Implementando un esquema de firmado digital para archivos utilizando infraestructura de clave pública

Colaboración
Yanet Castrejón Hernández; Mario Humberto Tiburcio Zúñiga; Norma Josefina Ontiveros Hernández; Sócrates Espinoza Salgado; Jesús Ángel Peña Ramírez, Tecnológico Nacional de México/Instituto Tecnológico de Zacatepec

Fecha de recepción: 14 de noviembre de 2022
Fecha de aceptación: 18 de diciembre de 2022

RESUMEN: Con el avance de las nuevas tecnologías como lo son el Internet, el correo electrónico, etc., se ha tenido que desarrollar nuevos sistemas de criptografía y cada vez es más importante ofrecer métodos seguros que garanticen la integridad y la autenticidad de la información. En este artículo se explica un método de clave pública que es en el que se basa el sistema de cartografía para garantizar la validez de las llaves combinado con el uso de una clave privada, proveyendo la confianza necesaria para que se lleve a cabo la comunicación entre quienes corresponda.

Un tercer ente debe garantizar la validez de las llaves proveyendo la confianza necesaria para realizar la comunicación. La Public Key Infrastructure (PKI), Infraestructura de Clave Pública se basa en un modelo de confianza, donde uno de sus componentes es la Autoridad de Certificación, en el cual los usuarios confían que las claves públicas gestionadas por dicha PKI son auténticas.

PALABRAS CLAVE: Autoridad Certificadora, Certificado Digital, Clave Pública, Firma Digital, PKI.

ABSTRACT: With the advancement of new technologies such as the Internet, email, etc., new cryptography systems have had to be developed and it is increasingly important to offer secure methods that guarantee the integrity and authenticity of the information. This article explains a public key method that is the one on which the mapping system is based to guarantee the validity of the keys combined with the use of a private key, providing the necessary trust for communication between who corresponds.

A third entity must guarantee the validity of the keys, providing the necessary confidence to carry out the communication. The Public Key Infrastructure (PKI), Public Key Infrastructure is based on a trust model, where one of its components is the Certification Authority, in which users trust that the public keys managed by said PKI are authentic.

KEYWORDS: Certification Authority, Digital Signature, Public Key, Digital Certificate, PKI.

INTRODUCCIÓN

Firmado digital

El cifrado significa que el contenido de un documento se restringe mediante el uso de llaves. Hay distintos sistemas criptográficos: la criptografía simétrica y la criptografía asimétrica [1]. Actualmente, algunas empresas han incorporado herramientas tecnológicas para llevar a cabo sus procesos, esto ha originado un mayor intercambio de datos y se hace necesario proteger la información, ya que han surgido proble-

mas como la suplantación de identidad, modificación de mensajes, así es como la criptografía se vuelve importante [2].

Existen diversos mecanismos para la autenticación de documentos, uno de ellos es la Infraestructura de Clave Pública. Por lo tanto; al implementar una Infraestructura de Clave Pública (PKI), como mecanismo de seguridad para la autenticación de documentos electrónicos firmados por el personal y las autoridades, entonces los documentos emitidos podrán ser validados a través del sistema Web CertITZ, garantizando la autenticación, confidencialidad, el no repudio y la integridad. [3], [4], consiguiendo así la garantía de alcanzar el objetivo de proporcionar la confianza necesaria para que se lleve a cabo la comunicación entre quienes corresponda.

Problemática de investigación

En la actualidad, cada vez es más importante la integridad y la autenticidad de la información. Muchas empresas utilizan la tecnología para automatizar y agilizar sus procesos internos, dejando a un lado la gestión de documentos, descuidando la seguridad y el cifrado de los mismos.

Aún cuando en la criptografía, se tiene ciertos elementos de seguridad como la confidencialidad, surge el problema de suplantación de identidad. Este problema se resuelve con llaves públicas que identifiquen indubitadamente a las partes que se comunican.

MATERIAL Y MÉTODOS

Criptografía simétrica y asimétrica

La criptografía simétrica utiliza una clave para codificar y decodificar [5].

Véase 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 al cifrar el mensaje y Ana al recibir el mensaje, esté lo descifrará con la misma clave que acordaron.

