LA IMPORTANCIA DEL CERTIFICADO Y FIRMA DIGITAL

Yanet Castrejon Hernández ([yanet.ch@zacatepec.tecnm.mx](mailto:yanet.ch@zacatepec.tecnm.mx)), Mario Humberto Tiburcio Zuñiga ([mario.tz@zacatepec.tecnm.mx](mailto:mario.tz@zacatepec.tecnm.mx)), Tomas Emanuel Higareda Pliego ([tomas.hp@zacatepec.tecnm.mx](mailto:tomas.hp@zacatepec.tecnm.mx)), Norma Josefina Ontiveros Hernández ([norma.oh@zacatepec.tecnm.mx](mailto:norma.oh@zacatepec.tecnm.mx)), Socrates Salgado ([socrates.s@zacatepec.tecnm.mx](mailto:socrates.s@zacatepec.tecnm.mx))

RESUMEN

En la actualidad cada vez es más importante la confidencialidad, la autenticidad y la integridad de la información, varias empresas utilizan la tecnología para llevar a cabo sus procesos internos, dejando aún lado la gestión de documentos sin preocuparse por garantizar la seguridad y cifrado evitando el filtrado de información confidencial.

El cifrado significa que un documento se bloquea mediante llaves, esto permite la restricción del acceso al documento, hay distintos sistemas criptográficos, la criptografía simétrica y asimétrica. La criptografía simétrica se caracteriza por usar la misma clave para cifrar y descrifrar el mensaje que se quiere enviar. Este tipo de criptografía al transmitir se hace de manera insegura por lo que no se garantiza el no repudio.

Sin embargo la criptografía asimétrica o conocida comúnmente como clave pública se caracteriza por el uso de claves distintas para cifrar y descifrar, es decir cada usuario tiene un par de claves, una clave pública que conoce todo el mundo y una clave privada que solamente el titular puede conocer y es el responsable de resguardar dicha clave. Otro elemento importante es el uso de la función de hash o resumen y el resultado al aplicar este algorimo es la huella digital, este resultado tiene la misma longitud de bits, una caracteristica es que no es posible obtener el mensaje original a partir del resumen y otra característica es que prácticamente es imposible que haya dos resúmenes iguales correspondientes a dos mensajes diferentes.

Aún cuando se tiene ciertos elementos básicos de seguridad como la confidencialidad, la integridad, surge el problema de suplantación de identidad y se resuelve con los certificados digitales en lo que además de la clave pública del usuarios, se tiene la firma de una entidad de confianza que es reconocida por ambas partes, garantizando que dicha clave pública pertenece al titular que se identifica, de esa manera se puede iniciar la comunicación de manera segura. La Infraestructura de Clave Pública (PKI) donde uno de sus componentes es la Autoridad de Certificación. La PKI en sentido general se basa en un modelo de confianza, en el cual los usuarios confían que las claves públicas gestionadas por dicha PKI son auténticas (ADAMS & LLOYD, 2002).

Palabras Claves: PKI, firma digital, certificado digital

INTRODUCCIÓN

En la actualidad algunas empresas han incorporado herramientas tecnologicas para llevar acabo sus procesos, esto ha originado un mayor intercambio de datos y se hace necesario proteger la información, ya que han surgido problemas como la suplantación de identidad, modificación de mensajes, asi es como la criptografía se vuelve importante.

Existen diversos mecanismos para la autenticación de documentos, la Infraestructuras de Clave Pública (PKI), puede ser definida como un conjunto de recursos de software, hardware, politicas, procedimientos y usuarios que posibilitan el uso de la criptografía de clave pública, con todos estos elementos garantizan la confidencialidad, autenticación, integridad y no repudio.

CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA

La criptografía simétrica utiliza una clave para codificar y decodificar, su desventaja es que al usarse al transmitir, dicha clave debe ser incluida en el emisor y receptor, debiendo transmitir la clave de forma segura (LUCENA, 2010). El cifrado asimétrico debe existir una clave pública conocida por todo el mundo y una privada que debe conocerla solo el propietario; y lo que se cifra con una clave, solo puede descifrarse con la otra. Es decir, cualquier persona puede cifrar un mensaje con la clave pública, pero solo el propietario de la clave privada puede descifrarlo. Siendo la criptografía asimétrica una de las más fiables especialmente por la incorporación de algoritmos de firma digital (JOSHI & KARKADE, 2015) que avalan la identidad del firmante y la integridad de un mensaje.

Veasé en la Figura 1 Criptografía simétrica, donde se encuentra el usuario Pedro que es el emisor y Ana como receptor, antes de comunicar el mensaje se ponen de acuerdo sobre la clave que van a utilizar, cuando Pedro cifra el mensaje con la clave que hayan acordado y Ana lo recibe, esté lo descrifrará con la misma clave que acordaron, a medida que aumenta el número de usuarios, aumenta el número de claves.

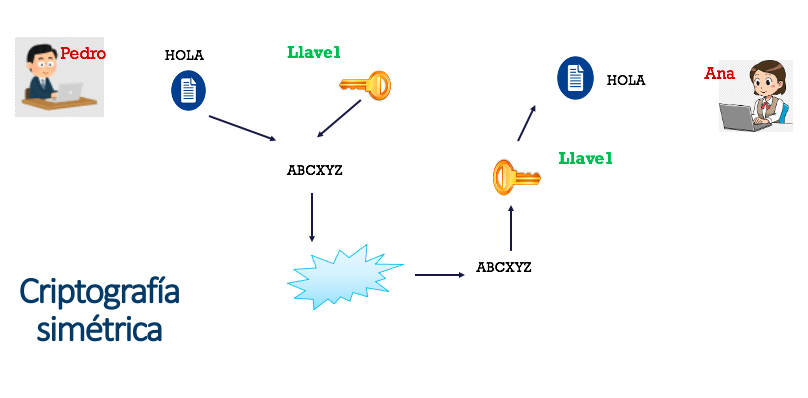


Figura 1 Criptografía simétrica

En la siguiente Figura 2 Criptografía asimétrica, se muestra el uso de dos llaves, la pública y la privada, donde solo existe una llave privada por llave pública, para uso único del propietario y es la que se usa para firmar electrónicamente. La pública debe estar a disposición de todos los usuarios y se usa para encriptar la información.

Entonces la criptografía asimétrica utiliza dos claves distintas con una relación matemática entre si. La clave pública es la responsable de la codificación y la clave privada permite el descrifrado.

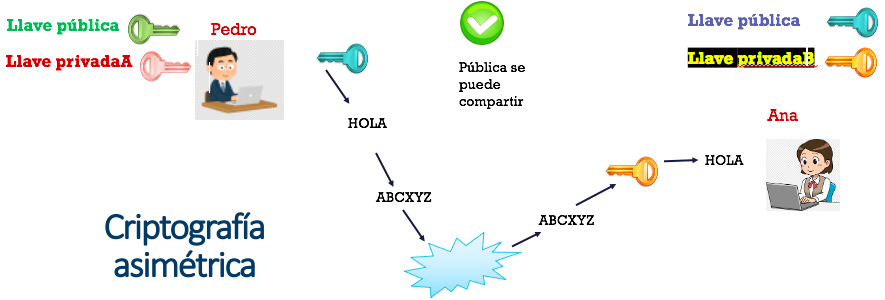


Figura 2 Criptografía asimétrica

## FIRMA DIGITAL

Con la criptografía de llave pública es posible implementar el concepto de firma digital. El esquema de operación es similar al proceso de cifrado, solo que la llave pública y privada son invertidas, es decir la llave privada se emplea para generar la firma del mensaje o documento electrónico y la llave pública se utiliza para verificar dicha firma (véase en laFigura 3 Firma Digital).

* El emisor calcula el ​hash​\* del mensaje M y lo cifra con su clave privada.
* El emisor envía el mensaje M junto con la firma del hash al receptor.
* El receptor, a través de la clave pública del emisor, descifra el hash que ha recibido cifrado.
* El receptor, una vez descifrado, obtiene un hash.
* A continuación, el receptor calcula el hash del mensaje M y si coincide con el hash obtenido al descifrar, se considera el mensaje como auténtico. Si no, significa que ha sido alterado.

