Blockchain aplicado a servidores de claves PGP

Trabajo Terminal No. 2019-B053

*Alumnos: *Estudillo Carranza Marco Antonio, Contreras Dothe Héctor Manuel*
Directores: Díaz Santiago Sandra, Moreno Cervantes Axel Ernesto
e-mail: marco_escar@hotmail.com

Resumen – Pretty Good Privacy (PGP) es utilizado ampliamente para brindar seguridad proporcionando autenticación, confidencialidad, integridad de los datos y no repudio. Se ha convertido en un estándar IETF conocido como OpenPGP, el cual implementa cifrado asimétrico con certificados compartidos a través de una red de servidores de claves. Sin embargo, esto requiere seguir una complicada serie de procesos en los que se incluye estar al tanto de la llave pública de cualquier usuario con el que se desee establecer una comunicación. Dichas llaves son gestionadas por los propios usuarios de la red, haciendo cada vez más costosa la validación de certificados conforme va creciendo la red. En el presente trabajo proponemos una forma diferente de administrar la infraestructura de los servidores de llave pública, utilizando la tecnología de blockchain.

Palabras clave – Blockchain; PGP; PKI; Servidores de llave pública.

1. Introducción

Las necesidades de protección de la información se han incrementado en gran medida con la utilización de los ordenadores y las redes de comunicaciones. La criptografía proporciona herramientas tales como PGP, que permiten proteger la comunicación entre dos partes para que nadie pueda entender su contenido y garantizar que solo el usuario receptor de un mensaje pueda leerlo o interpretarlo.

PGP es un protocolo utilizado para cifrar, descifrar y firmar mensajes o archivos mediante un par de claves. Es utilizado principalmente para cifrar comunicaciones en la capa de aplicación, generalmente en mensajes de uno a uno. La necesidad de su uso se aplica cuando se desea estar seguro de que sólo el receptor deseado puede acceder al mensaje, frustrando los esfuerzos de que terceras partes puedan interceptarlo y por ende descifrarlo. También se utiliza cuando se desea verificar la identidad del remitente. [1]

Aunque su propósito principal es la comunicación de correo electrónico cifrada de extremo a extremo, también se utiliza para mensajes cifrados y otros casos de uso, como los administradores de contraseñas, cifrado local de documentos o como firma de paquetes de software. [2]

Existen diferentes variaciones de PGP: OpenPGP, PGP y GPG, aunque generalmente todos hacen lo mismo. Cuando alguien menciona PGP, usualmente es seguro asumir que se está refiriendo al estándar OpenPGP.

PGP combina varios procesos de cifrado: hashing, compresión de datos, cifrado de clave simétrica y cifrado de clave pública. Una clave pública siempre está asociada a un nombre de usuario o dirección de correo. Durante el proceso de cifrado, PGP comprime los datos y se genera una clave aleatoria única que luego se utilizara para descifrar el mensaje realizando un proceso inverso del lado del receptor, garantizando así la seguridad del mensaje. PGP también soporta firmas digitales, lo que permite verificar la integridad y autenticidad de un mensaje para saber si este realmente fue enviado por quien dice, y saber si no fue alterado en el camino. [3]

Para el envío de información cada usuario debe contar con una llave pública y otra privada. El proceso se describe a continuación:

1. El remitente deberá de obtener la llave pública del destinatario.
2. La información (por ejemplo, un mensaje de correo electrónico) se cifrará con una clave simétrica temporal.
3. La clave simétrica temporal se cifrará con la clave pública del receptor.
4. Se agrega la clave simétrica cifrada al mensaje.

Como la clave pública se deriva de la clave privada, pero no viceversa, solo el titular de la clave privada puede descifrar y leer el mensaje. La distribución y gestión del par de llaves PGP es uno de los principales problemas que deben resolverse. [4]