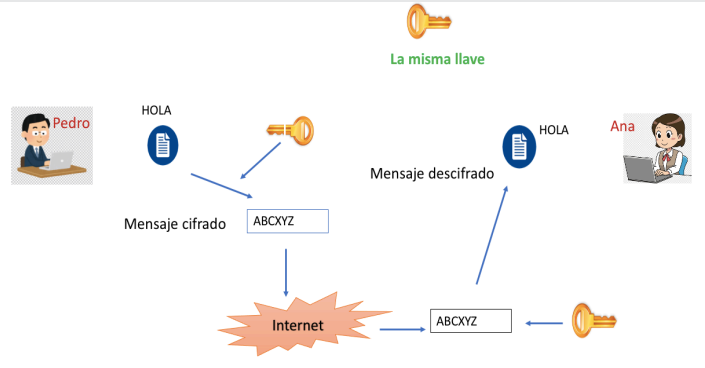

Figura 1. Criptografía Simétrica.
Fuente: https://isohub.org/criptografia-iso-27001

En la criptografía asimétrica debe existir una clave pública conocida por todo el mundo y una clave privada que debe conocerla solo el propietario. Es decir, cualquier persona puede cifrar un mensaje con la clave pública, pero solo el propietario de la clave privada puede descifrarlo [6].

En la Figura 2: Criptografía Asimétrica, se muestran dos llaves, una pública y una privada, donde la pública debe ser conocida y a disposición de todo el mundo y está se usa para encriptar el mensaje, en cuanto a la llave privada solo es exclusiva y conocida por el titular y es la que se usa para firmar electrónicamente.

Figura 2. Criptografía Asimétrica.
Fuente: https://isohub.org/criptografia-iso-27001/).

La criptografía asimétrica es una de las más fiables especialmente por la incorporación de algoritmos de firma digital que avalan la identidad del firmante y la integridad de un mensaje.

Firma digital

El concepto de firma digital es similar al proceso de cifrado, con la llave pública se implementa el concepto de firma digital, véase en la Figura 3.

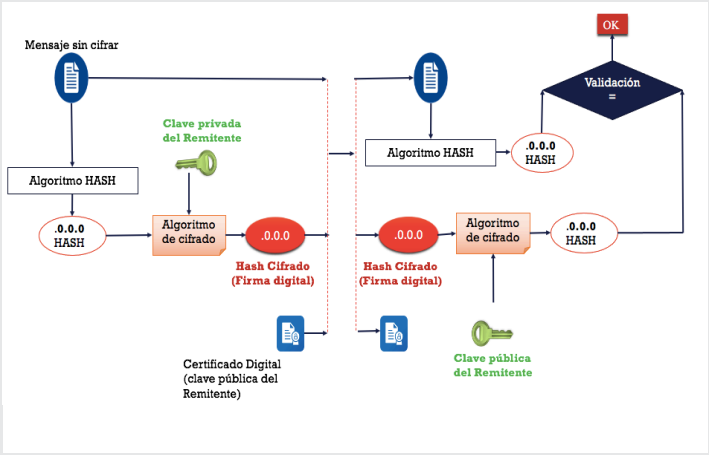

Figura 3. Firma Digital.
Fuente: https://www.researchgate.net/publication/317121299.

- El emisor calcula el hash * del mensaje original (Msj) y lo cifra con su llave privada.
- El emisor envía el Msj junto con la firma del hash al receptor.
- El receptor, a través de la llave pública del emisor, descifra el hash que ha recibido cifrado.
- El receptor, una vez descifrado, obtiene un hash.
- El receptor calcula el hash del mensaje Msj y si coincide con el hash obtenido al descifrar, se considera el mensaje como auténtico. Si no fuera así, entonces significa que ha sido modificado.

El uso de la función de hash o resumen y el resultado al aplicar este algoritmo es la huella digital, este resultado tiene la misma longitud de bits, una característica importante que no puede haber dos resúmenes iguales que vengan de dos mensajes diferentes y otro punto importante es que no es reversible, es decir no se puede obtener el mensaje original a partir del resumen.

Infraestructura de clave pública

Una Infraestructura de Clave Pública es una combinación de hardware, software, políticas y procedimiento de seguridad. Este sistema, permite vincular las llaves públicas con sus respectivas entidades. De este modo, un organismo externo en el cual confían las partes implicadas garantiza que una llave 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 llave privada y las políticas de seguridad aplicada.

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

En la Figura 4, se muestran los componentes del modelo PKI.

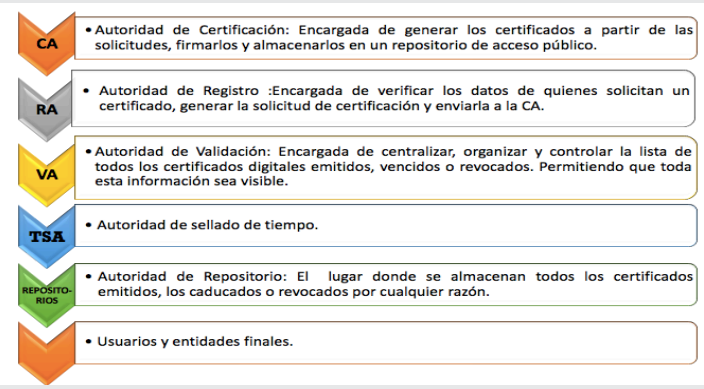

Figura 4. Componentes PKI.
Fuente: Elaboración propia.

