El ABC de los documentos electrónicos seguros

Ignacio Mendívil

Índice

El ABC de los Documentos Electrnicos Seguros

BORRADOR - DOCUMENTO EN PROCESO

7 de octubre de 1999

Ignacio Mendvil
SeguriData

INTRODUCCION

Dos problemas aquejan a los documentos electrónicos : La Confidencialidad y la Autenticidad.

La confidencialidad se refiere a la capacidad de mantener un documento electrónico inaccesible a todos, excepto a una lista determinada de personas. La autenticidad se refiere a la capacidad de determinar si una lista determinada de personas han establecido su reconocimiento y/o compromiso sobre el contenido del documento electrónico. El problema de la autenticidad en un documento tradicional se soluciona mediante la firma autógrafa. Mediante su firma autógrafa, un individuo, o varios, manifiestan su voluntad de reconocer el contenido de un documento, y en su caso, a cumplir con los compromisos que el documento establezca para con el individuo.

Existe una diferencia sutil pero muy importante entre el concepto de autenticidad y el concepto de no-repudiación. Por ejemplo usted puede presenciar que un documento fue escrito por alguien pues lo vio en persona. Si el documento no esta firmado autógrafamente usted estará absolutamente convencido de su autenticidad pero no podrá probarlo pues sin la firma autógrafa es imposible establecer el vinculo entre la voluntad de la persona y el contenido del documento. Si se puede probar a terceros que efectivamente el documento es autentico entonces se dice que el documento es no-repudiable. Si un documento es no-repudiable es autentico pero no viceversa.

Una característica básica de un documento autentico es su integridad. En un documento tradicional como un contrato o cheque, si se aprecian modificaciones o tachones el documento es prácticamente invalidado. En un documento electrónico en donde por errores de transmisión o fallas en el medio de almacenaje o intencionadamente se modifica el contenido original del documento entonces el documento pierde su integridad y por tanto su autenticidad. Si un documento es autentico entonces es integro pero no viceversa.

Estos problemas, confidencialidad, integridad, autenticidad y no-repudiación se resuelven mediante la tecnología llamada ¨Criptografía¨. La criptografía es una rama de las matemáticas, que al aplicarse a mensajes digitales, proporcionan las herramientas idóneas para solucionar los problemas antes mencionados. Al problema de la confidencialidad se le relaciona comúnmente con técnicas denominadas de "encripción" y el problema de la autenticidad mediante técnicas denominadas de "firma digital", aunque ambos en realidad se reducen a procedimientos criptográficos de encripción y desencripción.

La criptografía en realidad no es solo una rama de las matemáticas sino una disciplina que puede reunir otras áreas de la ciencia sin embargo es en las matemáticas en donde la criptografía moderna encuentra los fundamentos más trascendentes. En general la criptografía es el uso de problemas de difícil solución a aplicaciones especificas. Por ejemplo un problema de difícil solución es encontrar los factores de un número que es producto de dos números primos. Cómo podemos aplicar este problema de difícil solución a un caso especifico es un asunto del campo de la criptografía. En particular cómo podemos aplicar este problema de difícil solución al tema de la confidencialidad de información digital es un asunto de la criptografía. El fundamento y los procedimientos de operación para efectivamente dar solución a un problema especifico constituyen un criptosistema.

El criptoanálisis es la actividad que se encarga de estudiar las debilidades de un criptosistema y su objetivo es el de encontrar soluciones fáciles al reto implantado en el criptosistema.

Ambas actividades, la criptografía y el criptoanálisis son parte de la disciplina denominadacriptología.

En un sistema en donde la forma tradicional de realizar operaciones comerciales esta siendo reemplazado por métodos electrónicos resulta de suma importancia contar no solo con la tecnología, sino con un marco legal que norme la validez de los documentos electrónicos. Es importante que en nuestro país contemos con una base legal que conceda, a los documentos firmados digitalmente, un tratamiento similar a la de los documentos tradicionales firmados autógrafamente. El problema de la confidencialidad no es tampoco un problema estrictamente técnico también es conveniente estudiar las implicaciones legales del uso de esta tecnología que permite al individuo mantener información confidencial fuera del alcance del Estado, sea esta información licita o ilícita.

Este documento tiene como objetivo presentar, con un enfoque no técnico, los principios y principales problemas en el uso de las técnicas criptográficas en la solución de los problemas de confidencialidad y autenticidad de documentos electrónicos. La idea es que sirva de marco de referencia para que técnicos y no técnicos tengamos una idea clara del problema. Un problema de este tipo requiere del trabajo interdisciplinario de criptógrafos, analistas, especialistas en seguridad de datos, abogados, etc.

El documento se divide en dos partes. La primera parte esta dedicada al problema de la **no-repudación** de los documentos electrónicos, la segunda esta dedicada al problema de la **confidencialidad**.

FIRMA DIGITAL DE DOCUMENTOS DIGITALES
CONCEPTOS

A mediados de la década de los setenta dos matemáticos de la Universidad de Standford y otros del Instituto Tecnológico de Massachusetts, descubrieron que al aplicar algunas fórmulas y conceptos matemáticos, era posible solucionar la problemática de la confidencialidad y autenticidad de la información digital. A este conjunto de técnicas se les denomino como la Criptografía de Llave Pública. El modelo de llave pública mas conocido y utilizado mundialmente es el denominado RSA por las siglas de los apellidos de los descubridores Rivest, Shamir y Adelman. El esquema propuesto en RSA consiste en lo siguiente.

Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denomina llaves. Una llave es un número de gran tamaño, que usted lo puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes.

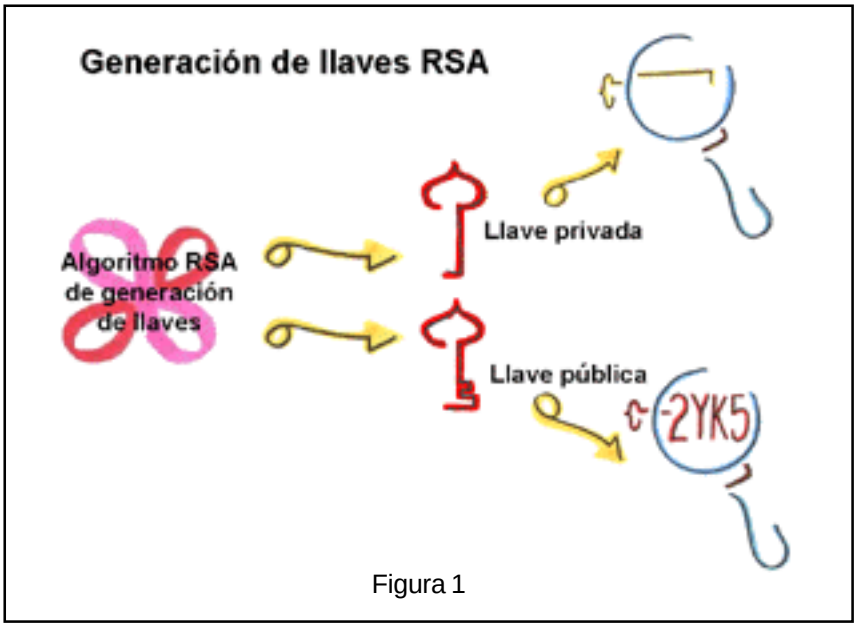

Figura 1

Las llaves pública y privada tienen características matemáticas, su generación es siempre en parejas, y están relacionadas de tal forma que si dos llaves públicas son diferentes, entonces,las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes.

La idea es la de que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la pude dar a conocer a los demás individuos.

El procedimiento de firmado consiste en que mediante un programa de cómputo, un sujeto alimenta un documento a firmar y su llave privada (que solo el conoce). El programa produce como resultado un mensaje digital denominado firma digital. Juntos, el documento y la firma constituyen el documento firmado.

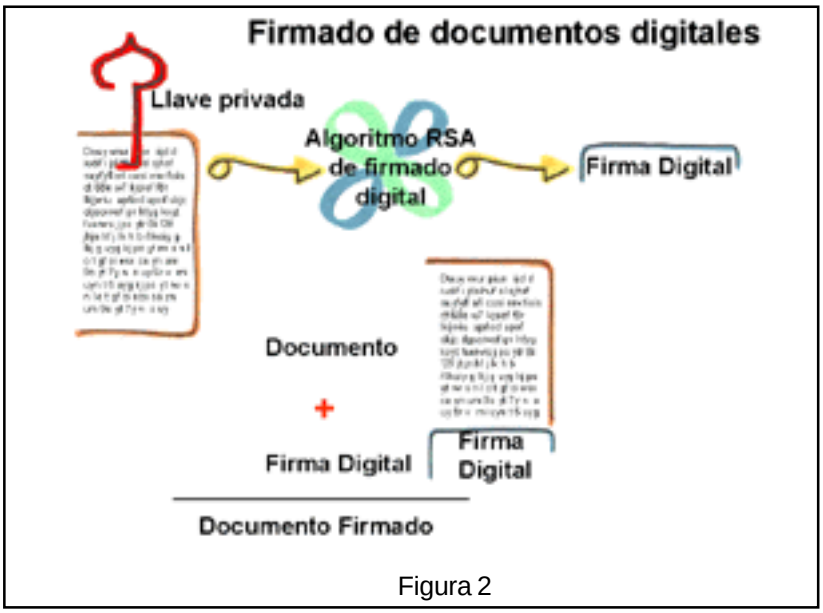

Figura 2

Es conveniente señalar que, a diferencia de la firma autógrafa, si dos documentos son diferentes entonces la firma digital es diferente. En otras palabras la firma digital cambia de documento a documento, si un sujeto firma dos documentos diferentes producirá dos documentos firmados diferentes. Si dos sujetos firman un mismo documento, también se producen dos diferentes documentos firmados.

El proceso de autenticación consiste en que mediante un programa de computo se alimenta un documento firmado y la llave pública del supuesto firmante, el programa indica si es autentico o no es autentico.

Figura 3

Es conveniente señalar que si la parte del documento o la parte de la firma es modificado, aunque sea ligeramente, entonces, el procedimiento de autenticación indicará que el documento no es autentico. Si una llave pública autentica un documento firmado, entonces quiere decir que el documento fue firmado con la correspondiente llave privada. La siguiente figura ilustra lo anterior, en donde el símbolo x indica una alteración.

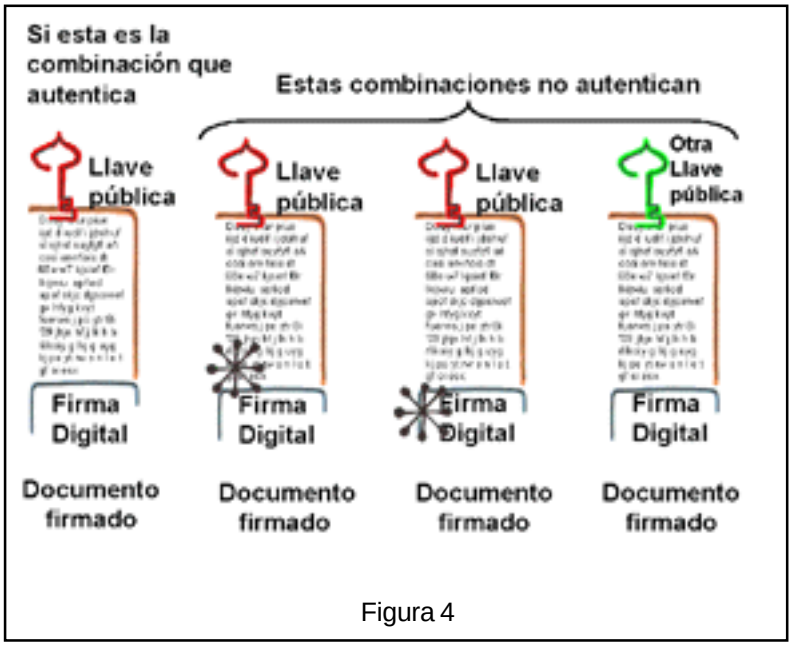

Figura 4

Lo anterior se puede resumir en lo siguiente: Si un documento firmado autentica con una determinada llave pública, entonces, el documento fue firmado con la correspondiente llave privada. Es decir, si un individuo tiene asociada la llave pública que autentica el documento, entonces, el documento fue efectivamente firmado por ese individuo. En realidad, a diferencia de la firma autógrafa la cual es una biometría y efectivamente prueba el acto personal de firmado, la firma digital solo prueba que se utilizó la llave privada del sujeto y no necesariamente el acto personal de firmado. En consecuencia, no es posible hacer irrefutable el que un individuo firmó un documento, en realidad tenemos que hacer irrefutable que es el individuo el responsable de que el documento hubiese sido firmado con su llave privada. En otras palabras, si un documento firmado autentica con la llave pública de un sujeto, entonces el sujeto, aunque no lo haya hecho, debe de reconocer el documento como autentico. Por lo tanto el sujeto debe de responsabilizarse de mantener su llave privada en total secreto y no revelársela a nadie, pues de hacerlo se vuelve responsable del mal uso de la misma.