Figura 3 Firma Digital

Datos Originales



[Esta foto](http://elciberpastor.blogspot.com/2016/10/la-llave-que-abre-las-puertas-del-cielo.html) de Autor desconocido está bajo licencia [CC BY-NC](https://creativecommons.org/licenses/by-nc/3.0/)



Algoritmo de Hash

**.0**

**0.0**

Algoritmo de cifrado asimétrico

**.0**

**0.0**



Hash

Hash Cifrado

(firma digital)

Clave privada del Remitente

Certificado Digital (Clave pública del Remitente)

Datos Originales



[Esta foto](http://elciberpastor.blogspot.com/2016/10/la-llave-que-abre-las-puertas-del-cielo.html) de Autor desconocido está bajo licencia [CC BY-NC](https://creativecommons.org/licenses/by-nc/3.0/)

Algoritmo de Hash

**.0**

**0.0**

Algoritmo de cifrado asimétrico

**.0**

**0.0**



Hash Cifrado (Firma Digital)

Clave pública del Remitente



Hush

**.0**

**0.0**

Hash

Validación

OK

INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

En criptografía, una Infraestructura de Clave Pública (Public Key Infrastructure) es una combinación de hardware, software, y políticas y procedimiento de seguridad, que permiten la ejecución con garantías de operaciones criptográficas. Este sistema, permite vincular las claves públicas con sus respectivas entidades. De este modo, un organismo externo en el cual confían las partes implicadas garantiza que una clave pública pertenece a una entidad. Las operaciones criptográficas de clave pública utilizan unos algoritmos de cifrado conocidos y accesibles para todos. Por eso, la seguridad proporcionada por la tecnología PKI, está mayormente ligada a la privacidad de la clave privada y las políticas de seguridad aplicadas.

Los algoritmos de cifrado, atendiendo tipo de clave empleado se clasifican en: cifrado de clave simétrica y cifrado de clave pública (o asimétrica). (MENEZES ET AL., 1996). Descifrar un mensaje con una clave pública proporciona la garantía de que el mensaje fue cifrado por el dueño de la clave privada asociada a esta, lográndose la autenticidad del emisor (SEPÚLVEDA & SEPÚLVEDA, 2005).

Con el objetivo de garantizar seguridad y confianza en una comunicación electrónica entre las partes involucradas, se emplea una Infraestructura de Clave Pública cuya base es la criptografía asimétrica o de clave pública (ADAMS & LLOYD, 2002) (RAINA, 2003).

El principal objetivo de un sistema PKI es la gestión y distribución de claves públicas, la cual es llevada a cabo por una Autoridad Certificadora (AC). La PKI en sentido general se basa en un modelo de confianza, en el cual los usuarios confían que las claves públicas gestionadas por dicha PKI son auténticas (ADAMS & LLOYD, 2002).

A continuación se muestra los componentes del modelo PKI (veáse en la *Figura 4 Componentes PKI*)

Figura 4 Componentes PKI

DESARROLLO TEÓRICO

Se ha definido que una PKI es una infraestructura de seguridad basada en criptografía de clave pública, esta compuesta por normas, hardware, software, que brinda un servicio a individuos u organizaciones la confianza necesaria para identificarse entre sí.

Los componentes de una infraestructura de llaves públicas pueden variar de acuerdo a su implementación, para ello se van a definir funciones:

* Autoridad de Certificación (CA).

1. Generar Certificados. En primera instancia la CA emite su propio certificado firmado por si misma (self signed).
2. Revocar Certificado. La CA puede revocar un certificado que el emisor ha solicitado previamente a través de la RA, muestra el estado en que se encuentran dichas solicitudes. Permite filtrar por solicitudes aceptadas, en trámite o simplemente mostrar todos los certificados del sistema. Se encarga de certificar de actualizar la tabla de certificados de la base de datos.
3. Aceptar / Denegar. Es la encargada de aprobar o denegar las solicitudes que la RA le transmite sobre la creación de certificados.
4. Gestionar CRL. Se encarga de crear una nueva lista de revocación
5. Cifrar Documentos. Cifrar el contenido de los documentos

* Autoridad de Verificación (VA).

