C A P Í T U L O II

TÉCNICAS DE IDENTIFICACIÓN DIGITAL

2.1 Identificación y Autenticación

2.2 Mecanismos de Autenticación

2.3 Certificados de Servidores

2.4 Certificados de Clientes

2.5 Metodología de Firmas de Código

2.6 Algoritmos de Generación de Firmas Digitales

2.7 Otros Métodos de Generación de Firmas Digitales

2.1 Identificación y Autenticación

En las transacciones actuales que se realizan a través de distintos medios ya sea electrónicos o por el Internet a través de medios electrónicos es muy importante que una persona sea identificada plenamente al momento de proporcionar sus datos personales y exista la confianza y seguridad de que la persona que está del otro lado sea realmente quien dice ser, y a la vez se pueda determinar si los datos que ha proporcionado son verdaderamente los correctos.

Verificación o Autenticación implica determinar la validez de la identidad de una persona, por medio de la presentación de una muestra biométrica. La idea es poder resolver la pregunta "Soy yo quien digo ser?". La respuesta es Si o No, y en sistemas de verificación o autenticación, esta respuesta permite brindar o negar acceso a instalaciones, a información, o aceptación en cualquier otra aplicación.

La necesidad de Identificación

La principal ventaja de la identificación es que se cuenta con una herramienta con la que una persona pueda probar su identidad. Utilizada en un sinnúmero de actividades ya sea comerciales, transaccionales, de negocios, legales, etc. Es además una herramienta efectiva usada por los gobiernos para la seguridad de sus pueblos (cedulación, pasaportes, policía, impuestos, etc.) En el Internet las cosas son más complicadas y no tan limpias y transparentes, software en línea, tiendas virtuales, negocios en línea, empresas de servicios por la Red, deben tener mecanismos claros y confiables para determinar que la información de sus clientes y sus proveedores sea la correcta, de esta manera se asegurarán sobrevivir en un ciberespacio cada vez más difícil y peligroso.

Generalmente qué determina que un sistema biométrico sea de verificación o de identificación? Básicamente, el número de usuarios. No es lo mismo implementar un sistema de control de acceso en un edificio con 200 usuarios, o un control de máximo 30 estudiantes en un centro de cómputo, o el registro de tiempos de trabajo de empleados en un bar, o el restringido acceso a una bóveda de un banco, o el control de los millones de habitantes de una ciudad. Cada una de estas aplicaciones tiene una forma distinta de implementarse, y por ende, el que sea un sistema de verificación o de identificación. Por lo general, entre mayor el número de usuarios, mayor es la necesidad de manejar y controlar bases de datos y mayor es la necesidad de sistemas de identificación. [LIB 01].

2.1.1 Sistemas basados en credenciales

Es una forma probada de comprobar la identidad de una persona en el mundo físico, mediante credenciales certificadas por una autoridad confiable. Un pasaporte, una licenciad de conducir, una tarjeta de crédito, una tarjeta de membresía, comprueban la identidad de quien las presenta, para respaldar su presentación se apoyan en el nombre de un gobierno nacional, un estado, provincia, una embajada, etc. Estos tipos de credenciales son a prueba de falsificación y alteraciones, de tal manera que quien las porta no pueda modificarlas, y también para evitar que las emita alguien diferente del gobierno u organización correspondiente.

Identificaciones a prueba de alteraciones

En la actualidad en muchos países se está utilizando las técnicas de protección contra alteraciones y falsificaciones que consiste en métodos de fabricación a base de ***películas fílmicas*** con ciertos códigos y claves de seguridad imposibles de ser copiadas e imitadas. Las mismas que están protegidas por patentes y secretos comerciales. También existen

técnicas de ***holograma de seguridad*** que se utilizan en las tarjetas de crédito, discos compactos, paquetes de software.

2.1.2 Sistemas basados en computadoras

El principal problema de la identificación a través de la computadora es no tener un mecanismo adecuado para de inicio poder saber si un usuario que ingresa a trabajar es o no quien supone ser, para esto se necesitaría un programa o una aplicación que logre determinar de una manera confiable y segura la identidad de los usuarios.

Sistemas Basados en Claves de Acceso

Si una persona tiene una cuenta en un sistema determinado, para hacer uso de el requiere de una identificación que consta de ***un login y un password***, que el usuario ingresa y si es correcto el sistema asume que el usuario es quien dice ser. La desventaja que se tiene es que un usuario en especial puede ceder su contraseña o esta puede ser robada y usada para otros fines. Como son fáciles de usar, conocidas y no requieren de hardware especial, las claves de acceso siguen siendo el sistema de identificación más popular en el mundo computacional hoy en día.

Problemas con el uso de claves de acceso para la identificación.

- ✓ La computadora debe tener la clave de acceso archivada antes de intentar comprobar la identidad del usuario.
- ✓ La clave de acceso puede ser interceptada al enviarse a la computadora. Alguien que la consiga puede suplantar al usuario.
- ✓ Las personas pueden olvidar sus claves de acceso.
- ✓ Las personas eligen claves predecibles con facilidad.
- ✓ Las personas confían sus claves a otras personas. [LIB 01].

Biométrica.- Es otra técnica usada en la identificación de las personas, se trata de usar algún rasgo o una medición física de la persona y compararla con un perfil almacenado con anterioridad.

Formas de biométrica

- ✓ La imagen del rostro de una persona
- ✓ Huellas digitales
- ✓ Huellas de pie y estilos de caminar
- ✓ Forma y tamaño de la mano
- ✓ Patrón de Vasos sanguíneos en la retina
- ✓ Patrones de DNA
- ✓ Impresiones de Voz
- ✓ Técnicas de caligrafía
- ✓ Formas de teclear

Existen formas para utilizar sistemas de identificación biométrica (que se detalla en el apartado 2.2.4). [WWW 018]

2.1.3 Autenticación basada en firmas digitales.

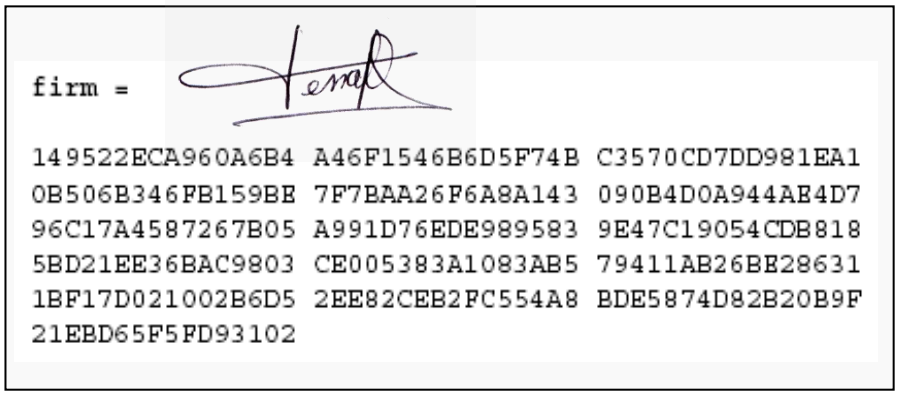


Figura 2.1 Firma Digital

La autenticación basada en firmas digitales, es un conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian a un documento electrónico (Disquete, CD, Disco Duro, o

Tarjeta Inteligente), que permite identificar a su autor. Cuando esta identificación es altamente fiable y permite detectar cualquier alteración del documento no autorizada es porque los dispositivos empleados en la creación de la firma son seguros, por cumplir ciertas exigencias técnicas, y porque el Prestador de Servicios de Certificación que ha intervenido esta "acreditado" entonces se habla de "firma electrónica avanzada".

La clave privada (secreta), generalmente se encuentra incorporada en tarjetas inteligentes de uso personal e intransferible por estar protegida por un código secreto que sólo su titular conoce, similares a las de crédito, que incorporan un chip que contiene información de su titular, la entidad que la ha emitido y el conjunto de bits en que consiste la clave.. Dentro de la categoría genérica de firma electrónica, es necesario hacer una subdivisión entre firma electrónica en general y firma electrónica segura, refrendada o firma digital. Esta distinción tiene su origen en la cifra de la firma electrónica, en la tecnología que se ha aplicado para poder calificar a la firma como segura o no. Además, tiene repercusiones posteriores, puesto que la legislación prima a las firmas digitales o firmas electrónicas seguras (a nivel nacional como internacional). La diferencia principal entre ambos tipos de firma, radica en el sistema criptográfico que se ha utilizado. Para las firmas electrónicas en general se utilizan un sistema criptográfico simétrico o de clave secreta; mientras que para la firma digital el método utilizado es asimétrico o de clave pública.

Una firma digital es una cadena de datos creada a partir de un mensaje, o parte de un mensaje, de forma que sea imposible que éste mensaje sea repudiado y que quien recibe el mensaje pueda asegurar que quién dice que lo ha enviado es realmente quien lo ha enviado, es decir, el receptor de un mensaje digital puede asegurar cual es el origen del mismo

(autenticación). Así mismo, las firmas digitales pueden garantizar la integridad de los datos, es decir que no se hayan modificado durante su transmisión. [WWW 005].

Los sistemas de clave pública permiten cumplir los requisitos de integridad del mensaje, autenticación y no repudio del remitente utilizando **firmas digitales**. El procedimiento de firma digital de un mensaje consiste en extraer un "**resumen**" (*hash*) del mensaje, cifrar este resumen con la clave privada del remitente y añadir el resumen cifrado al final del mensaje. A continuación, el mensaje más la firma (el resumen cifrado) se envía como antes cifrados con la clave pública del destinatario. Para la mayoría de los sistemas de identificación, una de las principales ventajas en el mejoramiento de identificación es usar las firmas digitales. Una ***llave privada*** que es utilizada para firmar un bloque de datos ya sea un documento de texto, un documento HTML, un mensaje de correo u otro que vaya a ser enviado a su destinatario por medio de la Web. Una ***llave pública*** que es utilizada para verificar la firma una vez puesta sobre el documento, que se generan a partir de un sistema de generación criptográfico.

2.1.4 Normas y Estándares de Certificación

2.1.4.1 ANSI X9,79

La criptografía de clave pública, forma parte de los estándares internacionales: ISO 9796 ("Organización de Estándares Internacionales"), ANSI X9. (Instituto Americano de Estándares Nacionales) y por tanto su aplicación y regulación está ligada a estos estándares. [WWW 006].

2.1.4.2 RFC 2527, ITU-T X509, X500

El RFC[15] 2527 es una especificación del *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" propuesto por S. Chokhani y W. Ford, del Internet Engineering Task Force (IETF), para todos los documentos relacionados con la Certificación Digital. RFC 2527 es parte del estándar ITU-T X.509 de la Unión Internacional de Telecomunicaciones, del Sector de Estandarización de Telecomunicaciones (que se describe en el apartado 2.2.3) que se incluyen en el conjunto de estándares X.509 de Tecnología de la Información, Interconexión de Sistemas Abiertos. [WWW 007].

Certificados y **marco de trabajo de la Certificación.**

La RFC 2527, presenta un marco que asiste a quienes escriben la política de certificación o las prácticas de certificación para las autoridades de certificación y PKI's. Se trata de establecer una clara relación entre la Política de Certificación (CP) y las Prácticas de Certificación (CPS), CP y presentar un perfil para asistir a los escritores en sus tareas. El documento identifica los elementos que deben ser considerados durante la formulación. El propósito es que no se definan CPs o CPSs particulares, para cada PSC o PKI. El rango de aplicación de este documento está limitado a la discusión de contenidos de la Política de Certificación (como se define en la *X.509)* o CPS. El documento presenta las siguientes definiciones: A) Política de certificación (Certificate Policy, CP).- Conjunto de reglas que indican la aplicabilidad de un certificado en una comunidad y/o clase de aplicación con requerimientos de seguridad comunes. B) Trayectoria o camino de certificación (Certificate path).- Es una secuencia ordenada de certificados con los cuales, en conjunto con una clave pública del objeto

[15] Request form Comment, Petición de Comentarios.

inicial en la ruta o trayectoria (path), se puede proceder a obtener el objeto final en la ruta o trayectoria (path). C) Declaración de prácticas de Certificación (Certification practice statement, CPS).- Es una declaración de las prácticas que la autoridad certificadora emplea para la emisión de certificados. D) Campos del certificado (Certificate fields).- En la *X.509*. Existen los siguientes campos para soportar las políticas de certificación:

- ✓ Políticas de certificación (Certificate Policies extension).- Esta extensión tiene dos variantes, críticas y no críticas. Firma electrónica y certificación digital.
- ✓ Mapeo de la política (Policy mappings extension).- Puede ser utilizado únicamente en los certificados de las PSC. Permite indicar si ciertas políticas en su propio dominio pueden ser consideradas equivalentes a otras políticas en el dominio de la PSC usuaria.
- ✓ Restricciones de la política (Policy Contrains Extension).- Soporta dos características opcionales. La primera habilita a la PSC para requerir de una política de certificación explícita que debe estar presente en todos los caminos de certificación subsecuentes cuando el certificado abandona el dominio de confianza. La segunda es habilitar a la PSC a desactivar el mapeo de la política, con lo cual la PSC evita que una PSC de mayor jerarquía imponga su dominio de confianza a una PSC usuaria.

E) Calificadores de Política (Policy Qualifiers).- Permite la utilización de políticas estandarizadas (o definida por parámetros), punteros a sitios donde se publican la CPS. La *X.509* no determina el propósito de este campo. Firma electrónica y certificación digital. [LIB 03].

X500.- es un estándar internacional aplicable a las diferentes Políticas de Certificación Digital, Es un estándar de servicios de directorio para

búsquedas de objetos (organizaciones, personas) en la Red. Basa su funcionamiento en el modelo de referencia OSI y consiste en una base de datos global sobre objetos tales como personas y organizaciones, similares a un directorio telefónico que abarca todo el mundo.

Debido a su gran tamaño el directorio X500, se halla distribuido a lo largo de todo el mundo en una serie de servidores llamados DSA[16] en los cuales reside la información. Normalmente los DSA contienen sólo la información de la organización a la que pertenecen, cuando es necesario consultar información sobre otras organizaciones o entidades, éstos servidores cooperan entre si para disponer de dicha información. Las máquinas que acceden a los DSA para hacer las consultas se denominan DUAs [17]. X500 consiste en un conjunto de Entradas[18] que contienen información sobre un objeto. En el caso de una persona, el nombre de una entrada normalmente es el atributo CommonName[19], pero como pueden existir en la red miles de personas con ese nombre el directorio está estructurado como un árbol, en cada nodo del árbol hay un atributo. El nombre completo del objeto está compuesto por la serie de atributos que se forman al recorrer el árbol desde la raíz hasta llegar al objeto.

En cada nivel del árbol se considera un atributo, este es:

- ✓ Pais [Country (c)]
- ✓ Organización [Organization (o)]
- ✓ Unidad organizacional [Organizational Unit (ou)]
- ✓ Nombre [CommonName (cn)]

La jerarquía, queda organizada de la siguiente forma: En el nivel más alto están los países (Country), por debajo de este las organizaciones (Organization), que constituyen entradas en el directorio y bajo éste uno o más niveles de unidades organizacionales (Organizacional Units).

[16] Directory System Agents, Agentes del Sistema de Directorio.
[17] Directory User Agents, Directorio de Agentes de Usuario
[18] Colección de atributos en el que cada uno describe un aspecto del mismo.
[19] Nombre de la Persona u Organización.

Finalmente está el nombre de la persona (cn). Cada objeto queda definido de forma única por la serie de atributos obtenidos al recorrer el árbol desde el nodo raíz hasta llegar al objeto. [WWW 010].

Ejemplo:
cn=Luis Suárez, o=Universidad Técnica del Norte, ou= Departamento de Sistemas, c=EC Esto llevado al formato de la Nomenclatura Nombre Amigable se vería:
Luis Suárez, Universidad Técnica del Norte, Departamento de Sistemas, EC

2.1.4.3 ISO/IEC 9594

Internacional Estándar Organization/Internatinal Electronic Common, es una norma estándar idéntica a ITU-T X.509 que es utilizada para brindar Servicios de Seguridad en los procedimientos de Autenticación de los usuarios. Este estándar fue publicado en Septiembre de 1995 y actualmente su estado es: Estado/Versión IS, Estándar Internacional/ Aprobado.

Campo de aplicación y alcance.- la norma 9594 especifica la forma de autenticación de la información que tiene el directorio, describiendo como obtener del mismo los datos necesarios. Define los caminos en los que las aplicaciones deben usar esta información para realizar la autenticación y describe como otros servicios de seguridad, deben de ser sostenidos por la autenticación. También describe dos niveles de autenticación; La autenticación simple que usa una contraseña como verificación de la identidad y ofrece una protección limitada contra accesos no autorizados y la autenticación fuerte que implica credenciales y usa técnicas criptográficas.