Es claro que un sujeto, en el proceso de autenticar un documento firmado debe de contar con, digamos un archivo, que contiene la llave pública del supuesto firmante. Es decir, el sujeto que autentique documentos firmados por 10 individuos deberá contar con 10 archivos o con una base de datos conteniendo las 10 llaves públicas de los posibles firmantes. Si este número lo aumentamos a 100, 1000 o a un 1,000,000 el problema crece considerablemente. Una solución a este problema de manejo de llaves se basa en el concepto conocido como Certificado Digital.

EL CERTIFICADO DIGITAL

El Certificado Digital es en si un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificadora, dicho documento establece una liga entre un sujeto y su llave pública. Es decir, el Certificado Digital es un documento firmado por la Autoridad Certificadora (AC), el documento contiene el nombre de un sujeto y su llave pública.

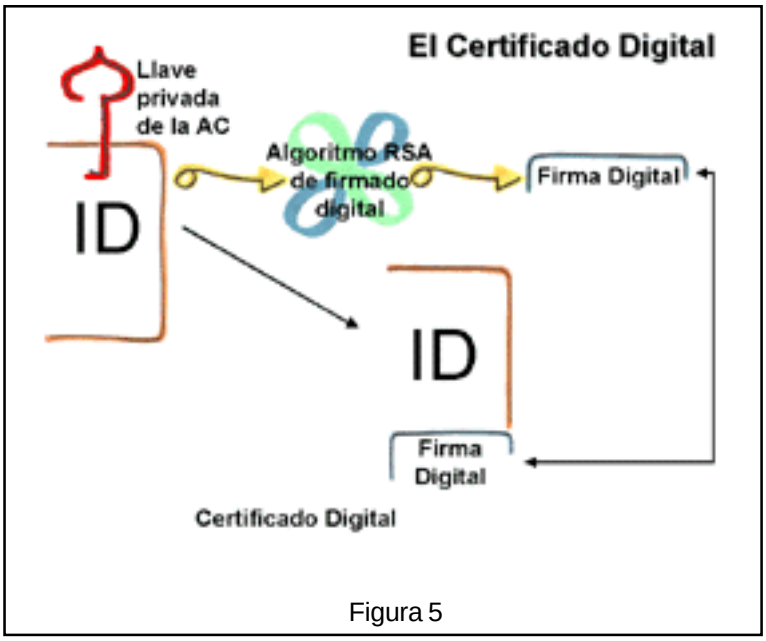

Figura 5

La parte señalada como ID contiene el nombre de un sujeto y de su llave pública, como se ilustra en la siguiente figura.

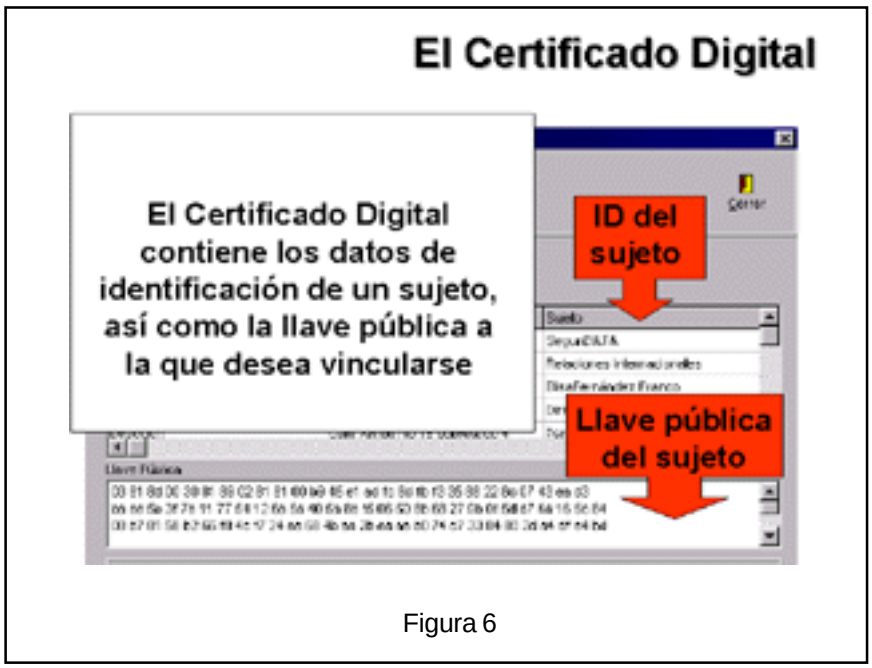

Figura 6

La idea es que quienquiera que conozca la llave pública de la AC puede autenticar un Certificado Digital de la misma forma que se autentica cualquier otro documento firmado, como se ilustra en la siguiente figura.

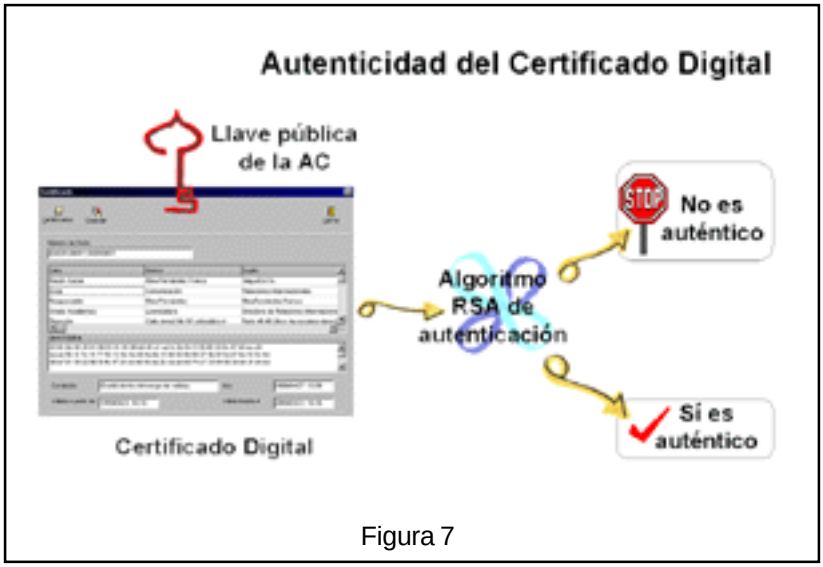

Figura 7

Si el Certificado es auténtico y confiamos en la AC, entonces, podemos confiar en que el sujeto identificado en el Certificado Digital posee la llave pública que se señala en dicho certificado. Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la llave pública de la AC podrá autenticar el documento, como se ilustra en la siguiente figura.

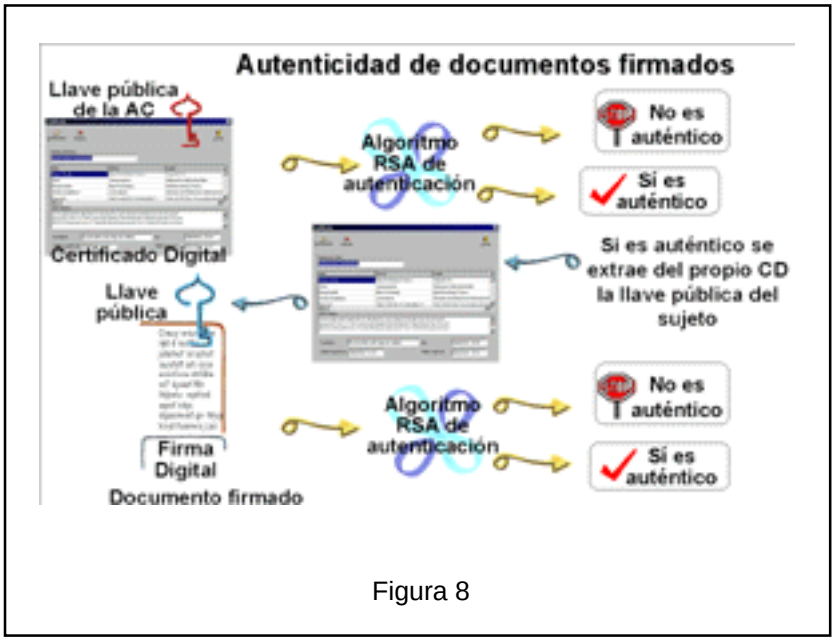

Figura 8

Por varias razones es conveniente que los Certificados Digitales tengan un periodo de validez, este parece ser un principio básico en la emisión de cualquier tipo de identificación. Existe otra razón de carácter técnico y se refiere a que de vez en vez es conveniente que el usuario renueve sus llaves, cada vez aumentando ligeramente el tamaño.

El carácter perecedero de las llaves da como resultado otra diferencia notable entre la firma digital y la firma autógrafa, la cual tiene un carácter perenne. Sin embargo, en el sistema tradicional de escrito firmado autógrafamente también existe el problema de autenticar un escrito, no solo en el contexto, de autenticar la firma autógrafa, sino además autenticar la capacidad del sujeto para comprometerse al contenido del mismo. Por ejemplo un escrito tradicional, que compromete a una persona moral, es valido solo si la persona física que lo firma tiene la capacidad legal para comprometer a la persona moral. Una persona física que compromete a una moral, debe pues, contar con poderes legales para tal efecto, dichos poderes pueden tener una caducidad o pueden incluso ser revocados o anulados.

El estándar, internacionalmente aceptado, para Certificados Digitales, es el denominado X.509de la CCITT. Los campos básicos del certificado X.509 se ilustran en la siguiente figura.

