REV ESP PATOL 2003; Vol 36, n.º 2: 171-180

ARTÍCULO INVITADO

Firma electrónica y manejo de privilegios en sanidad

Olga Ferrer Roca, Karim Franco, Pablo Pulido, Pedro Escobar, Álvaro Cardenes

Cátedra UNESCO de Telemedicina. CATAI (http://www.teide.net/catai). Facultad de Medicina. Universidad de la Laguna. Tenerife. catai@teide.net

INTRODUCCIÓN

En los últimos años se ha puesto en evidencia la urgente demanda de seguridad en las transacciones electrónicas del entorno sanitario. Aun sabiendo que la legislación española es modélica y una de las más avanzadas en la protección de la privacidad de los datos (1-3), las autoridades sanitarias y particularmente los usuarios desconocen la infraestructura necesaria en términos de software y hardware, así como los requerimientos en la gestión de los datos.

Siendo uno de los criterios esenciales de la información sanitaria la protección de la privacidad y la salvaguarda de la intimidad del paciente, los aspectos reglamentarios de privacidad y seguridad electrónica son críticos y a pesar de ello prácticamente desconocido para la mayoría de los médicos y de los colegios profesionales.

Las organizaciones sanitarias y aseguradoras tienen la responsabilidad de poner todos los medios disponibles para que el intercambio de información no sólo sea seguro, sino que cumpla la normativa vigente.

De acuerdo con las leyes vigentes (1-3) los pacientes son los propietarios de su información médica por lo que el marco debe proporcionar a los consumidores las herramientas para asegurar que los accesos de su propia información médica son seguros. Además las leyes sobre la protección de datos sensibles obligan a que estos accesos tengan el máximo nivel de seguridad.

Por lo tanto para gestionar información médica y de acuerdo a la normativa vigente es estrictamente necesaria la puesta a punto de los llamados TTPs *(Trusted Third Parties* o Notarios electrónicos) que permita autenticar, autorizar, administrar y auditar cualquier acceso o modificación de los datos relacionados con la salud de los ciudadanos.

En los próximos apartados queremos explicar las razones por las cuales los TTPs genéricos son insuficientes y en el ámbito sanitario se necesitan servicios altamente especializados. Además de informar al usuario de que por el momento, en nuestro entorno, las exigencias legales distan muchos de aplicarse correctamente.

La única forma de conseguir transacciones electrónicas seguras y adecuadas a la normativa de protección de datos es involucrar a las Autoridades de Certificación (CA) y de Registro (RA) para que actúen como certificadores externos para que proveedores, asegurados y consumidores accedan a la misma con todas las garantías de protección e integridad de los datos.

Cualquier aplicación en el entorno sanitario desde un e-mail hasta el acceso al sistema de información hospitalario (HIS) o la prescripción electrónica demanda unos requerimientos mínimos de garantía bajo una infraestructura de Llave Pública (PKI).

DEFINICIÓN de PKI

Una PKI o Infraestructura de llave pública, estructura mínima que la ley estipula para acceder a datos personales altamente sensibles (como la historia clínica o datos sanitarios o de la vida sexual), la constituyen las Autoridades de Certificación, los Certificados Digitales, los mecanismos para asegurar los accesos a las Listas de Revocación de Certificados, el mani-

fiesto o Política de Certificación y los métodos para validar la emisión de certificados.

En el entorno sanitario la PKI sirve para autenticar, encriptar y realizar firmas digitales que aseguren la confidencialidad, y control del movimiento de las historias clínicas electrónicas u otra información sensible, tanto en su aspecto clínico como administrativo.

REQUERIMIENTOS PARA MANEJAR Y ACCEDER A DATOS SANITARIOS

Incluye los:

Requerimientos de autenticación

En sanidad las interacciones múltiples y multidisciplinarias generan documentos o informes que son reutilizados y actualizados por un gran número de autores. Por ello es esencial que la información que se suministra sea fiable y atribuible con total certeza a los autores que la generan.

Además, al tratarse de información personal altamente sensitiva, es esencial que no pueda ser accesible por personas no autorizadas. De ahí que la autenticación del personal con permiso de acceso sea esencial.

