Grupo CLAI: AUTORIZA7, primera aplicación certificada PA-DSS v3.2 en entornos IBM Power i

Para dar solución a la necesidad de poder contar con aplicaciones seguras sobre sistemas "Mini y Mainframe" (de alto uso en entornos financieros a nivel mundial), el grupo CLAI (Compañía Latinoamericana de Aplicaciones Informáticas) e Internet Security Auditors trabajaron en conjunto para lograr la certificación de la aplicación AUTORIZA7 en la norma PA-DSS v3.2 como la primera aplicación de pago a nivel mundial que corre sobre estos sistemas, en concreto, la plataforma IBM (*) Power i.

Luis Fernando Carmona Granados / David Andrés González Lewis

El Grupo CLAI está formado por un grupo multinacional de empresas con presencia en 8 países, implementaciones en 17 países y es especialista en el desarrollo de plataformas tecnológicas para sistemas de pago en el sector financiero y *retail* para el que crearon un conjunto de soluciones que cubren los procesos transaccionales de extremo a extremo para estos. Entre los productos desarrollados, AUTORIZA7 es un *switch/gateway* de pagos que tiene la capacidad de hacer autorización de transacciones, entre otras funcionalidades (ver esquema de módulos en la **Figura 1**). Esta aplicación fue construida para ejecutarse en sistemas Mainframe de IBM y puntualmente la aplicación se certificó en el sistema operativo IBM i v7.1.

Módulos AUTORIZA7

Figura 1.- Esquema de módulos de la plataforma Autoriza7.

Los sistemas Power, son plataformas que integran el software, hardware, base de datos y seguridad en un único componente altamente escalable que garantiza la no dependencia entre los componentes. El sistema está basado en objetos (archivos, programas, bases de datos, etc.) y en bibliotecas, dando un rendimiento y robustez propicio para sistemas que requieran alto procesamiento como es necesario en el sector financiero y, en general, en todos aquellos donde se emplean este tipo de sistemas.

CLAI, viendo la oportunidad que se necesitaba cubrir en un mercado internacional cada vez más exigente, en el cual las certificaciones de calidad y seguridad son imprescindibles en el sector donde se sitúan sus clientes y donde el cumplimiento de las normas PCI son un sello de garantía ante estos, se planteó llevar a cabo el ambicioso proyecto de alinear AUTORIZA7 a los requerimientos de la norma para Aplicaciones de Pago del PCI SSC, PA-DSS en su última versión (inicialmente la 3.0 y finalmente la 3.2).

Para lograr el cumplimiento, CLAI escogió a **Internet Security Auditors** por su amplia experiencia de más de 10 años de en proyectos de implementación y certificación relacionados con las normas PCI y la única con equipos de consultores QSA y PA-QSA en España y Colombia.

En el proyecto, se realizaron una serie de tareas para que la aplicación cumpliera con los estándares de seguridad exigidos por el PCI SSC. Principalmente se hicieron ajustes al código de la aplicación y configuración de la infraestructura sobre la cual se ejecuta para hacer una alineación con los requerimientos de la norma. Para esto se debió hacer el esfuerzo en identificar el estado de cumplimiento de la aplicación con respecto a la última versión de la norma, con eso poder identificar las tareas necesarias para llegar al tan anhelado cumplimiento.

Los retos

La particularidad del entorno tecnológico de la plataforma donde se despliega AUTORIZA7 iba a hacer bastante complejo ciertos aspectos críticos en el proceso de alineamiento y cumplimiento con PA-DSS v3.2, por lo que se tuvieron que definir estrategias adecuadas en el proceso de implementación de los requerimientos, por supuesto, viables para CLAI y, por ende, para los clientes que deberían desplegar la aplicación.

• **Garantizar el almacenamiento seguro del PAN (*Primary Acount Number*)**: Para simplificar en la medida de lo posible este requerimiento se decidió implementar una solución de 'tokenización' del PAN y hacer uso del *token* en todas las funcionalidades dentro de la aplicación , reduciendo así el esfuerzo de cifrar el PAN en solo una ubicación y no almacenar la información sensible, reduciendo el riesgo (ver **Figura 2**).

