Nociones sobre
Infraestructura de Clave Pública.

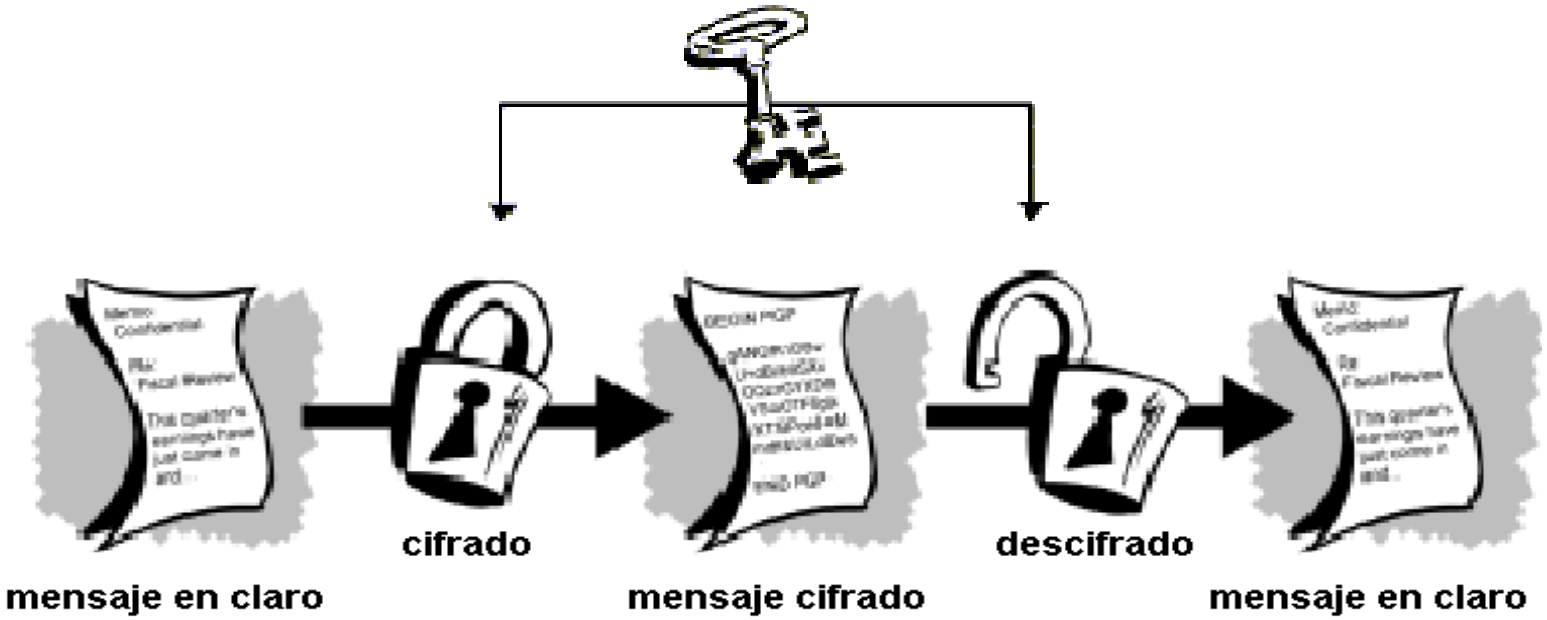
Conceptos Básicos sobre Criptografía.

- Algoritmo criptográfico.
- Cifrado digital.
- Confidencialidad

- Clave Simétrica.
- Clave Pública.

Criptografía de Clave Simétrica.

- Velocidad.
- Necesidad de distribución de la clave.



Algoritmos más utilizados.

- **DEA.** (Data Encryption Algorithm)
  - En ocasiones se conoce con el nombre del estándar, DES.
  - Utiliza una longitud de clave de 56 bits y un bloque cifrador de 64 bits.

- **TRIPLE - DES.**
  - Aplicación de 3 operaciones de cifrado consecutivas con el cifrador de 64 bits del algoritmo DEA.
  - Se necesita una clave de un tamaño 3 veces superior a la de DEA: 3x56=168 bits.

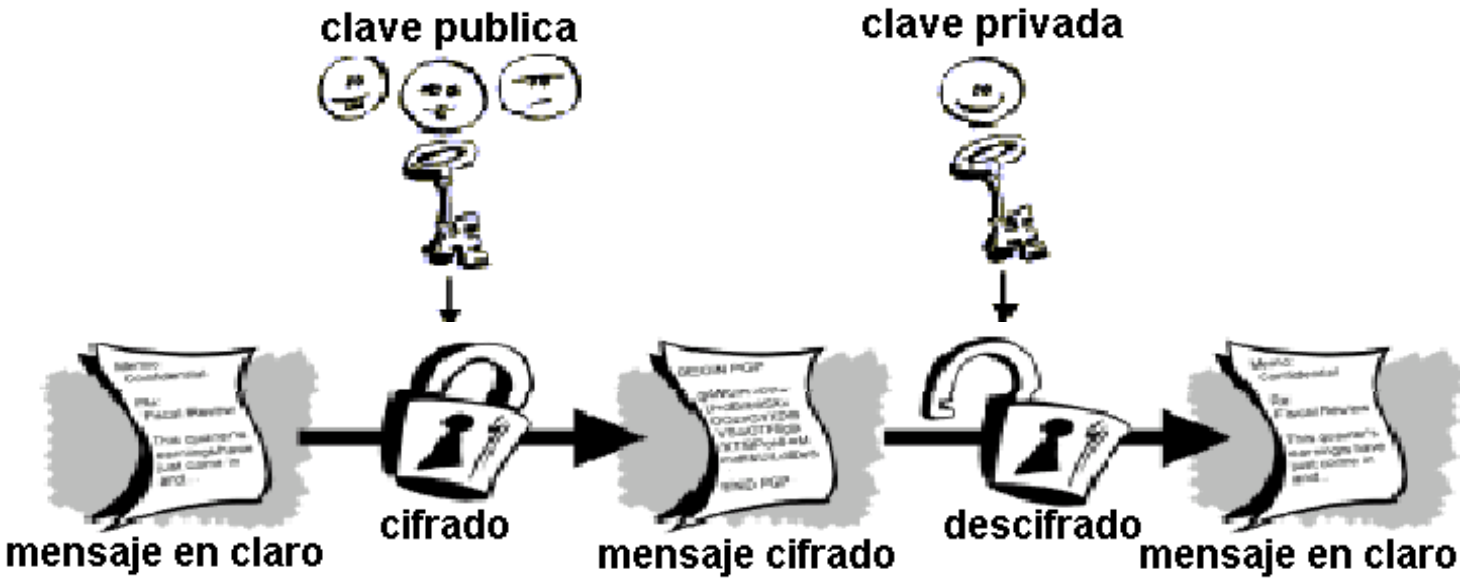
Algoritmos más utilizados.

- **AES.** (Advanced Encryption Standard)
  - Conjunto de especificaciones orientadas al desarrollo de un algoritmo criptográfico de mayor calidad que DES.
  - Los algoritmos propuestos a concurso han sido Rijndael, RC-6, MARS, Twofish y Serpent.
  - Recientemente ha resultado ganador el algoritmo Rijndael.

Criptografía de Clave Pública.

Clave Publica

- Cada usuario posee una pareja de claves.
  - Clave pública para cifrado.
  - Clave privada para descifrado.



- Lentitud

- La infraestructura de clave pública ayuda a autenticar a las personas con las que se tiene una conversación y a mantener en secreto lo que dicen.

Ejemplo de funcionamiento de una PKI

Criptografía de Clave Pública.

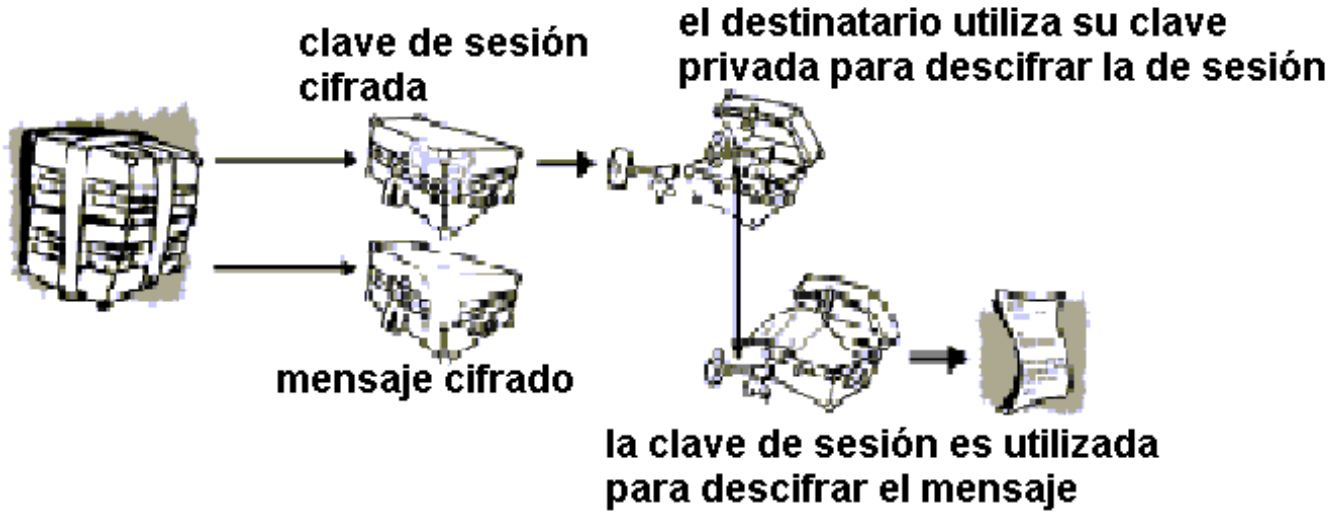
Solución

- Generación aleatoria de la *clave de sesión*.
- Cifrado del mensaje con dicha clave.
- Cifrado de la clave de sesión mediante cada clave pública de los usuarios destinatarios.