Requerimientos de integridad

La integridad de la información sanitaria no es sólo un problema de seguridad sino en muchos casos de supervivencia porque afecta a las pautas de tratamiento o a las actuaciones de urgencia o agresivas que conllevan riesgo para el paciente. Como cualquier información altamente sensible, tiene el riesgo de manipulación o borrado. Por ello debe asegurarse en todo momento que esté integra y no haya sido manipulada.

Requerimientos de confidencialidad

Como consecuencia de las afirmaciones anteriores siempre existe la posibilidad de violación de esta información con finalidades varias incluso por intereses personales o financieros. Una vez violados los derechos de privacidad del paciente estos no pueden ser restituidos.

Requerimientos de autorización

Dado que la historia clínica pertenece al paciente, este es el único que, para el adecuado seguimiento y tratamiento, puede autorizar su utilización a una institución o a un médico. En este contexto el concepto de autorización para poder acceder a la información privada es un elemento esencial.

Requerimientos de control de acceso

Igualmente debe llevarse un estricto control de acceso para las personas con autorización. El acceso a la información por parte de las personas o entidades con autorización debe ser tan sólo para aquellas funciones o aspectos para los cuales están autorizados. Y tener presente que un acceso no autorizado puede traer consecuencias irremediables.

En este marco, es de obligado cumplimiento la utilización de estándares de seguridad apropiados que reduzcan significativamente el riesgo de acceso no autorizado o vulneren la información sanitaria de un paciente.

De acuerdo con las leyes españolas vigentes, el único sistema que asegura una adecuada cadena de confianza es la PKI con Certificados de clave pública y utilización de claves privadas. Sin embargo el grupo de estandarización europeo sobre seguridad en material sanitaria (TC-251 WG4) aboga por la necesidad de extender estos aspectos al entorno de infraestructura de manejo de privilegios (PMI) utilizando como veremos no sólo los Certificados de Atributos sino además los Certificados de Calificación ligados al PKI.

La razón de este artículo es explicar a la comunidad médica las peculiaridades que en un entorno sanitario deben tener las infraestructuras PKI y PMI, habida cuenta que el desconocimiento de las leyes no exime su cumplimiento.

Por ello debemos extender los requerimientos a aquellos ligados al PKI en el entorno sanitario.

Requerimientos de política de gestión de los PKI en sanidad

Las PKI sanitarias necesitan de: 1) Un alto nivel de confianza para cada uno de los servicios de seguridad que gestionan, a saber: autenticación,

integridad, confidencialidad, firma digital, autorización y control de acceso. 2) Un alto nivel de disponibilidad de las infraestructuras. La sanidad trabaja las 24 horas al día, por lo que la obtención de certificados, su revocación o la consulta de las listas de revocación deben estar siempre disponibles, ya que de ello depende la seguridad del sistema. 3) Un alto nivel de Confianza, en la información recibida y ligada a un paciente o proveniente de cualquier actor sanitario. 4) Una compatibilidad con el entorno de Internet, ya que con toda probabilidad el intercambio de información entre diferentes entidades sanitarias no ubicadas en una red privada virtual va a realizarse por Internet. 5) Necesita simplicidad en la evaluación y comparación de las políticas de certificación, porque más pronto o más tarde deberá transmitir información a otros entornos sanitarios (otras autonomías e incluso otras naciones) que necesitarán para evaluar la autenticidad de los datos el reconocimiento de los certificados estandarizados adjuntos.

CERTIFICADOS

Un certificado en el entorno electrónico de seguridad, es un conjunto estructurado y estandarizado de datos [norma X.509] con extensiones que permiten asociar atributos adicionales y manejar la jerarquía de certificados (dependencia).

Siguiendo las normativas de referencia (4) los certificados para la seguridad electrónica que van a gestionarse en el ámbito sanitario están listados en la figura 1 sacada de la norma de estandarización TC251-WG4-DTS 17090.

1. Certificados de Llave Pública

En la seguridad electrónica sanitaria y en general en entornos que se requieren una alta seguridad, los Certificados de Llave pública (PKC) van dirigidos a los aspectos de identificación, y aunque como veremos la identificación puede utilizarse para autorizar, no contiene información sobre autorización, aspecto este esencial en el entorno sanitario.