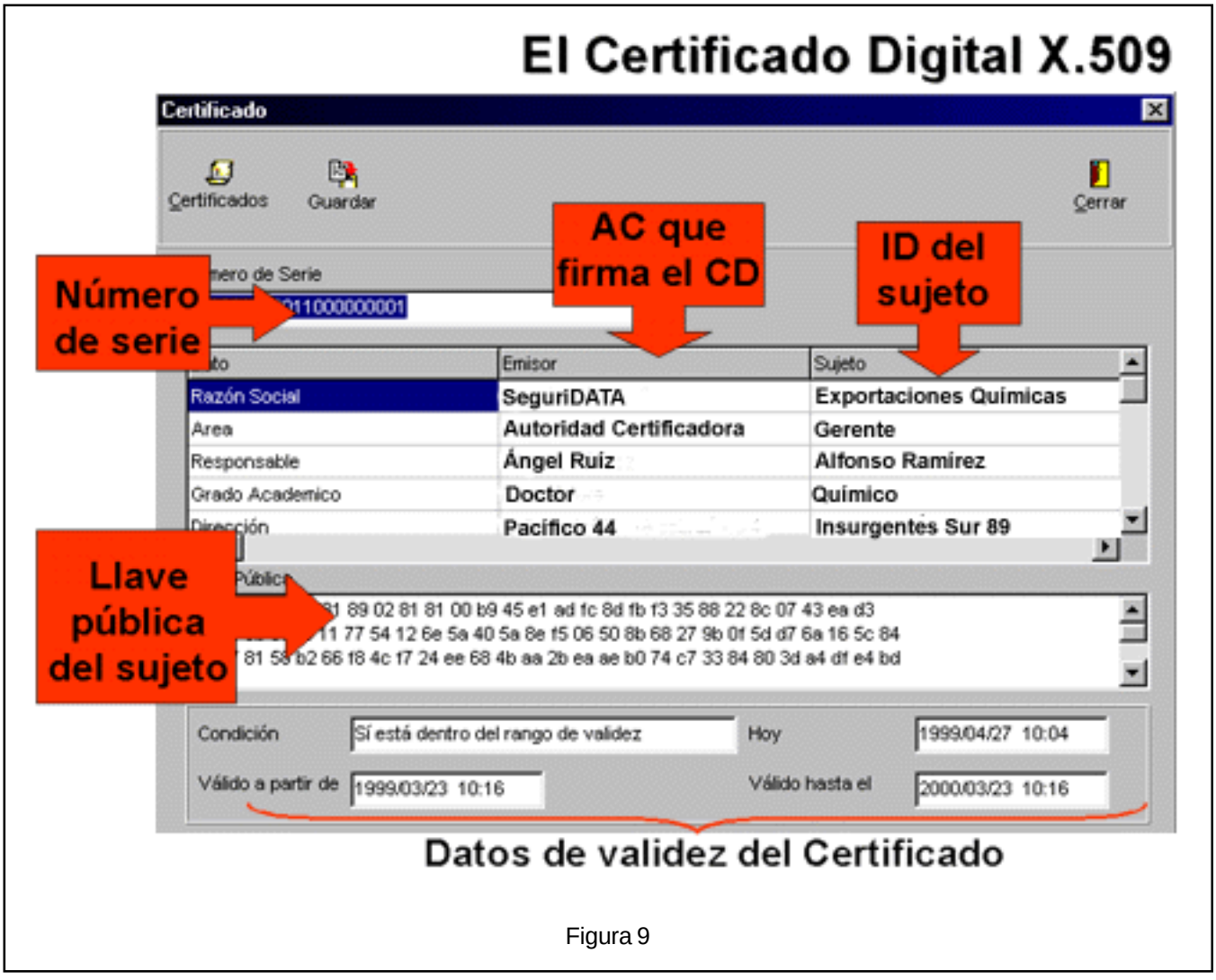

Figura 9

El número de serie es un número asignado por la Autoridad Certificadora y tiene el objeto de identificar unívocamente a cada certificado emitido por dicha AC. Por otra parte, debido a que las operaciones electrónicas se pueden realizar entre puntos geográficos muy diferentes, con diversidad de horarios, las fechas a las que hacemos referencia en este documento, estarán expresadas en la notación conocida como Tiempo Universal Coordinado (UTC) o Tiempo del Meridiano de Greenwich. Una fecha en formato UTC, contiene el año, mes, día, hora, minutos y segundos siempre en relación a la hora del meridiano de Greenwich.

LA LISTA DE CERTIFICADOS REVOCADOS O CRL

Ahora bien, si observamos la figura 8, que nos ilustra el procedimiento de autenticación, y en virtud de la necesidad de verificar que un certificado no este revocado, es evidente la necesidad de contar con un archivo, directorio o base de datos que contengan los certificados revocados y por cada uno de ellos la fecha y hora a la que fueron revocados. Una primera aproximación a este directorio de certificados revocados es la conocida como "Lista de Certificados Revocados" o CRL por sus siglas en ingles. Un CRL es un archivo, firmado por la Autoridad Certificadora, que contiene la fecha de emisión del CRL y una lista de certificados revocados, cada uno de ellos con la fecha de revocación. Con el objeto de ahorrar espacio, no se incluye todo el certificado sino únicamente su número de serie (Ver figura 9). El CRL se ilustra en la siguiente figura.

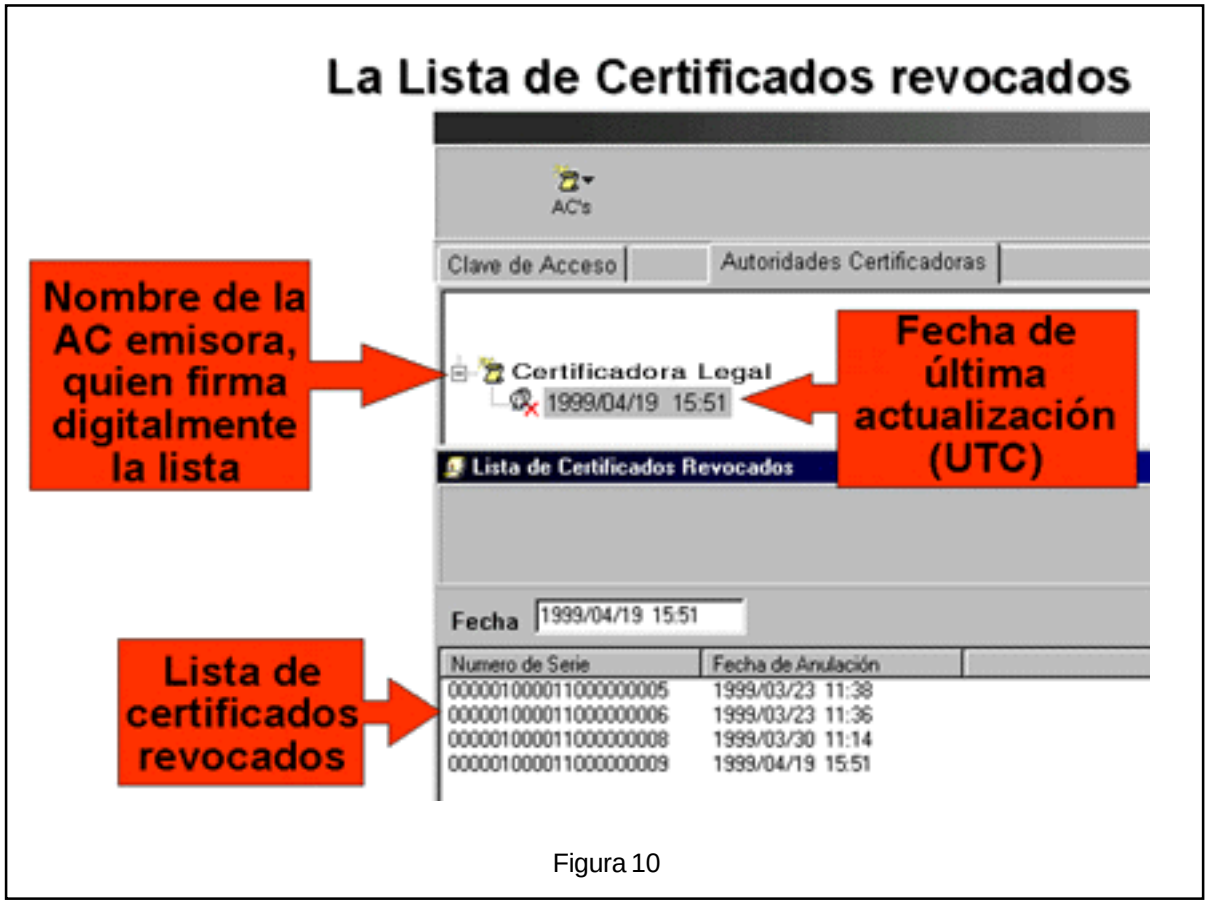

Figura 10

Un CRL puede ser autenticado como cualquier otro documento firmado digitalmente, en este caso con la llave pública de la Autoridad Certificadora. Una vez autenticado, podemos confiar en su contenido y determinar con certeza si un certificado esta revocado o no, esto es hasta la fecha definida por "Ultima Actualización". El CRL es muy útil en algunos casos, por ejemplo :

1.- El sujeto A recibió un documento firmado por el sujeto B el día 13 de Marzo de 1997.
2.- Autentica el documento de acuerdo al procedimiento ilustrado en la figura 8 y resulta autentico.
3.- La AC pública el CRL diariamente de manera que el sujeto A obtiene, al siguiente día,una copia del CRL cuya fecha UTC es la 0 horas del día de 14 de Marzo de 1997, laautentica con la llave pública de la AC.
4.- El sujeto A extrae, del certificado del sujeto B, el número de serie de dicho sujeto.
5.- Consulta el CRL para determinar si el número de serie de B se encuentra listado en él.

En caso de encontrar que, el número de serie de B, si esta en el CRL, entonces, el sujeto A no puede confiar en el documento firmado, en caso contrario, el sujeto A si puede confiar en él.

Ahora bien, supongamos que el sujeto B, revoca su certificado el día 15 de Marzo de 1997 y refuta la validez del documento el día 17 de Marzo de 1997. Nótese que el número de serie del certificado del sujeto B aparece en el CRL del día 16. Cuales serían entonces los elementos de prueba que el sujeto A tendría que demostrar :

1.- Que el documento recibido, es autentico, de acuerdo al procedimiento de la figura 8.
2.- Que al 14 de Marzo de 1997, el certificado del sujeto B no había sido revocado, mediante el CRL de ese día.
3.- Que recibió el documento antes del 14 Marzo de 1997.

Los puntos 1 y 2 son fácilmente demostrables por el sujeto A, pero el punto 3 no, aun cuando la fecha del firmado del documento este explícitamente descrito en el cuerpo del documento. En un documento tradicional firmado autógrafamente, en donde la fecha del documento es normalmente expresada en el cuerpo del escrito, y el firmante expresa con su firma la aceptación de dicha fecha, como aquella en la que el documento es firmado. Nótese que el que un documento firmado este fechado, esto no significa que el documento fue firmado en esa fecha sino solo la voluntad del firmante para reconocerla como la fecha en la que se firmo el documento. En los documentos electrónicos firmados digitalmente el problema es mas complejo puesto que el sujeto B puede argumentar que el documento fue hecho en forma apócrifa después del día 15 y simplemente se especifico Marzo 13 como la fecha de firmado. La solución a este problema se le conoce como "Recibo Electrónico" o simplemente Recibo.

El recibo es un documento firmado digitalmente que contiene un mensaje y a continuación contiene una fecha. Al firmante del recibo le llamaremos "Emisor del Recibo". Supongamos que el emisor del recibo es una persona o entidad en la que todos confiamos y de la que conocemos su llave pública. A esta persona o entidad le denominaremos "**Autoridad de Oficialía de Partes**" y su función es la de recibir mensajes electrónicos, concatenarles la fecha actual, y el resultado se firma con su llave privada. El resultado es una prueba de que un mensaje electrónico existió a una determinada fecha como se ilustra en la siguiente figura.

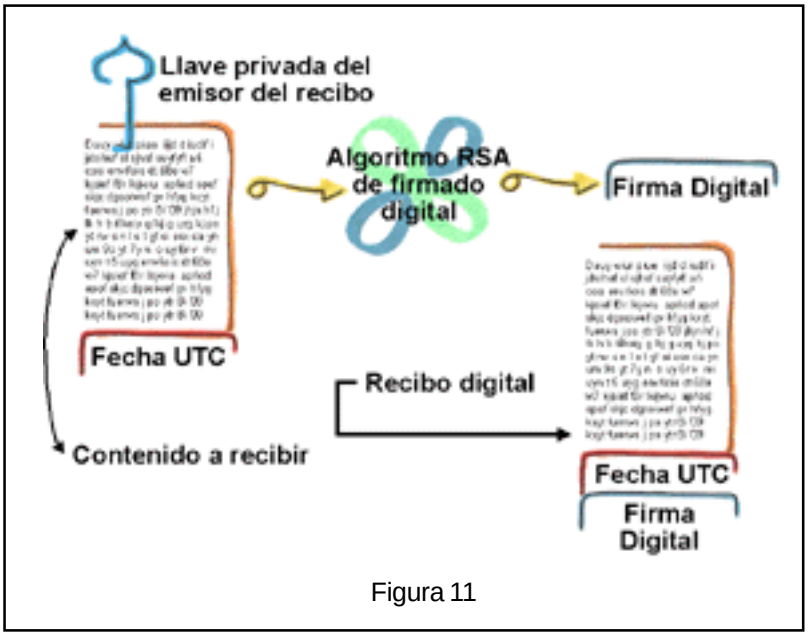

Figura 11

Ahora bien, que pasa si el sujeto A es quien refuta haber recibido dicho documento. Entonces el sujeto B tiene que probar :

1.- Que el sujeto A recibió el día 13 de Marzo el documento firmado.
2.- Que dicho documento firmado es autentico de acuerdo al procedimiento descrito en la figura 8.
3.- Que al menos al día 14 de Marzo, su número de serie no aparecía en el CRL.