Criptografía de Clave Pública.

Descifrado

- Descifrado de su clave de sesión mediante su clave privada.
- Descifrado del mensaje con la clave de sesión.



Infraestructura de clave pública

- **Autoridad de Certificación (CA)**
  - Gestión de certificados.
- **Autoridades de Registro (RA)**
  - Autoriza la asociación entre una clave pública y el titular del certificado.
- **Partes utilizadoras**
  - Verifican certificados y firmas.
- **Repositorios (Directorios)**
  - Almacenan y distribuyen certificados y estados (expirado, revocado)
- **Titulares de certificados**
  - Entidades finales/usuarios
- **Autoridad de Validación (opcional)**
  - Suministra información de forma online (en tiempo real) sobre el estado del certificado.

Algoritmos más utilizados.

- **RSA.**
  - Utilizado para realizar tanto cifrado de clave pública como firma digital de datos.
  - La generación de la firma es más lenta que la verificación.

- **DSA.** (Digital Signature Algorithm).
  - Utilizado para firmas digitales y verificaciones de firmas.
  - El proceso de firma es más rápido que el de verificación, al contrario que con RSA

Algoritmos más utilizados.

- **ElGamal**.
  - Implementa tanto firma digital como cifrado de datos.
  - El cifrado de datos no se realiza de la misma forma que la verificación de la firma digital y el descifrado tampoco se realiza de la misma manera que la firma.

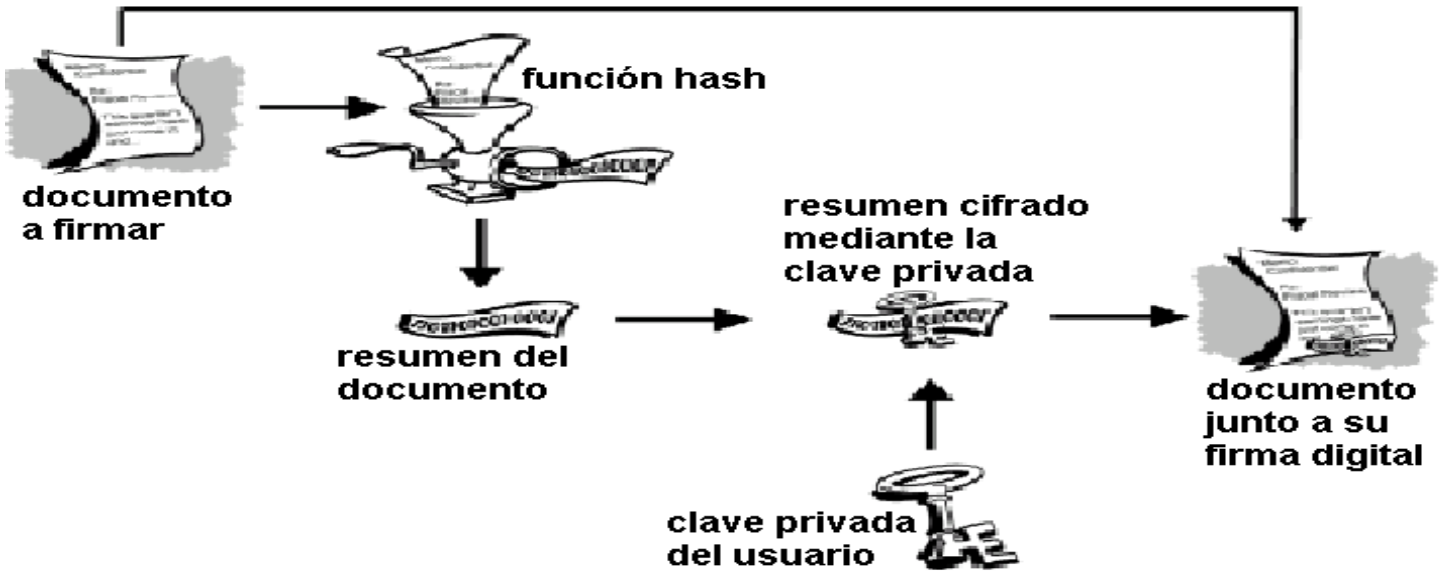
- **Algoritmo de Curvas Elípticas**
  - Posee la ventaja de que, ante una misma longitud de clave, se consigue mucho más seguridad.

Firma Digital.

- Garantiza
  - Autenticidad del origen.
  - Integridad de los datos.
  - No repudio en el origen.
- Cifrado del mensaje utilizando la clave privada.
- Para evitar la lentitud se hace una operación hash: resumen asociado univocamente a los datos y de longitud fija.

Firma Digital.

Proceso:



Firma Digital.

Proceso de verificación:

- Descifrado del resumen mediante la clave pública de quien dice haber firmado el documento.
- Generar un resumen del documento original.
- Comparación de los resúmenes.

Almacenamiento de la Clave Privada.

Soporte lógico

- Se almacena en un fichero de disco o cualquier otro dispositivo lógico.
- La ejecución de la operación criptográfica se realiza por por una aplicación que implementa los algoritmos criptográficos, utilizando para ello las claves contenidas en ficheros de disco.
- Desventaja: es susceptible de ser duplicada.

Almacenamiento de la Clave Privada.

Soporte físico

- Se almacena en un dispositivo físico como puede ser una tarjeta inteligente, una tarjeta de expansión o cualquier elemento cuya duplicación sea muy difícil de realizar.

- Ventaja fundamental: dificil duplicación.

- Existen dispositivos hardware con capacidad propia de procesamiento criptográfico, con lo que se tiene la certeza de que la clave privada jamás es extraída del dispositivo.

Almacenamiento de la Clave Privada.

Tarjeta Inteligente

- Mecanismo muy utilizado como soporte para las claves criptográficas debido a:
  - Su reducido tamaño.
  - Su estandarización.
  - Su uso extendido.
- Tecnología y aplicaciones.
- Ventajas de la Tarjeta Inteligente en Cuanto a Seguridad.

Almacenamiento de la Clave Privada.

Tecnología y Aplicaciones

- La evolución de las tarjetas inteligentes ha venido condicionada por:
  - La tecnología de integración de circuitos.
  - Las aplicaciones a las que se han dedicado.
- **Evolución**: incremento tanto de la capacidad de almacenamiento como de la velocidad de ejecución.
- **Aplicaciones**: entorno bancario, tarjetas de almacenamiento de información médica, tarjetas de acceso a servicios de telecomunicaciones como GSM y control de acceso y seguridad informática.
- **Tarjetas Java o Java Card**: permiten modificar los datos y los programas que la tarjeta puede ejecutar.
- **Ejemplos del uso en España**: en las tarjetas bancarias de crédito y débito, los módulos SIMM de teléfonos móviles GSM, la Tarjeta de la Seguridad Social (TASS), el proyecto CERES o la securización de equipos o aplicaciones informáticas.

Almacenamiento de la Clave Privada.

Ventajas de la Tarjeta Inteligente en Cuanto a Seguridad

- Tarjeta inteligente NO criptográfica:
  - Mecanismos de protección que impiden la lectura de la información que contiene.
  - Dificil duplicación de la información que contiene.
  - Un usuario de tarjeta es consciente de no tener su tarjeta y proceder inmediatamente a la revocación del certificado.
  - Impide un número de intentos superior a tres.
  - Soporte con alta portabilidad.
  - Facilita el paso al uso de tarjeta criptográfica.

- Tarjeta inteligente criptográfica:
  - Soporte de claves privadas más seguro existente actualmente.
  - Realización de los procesos de firma y cifrado internamente.
  - Protegida por PIN.
  - Disponibilidad de servicios en cualquier momento, gracias a su portabilidad.

Certificado Digital.

- Documento electrónico que asocia una clave pública con la identidad de su propietario.
- Otros atributos:
  - Ámbito de utilización de la clave pública.
  - Fechas de inicio y fin de validez del certificado...

Terceras Partes Confiables.

Modelo de confianza en terceras partes. TTP.