El único certificado digital que la ley permite para identificar de forma segura un actor o un

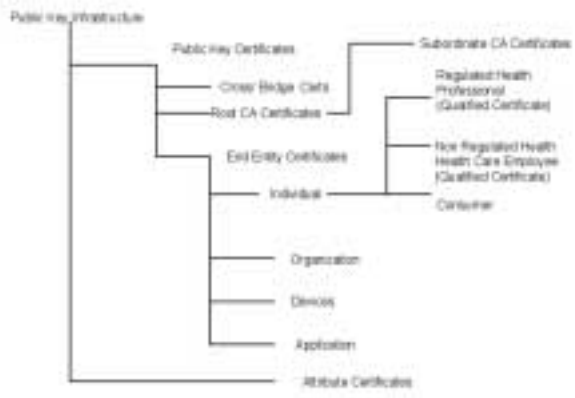

Fig. 1: Health Care Certificate Types.

punto en la cadena de asistencia sanitaria es aquel que contiene un par de llaves asimétricas (Pública y privada) tengan o no capacidad de encriptación. Es decir está integrada por: 1) un certificado X.509 de llave pública (PKC) [X.509] [RFC2459] que liga la identidad del cliente a la llave pública, asociado a 2) la llave privada obtenida de forma segura a partir de la pública y guardada en dispositivos de seguridad autorizados (tarjetas inteligentes, tokens, etc.) que se utiliza para la firma digital.

Estos aspectos quedan asegurados cuando las PKCs junto a la llave privada han sido emitidos por Autoridades de Certificación (CA) reconocidas —como la FNMT, Fábrica Nacional de Moneda y Timbre— que a su vez pueden autorizar a CAs subordinadas más próximas a los entornos sanitarios locales, generando una cadena de confianza constituida por el Certificado raíz (que se firma a sí mismo) y los certificados de las AC subordinados firmados por el certificado inmediatamente superior en la cadena de confianza.

Cada vez que se comprueba la validez del certificado de una identidad PKC (actor o punto de asistencia sanitaria) se analiza y comprueba toda la cadena de confianza en la que se basa este certificado. Si alguno de los certificados de la cadena de confianza no es válido, invalida a todos los subordinados y por lo tanto el actor o punto de asistencia sanitario queda invalidado para cualquier actuación segura.

Las peculiaridades de una PKI (Infraestructura de Llave Pública) sanitaria es que identifica: a) Los actores en el punto de actuación sanitaria b)

la responsabilidad legal ligada a la firma electrónica c) la identidad, formación y titulación del actor. Este certificado (PKC) como hemos comentado más arriba, no es apropiado para contener la información que gestiona las decisiones de autorización y control de acceso que en cambio pueden ser incluidas en los Certificado de Atributos (AC), otro tipo de certificados que pertenece a la PMI (Infraestructura de manejo de privilegios) y que más adelante detallaremos.

1.1. Certificados de entidades finalistas en el entorno sanitario

Los certificados PKC emitidos por las CAs especializadas en sanidad para las entidades finalistas, (llamadas así porque bajo ellas no existe ninguna otra entidad que dependa de su certificado) no sólo abarca a individuos sino a otras entidades físicas o jurídicas (fig. 1). Son entidades finalistas en el entorno sanitario los individuos, las organizaciones, el aparataje y las aplicaciones sanitarias y todas ellas deben ser pretejidas con el fin de asegurar de que todos los actores de la cadena sanitaria pueden identificarse y confiar en ellos. Piénsese por ejemplo que ocurriría si se violara la seguridad y en vez de acceder al HIS (Hospital Information System) se accediera a otra base de datos totalmente manipulada.

1.1.1. Certificados de identidad individuales

Son un tipo especial de certificados finalistas emitidos para autenticar tres tipos de individuos claramente identificables en el entorno sanitario. Como veremos más adelante por su importancia en el reconocimiento legal de las firmas electrónicas estos certificados pueden ser Certificados de Calificación.

1.1.1.1. Certificados de identidad para profesionales sanitarios reglados

Identifican a los profesionales sanitarios, que para poder ejercer su profesión necesitan una licencia o un registro de cuerpos gubernamentales o profesionales.

1.1.1.2. Certificados de identidad para profesionales sanitarios no reglados

Identifican aquellos profesionales sanitarios que no están sujetos a registro o licencia por parte de los órganos gubernamentales. Incluye además:

— Certificado de identidad de proveedores sanitarios avalados

Identifica a aquellos individuos activos en su comunidad sanitaria que están avalados por organizaciones o profesionales sanitarios reglados.

