



SUCCESS STORY

Deutsche Post World Net

VeriSign sécurise la Deutsche Post World Net

Aperçu de la solution

Branche
Poste

Enjeu

Sécurisation optimale de l'échange de données des clients auprès de la Deutsche Post World Net par certificats de serveur SSL.

Solution

VeriSign a mis à la disposition de la Deutsche Post World Net une solution rapide, efficace et flexible pour la commande et l'administration de certificats de serveurs SSL, assurant ainsi la rationalisation des processus d'affaires et une sécurité plus élevée dans la transmission de données sensibles.

Résultats

- La certification et l'installation des certificats SSL s'effectue grâce à VeriSign en quelques heures au lieu de trois jours jusqu'ici

La poste est l'un des principaux outils de la communication entre les humains. Les gens peuvent entrer mutuellement en contact et échanger réciproquement des nouvelles, des événements, des développements et leurs sentiments très personnels. Dès le premier jour, il y a toutefois eu des doutes si toutes les informations confiées à la poste restent véritablement privées et confidentielles jusqu'à ce qu'elles arrivent à leur destinataire.

Faisons un bond dans l'ère des informations électroniques : bien que les outils de communication aient fait l'objet d'une évolution dramatique, les doutes sont restés les mêmes. Comment pouvons-nous être sûrs que les informations privées que nous expédions électroniquement seront traitées comme confidentielles jusqu'à ce qu'elles arrivent à destination?

Le groupe Deutsche Post World Net a relevé ce défi. Depuis les racines de l'entreprise en l'an 1490, lorsque Franz von Taxis a fondé la première poste moderne en Europe, la confidentialité des nouvelles a sans cesse occupé le centre de la poste allemande. Aujourd'hui, bien plus de 70 millions d'envois postaux sont transportés chaque jour par l'entreprise — en respectant les plus hauts standards de sécurité. Et pour la Deutsche Post World Net, ce qui est valable pour une vraie lettre l'est également pour les données électroniques. C'est pourquoi la Deutsche Post World Net fait intervenir le procédé d'encodage Secure Socket Layer (SSL), tant pour la protection des données d'affaires internes que pour les données de ses clients.

Martin Hagen, conseiller de système responsable des certificats SSL, veille sur tous les certificats SSL de serveurs auprès de la Deutsche Post, de la DHL et de la Postbank. Dans ces divisions de l'entreprise, d'innombrables applications ont besoin de certificats



Where it all comes together.™

- Réduction de la charge de travail des administrateurs de système et des services spécialisés grâce à la suppression d'opérations de processus superflues
- Programme de protection protégeant la Deutsche Post World Net d'un éventuel dommage financier causé par les produits VeriSign

SSL de serveurs. Parmi ces dernières comptent par exemple FRANKIT, STAMPIT, WEBTRANSFER, les systèmes Trac-and-Trace, e-post, les opérations bancaires en ligne ainsi que les applications pour les prestations de service et les offres qui sont proposées par l'intermédiaires des sites Internet du groupe.

Le partenaire de Martin Hagen pour la fourniture de certificats SSL de serveurs est VeriSign, un leader de la fourniture de services pour les infrastructures IT commerciales critiques, avec lesquelles l'Internet et les réseaux de télécommunication deviennent plus intelligents, plus fiables et plus sûrs.

+ La sécurité des données—d'une importance croissante

« Les données qui étaient autrefois archivées sur papier dans des classeurs ou des dossiers sont aujourd'hui transmises électroniquement. Dans certaines entreprises, ce sont plus de 90% de toutes les informations qui ne sont plus transportées qu'électroniquement. Il en résulte naturellement des exigences beaucoup plus grandes en matière de sécurité, » explique Martin Hagen. « Une entreprise qui transporte autant d'informations confidentielles que la Deutsche Post World Net se doit d'avoir toujours un pas d'avance dans la mise en place des mécanismes de protection des données les plus récents au monde. »

Au cours des trois dernières années, la Deutsche Post World Net a drastiquement renforcé les structures de sécurité. Parmi les mesures prises, on compte par exemple la mise en place des technologies antivirus les plus modernes. Au sein de la stratégie de sécurité, les certificats SSL de serveurs constituent un élément clé, notamment pour la communication en ligne.