- La validez de un certificado es la confianza en que la clave pública que contiene pertenece al usuario indicado en el certificado.
- Dos usuarios que no han tenido relación previa pueden confiar entre sí si ambos tienen relación con una tercera parte, que puede dar fé de la fiabilidad de los dos.
- La mejor forma de distribución de las claves públicas de los usuarios es que algún agente en el que todos confien las publique en un repositorio al que todos tengan acceso.
- La TTP que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública es la Autoridad de Certificación.(CA)

PGP.

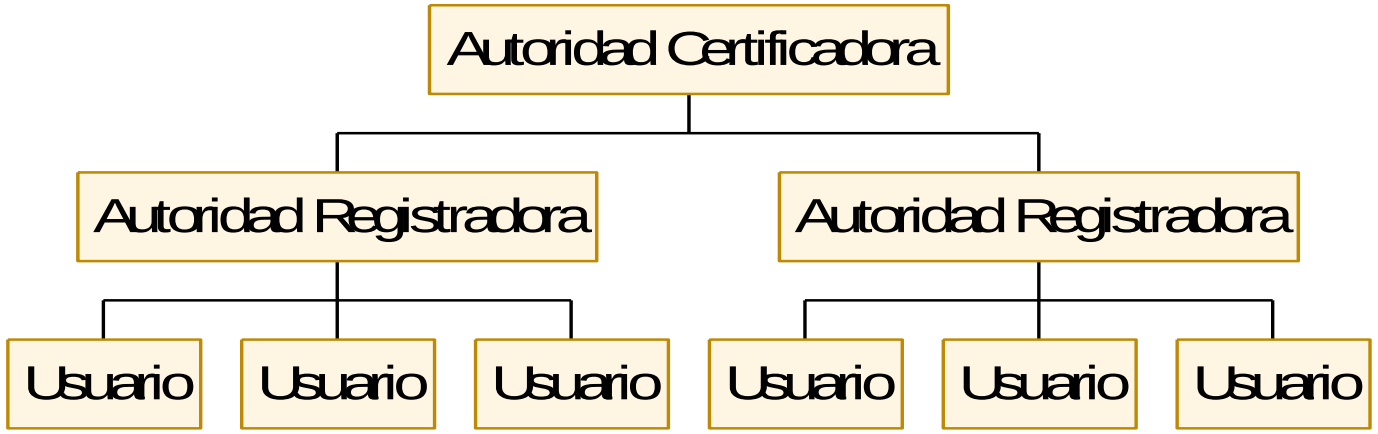
Privacidad bastante buena (PGP).

- Es un programa informático que utiliza técnicas criptográficas de clave pública para realizar cifrado y firma digital de documentos y correo electrónico.
- Diferencias con PKI:
  - Cada usuario genera y gestiona sus claves y se encarga de hacer llegar su clave pública al resto de los usuarios.
  - Formato del certificado, contiene:
    - Versión de PGP utilizada.
    - Clave pública del titular.
    - Periodo de validez
    - Firma realizada con la clave privada asociada a la pública que se está certificando.
  - El propio titular del certificado garantiza su integridad, en lugar de una TTP.

Estándares de Criptografía Clave Pública.

- Los PKCS (#1-15) establecen las recomendaciones relacionadas con la criptografía de clave pública.
- Desarrollados y mantenidos por los laboratorios RSA
- Más importantes:
  - PKCS#1: Cifrado y firma digital RSA. Base del resto.
  - PKCS#7: Mensaje criptográfico: CMS (Cryptographic Message Sintax) es la RFC 2630
  - PKCS#9: Tipos de datos usados por otros PKCSs
  - PKCS#10: Envío de clave pública a la CA
  - PKCS#11: API para uso de dispositivos criptográficos (tarjeta)
  - PKCS#15: Complementario a PKCS#11. Formato de la información almacenada en la tarjeta.

Infraestructura de Clave Pública (PKI).



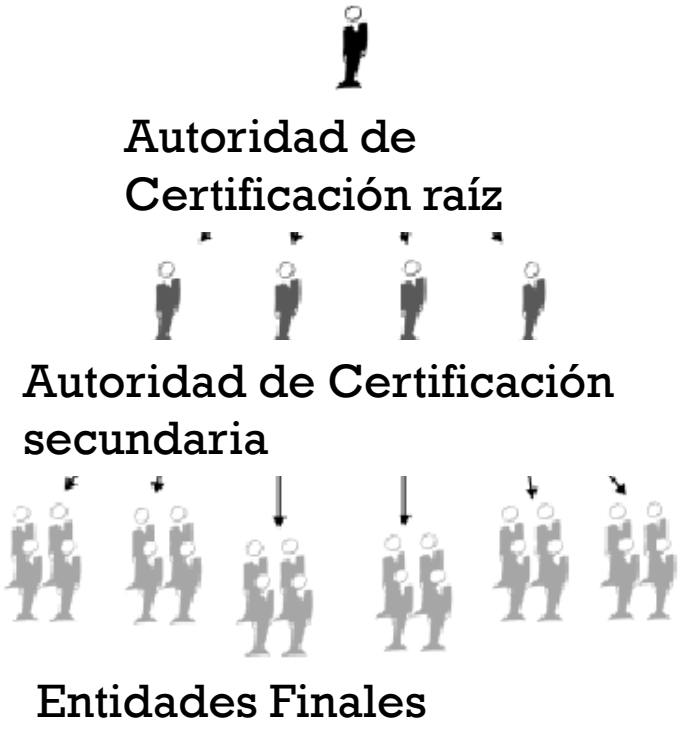
PKI: Ofrecen

- Registro de claves
- Revocación de certificados
- Selección de claves
- Evaluación de la confianza
- Recuperación de claves

Autoridad Certificadora: entidad confiable que

- emite los certificados digitales de los usuarios
- crea las claves de los usuarios (opcionalmente)

Certificación Jerarquizada



Autoridad de Certificación raíz

- Emite certificados a Autoridades de Certificación subordinadas a ella (CAs secundarias).
- Firma digitalmente con su clave pública:
  - los certificados digitales de las CAs secundarias
  - su propio certificado digital

Autoridades de Certificación secundarias

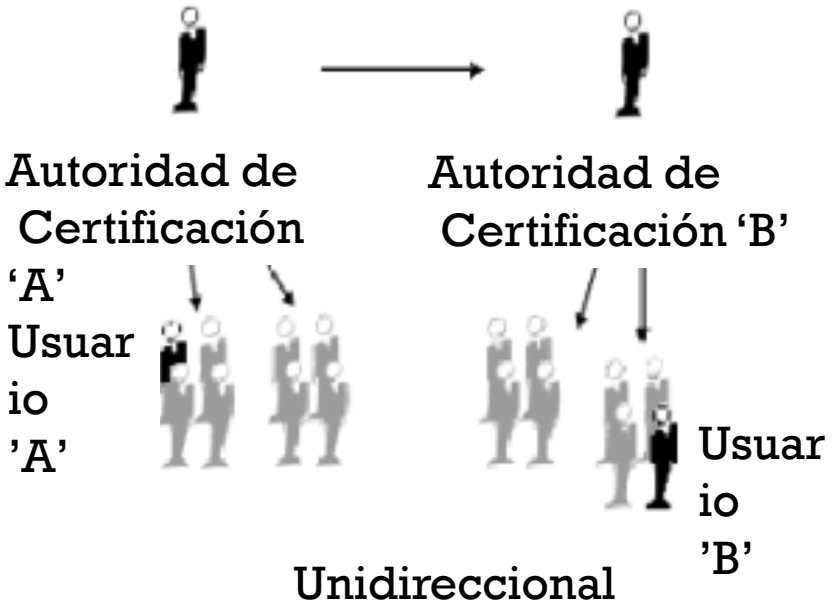
- Emiten los certificados a las Entidades Finales (EEs, End Entities) o incluso a otras Autoridades de Certificación subordinadas de ellas.
- Firman digitalmente con su clave privada:
  - los certificados digitales de las Entidades Finales
  - los cerificados digitales de otras Autoridades de Certificación subordinadas de ellas

Entidades Finales

Elementos de una PKI que no son Autoridades de Certificación.

Pueden ser un usuario humano, un ordenador o, incluso, un agente software.

Certificación Cruzada.