— Certificados de identidad de empleados avalados por organizaciones sanitarias

Identifica a los empleados avalados por organizaciones o profesionales sanitarios.

1.1.1.3. Certificados de Identidad de Pacientes/Consumidores

Identifica a los individuos que pueden recibir los servicios de los profesionales sanitarios tanto reglados como no reglados.

1.1.2. Certificado de identidad para organizaciones

Para aquellas organizaciones sanitarias con fines de identificación o encriptación. El memorando IETF, RFC2527 incluye para ellos el campo denominado organisational unit name (nombre de la unidad organizativa).

1.1.3. Certificados de identidad de los aparatos

Que tienen por finalidad identificar individualmente y autenticar los aparatos que existen en la cadena de servicio sanitario (servidores, aparataje médico, sistemas de monitorización, prótesis, etc.).

1.1.4. Certificado de aplicaciones

Cada aplicación de software (sistemas de información computarizados) en el entorno sanitario necesita ser identificada y autenticada individualmente. Por ejemplo el HIS (Sistema de información hospitalaria) necesita un certificado de aplicación.

1.2. Identificación legal mediante certificados de calificación

El desarrollo de los Certificados de Calificación deriva de las demandas legislativas que muchos países imponen a los entornos sanitarios o a cualquier proveedor de servicios que admita la firma electrónica; así como de los requerimientos que firmantes y verificadores deben poseer para que su firma electrónica sea reconocida legalmente.

Para entenderlo debemos conocer inicialmente que es una Firma Electrónica o Firma Digital. Una firma digital es una transformación criptográfica de los datos que permite probar el *origen* y la *integridad* de los mismos; se genera utilizando la llave privada del que envía para realizar una operación matemática sobre el mensaje. El método que se utiliza implica el uso de la llave privada y de una operación matemática unidireccional (es decir no puede revertirse) como el algoritmo de Hash. De esta forma se produce un número Hash a partir del mensaje original que se agrega al enviar el mensaje. Una vez recibido el mensaje se utiliza la llave pública del emisor para llevar a cabo la misma operación en el mensaje y se comparan los resultados del número Hash con el que se ha recibido adjunto al mensaje. Si los dos son idénticos significa que el receptor tiene la seguridad de que recibe el mensaje de la persona que dice ser el firmante y además de que el texto o mensaje recibido no ha sido manipulado.

El grado de seguridad de que el firmante es quien dice ser, es altísimo ya que como sabemos la llave privada forma parte de la llave pública constituyendo el denominado par de llaves característico de los PKIs. El nivel de seguridad viene ligado a la Autoridad de Certificación que firma el certificado digital con su propia llave privada. Al firmarlo la Autoridad de Certificación se hace responsable de la información contenida, dando al propietario un cierto nivel de autenticación. El nivel de seguridad que se alcance depende de la política expresa de la Autoridad de Certificación (ver más adelante) y del manejo práctico de las llaves de los solicitantes y de sí misma.

Razón por la cual las Autoridades de Certificación de los individuos reglados en el sistema sanitario deberían ser especificas, ya que manejan datos muy concretos ligados a la formación, autorización de prácticas médicas y especialidad de los firmantes. Pero además y dada la responsabilidad legal ligada a la firma de los responsables sanitarios el Certificado en sí mismo debe conseguir una altísima seguridad de los datos que certifica de ahí la necesidad de los denominados Certificados de Calificación. Éstos son certificados cuyo propósito primario es la identificación de las personas con un altísimo nivel de seguridad en su firma digital y que son particularmente relevantes en cuanto al *reconocimiento legal de la firma electrónica.*

En este contexto los certificados de calificación se utilizan para asegurar con un alto nivel de fiabilidad los individuos del entorno sanitario tanto los profesionales reglados como los no reglados.

1.2.1. Extensión propia de los certificados de calificación

Se recomienda por lo tanto que los profesionales sanitarios reglados y no reglados posean entre los atributos del Directorio Sujeto –ver más adelante- el denominado qcStatement (Declaración para certificados de calificación)

Las especificaciones detalladas se encuentran en el documento de estandarización: «IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile».