+ Base de confiance dans le partenariat

Le partenariat entre la Deutsche Post World Net et VeriSign a commencé en 2003. La Deutsche Post World Net voulait changer de son ancien fournisseur de certificats SSL pour rejoindre VeriSign et s'est décidée pour la mise en œuvre de la Managed Public Key Infrastructure pour SSL (MPKI pour SSL) de VeriSign comme solution d'entreprise. Pour Martin Hagen se sont ouvertes à-partir de là des voies entièrement nouvelles pour relever les niveaux de sécurité et pour améliorer l'automatisation des processus de sécurité. Avant tout, de nombreuses mesures administratives jusqu'ici effectuées manuellement ont pu être aménagées de façon à en réduire les coûts.

« Avec le procédé utilisé jusqu'alors, il fallait de deux à trois jours avant qu'un certificat ne puisse être mis à disposition. De plus, nous étions obligés de gérer entre 20 et 30 comptes d'administrateurs pour être à même d'aménager un environnement sûr aux différents services » explique Hagen.

« En optant pour VeriSign, nous avons pu nettement améliorer nos services. VeriSign est tout simplement flexible. Les certificats sont disponibles en l'espace de quelques heures seulement et l'ensemble du processus est plus efficace et plus transparent. Il me suffit d'envoyer un lien au service concerné pour effectuer la disposition en ligne du certificat, c'est d'envoyer un lien au service respectif. Lors d'une nouvelle demande de certificat, la demande existante est contrôlée en ligne, et l'affaire est réglée. VeriSign a ainsi réduit de manière considérable des tâches inutiles. »

Hagen est convaincu que la solution de VeriSign réduit également le nombre des applications qui doivent être gérées par les différents services. En effet, MPKI pour SSL permet une utilisation intuitive des outils de certification. Pour illustrer cette expérience, Hagen renvoie à une présentation PowerPoint d'environ 20 pages avec le



« VeriSign s'est révélé être un partenaire extrêmement fiable pour la Deutsche Post World Net. VeriSign fait preuve de flexibilité et de compréhension pour les problèmes des clients. L'entreprise réagit à nos besoins et nous fournit le support nécessaire pour les missions qui sont les nôtres. »

Martin Hagen
Conseiller de système,
Deutsche Post AG
Infrastructure IT SNL
Gestion de l'infrastructure
Shared Services

mode d'emploi pour la commande d'un certificat avec l'ancien système. Depuis la mise en place de la solution VeriSign, c'est devenu superflu. Mais VeriSign se distingue également dans les modalités de paiement également d'une manière positive des autres solutions. Ainsi, avec MPKI pour SSL, la Deutsche Post World Net n'est plus obligée de payer individuellement chaque certificat avec une opération de facturation séparée, mais tous les certificats utilisés peuvent être facturés trimestriellement. Cela permet à Martin Hagen de réduire encore plus et de manière rationnelle ses tâches administratives. En outre, Hagen sait apprécier le service de garantie de VeriSign. VeriSign est le seul fournisseur qui entretient pour ses certificats un programme de protection contre les dommages financiers. L'ensemble du processus d'autorisation pour les certificats est contrôlé par des experts comptables de KPMG.

Hagen résume : « VeriSign s'est révélé être un partenaire extrêmement fiable pour la Deutsche Post World Net. VeriSign fait preuve de flexibilité et de compréhension pour les problèmes des clients. L'entreprise réagit à nos besoins et nous fournit le support nécessaire pour les missions qui sont les nôtres. »

Rendez-nous visite sur le site www.verisign.fr.