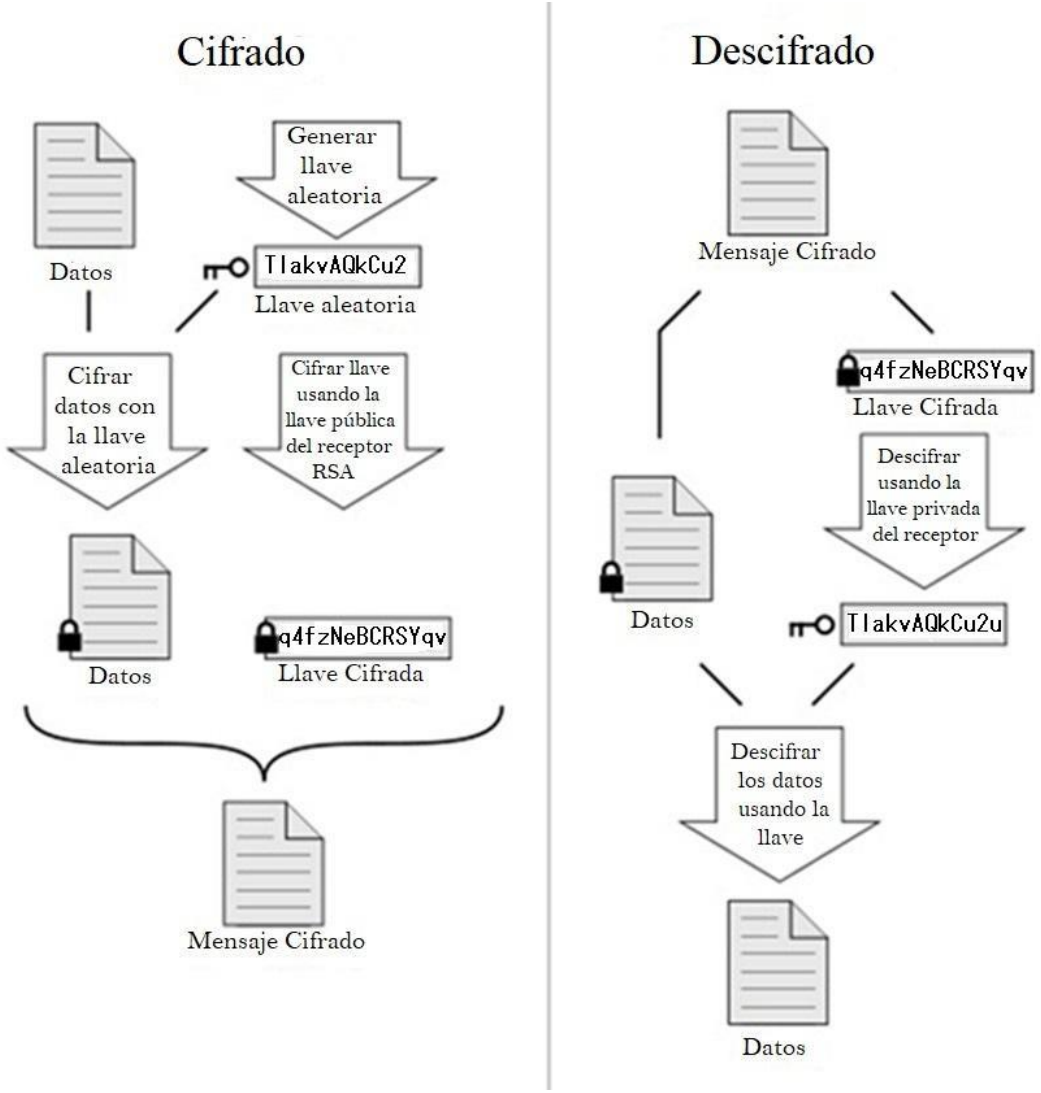

Figura 1.1. Diagrama de Operación del Protocolo PGP

A diferencia de la jerarquía centralizada tradicional de infraestructura de clave pública (PKI - Public Key Infraestructure), utilizada para emitir certificados SSL/TLS por una autoridad certificadora (CA - Certificate Authority) PGP adopta una red distribuida para la confirmación de identidad de certificados, conocida como "Red de Confianza" (Web of Trust - WoT). Por lo tanto, no existe una autoridad central en la que todos puedan confiar, en vez de ello, los participantes firman las claves de los demás y así, van construyendo la red de llaves públicas individuales. Esto a su vez, permite a los usuarios distribuir sus llaves públicas como certificados de identidad e incluso, nos brinda una cierta independencia, ya que cualquier usuario puede generar un par de claves y distribuir su clave pública directamente. Dado que no existe una autoridad centralizada, los usuarios pueden actualizar la fecha de vencimiento de su par de llaves y revocarlas en cualquier momento. De igual modo, se tiene la libertad de subir la llave pública a un repositorio de llaves y/o distribuirla directamente a otros usuarios.