1. Información Certificado.
2. Consultar CRL. Muestra las listas CRL que hubiera, así como los certificados revocados..
3. Búsqueda de Certificados Revocados.

* Autoridad de Registro (RA)

1. Gestión Solicitud Certificados. Se encargará de gestionar las solicitudes recibidas de los usuarios para la solicitud de certificados.
2. Gestión revocación Certificados. Se encargará de gestionar las solicitudes de revocación de certificados recibidas por los usuarios.
3. Gestión ciclo vida certificados

* Usuario

1. Solicitar Certificado.
2. Solicitar Revocar Certificado.
3. Visualizar documentos cifrados.
4. Envío de documentos cifrados y firmados.

RESULTADOS

Como se ha comentado, la confidencialidad de la información es un factor fundamental, y la PKI se encarga de garantizar la protección y seguridad de los mensajes, su integridad, autenticación y el no repudio.

Para Implementar un PKI se necesitan varios elementos, ademas de una infraestructura de red segura, un sistema o programa que permita administrar PKI, se necesitan procedimientos y politicas de creación, de emisión, de renovación y de revocación de certificados, se requiere una autoridad de certificación, una autoridad de registro, basados en criptografía asimétrica, un repositorio de claves y software para los clientes.

Considerando que la firma digital basada en Infraestructura de Clave Pública implementa operaciones criptográficas garantizando la autenticidad del emisor, la integridad de la información transmitida que una firma generada tradicionalmente, y que sus principios fundamentales son muy similares a los de una firma autógrafa donde su propietario puede crearla, puede ser verificada por su emisor y receptor, no puede ser repudiada por su remitente, por lo tanto es recomendable utilizar PKI, y la arquitectura tendría que ser de la siguiente manera (veáse en la *Figura 5 Uso del certificado*).

El ejemplo sería de la siguiente manera, el emisor quiere comunicarse de manera segura con el receptor , se requiere tener un mecanismo para garantizar el no repudio, la confidencialidad, la autenticación.

1. Donde el emisor crea una solicitud de certificado a la Autoridad de Registro.
2. La Autoridad de Registro autoriza la asociación entre una clave pública y el titular de un certificado, luego la Autoridad de Registro envía una solicitud a la Autoridad de Certificación para la aprobación de políticas y para ser firmado.
3. El resultado de la firma del certificado es enviado de vuelta al emisor a través de la Autoridad de Registro.
4. En esta parte el emisor puede notificar que su clave pública es confiable.
5. El receptor pregunta a la Autoridad de Validación el estado de la certificación, en ocasiones el receptor pregunta directamente a la Autoridad de Certificación, para así obtener la clave pública del emisor.
6. Al tener ambas llaves públicas pueden iniciar a comunicarse de manera segura.

