Modelo para la implementación de historias clínicas electrónicas centralizadas y con validez legal

Franco Vinciarelli[1], Miguel Angel Robledo[2], y Natacha Dinsmann[3]

Área de Informática Educativa y TeleSalud
Facultad de Ciencias Médicas
Universidad Nacional de Rosario

[1]vinciarellifranco@gmail.com
[2]miguelarobledo@gmail.com
[3]ndinsmann@hotmail.com

Resumen. Este trabajo propone y analiza un nuevo modelo para gestionar información digital, y por ende documentación electrónica, producto de la interacción entre pacientes y profesionales de la salud con el objetivo de construir la historia clínica electrónica única de una persona, pudiéndose utilizar a niveles locales, nacionales e internacionales.
Este modelo se basa en la implementación de servicios informáticos TICs orientados a redes y el uso de la tecnología de clave pública mediante firma digital. La nueva propuesta resuelve la integración de sistemas de salud disímiles (productores de documentos), la asignación de las propiedades de autenticación y no repudio e integridad para dotar de valor legal la información (documentos o mensaje) suministrada y acondicionamiento de los documentos para ser persistidos en repositorios centrales o distribuidos definidos por el usuario.
Finalmente se presenta una aplicación de software posible de implementar en entornos de escritorio o dispositivos móviles donde se adopta el modelo propuesto para ejemplificar su funcionamiento.

1 Introducción

En la actualidad no existe un estándar definido que establezca lineamiento para la implementación de un repositorio universal integrado de historias clínicas digitales de personas que pueda dar respuesta a la demanda constante de información tanto para el trabajo diario de los profesionales de la medicina (en ámbitos públicos como privados) como para los ciudadanos en general en el cuidado de su salud a nivel local y nacional.

Si bien existen estándares que definen cómo debería ser modelado un sistema informático para salud (medicina) dentro de los cuales podemos mencionar openehr[1], hl7[2], iso/tc 215[3], entre otros; sus usos requieren modificaciones importantes a los sistemas ya implementados, situación que en general es prohibitiva o es inviable su implementación por distintas razones, dentro de las cuales podemos mencionar: su costo de desarrollo, el esfuerzo de adaptación de las constantes nuevas tecnologías que se suceden en la medicina, la poca experiencia concreta o desconocimiento en la utilización de los mismos, entre otros.

Surgen además, inconvenientes en la trazabilidad de la información de la persona-paciente, que al ser tratado en diferentes instituciones (en la misma o diferente región geográfica), generan registros de datos clínicos independientes, asignándole a esta información un carácter parcial y dificultando su integración.

A los problemas mencionados, las actuales implementaciones de registros electrónicos en sistemas de salud presentan otros problemas frecuentes dentro de los cuales los más frecuentes y críticos son duplicidad de la información, desprotección legal de los profesionales y pacientes a los que refieren los documentos generados, dificultades en el acceso a la información, costoso mantenimiento de documentos, entre otros.

En el presente trabajo se propone una nueva metodología que, con el objetivo de dar solución a los problemas mencionados, hace uso de tecnologías existentes como internet, el formato de documento portable ISO32000-1:2008[4] y la firma digital de documentos, y describe los lineamientos a tener en cuenta y los pasos a seguir para resolver estos problemas.

2 Problema

Los grandes avances en tecnologías de comunicación y gestión de la información aún no pudieron tener un impacto relevante en la implementación en los sistemas de salud con el fin de garantizar los derechos a la salud de las personas con la máxima calidad de servicio posible y el acceso a su historia clínica completa con independencia del centro de salud desde donde se atienda.

Es requerimiento, desde hace décadas, contar con un repositorio de documentos de registros clínicos digital de los ciudadanos con características legales idénticas a las de soporte papel firmados holográficamente. Este repositorio debe poder integrar y permitir acceso continuo desde distintas locaciones y por distintos tipos de usuarios para consulta o actualización.

---

[1] OpenEHR http://www.openehr.org/

[2] Health Level Seven http://www.hl7.org/

[3] ISO/TC 215 Health informatics http://www.iso.org/iso/iso_technical_committee?commid=54960

[4] ISO 32000-1:2008 http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502

Para ejemplificar ésta problemática en nuestro ámbito laboral, "En la ciudad de Rosario, Santa Fe, Argentina que cuenta con 54 centros de salud y 5 Hospitales Municipales donde se cuenta con varios sistemas informáticos generadores de documentos clínicos, su totalidad son persistidos en soporte papel en distintas carpetas en diferentes nosocomios. Existen dificultades para mantener, integrar y utilizar estos registros de salud del paciente. Esta problemática se da en cada localidad de nuestro país, agravado cuando se desea realizar una interacción entre provincias o ciudades diferentes donde se presentan particularidades de implementación.

Desde el ámbito tecnológico, esta demanda insatisfecha tiene sus bases en las dificultades para dar solución en forma integral en las siguientes situaciones problemáticas:

1- ¿Cómo dotar de legalidad a los documentos producidos?.

2- ¿Qué formato adoptar como estándar?.