• **Garantizar el uso algoritmos de cifrado robustos para proteger los datos almacenados**: Para conseguir este objetivo se aprovechó la tecnología que provee el fabricante de la plataforma con el fin de facilitar compatibilidad, integración, gestión, etc. por lo que se emplearon tarjetas criptográficas propietarias de la plataforma IBM, con las cuales se cifra y se gestiona la administración y protección de las llaves de cifrado. Entre las tarjetas soportadas con las que se realizaron pruebas están los modelos PCIe 5.3, 4.4, 4.2, 4.1 y PCI-X 3.30, 3.25, 3.23, 3.20 y 2.54 con todas ellas se obtuvieron resultados óptimos.

• **Disponer de la información de auditoría necesaria en la aplicación**: se implementó la generación de eventos de auditoría en la aplicación para poder registrar cualquier tipo de actividad que pudiera detectar, identificar y apoyar en la contención de un incidente. Para lo que se complementaron los registros del JOURNAL (herramienta del sistema que es capaz de registrar todo evento relacionado con la seguridad a un nivel de detalle muy completo) con los eventos administrativos de auditoría propios de la aplicación.

(*) http://blog.isecauditors.com/2016/12/breve-analisis-de-9-tecnicas-para-minimizacion-del-fraude-en-transacciones-comercio-electronico.html

• **Cumplimiento con los estándares de desarrollo seguro de software**: Sin duda este fue uno de los aspectos más relevantes en una aplicación con años en sus espaldas, equipos de desarrollo en diferentes países y una exigencia importante relacionada con la calidad y seguridad de la aplicación. El objetivo de este requerimiento implicaba desde la formación a los equipos de desarrollo (quizás la labor más fácil del proceso), hasta integrar e implementar de forma íntegra en la aplicación estas buenas prácticas alineadas con metodologías de seguridad. Lógicamente, OWASP y sus proyectos de codificación segura son el lugar de referencia para definir la implementación de controles de seguridad en todas las fases del ciclo de vida de desarrollo de software.

• **Realizar todas las revisiones técnicas sobre la aplicación y su codificación**: validando procesos con Análisis de Riesgos, llevando a cabo revisiones de código fuente en busca de vulnerabilidades y realizando pruebas de penetración para garantizar una construcción del software alineado con los requerimientos anteriormente definidos, la rigurosidad de estas pruebas se puede evidenciar con el hecho de que en el desarrollo de estas pruebas se pudieron detectar vulnerabilidades de día cero en la plataforma.

• **Definición e implementación de procesos de Gestión de Cambios**: También se definió e implementó un estricto control de cambios para identificar todos los posibles impactos sobre la aplicación que vayan a desviar el cumplimiento logrado.

• **Facilitar y simplificar el cumplimiento de PCI DSS**: Por definición, una aplicación certificada bajo PA-DSS garantiza que ésta cumple con los requerimientos de PCI DSS cuando se despliega y utiliza en ese entorno. Es más, precisamente la certificación facilitará y ayudará en la consecución del objetivo de cumplimiento de PCI DSS a los clientes de AUTORIZA7, gracias a la "eliminación" de la validación sobre si esa aplicación cumple con los requerimientos de la norma dentro del ambiente. Para alcanzar este objetivo, se definieron guías de aseguramiento del Sistema Operativo, definición de puertos y protocolos seguros, segmentación de plataformas críticas y pruebas al alcance donde comúnmente corre la aplicación, entre otros. Toda esta información detallada y precisa fue incluida en la Guía de Implementación, documento clave para un despliegue adecuado de la aplicación certificada.

Entre los controles en los que se apoya la aplicación para obtener el objetivo conjuntamente se encuentran:

• Autenticación ofrecida por el IBM iSeries con gestión de contraseñas y de usuarios robusta.

• Cifrado mediante las tarjetas criptográficas.

