DESARROLLO DE UN SISTEMA PARA LA FIRMA DIGITAL DE REGISTROS MÉDICOS

CONFERENCE PAPER · JANUARY 2006

READS
305

5 AUTHORS, INCLUDING:

Adrián Gomez
Hospital Italiano de Buenos Aires
90 PUBLICATIONS **138** CITATIONS
SEE PROFILE

Damian Borbolla
Hospital Italiano de Buenos Aires
29 PUBLICATIONS **59** CITATIONS
SEE PROFILE

Daniel Luna
Hospital Italiano de Buenos Aires
158 PUBLICATIONS **279** CITATIONS
SEE PROFILE

Enrique R Soriano
Hospital Italiano de Buenos Aires
121 PUBLICATIONS **1,362** CITATIONS
SEE PROFILE

DESARROLLO DE UN SISTEMA PARA LA FIRMA DIGITAL DE REGISTROS MÉDICOS

A. GÓMEZ, F. PLAZZOTTA, F. CAMPOS, M. MARTÍNEZ, J. SEVERINO, F. PEDERNERA, A. MAURO, D. BORBOLLA, D. LUNA, E. SORIANO, F. GONZÁLEZ BERNALDO DE QUIRÓS.
Departamento de Información Hospitalaria, Hospital Italiano, Buenos Aires, Argentina.

El avance tecnológico sobre tecnologías montadas en entornos compartidos requiere de un tratamiento especial con respecto al manejo de documentación sensible, por esto, el presente trabajo describe los mecanismos tecnológicos utilizados para realizar el proceso de firma digital de documentos clínicos basados en el estándar XML. Es por ello que el Hospital Italiano de Buenos Aires desarrolló un sistema para aplicar la Firma Electrónica/Digital a los documentos asistenciales en el contexto de una Historia Clínica Electrónica, creando su propia infraestructura PKI, almacenando las claves pública y privada en un E-Token. Luego de registrar todos los eventos asistenciales que genera el proceso de atención se crea un documento clínico utilizando el estándar CDA (Clinical Document Architecture). El compendio de toda la actividad del médico, documentada en un único archivo XML, con el agregado de la Firma Electrónica/Digital provista por el e-token y de un servicio de Time Stamping (también firmado), permitirá crear un registro fiable y único de los actos médicos. Para lograr administrar las claves y el otorgamiento de los e-tokens fue necesario modificar el sistema de alta, baja y modificación de personas con el rol institucional, así como un estricto control normatizado de los procesos involucrados. Actualmente se está realizando una prueba piloto para la puesta a punto del sistema y las normas y procedimientos creados a tal fin.

1. Introducción

Al firmar una persona un documento en papel con una pluma, realiza trazos con características tales, que sólo esa persona puede realizarlos. De esa manera se deja constancia que sólo ese individuo es el responsable de lo que dice el documento. Además se firma al final del contenido para dejar constancia que lo que se refrenda no ha sido modificado, firmando posteriormente cada modificación o escritura posterior que halla sido realizada en el mismo. De esta manera, se garantiza la autoría o acuerdo con el contenido e integridad de la información.

En el ámbito médico se sigue esta misma modalidad, el médico al terminar de registrar en papel la atención realizada a un paciente, firma y sella al final del registro. Cada registro posterior debe ser firmado, pero esta firma solo indica la autoría de la modificación desde la firma previa.

En la Argentina el ejercicio de la medicina, odontología y actividades auxiliares se encuentra bajo la normativa de la ley 17.132 promulgada en el año 1967, que en su artículo 19 especifica que *"...las prescripciones y/o recetas deberán ser manuscritas, formuladas en castellano, fechadas y firmadas. La Secretaría de Estado de Salud Pública podrá autorizar el uso de formularios impresos solamente para regímenes dietéticos o para indicaciones previas a procedimientos de diagnóstico..."*. Esto podría ser considerado un obstáculo en la implementación de la firma digital en documentos médicos[1].