3- ¿De qué manera integrar los distintos sistemas que actualmente poseen las distintas organizaciones del área de salud en cuanto productores de documentos en distintos formatos de texto e imágenes con el menor impacto posible?.

4- ¿Qué formato utilizar para persistir los documento generados que permita sin agregados de piezas de software particulares la visualización y verificación de sus propiedades?.

3 Solución

En esta sección, damos respuesta a las interrogantes planteadas en el apartado anterior y mostramos cómo, a partir de un nuevo modelo de diseño general, es posible particularizarlo para luego formalizar una solución informática que resuelva las situaciones problemáticas particulares y en conjunto, la situación problemática general de contar con un repositorio integral de documentos de historias clínicas electrónicas de una persona.

Como se mencionó en las secciones anteriores, el problema tecnológico para la implementación de un repositorio de historias clínicas, desde el punto de vista tecnológico, se encuentra sustentada por la dificultad de “integrar” las situaciones problemáticas particulares. Esta integración puede resolverse a partir del modelo de solución general que proponemos cuya gráfica de modelo se muestra en la figura 1.

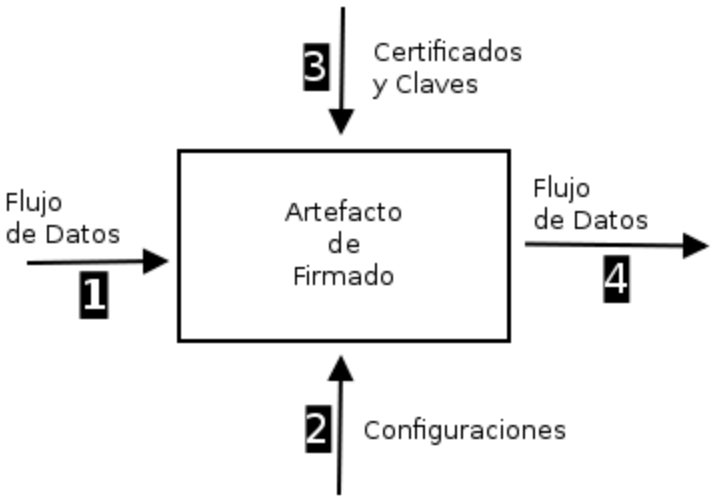

Fig. 1. Módulo general de la solución propuesto

A partir de la observación del modelo general de la figura anterior, podemos aplicarlo al problema general planteado en el presente trabajo y concluir que lo resuelve de la siguiente manera:

"Dado el caso, en que se requiere integrar un conjunto de flujos de datos con origen en distintos sistemas informáticos, para procesar su firma y posteriormente encapsularlos en un formato estándar para su distribución, se deberá construir un artefacto de firmado, autocontenido en sus funcionalidades y preferentemente externo a todos los sistemas productores de datos que hacen uso de éste, que permita ser alimentado en sus entradas por los datos a firmar (entrada 1) y un conjunto de parámetros de configuración que afecte su funcionamiento (entrada 2) . Una vez invocado para el procesamiento de los datos, éste deberá gestionar el acceso a la información requerida para producir la firma digital (entrada 3) para finalmente, emitir como resultado (salida 4) los datos de entrada junto a su firma digital correspondiente"

Conforme lo expuesto, mostramos a continuación un diagrama funcional de las partes componentes generales del artefacto firmador que se corresponden a las funcionalidades requeridas descriptas anteriormente.

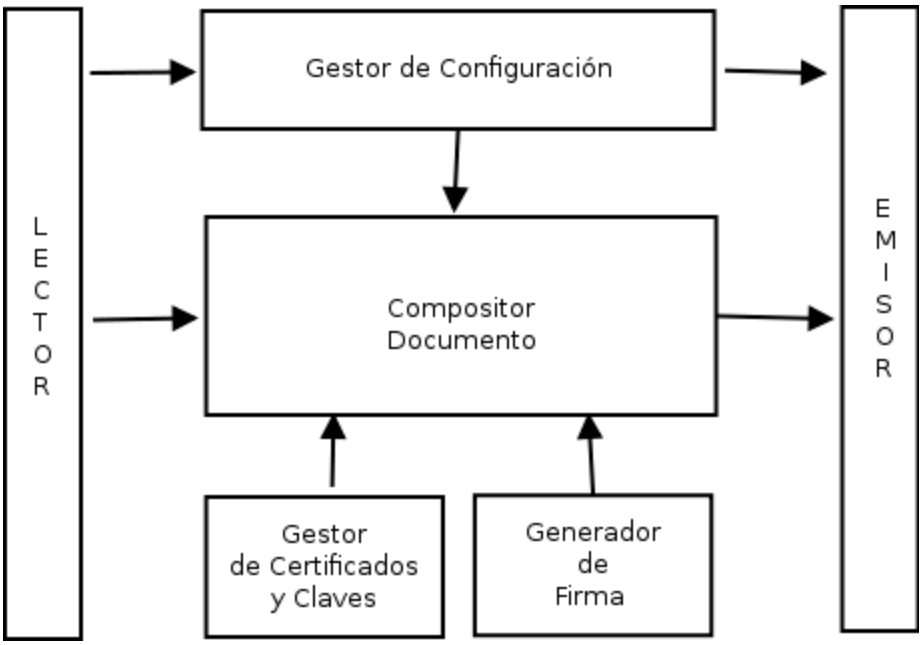

Fig. 2. Diagrama funcional de las partes del componente

Hasta aquí, se ha expuesto un modelo de solución general. A continuación se muestra, la flexibilidad del modelo propuesto para ser particularizado en un modelo de solución concreta fácilmente portable a una solución de software.

