Ciencias Matemáticas, Vol. 33, No. 1, Pag. 13-17, 2019

Depósito y Recuperación de Llaves, un Elemento a Considerar para la Infraestructura de Llave Pública en Cuba

Key Escrow and recovery, an aspect to take into account for the Public Key Infrastructure

Teresa Bernarda Pagés López*

Resumen Se caracteriza el mecanismo de depósito y recobrado de llave en el mundo, teniendo en cuenta el estudio académico realizado por varios autores. Se expone una caracterización de la Infraestructura de Llave Pública en Cuba, desde el documento legal que la pone en vigor. Se propone la inclusión del mecanismo de depósito y recobrado de llave en la Infraestructura de Llave Pública de Cuba.

Abstract We qualify the key escrow and key recovery mechanisms in the world, having in beading the academic study accomplished for several authors. We expose the Cuba's Public Key Infrastructure characteristics since law document. We propose inclussion key escrow and key recovery mechanisms in the Cuba's Public Key Infrastructure.

Palabras Clave
Infraestructura de Llave Pública (ILP), depósito de llaves, recobrado de llaves.

[1] *Instituto de Criptografía, Universidad de la Habana, La Habana, Cuba, teresa.bernarda@matcom.uh.cu*

Introducción

Dentro del variado escenario que ofrecen hoy las nuevas Tecnologías de la Información (TI), son propuestos para los sistemas de protección criptográfica una serie de requisitos que acompañan al cifrado y están relacionados con el depósito y la recuperación de las llaves, así como por la existencia de terceras partes confiables que permiten a las agencias del gobierno realizar interceptaciones ocultas a las comunicaciones, a partir de que tienen el acceso a las llaves de cifrado que estos les proporcionan. Estas exigencias, reconocidas en la literatura académica y especializada como key escrow y key recovery son aplicables bajo el cumplimiento de disímiles propiedades asociadas con posibles riesgos técnicos, costos adicionales e implicaciones que acarrea el instaurar este tipo de sistemas. Es un mecanismo que beneficia al fortalecimiento de la Seguridad Nacional de muchos países. Su implementación y uso están asociados a diferentes objetivos y niveles de usuarios, dentro de los que se destaca como el más positivo: proteger a la sociedad de individuos inescrupulosos que utilizan los sistemas de comunicaciones con intenciones criminales y terroristas. Sin dejar de mencionar otros relacionados con la salva de datos e información importante que son vitales para el desarrollo de cualquier nación. Sin embargo, este tema también tiene su lado de abstención, relacionado con el temor de los individuos a la violación de su privacidad. Desde hace aproximadamente 20 años, prestigiosos académicos en el área de la Criptografía, han publicado los resultados de sus investigaciones sobre el presente tema. Un estudio relevante sobre key escrow es dado por D.E. Denning and D. K. Branstad en [1,2,3]. Otra arista del análisis está relacionada con su legalidad y estandarización a partir del reconocimiento que realizan los principales grupos de trabajo académicos que lo asumen y tienen en cuenta como elemento necesario dentro del desarrollo tecnológico actual. [1,2,3]. En Cuba, durante años se ha trabajado por la instauración de una Infraestructura de Llave Pública (ILP), aspecto que fue asumido y legalizado con la Resolución No. 2 de 2016. Sin embargo, a pesar de que la estructura organizativa de la sociedad y sus leyes la favorecen, no se asumió como parte de la tecnología desarrollada en la ILP un sistema de depósito y recobrado de claves, que sin lugar a dudas favorecería lo dispuesto. En el presente trabajo se da una propuesta de solución, organizativa y técnica que permitirá establecer de manera voluntaria estos mecanismos dentro de las Infraestructura de Llave Pública corporativa desplegada en el sistema empresarial o en las cooperativas que hoy, se establecen en el trabajo por cuenta propia. Merece señalar, además, que este mecanismo resulta de mucha utilidad en instituciones del Estado que manejen información sensible.