- **Certificado cruzado:** documento electrónico firmado digitalmente por la CA en el que se asocia la clave pública de la otra CA a su identidad.
- **Certificación cruzada unidireccional:**

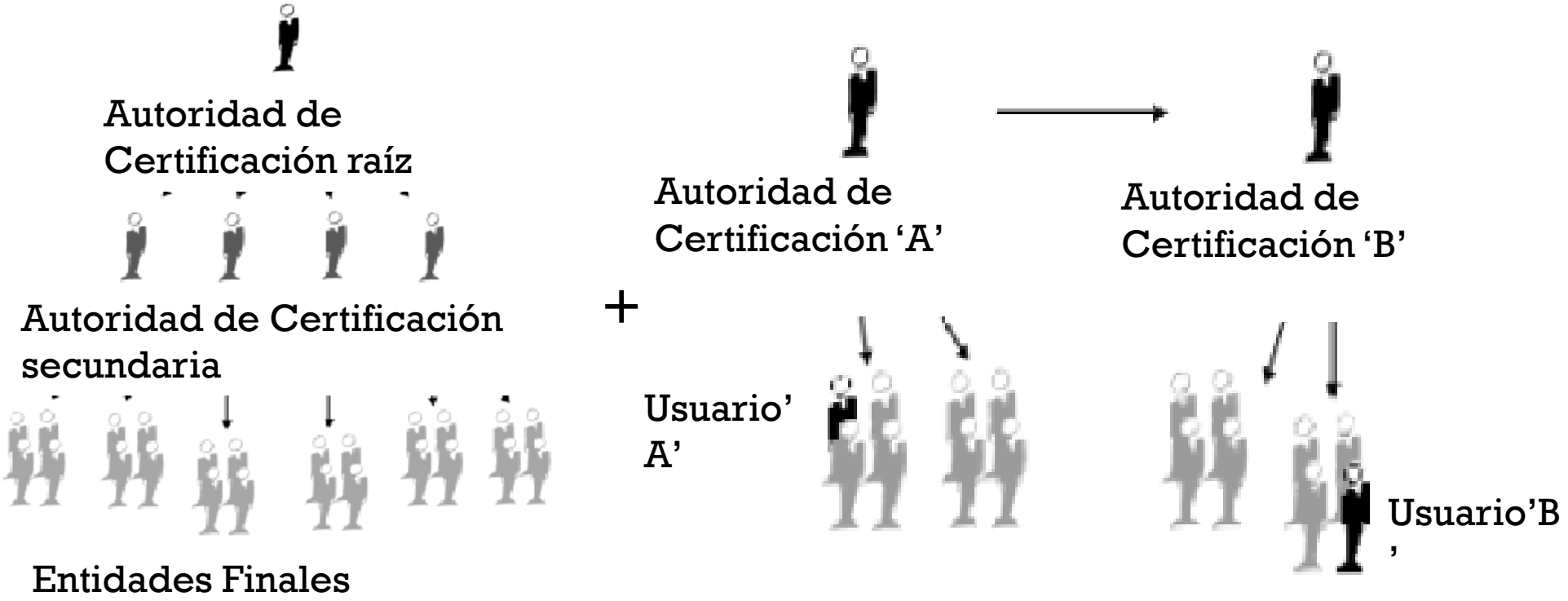
  CA 'A' emite un certificado cruzado a la CA 'B'.

  El usuario 'A' reconocerá los certificados emitidos por CA 'B' como si fueran de su propia CA. Usuario 'B' fiable.
- **Certificación cruzada bidireccional o mutua:**

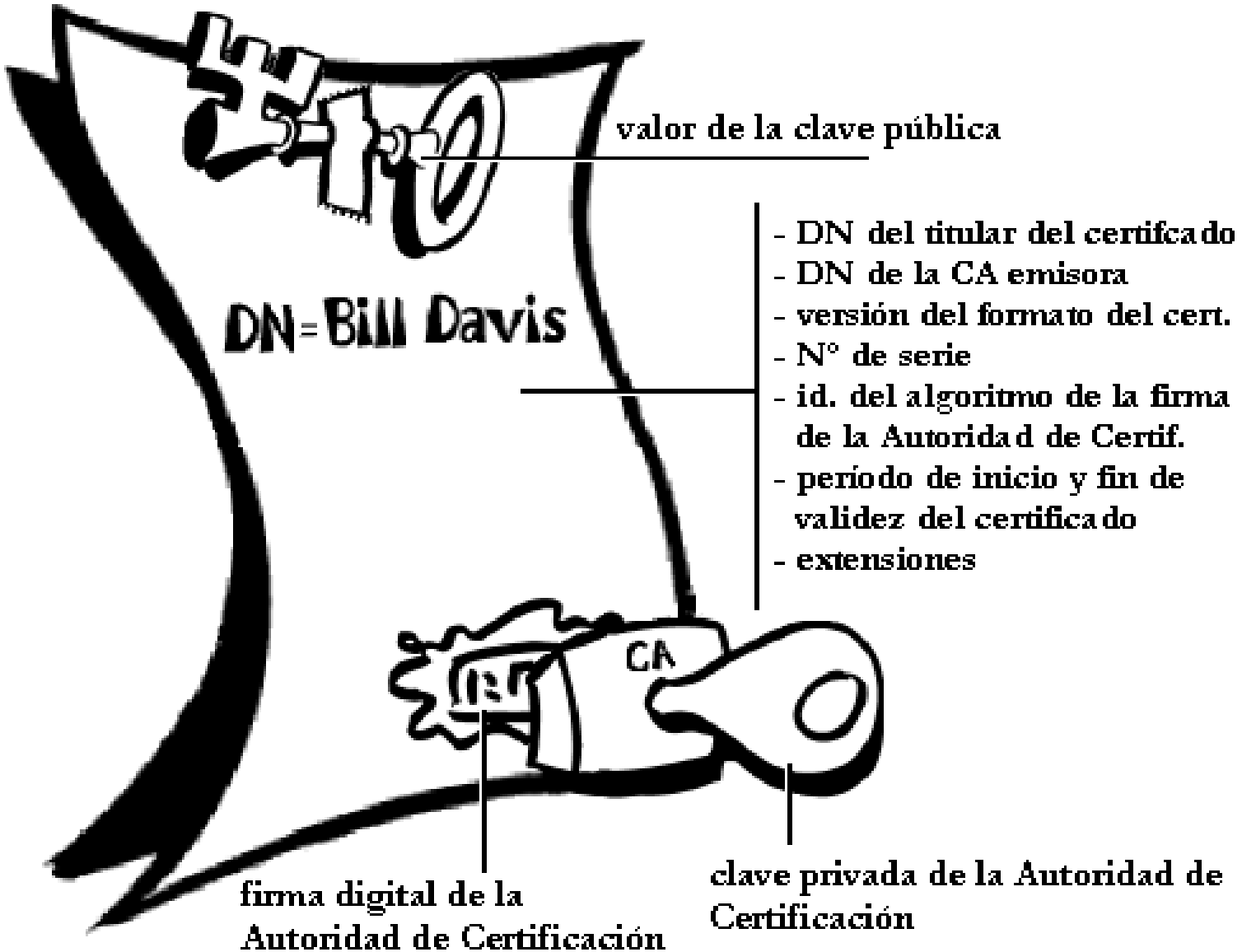
  CA 'B' emite también un certificado a la CA 'A'

  Usuario 'B' reconocerá los certificados del usuario 'A'.

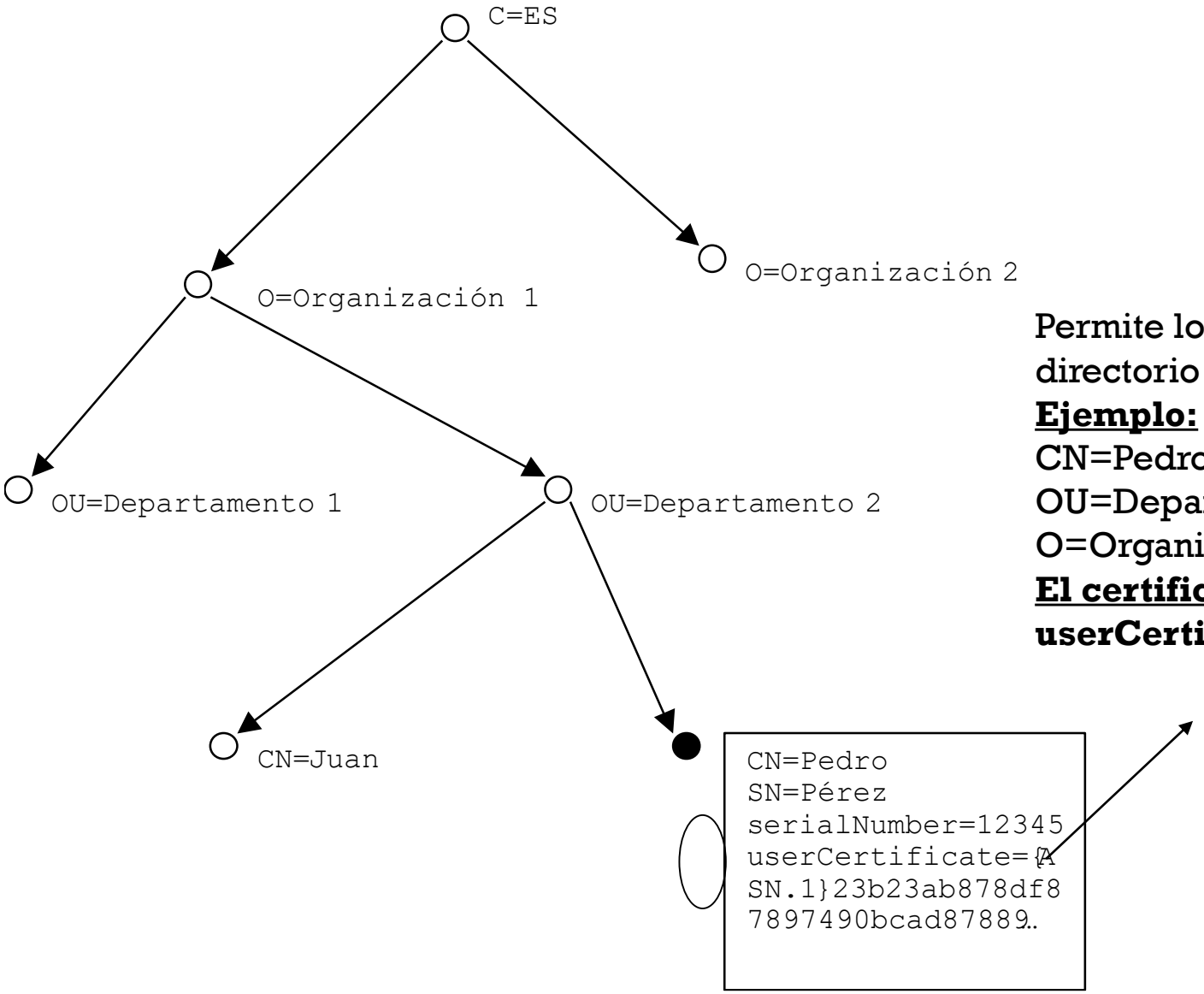
Certificación Híbrida.



