



ESTUDIO DE CASOS

Deutsche Post World Net

VeriSign protege a Deutsche Post World Net

La solución resumida

Sector
Correos

Reto
Protección óptima del intercambio de datos de los clientes de Deutsche Post World Net mediante certificados de servidor SSL.

Solución
VeriSign pone a disposición de Deutsche Post World Net una solución rápida, eficiente y flexible para la solicitud y administración de certificados de servidor SSL, originando de esta manera procesos comerciales más directos y una mayor seguridad en la transmisión de datos sensibles.

Resultados

- Gracias a VeriSign, la emisión e instalación de certificados de servidor SSL requiere sólo unas pocas horas y no, como antes, tres días

El correo constituye una de las herramientas principales de la comunicación interpersonal. Las personas pueden ponerse mutuamente en contacto e intercambiar mensajes y compartir acontecimientos, desarrollos y sus sentimientos más personales. Sin embargo, ya desde el momento de su invención se puso en duda que la información transmitida por correo permaneciese verdaderamente confidencial hasta llegar a su destinatario.

Demos ahora un salto a la era de la información electrónica: Aunque las herramientas de comunicación han experimentado una evolución dramática, las dudas siguen siendo las mismas. ¿Cómo podemos estar seguros de que la información privada que transmitimos cada día por vía electrónica es tratada confidencialmente hasta haber alcanzado su lugar de destino?

El Grupo Deutsche Post World Net ha asumido plenamente este reto. Desde los comienzos de la empresa en 1490, año en el que Franz von Taxis fundó la primera compañía de correos moderna de Europa, la confidencialidad de la correspondencia ha sido siempre elemental para Deutsche Post. La empresa transporta hoy en día más de 70 millones de envíos postales diarios observando las normas de seguridad más elevadas. Y lo que es aplicable a una carta es también aplicable en Deutsche Post World Net a los datos electrónicos. Por esta razón, Deutsche Post World Net emplea el procedimiento de encriptación Secure Socket Layer (SSL) para la protección de la información comercial interna y de los datos de su clientela.

Martin Hagen, el Asesor de Sistema responsable de los certificados SSL se encarga de mantener todos los certificados de servidor SSL para Deutsche Post, DHL y Postbank. Incontables aplicaciones en dichas divisiones requieren certificados de servidor SSL, entre ellas figuran, por ejemplo, FRANKIT, STAMPIT, EBTRANSFER,



Where it all comes together.™



- Reducción de la carga de trabajo de los administradores de sistema y departamentos especializados mediante la eliminación de etapas de proceso redundantes
- Protección de los certificados de VeriSign mediante un programa especial contra daños económicos para Deutsche Post World Net

los sistemas Trac and Trace, epost y el servicio bancario en línea, así como las aplicaciones para los servicios y las ofertas anunciadas a través de las páginas web del grupo empresarial.

El socio de Martin Hagen en la puesta a punto de certificados de servidor SSL es VeriSign, un proveedor líder de servicios para infraestructuras de TI sensibles que las hacen más inteligentes, fiables y seguras.

+ La importancia de la seguridad de datos crece continuamente

“Los datos que antes se archivaban sobre papel en archivadores o carpetas son transmitidos hoy en día por vía electrónica. En algunas empresas, más del 90 de ciento de la totalidad de la información e transportada sólo electrónicamente, lo cual provoca, por supuesto, un notable aumento de los requisitos de seguridad”, explica Martin Hagen. “Una empresa que transmite semejante volumen de información confidencial como Deutsche Post World Net ha de estar siempre al día en la implementación de los mecanismos de protección de datos más recientes.”

Deutsche Post World Net ha incrementado drásticamente sus estructuras de seguridad en los últimos tres años, adoptando, por ejemplo, las más sofisticadas tecnologías de cortafuegos. Los certificados de servidor SSL constituyen uno de los elementos clave en la estrategia de seguridad, en particular en el área de la comunicación en línea.

+ Relación de mutua confianza

La cooperación entre Deutsche Post World Net y VeriSign comenzó en el 2003. Deutsche Post World Net deseaba cambiar de su anterior proveedor de certificados SSL a VeriSign, optando por la introducción de VeriSign® Managed Public Key Infrastructure for SSL (MPKI for SSL) como solución para el conjunto de la empresa. Para Martin Hagen se abrieron así vías completamente nuevas para aumentar los grados de seguridad y mejorar la automatización de los procesos de seguridad. Sobre todo resultaba posible llevar a cabo con una mayor eficiencia de gastos muchas de las medidas administrativas ejecutadas anteriormente a mano.

“En el procedimiento empleado previamente se necesitaban dos o tres días para la puesta a punto de un certificado. Además, teníamos que mantener entre 20 y 30 cuentas de administrador a fin de poder establecer entornos seguros para los diferentes departamentos”, recuerda Hagen.

“El cambio a VeriSign nos ha permitido mejorar considerablemente nuestros servicios. VeriSign es simplemente flexible. Los certificados están disponibles en unas pocas horas y el proceso entero es más eficiente y transparente. Lo único que hace falta para la puesta a disposición en línea del certificado es enviar un enlace al departamento correspondiente. En caso de una nueva solicitud de certificado se verifica el presente certificado en línea y ya está. VeriSign ha reducido así de modo perceptible los trabajos innecesarios.”

Hagen está convencido de que la solución de VeriSign reduce asimismo la cantidad de aplicaciones a administrar por los diferentes departamentos, ya que VeriSign MPKI for SSL permite un manejo intuitivo de las herramientas de certificación. Hagen pone como ejemplo la presentación Power Point de unas 20 páginas con las instrucciones para el pedido de certificados que se requería en el sistema anterior. Una presentación absolutamente superflua tras la introducción de la solución de VeriSign.



SUCCESS STORY

“VeriSign ha demostrado ser un socio extremadamente fiable para Deutsche Post World Net. VeriSign es flexible y entiende las necesidades de los clientes. La empresa atiende a nuestros deseos y nos proporciona la asistencia necesaria para la ejecución de nuestras tareas.”

Martin Hagen
Asesor de Sistema,
Deutsche Post AG,
SNL IT Infrastructure -
Infrastructure Management
Shared Services

Pero VeriSign también se diferencia positivamente de otras soluciones en las modalidades de pago: Con VeriSign MPKI for SSL, Deutsche Post World Net ya no tiene que abonar cada certificado a través de una operación contable propia, pudiendo liquidar ahora trimestralmente todos los certificados empleados, lo cual representa para Martin Hagen otra práctica reducción de cargas administrativas. Hagen sabe apreciar además el servicio de garantía ofrecido por VeriSign. Éste es actualmente el único proveedor que ofrece junto con los certificados un programa de protección contra daños económicos. El proceso completo de autorización de los certificados es vigilado por los auditores de KPMG.

Hagen resume: “VeriSign ha demostrado ser un socio extremadamente fiable para Deutsche Post World Net. VeriSign es flexible y entiende las necesidades de sus clientes. La empresa atiende nuestros deseos y nos proporciona la asistencia necesaria para la ejecución de nuestras tareas.”

Visítenos en www.verisign.es