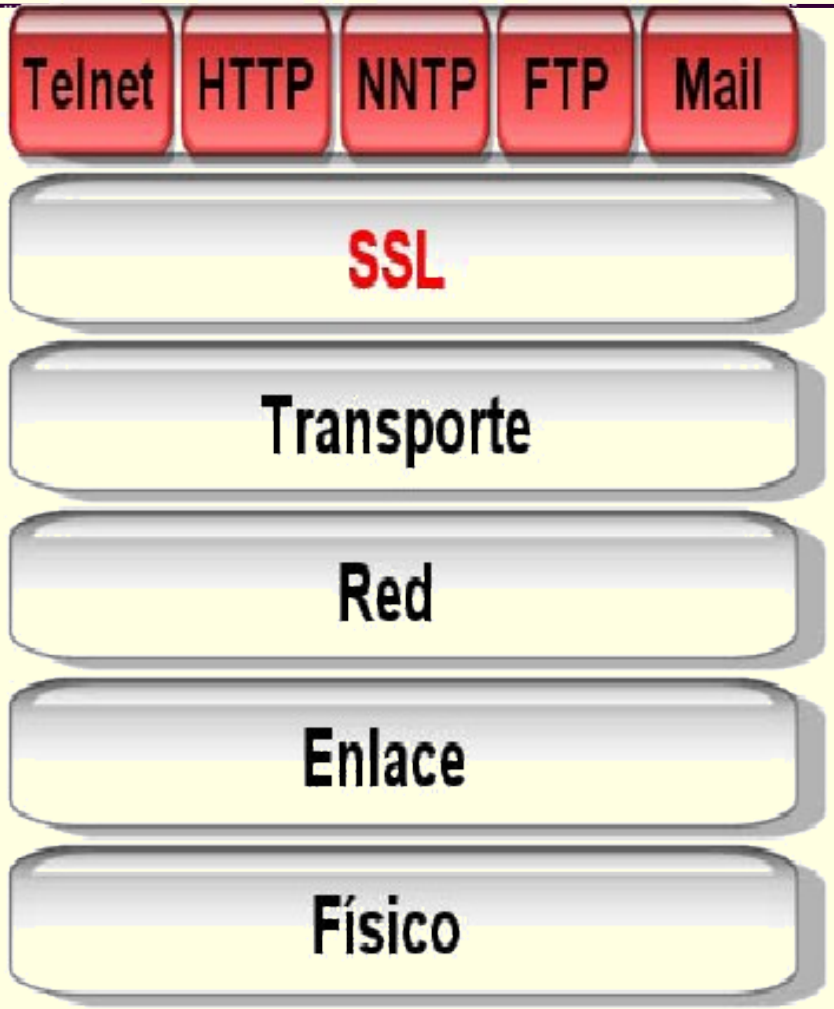
Funcionamiento de SSL

- Algoritmos de cifrado simétrico:
  - DES, 3DES, RC2, RC4, IDEA
- Algoritmos de clave pública:
  - RSA
- Algoritmos de resumen
  - MD5, SHA
- Certificados
  - DSS, RSA
- Clave de sesión distinta en cada transacción

SSL pasos para crear un canal seguro

- 1 Acordar qué algoritmo usar (Fase hola)
  - DES, RC2,RC4..
- 2 Autenticación
  - Intercambio certificado x.509v3
- 3 Generación de clave de sesión para cifrar la comunicación
- 4 Verificación de canal seguro
- A partir de ahí, comunicación segura

