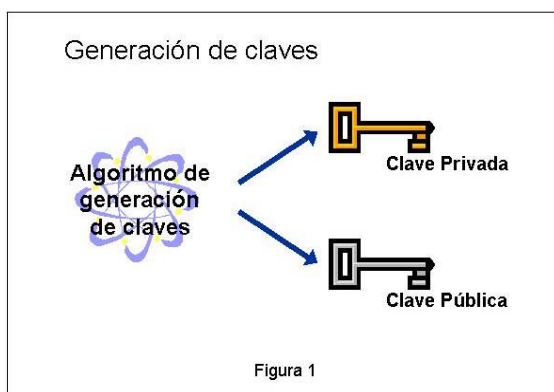


Introducción a la Firma Digital

Uno de los principales desafíos que se plantea en la utilización de documentos electrónicos es determinar su autenticidad, es decir la capacidad de asegurar si una determinada persona ha manifestado su conformidad sobre el contenido del documento electrónico.

Este desafío es resuelto por lo que comúnmente se denomina como “firma digital”, que se basa en procedimientos criptográficos. Su función respecto de los documentos digitales es similar a la de la firma de puño y letra en los documentos impresos: ser el sello irrefutable que permite atribuir a una persona algo escrito o su conformidad en un documento. El receptor, o un tercero, podrán verificar que el documento esté firmado, sin lugar a dudas, por la persona cuya firma aparece en el documento y que éste no haya sufrido alteración alguna. El sistema de firma digital consta de dos partes: un método que haga imposible la alteración de la firma y otro que permita verificar que la firma pertenece efectivamente al firmante.

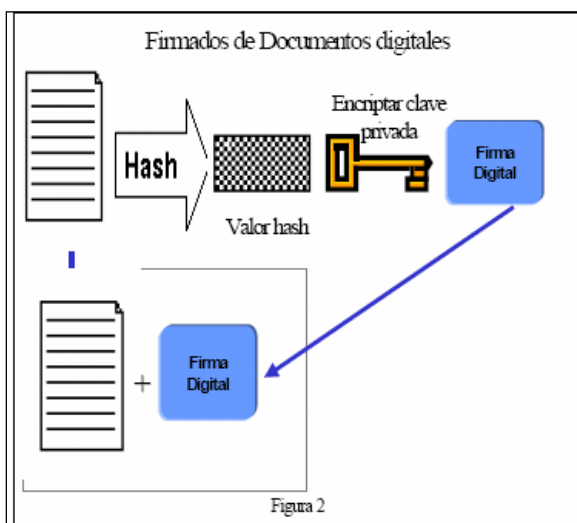
Este documento tiene como objetivo presentar, con un enfoque no técnico, los principales desafíos en el uso de las técnicas criptográficas para establecer la autenticidad de documentos electrónicos.



Mediante un algoritmo cualquier persona puede obtener un par de números matemáticamente relacionados, denominados claves. Una clave es un número de gran tamaño, que se puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes.

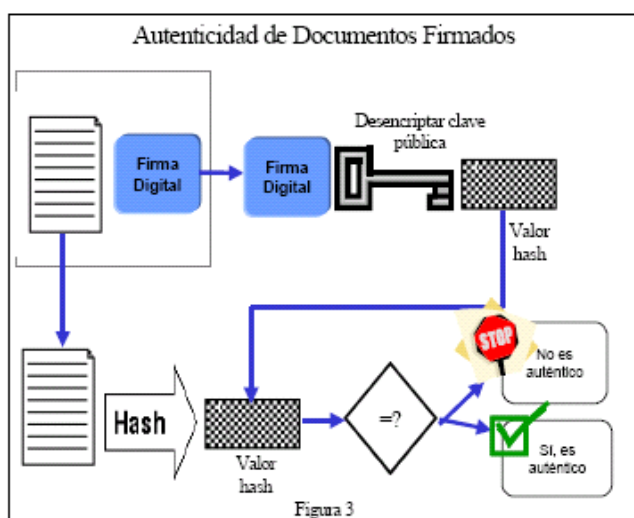
Cada persona genera un par de claves: pública y privada. La primera de ellas debe ser conocida por todos, mientras que la segunda es mantenida en secreto por el usuario. Existen diversas formas de almacenar una clave privada: en un archivo en el disco rígido de una PC o en una tarjeta inteligente (smartcard).