Para construir una solución concreta, es menester contar con mayores precisiones respecto a cómo particularizar cada componente funcional del artefacto del modelo general en correlación a las situaciones problemáticas particulares. Por ello, a continuación mencionamos las dificultades planteadas y soluciones adoptadas.

¿Cómo dotar de legalidad a los documentos producidos por sistemas de salud que se equiparen con los de soporte papel?

La Firma digital es una herramienta tecnológica que permite garantizar la integridad, inalterabilidad y autenticidad de los documentos enviados por medios electrónicos, así como también permite verificar su autoría .

Es una cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente. La creación y verificación de firmas digitales se realiza mediante procedimientos técnicos, y supone la existencia de normas que respaldan su valor legal.

Funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante. Mediante una función matemática, genera una huella digital del mensaje, la cual es cifrada con la clave privada del firmante. Permite establecer en documentos digitales, características que eran

propias de los documentos en forma física o papel brindándonos las siguientes propiedades importantes:

- *Autoría*: implica poder atribuir de forma que no admite duda, que el mensaje electrónico recibido es de una determinada persona, autora del mensaje.
- *Integridad*: implica la certeza de que el mensaje recibido por el receptor es exactamente el mismo mensaje enviado por el emisor, sin que haya sufrido alteración alguna durante el proceso de transmisión.
- *No repudio*: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado.

Con la implementación de firma digital, ya no es necesario desplazarse desde un lugar de trabajo o la casa para realizar trámites que muchas veces requieren largas esperas, puesto que no se requiere desde ahora de la presencia física de las partes para la suscripción de acuerdos. Se abre paso a una multitud de nuevas formas de contratación de trámites públicos y privados que pueden realizarse digitalmente con mayor seguridad [1] . Gráficamente se ilustra el proceso en la Figura 3.

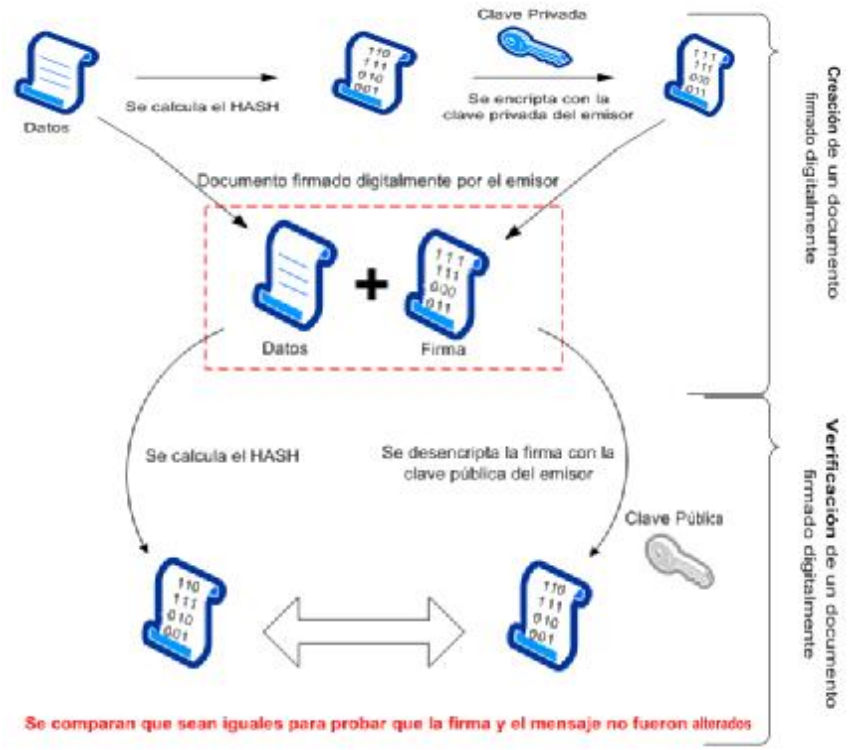

Fig. 3. Proceso de Firmado y verificación

Por lo expuesto, la firma digital satisface las propiedades autenticación de origen, no repudio e integridad permitiendo satisfacer sobre cualquier mensaje (información o documento) digital las mismas propiedades que satisface la firma holográfica sobre un documento en papel.

En nuestro país, a partir de la sanción de la Ley 25.506/2001[5] y toda su normativa complementaria, se cuenta con el marco regulatorio para la aplicación de firma digital. Dicha ley establece la plena validez de la firma digital y la firma electrónica al decir *"...se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley..."* y las equipara a la firma hológrafa cuando dice *"...cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital..."*.