La autenticación sólo se proporciona en el contexto de un sistema definido de seguridad, por lo que debe de ser el usuario de una aplicación determinada el que ha de establecer dentro del estándar su propio sistema de seguridad. El protocolo usado por las aplicaciones para obtener credenciales del directorio es el protocolo de acceso al directorio definido en ISO/IEC 9594-5 [WWW 008]

Partes de la Norma ISO/IEC 9594

- ISO/IEC 9594-1: Overview of concepts, models and services, Conceptos de Revisión Global, Servicios y Modelos.
- ISO/IEC 9594-2: Models, Modelos
- ISO/IEC 9594-3: Abstract service definition, DEfinición de Servicio Abstracto.
- ISO/IEC 9594-4: Procedures for distributed operation, Procedimientos para Operaciones Distribuidas.
- ISO/IEC 9594-5: Protocol specifications, Especificaciones de Protocolo.
- ISO/IEC 9594-6: Selected attribute types, Tipos de Atributos Seleccionados.
- ISO/IEC 9594-7: Selected object classes, Clases de Objetos Seleccionados.
- ISO/IEC 9594-8: Authentication framework, Estructura de Autenticación
- ISO/IEC 9594-9: Replication, Replicación.
- ISO/IEC DIS 9594-10 Part 10: Use of Systems Management for Administration of the Directory, Uso de Administración de Sistemas para Administración de Directorio. [WWW 009].

2.2 Mecanismos de Autenticación

2.2.1 Infraestructura de llaves públicas

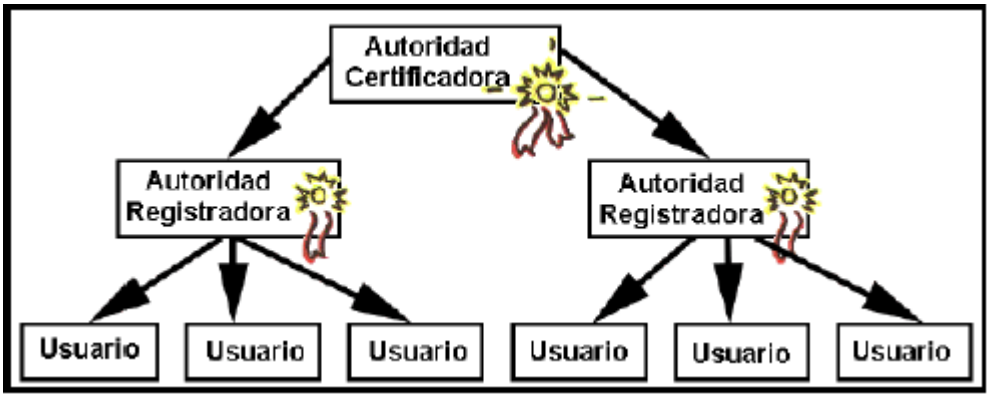


Figura 2.2 Infraestructura de Clave Pública

PKI [20] es una infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de **certificados digitales**[21]**,** es la combinación de productos de hardware y software, políticas y procedimientos tendientes a proveer un nivel adecuado de seguridad para poder realizar transacciones electrónicas a través de redes públicas, como Internet [WWW 005].

El propósito general es proveer a cada usuario de un solo par de claves (una pública y una privada) independientemente del número de usuarios con los que desee comunicarse. Estas claves tienen la propiedad de que cada una de ellas invierte la acción de la otra pero, a partir de una clave no se puede obtener la otra clave. De esta manera se define un método de cifrado que se denomina ***Cifrado de Clave Pública***,[22] La clave privada deberá ser custodiada por el usuario o a su vez por una Entidad Certificadora y es imprescindible que se mantenga en secreto. La clave pública, se publicará junto con la identidad del usuario. Así cuando se quiera enviar un mensaje seguro a un usuario se cogerá la clave pública

[20] Public Key Infraestructre, Infraestructura de Clave Pública
[21] Documento Digital que identifica a una persona en cualquier transacción electrónica.
[22] Fijamiento de una clave del usuario como pública y la otra clave como privada.

de éste y se utilizará para cifrar el mensaje que se quiera enviar. El resultado de esta operación será el texto cifrado que sólo el propietario de la clave privada correspondiente a esa clave pública podrá descifrar.

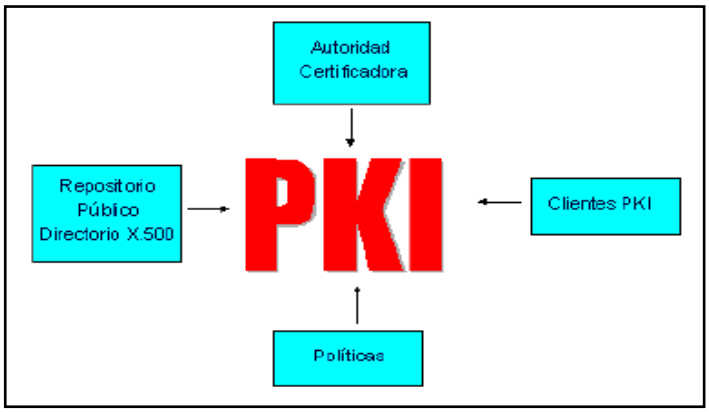


Figura 2.3 Componentes de una PKI

PKI es un sistema para verificar la autenticidad de cada interlocutor implicado en una transacción de Internet, ofrecer protección frente al fraude o al sabotaje y evitar el rechazo de las transacciones con el fin de ayudar a los consumidores a protegerse frente a la denegación de las transacciones. Organizaciones terceras, de confianza, llamadas autoridades certificadoras (AC), emiten certificados digitales que especifican componentes clave de la identidad del usuario. Durante una transacción en Internet, los mensajes cifrados y firmados se dirigen automáticamente a la autoridad de certificación, donde se verifican los certificados para que la transacción pueda continuar. La PKI puede estar incorporada en aplicaciones de software o bien ofrecerse como servicio o como producto. De acuerdo a los líderes de e-business[23], éstos están de acuerdo en que las PKI son cruciales para la seguridad y la integridad de las transacciones, y el sector del software está adoptando estándares abiertos para su uso.

[23] Negocios por Internet.

Una estructura de Clave Pública consiste en

a) Una Política de Certificación

Establece y define la dirección que debe seguir una organización respecto de la seguridad de su información considerando los procesos y principios establecidos para el uso de medios criptográficos. Incluye también documentos de cómo las personas o la organización deberán manejar sus claves a fin de establecer el nivel de control deseado de acuerdo a los riesgos existentes. Estos aspectos son agrupados en una Política de Certificación (Certification Practice Statements) **CPS,** en que se detallan los procedimientos operacionales, como el funcionamiento de la autoridad certificadora, las actividades de administración de los certificados, las características de los certificados, etc.

b) Una Autoridad Certificadora

Encargada de realizar la emisión y administración de los certificados digitales durante todo el ciclo de vida de los mismos.

c) Un sistema de administración de certificados

Establece el tratamiento que recibirán los certificados generados, desde el procedimiento de generación hasta su revocación o re-certificación (solo si estuvo suspendido) y la manera en que serán distribuidos los certificados.

d) Un conjunto de aplicaciones que hacen uso de la tecnología PKI

De manera general, la PKI establece diferentes procedimientos para:

- ✓ Emisión de certificados digitales.
- ✓ Revocación de certificados digitales.
- ✓ Consulta de certificados digitales.

2.2.2 Infraestructura de NTLM

Cuando se va a acceder a un recurso compartido en un servidor remoto, éste servidor es el encargado de autenticar al cliente quien se conecta, para luego poder autorizarlo o no, a acceder al recurso. Dependiendo del sistema operativo con el que están trabajando el cliente, y el servidor, y si se está en un grupo de trabajo o un dominio, se utilizará el protocolo más seguro que sea admitido por las partes que interactúan. Los sistemas operativos Windows 9x soportan autenticación LM (Lan Manager), Windows NT soporta LM y NTLM (NT Lan Manager), y Windows 2000 y XP soportan LM, NTLM y Kerberos[24]. [WWW 011].

Cuando un usuario envía la orden para acceder a un recurso compartido ***file://server/recurso*** se efectúan los siguientes pasos:

- ✓ Resolución de nombre a una dirección IP
- ✓ Resolución de la dirección MAC del próximo salto (ARP)
- ✓ Establecimiento de sesión TCP
- ✓ Establecimiento de sesión NetBIOS (dependiendo de los sistemas operativos que intervienen)
- ✓ Negociación SMB (Server Message Block)
- ✓ Autenticación Challenge-Response.

El mecanismo de autenticación Challenge-Response abarca la Autenticación propiamente dicha y la Negociación SMB[25]. Durante esta "negociación de dialecto" el Cliente envía la lista de dialectos que comprende, el Servidor selecciona uno que normalmente el más nuevo y devuelve esa información al Cliente, conjuntamente con esta información envía el Challenge[26], generado por el Servidor y enviado al Cliente. El Cliente conoce la contraseña del usuario y guarda en memoria protegida el resultado de pasar esta contraseña por una función establecida de Hash.

[24] Protocolo de Autenticación de usuarios en Internet
[25] Protocolo de Autenticación a nivel Capa de Aplicación usado en las Redes Microsoft.
[26] Secuencia de caracteres de longitud determinada pero que no se conoce su contenido.

Cuando recibe el Challenge, el cliente utiliza este Hash más otras funciones matemáticas para encriptar el Challenge recibido, y el resultado es enviado al Servidor. Esto es el Response[27], que incluye el nombre de usuario. El Servidor recibe el Response, lo procesa, igual que el Cliente pero en sentido inverso (para desencriptar) y con la versión local que tiene de la contraseña de ese usuario. Si el resultado de desencriptar el Response, con la versión propia de la contraseña, es igual al Challenge, entonces el usuario demostró conocer la contraseña correcta sin necesidad de enviarla.

[27] Respuesta enviada por parte del Cliente al Servidor una vez que se encripta el Challenge.

2.2.2.1 Protocolos de certificación digital

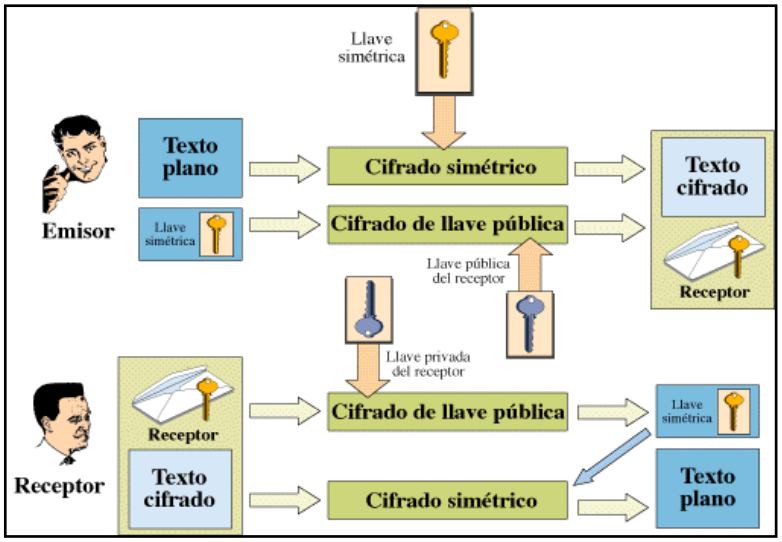


Figura 2.4 Protocolos de Certificación Digital

PEM	Protocolo encargado de proveer privacidad y autentificación para sistemas de correo basados en el RFC 822.
IPSEC	Grupo de extensiones del protocolo IP, provee servicios de comunicación segura y encriptada entre dos equipos a través de una red no segura, de un modo transparente para las aplicaciones.
SET	Protocolo de transacciones electrónicas seguras en redes abiertas, basado en la criptografía de llaves públicas y privadas RSA.
PGP	Protocolo que proporciona Autenticación y Confidencialidad tanto en el envío de mensajes por correo electrónico como en la protección de datos almacenados.
S/MIME	Protocolo de intercambio de objetos por Internet, es una extensión del estándar MIME de Internet, es un estándar "de hecho" propulsado por RSA Data Security, incorpora servicios de firmas electrónicas y de encriptamiento a MIME y se ajusta al PKCS # 7de RSA.
SHTTP	Protocolo de Transferencia de Hiper Texto Seguro, S-HTTP es una extensión sobre el estándar HTTP para la transferencia Web, su propósito es encriptar la información durante una sesión HTTP, permite cifrado y autentificación digital, incorpora cabeceras MIME para aportar confidencialidad, autenticación, integridad e irrenunciabilidad de las transacciones.
SSL	Capa de Conexiones Seguras, protocolo utilizado para establecer comunicaciones seguras, enviar información encriptada por Internet. Proporciona Autenticación, no repudio mediante firmas y certificados digitales, privacidad de la transmisión mediante codificación de los datos. Integridad de los datos entre ambos extremos de una conexión.

PEM *(Privacy Enhanced Mail)*

Es un estándar oficial de Internet el cual se describe con cuatro RFC desde el 1421 al 1424 (WWW 012), encargado de proveer privacidad y autentificación para sistemas de correo basados en el RFC 822. Sin embargo, presenta algunas diferencias en enfoque y tecnología.

Funcionamiento.- Los mensajes enviados usando PEM son inicialmente convertidos a una forma normalizada, de tal manera que tengan las mismas características sobre el uso de un espacio en blanco, tabuladores, y el uso de retornos de carro y avances de línea. Esta transformación se realiza para eliminar los efectos sobre el agente emisor que transfiere el mensaje evitando que lo modifique o presente tendencia a modificarlo. Sin la normalización, tales modificaciones podrían afectar el mensaje desde su salida hasta que llega a su destinatario. Un compendio de mensaje (hash) es calculado usando MD2 o MD5[28], y la concatenación de la función de dispersión y el mensaje son encriptados usando DES y se genera una llave de 56 bits que no es tan segura. El mensaje encriptado puede ser codificado usando Radix-64 y transmitido al recipiente.

IPSEC *(IP Security)*

IPSec es un grupo de extensiones de la familia del protocolo IP. Provee servicios de comunicación segura y encriptada entre dos equipos a través de una red no segura, similares a SSL, de un modo que es transparente para las aplicaciones y mucho más robusto. Puede crear túneles cifrados (VPNs)[29], o simple cifrado entre computadoras.

[28] Algoritmos de Encriptación para el cálculo de resúmenes de mensajes.
[29] Redes Privadas Virtuales

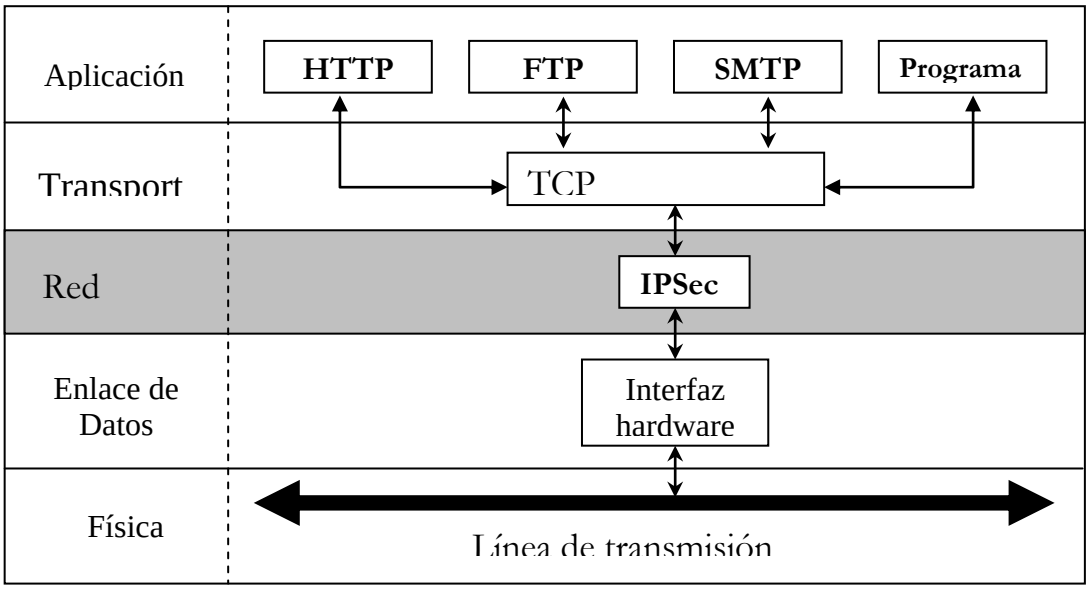


Figura 2.5 Capa IPSec [LIB 04]

Servicios:

- ✓ Confidencialidad de la transmisión a través de codificación para los datos.
- ✓ Integridad, garantiza que los datos no puedan ser cambiados en el viaje.
- ✓ Autenticidad, firma los datos de modo que otros puedan verificar quien lo envía.
- ✓ Asegura que una transacción sólo se puede llevar a cabo una vez. No permitiendo que nadie pueda grabar una transacción, y luego replicarla, como si se hubieran recibido múltiples transacciones del

IPSec provee confidencialidad, integridad, autenticidad, y protección a la réplica a través de dos nuevos protocolos:

- ✓ **Cabecera de Autenticación** (AH, "Authentication Header") que provee autenticación, integridad, y protección a la réplica, aunque no brinda confidencialidad. Contiene resúmenes hash de los datos e información de identificación de la trama.
- ✓ **Cargo de Seguridad Encapsulado** (ESP, "Encapsulated Security Payload") provee autenticación, integridad, protección a la réplica, y confidencialidad de los datos, brindando seguridad a

toda la información que sigue a la cabecera en el paquete transmitido. La cabecera del ESP permite reescribir el cargo en modo cifrado, y no considera los campos de la cabecera IP que van delante, por lo tanto no garantiza nada excepto el cargo.

