Apéndice.

Comparación entre MPKI y AppScan DE.

Manager PKI (Public Key Infrastructure).

La seguridad y la confianza son partes integrales de los negocios hoy en día. Hoy más que nunca, los negocios deben proteger sus recursos de ataque así como la implementación en medidas de seguridad en procesos administrativos, de personal, clientes y socios de negocios.

El managed PKI engloba los valores de:

- Autenticación.
- Autorización.
- Confidencialidad.
- Integridad.
- Irrefutabilidad.

El managed PKI es un servicio administrado, por lo tanto se puede implementar una solución PKI de una forma rápida, para englobar los componentes importantes de confianza. Actualmente el managed PKI da servicio a millones de negocios y usuarios a nivel internacional **[VeriSign, 2004].**

.

El managed PKI asegura sus:

- Aplicaciones.
- Comunicaciones.
- Transacciones.

De esta manera, asegurando estos tres conceptos, logra una infraestructura confiable entre uno y el mundo.

¿En dónde empieza la confianza?

La confianza empieza con la Autoridad Certificadora (CA) durante una implementación Managed PKI. La CA establece políticas de confianza y controla los certificados digitales, los cuales únicamente se entregarán autenticados y verificados.

Debido a que la CA, cumple con los parámetros de verificación y autenticación, todos los certificados emitidos por ésta son confiables, el Managed PKI permite comunicaciones y transacciones seguras entre uno y personas confiables, usando métodos de criptografía probados **[VeriSign, 2004]**.

.

La empresa que hospeda y administra los CA´s es VeriSign, empresa reconocida mundialmente; esta se basa en su experiencia e infraestructura de seguridad, bajo los estándares más estrictos:

- Centro de datos de alta disponibilidad.
- Escalables a millones de usuarios.
- Servicio al Cliente las 24 horas del día.
- Infraestructura de alta seguridad.
- Controles internos auditables.
- Cuenta con los mejores expertos de seguridad en la industria.

Todos estos respaldados por los mejores Acuerdos de Servicio en la Industria, para que uno desarrollé sus requerimientos legales y de seguridad.

Dependiendo de las políticas de confianza de la empresa, VeriSign hospedará CA´s privadas o públicas. Las privadas permiten que el usuario personalice sus propias políticas confianza, mientras que las públicas se convierten, de forma inmediata, en parte de la Red de Confianza de Verisign (VTN).

Cuando un usuario pertenece a la Red de Confianza de Verisign, inmediatamente puede acceder a millones de usuarios confiables, sin tener que establecer su propia comunidad de confianza.

El servicio de Managed PKI permite que el usuario obtenga certificados digitales firmados por una Autoridad Autenticadota hospedada por Verisign, aprovechando las capacidades de infraestructura, confianza y seguridad que brinda esta, para que el usuario pueda enfocarse solamente a su negocio.

A continuación veremos como funciona el Managed PKI:

Por ejemplo si un nuevo usuario intenta acceder a una aplicación segura en un servidor empresarial, su acceso será denegado si éste no cuenta con el certificado digital correspondiente. Para que pueda acceder al servidor seguro, el usuario será diseccionado a un servidor de inscripción para obtener su certificado digital, que será hospedado en Verisign o en la empresa **[VeriSign, 2004]**.

Cuando el usuario navega en la página de inscripción, llena un formato personalizado para solicitar su certificado digital, y lo manda al servidor de inscripción. La petición de certificado será guardada para una aprobación manual, o se mandará a un servidor de autenticación, el cual la aprueba o la rechaza en base a la información personal proporcionada en la inscripción. Si se aprueba la petición Verisign genera un certificado firmado digitalmente por una Autoridad Certificadora, y es mandado directamente al usuario. El acceso a la aplicación segura es concedido en base al nuevo certificado digital del usuario y a la llave privada correspondiente, y el usuario podrá acceder a la aplicación segura por el tiempo en que el certificado digital sea válido.

El servicio administrado Managed PKI puede soportar las aplicaciones de seguridad más fuertes del mercado, tales como:

- Banca Electrónica.
- Comercio Electrónico.
- Administración de Proveedores.
- Servicios Médicos.
- Gobierno.

AppScan DE.

AppScan DE brinde una solución para automatizar los análisis de vulnerabilidades y pruebas de penetración de sus aplicaciones y plataformas Web. Elimina los exámenes manuales que eran necesarios antes de implementar una aplicación, genera reportes que determinan la mejor manera de cumplir con estas auditorías para asegurar sus aplicaciones, antes de su implementación.

AppScan DE es una poderosa herramienta de pruebas que permite el rápido desarrollo de la seguridad. Esta herramienta ayuda a hacer que la lógica de la aplicación sea resistente a ataques sin tocar su presentación o eficacia. **AppScan DE** detecta los defectos de la seguridad automáticamente; como un componente integrado al desarrollo de la empresa, esta herramienta, automatiza las pruebas de creación de escritura, modificación y proceso de mantenimiento, asegurando confiabilidad y pruebas que son repetibles **[Sanctum, 2004].**

AppScan DE es una herramienta que ayuda a las empresas a reducir costos y a crear aplicaciones confiables y resistentes contra hackers, en el ambiente de desarrollo. **AppScan DE** crea "Vulnerabilidades Potenciales" que son los defectos potenciales de la seguridad en el código y entonces los prueba para verificar que ellos existen. **AppScan DE** reporta los errores o defectos de la aplicación, luego se los proporciona al usuario para empezar a arreglar estos errores.

Después de estas breves descripciones de estos dos sistemas, podemos decir que las dos son muy buenas opciones para asegurar las Aplicaciones Web del CENTIA. Sin embargo, considero que **AppScan DE** es una opción mejor que el Managed PKI porque se enfoca más a descubrir cuáles son las vulnerabilidades potenciales que tienen las Aplicaciones Web, y es ahí, donde los hackers pueden atacar el sistema. Como observamos, Manager PKI asegura las Aplicaciones creando certificados digitales, pero no sabe cuales son las vulnerabilidades del sistema; si un hacker encuentra estas vulnerabilidades puede ser un gran problema para la empresa, o bien, si emplea cualquier técnica de hackers avanzadas para penetrar al sitio, rompiendo el esquema del certificado digital, sería un caos total **[Sanctum, 2004].**