La clave pública y privada tienen características únicas, su generación es siempre en parejas y están relacionadas de tal forma que todo lo que sea encriptado por una de ellas sólo podrá ser descifrado por la otra.



Para firmar un documento se aplica sobre el mismo, una función unidireccional de resumen (función hash) para obtener un valor hash, que no es más que el resumen del documento. Para obtener la firma digital, se encripta el valor hash con la clave privada del firmante. La creación de la firma digital se lleva a cabo a través de un algoritmo que combina los caracteres que conforman la clave privada con los caracteres del documento. De este modo se obtiene la “firma digital”. Juntos, el documento y la firma digital constituyen el documento firmado.

Es importante señalar que, a diferencia de la firma autógrafa, todas las firmas digitales generadas por una persona son diferentes entre sí. En otras palabras la firma digital cambia con cada documento firmado. Por otra parte, si dos personas firman un mismo documento, también se producen dos diferentes documentos firmados, ya que la clave privada utilizada es diferente.



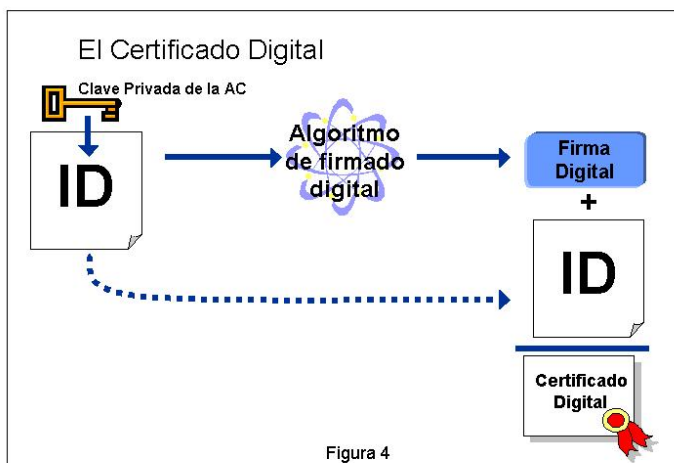
Para validar la autenticidad de un documento firmado, el receptor del mismo debe crear un valor hash del documento transmitido y también debe descriptar la firma digital con la clave pública del firmante, una vez que obtiene los valores hash, los compara para determinar la autenticidad del documento firmado.

Si el documento o la firma es modificada, aunque sea ligeramente, el procedimiento de autenticación indicará que el documento firmado no

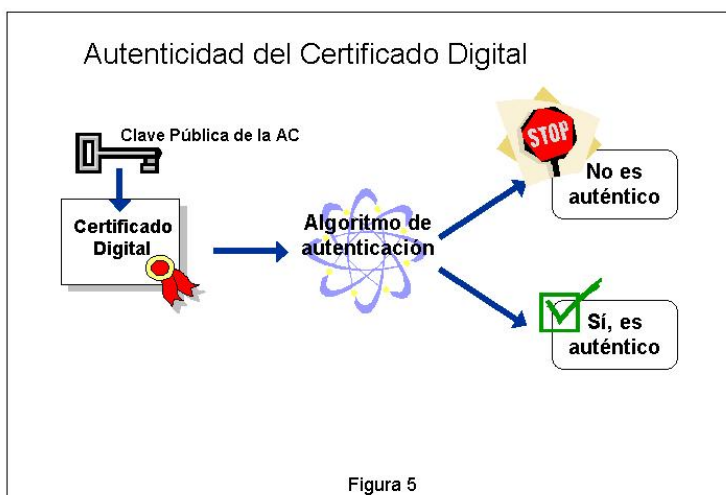
es auténtico.

