UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Titulo: Seguridad en entornos BPM: integrando firma digital en procesos con altos requerimientos de autenticación e integridad
Autor: Ivan Grcevic
Directoras: Lic. Patricia Bazán - Lic. Paula Venosa
Asesor profesional: Jose Martinez Garro
Carrera: Licenciatura en Sistemas

Resumen

En esta tesina, me propongo integrar conceptos de criptografía y BPM (Business Process Management). La integración que propongo es en ambos sentidos. Por un lado, la seguridad en un entorno de BPM debe verse aumentada gracias a la criptografía. Por otro lado, la administración necesaria para mantener un esquema de seguridad de mecanismos criptográficos, debe verse simplificada al estar orientada a BPM e integrada con otros procesos de una determinada organización.

En particular, los mecanismos de seguridad y criptografía que se utilizan en este trabajo son las conexiones TLS, el protocolo HTTPS, la criptografía de clave pública y la firma digital. Como la administración de un esquema de criptografía de clave pública es compleja, se pretende también que la forma en que se integren con los procesos de BPM sea lo más transparente posible, reduciendo el impacto en la dificultad de uso de los sistemas.

Es de especial interés realizar el trabajo utilizando una herramienta de BPM de código fuente abierto, Bonita BPM, y mantener un equilibrio entre dos aspectos que suelen ser incompatibles: por un lado el nivel de transparencia y simplicidad para el usuario final y por otro lado un alto nivel de agregado de seguridad.

Palabras Claves

Actores, Ataques, Automatización de procesos, BPM, BPMS, Bonita BPM, Business Process Management, Certificado, Ciclo de vida, Clave privada, Clave pública, Criptografía, Diagrama, Distribución de claves, Evento, Firma Digital, Formulario, HTTPS, Integración, Modelos de proceso, Organización, Patrón, Procesos de Negocio, Seguridad, Senda, TLS, Tarea, Variables de Negocio, X.509

Trabajos Realizados

- *Análisis de las posibles alternativas de integración de la firma digital en un entorno de BPM y elaboración de una propuesta de integración.*
- *Implementación de una prueba de concepto en un proceso puntual, utilizando como ejemplo un caso real de una empresa de asistencias médicas para viajeros.*
- *Para el diseño e implementación de estos procesos se utilizó Bonita Studio y se integró a la herramienta código específico creado para la solución de criptografía de esta tesina.*
- *Redacción del informe final, incluyendo un marco teórico de criptografía, firma digital y BPM, una explicación del esquema planteado y el detalle de los procesos y mecanismos criptográficos implementados, las integraciones realizadas y conclusiones obtenidas.*

Conclusiones

En primer lugar, se ha logrado un adecuado nivel de transparencia para el usuario final de la herramienta de BPM a pesar de haber integrado un mecanismos de seguridad como la firma digital. En segundo lugar, la integración de la gestión de claves en los procesos de la organización es una integración mucho más simbiótica que la mera introducción de un mecanismo de firma para completar ciertas tareas. Es decir, BPM se ve enriquecido por los mecanismo criptográficos, y a su vez la gestión de claves para la utilización de dichos mecanismos se implementa orientada a procesos, y como parte de los procesos de la organización. En tercer lugar, esta solución no es una solución genérica: los conceptos planteados deberán ser adaptados a cada organización según su estructura y procesos específicos. En cuarto lugar, tareas que normalmente serían realizadas por fuera de la gestión por procesos -probablemente por administradores de sistemas-, como el alta y baja de usuarios y claves, en este esquema son también implementados como procesos de negocio.

Trabajos Futuros

Estudio de alternativas a la firma digital, que permitan lograr una mejora en los atributos de seguridad de los procesos de negocio. En el marco de la constante evolución de la web y los dispositivos móviles, tecnologías emergentes, distribuidas y basadas en Cloud pueden ser objeto de estudio para tal fin. Por ejemplo, podría analizarse una integración con una aplicación de generación de códigos para autenticación en dos pasos. Estas aplicaciones, como por ejemplo Google Authenticator, permiten a los sistemas integrarse de forma tal que los usuarios pueden utilizarlas para obtener desde su dispositivo móvil un código que cambia cada 60 segundos y sirve como segundo factor de autenticación. Un atacante que quiera realizar acciones en nombre de un usuario, deberá tener acceso a su dispositivo móvil además de averiguar su contraseña.

Fecha de la presentación: OCTUBRE 2018