Sin embargo, a pesar de los beneficios que se mencionan, PGP le deja al usuario la tarea de determinar la confiabilidad de las claves públicas de los destinatarios, así como la gestión de las mismas, recayendo en él la responsabilidad de actualizar y revocar los certificados. Estos cambios de revocación y actualización pueden llegar a tomar una cantidad de tiempo bastante alta, comprometiendo la seguridad de los certificados y por ende de los usuarios dentro de la red, haciendo mucho más costosa tanto en tiempo como en recursos la validación de las rutas de certificación conforme la red de usuarios va creciendo.

Es por ello que en el presente trabajo se propone adoptar un enfoque diferente para la gestión de las claves, basándonos en el esquema de blockchain, el cual permite entre otras cosas, la flexibilidad de que se pueda llevar una gestión descentralizada. Al final, el control del proceso sigue siendo de los usuarios, quiénes son los encargados de gestionar las llaves públicas de todos los presentes dentro de la red de confianza, respetando una de las grandes ventajas que representa PGP pero con la gran aportación de que cualquier transacción que se realice, actualización y/o revocación de certificados, deberán ser validados previamente por todos los nodos que componen la red, los cuales certificarán la autenticidad de los mismos.

Se elige blockchain por ser una tecnología distribuida, donde cada nodo de la red almacena una copia exacta de la cadena de bloques, la cual llevará un control de todos los registros y/o alteraciones que se vayan llevando a cabo dentro de la red, garantizando con ello la disponibilidad de la información en todo momento. En caso de que un atacante quisiera provocar alguna alteración en la cadena, debería anular la de todos los nodos de la red, ya que basta con que al menos uno esté operativo para que la información esté disponible. Por otro lado, al ser un registro consensuado, donde todos los nodos contienen la misma información, resulta casi imposible alterar la misma, asegurando así su integridad. Si un atacante quisiera modificar la información en la cadena de bloques, debería modificar la cadena completa en todos los nodos. [5]

A continuación, se presenta una tabla con la información de trabajos similares.

Nombre del proyecto	Primitiva	Objetivo del proyecto
BlockPGP: A Blockchain-based Framework for PGP Key Servers [6]	Optimización del protocolo PGP.	Proponer un marco de gestión de la infraestructura de los servidores de llave de PGP, utilizando blockchain..
TOFU for OpenPGP [7]	Detección de nuevos ataques a usuarios en PGP.	Diseño e implementación de la política de confianza de primer uso o trust-onfirst-use(TOFU) en PGP, para detectar ataques nuevos en usuarios que previamente hayan verificado las firmas.
From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain [8]	Proporcionar un nuevo formato de verificación de certificados PGP.	Diseñar e implementar un prototipo de mejora sobre PGP, aprovechado la cadena de transacciones de Bitcoin y blockchain.

Tabla 1. Proyectos similares

2. Objetivo

Objetivo General

Diseñar e implementar un esquema más eficiente y seguro para la gestión de claves públicas en la infraestructura del protocolo PGP utilizando la estructura de blockchain.

Objetivos específicos

- Diseñar la arquitectura para la gestión de claves descentralizada.
- Implementar arquitectura de PGP con blockchain.

3. Justificación

PGP es posiblemente uno de los cifrados más extendidos en la actualidad para las comunicaciones de datos a través de Internet. Sin embargo, a pesar de su gran difusión, su estructura sigue siendo un problema a resolver, ya que por la forma en que opera, se vuelve complejo de gestionar para los usuarios que lo utilizan y también abre brechas de seguridad que pueden ser aprovechadas por los atacantes.
Es por ello que se plantea el uso de la tecnología blockchain, ya que éste esquema permite el intercambio de información y transacciones entre dos o más participantes mediante un mecanismo completamente seguro e irreversible. Esta operación no requiere de un intermediario centralizado que identifique y certifique la información, sino que está distribuida entre los múltiples participantes de la red que registran y validan las transacciones sin que haya necesidad de confianza entre ellos. Cada participante cuenta con una copia exacta de la información, permitiendo llevar a cabo transacciones trazables y confiables.