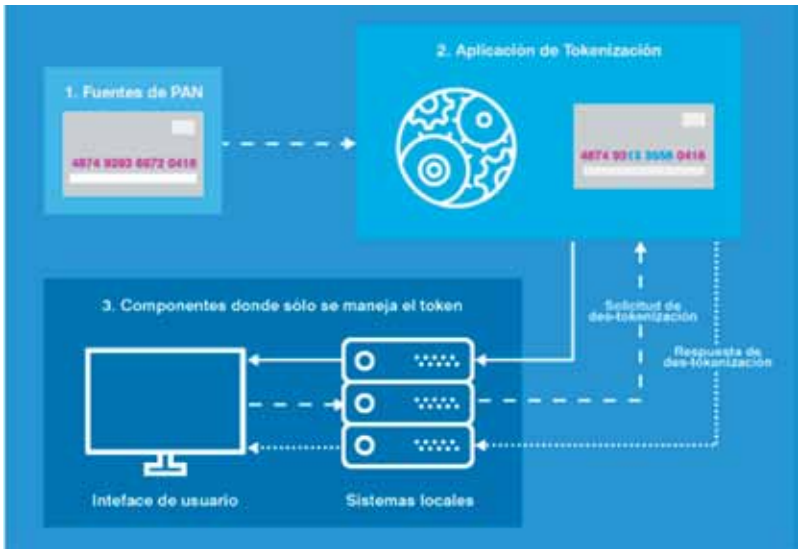

Figura 2.- Esquema clásico de 'tokenización'.

• Niveles de Seguridad (QSECURITY) ofrecidos por el sistema.

• Auditoria de eventos mediante el JOURNAL.

• Uso y soporte de servicios, protocolos y puertos seguros.

Conclusiones y beneficios

La fortaleza de disponer una aplicación certificada en PA-DSS garantiza el tratamiento de los datos de tarjetahabientes de forma robusta en entornos donde la seguridad es un factor crítico; adicionalmente, la construcción de aplicaciones seguras en plataformas tan robustas como las de IBM Power i, hace que la aplicación sea altamente escalable y confiable para la misión crítica del procesamiento transaccional dando un conjunto de garantías pocas veces visto para los usuarios de la aplicación certificada.

El principal beneficio de lograr la certificación PA-DSS apunta a que las entidades que adquieren y usan AUTORIZA7 en sus tareas de procesamiento, transmisión y almacenamiento de los datos de tarjetahabientes, tienen la garantía que se han implementado procesos robustos desde la concepción de la aplicación hasta su puesta en marcha y mantenimiento.

Asimismo, se han dejado implementadas políticas, procesos y procedimientos que aseguran el mantenimiento de la certificación PA-DSS que la misma norma obliga, para mantener la aplicación bajo unos estándares de seguridad permanentes ofreciendo esa garantía de forma continuada a clientes, socios y cualquier parte interesada como una aplicación altamente confiable.

Como comentario final y para enfatizar el mérito de este hito conseguido, se debe resaltar el hecho de que, en el momento de escribir este artículo, de las 785 aplicaciones listadas en el sitio web del PCI SSC válidas para nuevos despliegues a nivel mundial sólo hay 83 del tipo Payment Gateway/Switch, es decir, del mismo tipo que AUTORIZA7 y, entre éstas, únicamente la de CLAI está certificada en la plataforma Power i de IBM. Hecho que refuerza el valor de la certificación y del esfuerzo realizado por CLAI, en el que Internet Security Auditors ha colaborado estrechamente como asesor especializado en las Normas PCI. ■

CLAI, viendo la oportunidad que se necesitaba cubrir en un mercado internacional cada vez más exigente, en el cual las certificaciones de calidad y seguridad son imprescindibles en el sector donde se sitúan sus clientes y donde el cumplimiento de las normas PCI son un sello de garantía ante estos, se planteó llevar a cabo el ambicioso proyecto de alinear Autoriza7 a los requerimientos de la norma para Aplicaciones de Pago del PCI SSC, PA-DSS en su última versión.

Luis Fernando Carmona Granados
CEO
GRUPO CLAI
(Compañía Latinoamericana de Aplicaciones Informáticas)

David Andrés González Lewis
CISM, CSSLP, QSA, PA-QSA, PCIP, ISO 27001 IA
Consultor de Seguridad de la Información
INTERNET SECURITY AUDITORS