Para probar el punto 1, parece irremediable que el sujeto B requiere de un recibo del sujeto A atestiguando el documento recibido con la fecha del 13 de Marzo. El punto 2, se prueba mediante el documento firmado, y el punto 3 mediante el CRL del día 14 o posterior. Hay un aspecto adicional y se refiere a que el recibo del sujeto A es, en sí, un documento firmado que exige el mismo tratamiento que se le dió al documento firmado por B y recibido por A. El círculo se rompe, sin embargo pues, el sujeto B puede autenticar el recibo de A y solicitar a la AOP un recibo atestiguando el recibo de A. Un flujo mas sencillo y seguro es el que se ilustra en la siguiente figura.

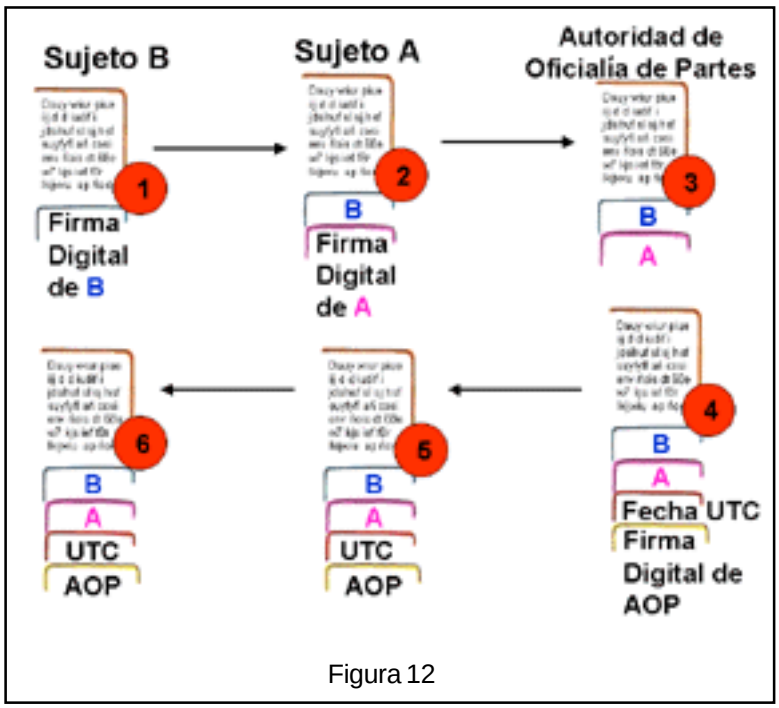

Figura 12

En la figura 12 observamos los siguientes procedimientos :

1.- El sujeto B firma un documento y se lo envía al sujeto A.
2.- El sujeto A firma el documento firmado en 1 y se lo envía a la Autoridad de Oficialía de Partes.
3.- La AOP recibe el contenido a atestiguar.
4.- La AOP agrega la fecha UTC, firma el recibo y se lo envía al sujeto A.
5.- El sujeto A recibe de la AOP el recibo, guarda una copia y se lo transmite al sujeto B
6.- El sujeto B guarda una copia del recibo de la AOP.

PRUEBAS POSIBLES PARA DETERMINAR LA AUTENTICIDAD

El recibo de la AOP y un CRL de fecha posterior a la fecha de emisión, se convierten en pruebas necesarias y suficientes para ambos sujetos, como se ilustra en la siguiente figura.

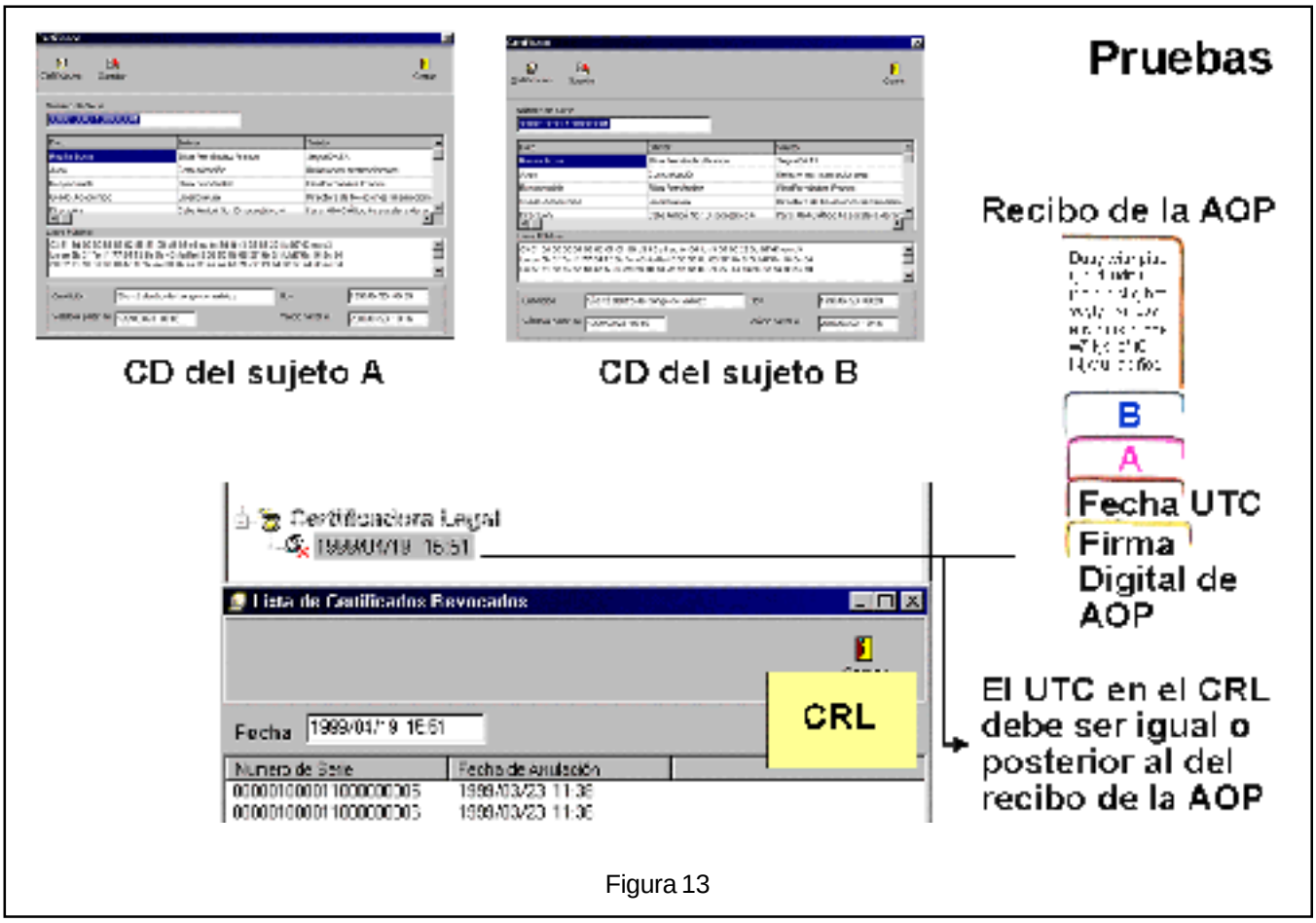

Figura 13

El procedimiento de prueba se ilustra en la siguiente figura.