Los dos protocolos, pueden ser usados en modo túnel y en modo transporte.

Modo Túnel, el paquete IP es encriptado y encapsulado en otro datagrama con nueva cabecera IP no cifrada, La dirección de destino de Internet en la añadida cabecera IP debe ser un host, pero puede ser una entrada de seguridad (security gateway), tal como un cortafuegos o un router habilitado. De esta manera, incluso si un paquete es capturado, el interceptor no leerá mucho por examinación de la dirección de destino. El interceptor no será capaz de decir cual host detrás de la entrada de seguridad (security gateway) recibirá el paquete IP.

Modo de Transporte, el paquete IP es enviado directamente al destino sin ser encapsulado. La cabecera principal IP es seguida por el ESP o la cabecera AH y por el resto del paquete IP (encriptado en el caso de ESP).

Asociaciones de Seguridad (SA)

- ✓ Una SA consta de la información que necesita una entidad IPsec para soportar un sentido del tráfico (saliente o entrante) de una conexión de un protocolo IPsec.
- ✓ El contenido de una SA varía para cada conexión, y puede incluir claves de autenticación o cifrado, algoritmos específicos, tiempos de vida de las claves, direcciones IP.
- ✓ Una SA indica a un dispositivo IPsec cómo procesar paquetes IPsec entrantes, o cómo generar paquetes IPsec salientes

- ✓ Los dispositivos IPsec insertan un campo en la cabecera de IPsec (Índice de Parámetros de Seguridad) para asociar un cierto datagrama a la SA adecuada en las máquinas que los procesen.
- ✓ Los dispositivos IPsec almacenan las SAs en una base de datos (SAD). [WWW 014].

SET (Transacción electrónica segura)

Es un protocolo estándar para transacciones electrónicas seguras en redes abiertas como Internet, desarrollado por las empresas Visa y MasterCard con la asesoría de empresas como IBM, Netscape y RSA entre otras. El protocolo está basado en la criptografía de llaves públicas y privadas RSA.

SET agrupa a las siguientes entidades en un solo sistema de pago:

- ✓ **Tarjeta habiente**: aquella persona poseedora de una tarjeta de crédito.
- ✓ **Emisor**: entidad financiera que emite la tarjeta.
- ✓ **Comerciante**: es la empresa que vende bienes o intercambia servicios por dinero.
- ✓ **Adquirente**: institución financiera que establece una cuenta con el Comerciante y procesa autorizaciones y pagos.
- ✓ **Intermediario para pago**: dispositivo operado por un adquirente o designado a un tercero para que procese los mensajes de pago, incluyendo instrucciones de pago de un tarjeta habiente.
- ✓ **Marcas**: Las instituciones financieras emiten tarjetas con marcas en ellas, para hacer publicidad a la marca y establecen ciertas reglas de uso y aceptación de sus tarjetas y proveen redes que las interconectan a las instituciones financieras.
- ✓ **Terceros**: los emisores y los adquirentes pueden asignar a terceros para el procesamiento de las transacciones.

El protocolo SET fue diseñado para lograr

- ✓ Confidencialidad de la información.
- ✓ Integridad de los datos
- ✓ Autenticación de la cuenta del tarjeta habiente
- ✓ Autenticación del comerciante
- ✓ Interoperabilidad

Funcionamiento.- Una vez todos los participantes estén registrados ante una autoridad certificadora, se inicia el proceso de transacciones seguras. Procedimiento que se indica a continuación con un ejemplo de una solicitud de compra:

- ✓ El tarjeta habiente inicia la solicitud del certificado del intermediario, luego de haber seleccionado los ítems a comprar. Para poder enviar mensajes SET, debe obtener una copia de la llave pública del intermediario de pago. El mensaje del tarjeta habiente indica qué tarjeta va a ser utilizada para la transacción.
- ✓ El comerciante asigna un identificador único a la transacción y le envía al tarjeta habiente su certificado y el certificado del intermediario de pago para la tarjeta seleccionada además del identificador de la transacción.
- ✓ El tarjeta habiente recibe la respuesta, verifica la autenticidad de los certificados. El software SET del tarjeta habiente genera la orden de compra y la información de pago y una firma doble para ambas obteniendo y concatenando los menssager digest[30] de las dos, computando el digest de la concatenación y encriptándolo utilizando su llave privada. El software SET del tarjeta habiente genera una llave aleatoria simétrica de encriptación y la utiliza para encriptar la firma doble. Luego se encripta el número de cuenta del tarjeta habiente y la llave simétrica utilizando la llave pública

[30] Funciones Hash de la orden de compra y la información de pago.

del intermediario de pago. Por último se transmite el mensaje que contiene la orden de compra y la información de pago.

- ✓ Cuando el comerciante recibe la orden, verifica la firma del tarjeta habiente utilizando su certificado y además chequea que el mensaje no haya sido alterado, haciendo uso del messager digest. El comerciante envía la información de pago al intermediario. Luego de procesar la información de la orden, el comerciante genera y firma un mensaje de respuesta en el que indica que la orden fue recibida. Si se logra autorización del pago, el comerciante envía la mercadería o presta el servicio por el que se le pagó.
- ✓ Cuando el software del tarjeta habiente recibe la respuesta del comerciante, verifica la autenticidad de éste, y muestra al usuario un mensaje de que la orden se realizó exitosamente. El tarjeta habiente puede luego averiguar el estado de su orden enviando una solicitud en un mensaje diferente, para saber si fue aprobado el pago, y cuándo le fue enviada la mercancía.

No es necesario hacer la autorización antes de enviar un mensaje al tarjeta habiente, este proceso se puede llevar a cabo después entre el comerciante y el intermediario de pago. El proceso es el siguiente:

- ✓ El software del comerciante genera y firma una solicitud de autorización, la cual incluye la cantidad a ser autorizada, el identificador de la transacción de la información de la orden y otra información sobre la transacción. La solicitud es encriptada utilizando una nueva llave simétrica generada aleatoriamente, que a su vez sé encripta utilizando la llave pública del intermediario. La solicitud de autorización y las instrucciones de pago son enviadas al intermediario. Cuando el intermediario de pago recibe la

solicitud, desencripta y hace las verificaciones necesarias tanto del comerciante como del tarjeta habiente, también se verifica que el identificador de la transacción sea el mismo para el tarjeta habiente y para el comerciante. El intermediario entonces formatea y envía la solicitud de autorización al emisor de la tarjeta. Luego de recibir una respuesta, el intermediario firma y envía la respuesta al comerciante. Esta respuesta incluye la respuesta del emisor y una copia del certificado del emisor, opcionalmente puede haber un token de captura que el intermediario puede necesitar para procesar una solicitud de captura. Este token solo es necesario si es requerido por el adquirente. El comerciante recibe la respuesta del intermediario, desencripta y hace las verificaciones. Almacena la respuesta de autorización y captura el token que será utilizado a través de una solicitud de captura. El comerciante entonces puede proceder a enviar las mercancías o prestar el servicio.

Luego de procesar la orden de un tarjeta habiente, el comerciante solicitará que se le pague, habrá un lapso de tiempo significativo entre la solicitud de autorización y la solicitud de pago. El proceso es el siguiente:

- ✓ El software del comerciante genera y firma una solicitud de pago que incluye la cantidad final de la transacción, el identificador de la misma y otra información adicional. Nuevamente se genera una llave simétrica aleatoria, que se encripta con la llave pública del intermediario de pago. Se envía al intermediario la solicitud de captura y opcionalmente el token de captura si esté venía en la respuesta de autorización. Varias solicitudes de captura pueden ser enviadas en un mismo mensaje para su procesamiento por lotes.

- ✓ El intermediario de pago verifica la autenticidad e integridad del mensaje que le llega y utiliza esta información para hacer una solicitud de pago al emisor a través de un sistema de pago. Cuando llegue la respuesta el intermediario firma y encripta el mensaje y se le envía la respuesta al comerciante.
- ✓ El comerciante almacena la respuesta para hacer balance con el pago recibido del adquirente.

PGP *(Pretty Good Privacy)*

Privacidad Bastante Buena, es un protocolo que proporciona Autenticación y Confidencialidad tanto en el envío de mensajes por correo electrónico como en la protección de datos almacenados. En su especificación estándar, PGP incorpora los algoritmos CAST y triple-DES para el encriptamiento de mensajes, RSA y DSA para firmas electrónicas y MD5, RIPEMD-160, y SHA-1 para el cálculo de compendios de mensajes. La compatibilidad con el correo-e se hace mediante una conversión de tipo Radix-64.

Creado a inicios de 1991 por Phill Zimmerman, PGP cubre el hueco existente en la seguridad del usuario normal en el intercambio de correo electrónico. PGP usa algoritmos simétricos y de clave pública, introduce de **anillo de llaves** un fichero ideado para ir guardando las claves públicas de los demás, lo que le ha hecho tener cierta aceptación para ciertas aplicaciones. Actualmente es Estándar Internacional con numerosos productos en varios campos.

Firma digital y confianza

PGP incluye un servicio de firma digital basada en el algoritmo de autentificación DSA. Tiene métodos para proteger de ataques de intermediario, a los que todo algoritmo de clave pública está expuesto.

PGP permite a un usuario de confianza firmar claves, para que así podamos confiar en la autenticidad de la clave y saber que ésta no es falsa.

Funcionamiento

Cuando se desea mandar un correo o fichero encriptado, PGP lo encripta usando un sistema simétrico, generalmente IDEA o DES que son más rápidos, usando un método pseudo aleatorio muy seguro, que posteriormente se encripta con RSA. Se envían el documento cifrado con la clave aleatoria y ésta encriptada con la llave RSA privada del destinatario. El mensaje cifrado será una secuencia de caracteres ASCII que puede ser manipulada en un editor de texto o enviada por correo electrónico. Cuando el destinatario recibe el correo y desea desencriptarlo, su programa PGP primero descifra la clave simétrica con su llave privada RSA, y luego descifra el documento usando la clave desencriptada. El proceso se ilustra en la siguiente figura.

Normalmente el sistema PGP viene implementado mediante alguna aplicación específica, que se instala en el computador del usuario. Esta aplicación se integra perfectamente con los programas de correo más comunes, permitiendo al usuario su uso directo.

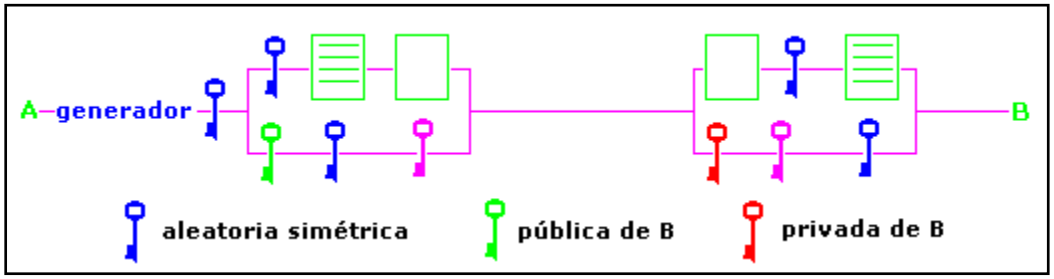


Figura 2.6 Proceso de envío de un correo electrónico en PGP

En el caso de querer enviar un e-mail encriptado a otra persona, es necesario en primer lugar que la misma tenga un programa PGP instalado, y después que se tenga la llave pública del destinatario. Si existe

la necesidad de cifrar mensajes para muchos destinatarios diferentes se debe gestionar los distintos ficheros de llave pública. Para ello, PGP facilita un **llavero**[31]. Cuando el usuario recibe uno de ellos, solo deberá colocarlo en el llavero para tenerlo disponible siempre que desee. PGP dispone de diferentes servidores que poseen bases de datos con las claves públicas de los usuarios de PGP en caso de que un usuario reciba un mensaje de una persona de la cual no conoce su clave pública. Basta acudir a los mismos y solicitar el fichero de clave correspondiente a la persona que nos interesa. [WWW 014].

S/MIME (Secure / Multipurpose Internet Mail Extensión)

Extensiones Seguras Multipropósito de Correo en Internet, es un protocolo de intercambio de objetos por Internet. Cada objeto especifica tanto su semántica como el medio de codificación utilizado. S/MIME fue desarrollado por RSA Data Security, Inc. Se establece en el formato X.509V.3 para los certificados y en el formato ASN.1 DER para datos. S/MIME es una extensión del estándar MIME de Internet, es un estándar "de hecho" propulsado por RSA Data Security. Además, de las partes convencionales de los mensajes electrónicos (encabezado y cuerpo), el formato MIME permite estructurar al cuerpo de un mensaje para incluir archivos no meramente de texto. S/MIME incorpora servicios de firmas electrónicas y de encriptamiento a MIME y se ajusta al PKCS de RSA #7.

S/MIME utiliza dos procedimientos para firmas digitales

- ✓ El "firmado limpio" (clear signed) cuando se interactúa con clientes que no son S/MIME, ya que la firma se coloca como un anexo-MIME, codificado en Base64 llamado "smime.p7s", fuera

[31] Modulo que se encarga de gestionar y administrar los distintos ficheros de Llave Pública.

del texto (abierto) del mensaje. Sin embargo, algunos "gateways" de correo-e pueden recodificar los anexos MIME alterando en consecuencia el contenido del mensaje.

- ✓ El "firmado opaco" (opaque signing) busca evitar los problemas del formateo en tránsito que realizan algunos "gateway". Un mensaje se codifica a la MIME, en Base-64, en un solo anexo. El problema es que el mensaje será ilegible para usuarios que no utilicen S/MIME.

Las partes del protocolo son:

S/MIME Versión 2 Message Specification (RFC 2311)

S/MIME Version 2 Certificate Handling (RFC 2312)

PKCS #1: RSA Encryption Version 1.5 (RFC 2313)

PKCS #10: Certification Request Syntax Version 1.5 (RFC 2314)

PKCS #7: Cryptographic Message Syntax Version 1.5 (RFC 2315)

Description of the RC2 Encryption Algorithm (RFC 2268)

Estos RFC's, tienen el carácter de informativos. S/MIME V.2 no es un estándar del IETF. S/MIME requiere el uso de una llave de intercambio RSA, lo que es gravado por las patentes americanas influenciado por RSA Data Security, Inc. lo que favorece que la versión 2 de S/MIME requiera el uso de criptografía débil (llaves de bits).

Algunos productos basados en S/MIME son:

Microsoft's Outlook Express (es parte del Internet Explorer 4.1).

Netscape's Messenger (Communicator 4.4)

OpenSoft Corp. ExpressMail 2.5 es un "cliente" para correo de Internet.

Baltimore Technologies' MailSecure

Worldtalk Corp.'s WorldSecure Client 2.2

S-HTTP *(Secure-Hiper Text Transfer Protocol)*

Protocolo de Transferencia de Hiper Texto Seguro, Desarrollado por IIT (Interprise Integration Technologies), constituye una ampliación del protocolo básico HTTP (Hypertext Transfer Protocol).

S-HTTP es una extensión sobre el estándar HTTP para la transferencia Web, su propósito es encriptar la información durante una sesión HTTP. Permite tanto el cifrado como la autentificación digital, S-HTTP es un protocolo de nivel de aplicación, es decir, extiende el protocolo HTTP por debajo, incorporando cabeceras MIME para aportar confidencialidad, autenticación, integridad e irrenunciabilidad de las transacciones.

S-HTTP soporta una gran variedad de mecanismos de seguridad para los clientes y servidores de HTTP, ofreciendo las opciones de servicios de seguridad apropiados para los usos finales del Internet. Es compatible con HTTP, por lo que un cliente que utilice S-HTTP puede acceder a un servidor que utilice HTTP, y un servidor que utilice HTTP puede servir a clientes que no lo utilicen. S-HTTP soporta transacciones seguras extremo a extremo por lo que no es necesaria la utilización de claves públicas. Ofrece una gran flexibilidad a la hora de utilizar algoritmos, modos y parámetros criptográficos; el servidor y el cliente deben negociar dichas características.

S-HTTP permite controlar el tiempo de validez de los mensajes, mediante mecanismos de preguntas-respuestas e introducción de la fecha-hora en la cabecera. Los mensajes se pueden proteger mediante firma digital, autenticación y cifrado, o cualquier combinación de las tres. Tanto el Servidor como el cliente deben ponerse de acuerdo sobre los requerimientos y preferencias en los elementos criptográficos que se van

a utilizar. A continuación se describen algunos de los parámetros que se pueden negociar:

- ✓ Tipos de certificados de clave pública que se aceptarán. Actualmente, el único tipo permitido es X.509 en todas sus versiones.
- ✓ Tipos de algoritmos que se podrán utilizar para el intercambio de claves. Actualmente, se permiten "RSA", "Outband", "Inband" y Kerberos.
- ✓ Tipos de algoritmos de firma digital. Los valores permitidos son "RSA", y "NIST-DSS".
- ✓ Tipos de algoritmos de cálculo de un código hash (resumen). Los valores permitidos son "RSA-MD2", "RSA-MD5" y "NIST-SHS".
- ✓ Tipos de algoritmos de cifrado simétrico para cifrar el mensaje. Los valores definidos son "DES-CBC", "IDEA-CFB", "RC4".

