Artículo original

Esquema de confianza basado en Infraestructura de clave pública (PKI) para el intercambio de información clínica electrónica en el sistema XAVIA HIS

PKI-based trust scheme for the exchange of electronic clinical information in the XAVIA HIS system

Ing. Yanssel Urquijo Morales[1]* 0000-0001-8738-0138
Dr.C. Arturo Orellana García[1] 0000-002-3652-969X

[1] Universidad de Ciencias Informáticas. Centro de Informática Médica, La Habana, Cuba

*Autor para la correspondencia: yurquijo@uci.cu

RESUMEN

La seguridad informática se ha convertido en una necesidad y un derecho de todos los ciudadanos. Los sistemas informáticos empleados en el sector de salud poseen un almacenamiento digital fácil y sostenible que debe garantizar la privacidad e integridad de la información, lo cual constituye cuestión delicada. En Cuba no está definido un esquema PKI (Públic Key Infraestructure) o Infraestructura de Clave Pública, centralizado a nivel nacional que propicie y garantice la seguridad de la información sensible en el sistema de salud pública, lo cual pone en riesgo la autenticidad, integridad y confidencialidad de los datos médicos personales.

Este trabajo tiene como objetivo diseñar una estructura de seguridad centrada en la PKI entre las instituciones de salud, a partir de la infraestructura de llave pública nacional como autoridad de certificación raíz.

Se realizó un análisis documental sobre la actualidad del tema, se realizaron entrevistas a administrativos, gestores hospitalarios y especialistas en seguridad informática, lo cual permitió crear las bases de la investigación.

Se obtuvo un esquema de confianza que propicia el intercambio seguro de los registros médicos de los pacientes entre instituciones de salud. La implementación de una infraestructura PKI en el sector sanitario permite que las instituciones que requieran intercambiar registros médicos, a través de una red, puedan hacerlo con un alto nivel de seguridad.

Palabras Clave: firma digital; PKI; sector de salud; seguridad de la información; XAVIA HIS.

ABSTRACT
Computer security has become a necessity and a right for all citizens. The IT systems used in the health sector have much easier and more sustainable digital storage and guarantee the privacy and integrity of information, which are sensitive issues. In Cuba, there is no centralized PKI (Public Key Infrastructure) scheme at the national level that promotes and guarantees the security of sensitive information in the public health system, which puts the authenticity, integrity and confidentiality of personal medical data at risk.
The aim of our work was to design a security structure centered on PKI among health institutions, based on the national public key infrastructure as root certificate authority (CA). In order to achieve this, a documentary analysis was carried out on the current state of the art in the subject; as well as interviews with administrative staff, hospital managers and specialists in computer security, which allowed the research bases to be created.
As a result, a trust scheme was obtained that promotes the secure exchange of patients' medical records between health institutions. The implementation of a PKI infrastructure in the health sector allows institutions to exchange medical records through a network with a high level of security.
Keywords: digital signature; PKI; health sector; information security; XAVIA HIS.

Recibido: 12/6/2020

Aprobado: 29/9/2020

Introducción

La aplicación de las Tecnologías de la Información y las Comunicaciones (TICs) en el sector salud no solo suponen desarrollo y evolución sino una transformación del pensamiento y organización de los procesos sustantivos del sector. La digitalización de los sistemas de salud a nivel mundial ha mejorado significativamente la calidad de vida de los usuarios, además de reducir costos y tiempos de atención.

En el entorno de la salud, los sistemas de información se han vuelto más complejos ya que abarcan más áreas y procesos de información. De esta forma se tiene que existe una cantidad cada vez mayor y heterogénea de sistemas y plataformas. Este hecho exige una mayor integración y necesidad de intercambio de información según se establece en los principios de la estrategia de informatización del sector de la salud en Cuba [(1)].

Los datos personales de salud son datos sensibles. La protección de la privacidad y la salvaguarda de la intimidad del paciente es uno de los criterios esenciales al tratar la

información sanitaria, los aspectos reglamentarios de privacidad y seguridad electrónica son críticos. Los resultados de los actos médicos (consultas, resultados de análisis de laboratorio, procedimientos médicos, informes operatorios, complementarios) requieren que en el intercambio de información entre el emisor y receptor exista absoluta confianza de que los datos no han sido alterados.

