Seguridad en Entornos BPM: Firma Digital y Gestión de Clave

Patricia Bazán , Paula Venosa, Nicolas Macia, Ivan Grcevic
LINTI, Facultad de Informática, UNLP

1. Resumen

Los sistemas de gestión de procesos de negocio (en inglés BPMS - *Business Process Management Systems*) se están estableciendo como las soluciones de IT adoptadas por las organizaciones actuales que buscan transformar su visión funcional clásica por un enfoque basado en procesos de negocio. Un proceso representa las tareas que la organización debe realizar para producir sus productos, el orden de ejecución de las mismas y las personas responsables de realizarlas.
En este sentido los BPMS, vistos como sistemas de información, deben incorporar mecanismos para garantizar los atributos de seguridad de autenticidad, confidencialidad, integridad, no repudio y disponibilidad.
La línea de investigación presentada propone incorporar conceptos de firma digital a un BPMS y a su vez, aplicar BPM a la gestión de seguridad, en particular al proceso de gestión de claves y su aplicación para la firma digital.

Palabras clave: Firma digital – BPMS – Seguridad — SGSI

2.Contexto

En el LINTI (Laboratorio de Investigación en Nuevas Tecnologías) [1] un grupo de docentes investigadores se dedican a estudiar temas relacionados a seguridad y privacidad en redes, en particular, lo referente a certificados digitales, su gestión y aplicación. Por otra parte, otro grupo aborda la línea de trabajo vinculada a metodología BPM, en particular, sus soluciones tecnológicas.
En esta propuesta se entrelazan ambas líneas de trabajo desde un punto vista de aplicación práctica incorporando firma digital en procesos de negocio que, por su criticidad, demanden altos requisitos de autenticidad, no repudio e integridad.

3. Introducción

Los procesos de negocios como concepto clásico modelan y ejecutan tareas repetitivas y estructuradas de una organización a fin de producir los productos (o servicios) ofrecidos por la misma. La gestión de procesos de negocio se basa en la idea de que cada producto es el resultado de un conjunto de actividades que se realizan a fin de obtener dicho producto [5]. Por este motivo, la correcta y eficiente gestión de los procesos de negocio es un aspecto importante para la productividad de toda organización, ya que permite identificar las tareas que la misma debe realizar para producir sus productos, el orden de ejecución de las mismas y las personas responsables de realizarlas.
Los BPMS constituyen la herramienta tecnológica para alcanzar este objetivo y que puede enriquecerse incorporando los conceptos de firma digital [4], que garantiza que los datos han llegado al sistema tal como fueron ingresados (integridad), que el usuario que completó la tarea es realmente quien dice ser (autenticidad) y que no pueda evadir responsabilidades sobre la tarea completada (no repudio).
De esta manera no sólo se aplica la firma digital para proteger documentos como mensajes, facturas, transacciones

comerciales, notificaciones, decretos; sino que cualquier tarea completada, desde ingresar datos de una venta hasta aprobar un presupuesto, podría estar digitalmente firmada.

Como ejemplo, consideremos una compañía de seguros que ha incorporado la gestión por procesos. Los productores tratan cada caso de siniestro y los supervisores deberán aprobar ciertas solicitudes creadas por los productores. A su vez, los supervisores pueden derivar ciertos casos a los abogados especialistas y peritos. Estos últimos evaluarán los casos críticos y aprobarán ítems de las solicitudes de cobertura ante el siniestro. Este tipo de proceso tiene distintos niveles de seguridad para cada tarea. Los productores tienen requerimientos de seguridad de **autenticidad** e **integridad**, mientras que para los supervisores podemos agregar el requerimiento de **no repudio**. Si un supervisor dice no haber aprobado una solicitud, puede alegar la posibilidad de un fraude producido por un atacante externo y eludir responsabilidades sobre sus acciones. Similar situación se plantea para las tareas realizadas por los abogados especialistas y peritos.

Los BPMS actuales incluyen sólo un mecanismo de autenticación a través del inicio de sesión web con nombre de usuario y contraseña, que permite garantizar la autenticidad del usuario que inicia sesión. Esto cubre un aspecto muy recortado de los servicios de seguridad enunciados.

3.1- Seguridad en BPMS

La propuesta de incorporar seguridad en BPMSs se aborda desde dos enfoques: 1- Incorporar firma digital en las tareas para autenticidad, no repudio e integridad, 2- definir un proceso específico para la gestión administrativa de claves y certificados asociados.

3.1.1- Firmado de tareas

Hoy en día muchas aplicaciones incorporan las firmas digitales para garantizar autenticidad y no repudio del autor o emisor, e integridad de los datos firmados. Si bien un sistema BPM podría incorporar la funcionalidad de firmar documentos o mensajes, como lo hacen las aplicaciones de correo electrónico o los editores de pdfs, ésto no sería una verdadera integración de firma digital con BPM, sino una integración más con un servicio dentro de un proceso de BPM común y corriente.