S-HTTP tiene algunas ventajas como: su flexibilidad y su integración dentro de HTML. Entre sus debilidades se puede mencionar los efectos derivados de mantener la compatibilidad hacia atrás y la necesidad de implementar servidores que soporten las extensiones a HTML aportadas por el protocolo S-HTTP.

2.2.2.2 SSL (Secure Socket Layer)

Capa de Conexiones Seguras, SSL es un protocolo de propósito general utilizado para establecer comunicaciones seguras, enviar información encriptada por Internet. Fue creado por Netscape Communications Corporation en 1994, su función principal es operar como una capa adicional entre el protocolo TCP/IP nativo y la Capa De Aplicación en el modelo de referencia OSI.[32] [LIB 02].

[32] Open System Interconection, Sistema de Interconexión Abierto.

Características

- ✓ Autenticación y no repudiación del cliente y del servidor mediante firmas y certificados digitales.
- ✓ Privacidad de la transmisión mediante codificación de los datos.
- ✓ Integridad de los datos entre ambos extremos de una conexión.
- ✓ SSL opera en la capa de transporte de TCP/IP un nivel debajo de los protocolos específicos de aplicación tales como NTTP (News), HTTP(Web) y SMTP (e-mail).
- ✓ Flexibilidad con respecto a escoger el algoritmo de encriptamiento Simétrico, la función de verificación de mensaje y el método de autenticación.
- ✓ Usa cualquier DES, Triple DES, RS2 ó RS4, para la encripción simétrica.
- ✓ Usa MD5 ó SHA como algoritmos de hashing, para la verificación de mensajes.
- ✓ Usa llaves posibles y Certificados RSA, para Autenticación ó operar en modo anónimo en donde el intercambio de llaves de Diffie-Hellman es usado.
- ✓ Dispone de una variedad de longitudes de llaves para los algoritmos de encriptamiento incluidas las longitudes truncadas usadas para las versiones de software de SSL de exportación (de Estados Unidos).
- ✓ SSL requiere un protocolo confiable de transporte (como TCP) para la transmisión y recepción de los datos.

Cuando una conexión SSL se establece todas las conexiones entre el servidor y el navegador están encriptadas, incluyendo:

- ✓ El URL del documento Pedido
- ✓ El contenido del documento pedido
- ✓ El contenido de cualquier campo de una forma
- ✓ Las Cookies enviadas del Navegador al Server
- ✓ Las Cookies enviadas del Servidor al Navegador
- ✓ El Contenido del Headder de HHTP [LIB 01].

SSL tiene dos capas

- ✓ *SSL Record Protocol*, que es una capa de más bajo nivel y se encarga de encapsular los protocolos de nivel más alto.

- ✓ *SSL Handshake Protocol*, que se encarga de la negociación de los algoritmos de encriptación, así como la autentificación entre el cliente y el servidor.

SSL RECORD PROTOCOL.- Una vez establecido un canal de transmisión seguro, se puede dar el intercambio de datos. Cuando el

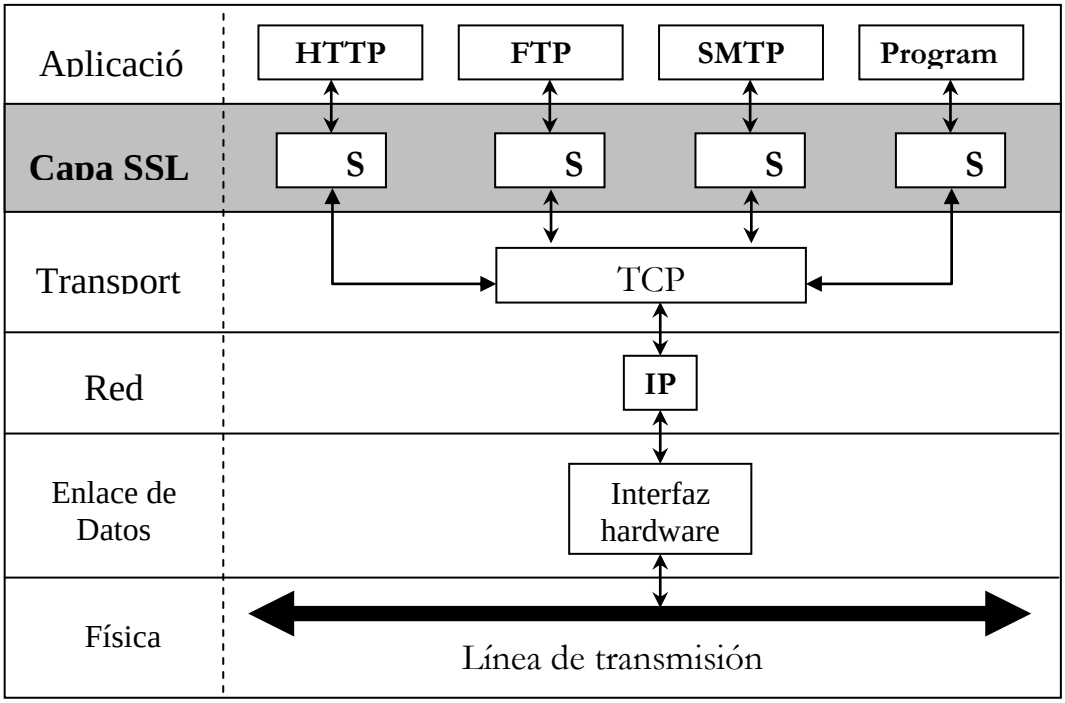


Figura 2.7 Capa SSL

servidor o el cliente desea enviar un mensaje al otro, se genera un Digest33, mensaje y Digest son encriptados, verificados mediante del Digest y son enviados. Cualquier usuario que utilice un navegador de Internet que soporte SSL, puede establecer con facilidad una conexión segura con solo crear una conexión encriptada con el servidor remplazando "http" del URL por "https".

[33] Resumen del mensaje para comprobar la integridad, utilizando un algoritmo de hash de una vía acordado durante el Handshake

SSL HANDSHAKE PROTOCOL

El objetivo del protocolo es autenticar al servidor y opcionalmente, al cliente, terminando con una llave secreta simétrica que tanto el cliente como el servidor pueden usar para enviar mensajes encriptados.

Los pasos del proceso son:

- ✓ El cliente abre una conexión al puerto del servidor y envía un mensaje "ClientHello", que lista las capacidades del cliente, incluyendo la versión de SSL que tiene, los ***cipher suites***[34] que soporta, y los métodos que compresión que tiene.
- ✓ El servidor responde con un mensaje "ServerHello", que contiene los cipher suites y compresión de datos que a escogido, así como un ID de sesión que identifica a la conexión. El servidor es el responsable de escoger el cipher suite y métodos de compresión. Si no hay coincidencias entre los cipher suites soportados entre cliente y servidor, entonces el servidor envía un mensaje de "handshake failure" (falla de conexión) y termina la conexión
- ✓ El servidor envía sus certificados. Si está usando autenticación basada en certificados (casi siempre), envía su certificado de sitio X.509v3 firmado. Si el certificado esta firmado por una autoridad non-root, el servidor también envía la cadena de certificados firmados que llegan hasta una Autoridad de Certificación primario.
- ✓ El servidor envía al cliente una solicitud de certificado (opcional). Si el certificado de los clientes están siendo usados para autenticación de clientes, el servidor le envía al cliente un mensaje de solicitud de certificado.

[34] Combinación de los Algoritmos de Encriptamiento Simétrico, métodos de verificación de mensajes y autenticación.

- ✓ El cliente envía su certificado (opcional). Si el servidor lo ha pedido, el cliente envía su certificado X.509v3 firmado, si no lo tiene, envía una alerta de "no certificate". El servidor puede decidir abortar en este punto con una falla de conversación (handshake), o continuar adelante.
- ✓ El cliente envía un mensaje "ClientKeyExchange". Aquí es donde la llave de sesión simétrica es escogida. Los detalles varían dependiendo del cipher suite escogido, pero en el caso más típico, el cliente genera un secreto "pre-master" usando un generador de números random. Este secreto será usado tanto del lado del cliente como del servidor para generar el verdadero secreto que es usado como la llave de la sesión. El navegador cifra el secreto usando la llave publica RSA del servidor (que la obtuvo del certificado del servidor) para crear un sobre digital. El sobre es enviado al servidor.
- ✓ El cliente envía un mensaje de "CertificateVerify" (Verificación de Certificado) (opcional). Si se esta usando autenticación del cliente, éste se tiene que autenticar con el servidor mostrando que el conoce la llave privada de RSA correcta. El mensaje "CertificateVerify" consiste en el secreto pre-master, que ha sido manipulado en varias formas para que sea mas difícil de verlo si alguien esta escuchando la conversación. El secreto es firmado con la llave secreta RSA del cliente y enviada al servidor, que procede a validarla chocándola contra el certificado del cliente. El servidor no tiene que probar su identidad, puesto que el cliente envía el secreto pre-master al servidor usando la llave pública del servidor, solo el legítimo poseedor del certificado del servidor podrá descifrarlo y usarlo.

- ✓ El cliente y el servidor envían el mensaje "ChangeCipherSpec" (Confirmación de Intercambio de mensajes). Este es un mensaje que confirma que tanto el cliente con el servidor están listos para empezar la comunicación usando la llave y cifrado acordado.
- ✓ El cliente y el servidor envían el mensaje "finished" (terminar). Este mensaje consiste en el hash de MD5 y SHA de toda la conversación hasta este punto y permite a las partes confirmar que los mensajes fueron recibidos intactos y no fueron modificados en el camino.

Versiones de SSL.

- ✓ **SSL-1**.- usando internamente en el Netscape tiene serios errores y nunca fue liberado.
- ✓ **SSL-2**.- fue incorporado al Netscape Navigator versión 1.0 al 2.x. La versión 2.0 tenía algunas debilidades relacionadas con ataques del hombre en el medio. Hubo un episodio embarazoso en donde 2 estudiantes de la universidad rompieron la implementación SSL V2.0 en minutos explotando un error en el generador de números randómicos en el Netscape.
- ✓ **SSL**-3.- es la última versión que está disponible actualmente.

TLS *(Transport Layer Security)*

Es otra de las extensiones de SSL conocida como Seguridad en la Capa de Transporte (TLS). TLS basa su estructura en la especificación del Protocolo SSL 3.0, publicada por Netscape. SSL se envió como un borrador al Cuerpo de Ingenieros de Internet (Internet Engineering Task Force IETF) y se convirtió en el estándar RFC 2246 (Transport Layer Security TLS 1.0). Los dos protocolos se diseñaron para proporcionar

integridad y privacidad de datos entre dos aplicaciones que se comunican.

Capas de TLS

- ✓ ***Record Protocol de TLS***, el cual se dedica a codificar y decodificar los mensajes que se trasmiten y reciben.
- ✓ ***HandShake Protocol de TLS*** es un conjunto de subprotocolos que se usan para permitir a las partes de la comunicación estar de acuerdo respecto a los parámetros de seguridad, autenticación y condiciones de informes de error.

2.2.2.3 PKCS #7

Es uno de los estándares criptográficios utilizados por el protocolo SSL y los certificados X.509, **PKCS (Public Key CryptoSystem),** de los Laboratorios RSA, y uno de los protocolos más extendidos dentro de la seguridad. Consisten en un conjunto de documentos con especificaciones sobre Seguridad cuyo alcance es la Infraestructura de Clave Pública y La Criptografía. Entre las especificaciones que se incluyen en la PKCS #7, tiene que ver con definir una sintaxis genérica para mensajes que incluyan mejoras criptográficas, tales como firma digital y/o cifrada.

Los documentos de la serie PKCS fueron publicadas por primera vez en 1991 y son ampliamente referenciados e implementados. Las contribuciones de la serie de PKCS forman parte de muchos estándares formales y de facto, incluyendo los documentos del ANSI X9, PKIX, SET, S/MIME, y SSL. Su alcance es la Infraestructura de Clave Pública y criptografía. [WWW 001], [WWW 015].

2.2.2.4 PKCS #10

PKCS #10 Certification Request Syntax Standard, es otro de los estándares más utilizados, describe la sintaxis para un requerimiento de certificación de una clave pública, de un nombre, y posiblemente de un conjunto de atributos. (RFC 2314) [WWW 001], [WWW 016].

2.2.3 Infraestructura de llave pública PKI (X.509)

X.509 es un estándar internacional para Certificados Digitales de Llaves Públicas publicado en 1993 por la Unión Internacional de Telecomunicaciones (ITU), que es utilizado por la mayoría de protocolos criptográficos existentes actualmente, y viene incluido en la mayoría de navegadores de Internet de Microsoft y Netscape, que sirve para dar información acerca del formato y contenido de los Certificados Digitales. X.509 establece en detalle la estructura de información que contendrán los certificados digitales y su formato.

El X509 aporta los aspectos seguros y especifica las estructuras de datos para las claves seguras y las listas de rechazo, así como las metodologías para manipular y certificar los certificados a nivel del sistema usando las Autoridades de Certificación (AC).

Los elementos de información importantes en las transacciones no son las claves criptográficas sino los certificados X509 por los que se transmiten estas claves públicas y las listas de certificados rechazables aplicadas cuando los certificados ya no son válidos. Generalmente los certificados suelen estar almacenados en formato PEM (Privacy Enhanced Mail), que es la codificación DER en base 64 con cabecera y cola añadidos. La definición de la estructura en notación ASN.1 (*Abstract Syntax Notation One*) es la siguiente:

```
Certificate ::= SEQUENCE {
    tbsCertificate            TBSCertificate,
    signatureAlgorithm        AlgorithmIdentifier,
    signature                 BIT STRING }

TBSCertificate ::= SEQUENCE {
    version [0]               Version DEFAULT v1,
    serialNumber              CertificateSerialNumber,
    signature                 AlgorithmIdentifier,
    issuer                    Name,
    validity                  Validity,
    subject                   Name,
    subjectPublicKeyInfo      SubjectPublicKeyInfo,
    issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,
                      -- If present, version must be v2 or v3
    subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
                      -- If present, version must be v2 or v3
    extensions [3]            Extensions OPTIONAL
                      -- If present, version must be v3 }  [LIB 01].
```

La semántica de sus campos es la siguiente

- ✓ **Versión.-** Indica si la versión del certificado X.509 es la 1, 2, ó 3.
- ✓ **Número de serie.-** Es un entero asignado por la AC emisora y que identifica unívocamente al certificado dentro del conjunto de certificados emitidos por ésta AC.
- ✓ **Firma.-** Identifica al algoritmo utilizado por la AC para firmar el certificado.
- ✓ **Emisor.-** El nombre del emisor identifica a la entidad que ha firmado el certificado y sigue la nomenclatura de nombres distinguibles (DNs, *Distinguished Names*) de X.500.

- ✓ **Validez.-** Indica el intervalo de tiempo durante el cual el certificado es válido.
- ✓ **Usuario o sujeto.-** Es un nombre distinguible X.500 que identifica de forma unívoca al poseedor o dueño del certificado.
- ✓ **Información de clave pública del usuario.-** Contiene la clave pública del usuario junto con el identificador del algoritmo con el que se ha de utilizar.
- ✓ **Identificadores únicos de emisor y de usuario.**- Es una cadena de bits opcional que identifica al emisor o al usuario en el caso de que su DN sea reutilizado con el paso del tiempo.
- ✓ **Campos de extensión.-** Permiten adicionar nuevos campos a la estructura sin tener que modificar la definición ASN.1 del certificado.

Cada uno de estos campos consiste en:

a) Un identificador de extensión.

b) Un valor que indica si es o no crítico, y

c) Una codificación canónica de un valor de un tipo ASN.1 asociado con la extensión identificada. [WWW 021].

Extensiones estándares

Las organizaciones ISO/IEC, ITU y ANSI han definido un conjunto de extensiones estándares para ser utilizadas en los certificados X.509v3, las cuales proporcionan métodos para asociar atributos adicionales con usuarios o claves públicas y para gestionar la jerarquía de certificación y la distribución de Listas de Revocación de Certificados (CRL). Las Autoridades de Certificación, tienen la capacidad para definir como críticas o no críticas las extensiones: *Key usage, Certificate policies, Subject alternative names, Issuer alternative names, Basic constraints, Name constraints y Policy constraints*; todas las demás son siempre no críticas. Las extensiones

estándares pueden dividirse en varios grupos según el aspecto con el que están relacionadas:

Información de claves y políticas.- Estas extensiones facilitan la implementación de las infraestructuras de clave pública y permiten limitar los fines con los que los certificados y las correspondientes claves públicas pueden ser utilizados.