Según Gutiérrez (2018), como requerimiento de seguridad y confidencialidad, estos sistemas deben cumplir con los requerimientos legales comunes e incluir entre otros, un adecuado control de acceso e identificación, registro de acciones realizadas, protección para la integridad de los datos y todas aquellas medidas que garanticen la fiabilidad del sistema. Para lograrlo se debe tener presente que la seguridad de la información médica se basa en cinco aspectos fundamentales [(2)]:

1. Privacidad**:** hace referencia a que la información médica no pueda ser accedida por un tercero que no esté relacionado al proceso de atención.
2. Evitar el Repudio**:** hace referencia a la autoría del documento, sólo el poseedor de la firma digital es el responsable por los datos generados y guardados.
3. Autenticidad: se refiere al carácter auténtico del documento, es decir que sea el original.
4. Integridad: relacionado con el anterior, se refiere al contenido de la información médica impidiendo que sea alterado de su registro original.
5. Cronología o temporalidad**:** relacionada directamente con la integridad, permite tener registro de la fecha y hora de la creación de la información original, dando así a los datos una secuencia temporal.

La gestión de la información resultante de los actos médicos requiere el empleo de mecanismos que permitan autenticar, autorizar, administrar y auditar cualquier acceso o modificación de los datos de los pacientes. Cualquier aplicación desarrollada para este fin demanda mínimos requerimientos de seguridad.

El Sistema de Información Hospitalaria XAVIA HIS, es una solución integral para la gestión médica de hospitales y centros de salud, desarrollado por el CESIM de la Universidad de Ciencias Informáticas (UCI). El sistema XAVIA HIS permite la recolección, almacenamiento, procesamiento y comunicación de la información relacionada con la atención al paciente. Esta información es manejada de forma integrada y única (Historia Clínica Electrónica única) siguiendo el estándar Clinical Document Architecture (Arquitectura de Documentos Clínicos, CDA por sus siglas en inglés).

El sistema XAVIA HIS, cuenta con la funcionalidad de firma y validación digital que garantiza la integridad, temporalidad, autenticidad y autoría de los documentos clínicos electrónicos que se generan en las entidades hospitalarias que lo utilizan. El sistema brinda la posibilidad de

crear una Autoridad Raíz que permite generar los certificados y firmas digitales de los usuarios en el momento en que estos son añadidos al sistema.

En septiembre del 2016, Cuba dictó la Resolución Ministerial No. 2/2016 donde se definió la Infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial de la República de Cuba. Se designó al Servicio Central Cifrado del Ministerio del Interior (MININT) como la Autoridad Raíz de la Infraestructura y se aprobó el Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública.

Actualmente, la PKI nacional cubana cuenta con una Autoridad Certificante Raíz administrada por el Servicio Central Cifrado del MININT.

Este trabajo tiene como objetivo diseñar una estructura de seguridad centrada en la PKI entre las instituciones de salud, a partir de la infraestructura de llave pública nacional como autoridad de certificación raíz.

Métodos

En la realización de este trabajo se hizo una revisión sistémica de la literatura relacionada con el tema en el sector de la salud. Se investigaron las características y elementos fundamentales de la infraestructura de llave pública como mecanismo de seguridad existente para el intercambio de información. Se realizaron entrevistas a administrativos, gestores hospitalarios y especialistas en seguridad informática.

Infraestructura de llave pública (PKI)

Los aspectos fundamentales de seguridad de la información médica planteados se satisfacen mediante el despliegue de una infraestructura de clave pública o Public Key Infraestructure (PKI) y el uso de los certificados digitales.