La diferencia entre firma digital y electrónica radica fundamentalmente en que la primera es generada en una infraestructura que cumple absolutamente todos los requisitos que se establecen en la presente ley, incluido el licenciamiento de la autoridad que emite los certificados digitales. En caso de que no se cumplan todos los requisitos, la firma se denomina electrónica y carece de la presunción del no repudio, por lo cual ante un eventual fallo judicial, se invierte la carga de la prueba. En el caso de firma digital existe la presunción del no repudio, por lo que quien cuestione la firma tiene la carga de la prueba.

La aclaración anterior es importante porque es necesario saber que ambas tienen valor probatorio, sólo que el tratamiento judicial es distinto en caso de litigios. Esto es a los fines de comprender que en caso de no contar con una política específica de generación de certificados digitales para una determinada aplicación, existe la posibilidad de implementar firma electrónica, con plena validez jurídica de acuerdo al marco normativo nacional.

Considerando que tecnológicamente tienen el mismo comportamiento, la solución propuesta puede ser aplicada con firma digital o firma electrónica dependiendo si la Autoridad Emisora de Certificados que emita los certificados de firma de cada profesional es un Certificador Licenciado en nuestro país[6].

¿Qué formato adoptar como estándar?

Si bien la firma digital puede ser aplicada a cualquier formato de documentos es nuestro interés utilizar lineamientos de estándares abierto con fuerte consenso internacional. Existen dos estándares para firma electrónica avanzada como son el formato PAdES (PDF Advanced Electronic Signature) estándar ETSI TS 102 778[7] el cual establece restricciones y extensiones al estándar Portable Document Format (PDF) ISO3200:2008 para poder incluir firma electrónica avanzada [2][3][4][5][6][7] y el formato XAdES (XML Advanced Electronic Signature) estándar ETSI TS 101 903[8] el cual establece restricciones y extensiones al formato de firma XMLD-Sig para

[5] Ley Nacional de Firma Digital N° 25.506
http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[6] Infraestructura de Firma Digital de la República Argentina (IFDRA)
https://www.jefatura.gob.ar/ente-licenciante_p144

[7] ETSI TS 102 778
http://www.etsi.org/standards-search?search=ETSI+TS+102+778&page=1&ed=1&sortby=1

[8] ETSI TS 101 903
http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=35243

poder aplicar firma electrónica avanzada en formato XML (eXtensible Markup Language).

En el modelo propuesto como solución se adopta el formato PAdES por la portabilidad del documento resultante. Cabe destacar que , por la independencia de los módulos o servicios propuestos el formato XAdES podrá ser aplicado si el escenario lo requiere.

¿De qué manera integrar los diferentes sistemas que actualmente poseen las organizaciones del área de salud en cuanto productores de documentos en distintos formatos de texto e imágenes con el menor impacto posible?

Los sistemas preexistentes deberán ser capaces de hacer uso del artefacto de firmado antes mencionado como servicio.

Para ello deberán implementar una nueva funcionalidad que se implementará dentro del sistema particular, en los casos en que se posea acceso al código fuente, o como artefacto de software externo.

A continuación se sugiere una probable implementación de la nueva funcionalidad:

```
void integrar  (Documento documento) {
     String paginas[] = new String[documeto.cantPag];
      for (int i=0;i<documento.cantPag;i++) {
          paginas[i]=base64_encode(new Imagen(documento.pagina(i)));
     }

     invocar_servicio_externo(paginas,documento.cantPag);
}
```

Como se ve, la nueva funcionalidad puede implementarse de manera sencilla y su funcionamiento es simple.

Esta recibe como parámetro de entrada el documento producido por la salida de un sistema particular, y por cada página del documento genera una imagen que almacena en un arreglo codificada en Base64. Finalmente, se hace uso del artefacto de firmado invocándolo, pasando el arreglo de imágenes y su extensión.

El formato de codificación base64 para el tratamiento de los documentos es parte de la selección tecnológica propuesta. Su selección tiene por fundamento adoptar un formato de gestión de flujos de datos que permita la manipulación de cualquier tipos de datos (especialmente los binarios) como cadenas de caracteres que se ajuste sin problemas a protocolos de red como HTTP.

¿Qué formato utilizar para persistir los documento generados que permita sin agregados de piezas de software particulares la visualización y verificación de sus propiedades?

En la actualidad existen dos formatos de archivos que son aceptados internacionalmente como contenedores de datos y firmas digitales.

XML en su reglamentación XAdES y PDF en su reglamentación PAdES.

En este modelo adoptamos la implementeación mediante documentos PDF ya que entendemos el proceso de validación de las firmas que éste porta es para el usuario final mucho más fácil debido a la amplia difusión de visualizadores de PDF.

Conforme lo expuesto, nos encontramos ya en condiciones de utilizar como guía el modelo general de gestión de documentos antes propuesto y aplicar las restricciones requeridas por las respuestas dadas a las situaciones problemática particulares, para arribar al siguiente modelo de solución que aplica satisfactoriamente a la integración de documentos de registros clínicos de una persona.