Dentro de este grupo se encuentran:

- ***Authority key identifier.***- Proporciona un medio de identificar una determinada clave usada para firmar un certificado.
- ***Subject key identifier.***- Permite identificar una determinada clave pública utilizada en una aplicación.
- ***Key usage.-*** Indica para qué se ha utilizado la clave en cuestión: firma digital, servicio de no repudio, etc.
- ***Private key usage period.-*** Especifica el periodo de validez de la clave privada asociada al certificado de firma digital.
- ***Certificate policies.-*** Incluye información acerca de la política que gobierna el uso del certificado.
- ***Policy mappings.-*** sólo puede ser empleado en certificados de ACs, permite al emisor indicar que una de sus políticas es equivalente a otra empleada en el dominio de la AC poseedora del certificado en cuestión.

Atributos de emisor y usuario.- Proporcionan medios alternativos para identificar a los emisores o usuarios y también incluyen información adicional sobre el sujeto para facilitar que los usuarios del certificado consideren al sujeto confiable. Dentro de este grupo s encuentran:

- ✓ ***Subject alternative name.-*** Contiene uno o varios nombres alternativos para identificar al sujeto.
- ✓ ***Issuer alternative name.-*** Proporciona nombres alternativos para identificar al emisor del certificado o de la CRL.
- ✓ ***Subject directory attributes.-*** Puede contener cualquier atributo X.500 del sujeto del certificado y proporciona un medio para incluir información adicional a la incluida en los campos de nombre y que puede ser útil para identificar al sujeto.

Requisitos de caminos de certificación.- Estos campos permiten a las diferentes entidades de la jerarquía poder enlazar sus estructuras.

Dentro de este grupo se encuentran:

- ✓ ***Basic constraints.-*** Indica si el sujeto puede actuar como una AC o es sólo una entidad final.
- ✓ ***Name constraints.-*** Este campo, que sólo puede incluirse en certificados de ACs, restringe el campo de nombres válidos en los subsecuentes certificados emitidos por la AC asociada.
- ✓ ***Policy constraints.-*** Esta extensión puede ser utilizada por las ACs para especificar requisitos que pueden necesitar la identificación explícita de políticas de certificación o inhabilitar el mapeo de políticas para el resto del camino de certificación. [WWW 017].

2.2.4 Biométrica

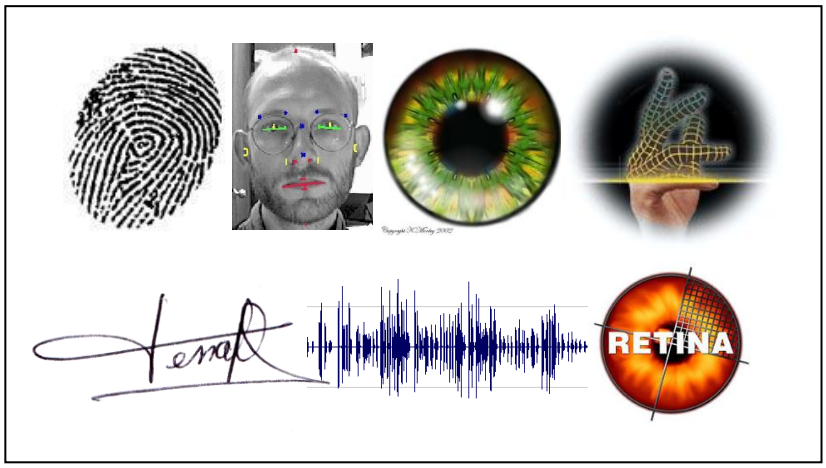


Figura 2.8 Formas Biométricas

Huella Digital	Método de identificación muy sencillo y seguro, utilizado para identificación de las personas, no representa ningún daño para las personas. Es un método que no tiene costos grandes.
Reconocimiento Facial	Método que usa para la identificación ciertas características de la cara tomadas con una cámara digital que no tienen variación en el tiempo. Es un método muy costoso.
Análisis del Iris	Método que se basa en obtener una extracción fotográfica del ojo y analizar su iris, único para cada persona.
Geometría de la Mano	Método de reconocimiento a través de rasgos característicos de la mano, se basa en algoritmos que proporcionan dichos rasgos.
Análisis de Firma	Es el método más seguro de reconocimiento y que no es rechazado por ninguna persona, el más idóneo para el reconocimiento de las personas.
Análisis de Retina	Método que se diferencia del análisis de iris por los métodos de extracción de los rasgos.

La Biometría es la ciencia dedicada a utilizar tecnología digital para determinar o verificar la identidad de personas, basada en rasgos físicos o biológicos de las personas que se puede obtener directamente de alguna parte del cuerpo humano, como la huella digital, la palma de la mano, el rostro, o patrones de iris. El objetivo de la autenticación por biometría es poder conseguir que las máquinas puedan realizar las operaciones de verificación de identidad que nosotros como humanos realizamos sin

darnos cuenta. Un sistema biométrico debe enfocarse y centrarse en la utilización de rasgos que sean distintos en todas las personas y que no tengan mucho cambio a lo largo del tiempo. Es decir, que el envejecimiento o los cambios de masa corporal no afecten el rasgo biométrico con el cual se determina la identidad.

Tecnologías Biométricas

Huella Digital.- Método de identificación y autenticación biométrica más usada, debido a su sencillez, y a la seguridad que presenta, no representa ningún daño posible por lo que es aceptado por la totalidad de las personas. La huella digital no se presta para imitaciones pues no existen dos huellas digitales iguales, gracias a la complejidad de puntos y crestas únicas en la huella.

Una huella digital es un conjunto de concavidades y convexidades en forma de arcos, líneas y espirales. El punto donde se interrumpe el continuo recorrido de una línea se le denomina "minutiae". Estos puntos son los responsables de que una huella sea única ya que la estructura y localización de éstos es completamente diferente entre una y otra huella.

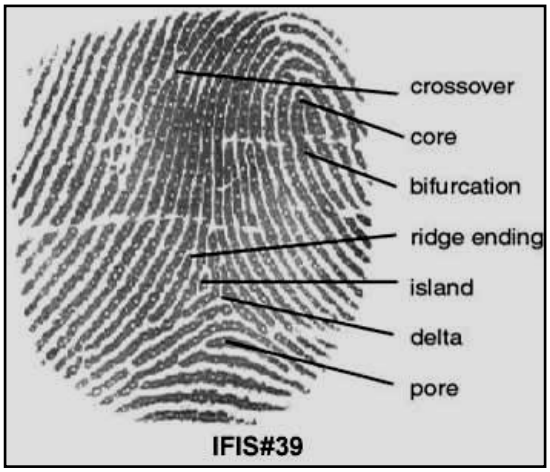
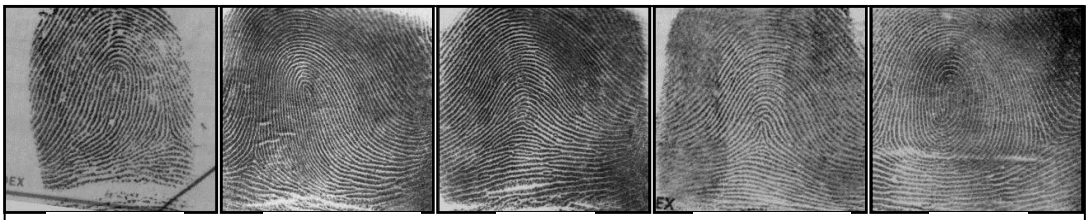


Figura 2.9 Estructura de la Huella Digital Humana

El minutiae más importante en una huella dactilar es el "core" o núcleo, es allí de donde comienzan a envolverse las demás líneas. Toda huella tiene un core. Un "crossover" representa la intersección de dos líneas formando una X. "Bifurcation" es una bifurcación del recorrido de una línea en dos, o la reunión de dos líneas en una sola, dependiendo del sentido del recorrido. "Ridge Ending" determina el fin del recorrido de una línea. "Island" es una línea pequeña pero más grande que un punto, que se encuentra solitaria y rodeada de otras líneas. "Delta" implica un sector donde el recorrido de las líneas visualiza un triángulo. Este tipo de minutiae es muy común y por lo general se encuentran en la parte inferior izquierda o derecha de muchas huellas dactilares. Un "pore" es un pequeño puntito característico, sobre una línea. Así como estos minutiae, existen muchos otros como "dots" los cuales son minutiae demasiado pequeñas para ser líneas, "ponds" o lagos que son sectores sin marcas entre dos líneas divergentes, "spurs" que como las espuelas son ramas que sobresalen al recorrido normal, como un intento de bifurcación, "bridges" o puentes entre dos grandes líneas, entre otros.

También existen clasificaciones del tipo de huella, como "left loop" que son huellas que se envuelven desde la izquierda, "right loop" que se envuelven desde la derecha, "arch" que tienen una forma de arco o montaña, "tented arch" que son arcos mucho más pronunciados, y "whorl" que presentan una forma de espiral hacia el core o centro.



Vista Izq.	Vista Der.	Arco	Montaña	Espir

Figura 2.10 Tipos de Huellas

El objetivo de la biometría es poder generar una representación computacional única y especial para cada huella dactilar., por esto la imagen obtenida pasa por un proceso de mejora y se le aplica un algoritmo, para generar así una identificación numérica única. De esta manera, se reduce el tamaño de un registro y se aumenta el número de usuarios que se pueden manipular. Lo que hace un algoritmo es buscar y extraer la minutiae o puntos característicos de la huella procesada, y el resultado de esto se denomina un "template", luego se guarda su "template" en una base de datos, o en alguna tarjeta.

Existen diferentes métodos para adquirir la imagen de la huella.

a) ***La tecnología óptica***.- consiste en iluminar la superficie de la huella y obtener la imagen, en donde se pueden distinguir crestas oscuras y valles claros. Esta es una lectura común como la que ofrece cualquier scanner de uso personal o de oficina.
b) ***La tecnología de silicona***.- un sensor hace el papel de un extremo de una capacitancia, y el dedo hace el papel del otro extremo. Se registra el valor de la capacitancia entre el dedo y el sensor y se convierte en una imagen digital en escala de grises, que ofrece más precisión que las obtenidas por sensores ópticos.
c) ***El ultrasonido.-*** transmite ondas de sonido y mide las distancias, por medio de la impedancia del dedo, el sensor y el aire. Los problemas que pueden existir con la huella digital, son: dedos fríos, alta o baja humedad, ángulo de localización del dedo en el sensor, la presión con que se coloca el dedo, cortadas en los dedos y actividades manuales que pueden afectar las huellas. [LIB 01].

Reconocimiento Facial

Esta tecnología utiliza características especiales de la cara que no tengan mucha variación en el tiempo. Gracias a esto, los cambios de peinados, o los bigotes y la barba no son un problema para la identificación. Existen dos tecnologías para la extracción de los rasgos faciales son:

- ✓ **El video estándar.-** captura una o varias imágenes que se mapean y registran los puntos claves de la cara, como la nariz, los ojos, la boca, etc, esto depende del algoritmo específico de cada empresa.
- ✓ **Las imágenes térmicas.-** analizan el calor causado por el flujo de sangre debajo de la piel de la cara. Esta tecnología no depende de la iluminación en el momento de extraer la imagen, lo cual es una ventaja a favor de las imágenes de video, también no es necesario que una persona esté presente para registrarla al sistema, ya que lo que se usa es una foto generada por una cámara digital.

Las dificultades de la tecnología de imágenes de video es que no cualquier cámara digital funciona para realizar el registro, debe ser una cámara de alta definición, específica para esta tarea. Por esto su costo sigue siendo muy elevado. Se considera el sistema más vulnerable y fácil de engañar, ya que es dependiente de la luz del ambiente, y el uso de elementos como gafas de sol impiden la correcta extracción de las características faciales. El reconocimiento facial, no genera un resultado concreto de identificación de un individuo, solo proporciona un listado de los registros más parecidos a una muestra. Por lo que el usuario del software deberá determinar los procedimientos a seguir para realizar la identificación completa de una determinada persona. El manejo de bases de datos es esencial para esta tecnología, por esto, los algoritmos deben ser muy eficientes en la búsqueda de registros, mientras más usuarios

tengan un sistema, más costoso será y mayor capacidad de cómputo requerirá.

Análisis de Iris del Ojo

El iris del ojo, es una característica humana única para cada ojo, posee mucha más información que la huella dactilar, haciéndolo un sistema de identificación y verificación muy especial. Ni siquiera los dos ojos de la misma persona tienen el mismo patrón de iris. Con la huella dactilar existen hasta diez posibilidades para registrar una persona, mientras que con el análisis de iris máximo dos por obvias razones.

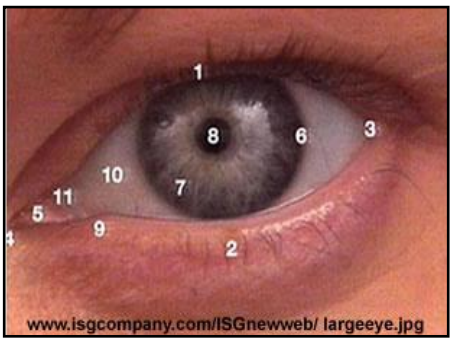


Figura 2.11 Iris del Ojo Humano

El análisis de iris implica una extracción fotográfica del ojo, tiene una estructura definida, compuesta de elementos como la corona, criptas (crypts), filamentos, pecas (freckles), hoyos (pits), y surcos (furrows). La persona a registrar se coloca frente del dispositivo, y una cámara busca la posición del ojo y realiza un zoom óptico hasta alcanzar el detalle necesario del iris y captura la imagen. Estas características son convertidas en un template de iris, como con otras tecnologías biométricas.

El problema de ésta tecnología es el elevado costo de los equipos necesarios para captar la imagen, pues depende de la iluminación del lugar y si la persona tiene gafas puestas o no; también los ojos oscuros

son difíciles de manipular y presentan complicaciones en el registro y verificación.

Geometría de la Mano

Este método registra datos específicos de la mano como su longitud, las curvaturas presentes, la estructura ósea, la longitud de los dedos, el grosor de los mismos, rasgos característicos de nacimiento o causados por lesiones anteriores. Esta tecnología está dominada por Recognition Systems, Inc, utilizan un algoritmo que toma 90 muestras y medidas diferentes de toda la mano y palma, generando un template de tan solo 9 bytes.

La geometría de la mano es un método efectivo, pero no contiene tanta información como otras tecnologías biométricas.

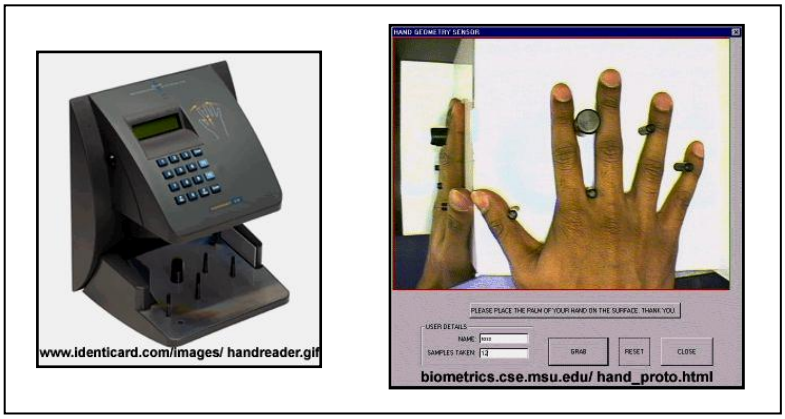


Figura 2.12 Geometría de la Mano

Los lectores de mano tienen un tamaño bastante grande, lo que no es muy útil en situaciones de control de acceso a instalaciones, donde un diseño sencillo y pequeño es requerido. Otra complicación es el costo de los equipos, y los posibles y comunes accidentes que pueden ocurrir en las manos.

Análisis de Firma Manuscrita

La firma manuscrita representa en toda sociedad, la manera por naturaleza de identificar la identidad de un individuo. Es el método más antiguo y más utilizado por la humanidad, en acciones legales y cualquier otra donde sea necesario determinar la aceptación de algo por parte de una persona. La biometría aplicada al análisis de la firma hace referencia a la manera en que una persona la realiza, analizando el orden de las líneas, la velocidad y la presión utilizada, entre otras. Existen tecnologías que comparan un registro o una imagen de la firma de la persona, con la firma hecha en papel, para dar fé de una transacción cualquiera. Estas tecnologías hoy en día no utilizan biometría, y son muy vulnerables a suplantaciones por medio de expertos. Es aquí donde entra y se aplica la biometría, determinando el comportamiento de la persona al realizar la firma. La firma final junto con estas variables son convertidas en un template, y el sistema se encarga de verificar que una persona dice ser quien es por su manera de plasmar su firma.

Reconocimiento de Voz

La voz es uno de los métodos de autenticación más utilizados por las personas. Inconscientemente, cuando una persona mantiene una conversación con alguien donde no lo puede visualizar, el cerebro trata de reconocer entre todos los registros de voz que ha guardado por toda una vida, la identidad de la otra persona que habla. Si no lo reconoce, supone inmediatamente que está frente a una persona desconocida.