1.3. Atributos especiales del directorio sujeto en el PKC sanitario

Los PKC individuales (particularmente en el ámbito sanitario), van a identificar no sólo a las personas sino también sus roles fijos o establecidos como consecuencia de sus estudios y entrenamiento homologado así como de su especialización. Por ello es necesario proveer un grupo especial de atributos en los PKC sanitarios con la finalidad de que los certificados de identificación tengan funcionalidad en su entorno.

Como los PKC individuales sanitarios se pueden utilizar tanto para la *autenticación* como para la *asignación de roles primarios* y estas extensiones no son criticas.

Las extensiones que un PKC sanitario debe poseer son el *hcRole attribute* (atributo del rol sanitario), además del *subjectDirectoryAttributes* (los atributos del Directorio sujeto)

1.3.1. HcRole Attribute

Un certificado de identidad sanitario se utilizara con toda probabilidad no sólo para verificar la identidad del actor sino para comprobar el rol o roles de este actor en la cadena sanitaria. La información de si un médico es además un cirujano es una información que no varía con el tiempo y por lo tanto es adecuado introducirla en un certificado de identidad personal PKC.

El atributo de rol sanitario (hcRole) permite la codificación de los datos propios del rol de los trabajadores sanitarios reglados y no reglados. Además este campo admite una extensión opcional introduciendo el HcProfessionalData, con los códigos nacionales o internacionales de identificación de las profesiones. Es decir permite la emisión de múltiples certificados y acepta tablas de clasificación asociadas.

Tiene la ventaja de que si los datos se introducen con códigos estandarizados que se reconozcan en toda España (o en Europa), sobretodo teniendo en cuenta las disposiciones para la tarjeta sanitaria unificada en la UE, convierte el PKC sanitario en una herramienta con operabilidad internacional para el reconocimiento de roles sanitarios.

1.3.2. subjectDirectoryAttributes

Esta extensión opcional y no crítica, se recomienda que este presente en todos los PKC del personal sanitarios y tiene por finalidad albergar otros atributos que puedan ser de interés. Uno de los más importantes es el de Calificación qcStatement que hemos visto anteriormente.

Aunque diseñada para sujetos y no presente en los PKCs de aparatos y aplicaciones, es importante destacar que todas las aplicaciones sanitarias deberían diseñarse para poder gestionar la extensión qcStatement de los certificados del personal sanitario.

2. Certificados de atributos

Un Certificado de Atributos (AC) es una estructura de datos firmada digitalmente por una Autoridad de Atributos que relaciona inequívocamente determinados atributos a la identidad del poseedor del certificado [X.509]

Un certificado de atributos sólo contiene grupos de atributos firmados digitalmente y aunque tiene una estructura similar a un PKC no contiene llave pública.

Los atributos que contiene especifican la pertenencia a grupos, el rol, tareas de seguridad y cualesquiera informaciones sobre control de acceso asociadas al propietario del AC.

En sanidad un AC va ligado a la información sobre autorización, y difiere de los roles o titulaciones propias de un PKC que pueden permitir una autorización pero que no contienen información sobre autorización, como veremos más adelante.

Los detalles de estandarización están disponibles en el «IETF Attribute Certificate Internet Draft I».

2.1. Uso del Certificado Digital para roles y titulaciones

Aun partiendo de la premisa que todo el personal sanitario no tiene el mismo rol en la cadena asistencial, es crítico saber que la «información de autorización» no tiene la misma extensión en el tiempo que la de identidad de los trabajadores sanitarios. Por ejemplo un médico especialista en pediatría puede trabajar durante un corto espacio de tiempo como consultor en otro hospital adquiriendo derechos de autorización que antes no tenía y que por supuesto no cubre su PKC.

Varias son las razones que aconsejan transportar la información sobre autorización en un certificado separado y distinto al PKC.

1. Si la información sobre autorización se coloca en una extensión del certificado PKC la vida media de este certificado se acorta. Por ejemplo en el ámbito legislativo español la validez del PKC es de 4 años.

2. El emisor de PKCs no tiene autoridad para gestionar información sobre autorización. Puede llegar a verificar si el poseedor del PKC es un médico especialista pero es raro que pueda verificar el rol que esta persona tiene en una institución sanitaria.

3. Las tareas de un emisor de PKCs se complicarían notablemente si tuviera que obtener información sobre autorización de una fuente autorizada.

