UNIVERSIDAD AMERICANA

Redes de comunicación

Unidad IV- Sistemas de Autenticación y firmas digitales

Recopilación de teoría referente a la materia

Ing. Luis Müller

2011

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

Contenido

Unidad IV – Sistemas de Autenticación y Firmas Digitales
Conceptos básicos. Tipos de algoritmos. Aplicaciones e-commerce

INTRODUCCIÓN HISTÓRICA

Desde que el hombre es consciente de sí mismo, e incluso desde antes, tiene la necesidad básica de comunicarse. De hecho la interrelación humana es una de las grandes bases del desarrollo actual. Pero es en los últimos tiempos cuando se le está dando a la comunicación la importancia que realmente tiene o en su defecto quizás se la valora demasiado. En cualquier caso, en nuestro tiempo, el valor de la comunicación queda claro y más con la aplicación de las nuevas tecnologías.

Una vez que el hombre se comunica también necesita tener una cierta privacidad en esa comunicación. Es decir, que únicamente el receptor o receptores a los que va dirigido el mensaje lo reciban.

Por lo que con esto comienza un nuevo aspecto en la comunicación, la parte que corresponde a la codificación de mensajes, encriptación, etc.

Desde tiempos antiguos se utilizan claves o códigos especiales para prevenir que personas que no son los destinatarios reales del mensaje puedan interferir e incluso modificar el contenido del mismo. Un claro ejemplo es la clave utilizada por Julio Cesar para transmitir mensajes que fueran ininteligibles cuando se interceptaran por sus enemigos. Consistía en cambiar cada letra del mensaje por la letra que estaba tres posiciones detrás en el abecedario. Por ejemplo la palabra PERRO quedaría codificada de la siguiente manera SHUUR. Pero claro esta clave es muy conocida, por lo que es totalmente inválida.

Certificados digitales

Los certificados digitales, tienen una similitud con las licencias de conducir, las primeras permiten viajar por las carreteras, los certificados digitales permiten navegar por internet, la principal característica es que da identidad al usuario y puede navegar con seguridad.

De igual forma que la licencia de conducir o un pasaporte sirve para dar identidad a quien la porta en ciertos casos, el certificado digital da identidad a una clave pública y se comporta como una persona en el espacio cibernético.

El nacimiento del certificado digital fue a raíz de resolver el problema de administrar las claves públicas y que la identidad del dueño no pueda ser falsificada.

La idea es que una tercera entidad intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado.

Esto fue inicialmente planteado por Kohnfelder del MIT en su tesis de licenciatura. Las tres partes más importantes de un certificado digital son: Una clave pública

La identidad del implicado: nombre y datos generales, la firma privada de una tercera entidad llamada autoridad certificadora que todos reconocen como tal y que valida la asociación de la clave pública en cuestión con el tipo que dice ser.

En la actualidad casi todas las aplicaciones de comercio electrónico y transacciones seguras requieren un certificado digital, se ha propagado tanto su uso que se tiene ya un formato estándar de certificado digital, este es conocido como X509 v.3 Algunos de los datos más importantes de este formato son los siguientes:

Versión: 1,2 o 3

Número de Serie: 0000000000000000

Emisor del Certificado: VeriMex

Identificador del Algoritmo usado en la firma: RSA, DSA o CE

Periodo de Validez: De Enero 2002 a Dic 2003

Sujeto: Anita

Información de la clave pública del sujeto: la clave, longitud, y demás parámetros

Algunos datos opcionales, extensiones que permite la v3

Firma de la Autoridad Certificadora

Un certificado digital entonces se reduce a un archivo de uno o dos koctetos de tamaño, que autentica a un usuario de la red.

En nuestro caso se trata de verificar la identidad de las personas que acceden a los sistemas informáticos o que envían mensajes electrónicamente. Para ello se utiliza la encriptación con todo su potencial.