Certificado Digital X.509 Versión 3.



Nombre distintivo.



Permite localizar información en un directorio X.500.

Ejemplo:

CN=Pedro + SN=Pérez,
OU=Departamento 2,
O=Organización 1, C=ES

El certificado digital, en el atributo **userCertificate**

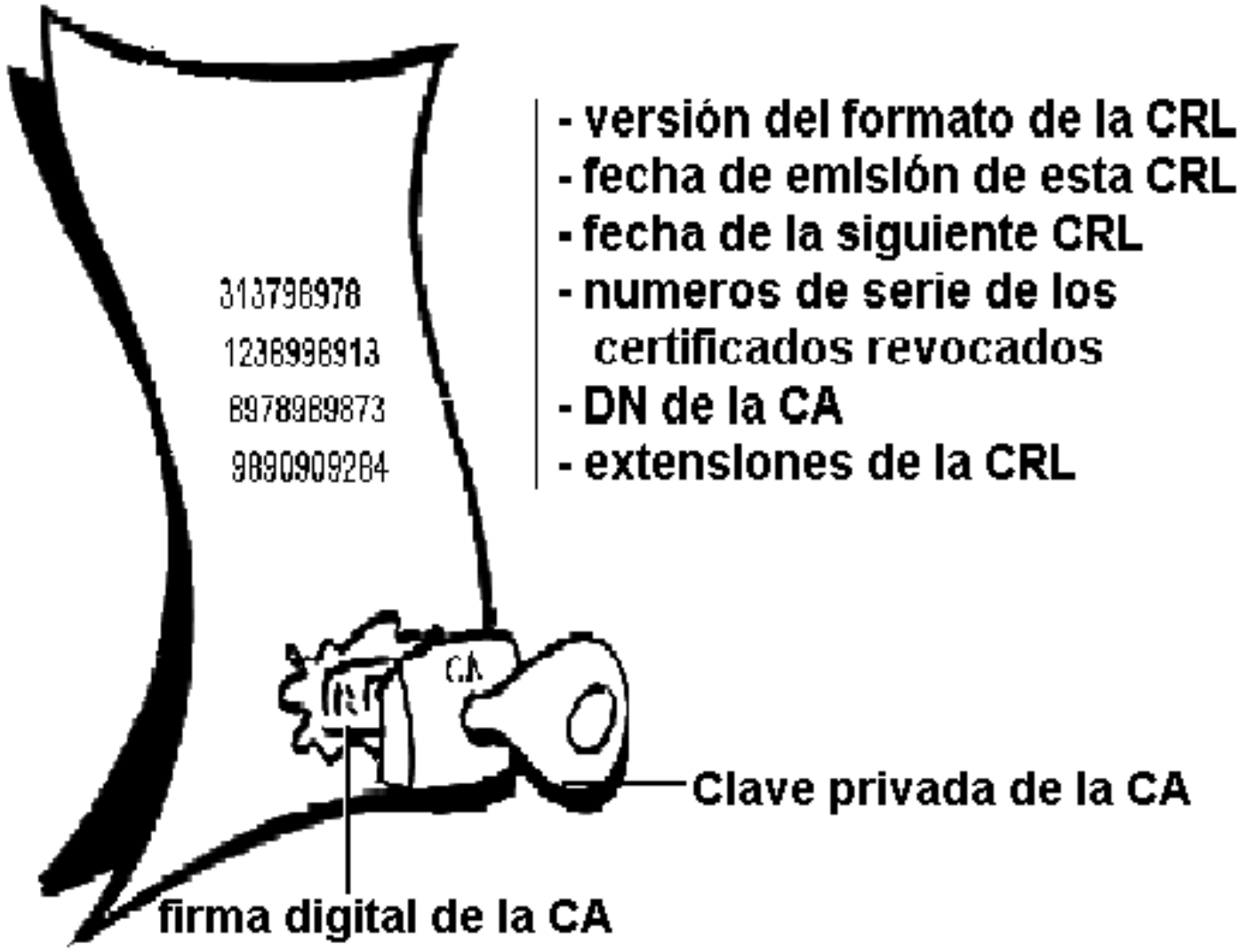
Lista de Revocación de Certificados.

- Documento digital
  - Firmado por la AC
  - Publicado en el repositorio de información accesible a todos los usuarios mediante el cual la CA indica todos los certificados que han sido revocados.

- En el caso de PKI de número de usuarios considerable, la lista de revocación está dividida en distintos fragmentos.

- Las listas de revocación son actualizadas cada cierto tiempo: la CA emitirá una lista de revocación en un determinado instante, que incluirá los números de serie de los certificados que se han revocado desde la emisión de la CRL anterior.

Lista de Revocación de Certificados.



Otras Terceras Partes de Confianza.

- Autoridad de Fechado Digital
  - Propuestas para el Fechado Digital
  - El Certificado de Tiempo
- Servidor OCSP

Autoridad de Fechado Digital.

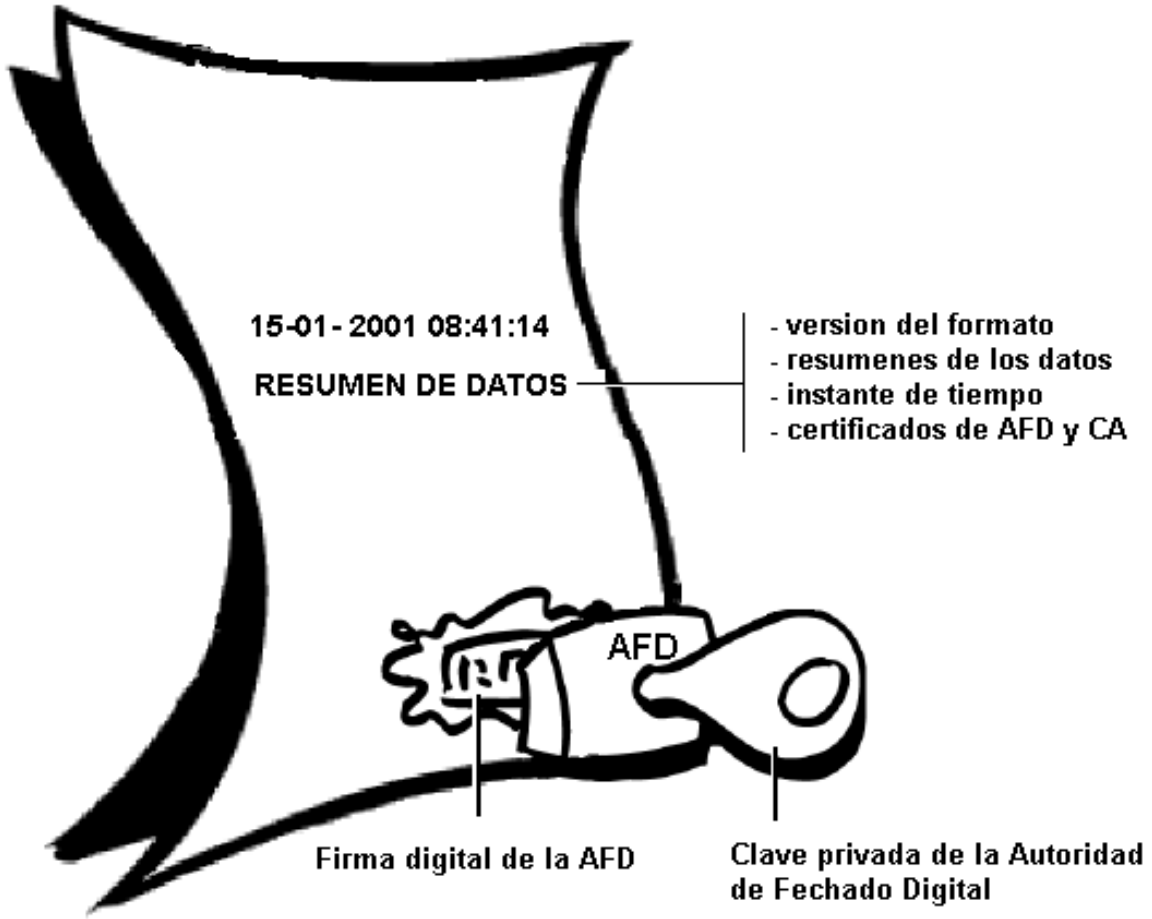
- Para el **No Repudio.**
- Ofrece evidencia de la existencia de documentos de un determinado momento de tiempo.
- Clave privada + certificado digital asociado + reloj fiable.
- AFD: emisión de certificados de tiempo.
  - **Propuestas para el Fechado Digital**
    - **PKIX**
    - **ISO:**

      Protocolo básico: **recoger** el resumen de un documento, que el cliente le envía+ **concatenarlo** con la fecha y hora + **firmar** el conjunto digitalmente.