Ubicación de SSL en la pila



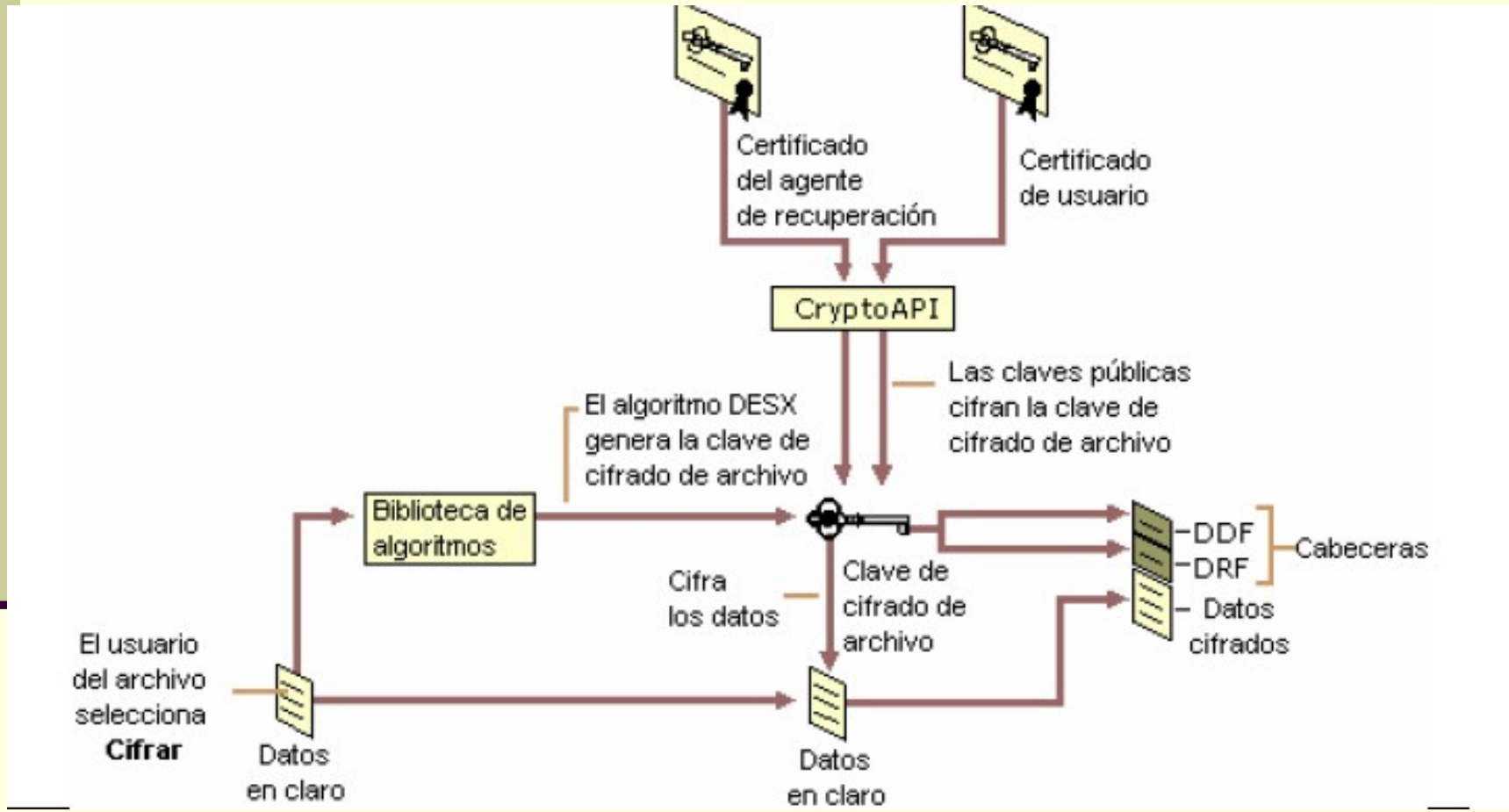
SSL

- Si el sitio es seguro:
  - Aparece un candado cerrado
  - El protocolo es *https*
  - Pinchando sobre el candado aparece información sobre el sitio y su certificado

Sistema de archivos cifrado

- Cada archivo tiene una clave de cifrado de archivo única (FEK), utilizada más adelante para descifrar los datos del archivo
- La FEK cifrada por la clave pública del usuario
- La FEK también está protegida por la clave pública de cada usuario autorizado para descifrar el archivo y por cada agente de recuperación
- La clave privada está protegida por la clave maestra del usuario
- La clave maestra está cifrada con DPAPI

Sistema de archivo cifrado



- Fuentes
  - Gonzalo Álvarez Marañón (CSIC)
- http://www.confianzaonline.org/
- http://sans.org/