4. Si se introduce información sobre autorización en un PKC no sólo se reduce su vida media sino que se incremente considerablemente el esfuerzo administrativo de revocación y reemplazo de PKCs.

Por esta razón es mucho mejor separar la información de autorización [INTERNET-DRAFT October 1999 4.1 X.509 Attribute Certificate]. Las especificaciones IETF sobre Certificados de Atributos determinan cómo se utiliza la llave pública para validar firmas digitales o operaciones criptográficas de acceso, pero reconoce que no todas las operaciones de solicitud y acceso manejan los mismos criterios. Las decisiones de control de acceso basadas en reglas, roles o categorías van a necesitar una información adicional. Bien es verdad que en algunos casos la identidad y la calificación pueden ser suficientes para un acceso limitado.

Por ello los datos que pueden gestionar una autorización pueden estar incluidos en

1. Una extensión del PKC o

2. Ubicados en un certificado de atributos (AC) separado.

1. Los PKCs tienen como finalidad certificar la identidad del propietario ligándola a su llave pública y se utiliza en alguna de las operaciones de acceso (Identificación /Autenticación, Cifrado/ descifrado) cuando éstas se sustentan en decisiones basadas en identidad, después de confirmar que su llave privada se corresponde con la llave pública contenida en el PKC y que los certificados de la cadena de confianza no están revocados.

2. Una vez comprobada la identidad, se puede utilizar el certificado de atributos (AC) para gestionar información «volátil» no ligada al PKC. Los AC suportan la transmisión de información basada en reglas sobre el personal sanitario.

2.2. Uso del Certificado de Atributos para la Autorización y Control de Acceso

Las especificaciones del IETF sobre Certificados de Atributos concluyen que no es deseable introducir información de autorización en los Certificados de llave pública (PKCs) y que con el fin de que los certificados sean multi-usos, los roles secundarios, la pertenencia a grupos o la gestión de seguridad deben ir en un Certificado de Atributos acompañante.

Tres son las razones que aconsejan la utilización de ACs en sanidad:

1. Aunque el PKC de identificación pueda contener roles esta información es insuficiente para establecer decisiones de control de acceso

La identifican de un médico como cirujano en nombre de una Autoridad de Registro (ver más adelante) no lo habilita para acceder y gestionar la entrada de un enfermo a través de urgencias.

Esta información es propia de un Certificado de atributos que está ligado a la llave pública del profesional sanitario.

2. El profesional sanitario puede tener múltiples certificados de atributos cada uno para un rol determinado y además un AC puede contener referencias a otro AC conteniendo privilegios adicionales. Todos ellos con una vida media mucho más corta que un certificado de identidad.

3. La información sobre autorización requiere el mismo tratamiento de protección que un PKC y un AC le da esta funcionalidad. Es simplemente un grupo de atributos firmados (o certificados) digitalmente.

2.2.1. Certificados de Rol (RC)

Un AC que contenga información de roles puede ser limitado o especificado por otro certificado denominado Certificado de Roles mediante una extensión que apunta al RC. El Certificado de Roles no es más que otro AC que define los roles de propietario y contiene una lista de privilegios asociados a este rol.

Lo importante de esta cadena es que el certificador (emisor de los ACs) puede ser un emisor distinto y se gestiona administrativamente (cadu-

cidad, revocación, etc.) de forma totalmente separada.

La mayoría de los entornos con autorización utilizan privilegios basados en roles (típicamente junto con privilegios basados en la identidad) para alguna de las operaciones. En estos casos el verificador debe saber a priori o tiene que descubrir los privilegios asociados a un rol determinado para autorizar/ denegar la entrada. El RC simplifica enormemente estas operaciones.

3. Autoridades en la PKI/PMI

Para que una infraestructura de llave pública (PKI) gestione de forma efectiva la seguridad de las comunicaciones del personal sanitaria tiene que cumplir los siguientes objetivos:

1. Tiene que asociar de forma segura y fiable los denominados «unique and distinguished names» (nombres únicos para cada actor) de los individuos, organizaciones, aplicaciones y aparatos que participan en el intercambio electrónico de información sanitaria.

2. Tiene que asociar de forma segura y fiable los roles profesionales de individuos, organizaciones y aplicaciones que participan en el intercambio electrónico de datos personales sanitarios, habida cuenta que estos roles se utilizan para acceder a la información.