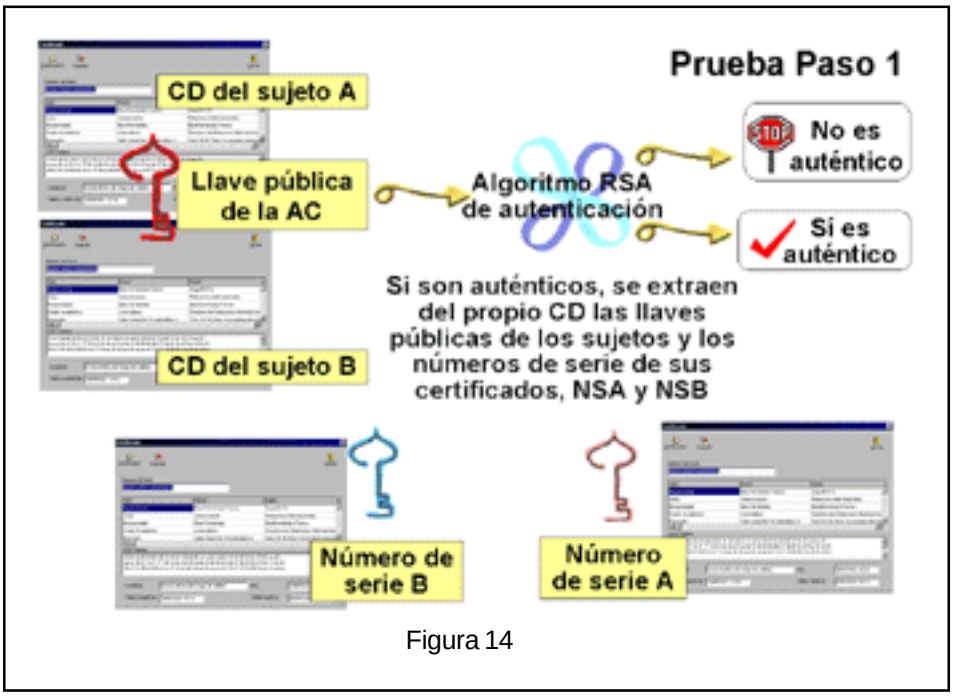

Figura 14

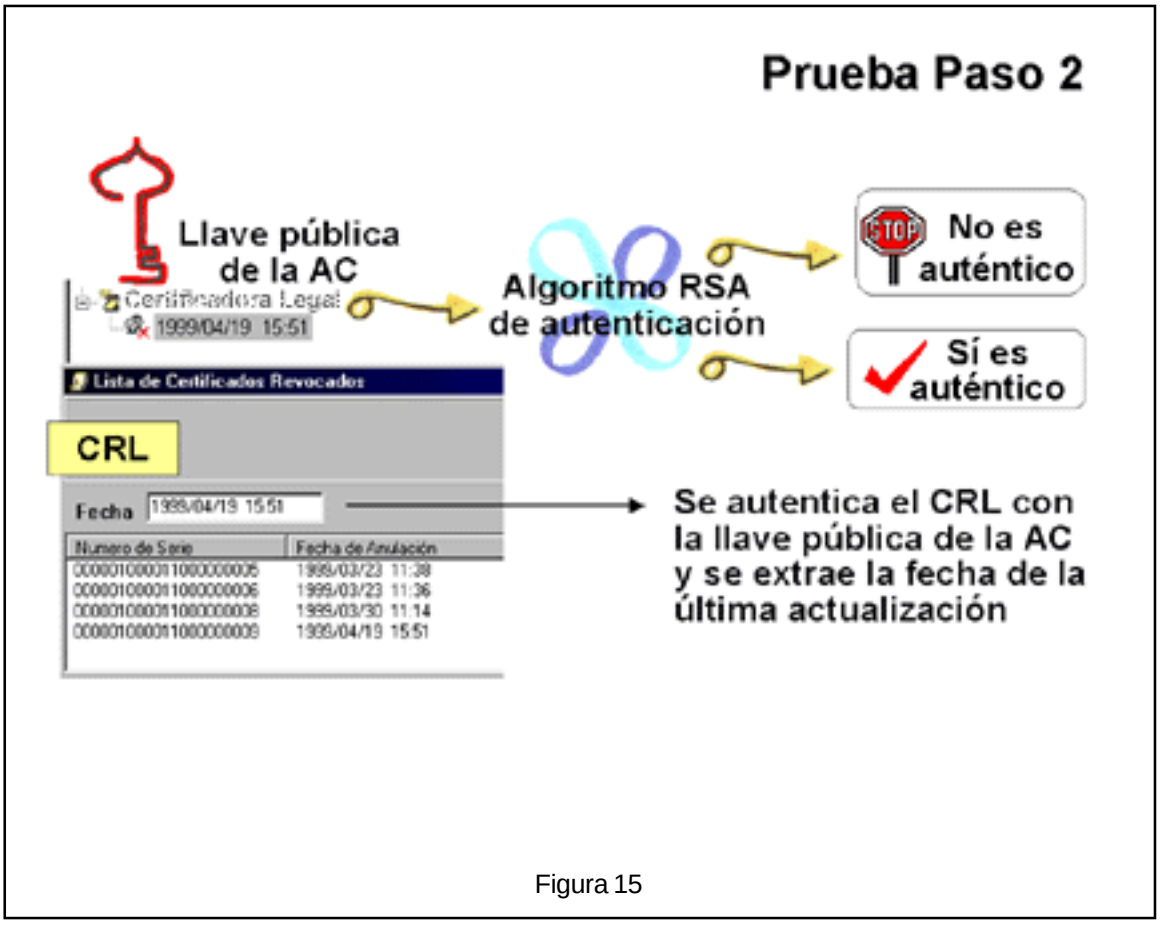

Figura 15

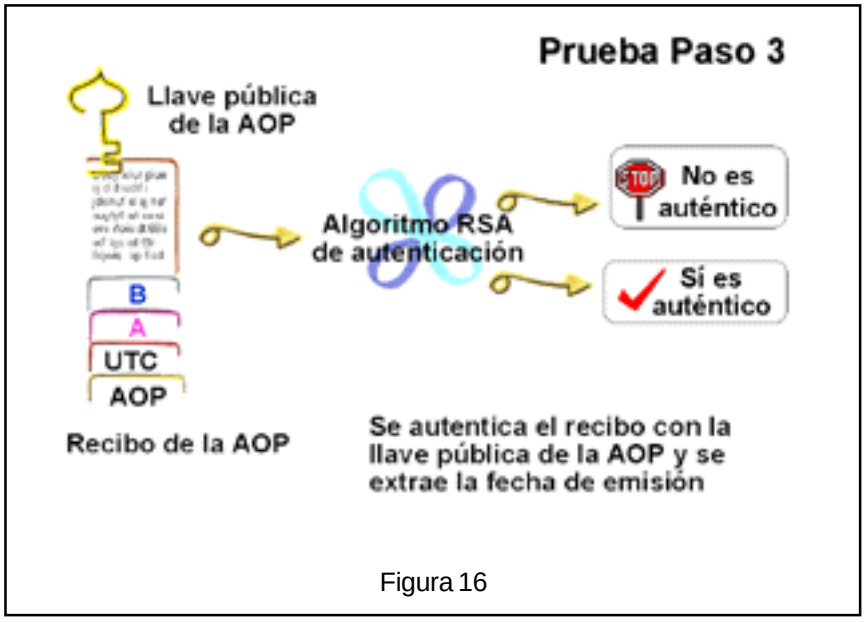

Figura 16

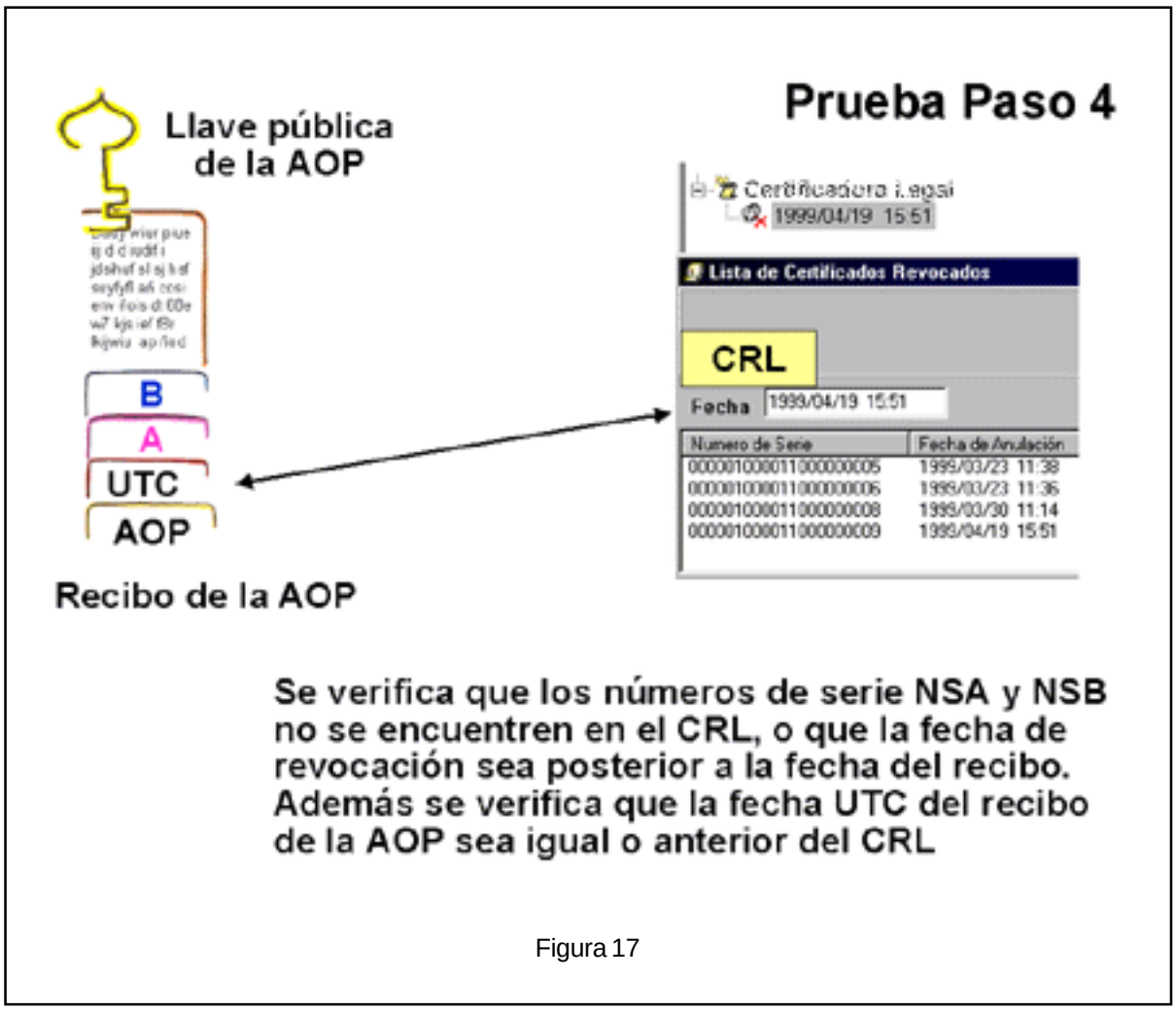

Figura 17

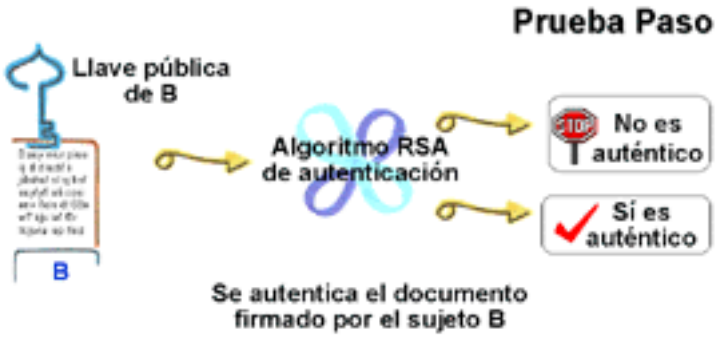

Figura 18

Figura 19

El uso de un CRL en procesos de autenticación, es adecuado sólo cuando el CRL tiene una fecha UTC igual o posterior a la fecha UTC que se pretende usar como referencia en la validez del documento, como se ilustra en el procedimiento de prueba de la figura 17. En aquellas ocasiones en que se requiere autenticar operaciones en el instante mismo en que son realizadas el uso del CRL es inadecuado. También puede resultar inadecuado que el CRL sea de un tamaño tal, que la transmisión o manejo resultasen en procesos lentos.

Esto es particularmente importante para aplicaciones del sector financiero, en donde se debe de actuar de inmediato ante el intercambio electrónico de transacciones financieras. La solución a este problema la ofrecen los denominados servicios de directorio o servicio de consulta de certificados.

Servicios de Directorio o de Consulta de Certificados

Los servicios de directorio o de consulta de certificados deben ser ofrecidos por un ente o persona en la que todos confiamos y que ofrece servicios electrónicos de consulta a un CRL actualizado al instante. Este ente recibe solicitudes de consulta sobre el estado de revocación de un Certificado Digital y responde indicando si está o no revocado, en caso de estar revocado, proporciona la fecha UTC de revocación del certificado. El procedimiento se ilustra en la siguiente figura.

Figura 20

Un documento firmado por un Servicio de Directorio que da "fe" de que un certificado no esta revocado en ese instante, es un mecanismo que asegura a quien hace la consulta que puede confiar en ese certificado ante cualquier autenticación de referencia a una fecha UTC igual o anterior a la fecha UTC que indica el Servicio de Directorio.

Es conveniente mencionar que el documento del Servicio de Directorio no necesariamente se tiene que guardar como prueba, pues en caso de disputa se puede recurrir a un CRL posterior a la fecha UTC de referencia. Es incongruente que habiendo respondido el Servicio de Directorio que un certificado era "NO REVOCADO" en una fecha X, ese certificado apareciese en un CRL posterior como revocado con fecha de revocación igual o anterior a X.

AUTORIDAD REGISTRADORA

Como se puede apreciar en las secciones anteriores, una de las principales funciones de la **Autoridad Certificadora** es la de precisamente "dar fe digital" de la liga entre el sujeto y su llave pública. Es lógico pensar que el procedimiento consiste en que el sujeto pruebe su identidad y, en caso de representar a una persona moral, los poderes legales para hacerlo. Además el sujeto debe de manifestar su voluntad de aceptar su llave pública y probar (mediante autofirmado de un mensaje) que es propietario de la correspondiente llave privada. Además de la documentación sustentadora es conveniente que el sujeto entregue a la AC un documento electrónico conteniendo sus datos y su llave pública. A dicho documento le denominaremos "**Requerimiento de Certificación**".

En principio, se propone que el proceso de certificación, sea un procedimiento que requiera de la presencia física del sujeto, junto con la documentación sustentadora y un **requerimiento de certificación**. Sin embargo la AC presentada es una sola persona o entidad, esto significaría que los sujetos deberían de presentarse ante esta persona o entidad. Esto no es viable, pues los servicios electrónicos se prestan entre puntos geográficamente separados.

La solución a este problema son las denominadas "**Autoridades Registradoras**". Una **Autoridad Registradora** es una persona o entidad autorizada por la AC y la auxilia en el procedimiento de "dar fe" de que los requisitos que un sujeto tiene que satisfacer sean satisfechos de acuerdo a un procedimiento establecido.

PROCESO DE CERTIFICACIÓN COMPLETO

En un primer paso, el sujeto genera su par de llaves en la intimidad de su computadora, construye además el requerimiento de certificación, que incluye la llave pública recién generada. El requerimiento de certificación es un documento autofirmado o firmado por el sujeto mismo. Como se verá mas adelante una Autoridad Registradora tiene la responsabilidad de autenticar el requerimiento y por tanto, obtener prueba de que el sujeto es propietario de la correspondiente llave privada.