1. Algunas ideas sobre depósito y recuperación de llaves en el mundo

El depósito de llaves ofrece un servicio valioso a individuos, organizaciones y a la sociedad. Al incorporar el depósito de llaves en su política criptográfica, los gobiernos están garantizando la custodia del material criptográfico y la seguridad de la información y las tecnologías que la crean, mueven y protegen. El programa de depósito de llaves propuesto por los gobiernos es generalmente voluntario, lo que no garantiza que los criminales seleccionen a este en lugar del cifrado que no tiene las llaves resguardadas, algo que continúa siendo un problema permanente para la seguridad, dado que no existen redes completamente inaccesibles.

Los sistemas de cifrado con recuperación de llaves proporcionan formas de acceso a la información (texto claro) independientemente del canal de cifrado y descifrado que se emplee. Un sistema de cifrado con depósito de llaves (Key Escrow) es un sistema de cifrado con una capacidad de descifrar salvas, esto permite a personas autorizadas (oficinistas de una organización, funcionarios del gobierno, usuarios en general) bajo ciertas condiciones establecidas, descifrar textos cifrados con la ayuda de información suministrada, por una o más partes confiables encargadas de custodiar las llaves que recobran datos especiales. Las llaves que recobran datos son las que permiten determinar la llave de cifre/descifre del dato, pero con ellas no se cifra/descifra directamente el dato. El término depósito de llaves o key escrow es usado para referirnos a las salvas de estas llaves de recobrado de datos. Otros términos también usados son archivos de llaves, salva de llaves, sistema de recobrado de llaves y terceras partes confiables.

1.1 Necesidad

La necesidad de poder contar con un sistema de depósito y recobrado de llaves puede estar dada por varias causas, en primer lugar, por la necesidad de cifrar datos confidenciales, ya sea en los procesos de almacenamiento y transferencia de documentos digitales, como en el aseguramiento del correo y el comercio electrónico, en la protección de datos en páginas web o en el uso de protocolo de conexión de redes seguras con este propósito. Otra causa de esta necesidad está relacionada con el problema que puede presentársele a los individuos con sus llaves, tipificados por el extrvío o por la presencia de llaves corruptas. También puede estar motivada por problemas que se presentan en las empresas, originados por descuido, ausencia o descontento de sus trabajadores o ante la imposibilidad de aplicar la ley de Seguridad Nacional.

1.2 Componentes y características del cifrado con depósito y recuperación de llaves

1. **Componente seguridad de usuario.** Este es un dispositivo de hardware o programa de software que proporciona capacidad de cifre y descifre de dato, aspecto importante para respaldar la función de depósito de llaves. Incluye también adjuntar un campo recobrado de dato para dato cifrado, que puede ser parte del mecanismo de distribución normal de llaves [1], [2]. Este componente cifra y descifra dato y ejecuta funciones que respaldan el proceso de recobrado de dato.

2. **Componente depósito de llaves.** Es operado por agentes responsabilizados con el depósito de llaves, administra el depósito o almacén y libera o usa datos recobrados de llaves. Puede ser parte de un sistema administrador de certificado digital de llave pública o de una infraestructura administradora de llave en general. Además, es responsable del almacenamiento de todas las llaves de recobrado de datos y de la asistencia del componente recobrado de datos que proporciona los datos o servicios requeridos.

3. **Componente recobrado de dato.** Se compone por los algoritmos, protocolos y equipamientos necesarios que permiten obtener el texto claro desde el texto cifrado, además de la información en el campo recobrado de datos. Se activa solamente ante la necesidad de ejecutar un recobrado de dato específico autorizado. Además, apoya recobrar el texto claro desde el dato cifrado usando información suministrada por el componente depósito de llaves, en el campo recobrado de datos.
   Estos componentes lógicos están interrelacionados entre sí, y el diseño de uno repercute decisivamente en los otros.