Varias definiciones se encuentran en diferentes fuentes bibliográficas acerca de lo que es una PKI, todas coinciden en definirla como una infraestructura de seguridad basada en criptografía de clave pública. Está compuesta por un sistema jerárquico de entidades que, mediante el empleo de criptografía, normas jurídicas, recursos humanos, hardware y software, brindan a sus suscriptores y a terceros (individuos u organizaciones), la confianza necesaria para identificarse entre sí de manera segura [3–6]. Estas garantías se basan en una autoridad de certificación (CA), por las siglas en inglés de Certificate Authority, en la cual se confía y nos asegura la vinculación o relación entre la identidad de un sujeto y su clave pública.

Los usuarios firman digitalmente los mensajes usando su llave privada, contenida en su certificado digital. El destinatario podrá comprobar la validez de la firma utilizando la clave

pública del usuario firmante contenida en el certificado expedido por la CA, comprobando así, la autenticidad e integridad del mensaje y evitando el repudio. Para el proceso de cifrado se utiliza la clave pública del destinatario, siendo este el único que puede descifrarlo con su llave privada, garantizando la confidencialidad del mensaje.

Componentes de la PKI

Los componentes de una infraestructura de llaves públicas pueden variar de acuerdo a su implementación. A continuación, se listan los principales que se encuentran en el núcleo de funcionamiento de una PKI [3], [5–7].

1. Autoridad de Certificación: Entidad de confianza probada, responsable de emitir y revocar los certificados digitales utilizados por usuarios aceptados por las Autoridades de Registro dependientes de ella, firmarlos y almacenarlos en un repositorio de acceso público [6]. La CA es también conocida como la tercera parte confiable (Trusted Third Party o TTP) [8], que garantiza la relación existente entre la clave pública y los datos del usuario inscritos dentro de un certificado digital [3].
2. Autoridad de Registro (RA), por las siglas en inglés de Registration Authority: Puede operar de forma autónoma, o formar parte de una autoridad de certificación. Sus funciones específicas consisten en registrar las peticiones que hagan los usuarios para obtener un certificado digital. Esta autoridad comprueba la veracidad y corrección de los datos que aportan los solicitantes en las peticiones, y las envía a una autoridad de certificación para que sean procesadas [4], [9], [10]. Es el punto de comunicación entre los usuarios de la PKI y la autoridad certificadora [10].
3. Autoridad de Validación (VA), por las siglas en inglés de Validation Authority: Es la entidad dentro de la Infraestructura que lleva la función de validación de las firmas digitales usando la llave pública [3], [11]. Se encargada de comprobar la vigencia de validez y no-cancelación de los certificados digitales de los suscriptores de un documento electrónico de los certificados digitales [4], [12].
4. Repositorio: Es la estructura que se emplea para almacenar la información relacionada con los certificados digitales válidos o revocados. Los dos repositorios más importantes son el repositorio de certificados y el repositorio denominado CRL´s o Listas de Revocación de Certificados [3], [5].
5. Suscriptor: Es el organismo, persona natural o sujeto que solicita y recibe un certificado digital por una autoridad certificadora [4], [6], [11]. Estos pueden firmar, verificar firmas por medio de las claves privadas correspondientes y cifrar datos mediante las claves contenidas en los certificados digitales [5].

Por su importancia en el sector de la salud, una PKI sanitaria debe contar también con el estampado de tiempo a la hora de firmar un documento. Es por ello que añadiremos como componente clave de la PKI la Autoridad de Sellado o Estampado de Tiempo.

6. Autoridad de Sellado o Estampado de Tiempo (TSA) por las siglas en inglés de Time Stamp Authority: Puede operar en línea o fuera de ella, es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo [3]. La TSA crea un sello electrónico invariable que entrega al solicitante, utilizando parámetros de tiempo real astronómico que obtiene de una fuente de alta fiabilidad técnica [4].

Certificado digital

Un certificado digital o certificado electrónico es un fichero informático generado por una entidad de servicios o certificación [6]. Un certificado contiene en conjunto de datos que identifica de forma única un par de claves y un propietario (como persona, organización, cuenta, dispositivo o sitio) que está autorizado a utilizar el par de claves. El certificado contiene la clave pública del propietario y opcionalmente otra información relacionada al mismo, y está firmada digitalmente por una entidad de certificación (es decir, una entidad de confianza), lo que enlaza la clave pública con el propietario [10], [11].