Si dos personas deciden reconocer legalmente la validez de la firma digital en los documentos electrónicos emanados de su intercambio electrónico de información, deben intercambiar sus claves públicas para que ambos puedan autenticar documentos firmados por ellos. Si estos individuos quisieran reconocer formalmente la validez de la firma digital, en caso de que no exista un marco legislativo que regule su aplicación, tendrían que suscribir un acuerdo formal, con firma autógrafa, donde se acepten las técnicas a utilizar y sobre todo donde conste el reconocimiento y aceptación de sus respectivas claves pública.

Es claro que una persona, en el proceso de autenticar un documento firmado digitalmente debe contar con un archivo que contenga la clave pública del supuesto firmante. Es decir que para autenticar un documento firmado por 10 personas se deberá contar con 10 archivos o con una base de datos conteniendo las 10 claves públicas de los posibles firmantes. Si este número aumenta a 100, 1000 o a un 1.000.000 el problema crece en forma considerable. Por otra parte, es sumamente importante determinar con seguridad la identidad del titular de cada clave pública. Una solución a este problema de manejo de claves se basa en el concepto conocido como Certificado Digital.



El Certificado Digital es en si un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificante (AC), mediante el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad. En general, contiene la identidad de la persona (nombre), su clave pública y el nombre de la AC. Todos estos datos son previamente validados por la AC, asegurando de esta forma la veracidad de la información.

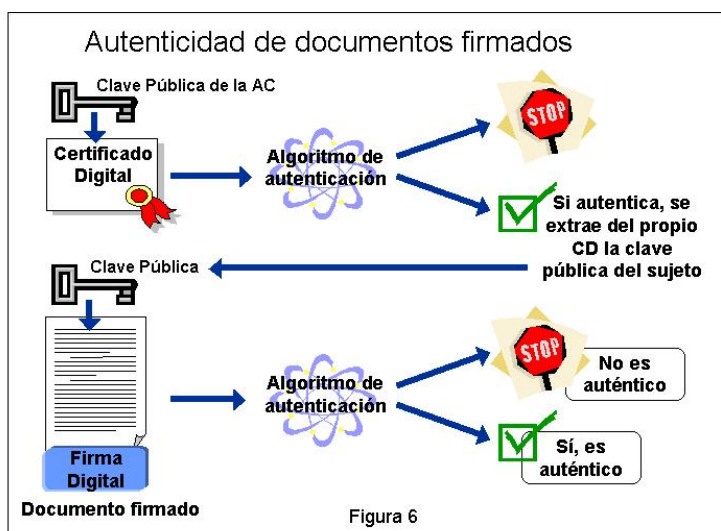


La idea es que cualquiera que conozca la clave pública de la AC puede autenticar un Certificado Digital de la misma forma que se autentica cualquier otro documento firmado, como se ilustra en la siguiente figura.

Si el Certificado es auténtico y confiamos en la AC, entonces, podemos confiar en que el sujeto identificado en el Certificado Digital posee la clave pública que se señala en dicho certificado. Los certificados ayudan a evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la clave pública de la AC podrá autenticar el documento, como se ilustra en la siguiente figura.

Se recomienda que los Certificados Digitales tengan un período de validez, luego del cual deberán ser renovados.



Ahora bien, puede suceder que en algún momento el titular de una clave pública no desee utilizar más la firma digital, o haya extraviado el soporte en el cual se encontraba guardada su clave privada. Para estos casos se recomienda efectuar la revocación del Certificado Digital y aquí surge 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 en 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 inglés. Un CRL es un archivo, firmado por la Autoridad Certificante, que contiene la fecha de emisión del CRL y una lista de certificados revocados, cada uno de ellos con la fecha de revocación.

Un CRL puede ser autenticado como cualquier otro documento firmado digitalmente, en este caso con la clave pública de la Autoridad Certificante. Una vez autenticado, podemos confiar en su contenido y determinar con certeza si un certificado está revocado o no, esto es hasta la fecha definida por "Última Actualización".