La parte central de una integración de firma digital para enriquecer la seguridad de una organización que implementa BPM, es la firma de tareas.

En el caso de la compañía de seguros presentado en la sección anterior, con el uso de una conexión segura a través de HTTPS, el usuario del BPMS puede confiar en la autenticidad del servidor y en la confidencialidad e integridad de los datos que el servidor le hace llegar.

En esta relación de confianza, supongamos que un **supervisor A** está realizando una tarea y el BPMS informa que un determinado **usuario B** ha realizado otra tarea importante previamente. El protocolo HTTPS garantiza que la información no fue modificada durante la trasmisión por la red. Ahora bien: ¿Puede el servidor estar seguro de que el **usuario B** realizó esa tarea?

La posibilidad de **firmar tareas** con una **clave privada** incrementa en forma significativa la seguridad brindada en torno a la **autenticidad y no repudio** del usuario y sus acciones [7].

Una vez que incorporamos un mecanismo de estas características, podemos decir que el servidor tendrá una certeza mucho mayor de la autenticidad del usuario. En ese caso el **supervisor A** puede confiar realmente, porque no sólo sabe que lo que le llega del servidor es certero y auténtico, también confía en que lo que previamente

llegó de otro cliente -el **usuario B**- al servidor era certero y auténtico.
En este sentido se define un subproceso abstracto para cada tarea que requiera firma digital y que denominaremos **Firma de Tarea**, cuyos participantes: el actor que ejecuta la tarea, la aplicación cliente que se ejecuta en el navegador por HTTPS, y el BPMS. Éste último verificará la firma basándose en la clave pública del usuario en cuestión.
Este proceso abstracto es un modelo en BPMN que luego se implementa con funcionalidades específicas del BPMS Bonita BPM [9].

3.1.2 Proceso de gestión de claves

La incorporación de firma digital a cualquier sistema de información conlleva realizar un conjunto de pasos administrativos para la gestión de claves y certificados que puede abordarse como un proceso adicional, no específicamente vinculado al negocio, pero que es compartido por todos los sistemas de información que incluyan firma digital.
Estos nuevos procesos formarán parte del Sistema de Gestión de Seguridad de la Información (SGSI) [3].
Las principales actividades relacionadas con la gestión de claves dentro de una

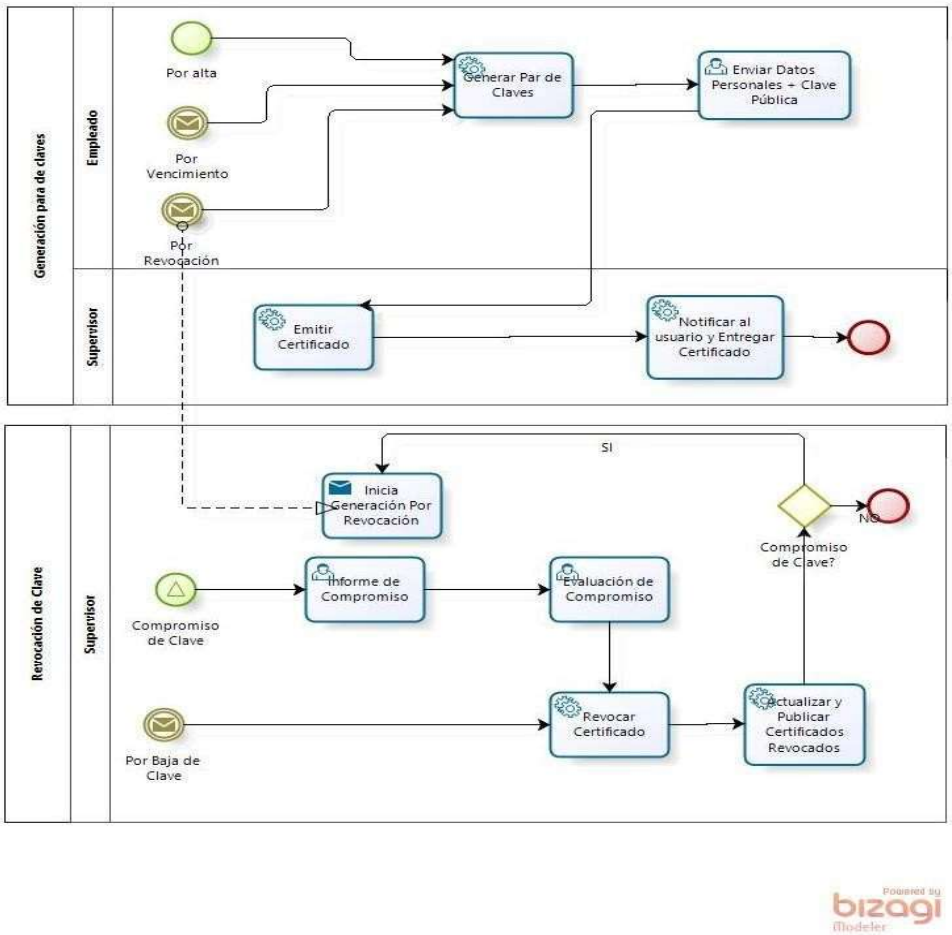

Figura 1 – Procesos de Generación y Revocación de Claves [11]