El certificado digital es un documento identificativo, que vincula a una persona o equipo con una clave pública, la cual a su vez está matemáticamente relacionada con una clave privada. La clave pública se emplea para el cifrado de información y la verificación de la firma digital, mientras que la clave privada se utiliza para realizar las operaciones opuestas.

Los certificados digitales deben estar firmados por la CA que los ha emitido para asegurar su validez. Solo las CA denominadas raíz firman el certificado con la misma entidad que están representando, son los llamados certificados autofirmados [6].

Existen varios formatos de certificados, el más extendido a lo largo de internet es el descrito en el estándar UIT-T X509. Dicho estándar define la estructura y los campos correspondientes, actualmente se encuentra en su versión 3 [3]. A continuación se detalla el formato del estándar X.509 v3 (Fig.1) [13].

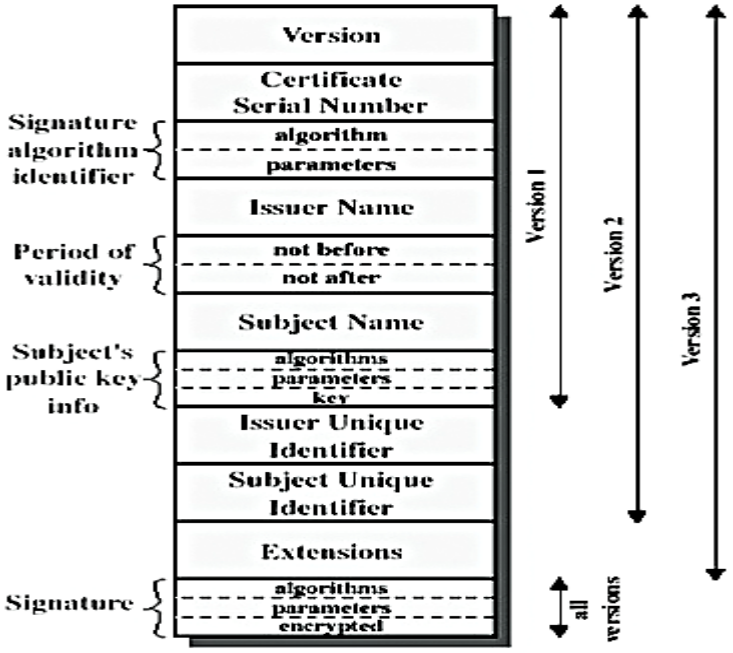

Fig. 1- Formato del Certificado X.509 versión 3. Fuente: [13]

Los certificados digitales (especialmente los emitidos para entornos de salud), van a identificar no sólo a las personas sino también sus roles fijos o establecidos como consecuencia de sus estudios, así como de su especialización y actuar profesional. Por ello es necesario proveer un grupo especial de atributos con la finalidad de que los certificados de identificación tengan funcionalidad en su entorno. Un certificado digital sanitario se utilizará con toda probabilidad no sólo para verificar la identidad del profesional de salud sino para comprobar el rol o roles de este en la práctica médica.

Escobar (2007), plantea que un certificado digital sanitario debe poseer la extensión hcRole attribute (atributo del rol sanitario), este atributo de rol sanitario (hcRole) permite la codificación de los datos propios del rol de los trabajadores sanitarios.

Firma digital

La firma digital es el resultado de una transformación criptográfica de los datos, donde un valor numérico se adhiere a un mensaje o documento. Permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación de origen), así como verificar que dicha información no ha sido modificada desde su generación (integridad) [3(, (5)].

Como se muestra a continuación (Fig. 2) [11], al firmar digitalmente un mensaje se utiliza la clave privada del usuario y sólo puede ser descifrado utilizando la clave pública asociada. Si se

puede descifrar correctamente, el firmante no puede negar que firmó el mensaje utilizando su clave privada (no repudio).