El avance tecnológico sobre tecnologías montadas en entornos compartidos requiere de un tratamiento especial con respecto al manejo de documentación sensible, la firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que estos documentos tengan la misma validez que aquellos firmados en papel, ya que por medio de la utilización de procesos matemáticos relaciona el documento firmado con información propia de la persona firmante, permitiendo que otras partes puedan reconocer la identidad del firmante y asegurarse que los contenidos no han sido modificados.
El objetivo del presente trabajo es describir el desarrollo de un sistema para aplicar la Firma Electrónica/Digital a los documentos asistenciales en el contexto de una Historia Clínica Electrónica

2.Descripción General

2.1. Escenario

A fines de la década del 90, en la Argentina se promulgaron normativas acerca de la seguridad informática. Concomitantemente en el Hospital Italiano de Buenos Aires (HIBA) se estaba llevando adelante un proyecto de informatización de la capa clínica [2][3]. Hoy dicho proyecto con más de 5 años de implementación y funcionamiento, registra en una Historia Clínica Electrónica (HCE) los datos médicos obtenidos del proceso de atención.
Nuestro proyecto, incluye como objetivo principal, generar los mecanismos de seguridad necesarios para operar y mantener un sistema de registro médico descentralizado, teniendo presente que la seguridad de la información médica se basa en cinco aspectos fundamentales:

- **La privacidad**: hace referencia a que la información medica no pueda se accedida por un tercero que no este relacionado al proceso de atención.
- **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.
- **Autenticidad**: Se refiere al carácter de auténtico del documento, es decir que sea el original.
- **La integridad**: Relacionado con el anterior, se refiere al contenido de la información médica impidiendo que sea alterado de su registro original.
- **La 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.

2.2. Ley de Firma Digital

En el año 1998 a través del decreto 427/98 se autoriza la utilización de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, otorgándole los mismos efectos que la firma ológrafa y estableciendo las bases para la creación de la Infraestructura de Firma Digital para el Sector Público Nacional [4]. En ese mismo año por medio de la Resolución 194 se establecen los estándares sobre tecnología de Firma Digital para la Administración Pública. Pero es recién a fines del año 2001 que se sanciona la Ley 25506 de Firma Digital, la cual fue finalmente reglamentada por el decreto 2628/02 en diciembre del año 2002.
Esta ley principalmente reconoce el empleo de la firma digital, firma electrónica y su validez jurídica, permitiendo la identificación fehaciente de las personas que realicen transacciones

electrónicas. De esta manera, cuando un documento requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital.

2.3. Firma electrónica

La figura de Firma Electrónica esta descripta en el artículo 5º de la Ley de Firma Digital. Es un proceso electrónico, que permite al receptor de un documento electrónico identificar, al menos formalmente a su autor. De este modo, será reconocida como firma electrónica cualquier señal, contraseña, código o clave que una persona haya asumido como símbolo de su propia identidad, y los documentos que esa persona firme usando dicha clave o código serán equivalentes a un documento firmado en papel.
La firma electrónica admite grados de seguridad, exclusividad e inviolabilidad, y tal como el documento firmado sobre papel, también admite grados de admisibilidad como prueba, en casos de controversia o conflicto de intereses. En caso de ser desconocida la firma electrónica, corresponde a quien la invoca acreditar su validez.
Las firmas electrónicas son parte de nuestra actividad diaria ya que las utilizamos en los cajeros automáticos, en compras con débito y en Internet para ingresar a un sitio que requiera reconocer al usuario.

2.4. Firma digital

La firma digital es la parte del certificado que permite al receptor del mensaje verificar la autenticidad del origen de la información, así como verificar que esta información no ha sido modificada desde su creación. De esta manera, la firma digital garantiza el no repudio de la autoría, pues su validez legal es equivalente a la de la firma manuscrita, esto la diferencia de la firma electrónica, la cual requiere acreditar la autoría. La firma digital se basa en la confianza que ofrece la infraestructura de clave pública y privada (Private Key Infraestructure) [5].
Para utilizar la firma digital y que ésta sea valida, el certificado digital de la persona que firma debe estar avalado o emitido por un certificador licenciado. Este certificador debe ser obtenido de algún organismo público u organización autorizada a emitirlos.