      Protocolo vinculado: además de insertar la fecha y hora, **serializa** los actos de firma.

      Protocolo distribuido: no utilizar un único fechador, sino varios.

El Certificado de Tiempo.



Aplicación de PKI en TIC.

- Orientadas a ofrecer soluciones a los problemas de:
  - falta de confidencialidad
  - autenticación

en los entornos de:

  - correo electrónico
  - navegación por páginas web.

Seguridad en la Web.

- **PROBLEMA:** Medidas de seguridad
- **SOLUCIÓN: SSL** (Netscape pionero)
  - Protocolo para la **securización** de canales de transmisión de información basados en la pila TCP/IP
  - **Protege** cualquier aplicación de arquitectura **cliente-servidor**.
  - Mayor utilización: entornos Web (protocolo HTTP)
  - Indicador: **https://** en la barra de direcciones
  - Interfaces:
- **PKCS#11** (Netscape)
- **CryptoAPI** (Microsoft)

Uso de SSL (Características).

PROPORCIONA:

- Servicios de seguridad:
  - Confidencialidad
  - Autentificación
  - Integridad
- Extensionalidad
- Autentificación
- Compatibilidad

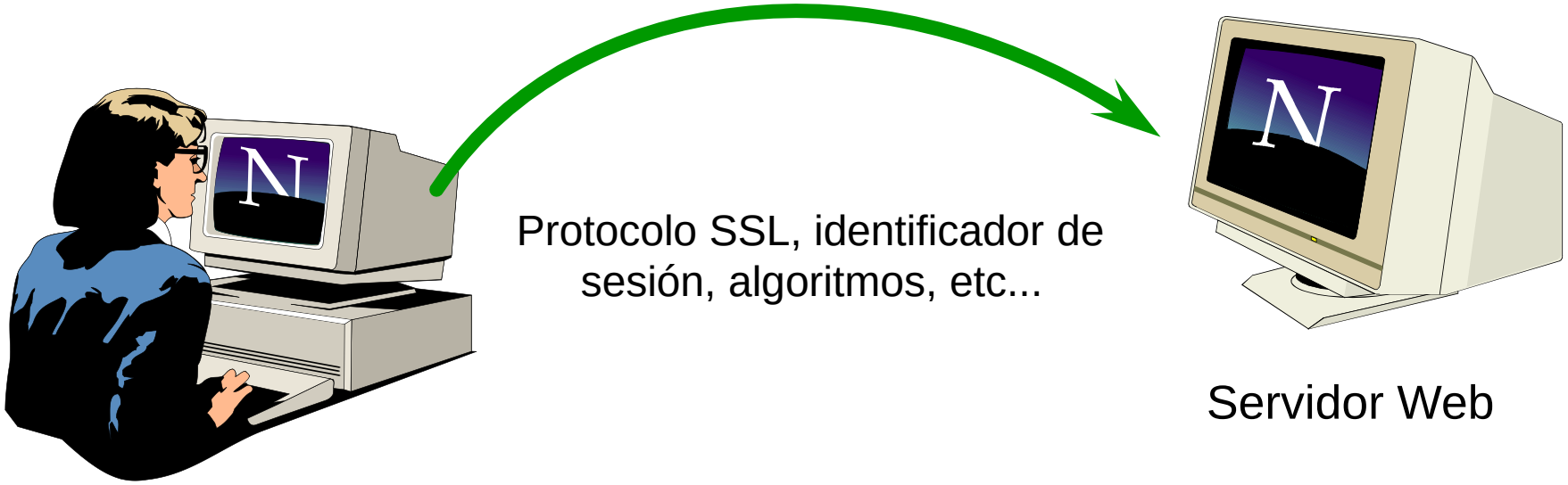
PROTEGE EN LOS ENTORNOS WEB:

- La dirección URL del documento requerido
- El contenido del documento requerido
- Las ‘’cookies” intercambiadas entre el navegador y el servidor
- El contenido de las cabeceras HTTP

Procedimiento de Autentificación de SSL o Handshake.

- Procedimiento para la autenticación entre el cliente y el servidor.
- El servidor presenta al cliente su certificado y, opcionalmente, le solicita un certificado para poder entrar.
- Se intercambia información sobre los algoritmos soportados así como una clave simétrica para el cifrado de la comunicación.
- Está compuesto por las siguientes fases:

El mensaje ‘’Hola’’ del Cliente.



⌘ Conectandose al sitio seguro mandamos un mensaje **‘’Hola”** desde el cliente al servidor Web, indicando que se solicita una sesión segura.

⌘ El mensaje **‘’Hola”** incluye información sobre el protocolo SSL, identificador de sesión, y algoritmos soportados por el cliente.

La Respuesta del Servidor.

- Protocolo SSL, identificador de sesión, algoritmos, etc...
- (Opcional) “Envía tu Certificado”

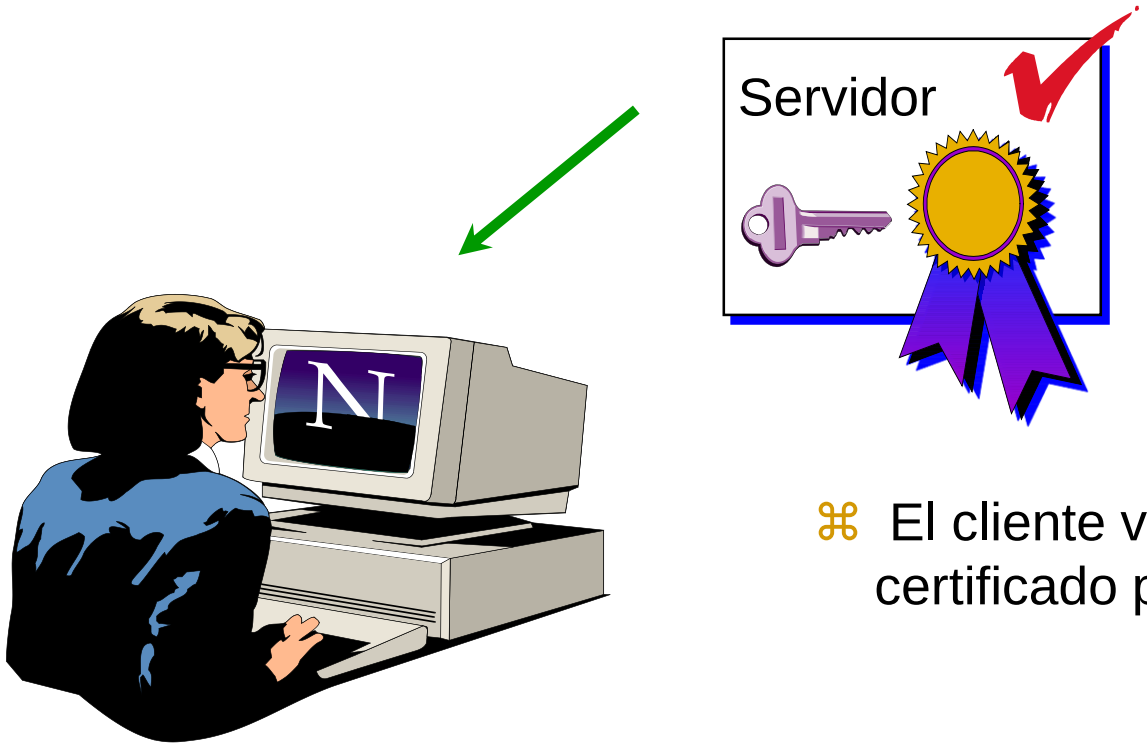
Servidor Web

⌘ El mensaje **‘’Hola”** del servidor incluye su certificado digital y la respuesta a los algoritmos soportados.

⌘ El cliente comprueba si la dirección contenida en el certificado coincide con la de conexión.