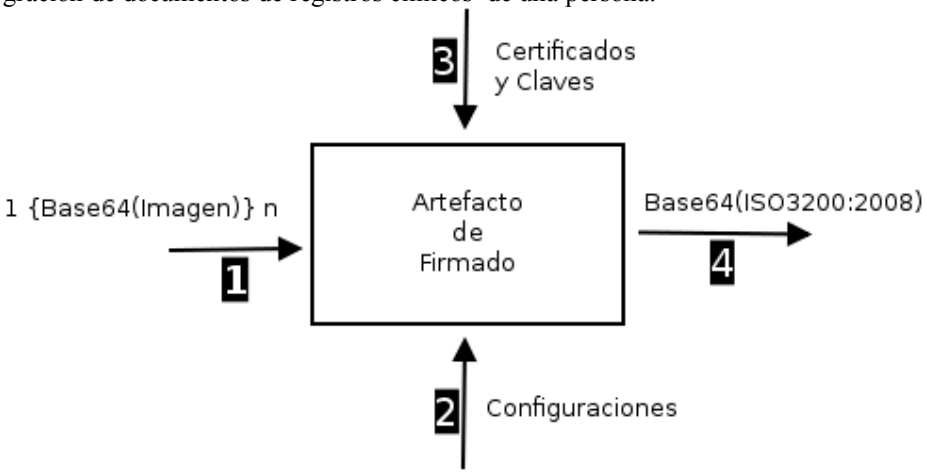

Fig. 4. Modelo General Particularizado

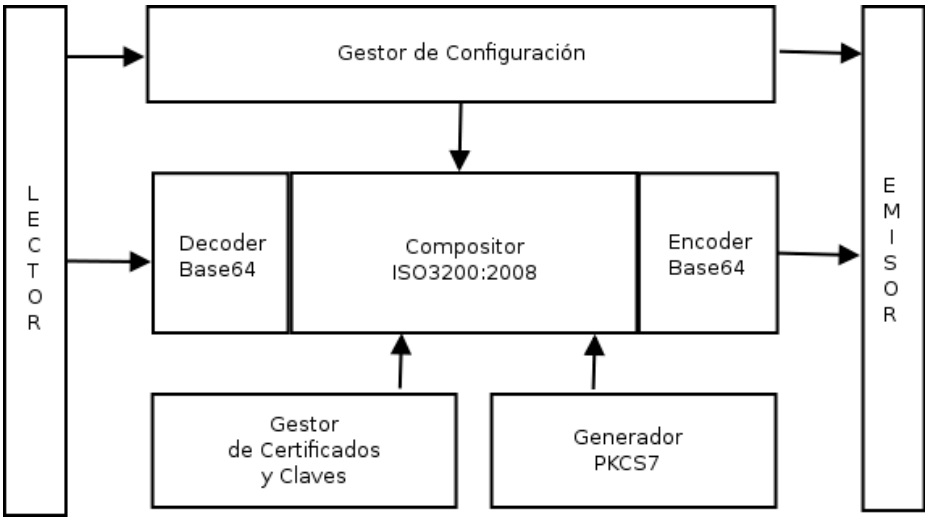

Fig. 5. Modelo de Componentes Particularizado

Si se observa la figura 4, se evidencia cómo el componente principal del artefacto general "Compositor de Documento" se ha particularizado a un "Compositor De Documentos ISO3200:2008" que incorpora un decodificador y codificador Base64 para interactuar con las componentes de lectura y escritura respectivamente. Este componente generará un documento en formato ISO32000:2008 que contendrá tantas páginas como imágenes se hayan pasado como entradas.

El modo de tratamiento de las imágenes y su cantidad, se determina a partir de la interacción con el componente de configuración. En la creación la firma digital del documento intervienen los componentes: "Gestor de Certificados y Claves" y "Generador de PKCS7". El primero se ha dejado sin particularizar para enfatizar que es responsabilidad del desarrollador definir cómo implementar el modo de captación y uso de los certificados y claves conforme los requerimientos legislativos del lugar de aplicación (ej: uso de dispositivos criptográficos token (PKCS#11[9]) o simple utilización de archivo PKCS#12[10] en sistema de archivos) . El componente siguiente "Generador de PKCS7" es una particularización del componente genérico "generador de firma" del modelo general que produce firmas digitales de un documento en formato PKCS#7 siendo este el estándar internacional de transporte de firmas digitales.

Finalmente se observa cómo el "Compositor De Documentos ISO3200:2008" comunica con un componente "emisor" utilizando una función de codificación Base64, situación que estandariza el formato de salida del documento resultado (que incluye la firma digital) en un formato plausible de ser distribuido a través protocolos de red para luego ser persistido.

[9] PKCS#11:http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.htm

[10] PKCS #12: Personal Information Exchange Syntax v1.1 https://tools.ietf.org/html/rfc7292

Completando la presente solución se exponen a continuación dos diagramas de secuencias.

En el primero, se muestra una interacción posible de los sistemas pre-existentes en una organización con el método particular propuesto.