Los componentes de una infraestructura de claves 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 sí mismo (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 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, 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

Es recomendable utilizar PKI para la firma digital de archivos, y la arquitectura tendría que ser como se muestra en la Figura 5.

Los puntos importantes a seguir. El usuario **E** quiere comunicarse de manera segura con el usuario **R**, se requiere tener un mecanismo para garantizar el no repudio, la confidencialidad, la autenticación.

1. Donde el usuario **E** crea una solicitud de certificado a la **RA**.
2. La **RA** autoriza la asociación entre una llave pública y el titular de un certificado, luego la Autoridad de Registro envía una solicitud a la **CA** para la aprobación de políticas y para ser firmado.

3. El resultado de la firma del certificado es enviado de vuelta al usuario **E** a través de la Autoridad de Registro.
4. En esta parte el emisor puede notificar que su llave pública es confiable.
5. El receptor pregunta a la **VA** el estado de la certificación, en ocasiones el receptor pregunta directamente a la **CA**, para así obtener la llave pública del emisor.
6. Al tener ambas llaves públicas pueden iniciar a comunicarse de manera segura.

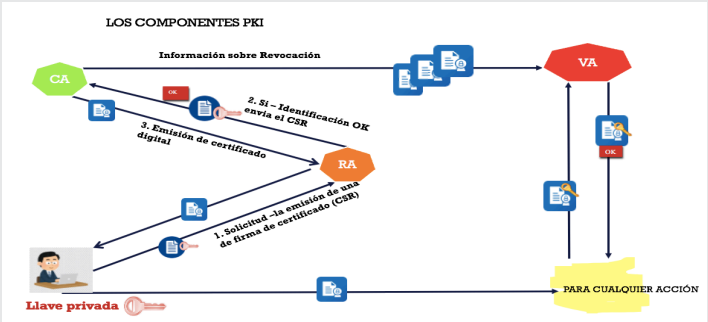

Figura 5. Uso del certificado.
Fuente: https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica.

Datos importantes que se 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 mensajes 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. Aquí, si un certificado esta revocado significa que no se podría 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 se tendrían las garantías de seguridad que 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.

• También en importante que se defina el tipo de algoritmo a utilizar, lo recomendado es el **RSA** (Rivest, Shamir y Adleman) que es un sistema criptográfico de clave pública que fue desarrollado en el año de 1979, y que hace uso de la factorización de números enteros y es válido tanto para cifrar como para firmar digitalmente [7], [8].

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

• El **DSA** (Digital Signature Algorithm, en español Algoritmo de Firma Digital) 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 y los datos personales del titular.

• Tener una herramienta para recoger entropía.

Con lo anterior se puede ir adaptando a las necesidades.

CONCLUSIONES

Se concluye que la creciente digitalización en los diferentes sectores educativos, sociales e 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, 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.

Se propone como trabajo futuro que se encripten archivos de forma masiva para agilizar los tiempos de validación.

BIBLIOGRAFÍA

[1] Maiorano A. H., (2009). "Criptografía: Técnicas de desarrollo para profesionales" 1ra. Ed. Buenos Aires: Alfaomega Grupo Editor Argentino.

[2] Pino Caballero G., (2002). "Introducción a la criptografía" Textos Universitarios / Ra-Ma Series Segunda edición, ilustrada, EditorRa-Ma S.A. Editorial y Publicaciones.

[3] Adams, C. S. L., (2002). "Understanding PKI: Concepts, Standards, and Deployment Considera-tions", 2 edn, Addison Wesley, USA.

[4] Ortega T. J., López Guerrero M. Á., García del Castillo Crespo E. C., (2005). "Introducción a la criptografía. Historia y actualidad", Ed. Universi-dad Castilla La Mancha.

[5] Lucena López, M. J., (2010). "Criptogra-fía y Seguridad en Computadores.", (http://sertel.upc. edu/tdatos/Libros/Lucena.pdf).

[6] Joshi, M. & Karkade, R., (2015). Network Se-curity 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.

[7] Barco C. G., (2007). "Bases matematicas de la criptografía de clave asimétrica: la aritmética mo-dular y la clave RSA." Vector, anual 2007, págs. 59+. Gale OneFile: Informe Académico link.gale.com/apps/doc/A258052730/IFME?u=a-non~5de27ffb&sid=googleScholar&xid=d4fae378. Consultado el 30 de noviembre de 2022.

[8] Wolfgag W., (2010). "Una introducción a la crip-tografía de clave pública." Segunda Edición. Edi-ciones Uninorte.