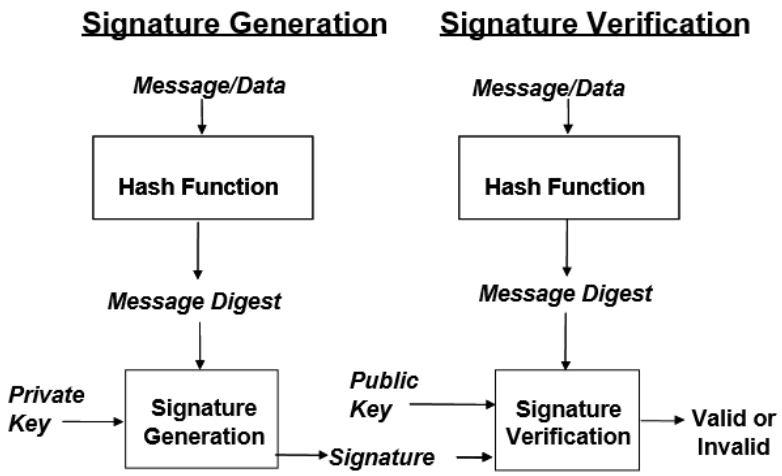

Fig.2- Proceso de Firma Digital. Fuente: [11]

Considerando que la firma digital basada en infraestructura de clave pública posee operaciones criptográficas se plantea que la firma digital permite [14]:

1. la identificación de la parte o partes firmantes.
2. la integridad, al verificar que la información firmada se recibe sin alteración alguna.
3. la confidencialidad, ya que al estar cifrado el contenido, sólo puede ser conocido por el firmante o por aquellos autorizados a acceder al documento.
4. el no repudio entre las partes, ya que al garantizar que el o los firmantes son quienes dicen ser, ninguno puede negar haber firmado, enviado o recibido el documento.

La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos. Para garantizar la seguridad de las mismas estas deben a su vez ser [5]:

1. Únicas: Las firmas deben poder ser generadas solamente por el firmante y por lo tanto infalsificable. Por tanto, la firma debe depender del firmante.
2. Infalsificables**:** Para falsificar una firma digital el atacante tiene que resolver problemas matemáticos de una complejidad muy elevada, es decir, las firmas han de ser computacionalmente seguras. Por tanto, la firma debe depender del mensaje en sí.
3. Verificables**:** Las firmas deben ser fácilmente verificables por los receptores de las mismas y, si ello es necesario, también por los jueces o autoridades competentes.
4. Innegables**:** El firmante no debe ser capaz de negar su propia firma.

5. Viables**:** Las firmas han de ser fáciles de generar por parte del firmante.

Resultados y discusión

Teniendo como premisa la integridad de los datos sensibles de los pacientes que son registrados en el sistema de información hospitalaria XAVIA HIS, este implementa el firmado digital de la documentación clínica que se genera. Según Ledo [15], el desarrollo de la infraestructura de firma y validación digital en el sistema informático XAVIA HIS, brinda la posibilidad de crear una Autoridad Raíz que posibilita la creación de las identidades digitales de los usuarios en el momento en que estos son añadidos al sistema. Además de crear la TSA para el sellado de tiempo, es posible exportar un certificado de confianza y ser cargado posteriormente en otra instalación hospitalaria que cuente con el sistema XAVIA HIS.

Si se requiere intercambiar información entre 2 o más entidades hospitalarias es necesario intercambiar sus certificados y adoptar un esquema de confianza de certificación cruzada, establecer relaciones de confianza de igual a igual. Puesto que es una solución de PKI nativa dentro de la aplicación, no hay personal que lleve una adecuada gestión de los certificados y CRLs, lo cual complejiza su mantenimiento y actualización de las identidades digitales de los usuarios, así como de la cadena de confianza entre entidades.

Para ello se hace evidente el uso de un tercero confiable que no sea el propio sistema. Una entidad externa que se encargue de gestionar los certificados digitales de las CA y RA que intervendrán en la infraestructura y del personal médico que interactúa con el sistema, posibilitando así su validación fuera de este.