2.5. Proyecto de Implementación en el Hospital Italiano de Buenos Aires

El proyecto de firma digital esta basado en la arquitectura Private Key Infraestructure (PKI), que contempla un sistema de claves públicas y privadas otorgadas por Autoridades Certificantes.
El Hospital Italiano de Buenos Aires tomó la iniciativa de crear su propia infraestructura PKI por intermedio de un desarrollo “in house” que posibilita llevar adelante todo el proceso de creación y administración de claves públicas y privadas.
El sistema de información de nuestra institución, registra todos los eventos médicos que genera el proceso de atención. Basado en un sistema de registro electrónico, el medico registra en la HCE web determinados ítems médicos que agrupamos de la siguiente forma:

- Problemas médicos.
- Evoluciones Médicas.
- Estudios solicitados.
- Observaciones clínicas.

- Prescripción Farmacológica.
- Fecha y Hora

Todos estos conceptos agrupados representan un evento medico o consulta medica, todo los datos médicos que un profesional registra en el acto de atención, se registra dentro de estos ítems que representan el evento en salud o la consulta medica propiamente dicha. Una vez terminada la consulta, el medico firma digitalmente el evento medico y se almacena en un repositorio seguro (ver figura 1) [6].

Tomamos la decisión de almacenar dichos eventos con el estándar propuesto por HL7 en su "Clinical Document Architecture" (CDA) y así generar un repositorio de eventos clínicos firmados (y no las bases analíticas transaccionales). El proceso de firma digital consiste en reunir la información médica ingresada, y se construye un archivo XML.

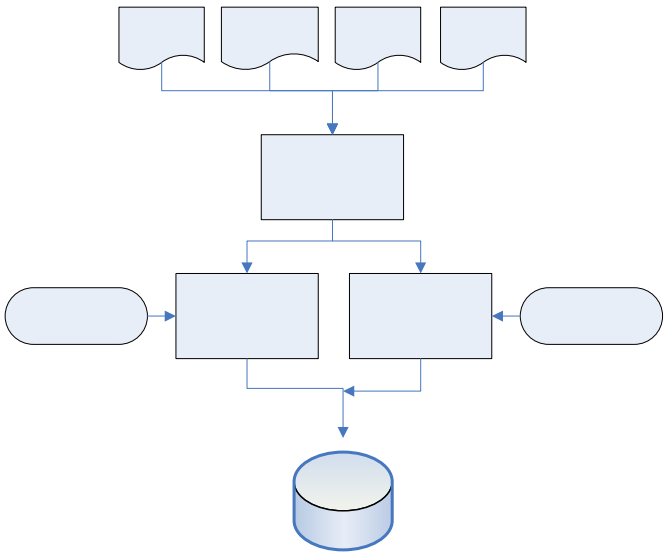

Figura 1. Generación de un Documento Firmado

El XML es un estándar en crecimiento utilizado principalmente en los entornos Web, desarrollando en los últimos tiempos un estándar que ayuda a generar seguridad en el entorno. La seguridad en XML combina algoritmos criptográficos con tecnología XML brindando un entorno seguro tanto para los usuarios como para las aplicaciones.

La firma digital de archivos XML es un estándar de seguridad recientemente implementado por el consorcio W3C [7].

A fin de garantizar su integridad y autenticidad, un documento digital debe cumplir con tres características principales:

- Poseer un hash, para garantizar la integridad del documento. Se trata de un identificador corto y único, una cadena de dígitos, generado luego de aplicar una fórmula matemática a un documento o secuencia de texto, únicamente correspondiente con el original e irreversible.
- Haber sido firmado con un sistema de claves privada y pública, para garantizar su autoría.
- Y poseer un servicio de Time Stamping, para darle temporalidad al documento.

