



## SUCCESS STORY

# Deutsche Post World Net

## Securing the Critical Web Services of an International Postal Service

### SOLUTION SUMMARY

#### Industry

Postal services

#### Challenge

Secure critical data transmitted electronically both to and from Deutsche Post World Net.

#### Solution

VeriSign® MPKI for SSL

#### Results

- SSL certificate authentication and installation was reduced from a timeframe of up to three days to a matter of hours
- VeriSign's solution significantly reduced certificate workload both for the administrator and within the individual departments

Ever since the fifteenth century, when the basis of Europe's modern postal system was formed, information security has been a primary focus of the Deutsche Post World Net concern. Today, the 70 million postal items the company delivers every day are handled with the utmost concern for security. Similarly, Deutsche Post World Net applies the highest security standards to the protection of electronic data. The Deutsche Post World Net concern embraces not only the Deutsche Post brand, but also the DHL and Postbank brands, and includes a comprehensive array of Web sites and services.

Deutsche Post World Net uses Secure Socket Layer (SSL) encryption to protect both its own critical business data and the data of its customers. Martin Hagen, the system consultant responsible for SSL certificates, decided in 2003 to switch to VeriSign as the provider of SSL protection. The switch overcame many of the problems that Deutsche Post World Net had experienced with SSL certification. Previously Deutsche Post World Net was waiting up to three days before an ordered certificate would be made available for use. In addition, the concern needed to maintain approximately 30 different accounts in order to provide services to its many departments, which was a significant administrative burden. Both problems were solved with VeriSign.

#### + First-Class Security

Throughout the last three years, Deutsche Post World Net has dramatically upgraded its security for data transmission, and SSL server certificates are a key part of that strategy. In addition to securing the company's many Web sites, SSL certificates secure myriad Web-based applications, including FRANKIT, STAMPIT, WEBTRANSFER, track and trace systems, epost, and even several online banking services.



Where it all comes together.™



## SUCCESS STORY

- VeriSign certificates are backed by a warranty program that protects Deutsche Post World Net against the unlikely event of error caused by VeriSign products
- Greater payment flexibility: Deutsche Post World Net's payment schedule switched from per-certificate basis to a quarterly account

*"VeriSign has shown itself to be a highly reliable partner for Deutsche Post World Net. VeriSign continually proves its value through its flexibility, its willingness to listen to and react to our needs, and through the quality of its support."*

Martin Hagen  
System Consultant,  
Deutsche Post World Net

To address the company's diverse security needs, Deutsche Post World Net adopted The VeriSign® Managed Public Key Infrastructure for SSL (MPKI for SSL) enterprise solution. According to Hagen, this solution improved the overall service, introduced a higher level of efficiency and automation into the process, and eliminated many of the small, but onerous administration tasks that burdened his daily workload. "The change to VeriSign offered us the chance to improve the service," said Hagen. "VeriSign is much more flexible than our previous provider. Certificates are available within hours and the entire process is more efficient and transparent. All I need to do is to send a link to the relevant department for an online enrollment. After receiving a certificate request, I approve it—then the matter is finished. It has greatly reduced my supervisory role."

Hagen says that VeriSign's solution has also reduced the application workload of the individual departments through the creation of a more intuitive process. Hagen once produced a PowerPoint® presentation that described some 20 steps required to obtain a certificate using the previous system. When Deutsche Post World Net implemented VeriSign MPKI for SSL, the process was so greatly simplified that no such description was necessary.

VeriSign MPKI for SSL also offers Deutsche Post World Net greater flexibility in processing payments. With the new solution, Deutsche Post World Net has changed its payment schedule from a per-certificate basis to a quarterly account, further reducing Hagen's administrative workload. Hagen also appreciates the warranty offered by the VeriSign solution. VeriSign is the only provider that backs its certificates with a program protecting against financial damage, and it submits its certificate authorization process to assessment by the chartered accountants KPMG.

In summary, Hagen says, "VeriSign has shown itself to be a highly reliable partner for Deutsche Post World Net. VeriSign continually proves its value through its flexibility, its willingness to listen to and react to our needs, and through the quality of its support."

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**