En un escenario determinado, donde un médico (suscriptor1) del hospital A (CA-1) recibe un pedido de interconsulta de otro profesional (suscriptor2) del hospital B (CA-2), quien decide enviarle la historia clínica y las impresiones diagnósticas de un paciente para que este emita su criterio. ¿Cómo se garantiza la integridad de los datos recibidos y la identidad del emisor?

1. El médico (suscriptor1) que recibe los datos, realiza una consulta la CRL para verificar que el certificado del suscriptor2 es válido. La ubicación de la CRL está incluida en el certificado del suscriptor2.
2. El suscriptor1 luego verifica quién firmó el certificado del suscriptor2 y encuentra que la CA-2 es la entidad autorizante. Como CA-2 es desconocida para suscriptor1, entonces verifica quien firmó el certificado de CA-2 y encuentra que CA-0, la CA raíz, es quien autorizó a CA-2 y quien también autorizó a CA-1, de quien suscriptor1 depende.
3. El suscriptor1 está ahora en condiciones de trabajar con confianza debido a que posee todas las garantías de seguridad respecto de autenticación, identificación, no alteración y no repudio, provistas por la PKI.

Esto se conoce normalmente como “caminar la cadena de confianza”, debido a que todas las partes que intervienen pertenecen a la misma PKI. Utilizando una única PKI para el Sistema de Salud Público cubano, siendo extensibles a entornos de trabajo de múltiples CA subordinadas, se garantiza la escalabilidad.

Por la complejidad y distribución geográfica de las unidades de salud pertenecientes al Sistema Nacional de Salud Cubano (SNS), se requiere la implementación de una PKI compleja. Bajo un esquema jerárquico teniendo como única CA raíz al Servicio Central Cifrado del Ministerio del Interior, se debe ir incorporando tantas CA como sean necesarias.

Como premisa debe existir una CA intermedia con autoridad para emitir certificados a otras CA y se encargue de gestionar todos los certificados de las instituciones sanitarias. Bien puede ser el propio MINSAP u otra empresa autorizada para comercializar certificados digitales de llave pública. En un nivel más bajo, las instituciones de salud implementarán sus CA y RA.

Estas CA pudieran ubicarse en las distintas instalaciones hospitalarias y atender las solicitudes de certificados del personal de salud que radica en el mismo para llevar un mejor control. Por otra parte, atendiendo a las limitaciones tecnológicas que muchos de estos puedan tener, se propone que las CA se ubiquen estratégicamente en hospitales centrales y tengan un carácter regional.

Por otra parte, una Autoridad de Registro puede operar de forma independiente y enviar las solicitudes a una CA para su procesamiento. En un esquema de certificación regional, estas RA pueden estar dispersas geográficamente en los distintos establecimientos de salud cercanos a una CA y funcionar de manera local, estas son llamadas Autoridades de Registro Local (LRA). Teniendo así, un mayor control de los datos suministrados por el personal médico, para luego enviarlos a la CA y ser procesados.

Este esquema permitiría que en el intercambio de información entre 2 entidades hospitalarias, pueda ser verificada su integridad a través de la CA raíz o CA intermedia (Fig.3).