4. Productos o Resultados esperados

El resultado del trabajo conducirá al diseño de una arquitectura basada en blockchain, que permitirá la gestión de los certificados de clave pública en la implementación del protocolo PGP. Para ello, se describirán las operaciones de las cuáles estará dotada la aplicación que se desarrollará a lo largo del trabajo propuesto:

- Los usuarios de la red podrán generar sus certificados de clave pública y privada con alguna de las herramientas de PGP existentes.
- Los certificados de claves sólo podrán ser cargados, actualizados y/o revocados únicamente por los propietarios de los mismos.
- Todos los participantes de la red tendrán una réplica sincronizada de la cadena de bloques que conformarán los certificados válidos.

Para lograr lo anterior, se describirá brevemente la forma en que operará la arquitectura a diseñar:

1. Los nuevos usuarios de la red generarán sus certificados.
2. Una vez que los usuarios ingresen a la red y cuenten con sus certificados, estos podrán darlos de alta, modificarlos y/o revocarlos si así lo desean.
3. Para que las operaciones mencionadas queden registradas en la cadena de bloques, éstas deberán ser validadas por todos los nodos de la red.
4. Una vez que la operación se valida, la transacción se registra en la cadena de bloques y la información se replica entre todos los participantes.

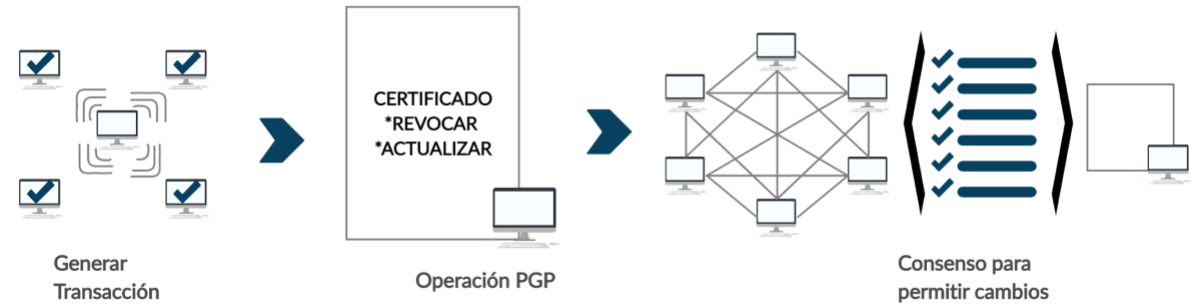

Figura 4.1: Diagrama de Operación del Proyecto.

Con lo anterior, se tiene un esquema en donde se propone el diseño y construcción de un enfoque que brinda mayor seguridad y trazabilidad de los certificados en el protocolo de comunicación PGP.

5. Metodología

Para el desarrollo del proyecto se propone utilizar la metodología en cascada, ya que esta nos permite manejar una estructura sencilla, con fases del proyecto claramente definidas, además de permitirnos tener una estimación muy acertada de la carga de trabajo que se tendrá a lo largo del trabajo terminal. Del mismo modo, esta metodología nos permite tener una representación cronológica de forma sencilla, lo cual para este caso, es adecuado ya que nos permitirá visualizar de mejor forma el manejo de tiempos del proyecto.

A continuación se presenta un diagrama del modelo en cascada que se usará en este proyecto.

Figura 5.1: Modelo en cascada de cinco niveles, basado en las propuestas de Winston W. Royce.

Como se puede observar, es un modelo de la metodología en cascada con una ampliación, ya que además de contar con las 5 etapas; análisis, diseño, implementación, verificación y mantenimiento también considera un proceso de comprobación de los resultados entre cada una de las etapas.

6. Cronograma

Nombre del alumno: Marco Antonio Estudillo Carranza

Etapa	Actividad	ENE	FEB	MAR	ABR	MAY	JUN	AGO	SEP	OCT	NOV	DIC
Análisis	Investigación de Blockchain y PGP											
	Reunión con los directores para retroalimentación											
	Blockchain que se aplicarán al protocolo PGP											
Diseño	Blockchain											
	Generar el documento de diseño de software(SDD).											
	Elaboración de la presentación de TT1											
	Evaluación de TT1											
Implementación	Desarrollo de la arquitectura propuesta											
	Generación del reporte técnico.											
	implementación del nuevo esquema											
Verificación	Pruebas de seguridad en la nueva arquitectura											
	Presentación del sistema a los directores.											
	Últimas pruebas de integración y seguridad											
	Elaboración de la presentación de TT2											
	Evaluación de TT2											