En el segundo, se ejemplifica cómo, a partir de la flexibilidad de configuración y utilización de la tecnología de clave pública (PKI) en la solución propuesta, es posible persistir los registros legales de salida en forma centralizada en un servidor teórico. En particular, supondremos que la política del servidor de persistencia indexa los registros por un identificador de paciente (Ej: tipo de documento y número) que se obtiene de los parámetros de configuración del artefacto de software y que la validación del cliente (profesional de la salud), para hacer uso de los métodos del sistema de almacén, se realiza a través de validación por certificados.

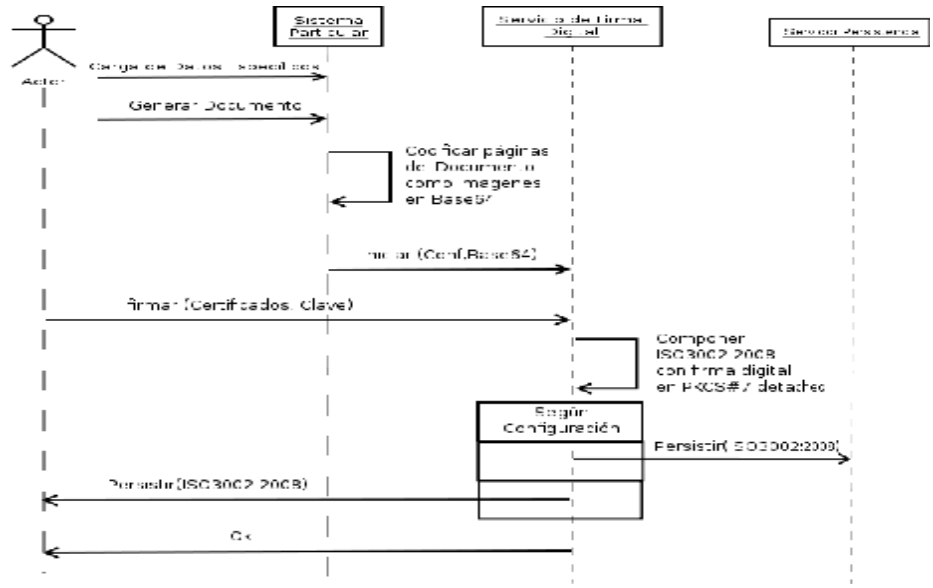

Fig. 6. Diagrama de Secuencias del uso del modelo por sistemas externos

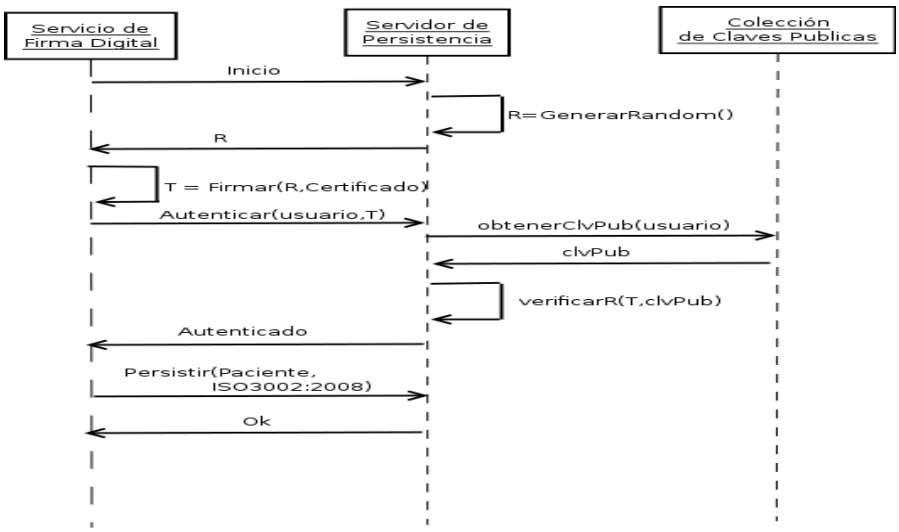

Fig. 6.1 Diagrama de Secuencias persistencia

4 Prototipo del modelo en dispositivos móviles

A continuación se expone un prototipo funcional de una aplicación que se ejecuta en dispositivos móviles con plataforma Android, donde se implementa el modelo presentado mostrando sus posibilidades de adaptabilidad. En particular, la aplicación permite a los profesionales de la salud emitir documentos de evoluciones de pacientes internados que se incorporan a su historia clínica.

En ésta aplicación el usuario (profesional de la salud) del sistema selecciona un paciente internado en una institución de una lista que obtiene de un servidor central que gestiona las internaciones. Acto seguido, se completan los campos requeridos para el formulario de evolución y se hace uso de un módulo funcional. Éste modulo funcional implementa cada uno de los componentes del modelo propuesto en el presente trabajo. A través del módulo funcional se invoca al componente que firma digitalmente el documento a través del uso del certificado digital de firma del profesional que emite la evolución y finalmente enviarlo a un repositorio general que lo persiste asociándolo al paciente.