Caracterización

El despliegue de las infraestructuras de cifrado, basadas en recuperación de llaves, requiere cumplir exigencias rigurosas de seguridad y confianza, lo que conlleva al incremento de su costo [3].
La adopción del cifrado con depósito y recuperación de llaves debe ser elección de los gobiernos, entidades e individuos, según la instacia y permisión de las leyes y regulaciones en cada lugar, esto conlleva a la aplicación de estándares internacionales, o al menos de soluciones debidamente certificadas en cada nivel. Resulta muy conveniente aprovechar la Infraestructura de Llave Pública como tecnología que adopte este mecanismo, lo que técnicamente es asequible por su modularidad [5, 6].
Los sistemas de cifrado con recuperación de llaves funcionan de diversas maneras. Existen propuestas de depósito de llaves que confían en el almacenamiento de llaves privadas por parte de instituciones del Estado y, más recientemente, por entidades privadas elegidas. Otros sistemas tienen agentes de depósito o agentes de recuperación de llaves que mantienen la capacidad de recuperar las llaves de una sesión de comunicaciones cifradas o archivos almacenados, en concreto; estos sistemas requieren que tales llaves de sesión estén cifradas con una llave conocida por un agente de recuperación e incluidas con los datos. Algunos sistemas son concebidos para distribuir la capacidad de recuperar llaves entre varios agentes, a partir de un sistema de secreto compartido [4].

2. La Infraestructura de Llave Pública en Cuba

En Cuba, actualmente rige la Resolución No. 2 de 2016 [8, 9], que pone en vigor la Infraestructura de Llave Pública (ILP) en interés de la protección criptográfica de la información oficial, con anexo de su reglamento que dispone su funcionamiento.

Su implantación proporciona el marco de acción para un amplio conjunto de componentes, aplicaciones, políticas y prácticas con las que se obtienen las cuatro funciones principales de seguridad: confidencialidad, autentificación, integridad y no repudio. Sin embargo, no se concierta nada acerca de la existencia de mecanismos, funciones, servicios o funcionarios relacionados con el depósito y recobrado de las claves.

Esto no significa que, de algún modo, para propósitos muy específicos esta es una exigencia de la propia infraestructura de llave pública. Un ejemplo muy sencillo que así lo ilustra es la necesidad de preservar durante un tiempo relativamente largo, 15 ó 10 años, las llaves de la Autoridad Raíz y de las autoridades de Certificación Intermedias, que responden al primer nivel jerárquico de la topología establecida, las cuales requieren mecanismos muy celosos para el resguardo seguro de sus llaves privadas.

En el caso de Cuba, dado las exigencias de sus regulaciones para la Criptografía [7], la Infraestructura de Llave Pública se suscribe a la autorización y supervisión del Ministerio del Interior lo que determina que cualquier propuesta de uso de algún mecanismo de depósito y recobrado de llaves, por parte de otros Organismos o instancias de la arquitectura nacional existente, debe ser consultado y aprobado por dicho Organismo.

Este es un tema bastante complicado de tratar porque encierra muchas miradas y no siempre la aplicación organizativa de la tecnología tiene el mismo efecto para diferentes plataformas en las que se despliega. Sin embargo, en el caso que nos ocupa, se proyecta una mirada que proporcione una solución para el contexto de la ILP, permitiendo organizar la seguridad de la misma en una red corporativa e institucional.

En el contexto mundial, según lo establecido por las normas y estándares internacionales [5, 6], la conceptualización de la ILP no incluye el control del material criptográfico. Sin embargo, en Cuba el flujo productivo de los certificados digitales involucra la generación, producción, distribución y almacenamiento de los criptomateriales [7], lo que determina que la estructura y funcionamiento de las ACs varíe con relación a las existentes en otras partes del mundo, aspecto que favorece nuestra propuesta de incluir el depósito y recobrado de llaves en nuestra infraestructura, bajo un control estricto y con personal calificado y certificado en estas funciones.

2.1 Necesidad

En el caso de nuestra propuesta de incluir el mecanismo de depósito y recobrado de llaves la necesidad está dada en primer lugar, a nivel del Estado, por un problema de Seguridad Nacional, por cuanto la ILP está administrada centralmente, posee una topología jerárquica estricta y tiene subordinada en el primer nivel todas las autoridades de certificación de todos los OACEs y principales entidades del país, esto significa que se incluyen las infraestructuras críticas y todo lo que determina el desarrollo político, económico y social de Cuba, razón importante para tener la información confidencial protegida criptográficamente.