Para los mensajes o correos se utilizan las firmas digitales, que no es más que añadir al mensaje un pequeño texto cifrado

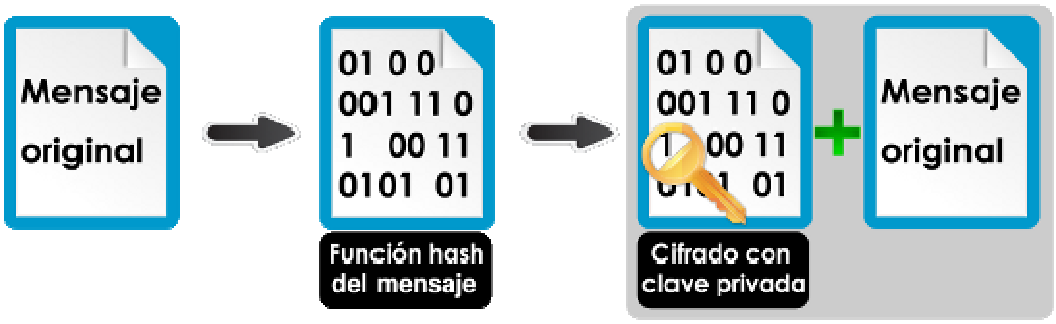
Firma electrónica

La firma electrónica es un conjunto de datos asociados a un mensaje que permite verificar su integridad y la identidad del firmante. La firma electrónica se basa en la criptografía asimétrica o de clave pública y se realiza de la siguiente manera:

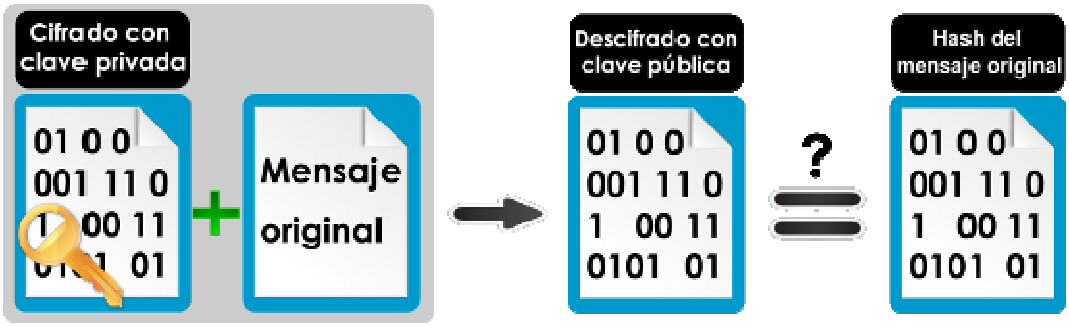
- El firmante dispone de un certificado con sus claves asociadas, una pública y otra privada. La clave pública del certificado es conocida también por el receptor.

- El firmante obtiene el resumen de los datos a firmar y lo cifra con su clave privada. El resultado es la firma electrónica que se añade al mensaje original.

- Una vez enviados los datos, el receptor descifra la firma adjuntada con la clave pública del emisor para obtener el resumen generado por el firmante. Por otro lado, realiza la función de resumen sobre los datos originales. A continuación se contrastan los dos resúmenes, el recibido y el generado. En caso de ser idénticos, la firma es correcta garantizándose la integridad de los datos así como la identidad del firmante. En caso contrario la firma no tiene ninguna validez, ya que demuestra que los datos han sido vulnerados.



Firma electrónica. Esquema vista emisor.



Firma electrónica. Esquema vista receptor.

Tipos de firma electrónica

Hay diferentes tipos de firma electrónica:

- **Firma básica**

Contiene un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio documento.

- **Firma avanzada**

Este tipo de firma electrónica permite identificar al firmante y detectar cualquier cambio posterior en los datos firmados. Está vinculada al firmante de manera única y a los datos a que se refiere. Debe crearse a través de medios que el firmante pueda mantener bajo su exclusivo control.

- **Firma reconocida**

La firma reconocida tiene las mismas características que la firma electrónica avanzada pero está basada en un certificado reconocido y ha sido generada mediante un dispositivo seguro de creación de firma, lo que le atribuye el mismo valor legal que a la firma manuscrita.