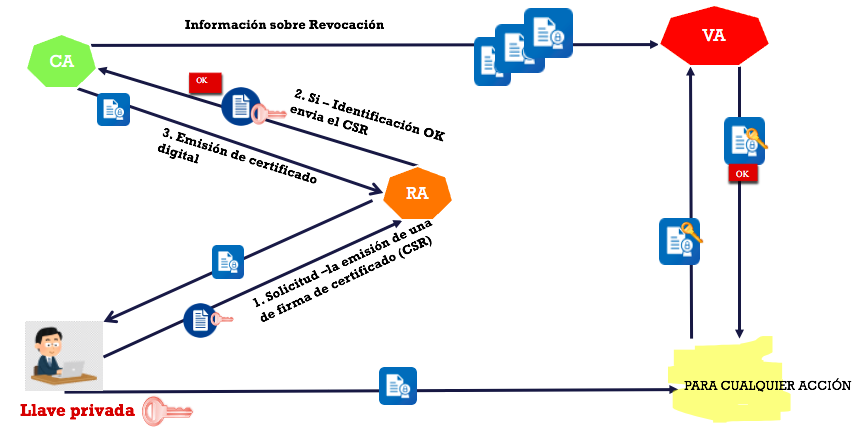


Figura 5 Uso del certificado

Datos importantes que se deben consideran para la implementación

1. Es importante definir los componentes que se van a utilizar como usuarios especiales.

* La CA (Autoridad de Certificación) que es el núcleo de la PKI, de la cual se va a encargar de la creación de certificados revocación, crear las listas de revocación, cifrar y firmar los documentos confidenciales para que solo el usuario al que va dirigido pueda verlo.
* La RA (Autoridad de Registro) que se va a encargar de ser el intermediario con el usuario y la CA. La RA gestionará las solicitudes de certificados, la gestión de altas, bajas y modificaciones, verificará que cumpla con todos los requisitos y le hará a su vez la solicitud a la CA para que genere el certificado.
* La VA (Autoridad de Verificación), tendrá que comprobar si un certificado se encuentra revocado o no. Donde si un certificado esta revocado significa que no podríamos utilizar su clave pública para cifrar ya que la relación de confianza entre el titular del certificado y dicha clave ha sido destruida y no tendríamos las garantías de seguridad que nos otorga un certificado que no está revocado.
* El titular del certificado debe tener bajo su poder y responsabilidad la clave privada, y su clave pública deberá estar en un repositorio. Un titular al perder su clave privada le podrían suplantar la identidad, es por ello que existe la revocación. Un documento digital que contiene la clave pública junto con todos los datos del titular, todo ello es firmado por una Autoridad de Certificadora, que es una tercera entidad de confianza que segura que la clave pública si corresponde con los datos del titular.

1. También en importante que se defina el tipo de algoritmo a utilizar, lo recomendado es el RSA.

El RSA Permite cifrar con la clave pública y descifrar con la clave privada.

El DSA se utiliza como un algoritmo de firma digital pero no se utiliza para cifrar datos.

Definir las políticas de generación de claves como el periodo de validez, datos personales del titular.

1. Tener una herramienta para recoger entropía.

Con lo anterior ya se puede ir definiendo para la implementación de una PKI y adaptarlo a las necesidades.

CONCLUSIONES

Se concluye que la creciente digitalización en los diferentes sectores educativos, sociales, industriales ha resultado una necesidad de verificación digital para proteger la infraestructura empresarial, donde la autenticación es un factor importante, y al usar la Infraestructura de Clave Pública se garantiza la autenticidad del emisor, la integridad de la información, la confiabilidad y el no repudio.

Sin embargo la falta de conocimiento sobre soluciones PKI en las empresas y la introducción de autoridades de certificación privada son factores que se espera que obstaculicen el crecimiento del mercado, por lo tanto es importante conocer dicha arquitectura o temas relacionados.

BIBLIOGRAFÍA

ADAMS, C.; S. LLOYD: Understanding PKI: Concepts, Standards, and Deployment Considerations, 2 edn, Addison Wesley, USA, 2002

MENEZES, A. J.; A. VANSTONE; C. V OORSCHOT: Handbook of Applied Cryptography, 816pp., .CRC Press, Inc., USA, 1996.

SEPÚLVEDA, J. C.; R. SEPÚLVEDA: Certificados Digitales, Características y Aplicaciones en la Seguridad de Documentos Digitales, En:  
Seguridad en Cómputo e Inteligencia Artificial, Sede de Pereira y Manizales. Universidad Nacional de Colombia, 2005.

JOSHI, M. & KARKADE, R., 2015: Network Security with Cryptography. International Journal of Computer Scien-ce and Mobile Computing, 4(1), 201-204. Recuperado de <https://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf>

LUCENA LOPEZ, MANUELJ., 2010: Criptografía y Seguridad en Computadores. (Consulta: 27 de julio de 2017) (<http://sertel.upc.edu/tdatos/Libros/Lucena.pdf>)