Existe además una necesidad condicionada por la seguridad de los datos de organizaciones que establecen ILP corporativas dentro de sus organismos y empresas. Finalmente, los individuos como entes sociales expresan la necesidad de la privacidad de sus datos, incluyendo los personales, que están recogidos en entidades estatales como pueden ser, entre otros, los hospitales, los registros de identificación y los centros laborales.

Una situación adjudicable a cualquiera de estas instancias es la necesidad de la salva de las llaves y datos ante la ocurrencia de fenómenos meteorológicos, accidentes o actos terroristas, entre otros. Es por ello que se aboga por tener más de una salva descentralizada geográficamente.

Hoy, nuestra sociedad llamada a informatizarse, necesita de estos servicios que aportan un mecanismo de seguridad dentro de la ILP.

2.2 Caracterización

El mecanismo de depósito y recobrado de llaves dentro de la infraestructura de llave pública estará caracterizada por:

- Alta exigencia de seguridad y confianza, lo que implica alta responsabilidad de todas las autoridades de certificación y funcionarios designados a estas tareas, identificados con un alcance amplio de sus funciones y aplicación de la Criptografía en el uso de algoritmos criptográficos simétricos y asimétricos que utilizan certificados digitales.
- Uso de Bases de Datos en almacenamientos tecnológicamente superiores, capaces de realizar el depósito y recobrado de llaves con procesos de verificación y validación.
- Diseño modular, interoperable y escalable que facilita su inserción con menos costos.
- Uso de protocolos, algoritmos y equipamiento actualizado, con alta capacidad de descifre, recobrado de llave y salva de datos y llaves.

2.3 Propuesta de Modificación

De acuerdo a lo expuesto anteriormente, nuestra propuesta está encaminada a realizar una modificación en el funcionamiento de la ILP, consistente en adicionar el mecanismo de depósito y recobrado de llaves, instaurándolo como un servicio opcional u obligatorio, en dependencia de las políticas que se establezcan en cada AC y conforme a su jerarquía u objeto social. Teniendo en cuenta lo que establece la Resolución 2 de 2016, en Cuba se reconocen en la estructura organizativa

de la ILP las siguientes entidades prestadoras de servicios criptográficos de certificación:

- Una Autoridad Raíz consignada al Servicio Central Cifrado del Ministerio del Interior.
- Prestadores corporativos, encargados de realizar actividades para el empleo de los certifcados digitales por los suscriptores en el marco interno de un órgano, OACE o entidad del Estado.
- Prestadores comerciales, básicamente empresas o entidades especializadas que, en el marco de su objeto social, están en capacidad de realizar a favor de terceros actividades de esta índole, mediante la venta de certifcados digitales y cobros por dichos servicios a suscriptores.

Lo que se traduce en la estructura estándar de la Infraestructura de Clave Pública (PKI) en el mundo, como: Autoridad Raíz, Autoridad de certificación (que se denominan intermedias, entre la raíz y el usuario final) Autoridad de Registro (en ocasiones pueden fusionarse con las autoridades de certificación) y Usuario, que puede ser, por ejemplo, una persona natural o jurídica, un software o un hardware.
Nuestra propuesta consiste en ampliar la funcionalidad de la ILP con la introducción del funcionario de depósito y recobrado de llaves, en autoridades de certificación de cualquier nivel.
Desde este punto de vista el procedimiento para la solicitud voluntaria de este servicio sería: el suscriptor, en modelo creado para este fin, solicita este servicio, el cual se anexa al de solicitud del certificado digital y operacionalmente, una vez que se genere el material criptográfico para el certificado digital y se entregue la llave privada (en el formato PKCS 12) al suscriptor, el funcionario de depósito y recobrado en función, depositará la llave privada cifrada en la base de datos creada para este fin, en el tiempo acordado.
Existe otra forma del servicio que responde a la obligatoriedad del mismo cuando los requerimientos de seguridad de la entidad así lo requieran, en este caso es un servicio que se da siempre y estará asociado a entidades del Estado que manejan información sensible tanto, científica, diplomática, económica, militar como de otra índole.
Las llaves depositadas estarán cifradas por una llave de sesión y el acceso a ella para el recobrado se hará a través de un protocolo criptográfico de secreto compartido, en el que deben intervenir al menos dos partes:

- Autoridad de certificación/registro.
- Funcionario responsable del depósito/recobrado.