- **Firma fechada**

Firma electrónica a la que se le ha añadido un sello de tiempo. El sellado de tiempo (o *timestamping*) es un mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La autoridad de sellado de tiempo (TSA, del inglés *Time Stamping Authority*) actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

- **Firma validada**

Firma electrónica fechada a la que se le ha añadido información sobre la validez del certificado procedente de una consulta de CRL u OCSP realizada a la Autoridad de Validación.

- **Firma longeva**

Firma electrónica validada dotada de validez a lo largo del tiempo. Esto se consigue al ir refirmando y actualizando los sellos de tiempo de forma regular. Este proceso de refirmado se utiliza para garantizar que unos datos que fueron firmados con un algoritmo que era válido en su día, pero inseguros actualmente debido a la evolución tecnológica, no pierdan valor ya que se han ido refirmando siempre con algoritmos criptográficos seguros en cada momento.

¿QUÉ ES LA AUTENTICACIÓN?

El Authentication fue definido por Arnnei Speiser en 2003 mientras que la Web basó el servicio que proporciona en la autentificación de usuarios finales que tienen acceso (Log in) a un servicio de Internet.

En materia propiamente de autenticación lo que se pretende no es que se pueda leer el mensaje por personas ajenas, sino que se pueda asegurar la procedencia del mismo.

Todo esto no es nuevo ya que lo hemos estado utilizando desde muy antiguo:

- Los reyes de la edad media sellaban sus cartas lacrándolas y poniéndoles el sello en el lacrado.
- En mensajería usual (como CORREOS, empresas como SEUR, WRW, etc.) ponemos nuestra firma en cada envío.
- En las transferencias bancarias es necesario la firma de la persona que tiene la cuenta bancaria

Y por supuesto en materia de nuevas tecnologías también hay claros ejemplos:

- En los cajeros automáticos necesitamos una tarjeta identificadora y una clave de acceso a nuestra cuenta.
- En los accesos a los edificios de una cierta importancia como La Casa Blanca, el edificio central de la ONU en Bruselas, etc. muchas veces es necesario la posesión de una tarjeta identificadora y el siguiente escaneo de las huellas digitales.
- Y más cercano a nosotros es el acceso a sistemas Unix en los que cada cuenta de usuario necesita un log in y una clave de entrada.

Los objetivos que se pretenden con la autenticación en el envío de mensajes son los siguientes:

- Certeza de que el mensaje procede la persona que dice remitirlo.
- Se asegura de que ninguna persona ajena ha podido modificar el mensaje en cuestión.
- Seguridad por parte del remitente de que el receptor no

Autenticación

Autenticación o **autentificación** es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, es decir que reclama hecho por, o sobre la cosa son verdadero. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores.

Definiciones

Autenticación, **autentificación** (no recomendado) o mejor dicho **acreditación**, en términos de seguridad de redes de datos, se puede considerar uno de los tres pasos fundamentales (AAA). Cada uno de ellos es, de forma ordenada:

1. **Autenticación** En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.

2. **Autorización** Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
3. **Auditoría** Mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

Características de autenticación

Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable:

- Ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros).
- Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).
- Soportar con éxito cierto tipo de ataques.
- Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.

Mecanismo general de autenticación

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos.

El primer elemento necesario (y suficiente estrictamente hablando) por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único (valga la redundancia). Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como **log in**.