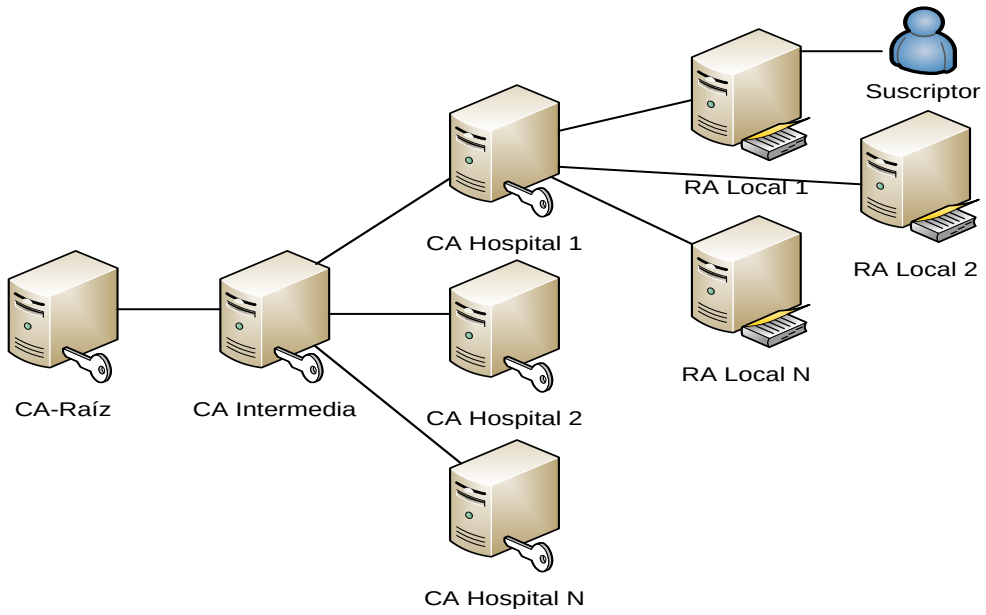

Fig. 3- Propuesta de arquitectura PKI para el MINSAP. Fuente: Elaboración propia

Una PKI sanitaria debe necesariamente basarse en la información suministrada por las instituciones de asistencia médica a la que pertenecen sus suscritores, ya que éstas son las entidades que validan y acreditan el ejercicio de la profesión de su personal. Por lo tanto, es prudente considerar que en estas entidades se implementarán las Autoridades de Registro Local (LRA) y serán los responsables de solicitar los certificados digitales con los datos de cada profesional, sus roles primarios y atributos.

El desarrollo de una infraestructura PKI bajo un esquema regional de salud, proporciona ventajas significativas, ya que toma en consideración sus características y requisitos de seguridad específicos. En este sentido se garantiza la escalabilidad para responder a la demanda de inclusión de nuevas instituciones sanitarias a la infraestructura. De acuerdo a las características técnicas de las instituciones de salud se les dará la responsabilidad de funcionar como una CA subordinada o LRA, previamente autorizado por una CA probada dentro de la infraestructura. Esto permitirá que los certificados de las nuevas entidades estén firmados por una entidad de confianza de la PKI, lo que garantiza caminar la cadena de confianza.

Bajo estas consideraciones, para firmar digitalmente la información médica generada en el sistema XAVIA HIS, se utilizarán los certificados digitales proporcionados por los propios profesionales de la salud. Garantizando así, que el intercambio de información sanitaria entre instituciones de salud este respaldado por los esquemas de seguridad que brinda la PKI.

Si bien la infraestructura descrita aquí es muy general, garantiza transacciones electrónicas seguras, adecuadas para la protección de los registros médicos sensibles. Se expone una breve descripción sobre los principios y conceptos básicos involucrados en una PKI. Se incluyen

temas como sus características y componentes fundamentales, los certificados y firmas digitales para entornos sanitarios.

Conclusiones

En el entorno sanitario la protección de la privacidad y la salvaguarda de la intimidad del paciente es uno de los criterios esenciales al tratar la información, los aspectos reglamentarios de privacidad y seguridad electrónica son críticos. La propia seguridad del paciente exige que la información no se haya alterado o manipulado durante su almacenamiento o transporte. En las acciones realizadas por el personal médico sobre los registros de salud se debe dejar constancia de quién (autoría) ha hecho qué y cuándo (cronología o temporalidad), de forma que este no pueda negarlo (no repudio). Después de registrado, este documento no puede ser modificado (integridad).

La forma de conseguir transacciones electrónicas seguras y adecuadas a la normativa de protección de datos, es empleando instrumentos como la firma digital con base en una PKI. Involucrar a las Autoridades de Certificación y Autoridades de Registro para que actúen como certificadores externos, da garantías de protección e integridad de los datos.

La implementación de una infraestructura PKI en el sector de salud pública cubano, le otorga a este un alto nivel de seguridad, pues PKI soporta autenticación, integridad, confidencialidad y no repudio. El empleo de la firma digital y los certificados digitales, así como la intervención de una autoridad certificadora, permiten que los usuarios que requieran intercambiar cualquier tipo de información, a través de una red, puedan hacerlo con un grado de confianza aceptable.