Nombre del alumno: Héctor Manuel Contreras Dothe

Etapa	Actividad	ENE	FEB	MAR	ABR	MAY	JUN	AGO	SEP	OCT	NOV	DIC
Análisis	Realizar trabajo de investigación											
	Reunión con los directores para retroalimentación											
	Generación del documento de especificación de requisitos(SRD).											
Diseño	Generar el documento de diseño de software(SDD).											
	Verificación de resultados esperados en la etapa anterior.											
	Elaboración de la presentación de TT1											
	Evaluación de TT1											
Implementación	Desarrollo del sistema*											
	Generación del reporte técnico.											
	Verificación de resultados esperados en la etapa anterior.											
Verificación	Pruebas del sistema.											
	Presentación del sistema a los directores.											
	Verificación de resultados esperados en la etapa anterior.											
	Elaboración de la presentación de TT2											
	Evaluación de TT2											

7. Referencias

[1] “PGP Encryption Software: What is it and How Does it Work?”. Consultado el 25 de Agosto de 2019, desde https://www.alienvault.com/blogs/security-essentials/explain-pgp-encryption-an-operational-introduction

[2] Jekull. "OpenPGP(2018, Feb)", Consultado el 25 de Agosto de 2019, desde https://www.openpgp.org/

[3] González, Gabriela. “Qué es PGP y por qué te interesa usarlo”. Consultado el 25 de Agosto de 2019, desde https://blogthinkbig.com/que-es-pgp

[4] C. Adams and S. Lloyd, “Understanding PKI: concepts, standards, and deployment considerations.” Addison-Wesley Professional, 2003.

[5] Yakubov, Alexander & Shbair, Wazen & State, Radu. (2018). "BlockPGP: A Blockchain-based Framework for PGP Key Servers". Consultado el 25 de Agosto de 2019, desde https://www.researchgate.net/publication/329337577_BlockPGP_A_Blockchain-based_Framework_for_PGP_Key_Servers

[6] WeLiveSecurity. Pastorino, Cecilia, “Blockchain: qué es, cómo funciona y cómo se está usando en el mercado”. Consultado el 27 de Agosto de 2019, desde https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

[7] H. Walfield,W. Koch ,"TOFU for OpenPGP", Consultado el 25 de Agosto de 2019, desde https://gnupg.org/ftp/people/neal/tofu.pdf

[8] Wilson, Duane, Ateniese, Giuseppe, “From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain”, Consultado el 25 de Agosto de 2019, desde https://www.researchgate.net/publication/281144277_From_Pretty_Good_To_Great_Enhancing_PGP_using_Bitcoin_and_the_Blockchain

8. Alumnos y Directores

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Art. 3, fracc. II, Art. 18, fracc. II y Art. 21, lineamiento 32, fracc. XVII de la L.F.T.A.I.P.G.
PARTES CONFIDENCIALES: No. de boleta y Teléfono.

Contreras Dothe Héctor Manuel. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2013380489, Tel. 55 5464 3385, email: manuel09b@gmail.com.

Firma:_____

TURNO PARA LA PRESENTACIÓN DEL TRABAJO TERMINAL:

Estudillo Carranza Marco Antonio. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2014630139, Tel.: 55 3280 9896, email: marco_escar@hotmail.com.

Firma:_____

Díaz Santiago Sandra. - Doctorado en Ciencias en Computación (CINVESTAV-IPN, 2014). Maestría en Ciencias (Matemáticas) (UAM-Iztapalapa, 2005). Licenciatura en Computación (UAM-Iztapalapa, 1998). Profesor titular en ESCOM (Departamento de Ciencias e Ingeniería de la Computación) desde 2004. Áreas de interés: criptografía, pseudoaleatoriedad, seguridad demostrable. Extensión: 52022, correo electrónico: sdiazs@gmail.com, sdiazsa@ipn.mx

Firma:_____

Moreno Cervantes Axel Ernesto. - M. en C. en Computación CINVESTAV. Ing. en Sistemas Computacionales ESCOM/IPN. Profesor de ESCOM/IPN (Dpto. de Sistemas Distribuidos) desde ____. Áreas de Interés: MRS, Redes. Ext. 52028, email: axelernesto@gmail.com

Firma:_____