3. (Opcional) Tiene que asociar de forma segura y fiable los atributos de individuos, organizaciones y aplicaciones que participan en el intercambio electrónico de datos personales sanitarios, habida cuenta que estos son datos complementarios para la securización.

Todo lo anterior debe realizarse de manera que se mantenga la confianza en todo aquel que confía en la integridad y confidencialidad de los datos sanitarios transmitidos de forma segura en un entorno de PKI.

Para ello cada Autoridad de Certificación (CA) de PKI sanitaria debe operar de acuerdo con un grupo de normativas hechas públicas que promocionen los objetivos anteriores. Además de la cadena de autoridades de certificación, encargadas de los PKCs de identidad y que se inicia con la que provee el certificado raíz, es estrictamente necesario tener una o varias Autoridades de Registro.

3.1. Autoridad de certificación (CA)

La CA o mejor el certificador es una autoridad fiable, en la que confían uno o varios grupos para la creación y adjudicación de certificados. Opcionalmente la CA puede también generar las llaves de los actores que así lo solicitan [ISO 9594-8]

La CA verifica la identidad de individuos o sistemas, les adjudica un nombre unívoco (Distinguished Name), y verifica que la información suministrada es veraz firmándola; y puede delegar alguna de sus funciones en Autoridades de Registro.

Una Autoridad de Certificación es una organización reconocida que posee todos los controles y procedimientos establecidos para asegurar el grado de confianza requerido. Los controles y procedimientos han de adecuarse a lo establecido en la norma ISO17799.

Gestión de las Listas de Revocación (CRLs)

Las CAs tienen un importante papel en la distribución de los certificados a los individuos, en el mantenimiento de los directorios de certificados (certificados asociados a su llave pública), en la revocación de aquellos que se invalidan y en asegurar que los grupos que en ella han confiado estarán prontamente informados de la revocación de sus certificados.

La revocación de un certificado es el acto de desactivar cualquier conexión entre el certificado y su dueño ya porque el certificado no sea de confianza o porque ha expirado su validez.

3.1.1. Obligaciones de las Autoridades de Certificación (CA)

Una CA es responsable de todos los aspectos de seguridad y manejo de los certificados, incluido el control a través de los sistemas de registro, verificación de la información contenida en el certificado, generación del certificado, publicación, revocación, suspensión y renovación. La CA es responsable de asegurar que todos los aspectos relacionados con sus servicios y operaciones que realiza están de acuerdo con los

requerimientos, presentaciones y garantías establecidas en su Política de certificación y en el manifiesto de procedimientos prácticos de Certificación.

Una CA de una PKI sanitaria tiene políticas y procedimientos adecuados a los servicios que proporciona. Debe proporcionar:

- Procedimientos de registro de usuarios potenciales antes de emitir el certificado, y en su caso de registro de los roles de los usuarios.
- Procedimientos para autenticar la identidad del dueño de un certificado potencial.
- Procedimientos para mantener la privacidad de cualquier información personal que se gestione sobre las personas a las que proporcionan certificados.
- Procedimientos para distribuir los certificados a sus usuarios y a los directorios pertinentes.
- Procedimientos para aceptar información sobre las incidencias ocurridas en las llaves privadas.
- Procedimientos para distribuir las listas de revocación de certificados (frecuencia de publicación, y cómo y cuándo se publican)
- Cualquier otro aspecto sobre el manejo, incluido el tamaño de las llaves, los procesos de generación de llaves, la vida activa de los certificados, la re-generación de llaves, etc.
- Procedimientos de certificación cruzada con otras Autoridades de Certificación.
- Controles de seguridad y auditorias.

3.2. Autoridad de atributos (AA)

Es una autoridad que asigna privilegios emitiendo Certificados de Atributos [X.509] de forma similar a como lo hacen las CAs subordinadas.

3.3. Autoridad de Registro (RA)

Una Autoridad de Registro es una entidad que establece las identidades de los grupos que lo solicitan y registra sus requerimientos de certificación con una autoridad de certificación. [ISOTC215/WG4 Glossary of Security Terms].

La autoridad de registro puede también verificar el rol de los solicitantes, su cargo o estatus laboral con el fin de guardarla en un Certificado de Atributos. Es posible además que una RA que verifica un tipo de atributos (estatus laboral...) sea distinta de la RA de una organización que verifica las cualificaciones profesionales de un médico para ejercer la medicina (Ej.: si está registrado en el Colegio de Médicos...)