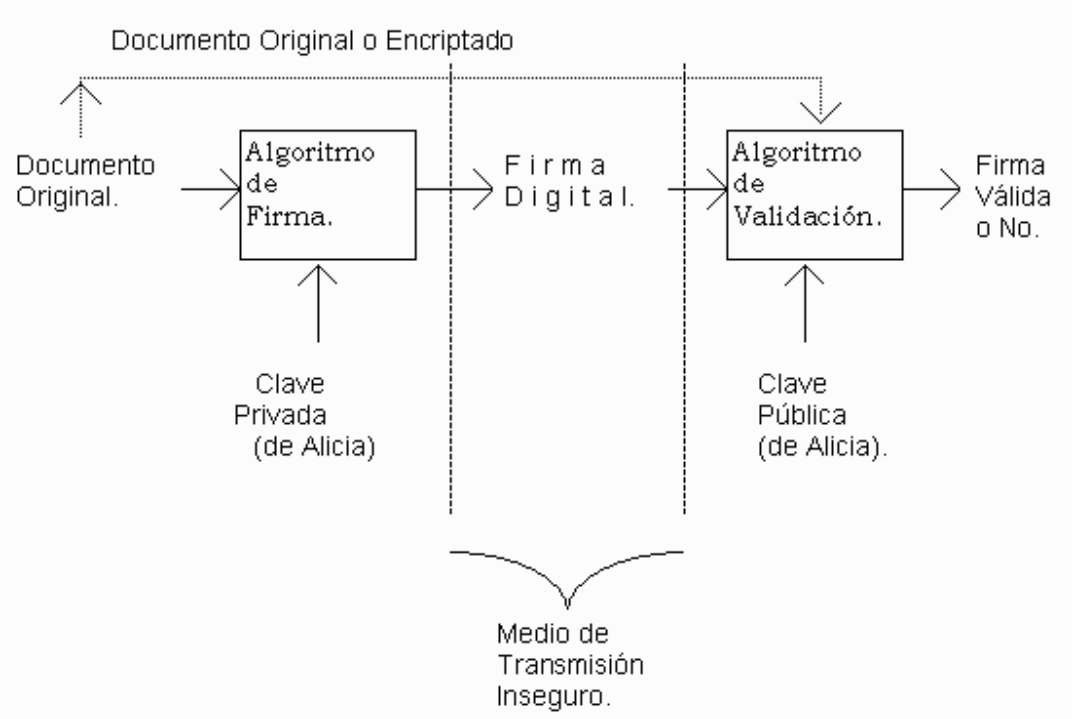
El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

Firma digital y autenticación.

La autenticación se efectúa de la siguiente manera:

1. Alicia firma un documento y procesa tanto su clave privada como el documento mismo, el producto se denomina firma digital y se adjunta al documento en el momento de enviarlo.
2. Juan verifica la firma mediante otro proceso que involucra al documento, la firma y la clave pública de Alicia.
3. Si los resultados mantienen una simple relación matemática, la firma se verifica como verdadera, de otro modo, la firma podría ser fraudulenta o el documento podría estar alterado y por lo tanto quedaría descartado.



Comercio electrónico

Al efectuar una operación comercial por Internet se presentan nuevos problemas, por ejemplo cómo saber que la tienda virtual existe verdaderamente, una vez hecho el pedido cómo saber que no se cambia la información, cuando se envía el número de tarjeta de crédito cómo saber si este permanecerá privado, en fin, para el comerciante también se presentan problemas similares, cómo saber que el cliente es honesto y no envía información falsa, etc.

Todos estos problemas pueden ser resueltos de manera satisfactoria si se implementan protocolos de comunicación segura usando criptografía.

Protocolos de seguridad

Un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica.

El ejemplo más común es **SSL** (**S**ecure **S**ockets **L**ayer) que vemos integrado en el navegador de Netscape y hace su aparición cuando el candado de la barra de herramientas se cierra y también sí la dirección de Internet cambia de http a https.

Otro ejemplo es **PGP** que es un protocolo libre ampliamente usado de intercambio de correo electrónico seguro, uno más es el conocido y muy publicitado **SET** que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito, **IPsec** que proporciona seguridad en la conexión de Internet a un nivel más bajo.

Estos y cualquier protocolo de seguridad procura resolver algunos de los problemas de la seguridad como la integridad, la confidencialidad, la autenticación y el no rechazo, mediante sus diferentes características.

Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

Enseguida vemos un escenario donde puede ocurrir algo de esto:

Por ejemplo sobre la seguridad por Internet se deben de considerar las siguientes tres partes: seguridad en el navegador (Netscape, Opera, ...), la seguridad en el Web server (el servidor al cual nos conectamos) y la seguridad de la conexión.