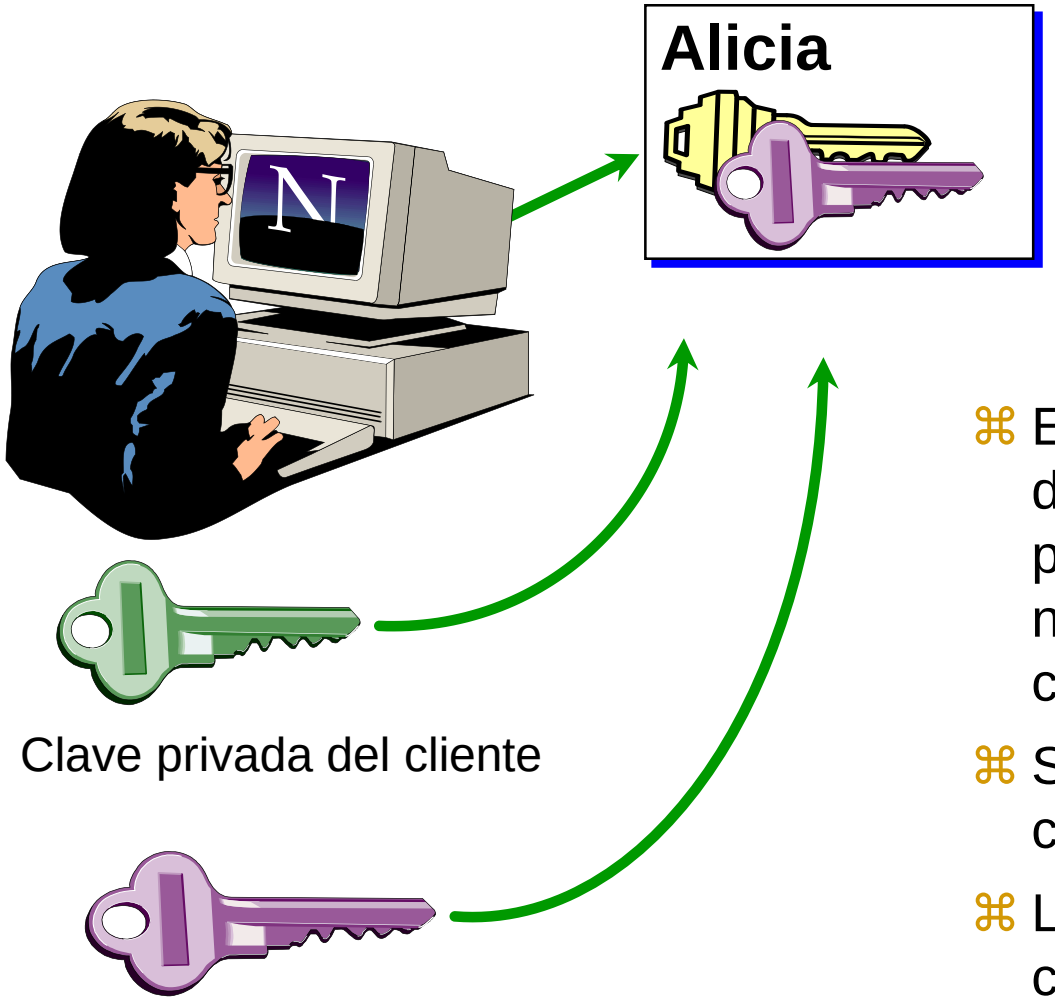
⌘ Si está configurada la autenticación de cliente, el servidor soluciona al cliente un certificado.

La Autentificación del Servidor.



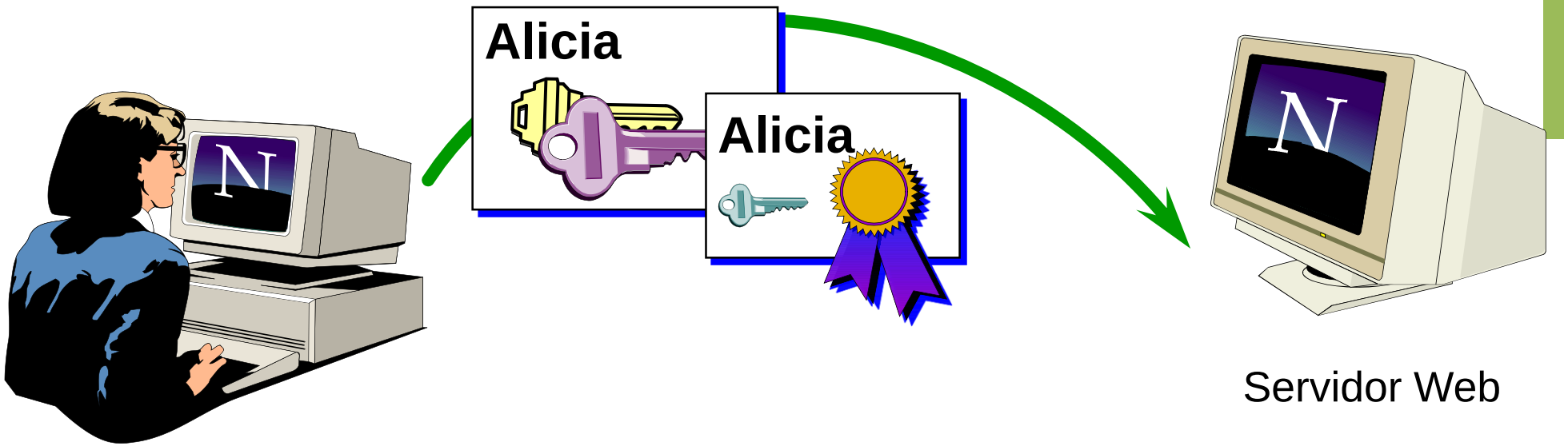
- El cliente verifica la firma del certificado presentado por el servidor.

Generación de la Clave Simétrica.



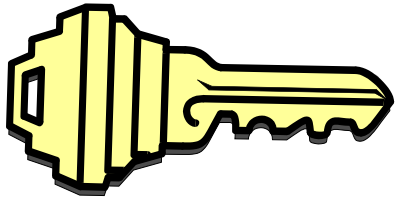
- El cliente firma digitalmente algunos datos, utilizando para ello su clave privada y el módulo criptográfico del navegador, o un dispositivo criptográfico externo.
- Se genera de forma aleatoria una clave simétrica.
- La clave simétrica se cifra usando la clave pública del servidor.

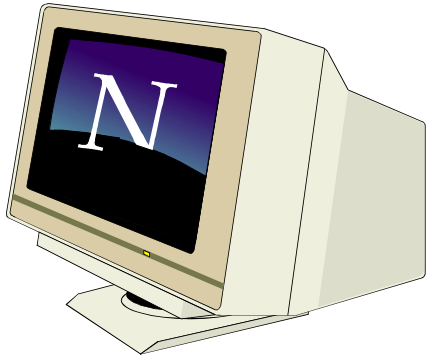
Envío de la Clave Simétrica.



- El cliente envía la clave simétrica cifrada al servidor para que cada uno tenga una copia de la clave.
- El cliente le envía también su certificado.

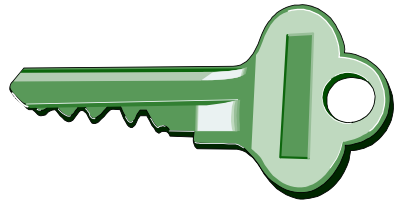
Descifrando la Clave Simétrica.





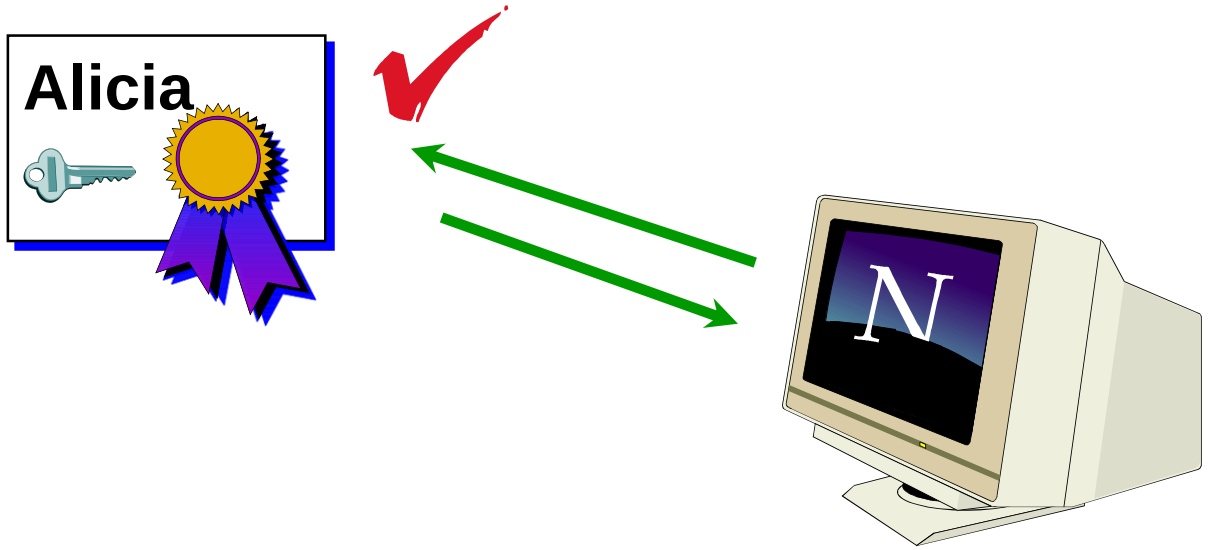
Servidor Web

- El servidor utiliza su clave privada para descifrar la clave simétrica.