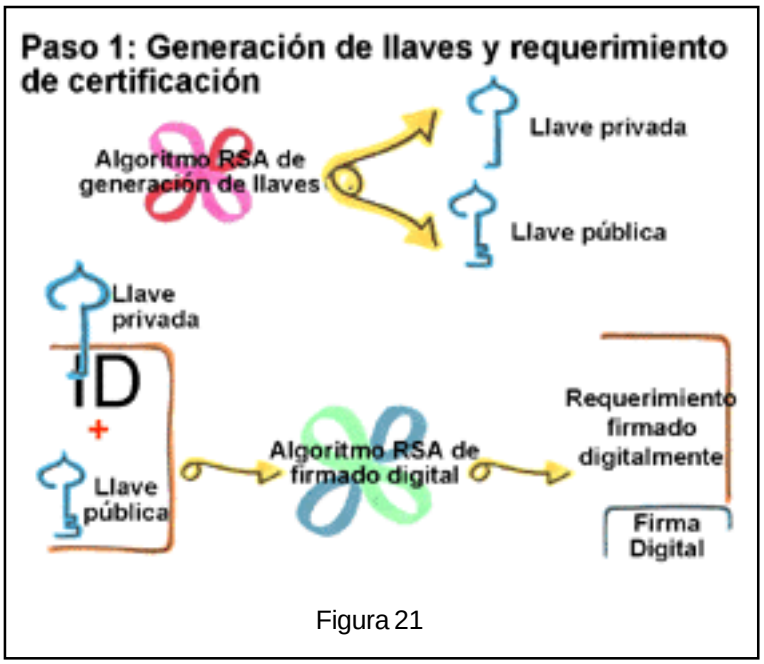

Figura 21

En el segundo paso, el sujeto se presenta ante una Autoridad Registradora y presenta su requerimiento de certificación y documentación sustentatoria. El programa de computo la Autoridad Registradora, extrae la llave pública que desea ostentar el sujeto, y autentica el requerimiento para demostrar que fue firmado con la correspondiente llave privada. Adicionalmente, verifica que la documentación sustentatoria es suficiente para acreditar la personalidad que el sujeto desea ostentar en el certificado.

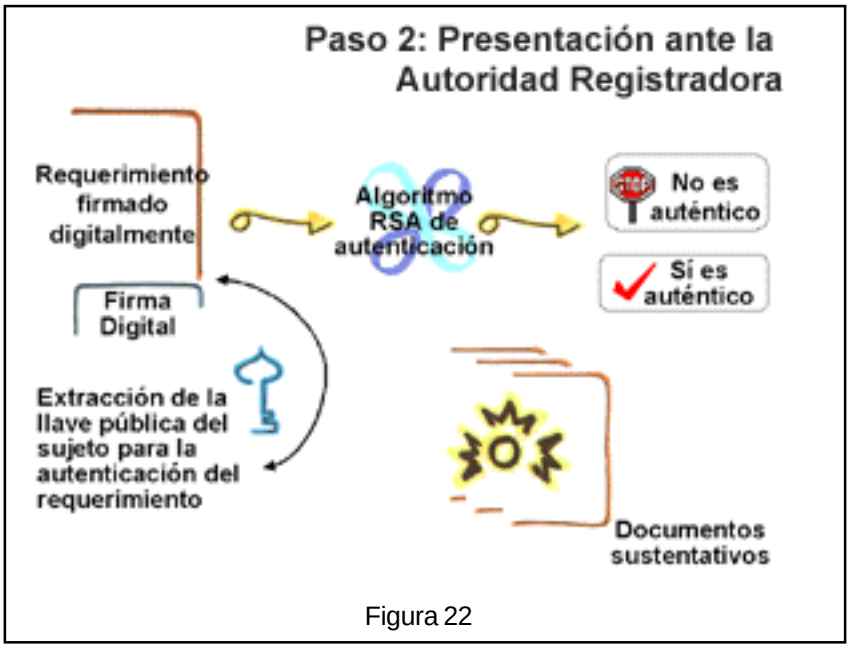

Figura 22

En el paso 3, la Autoridad Registradora firma con su llave privada el Requerimiento de Certificación como indicación a la Autoridad Certificadora de que ella ha verificado la correcta sustentación del certificado.

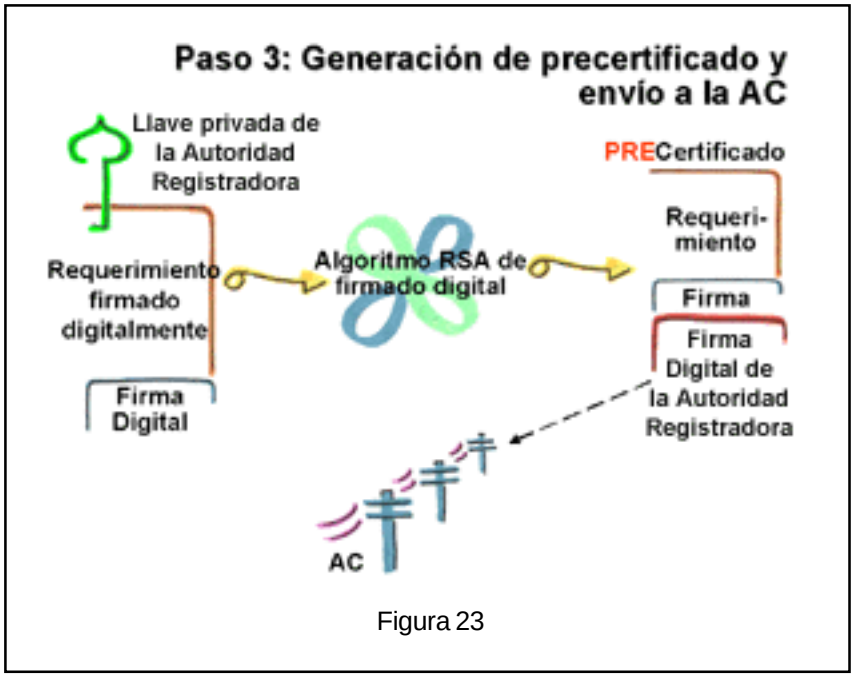

Figura 23

En el paso 4, la Autoridad Certificadora autentica que el precertificado provenga de una de las Autoridades Registradoras con las que colabora. Produce un nuevo certificando, estampando su nombre (de la AC), el número de serie y el periodo de validez. Así genera un nuevo certificado.

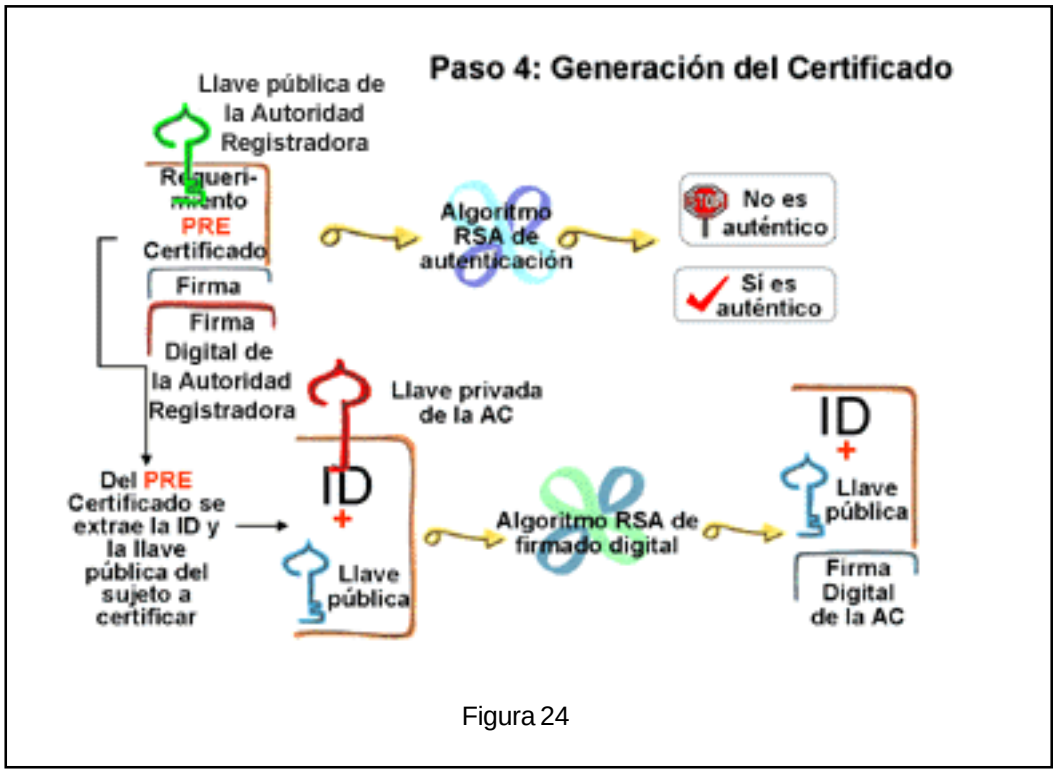

Figura 24

CONFIDENCIALIDAD

La criptografía ofrece dos tipos de algoritmos de confidencialidad: los simétricos y los asimétricos o de llave pública. La idea de los algoritmos simétricos es encriptar, es decir, codificar un mensaje o documento digital y producir un documento "ilegible" utilizando como base una palabra clave o contraseña como se ilustra en la siguiente figura. Usualmente, mediante un programa de computo, el sujeto A alimenta un algoritmo de encripción con un documento y teclea una palabra clave digamos "abcxyz". El resultado es un documento encriptado que le hace llegar al Sujeto B. El sujeto B toma el documento y lo alimenta a un algoritmo de desencripción con la palabra clave "abcdxyz" y obtiene como resultado el documento original.

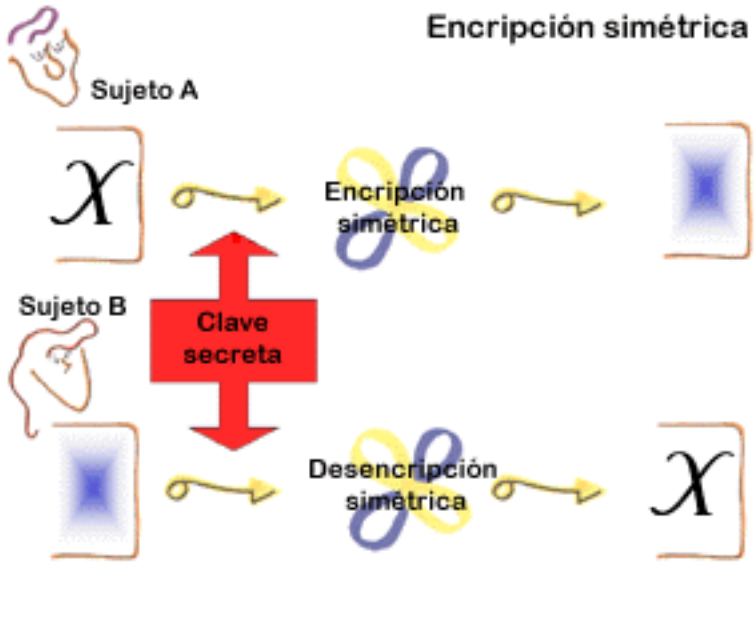

Figura 25

Observe que ambos sujetos comparten el secreto de la palabra clave "abcxyz". Si el sujeto A desea mantener intercambio electrónico de información encriptada con un sujeto C que no pueda leer los documentos confidenciales intercambiados con B, entonces el sujeto A tendría que acordar otra clave secreta con el sujeto C, digamos "qwerty". El hecho de que los individuos tengan que acordar claves secretas con el conjunto de individuos con los que desea mantener intercambio confidencial de información resulta en un manejo poco práctico. Una mejor solución la ofrece la criptografía de llave pública.

La criptografía de llave pública ofrece algoritmos de encripción y desencripción. Si un documento se encripta con una llave pública, entonces, solo se desencripta con la correspondiente llave privada. En algunos algoritmos como RSA, también sucede a la inversa, lo que se encripta con la llave privada solo se desencripta con la llave pública. El proceso de encripción con llave pública se ilustra a continuación.