La voz es una biometría de comportamiento. Los sistemas de reconocimiento de voz analizan y miden un espectro de la voz de un individuo a través del tiempo. Además, registran todos los cambios de frecuencias para generar con toda esta información, un template y

verificarlo junto con otro registrado con anterioridad. El reconocimiento de voz utiliza como base un micrófono o un dispositivo de captura de sonido, el cual cambia de características según la utilidad y la aplicación donde se implemente. Por lo general se utiliza el mismo dispositivo de captura para hacer el enrolamiento de un usuario al sistema, y para realizar las verificaciones necesarias, en el mismo ambiente donde se espera que funcione normalmente. Una gran ventaja de este sistema biométrico es que no se necesita ninguna clase de contacto con los elementos del sistema, pero la gran desventaja que tiene es la facilidad de suplantación de voces o de presentar voces pregrabadas para obtener verificaciones positivas.

Análisis de Retina

La diferencia entre un análisis de iris y un análisis de retina es el método de extracción de la información para generar un template. La retina se encuentra en la parte trasera del ojo humano, mientras que el iris se encuentra superficial. Para llegar a la retina se necesita de un mecanismo diferente, un pequeño láser que atraviesa todo el ojo y obtiene una imagen de la estructura venosa de la retina. Esta tecnología biométrica se ha probado como la más precisa y confiable, más no es muy atractiva debido a la intrusión necesaria en el ojo con el láser.

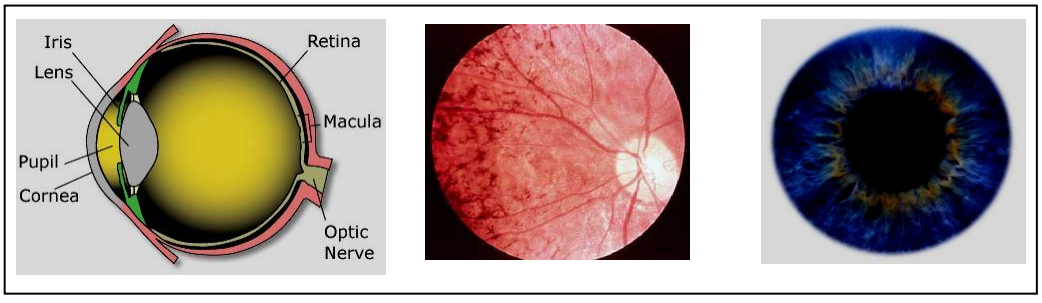


Figura 2.13 Estructura del ojo, Imagen de Retina, Imagen de Iris

Usos de la Biometrica

- ✓ Seguridad de Recursos Computacionales (IT Security)
- ✓ Control de Acceso a Edificaciones
- ✓ Autenticación de Usuarios en Transacciones Electrónicas y vía Web
- ✓ Control de tiempos de trabajo de Empleados
- ✓ Aplicaciones Civiles
- ✓ Aplicaciones Policíacas
- ✓ Seguridad y Aplicaciones Aeroportuarias [WWW 018].

2.2.5 Smart Card Intranet, Extranet e Internet

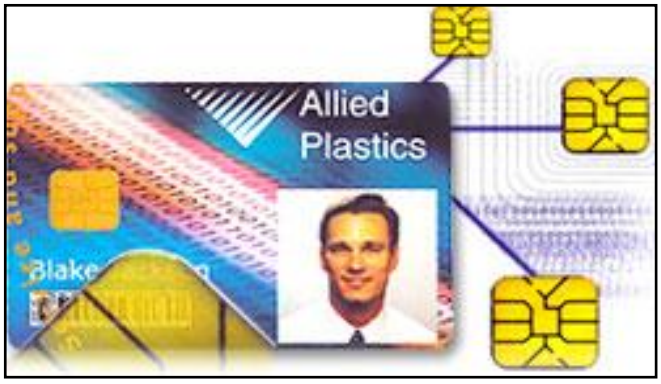


Figura 2.14 Tarjeta Inteligente

Tarjeta Inteligente de Contacto
Tarjeta que necesita ser insertada en un Terminal con lector inteligente, puede ser sincrónica o asincrónica, utilizadas para teléfonos públicos, dispensadores, peajes, etc.

Tarjeta Inteligente sin Contacto
Se diferencian de las tarjetas de contacto ya que utilizan diferentes protocolos de transmisión.

Tarjetas Superinteligentes
Tarjetas que poseen un microprocesador y un teclado, una pantalla LCD y una pila, funciona de manera independiente sin necesidad de insertarla en un Terminal.

Las Smart Card ***(SC)*** ó Tarjetas Inteligentes, conocidas también como "BUSINESS NET", son dispositivos plásticos parecidos a las tarjetas de

crédito, muy usados en varias aplicaciones, como servicios prepagados para teléfono, transportes y otros servicios de uso frecuente, así como también dispositivo de acceso físico o en sistemas computarizados, etc. Últimamente la Smart Card se usa como "token" [35] en un sistema de seguridad que usa criptografía, éstas llevan por dentro un circuito integrado o microprocesador con un sistema operativo que puede desarrollar cierto tipo de actividades como:

- ✓ Almacenar información
- ✓ Leer y escribir datos
- ✓ Encriptar información

Según sus características se clasifican en

- ✓ Smart Card con un chip que contiene sólo memoria de lectura.
- ✓ Smart Card con un chip que tiene un circuito integrado y un microprocesador que se conecta por contacto al exterior.
- ✓ Smart Card con una conexión electromagnética a un microprocesador externo.

Las tarjetas inteligentes nacieron en Europa a comienzos de los años 70, similares a las tarjetas bancarias o de crédito, capaces de incorporar un dispositivo programable. A finales de los años 80 aparecen con chips suficientemente pequeños, con capacidades de memoria muy reducidas. A principios de los 90 las tarjetas inteligentes son utilizadas en la telefonía móvil GSM que inicialmente en su Fase 1 requería muy poca capacidad de memoria, con tarjetas con 1K de memoria, luego con GSM Fase 2 en 1995 empleando tarjetas con 8K de memoria. A finales de 1997 aparecieron las tarjetas de 16K, algunas de las cuales ya implementaban GSM Fase 2+ con SIM. A lo largo de 1999 aparecen diferentes tarjetas Java, aunque con problemas de compatibilidad entre si, y a finales de 1999, aparecieron las tarjetas de 32K.

[35] Procedimiento que permite procesar o portar información personal (generar y guardar claves, etc.)

Componentes de una infraestructura de Tarjetas Inteligentes

- ✓ ***Certificados.-*** Datos digitales que enlazan de forma segura una clave pública con la entidad propietaria de la clave privada correspondiente.
- ✓ ***Autoridades de certificación.-*** Entidades de confianza que emiten los certificados digitales.
- ✓ ***Tarjetas inteligentes.-*** que contienen procesadores integrados y chips de memoria que se emplean para almacenar certificados y claves privadas, así como para llevar a cabo operaciones criptográficas de clave pública, como la autenticación, las firmas digitales y el intercambio de claves.
- ✓ ***Lectores de tarjetas inteligentes.-*** Dispositivos que conectan una tarjeta inteligente al equipo del usuario, también se pueden utilizar para instalar certificados en la tarjeta inteligente.
- ✓ ***Software de tarjetas inteligentes.-*** Software que el proveedor de la tarjeta inteligente suministra para administrar la misma. Algunas organizaciones han creado sus propias herramientas de software para el uso de funciones personalizadas.

Especificaciones de hardware de la Tarjeta Inteligente

- ✓ ***Memoria.-*** Cantidad de datos que deben almacenarse en la SC.
- ✓ ***Expectativa de vida.-*** La duración útil de la tarjeta inteligente.
- ✓ ***Reutilización.-*** Posibilidad de configuración de la tarjeta inteligente para un segundo usuario, si el usuario original abandona la organización.
- ✓ ***Tipo.-*** El tipo de tarjeta más adecuada para su organización.
  a) Tarjeta de crédito,
  b) Etiqueta adhesiva para tarjeta inteligente
- ✓ ***Dimensiones.-*** Tamaño, longitud y grosor de la tarjeta, dependiendo del tipo de tarjeta que especifique.

- ✓ ***Número.-*** La cantidad de tarjetas que necesita, si hay más usuarios que equipos, se necesitará más tarjetas que lectores. Si se utiliza la tarjeta inteligente en varios sistemas, se necesitará más lectores que tarjetas inteligentes. Si se especifica más de un tipo de tarjeta, se necesita indicar las unidades que se necesitarán para cada tipo.
- ✓ ***Tipo de lector de tarjeta de crédito.-*** El tipo de lector más adecuado para su organización. Ya sea por puerto **USB**, tarjeta de expansión **PCMCIA** o puerto de comunicaciones **Serie**
- ✓ ***Número de lectores de tarjeta inteligente.-*** La cantidad de lectores que necesita. Si el número de usuarios es superior al de equipos, necesitará más tarjetas inteligentes que lectores. Si utiliza su tarjeta inteligente en varios sistemas, necesitará más lectores que tarjetas inteligentes.
- ✓ ***Requisitos de rendimiento.-*** El tipo de rendimiento que se puede obtener. Incluye:
    a) Tiempo mínimo de inicio de sesión aceptable para conexiones directas de red.
    b) Tiempo mínimo de inicio de sesión aceptable para conexiones de acceso remoto.
    c) Posibilidad de utilizar credenciales alternativas.
    d) Posibilidad de limitar las conexiones mediante el uso de credenciales alternativas.

Interfaz directa de comunicaciones electrónicas

Las comunicaciones están en crecimiento constante. Cada nuevo avance ofrece un nuevo campo en el que puede aplicarse las tarjetas inteligentes. Las especificaciones físicas, eléctricas, el formato de los comandos y todo lo relacionado con tarjetas se especifica en la norma ISO 7816. [WWW 019].

Características de las Tarjetas Inteligentes

- ✓ **Inteligencia.-** Es capaz de almacenar cualquier tipo de información, además es autónoma en la toma de decisiones al momento de realizar transacciones.
- ✓ **Utiliza clave de acceso o PIN.-** Para poder utilizarse es necesario digitar un número de identificación personal, es posible además incorporar tecnología más avanzada como identificación por técnica biométrica, huella digital o lectura de retina.
- ✓ **Actualización de cupos**.- Después de agotado el cupo total de la tarjeta inteligente es posible volver a cargar un nuevo cupo.

Estructura

- ✓ **Zona Abierta:** Contiene información que no es confidencial (nombre del portador y su dirección).
- ✓ **Zona de Trabajo:** Contiene información confidencial. (Aplicaciones bancarias: cupo de crédito disponible, el número de transacciones permitidas en un periodo de tiempo).
- ✓ **Zonas Secretas:** La información es totalmente confidencial. El contenido de estas zonas no es totalmente disponible para el portador de la tarjeta, ni tiene por que conocerla la entidad que la emite ni quien la fabrica.

Funcionamiento.- Las tarjetas se activan al introducirlas en un lector de tarjetas. Un contacto metálico, o una lectura láser, permite la transferencia de información entre el lector y la tarjeta, actualmente existen tarjetas que permiten leer una tarjeta inteligente desde el propio ordenador personal. Las comunicaciones de las tarjetas inteligentes se rigen por el estándar ISO 7816/3, la tasa de transferencia de datos es de 9600 baudios en modo asincrónico.

Tipos de Tarjetas Inteligentes

Tarjeta Inteligente de Contacto

Estas tarjetas necesitan ser insertadas en una terminal con lector inteligente para que por medio de contactos pueda ser leída, existen dos tipos de tarjeta inteligente de contacto:

a) **Tarjetas Sincrónicas.-** poseen un chip de memoria para almacenar datos. Son desechables, cargadas previamente con un monto o valor que va decreciendo a medida que se la utiliza, una vez se acaba el monto la tarjeta se vuelve desechable, son utilizadas internacionalmente para el pago de peajes, teléfonos públicos, maquinas dispensadoras y espectáculos, etc. Dentro de esta categoría existen dos tipos de tarjeta:

   Memoria Libre: no tiene ningún mecanismo de protección para acceder a la información.

   Memoria Protegida: se necesita de códigos y pasos previos para tener acceso a la información.

b) **Tarjetas Asincrónicas:** tarjetas con microprocesador incluido, del mismo tamaño y grosor de una tarjeta de crédito, tienen una cinta magnética en la parte posterior. Dentro del plástico se encuentra un elemento electrónico junto con la memoria RAM, ROM y EEPROM en el mismo chip. Estas tarjetas tienen su uso generalizado en los bancos, tarjetas de crédito, etc. [WWW 019].

Tarjeta Inteligente sin Contacto

Tarjetas similares a las de contacto, con la diferencia de que utilizan diferentes protocolos de transmisión en la capa lógica y física, no utiliza contacto galvánico sino de interfase inductiva, puede ser de media distancia sin necesidad de ser introducida en una terminal de lector

inteligente. Las ventajas que tiene ésta tarjeta es que es más resistente a los elementos externos tales como la suciedad, rayones, humedad, etc.

Tarjetas Superinteligentes

Cumplen las mismas funciones que las tarjetas inteligentes con microprocesador, están equipadas con un teclado, una pantalla LCD y una pila. Esta tarjeta permite funcionar totalmente independiente por esto no hay necesidad de insertarla en una terminal.

Ventajas

- ✓ Gran capacidad de memoria
- ✓ Altos niveles de seguridad
- ✓ Reducción del fraude
- ✓ Información organizada
- ✓ Confiabilidad y seguridad en la información
- ✓ Facilidad de usos sin necesidad de conexiones en línea o vía telefónica
- ✓ Comodidad para el usuario
- ✓ A través de Internet los usuarios de tarjetas inteligentes podrán comprar por computador y pagar por red
- ✓ Garantía en las operaciones con dinero, cien por ciento efectivas.
- ✓ Menores costos para empresarios y usuarios.
- ✓ Estándares específicos ISO 7810, 7811, 9992, 10536.
- ✓ Privacidad.
- ✓ Administración y control de pagos más efectivo.

Desventajas

- ✓ Mayor posibilidad de contagio de virus.
- ✓ Molestias al recuperar información de una tarjeta robada.
- ✓ Por su tamaño se puede extraviar fácilmente.
- ✓ La tarjeta debe ser recargada.
- ✓ Mayor costo de fabricación.
- ✓ Dependencia de la energía eléctrica para su utilización.
- ✓ Es necesario un lector para tarjetas inteligentes.

Servicios más corrientes usando tarjetas inteligentes

- ✓ **Tarjetas de Telefonía Móvil:** Permite tener registro del abonado y clave de acceso.
- ✓ **Tarjetas de Salud.-** contienen un historial clínico o información relativa a enfermedades crónicas o alérgicas del paciente.
- ✓ **Monedero electrónico bancario:** El chip contiene información acerca del saldo monetario de la tarjeta en función de su uso (en establecimientos adecuados) y su carga en cajeros automáticos.
- ✓ **Tarjetas telefónicas:** sector que más uso hace de las tarjetas inteligentes. El chip contiene información acerca del saldo pendiente de uso en cabinas telefónicas preparadas para ello.

Beneficios

Presentan un coste por transacción menor que el de las tarjetas magnéticas convencionales. Permiten realizar transacciones en entornos de comunicaciones móviles, en entornos de prepago y en nuevos entornos de comunicaciones. A estos entornos no puede acceder la tarjeta tradicional. La tarjeta inteligente es un mecanismo muy seguro para el almacenamiento de información financiera o transaccional, la tarjeta inteligente es un lugar seguro para almacenar información como claves privadas, numero de cuenta, password, o información personal muy valiosa, esta capacidad se debe a:

- ✓ Encriptación.
- ✓ Clave segura (PIN).
- ✓ Clave secundaria de seguridad.
- ✓ Sistema de seguridad redundante.
- ✓ Firmas digitales.
- ✓ Alta seguridad en el acceso físico a: recintos, laboratorios, controles, salas informáticas.
- ✓ A través de sistemas biométricos, huella dactilar y retina.

2.3 Certificados de Servidores

Figura 2.15 Estructura de un certificado de Servidor

Certificados de Servidores
: Documento electrónico que certifica que un servidor pertenece a una determinada empresa.

Certificados para Empresas Certificadoras
: Documentos de entidades que emiten certificados, pueden ser públicas o privadas.

Los certificados son documentos digitales que atestiguan que una clave pública corresponde a un individuo o entidad determinados. De este modo se evita que intrusos utilicen una combinación de claves asegurando ser otra persona. Un certificado consiste en una clave pública y el nombre de su propietario. Este certificado es firmado por una autoridad de certificación (*Certification Authority*, CA), cuya clave pública es fácilmente verificable. Adicionalmente, puede contener la fecha de expedición del certificado, la de expiración de la clave, el

nombre del notario electrónico que emitió el certificado y un número de serie. De todo ello calcula la huella digital y la cifra con su clave privada.