Referencias

1. CUBA, Ministerio De Salud Pública De Cuba. Plan de desarrollo y uso de las Tecnologías de la Información y Comunicaciones del Sistema Nacional de Salud 2017 - 2021. Revista de Información científica para la Dirección en Salud. 2017.
2. Gómez A, Plazzotta F, Campos F, Martínez M, Severino J, Pedernera F, et al. Desarrollo de un sistema para la firma digital de Registros Médicos. En II Congreso de Tecnologías de Información en Salud 2006.
3. Castro Martínez FJ. Gestor de certificados digitales con PKI [tesis de graduación]. Universidad Carlos III de Madrid. 2013. [citado 11 Ene 2020]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/25903/PFC_FranciscoJavier_Castro_Martinez.pdf

4. Ministerio del interior. Resolución No. 2/2016. Gaceta Oficial, de la República de Cuba [Internet]. 2016. [citado 11 Ene 2020]. Disponible en: https://www.gacetaoficial.gob.cu/codbuscar.php.
5. Gallardo Urbini IM. Certificados digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada [tesis de maestría]. Argentina: Universidad Nacional de La Plata. [citado 11 Ene 2020]. Disponible en: http://sedici.unlp.edu.ar/handle/10915/72076
6. Ben Bouker Hmaddouch S. Estudio, propuesta y desarrollo de componentes avanzados para una PKI Híbrida [tesis carrera]. España: Universidad Politécnica de Cataluña.
7. Slagell A, Bonilla R, Yurcik W. A survey of PKI components and scalability issues. In 2006 IEEE International Performance Computing and Communications Conference. 2006 Apr 10.
8. Selvakumaraswamy S, Govindaswamy U. Efficient Transmission of PKI Certificates using Elliptic Curve Cryptography and its Variants. International Arab Journal of Information Technology (IAJIT). 2016 Jan;13(1). Revisar
9. Barker E. Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms. National Institute of Standards and Technology; 2016 Mar 11.
10. Chokhani S, Ford W, Sabett R, Merrill CR, Wu SS. Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC. 2003 Nov;(3647):1-94.
11. Gallagher P. Digital signature standard (DSS). Federal Information Processing Standards Publications.2013;FIPS:186-93.
12. Cuno A. Conceptos de Firma Digital. Identidad digital. La identificación desde los registros parroquiales al DNI electrónico. 2015. Lima Perú. RENIEC. Pags 107-73. [citado 11 Ene 2020]. Disponible en: https://www.iidh.ed.cr/capel/media/1479/indentidad-digital-la-identificaci%C3%B3n-desde-los-registros-parroquiales-al-dni-electr%C3%B3nico.pdf
13. Hawanna V, Kulkarni VY, Rane RA, Mestri P, Panchal S. Risk Rating System of X. 509 Certificates. Procedia Computer Science. 2016 Jan 1(89):152-61.
14. Escobar PP, del Fresno M, Arguiñarena E. Transacciones electrónicas seguras en salud. ResearchGate [Internet]. 2007 [cited 2019 Mar 4]. Available from: https://www.researchgate.net/publication/260311227_Transacciones_electronicas_seguras_en_salud.
15. Ledo D. Infraestructura de firma y validación digital de los documentos clínicos electrónicos generados por el sistema alas HIS. 2011 [tesis carrera]. Cuba: Universidad de las Ciencias Informáticas.

Conflicto de interés

Los autores declaran que no existen conflictos de intereses.

Contribuciones de los autores

Ing. Yanssel Urquijo Morales: Dirigió el proyecto, proporcionó documentación, realizó el análisis a interpretación de los resultados, generó estadísticas, elaboró y aprobó el informe final.

Dr.C. Arturo Orellana García: Aplicó métodos científicos para la búsqueda y recolección de información, realizó análisis y llegó a conclusiones de importancia para la investigación. Orientó y revisó el proyecto de investigación.