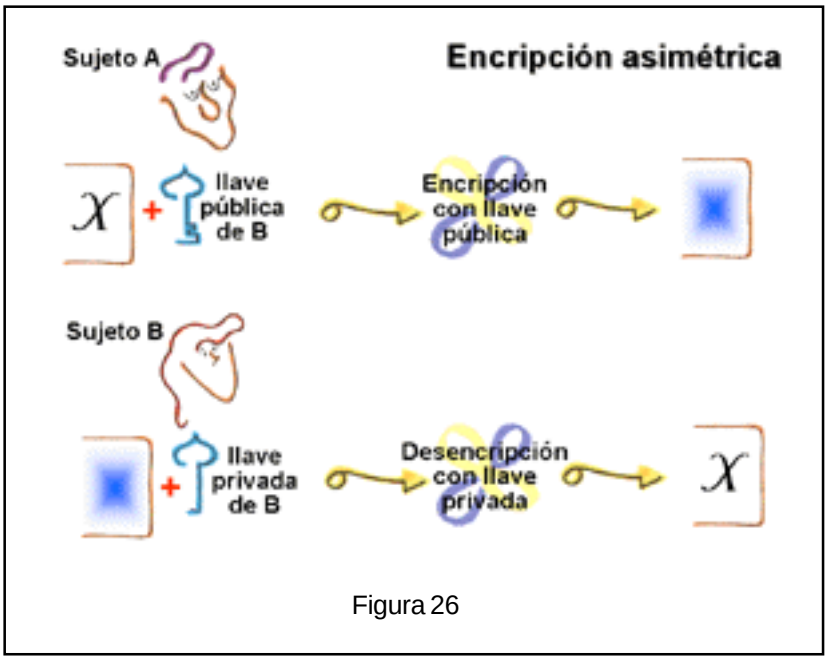

Figura 26

Observe que una vez encriptado el documento, solo el sujeto B, ni siquiera el sujeto A puede accesar el documento encriptado.

En la practica, no es conveniente encriptar todo el documento mediante algoritmos de llave pública. Una razón es la velocidad de los algoritmos de llave pública que son en el orden de 100 veces mas lentos que algoritmos simétricos. Además, algunos algoritmos de clave pública pueden ser sujetos de ataques matemáticos cuando son utilizados de esta forma. Otra razón es que si un sujeto desea encriptar un documento para digamos, cinco sujetos B,C,D,E y F, entonces tendrá que producir 5 archivos diferentes, uno para cada uno de los sujetos. La solución a este problema es el conocido como "Sobre Digital" que consiste en lo siguiente.

El sujeto A proporciona una palabra clave, digamos "asdfghj", esta se encripta con la llave pública del sujeto B. Posteriormente encripta el documento con un algoritmo simétrico de encripción. Juntas : la clave encriptada con la llave pública del sujeto B y el documento encriptado con la palabra clave constituyen un "Sobre Digital". El sujeto B recibe el sobre digital, extrae la clave secreta encriptada y la desencripta con su llave privada y obtiene la palabra clave "asdfghj", posteriormente desencripta con el algoritmo simétrico el documento encriptado. El procedimiento se ilustra en las siguientes dos figuras.

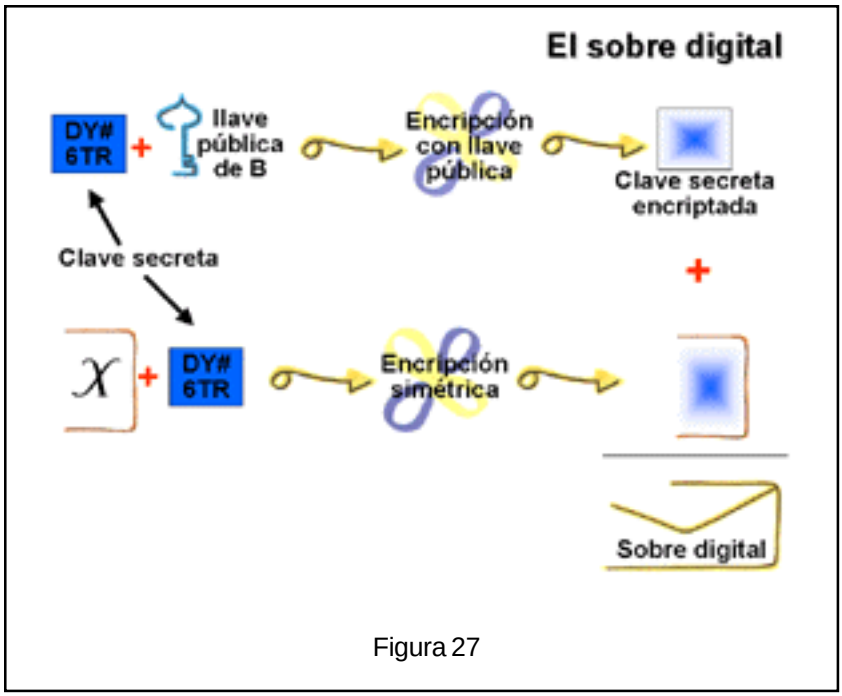

Figura 27

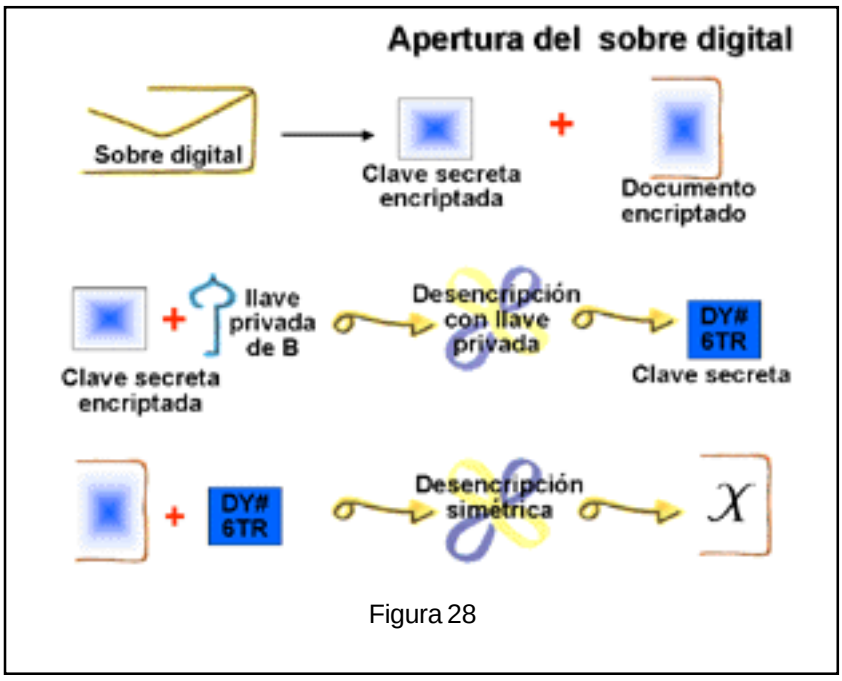

Figura 28

El "sobre digital" es un mecanismo rápido y versátil. Rápido, pues la encripción del documento se realiza mediante algoritmos simétricos y solo la llave de este algoritmo se encripta con llave pública. Versátil, porque si el sobre se desea producir para digamos 5 personas, lo único que se debe de hacer es anexar la llave de encripción simétrica encriptada con la llave pública de cada uno de los sujetos destinatarios del sobre, como se ilustra en la siguiente figura.

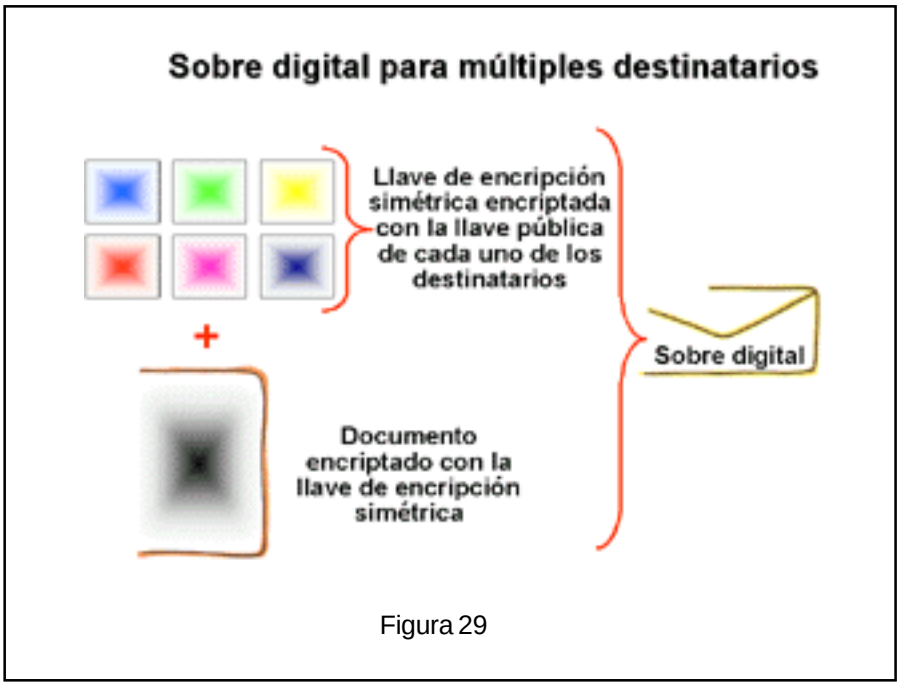

Figura 29

Normalmente, en un sobre digital, la llave de encripción simétrica no es proporcionada por el originador del sobre en forma de contraseña o palabra clave. La computadora sirve como auxiliar del sujeto, puesto que esta puede generar palabras aleatorias que pueden servir de contraseña, con la ventaja de que, al ser aleatorias son considerablemente mas difícil de adivinar. Una contraseña es típicamente una palabra que el sujeto crea a partir de asociaciones de ideas y estas son usualmente predecibles. Quiénes de ustedes no usan su nombre, apodo, su fecha de nacimiento, etc.?.

Como anotación al margen es prudente comentar que la palabra aleatoria es imprecisa, lo mas adecuado sería el termino pseudoaleatorio que refleja la naturaleza determinista de los algoritmos. Es decir, a las mismas entradas se producen las mismas salidas. Como los algoritmos son públicos, la clave es generar una entrada lo mas impredecible posible. Esta simple complicación es técnicamente relevante aunque esta fuera del alcance del documento.

MEDIDAS BÁSICAS DE SEGURIDAD

Esta sección tiene como objeto dar un panorama de la protección que la tecnología ofrece al sujeto usuario. La idea no es la de remotamente cubrir todas las posibles formas de falsificar una firma digital o de abrir sobres digitales. Sin embargo, por la trascendencia de una firma, o de la información confidencial, parece de fundamental importancia que el sujeto esté consciente de las limitantes, y que esté consciente del entorno y procedimientos que le garantizan una seguridad óptima.

No existe una forma ciento por ciento segura de garantizar la seguridad. Dependiendo del grado de importancia se deben de balancear aspectos de diseño de software y hardware para obtener un grado aceptable para enfrentar el riesgo.

En general, se puede afirmar que si la llave privada solo es conocida y accesible por el sujeto A, sería prácticamente imposible, para otro sujeto B, falsificar una firma digital del sujeto A, o abrir un sobre digital dirigido al sujeto A, utilizando métodos matemáticos. El atacante de un sistema va a centrar su esfuerzo en encontrar debilidades en la implementación del software o hardware de seguridad. A continuación se mencionan los 2 puntos de ataque mas comunes.

1.- Generación de Números Aleatorios

La generación de las llaves utiliza métodos pseudoaleatorios por lo que es muy importante que un sujeto B no pueda replicar el procedimiento que siguió un sujeto A cuando éste generó sus llaves. Este comentario también es aplicable a la llave simétrica que se utiliza para encriptar el contenido de un documento en un sobre digital. Esta es una responsabilidad fundamentalmente del software de seguridad.

2.- Ataque a la Llave Privada.

La llave privada, que normalmente reside en un archivo debe de mantenerse encriptada con un algoritmo simétrico, utilizando como clave una contraseña. La contraseña debe de ser elegida por el usuario en forma tal que resulte impredecible para quien intente adivinarlo por asociación de ideas. La encripción por contraseña es normalmente presa de ataques denominados de diccionario que buscan exhaustivamente entre un conjunto de palabras formadas por letras del abecedario. Existen técnicas de encripción basadas en contraseñas que eliminan los ataques de diccionario. Otro ataque más sutil se concentra en intentar por "prueba y error" las posibles contraseñas que un sujeto utiliza en base a asociación de ideas, por ejemplo, su apodo, el nombre de su esposa, su apodo y fecha de nacimiento, etc.