2.4 Requerimientos y Funcionalidad

- La llave privada debe ser generada por un proveedor de servicios criptográficos o el propio usuario a través de algún módulo criptográfico adquirido legalmente.
- El funcionario de depósito debe estar seguro de que la llave depositada es la correcta, al realizar el macheo con la llave pública del usuario.
- El funcionario de depósito es responsable de guardar cifrada la llave privada del usuario.
- El usuario y el funcionario de depósito/recobrado de llaves no deben conocerse entre sí.

3. Protocolos criptográficos utilizables para realizar el depósito y recobrado de llaves

El mecanismo de depósito y recobrado de llaves puede ser implementado por software o hardware. Consiste en el registro de la clave privada de un usuario en el depósito o almacen.
Una de las premisas importantes a tener en cuenta en estos protocolos es que cada parte esté en condiciones de determinar la identidad del resto de los participantes, evitando el acceso de intrusos. Para ello se requiere del secreto de la llave y la identificación de las partes con acceso, que solo es posible garantizar con la autenticación de usuarios y datos de origen, así como con la autenticación y confirmación de la llave. Sobre estos conceptos se construye la base de las relaciones de confianza de la ILP.
Un protocolo de establecimiento de llaves, autenticado con secreto compartido es definido utilizando el Algoritmo de Diffie-Hellman [4] con dos pasadas, para evitar ataques pasivos.
Sea A: Autoridad de certificación/registro.
Sea B: Funcionario responsable del depósito/recobrado de llave.
Se establece una comunicación entre las partes que van a compartir el secreto a través de un canal abierto, sea el caso propuesto realizar el intercambio entre A y B.
Resultado: Compartir conocimiento de la llave K por A y B sin que uno conozca la parte secreta del otro.

- Se selecciona aleatoriamente un número primo grande p del orden de los 2048 bits y un generador α de $\mathbb{Z}_p^*$ tal que $2 \leq \alpha \leq p-2$, y se publican.
- *A* selecciona como llave privada de larga duración un entero aleatorio a, tal que $1 \leq a \leq p-2$ y computa su correspondiente llave pública también de larga duración $z_A = \alpha^a (mod p)$.
- *A* selecciona aleatoriamente un valor secreto x, tal que $1 \leq x \leq p-2$ y calcula $\alpha^x (mod p)$.
- *B* selecciona como llave privada de larga duración un entero aleatorio b, tal que $1 \leq b \leq p-2$ y computa su correspondiente llave pública también de larga duración $z_B = \alpha^b (mod p)$.
- *B* selecciona aleatoriamente un valor secreto y, tal que $1 \leq y \leq p-2$ y calcula $\alpha^y (mod p)$.

- $A \rightarrow B : \alpha^x (mod p)$, B calcula el valor de la llave compartida $K = (\alpha^x)^b k_A^y mod p = \alpha^{(bx+ay)}$

- $B \rightarrow A : \alpha^y (mod p)$, A calcula el valor de la llave compartida $K = (\alpha^y)^a k_B^x mod p = \alpha^{(ay+bx)}$.