La identificación del rol de los profesionales sanitarios puede llevarse a cabo en las siguientes instituciones:

- Las Autoridades Nacionales o Autonómicas (hospitales o dependencias sanitarias).
- Colegio de Médicos o de cualquier otra especialidad sanitaria.
- Los colegios de sub-especialidades.
- Las aseguradoras públicas o privadas.

Un PKI sanitario tiene que basarse en las informaciones suministradas por estas entidades para la validación de las credenciales profesionales.

Por lo tanto es razonable considerar que algunas de estas entidades se transformaran en un futuro en CAs o RAs para sus afiliados. Tal es el caso de los Colegios de Médicos que emiten tarjetas de identidad a sus médicos y que en un futuro puede emitir Tarjetas electrónicas inteligentes conteniendo los PKC de identificación con la información sobre sus cualificaciones profesionales y sus roles primarios.

3.3.1. Obligaciones de una autoridad de registro

Una CA puede delegar las funciones de identificación y autenticación, de las cuales es responsable, a una Autoridad de Registro (RA).

Al iniciarse un registro, la primera función que debe llevar a cabo una autoridad de registro de una organización, es la verificación de la identidad del dueño del certificado y de su rol en el entorno sanitario.

También puede confiarse a la RA las solicitudes de revocación de certificados a las CAs en tiempo y forma.

Es recomendable que las RAs registren las acciones llevadas a cabo en nombre de las CAs con fines de control.

Una RA debe:

1. Asegurar que su llave privada sólo se utiliza para firmar demandas de certificados en el caso de que estas se hagan on line.

2. Certificar a las CAs que ha autenticado la identidad del dueño del Certificado..

3. Transmitir y guardar de forma segura la información de las solicitudes y los archivos del registro.

4. Iniciar la demanda de revocación (cuando sea aplicable).

COMENTARIO FINAL

Con esta exposición hemos querido divulgar los conocimientos que el personal sanitario debe poseer en el momento que manipule una información sanitaria en formato electrónico, con el fin de que no viole y utilice con propiedad las herramientas de seguridad a su alcance.

Estos y otros conceptos relacionados con la medicina, las tecnologías de la información y las telecomunicaciones deberían tomarse en consideración en la formación de médicos ya que están contenidas en el cuerpo de conocimiento de la Telemedicina (5,6).

BIBLIOGRAFÍA

1. Real Decreto 994/1999, de 11 de junio. Ministerio del Interior. Disponible en: http://www.mir.es/derecho/ rd/rd_99499.htm
2. Ley Orgánica 15/1999, 13 de diciembre. Protección de datos de carácter personal. Disponible en: http://www.i-3.org/docs/datos/lopd.pdf
3. Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. (B.O.E. 18-09-1999). Disponible en: http://www.aeat.es/normlegi/otros/ rdl1499.htm
4. CEN/TC 251 European Standardization of Health Informatics. http://www.centc251.org
5. Ferrer-Roca O, editor. Telemedicina. Madrid: Editorial Panamericana. 2001.
6. Ferrer-Roca O, editor. La Telemedicina: Situación actual y perspectivas. Madrid: Biblioteca Fundación Retevisión-Auna. 2001.

NORMATIVAS DE REFERENCIA

ISO/IEC 2382-8:1998	Information technology – Vocabulary -- Part 8: Security
ISO/IEC 7498-2	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
ISO/IEC 8824-1:1995	Information Technology - Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1). - Part 1: Specification of the basic notation
ISO/IEC 10181-1	Information technology – Open Systems Interconnection – Security frameworks for open systems – Overview.
ISO/IEC TR13335	Guidelines for management of IT Security – Part 1, Concepts and models for IT security.
ISO/IEC 14516	Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services
ISO/IEC 15945	Information technology – Security techniques – Specification of TTP services to support the application digital signatures
ISO/IEC 17799:2000	Information technology -- Code of practice for information security management
ITU-T X.509:1997	Recommendation X.509: The Directory - Authentication Framework. Equivalent to ISO/IEC 9594-8
IETF/RFC 2459	Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
IETF/RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF/RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile
ENV 13608-1	Health informatics - Security for healthcare communication - Concepts and terminology