Estados de un Certificado Digital

- ✓ **Activo o Preactivo.-** certificado que, generado en un determinado instante, sólo será válido en un lapso de tiempo posterior. Desde el momento en que se genera el certificado y hasta que llega el momento de entrar en vigencia, el certificado está en estado Preactivo. Cuando la fecha en curso cae dentro del intervalo de vigencia de un certificado, el cerificado está en estado Activo.
- ✓ **Suspendido**.- Cuando es necesario anular temporalmente la vigencia de un certificado, la AC emisora decide pasarlo al estado de Suspendido. Con ello no se está invalidando de forma irreversible el certificado, sino que se le retira de circulación hasta que se le vuelva a dar el estado de Activo.
- ✓ **Revocado**.- Cuando las condiciones que llevaron a la emisión de un certificado cambian antes de que éste expire, y son de importancia suficiente, la AC deberá anularlo; para ello, emite un segundo certificado especial, denominado **"de revocación"**, por el cual, desde ese instante desautoriza al certificado previo y lo hace de un modo irreversible.
- ✓ **Caducado.-** es el estado final de cualquier certificado, se produce cuando la fecha en curso es posterior a la fecha de caducidad indicada en el propio certificado. El estado de "**certificado caducado"** no le resta valor histórico ya que, mientras estuvo activo, las operaciones en las que participó eran perfectamente válidas.

2.3.1 Tipos de Certificados

Certificado para servidores.- Certifica que un servidor es de la empresa que dice y que el identificador del servidor es correcto

Certificados para empresas certificadoras.- Corresponden a entidades que certifican (pueden ser privadas o públicas, por ejemplo, una universidad). [LIB 01].

2.3.2 Autoridades Certificadoras de Servidores.

Una Autoridad Certificadora (AC) es una entidad u organización de confianza del emisor y del receptor del mensaje. Esta confianza de ambos en una 'tercera parte confiable' permite que cualquiera de los dos confíe a su vez en los documentos firmados por la AC, en particular, en los documentos que identifican cada clave pública con su propietario correspondiente y se denominan certificados. Las autoridades de certificación, conocidas como notarios electrónicos, deben ser entes fiables y ampliamente reconocidos que firman con conocimiento de causa y asunción de responsabilidades legales, las claves públicas de las personas, rubricando con su propia firma la identidad del usuario.

Todas las técnicas están encaminadas a garantizar que un mensaje ha sido enviado por un usuario y que son leídos únicamente por el usuario destinatario del mensaje y no sea suplantada su identidad. Para esto lo primordial es difundir al máximo las claves públicas de los usuarios, porque cuanta más gente la tenga, más improbable es que esa persona sea suplantada. Las AC deben tener en todo momento registrado cuales son los estados en los que se encuentran sus certificados. Estas entidades deben tener las "Listas de Certificados Revocados" LCR, como unas listas "negras" en las que se publica cuáles son los certificados que ha anulado para, con ello, desentenderse de las responsabilidades que

pudieran acarrear la utilización y/o aceptación por parte de algún agente de la red de los mencionados certificados.

Las AC expiden certificados digitales que pueden ser:

- ✓ **Certificados de Identidad.-** ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública, son los más usados actualmente.
- ✓ **Certificados de Autorización o Potestad.-** certifican otro tipo de atributos del usuario distintos a la identidad, como pueden ser, el pertenecer a una determinada asociación, disfrutar de una serie de privilegios, poseer un carnet de conducir, etc.
- ✓ **Certificados Transaccionales.-** atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero; el agente de registro al servicio de la AC Emisora.
- ✓ **Certificados de Tiempo o de Estampillado Digital de Tiempo.-** permiten dar fe de que un documento existía en un instante determinado de tiempo, por lo que constituyen un elemento fundamental de todos los servicios de registro documental y de protección de la propiedad intelectual o industrial que se están proponiendo.
- ✓ **Certificados personales.-** de los usuarios de la red, que garantiza que una dirección de correo y clave pública corresponden a una persona real y cierta.
- ✓ **Certificados para fabricantes de programas.-** Se utilizan para "firmar" el software y garantizar así que no ha sido alterado (por ejemplo con virus) [WWW 020].

Los certificados pueden adoptar múltiples formatos. El protocolo estándar más utilizado en Internet para certificar es la norma ITU-T

X.509 v3, la cual forma parte del servicio de directorio diseñado por ISO para el modelo OSI. (Como se puede ver en la Fig. 2.16).

En el certificado se incluyen:

número de versión

número de serie

información sobre la identidad del usuario (e-mail, etc.)

algoritmos y parámetros de encriptado que son utilizados por el certificador

firma de la autoridad certificadora

periodo de validez

información sobre la clave pública: algoritmo, parámetros, y la llave pública propiamente dicha.

clave pública del CA [LIB 01].

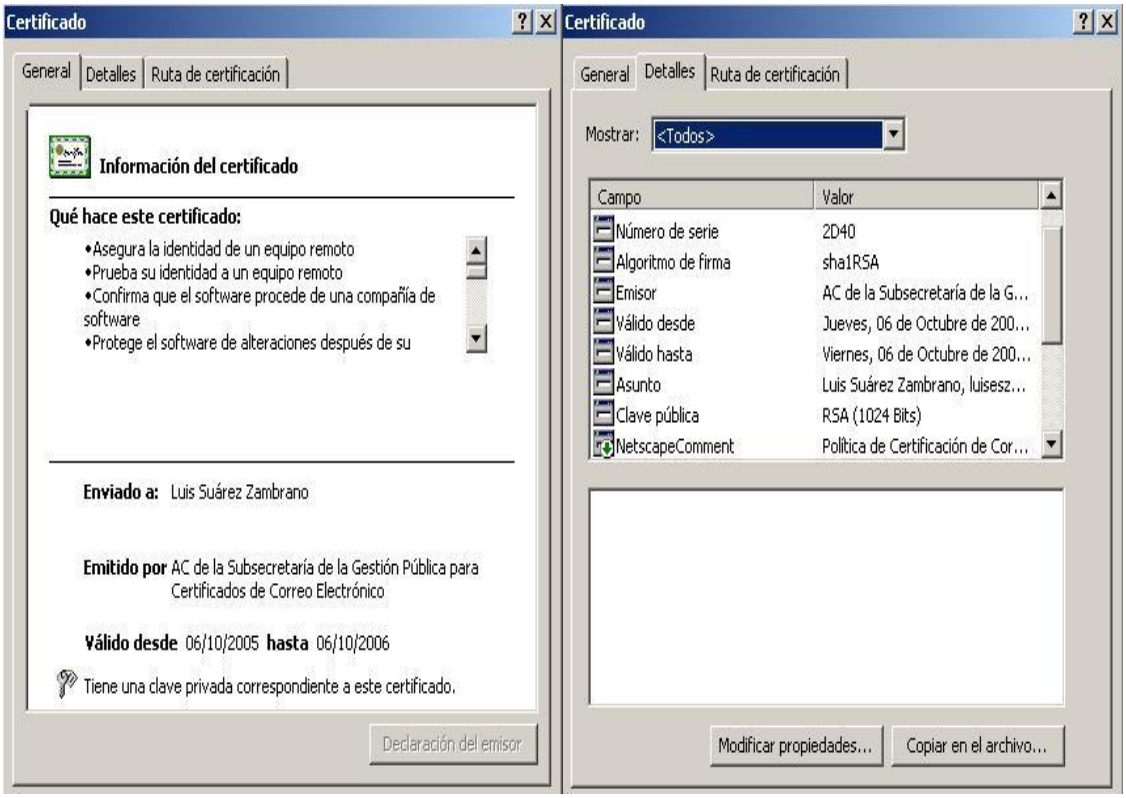


Figura 2.16 Estructura de un Certificado

Funciones de las Autoridades de Certificación

- ✓ **Generación y Registro de claves:** cada usuario deberá generar por sus propios medios, su par de claves. Este servicio puede estar a cargo de la propia Entidad de Certificación garantizando así el secreto de la información. Una vez, generada las claves, el usuario debe "registrar" su clave pública en la Autoridad de Certificación, para esto debe cumplir con los requisitos que la entidad publica en su documento público de Política de Emisión de Certificados incluida en su Política de Seguridad, esta autoridad devuelve al solicitante un certificado digital que atestigua la validez de su clave pública para actuar dentro del sistema. Los sistemas de autenticación basados en claves simétricas y secretas, como "Kerberos"[36], no permiten la generación local de claves, ésta es función de la Autoridad de Certificación.
- ✓ **Identificación de Peticionarios de Certificados:** La emisión de Certificados de Identidad Personal exigen el reconocimiento previo de los "identificadores intrínsecos"[37]. Según el número e importancia de los identificadores intrínsecos que las Autoridades de Certificación verifican, registran y archivan para la emisión de sus certificados de identidad. Una Autoridad de Certificación puede requerir sólo la Cédula de Identidad y comprobar que la fotografía y la apariencia del solicitante coinciden, otra puede exigir otros requisitos adicionales etc. Cada CA publica cuales son los requisitos y el protocolo a seguir para obtener cada uno de los tipos de certificados digitales que componen su oferta, de forma que, quién verifica el certificado de la clave, pueda establecer cual

[36] Protocolo autenticación de usuarios en el Internet.
[37] Elementos característicos y únicos, propios de un individuo, tales como firma, fotografía, huella dactilar, timbre de voz, fondo de ojo, marcas de nacimiento, etc.

es el nivel de confianza que le merece dicha clave pública y el correspondiente certificado.

- ✓ **Emisión de certificado:** Una Autoridad de Certificación puede ser cualquier organización o institución que se comprometa a ser garante de los extremos que aparecen en sus certificados y en su política de seguridad. Así, cualquier empresa puede actuar como una Autoridad de Certificados de Identidad a favor de sus empleados, o una universidad de sus estudiantes, etc. Además de los compromisos de verificación que se indican en la política pública de una Autoridad de Certificación, ésta se compromete a emitir certificados digitales únicos y perfectamente identificables a través de su número de serie. Dichas autoridades también son responsables de mantener un registro seguro y disponible sobre cual es el estado de cada uno de los certificados que emite, ya sea a) Activo o Preactivo, b) Suspendido, c) Revocado, d)Caducado

Las Autoridades de Certificación debe tener siempre publicada su "Listas de Certificados Revocados" como unas listas "negras" en las que la entidad emisora publica cuales son los certificados que ha anulado para, con ello, desentenderse de las responsabilidades que pudieran acarrear la utilización y/o aceptación por parte de algún agente de la red de los mencionados certificados.

- ✓ **Almacenamiento en la AC de su clave privada:** Las AC, verifican las condiciones que aparecen en sus políticas públicas de seguridad y, posteriormente, emiten y siguen el ciclo de vida de los certificados que emite. Las Agencias de Certificación son "firmadores" digitales, y deben disponer de una clave privada que sólo conocen ellos y que custodian con niveles de seguridad iguales o superiores a los declarados públicamente. Éstas se

generan y almacenan permanentemente en unidades hardware de alta seguridad, sometidas a sofisticadas medidas de seguridad física y dentro de entornos a prueba de intrusión electrónica, llamadas "Unidades de Firmado de Certificados" o CSUs.

- ✓ **Mantenimiento de las claves vigentes y revocadas:** Las AC pueden, dentro de los servicios que ofrecen al público, almacenar los certificados emitidos durante su periodo de validez. De este modo, en el caso de que uno de los agentes pierda su certificado, siempre podrá pedirle a la autoridad emisora que le envíe de nuevo una copia. Este servicio debe estar disponible para cualquier usuario ya sea una persona o institución o incluso Autoridades de Certificación que tienen asociados servidores públicos de certificados mediante los cuales cualquier agente puede solicitar los certificados de cualquiera de los demás agentes.

Servicios de directorio: En el caso de que alguien quiera encontrar la clave pública de un usuario del sistema, las Autoridades de Certificación dan Servicios de Directorio[38] mediante los cuales, cualquiera puede obtener la clave pública certificada de cualquier miembro con quien quiere ponerse en contacto o establecer relaciones de algún tipo. Un servicio de Directorio es una gran base de datos en la que cada entrada de usuario en el directorio contiene los certificados de las claves públicas de las que es titular, y cada entrada de una Autoridad de Certificación contiene todos los certificados emitidos para ella por otras Autoridades de Certificación ante las que está inscrita, y todos los certificados emitidos por ella misma para otras autoridades. [WWW 023].

[38] Especificado en el estándar X500 de las normas se seguridad para intercambio de datos en la Red.

2.4 Certificados de Clientes

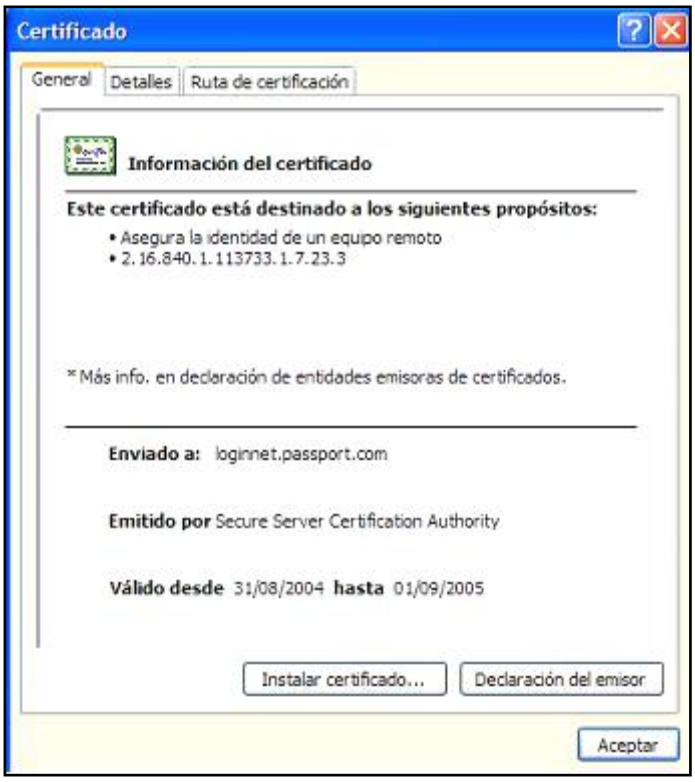


Figura 2.17 Certificado de Clientes

Certificados de Clase 1

Certificados que contienen, nombre de la persona, correo Electrónico y opcionalmente más datos de la persona

Certificados de Clase 2

Certificados que ofrecen mayor seguridad, contienen la mayoría de datos de una persona, que pueden ser relevantes.

Certificados de Clase 3

A las comprobaciones de la Clase 2, se añaden la verificación de crédito de la persona o empresa mediante algún servicio bancario

Certificados de Clase 4

A todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Un certificado de Cliente es un certificado digital diseñado para comprobar la identidad de un individuo. Al igual que los certificados de servidores y sitios web, los certificados de clientes ligan un nombre específico con una llave privada específica. Un certificado de cliente también es emitido por una Autoridad de Certificación.

Usos y Beneficios

- ✓ Pueden eliminar la necesidad de recordar nombres de usuario y claves de acceso, solo es necesario signar utilizando la firma digital al entrar a un espacio restringido.
- ✓ Las organizaciones pueden utilizar un certificado digital emitido por una Autoridad de Certificación como prueba de pertenecer a una organización, para no tener que disponer y desplegar una base de datos con toda la información de sus pertenecientes.
- ✓ Al contener los certificados digitales una llave pública de una persona, es posible utilizarlos para enviarle a dicha persona un correo electrónico o establecer comunicación con ella.
- ✓ Al contener los certificados digitales información de las personas tales como la edad, sexo, etc, es posible mediante éstos restringir el acceso a personas menores de edad a sitios con contenido restringido o permitir el acceso a espacios "solo" para mujeres o "solo" para hombres.

2.4.2 Tipos de Certificados

Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras de manera general, han dividido los certificados en varios tipos y dependiendo del tipo de certificado a emitir van a depender las medidas de comprobación de los datos y el costo en el mercado del mismo.

- ✓ **Certificados de Clase 1**: Certificado de Cliente que contiene: Nombre de la Persona, y opcionalmente su dirección de Correo Electrónico. Son los más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.
- ✓ **Certificados de Clase 2**: en los que la Autoridad Certificadora comprueba además el permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento. Certificados que ofrecen un mayor nivel de seguridad para las transacciones en Internet
- ✓ **Certificados de Clase 3**: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante algún servicio bancario
- ✓ **Certificados de Clase 4**: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Según la finalidad de los certificados electrónicos, éstos se dividen en:

1. **Certificados SSL para cliente**: identifican y autentican a clientes ante servidores en comunicaciones mediante el protocolo SSL, y se expiden normalmente a una persona física, un particular o un empleado de una empresa.
2. **Certificados SSL para servidor**: identifican a un servidor ante un cliente en comunicaciones mediante el protocolo SSL, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La

presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

3. **Certificados S/MIME**: usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autenticación, Integridad y No Rechazo. También se puede cifrar el mensaje con la llave pública del destinatario, lo que proporciona Confidencialidad al envío.
4. **Certificados de firma de objetos**: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de este tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.
5. **Certificados para AC**: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

Actualmente los certificados digitales para clientes están soportados en la mayoría de Navegadores de Internet y muchas otras aplicaciones basadas en SSL.

El soporte dado para certificados de clientes tiene cuatro principios fundamentales.

- ✓ **Creación de llaves.-** el navegador contiene código para crear una pareja de llaves, una pública y una privada, y la llave pública es

enviada a una Autoridad Certificadora mediante una transacción tipo POST de HTTP.