En este protocolo la seguridad descansa en la selección de los parámetros criptográficos que deberán corresponderse con los requerimientos criptográficos expuestos en [10, 11].
En el marco de la ILP también podemos realizar el depósito y recobrado de llaves usando certificados digitales con un algoritmo asimétrico. Por ejemplo, en el caso de usar el RSA, el procedimiento sería:
A envía a B un mensaje y B hace acuse de recibo con otro mensaje firmado.
Resultado: El protocolo logra autenticación mutua de entidad o usuario final y transporte de la llave secreta con autenticación de llave.
Sea, $P_x(y)$: denota el resultado de aplicar la llave pública de x al dato y.
$S_x(y)$: denota el resultado de aplicar la llave privada de x al dato y.
$Cert_x$ es un certificado que vincula la parte x, a una llave pública adecuada para cifrar y validar firma.
Disposición del Sistema: Cada parte puede adquirir la llave pública de la otra parte a priori.
Sea: $D_A = (r_A, B, P_B(k_1))$ el dato de A correspondiente a un valor aleatorio r_A, generado por A, un identificador de B y la llave secreta k_1 también generada por A y cifrada con la llave pública de B.
$D_B = (r_B, A, P_A(k_2))$ el dato de B correspondiente a un valor aleatorio r_B generado por B, un identificador de A y la llave secreta k_2 también generada por B y cifrada con la llave pública de A.
Mensajes del Protocolo:

$$A \rightarrow B : Cert_A, D_A, S_A(D_A), \quad (1)$$
$$A \leftarrow B : Cert_B, D_B, S_B(D_B) \quad (2)$$

A y B establecen comunicación por un canal inseguro utilizando este protocolo que les permite obtener llaves secretas compartidas y cifrar su información con la certeza de que esas llaves son de cada una de las partes que dicen ser.
De esta forma cada una de las partes involucradas en el depósito y recobrado de llaves pueden realizar el depósito de llaves siendo, cada una, responsable de una parte del secreto.
En este protocolo la seguridad descansa en la selección de los parámetros criptográficos que deberán corresponderse con los requerimientos criptográficos expuestos en [10, 11]. Este proceso solo es comprensible en el contexto de un protocolo, donde dos o más partes comparten el secretode la llave criptográfica que se usará para recobrar la llave depositada. En este caso las partes A y B deben intervenir de conjunto en este proceso para que sea efectivo.

Conclusiones

Con un sentido moderado de la seguridad se hace necesario poder contar con un mecanismo de depósito y recobrado de llave, incluso en el solo cumplimiento de los objetivos más nobles, relacionados con la seguridad del país y la preservación del orden que requiere una sociedad informatizada.
En este trabajo se caracteriza y explica el funcionamiento de este mecanismo para un contexto más amplio y se propone su adecuación al entorno cubano, aprovechando la cobertura que ofrece la infraestructura de llave pública, actualmente desplegada en el país.

Referencias

[1] Denning, D.E. and M. Smid (1994). Key escrowing today. IEEE Comm. Magazine, 32 (9), 58-68.

[2] Denning, D.E., Branstad, D.K.: A taxonomy of key escrow encryption systems. ACM, 39(3), 1996.

[3] Denning, D.E. (1996). Descriptions of key escrow systems. Comm. of the ACM, February 26, 1997.

[4] Adleman, L. M. A Subexponencial Algorithm for the Discrete Logarithm Problem with Applications to Cryptography, Proc. 20th IEEE Found. Comp. Sci. Symp. (1979), 55-60.

[5] NIST SP 800-57 Recommendation for Key Management, Part 1: General (Revised), March 2007.

[6] RFC 3647. Internet X.509 PKI Certificate Policy and Certification Practices Framework. Nov. 2003.

[7] Decreto-Ley No.199 Sobre Seguridad y Protección Información Oficial.

[8] Resolución No.2/2016, MININT, ISSN 1682-7511, Gaceta Oficial No.24, Extraood. 1/097/2016, Cuba.

[9] The Telecommunications Illustrated Dictionary. Pág. 552. J.K. Petersen, 2da edición. CRC Press 2002.

[10] Pagés L. T. y García G. A., Generación de Parámetros Criptográficos de Clave Pública Seguros. Boletín de la SCMC, vol. 9, No.1, abril 2011, pp. 47-56 SCMC ISSN 1728-6042 RNPS. 2017.

[11] Pagés L. T., Requerimientos de los Parámetros Criptográficos de la Infraestructura de Llave Pública en Cuba, Tesis de Doctorado, mayo 2012.

Referencias