A continuación se presentan las capturas de pantallas de las partes del sistema que implementan el modelo y se describe su correlación en el modo de uso. En la figura 7 se muestra la sección donde se establecen los parámetros de configuración del arte-

facto de software, a saber, la ubicación del certificado para firmas del usuario y la dirección URL del servidor de persistencia. Esta funcionalidad se corresponde a la configuración de la entrada 2 descripta en el modelo. Ésta acción es requerida, por única vez, en la primera ejecución de la aplicación.

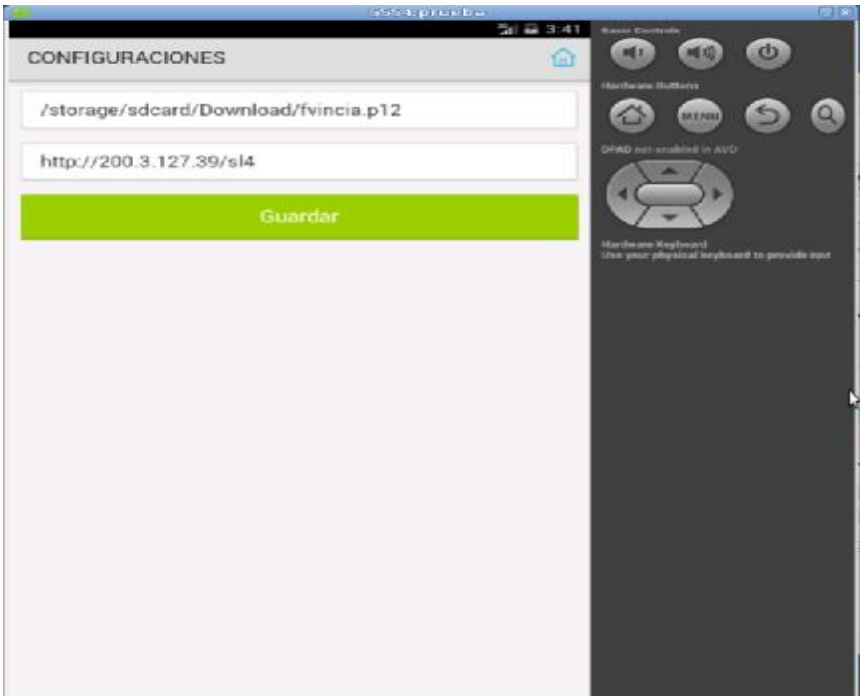

Fig. 7. Configuración Aplicación Móvil

Luego, en cada acción diaria del profesional, se debe completar el formulario de evolución. El documento de evolución será convertido a base64 para completar la entrada 1 del modelo y se genera con un formato como el que muestra la figura 8.

En esta instancia, el profesional debe validar el documento que se visualiza y en caso de conformidad debe elegir la opción Firmar, en caso contrario debe cancelar la operación.

En la figura 9 se muestra cómo se implementa la activación de la entrada 3 para la captura de la clave del certificado de firma con el fin de componer la firma digital del documento. Aquí se solicita una clave la cual, dependiendo del dispositivo de almacenamiento, puede ser una clave que protege encriptando por software al certificado dentro del dispositivo móvil o una clave de acceso a un dispositivo de almacenamiento criptográfico (smartcard, token criptográfico).

Una vez ingresada la clave de protección del certificado se produce el firmado digital del documento y su posterior envío a un servidor acorde a lo configurado, estas acciones se representan en las figuras 10 y 11 respectivamente.

Fig. 8. Vista previa de documento a Firmar Digitalmente

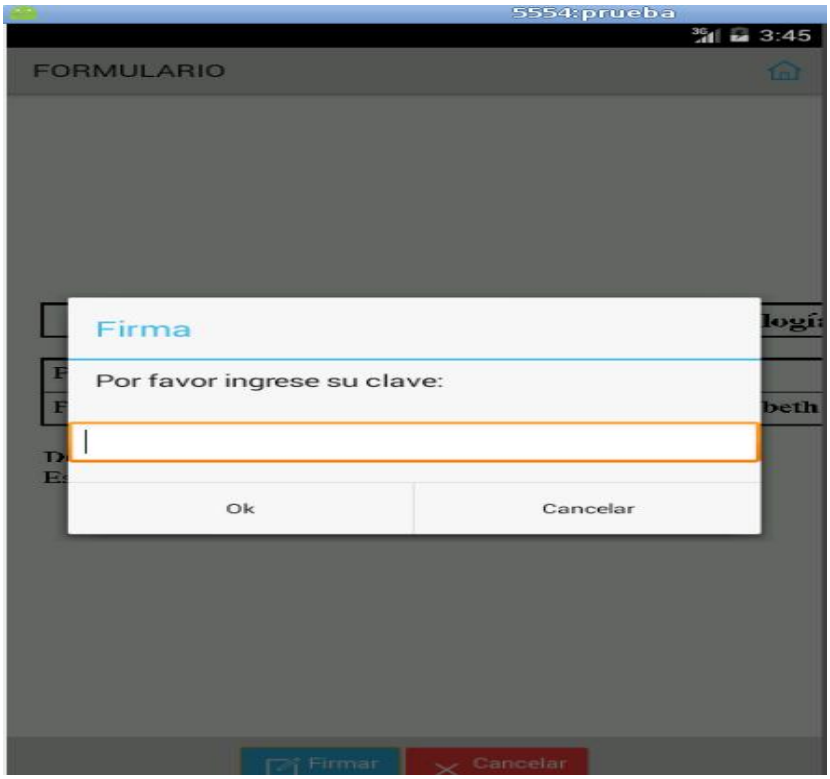

Fig. 9. Solicitud de Claves de acceso a certificado de usuario

Fig. 10. El artefacto firmando digitalmente documento.