La llave privada solo se debe encontrar desencriptada cuando está en la memoria de la computadora y mientras el programa de seguridad esté funcionando. Si el sujeto se encuentra en un entorno de cómputo en donde sea posible que un atacante realice un "vaciado" a disco del estado de la memoria del programa de seguridad, entonces la llave privada está en peligro.

Si se está en un entorno de cómputo en donde sea posible que un atacante intercepte el teclado, entonces su llave privada está en peligro. Si se está en un entorno de cómputo en donde sea posible substituir el programa de seguridad por uno falso que capture su contra-seña y su llave privada encriptada, entonces su llave privada está en peligro.

Las formas más seguras de evitar el robo de llaves privadas es el de firmar y abrir sobres en una computadora aislada física y virtualmente del mundo exterior. A dicha computadora deben de entrar mensajes a firmar y deben de salir mensajes firmados, nunca debe de salir ni exponer la llave privada. Este es el caso de por ejemplo, los Agentes Certificadores, Auto-ridades Certificadoras, y en general aplicaciones altamente sensitivas.

En general, recuerde que el conjunto de llave privada, software, computadora y el entorno de ésta, constituyen su instrumento de firma. El sujeto debe de proteger su instrumento de firma y en caso de determinar que su instrumento está en peligro, el sujeto debe de revocar su certificado, realizar el procedimiento para obtener uno nuevo con un nuevo par de llaves y restaurar su instrumento de firma.

REVISANDO EL RECIBO Y EL CONCEPTO DE DIGESTIÓN

Al aplicar el concepto de recibo en la Autoridad de Oficialía de Partes podemos apreciar dos problemas, el primero se refiere a que un atacante que intercepte la línea de comunicaciones de la Autoridad de Oficialía de Partes puede conocer el contenido del documento pues este viaja sin ninguna confidencialidad. El segundo se deriva del potencial tamaño del documento a ser atestiguado por la Autoridad de Oficialía de Partes. Una solución a este problema es el uso de algoritmos conocidos como "Algoritmos de Digestión", un algoritmo de digestión toma como entrada un documento de cualquier longitud y produce un mensaje digital de longitud fija con características singulares. Si dos digestiones de dos documentos son iguales entonces significa que ambos documentos son iguales, o son totalmente diferentes. La palabra "totalmente" utilizada como adjetivo en la oración anterior es subjetiva, pero en esencia, esume el espíritu de la idea : Si un documento produce una digestión X entonces cualquier variación al documento, por pequeña que sea, produce una digestión diferente de X.

La digestión X de un documento es irreversible, es decir, no puede conocerse el contenido del documento a partir de conocer X.

El emitir un recibo de la digestión de un documento es equivalente a atestiguar el documento en si, con la ventaja de que la cantidad de bytes a atestiguar es pequeña, por ejemplo, 16 bytes. Además la digestión no revela el contenido del documento.

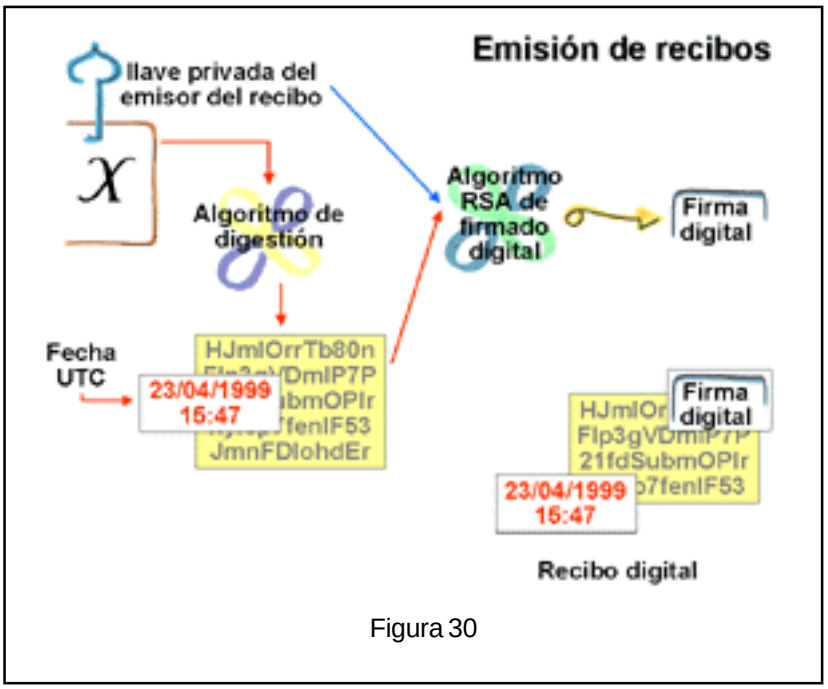

Figura 30

REVISANDO EL FIRMADO Y LA AUTENTICACIÓN

En realidad, el proceso de firmado y autenticado utilizan la digestión para obtener una "huella digital" del documento. Esta "huella digital" se alimenta a un algoritmo RSA de encripción con la llave privada y se obtiene la firma digital del documento.

En la sección sobre CONFIDENCIALIDAD mencionamos textualmente "La criptografía de llave pública ofrece algoritmos de encripción y desencripción. Si un documento se encripta con una llave pública, entonces, solo se desencripta con la correspondiente llave privada, y viceversa". Al hablar de confidencialidad siempre se habla de encripción con llave pública que se desencripta con la correspondiente llave privada. En la autenticidad siempre se habla del proceso inverso, la encripción con la llave privada y la desencripción con la llave pública.

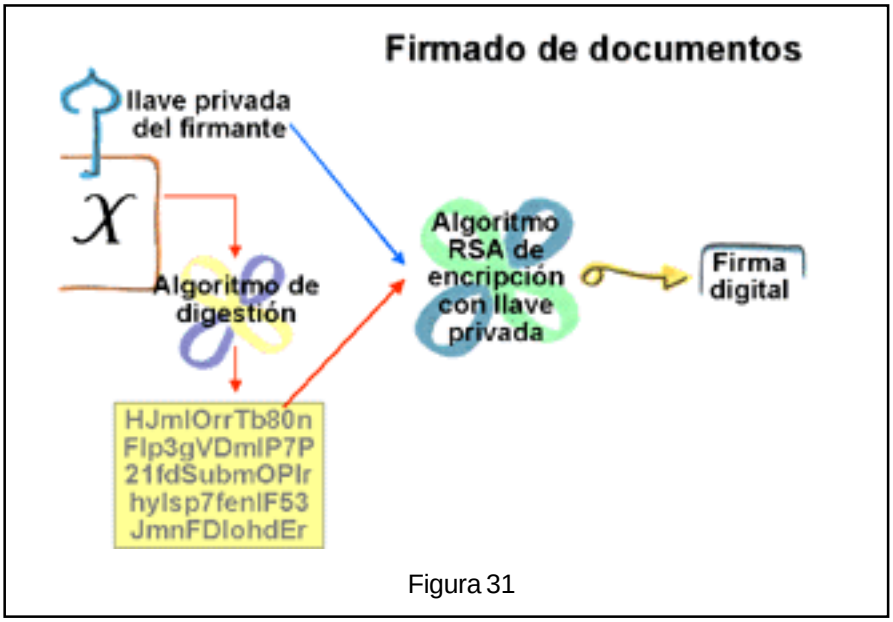

Figura 31

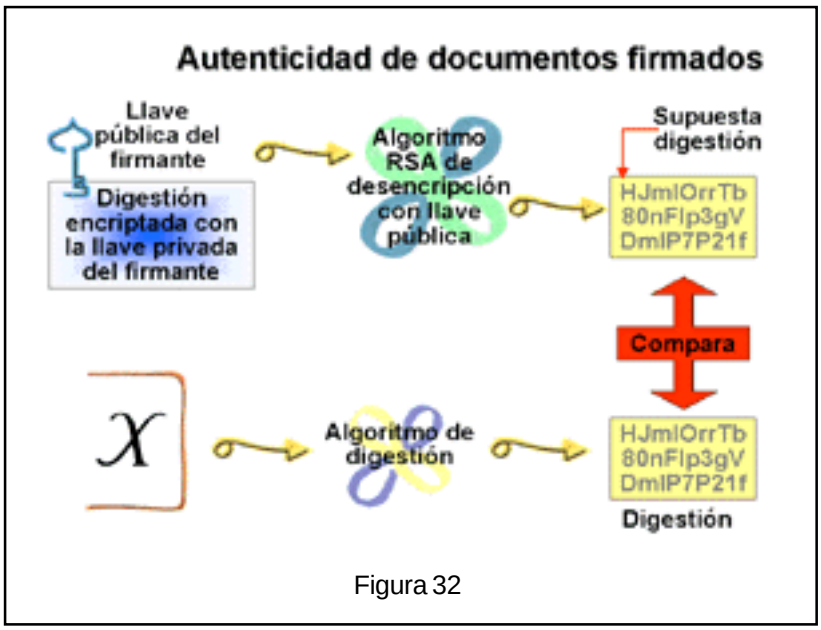

Figura 32

ESTÁNDARES PRINCIPALES

En las secciones anteriores hemos mencionado tres tipos de algoritmos criptográficos: Asimétricos o de llave pública, simétricos y de digestión.

Existen varios algoritmos de llave pública, algunos con promisorio futuro, sin embargo el más popular es el RSA. En algoritmos simétricos el mas famoso es el denominado DES y su variante DES-CBC, pero mas recientemente el algoritmo RC4 ha ganado terreno por su velocidad y versatilidad. DES utiliza llaves de 8 bytes, aunque de los 64 bits, se desechan los bits de paridad y resulta en llaves de tamaño efectivo de 56 bits. Un tamaño efectivo de 56 bits es bastante reducido hoy en día pero DES tiene la característica matemática de no ser grupo. Que no sea grupo significa que si un bloque M se encripta con una llave K1 y produce M' y posteriormente se encripta M' con otra llave K2 para obtener M'' no existe una tercera llave K3 tal que si se encripta M con K3 produce M''. En efecto, en DES si se encripta dos veces con dos llaves diferentes un bloque se aumenta el tamaño efectivo de llave. En la practica el denominado Triple DES o 3DES es el uso mas seguro de DES y consiste en utilizar tres pasos con tres llaves diferentes de 56 bits cada una.

RC4 utiliza llaves de longitud variable y por tanto puede ser menos seguro o más seguro que DES o 3DES, dependiendo del tamaño de la llave a utilizar. En DES o 3DES se encripta forzosamente en bloques de longitud múltiplo de 8 bytes, en RC4 se encripta en bloques de longitud arbitraria. En algoritmos de digestión los más conocidos son el MD2, MD4, MD5 y SHA-1. Publicaciones recientes, favorecen a SHA-1 por su fortaleza criptográfica.

Al margen de los algoritmos critpográficos que se utilicen, es necesario una convención para codificar los diferentes tipos de información, como por ejemplo un certificado, o un archivo firmado. Los programadores o analistas se refieren a estas convenciones como "formatos" o el anglicismo "lay-out". El estándar más popular en este sentido es el conocido como PKCS por ser las siglas de "Public Key Cryptography Standards".

En general el estándar PKCS son en realidad un conjunto de estándares que especifican las reglas de codificación de un requerimiento de certificación (PKCS #10), un certificado (PKCS #6 y #9), un mensaje firmado, o ensobretado, o firmado y ensobretado (PKCS #7). Además de reglas de codificación, PKCS define estándares para guardar la llave privada encriptada con un password (PKCS #5). El PKCS #1 especifica la funcionalidad del algoritmo RSA y el PKCS #3 especifica la funcionalidad del algoritmo Diffie-Hellman ya en desuso. El PKCS #8 especifica la sintaxis de la llave privada.