Un ejemplo de protocolo es **SET**, objetivo efectuar transacciones seguras con tarjeta de crédito, usa certificados digitales, criptografía de clave pública y criptografía de clave privada.

SSL Es el protocolo de comunicación segura más conocido y usado actualmente, **SSL** actúa en la capa de comunicación y es como un túnel que protege a toda la información enviada y recibida.**SSL** es usado en gran cantidad de aplicaciones que requieren proteger la comunicación.

Con **SSL** se pueden usar diferentes algoritmos para las diferentes aplicaciones, por ejemplo usa **DES**, **TDES**, **RC2**, **RC4**,**MD5**, **SHA-1**, **DH** y **RSA**, cuando una comunicación esta bajo **SSL** la información que se cifra es:

El URL del documento requerido

El contenido del documento requerido

El contenido de cualquier forma requerida

Los "cookies" enviados del browser al servidor

Los "cookies" enviados del servidor al browser

El contenido de las cabeceras de los http

El procedimiento que se lleva a cabo para establecer una comunicación segura con **SSL** es el siguiente:

1. EL cliente (browser) envía un mensaje de saludo al Server "ClientHello"

2. El servidor responde con un mensaje "ServerHello"

3. El servidor envía su certificado

4. El servidor solicita el certificado del cliente

5. El cliente envía su certificado: si es válido continua la comunicación si no para o sigue la comunicación sin certificado del cliente

6. El cliente envía un mensaje "ClientKeyExchange" solicitando un intercambio de claves simétricas si es el caso

7. El cliente envía un mensaje "CertificateVerify" si se ha verificado el certificado del servidor, en caso de que el cliente este en estado de autenticado

8. Ambos, cliente y servidor envían un mensaje "ChangeCipherSpec" que significa el comienzo de la comunicación segura.

9. Al término de la comunicación ambos envían el mensaje "finished" con lo que termina la comunicación segura, este mensaje consiste en un intercambio del hash de toda la conversación, de manera que ambos están seguros que los mensajes fueron recibidos intactos (íntegros).

Por ejemplo con **SSL** solo protege el número de tarjeta cuando se envía del cliente al comerciante, sin embargo no hace nada para la validación del número de tarjeta, para chequear sí el cliente está autorizado a usar ese número de tarjeta, para ver la autorización de la transacción del banco del comerciante etc., Además que el comerciante puede fácilmente guardar el número de tarjeta del cliente. En fin todas estas debilidades son cubiertas por **SET**, éste permite dar seguridad tanto al cliente, al comerciante como al banco emisor de la tarjeta y al banco del comerciante.

El proceso de **SET** es más o menos el siguiente:

1. **El cliente inicializa la compra:** consiste en que el cliente usa el browser para seleccionar los productos a comprar y llena la forma de orden correspondiente. **SET** comienza cuando el cliente hace clic en "pagar" y se envía un mensaje de iniciar **SET**.

2. **El cliente usando SET envía la orden y la información de pago al comerciante:** el software **SET** del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.

3. **El comerciante pasa la información de pago al banco:** el software **SET** del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.

4. **El banco verifica la validez del requerimiento:** el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.

5. **El emisor de la tarjeta autoriza la transacción:** el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.

6. **El banco del comerciante autoriza la transacción:** una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.

7. **El servidor del comerciante complementa la transacción:** el servidor del comerciante da a conocer que la transacción que la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.

8. **El comerciante captura la transacción:** en la fase final de SET el comerciante envía un mensaje de "captura" a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.

9. **El generador de la tarjeta envía el aviso de crédito al cliente:** el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.

SET requiere un certificado digital en cada paso de autenticación y usa dos pares de claves, una para el cifrado del sobre digital y otra para la firma, (SSL solo usa un par de claves), actualmente SET usa la función hash, SHA-1, DES y RSA de 1024 bits, estos parámetros fueron tomados para ser compatibles con los certificados existentes, aunque el piloto de SET usó el sistema asimétrico de cifrado con curvas elípticas y se piensa que soporte también curvas elípticas en la próxima versión de SET.