Fig. 11. El artefacto enviando documento resultado.

Finalmente, el documento persistido puede accederse desde cualquier puesto y validar que ha sido generado por el profesional al hacer uso del visualizador de documentos PDF como se representa en la figura 12.

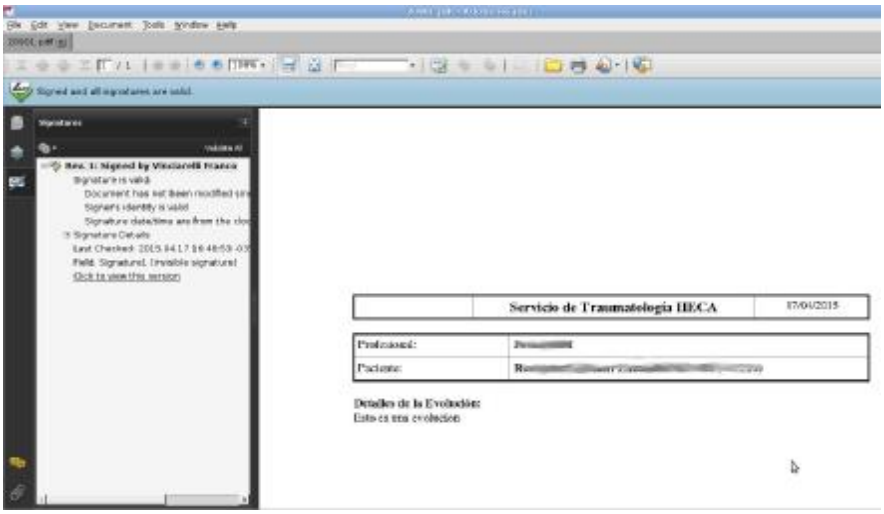

Fig. 12. Visualización del Documento Firmado Digitalmente

5 Conclusiones

El modelo que se propone aplica a la gestión de documentos digitales de historias clínicas para su firmado digital y su posterior uso. Este modelo es concebido como un artefacto, el cual posee como entradas flujos de datos a firmar, certificado y claves para la confección de la firma digital de los datos y un conjunto de parámetros de configuración que determinan su funcionamiento. Este artefacto es invocado como servicio por otros sistemas externos. El resultado de su uso, conlleva la obtención en la salida del artefacto de un flujo de datos compuesto por los datos pasados en su entrada más su firma digital.

Se ha trabajado con una implementación de un prototipo funcional de una aplicación que implementa el modelo propuesto. A través del prototipo se puede demostrar la independencia de una aplicación cliente para acceder a consultar documentos de registros clínicos, emitir la evolución de un paciente y actualizar la historia clínica del mismo. Además, el prototipo permite demostrar la sencillez de la operatoria para el profesional que interviene.

Referencias

1. Paulin G., Robledo M., Brusa G.: Diseño e implementación de time-stamping bajo un servidor confiable de fecha y hora, ISSN: 1850-2946 Pág. 1–19

2. PAdES Overview – a framework document for PadES http://www.etsi.org/deliver/etsi_ts%5C102700_102799%5C10277801%5C01.01.01_60%5Cts_10277801v010101p.pdf
3. PAdES Basic – Profile based on ISO 32000-1 http://www.etsi.org/deliver/etsi_ts%5C102700_102799%5C10277802%5C01.02.01_60%5Cts_10277802v010201p.pdf
4. PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles http://www.etsi.org/deliver/etsi_ts%5C102700_102799%5C10277803%5C01.02.01_60%5Cts_10277803v010201p.pdf
5. PAdES Long Term – PAdES-Long Term Validation Profile http://www.etsi.org/deliver/etsi_ts%5C102700_102799%5C10277804%5C01.01.02_60%5Cts_10277804v010102p.pdf
6. PAdES for XML Content – Profiles for XAdES signatures of XML content in PDF files http://www.etsi.org/deliver/etsi_ts%5C102700_102799%5C10277805%5C01.01.02_60%5Cts_10277805v010102p.pdf
7. Visual Representations of Electronic Signatures http://www.etsi.org/deliver/etsi_ts/102700_102799/10277806/01.01.01_60/ts_10277806v010101p.pdf
8. Adams and S. Lloyd, (1999), "Understanding Public-Key Infrastructure", Macmillan Technical Publishing.