infraestructura de firma digital son: 1- la generación y distribución de claves, 2- la revocación debido a claves comprometidas o a baja de usuarios. Estas actividades en parte pueden modelarse como un subproceso dentro de un proceso de negocio de Contratación de Personal o bien de Desvinculación del mismo.
Estos subprocesos son **Generación de par de claves** y **Revocación de claves**.
El subproceso de **Generación de par de claves** como se muestra en la Figura 1 tiene tres eventos de inicio posibles: 1- Por alta, se inicia el proceso como un subproceso de Contratación e Integración de Personal, 2- Por expiración, cuando una clave generada previamente alcanza su fecha de vencimiento y es necesario gestionar al usuario un nuevo par de claves y 3- por revocación de la clave de un usuario debido a un compromiso de su clave anterior.
El subproceso de **Revocación de clave** como se muestra en la Figura 1 tiene dos eventos de inicio posibles: 1- compromiso de la clave utilizada y 2- por baja de un empleado. El evento de compromiso se dispara cuando cualquier empleado informa sus sospechas de que su clave o la de otro empleado ha sido comprometida. Luego de evaluar si corresponde revocar la clave, se procede al subproceso de **Generación de par de claves.**

4. Líneas de Investigación, Desarrollo e Innovación

La incorporación de mecanismos para garantizar los atributos de seguridad en la ejecución del proceso de negocio, conlleva a mejorar las soluciones basadas en gestión por procesos, equiparándolas con cualquier sistema de información seguro.

Por otra parte, la gestión de procesos de negocio constituye una buena metodología para instrumentar infraestructuras de gestión de claves públicas y privadas.
Para alcanzar este objetivo, se trazan puntos en común entre las líneas de investigación vinculadas a modelado y desarrollo de sistemas de información basados en procesos de negocio con la línea de seguridad y privacidad en redes, ambas enmarcadas dentro del LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas) de la UNLP.

5. Resultados y Objetivos

El objetivo de este trabajo consiste en realizar una investigación en los campos de BPM y la firma digital, centrada en el análisis de la integración de estas dos tecnologías, con el fin de que la firma digital enriquezca los componentes de BPM y a su vez los conceptos de BPM se puedan aplicar al sistema de gestión de seguridad, en particular al proceso de gestión de claves y su aplicación para la firma digital [8].
Entre los principales resultados obtenidos en la incorporación de firmas digitales en un entorno BPM cabe resaltar el aporte brindado a los BPMS incorporando el uso de firma digital de manera nativa.
Por otra parte, la distribución segura de claves, así como la detección de claves comprometidas y su necesidad de revocación, resultan aspectos críticos para las organizaciones que de hecho se ven reguladas por normas internacionales [3][6] y cuya estructuración por procesos le brinda un mayor formalismo y agilidad en el uso.

6. Formación de Recursos Humanos

BPM y la mejora continua de procesos de

negocio aplicada a los ambientes de ejecución, es una línea de trabajo que ha formado docentes e investigadores en torno a la solución de problemas reales. Por su parte la línea de seguridad y privacidad en redes, particularmente en temas relacionados a criptografía y sus aplicaciones, reúne el interés de docentes y alumnos que se traduce en la realización de varias tesinas, 3 entre el año 2016 y el 2017, la continuidad desde el año 2007 del proyecto PKIGrid UNLP [2], infraestructura de clave pública para e-ciencia y, en consecuencia, la participación de docentes e investigadores del LINTI en la comunidad de TAGPMA[10] en forma activa.

7. Referencias

[1] http://www.linti.unlp.edu.ar/

[2] www.pkigrid.unlp.edu.ar

[3] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Figura 1 - Procesos de Gestión de pares de claves

[4] William Stallings. Cryptography and Network Security Principles and Practices. Prentice Hall. 5th Edition.

[5] Mathias Weske. Business Process Management. Concepts, Languages, Architectures. Springer Berlin Heidelberg New York. 2007

[6] Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S. „RFC 3647: Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework “, November 2003. *Obsoletes RFC2527*.

[7] Jutta Mülle, Silvia von Stackelberg and Klemens Böhm. Modelling and Transforming Security Constraints in Privacy-Aware Business Processes. IEEE International Conference on Service-Oriented Computing and Applications. 2011

[8] Jens Müller and Klemens Böhm. The Architecture of a Secure Business- Process-Management System in Service- Oriented Environments. Ninth IEEE European Conference on Web Services. 2011.

[9] http://es.bonitasoft.com/

[10] http://tagpma.es.net/

[11] http://www.bizagi.com/es