Clave privada del servidor

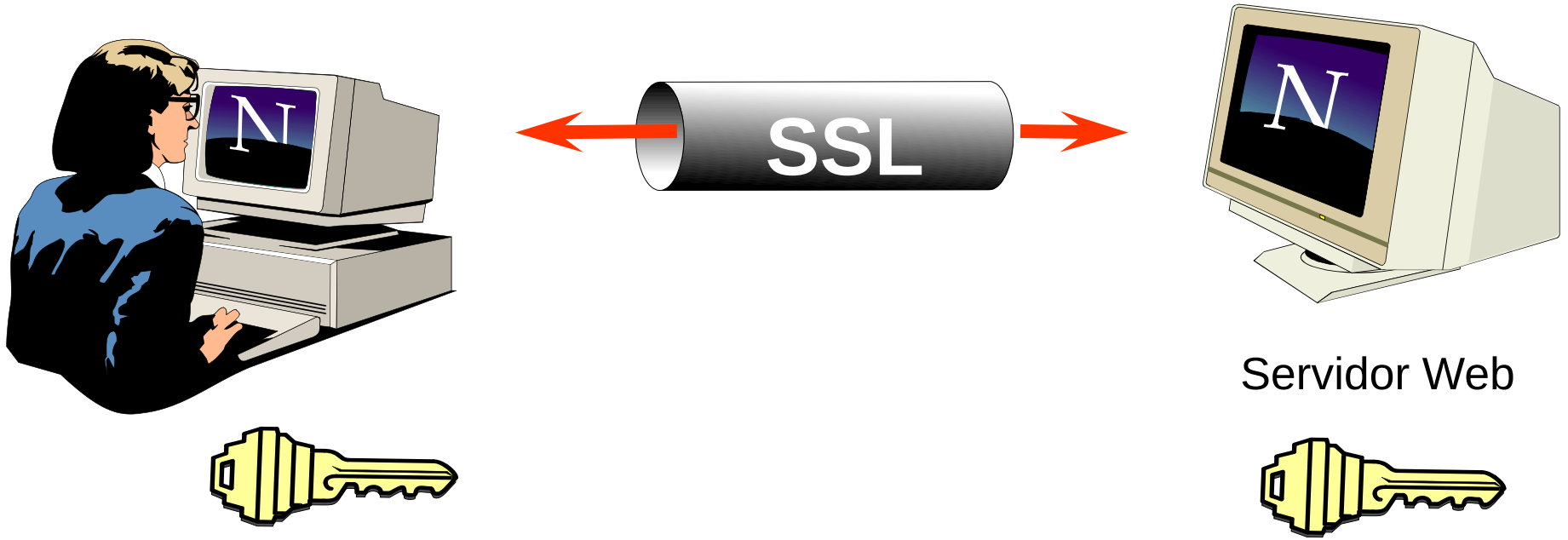
La Autentificación del Cliente.



⌘ El servidor verifica la firma de datos enviada por el cliente.

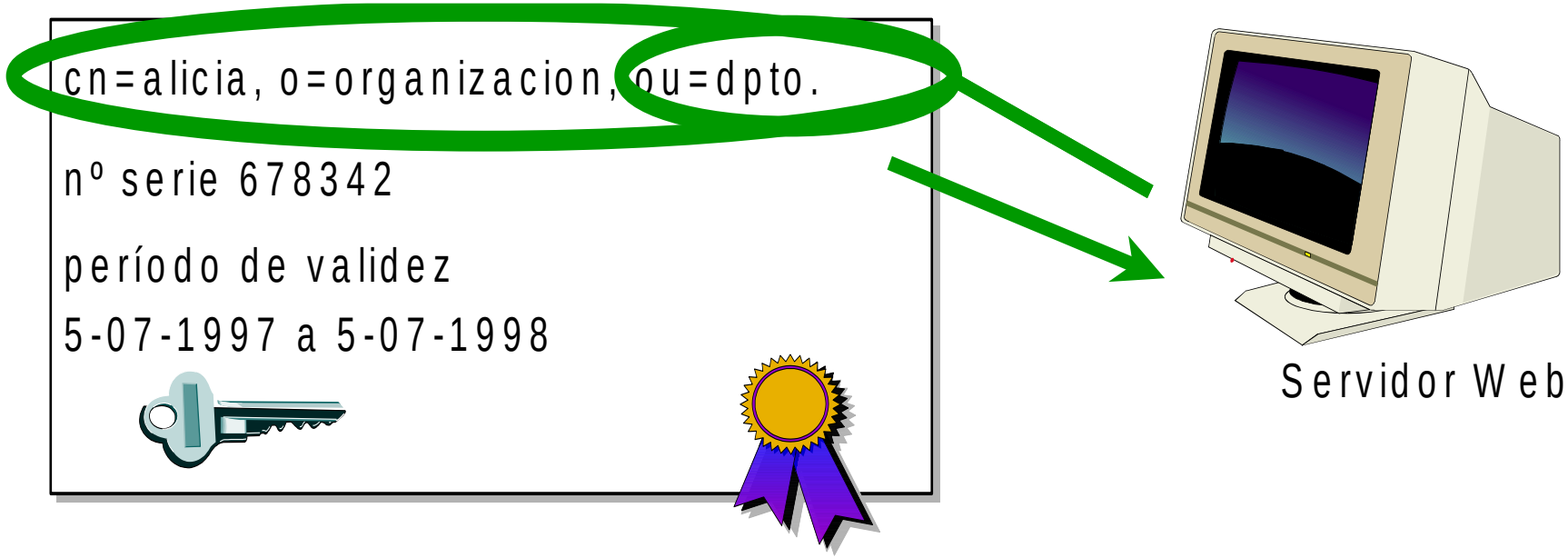
Servidor Web

Finalización del Proceso de Autentificación.



- El proceso de autenticación (“handshake”) finaliza con la posesión por parte de ambos de la clave simétrica.
- A partir de este momento, toda la información intercambiada irá cifrada con la clave simétrica.

Control de Acceso.



⌘ Opcionalmente, si está configurado de esa forma, el servidor web ofrecerá a las aplicaciones (CGIs) la información contenida en el certificado del cliente para poder realizar un control de acceso.

Seguridad en el Correo Electrónico: Uso de S/MIME.

S/MIME

- Conjunto de recomendaciones por las que se estudia la forma de integrar técnicas criptográficas de clave pública en las Extensiones Multipropósito para el Correo Electrónico.

- Conjunto de nuevos tipos MIME para los tipos de datos definidos en el estándar CMS.
  - Se consigue una forma de incluir información cifrada y firmada (utilizando algoritmos de clave pública) en cualquier aplicación que utilice MIME.

- Las aplicaciones cliente de correo de Netscape (Messenger) y Microsoft (Outlook Express) soportan directamente S/MIME versiones 2 y 3, utilizando, para ello, el mismo núcleo criptográfico y, por tanto, mismas claves y mismo repositorio de Autoridades de Certificación reconocidas, que en los respectivos navegadores.

- Otros productos: Eudora, Microsoft Exchange, Microsoft Outlook, Lotus Notes, etc.

Seguridad en el Correo Electrónico: Uso de S/MIME

- Cuando un usuario recibe un mensaje firmado digitalmente, después de verificar la firma del mensaje y la de los certificados (y, consulta a listas de revocación o servidor OCSP sobre el estado de revocación), se comprueba si la dirección de correo electrónico contenida en el certificado coincide con la del remitente del mensaje.

- En cuanto al cifrado de mensajes, debido a que se necesita la clave pública de los destinatarios, puede realizarse una búsqueda en el directorio en el que se encuentran publicados los certificados utilizando como criterio de búsqueda las direcciones de correo.
- En otras ocasiones, es el propio usuario quien se encarga de conseguir una copia de los certificados de los destinatarios, mediante una interfaz de búsqueda en el directorio para indicar el certificado de cada destinatario, o bien consultando su disco duro.

Firma Digital de Módulos Software.

- **Garantizar** la seguridad en el puesto en el que se produce la descarga del módulo software de manera que si necesita en su ejecución acceder a recursos del sistema, ha de estar firmado digitalmente utilizando una clave privada cuya clave pública correspondiente esté incluida en un certificado emitido por alguna de las AC configuradas como confiables en el navegador.

- El navegador, antes de proceder a la ejecución del módulo, verificará la firma del módulo y, en caso de que no exista tal firma o que ésta no se verifique correctamente, cancelará la ejecución.

- Adicionalmente, mostrará al usuario el certificado con el que se ha realizado la verificación y solicitará confirmación de su ejecución.

Firma Digital de Módulos Software.

- El usuario conocerá la identidad del firmante y considerará si puede o no fiarse de la ejecución.