Clave

Con el agregado de la Firma Electrónica/Digital provista por el e-token y de un servicio de Time Stamping (también firmado), permitirá crear un registro fiable y único de los actos médicos. En nuestro proyecto, las claves pública y privada de una persona son almacenadas en un E-Token. El E-Token es un componente electrónico con interfaz USB (Universal Serial Bus), similar a un dispositivo de memoria tipo flash (pendrive), pero a diferencia de éste, posee un microchip que tiene la capacidad de almacenar y procesar algoritmos criptográficos.

El time stamping de documentos es uno de los procesos mas complejos y problemáticos en la implementación de firma digital de documentos médicos. El momento exacto cuando ocurrió la carga primaria de la información es una de las variantes más importantes ya que se debe determinar en forma segura la existencia del documento médico en un determinado momento en el tiempo. Optamos por generar un proceso de impresión de la fecha y hora que se firme digitalmente por el sistema emisor y garantice de esta forma la veracidad del proceso.
El sistema persigue congelar el estado de cualquier objeto digital en un instante de tiempo, probando que el documento, tal y como se conoce, ya existía y no ha sido modificado hasta el presente.
Garantizada la identidad digital de la entidad que extiende el sello, se asegura que tal documento existía en la fecha y horas establecidas en el sello.
El registro horario firmado digitalmente por un servicio de time stamping se almacena con el registro del evento medico firmado por el usuario, de esta forma solucionamos el tema de la alteración de la fecha y hora en que se realizo el evento medico en el caso de accesos de súper usuarios. Además se almacena un archivo activo de las solicitudes de time stamp con su correspondiente firma digital para validación histórica (ver figura 2).

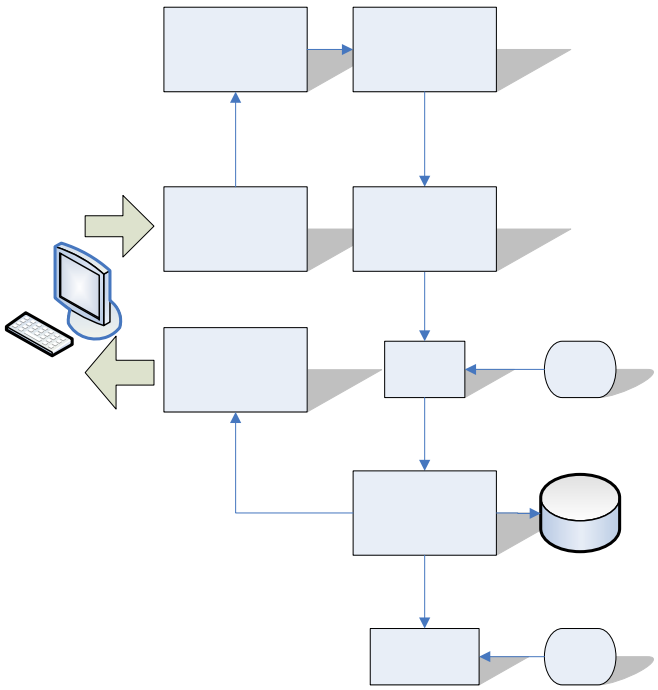

Figura 2. Proceso de Time-Stamping

2.6. Proceso informático de firma digital

El proceso de firma digital consiste en reunir la información médica ingresada, y se construye un archivo XML que contiene en un formato estándar, toda la información médica que representa el evento médico.
El generador del documento clínico XML calcula un único valor para el hash y encripta el valor del hash utilizando la clave privada almacenada en su token, dicha clave privada es generada por una autoridad certificante. Este archivo encriptado mantiene su información original y es certificado.
El proceso además permite validar el certificado del archivo XML generado, extrayendo la clave publica del archivo. El mensaje es desencriptado, se calcula el hash y se compara con el documento XML firmado.
Este proceso permite mantener una versión del documento medico, detectando posibles alteraciones en el registro original.
Se determina cual es el recurso a ser firmado identificado por el URI, y cada recurso referenciado se especifica en el elemento XML “Reference”. Se calcula el Digest (Hash) de