- ✓ **Obtención de Certificados.-** el navegador puede aceptar un certificado descargado desde la autoridad certificadora mediante HTTP.
- ✓ **Reto/Respuesta.-** el navegador de Internet pude utilizar una llave secreta que es almacenada previamente para firmar un reto generado al azar por un servidor SSL.
- ✓ **Almacenamiento Seguro.-** el navegador proporciona un lugar seguro para almacenar la llave secreta que dependiendo de la versión del Navegador, se la puede almacenar en un archivo encriptado. [LIB 01].

2.4.3 Autoridades Certificadoras de Clientes

Al igual que las Autoridades Certificadoras de Servidores, las empresas que proveen de estos servicios o pueden hacer para clientes que necesiten disponer de dichos certificados para realizar sus transacciones a través de la red, On-line, y enviar y recibir información por medios electrónicos.

En todo el mundo existen empresas que proveen de certificados tanto para Clientes Como para empresas y organizaciones que realizan sus actividades utilizando medios electrónicos. La finalidad principal de las Autoridades de Certificación de Clientes, es permitir que cualquier persona tenga una identificación con la cual de forma segura le permita realizar cualquier tipo de transacción, respaldado de la certificación de la Autoridad de Certificación que atestigua y da fe de que esa persona realmente es quien dice ser, y por lo tanto sella con su Certificado Digital dicha identificación como prueba de su validez.

Hoy en día la gran mayoría de empresas certificadoras ya sean privadas o Gobiernos que emiten Certificados Digitales sea de cualquier tipo, son empresas reconocidas mundialmente y merecen total aceptación por parte de sus usuarios, ya que han probado y demostrado ser competentes para sus funciones, reduciendo al mínimo los riesgos de pérdida e interceptación de información. Como ejemplo se pueden mencionar a VeriSign de Estados Unidos de Norteamérica, Geo Trust la más grande Certificadora y alojadora de páginas Web de Europa, El Gobierno de la República de Argentina, el Servicio Postal de EEUU,etc.

2.5 Metodología de firmas de Código

2.5.1 Tecnología de Autenticación de Microsoft

La firma de código es una técnica para signar programas ejecutables mediante firmas electrónicas, está diseñada para mejorar la confiabilidad del software distribuido por Internet. Su finalidad es proporcionar un sistema para descargar código de manera confiable y reducir el impacto de programas hostiles, incluyendo virus y caballos de Troya.

Muchos son los riesgos que se corren al entrar en un sitio web y descargar copias de programas ejecutables que supuestamente servirán, si es una página web confiable, se tendría la seguridad de que el software que se obtiene es confiable, pero qué decir de otros sitios web? ¿Cómo saber si los programas que allí se encuentran a disposición son alterados? O son una puerta de entrada para los hackers?

Para lograr una completa transmisión de un programa a través de Internet se necesitan dos factores:

1. Una firma digital que signa al programa ejecutable con una llave secreta.

2. Un certificado digital con la llave pública correspondiente, el nombre de la persona u organización a quienes pertenece y una firma digital signada por una autoridad certificadora reconocida. Estos dos aspectos se muestran en la Fig 2.17 que se muestra a continuación.

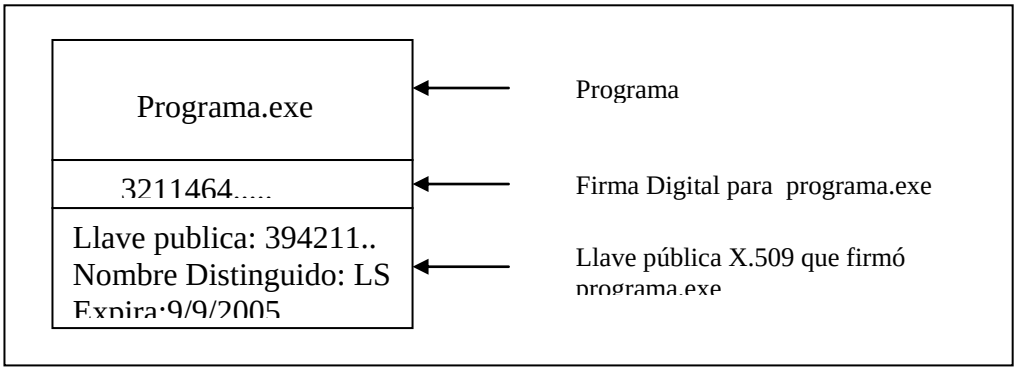


Figura 2.17 Diagrama de una Pieza de Código

La firma de código presupone la existencia de una infraestructura de llave pública, de lo contrario no se podría determinar a quien pertenece la firma puesta a un fragmento de código. Al momento de recibir un código cualquiera, es necesario revisar todas las firmas de código, al momento de descargar y antes y cada vez que se ejecute el programa. De esta manera se podrá detectar intentos hostiles de modificar el código, robo, como modificaciones accidentales resultantes de errores del sistema operativo o fallas de hardware. [LIB 01].

La firma de código se ha creado como una forma de crear responsabilidad para las personas que escriben y envían programas por Internet, y también para acostumbrar a los usuarios de Internet no ejecutar programas sin firmar.

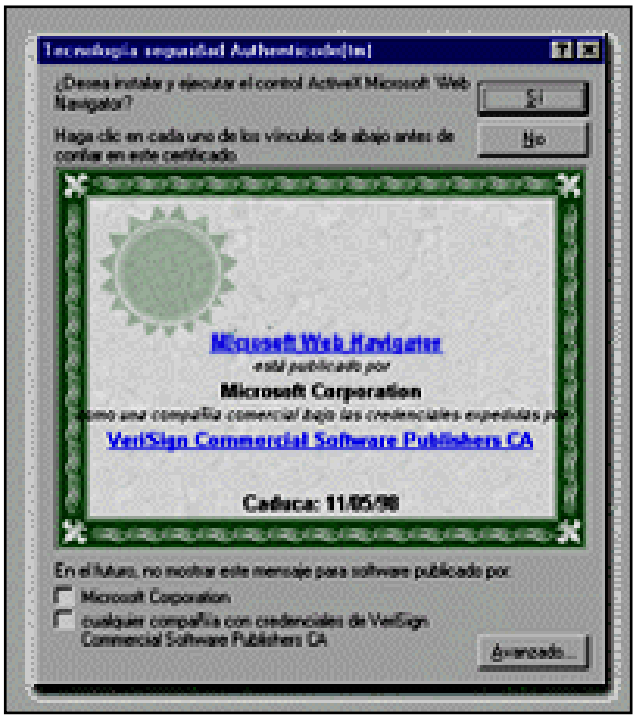


Figura 2.18 Formato de Autenticación de Certificados

La firma de código hoy

En la actualidad existen varias propuestas para la firma de código:

- ✓ **Authenticode.-** sistema desarrollado por Microsoft para firmar todo tipo de código descargado.
- ✓ **JAR.-** es un formato de archivo JAVA desarrollado por JavaSoft y Netscape, el cual puede ser utilizado para soportar firmas digitales. En realidad son archivos ZIP (empaquetados) con firmas digitales.
- ✓ Extensiones al sistema de calificación de contenido PICS para permitir a las organizaciones explicar los distintos tipos de certificados digitales.

La tecnología de Authenticode de Microsoft

Authenticode fue desarrollado y publicado por Microsoft en 1996 como parte de las tecnologías Internet Explorer 3.0 y Actives de Microsoft,

para firmar código digitalmente. Con esta tecnología se pretendió reducir los riesgos de hacer legalmente responsables a los editores de software por los programas que escriben y que pudieren caer en manos no autorizadas. En Authenticode se describen una serie de formatos de archivo para firmar archivos EXE de 32 bits, DLL y OCX de Microsoft. El archivo firmado contiene al archivo original sin firmar, la firma digital y un certificado digital X.509 v3 correspondiente a la llave pública necesaria para verificar la firma.

Desde su inicio Microsoft y VeriSign exigen a los editores de software tomen un **"juramento de editor de software"** un acuerdo obligatorio solicitado por las empresas en mención, en el cual el editor de software promete no firmar programas que contengan virus o que de alguna manera dañen a alguna computadora. Sin embargo esta técnica no asegura del todo que el software firmado con las llaves de Authenticode sea seguro, lo que pretende es otorgar a las Entidades Certificadoras las bases necesarias para revocar los certificados de editor de software que se utilicen para firmar código que no cumpla con los términos del juramento.

Microsoft Internet Información Server (IIS) e ISA Server funcionan en conjunción con Windows 2000 Server y ofrecen soporte para varios mecanismos de autenticación en HTTP. [LIB 01].

- ✓ **Básica:** utilizada para identificación no segura o poco segura de clientes, ya que el nombre de usuario y la contraseña se envían como texto codificado en base 64, que puede ser fácilmente descodificado. IIS autorizará el acceso a los servicios Web XML si las credenciales coinciden con las de una cuenta de usuario válida.

- ✓ **Básica sobre SSL:** igual que la autenticación básica, excepto que el canal de comunicación está cifrado y protege de ese modo el nombre de usuario y la contraseña. Una buena opción para entornos en Internet; sin embargo, el uso de SSL influye negativamente en el rendimiento.
- ✓ **Implícita:** utiliza algoritmos hash para transmitir las credenciales del cliente de forma segura. Sin embargo, es posible que no sea compatible con todas las herramientas de desarrollo para generar clientes de servicios Web XML. IIS autorizará el acceso a los servicios Web XML si las credenciales coinciden con las de una cuenta de usuario válida.
- ✓ **Autenticación de Windows integrada:** resulta útil sobre todo en entornos en Intranet. Utiliza NTLM o Kerberos. El cliente debe pertenecer al mismo dominio que el servidor o a un dominio en el que el dominio del servidor confía. IIS autorizará el acceso a los servicios Web XML si las credenciales coinciden con las de una cuenta de usuario válida.
- ✓ **Certificados de cliente a través de SSL:** requiere que cada cliente obtenga un certificado. Los certificados se asignan a las cuentas de usuario, que son utilizadas por IIS para autorizar el acceso a los servicios Web XML. Se trata de una solución viable para entornos en Internet, aunque el uso de certificados digitales no está muy extendido actualmente. Es posible que no sea compatible con todas las herramientas de desarrollo para generar clientes de servicios Web. [WWW 024].

2.5.2 Formas de Publicación

Para publicar con Authenticode es necesario obtener una copia del Kit de Desarrollo de Software (SDK, Software Developer's Kit) de Microsoft para ActiveX. Generalmente si no se dispone de dicho Kit, se lo puede descargar de la página web de la empresa Microsoft. Para los desarrolladores firmar software es un paso adicional que deben dar para publicar un programa, la firma de un programa es lo último que se debe realizar antes de publicar un programa, una vez publicado si se le realiza cualquier modificación al software, éste deberá signarse otra vez.

El programa signcode de Microsoft tiene la siguiente sintaxis:

```
Signcode –prog ArchDePrograma –spc archCredenciales –pvk archLlavePrivada
        -name nombreObra –info infoObra –gui –nocerts
        -provider nombreDeProveedorCripto –providerType n
        { -commercial | -individual }
        { -sha  | md5* }
```

Una vez ejecutado el programa se ejecutará también el asistente para firma de código (CSW) Code Sign Wizard, el cual le guiará en los pasos para firmar el código. El asistente para firmar código que está en el kit de desarrollo de software SDK tiene una interfaz fácil de emplear para firmar código, que le va guiando a través del proceso de firmado, de manera que no tenga dificultades durante el proceso.

2.5.3 Verificación de Firmas de Authenticode de Microsoft

En la actualidad las firmas de Authenticode solo pueden verificarse mediante programas desarrollados con el kit de desarrollo de software (SDK) de Microsoft para Actives. Esta herramienta incluye un programa llamado **chktrust** que permite a cualquier usuario verificar el certificado de un programa ejecutable y permite averiguar al usuario si confía o no

plenamente en dicho certificado. Este programa tiene las siguientes opciones:

```
c:\>chktrust
        Usage:  CHKTRUST [ - options] file name
        Las opciones son:
        - I     Archivo ejecutable de 32 bits
        - J     Clase de Java
        - C     Archivo tipo CAB
        - N     Sin interfaz de usuario en caso de no confianza
```

Si el certificado está firmado, chktrust muestra un certificado **"completo"** el mismo que contiene el nombre de la persona u organización que contiene el certificado que se utilizó para firmarlo, y el nombre de la autoridad certificadora que firmó el certificado, caso contrario el programa desplegará una lista de editores de software aprobados.

Chktrust devuelve un resultado de cero (0) si el usuario elige confiar en el programa.

```
c:\>chktrust  signed.exe
        Result : 0
```

Chktrust devuelve otro valor si el usuario no decide confiar en el programa

```
c:\>chktrust unsigned.exe
        Result : 800b004
        c:\>
```

Microsoft ha logrado implementar un soporte para Authenticode en Internet Explorer debido a los grandes peligros asociados con ActiveX y la información que éstos pueden robar al momento que son descargados a un computador, ya que no se puede establecer qué tipo de programa

se puede estar ejecutando detrás de una ActiveX, la solución más viable que Microsoft ha visto es dar la posibilidad de rastrear a los autores de los controles Actives mediante Firmas Digitales y su tecnología Authenticode. La teoría detrás de Authenticode es que el usuario se dará cuenta cuando un control haga daño y buscará una reparación, si esto no funciona entonces el usuario podría llevar al editor de software a los tribunales por los daños hechos por la ActiveX de dicho editor.

Una forma de controlar las ActiveX es dando niveles de seguridad al funcionamiento de Internet Explorer, por lo general el nivel predefinido es el Alto, entonces en este nivel Internet Explorer sólo ejecutará controles ActiveX firmados digitalmente con una llave secreta para la que exista el certificado digital válido de editor de software, cuando esto ocurre Internet Explorer muestra l usuario la información correspondiente a la persona u organización que firmó el código y el nombre de la autoridad certificadora que firmó el certificado digital del editor de software.

2.5.4 Certificados de Editores de software

Un editor de software posee certificados digitales emitidos por cualquier Autoridad Certificadora reconocida, lo que se debería entender que Authenticode de Microsoft debería trabajar con dichos certificados, pero no existen muchas Autoridades Certificadoras que emiten este tipo de certificados, una de ellas es VeriSign. Esta Autoridad emite dos tipos de certificados de editor de software:

a) **Certificados Individuales.-** que se basan en los certificados digitales clase 2 de VeriSign.

b) **Certificados Comerciales.-** que se basan en los certificados clase 3 de VeriSign, similares a los que la compañía emite para servidores Web. [WWW 024].

2.6 Algoritmos de Generación de Firmas Digitales

Sobre Digital.- es utilizado para resolver el problema de distribución de claves cuando se usan algoritmos simétricos, son generados utilizando un algoritmo de clave pública. Para ello se encripta una clave de sesión con la clave pública del destinatario del mensaje. Solo el destinatario podrá abrir el sobre y recuperar la clave de sesión necesaria para desencriptar el mensaje encriptado.

Compresión.- La seguridad de un sistema criptográfico no depende únicamente del algoritmo de encripción utilizado, sino que también depende de la cantidad de mensajes diferentes que pueden ser generados. Se puede aumentar la seguridad reduciendo la redundancia de los mensajes. Esto se logra utilizando algoritmos de compresión, que eliminan la redundancia del mensaje original. Después de ser encriptado-transmitido-desencriptado, el mensaje es expandido para recuperar el formato original.

A continuación se enlistan la mayoría de algoritmos y funciones que permiten generar firmas digitales, los más importantes se estudian a detalle en el Capítulo 3.

Algoritmos simétricos más comunes

- ✓ Algoritmo DES
- ✓ Algoritmo DESX
- ✓ Algoritmo Triple-DES
- ✓ Algoritmo RC2

- ✓ Algoritmo RC4
- ✓ Algoritmo RC5

Algoritmos Asimétricos más comunes

- ✓ Algoritmo RSA
- ✓ Algoritmo *DSA*
- ✓ DH (Diffle-Hellman)
- ✓ El Gamal
- ✓ Algoritmo Rijndael
- ✓ ECC, Algoritmo Basado en Curvas Elípticas.
- ✓ Sistema Probabilístico.

Funciones digest más utilizadas

- ✓ HMAC
- ✓ MD2
- ✓ MD4
- ✓ MD5
- ✓ SHA
- ✓ SHA1

Otros algoritmos de Encripción

- ✓ Sistema de Rabin.
- ✓ Sistema de Merkle-Hellman.
- ✓ Sistema de McEliece.
- ✓ AES (Advanced Encryption Standard).

2.7 Otros métodos de generación de firmas digitales

El Algoritmo DSS

En este algoritmo existen dos claves para cada persona. Una de ellas crea la firma y se mantiene secreta. La otra - la clave pública - verifica la firma. El DSS fue desarrollado por el U.S. National Institute of Standards and Technology (NIST) con la colaboración de la National Security Agency (NSA). Sólo están obligadas a utilizarlo las compañías que mantienen negocios con el gobierno americano, y muchas prefieren no hacerlo porque es un sistema exclusivamente de firma. El NIST eligió esta solución limitada, porque el gobierno de EE.UU. pretende desalentar el uso de cualquier software de cifrado que cercene su capacidad para fisgonear en asuntos ajenos.

El software que sólo proporciona autentificación, como el DSS, puede exportarse libremente en los productos, mientras que el software que emplea RSA para cifrado general está sometido a severas restricciones.