cada recurso, este cálculo de un recurso identificado se representa en el elemento "DigestValue", y por medio del elemento "DigestMethod", se identifica el algoritmo utilizado para calcularlo [8] [9].
Luego se firma el documento calculando el digest y se almacena la firma en el elemento "SignatureValue". Se agrega la información de la clave pública almacenada en el elemento "KeyInfo", aquí la clave es necesaria para la verificación posterior de la firma.
Los documentos médicos firmados son almacenados en un servidor seguro el cual oficia de repositorio de documentos firmados. Cualquier tipo de información médica puede ser verificada por intermedio de determinados procedimientos, los cuales validan si la información almacenada difiere de su registro original.

3. Discusión - Impacto Asistencial

Normalmente, el médico valida su identidad una única vez al ingresar a la HCE, mediante un nombre de usuario y una contraseña. Esta contraseña es otorgada luego de que el profesional firma un convenio de confidencialidad al concluir su capacitación en el uso del sistema. Todas las acciones realizadas por el profesional a través de la HCE, o que constan en la misma, quedan registrados a nombre del usuario.
El compendio de toda la actividad del médico, documentada en un único archivo XML, con el agregado de la Firma Electrónica/Digital, provista por el token, permitirá crear un registro fiable y único de los actos médicos.
La implementación de la firma electrónica/digital en un registro electrónico de salud es un verdadero desafío, ya que conlleva un importante impacto tecnológico y organizacional. Actualmente se está realizando una prueba piloto para la puesta a punto del sistema y las normas y procedimientos creados a tal fin.

Referencias

1. *Ley 17132 - Regimen Legal del Ejercicio de la Medicina, Odontología y Actividades Auxiliares de las mismas.*, in *Boletín Oficial de la República Argentina*. 1967.
2. Gonzalez Bernaldo de Quiros, F., et al. *Desarrollo e implementación de una Historia Clínica Electrónica de Internación en un Hospital de alta complejidad*. in *6to Simposio de Informática en Salud - 32 JAIIO*. 2003. Buenos Aires, Argentina: Sociedad Argentina de Informática e Investigación Operativa (SADIO).
3. Luna, D., et al. *Implementación de una Historia Clínica Electrónica Ambulatoria: "Proyecto ITALICA"*. in *6to Simposio de Informática en Salud - 32 JAIIO*. 2003. Buenos Aires, Argentina: Sociedad Argentina de Informática e Investigación Operativa (SADIO).
4. *Ley 25506 - Ley de Firma Digital.*, in *Boletín Oficial de la República Argentina*. 2001. p. 1.
5. *Infraestructura de Firma Digital de la República Argentina*. 2004, Subsecretaria de la Función Pública.
6. *Extensible Markup Language (XML) 1.0 (Third Edition)*, T. Bray, Editor. 2004, W3C.
7. Gonzalez Bernaldo de Quiros, F., et al. *Migración a plataforma web de una Historia Clínica Electrónica*. in *CBIS'2004 - IX Congresso Brasileiro de Informática em Saúde*. 2004. Ribeirao Preto-SP. Brasil.
8. *XML-Signature Syntax and Processing*, I.R.S. 3075, Editor. 2001, IETF RFC Standard 3075.
9. Imamura, T.D., B. Simon, E., *XML Encryption Syntax and Processing*. 2002, W3C.

Contacto:

Lic. Adrián Gómez,. Departamento de Información Hospitalaria Hospital Italiano de Buenos Aires. Gascón 450 Ciudad Autónoma de Buenos Aires. Argentina. adrian.gomez@hospitalitaliano.org.ar