



CASE STUDY

Secure Data Exchange

Strong encryption creates consumer trust and protects critical company information in transit, over the Internet

“The attractive price point of SSL Certificates isn’t the only reason why O₂ uses VeriSign’s MPKI for SSL. Efficient management of SSL across server sites and server types, and increased visibility for administrators are hugely decisive factors.”

Daniel Stricharz, Security Specialist,
O₂ GmbH & Co. OHG



VeriSign Managed PKI for SSL

VeriSign Managed PKI for SSL (MPKI for SSL) offers a fast, efficient, and cost-effective way to order and administer SSL Server Certificates.

+ Overview

O₂ Germany, a subsidiary of Telefónica O₂ Europe and a member of the Spanish telecommunications group, Telefónica S.A., offer their customers virtually country-wide GSM coverage in Germany through their own cellular network and their Roaming Agreement with T-Mobile. At the forefront of innovation, they are developing further mobile data services, based on GPRS and UMTS technology. Within O₂ Germany alone, 4,700 employees ensure the peace of mind of more than 10 million mobile phone customers.

+ User-friendly Online Services

The online portal operated by O₂ Germany, o2online.de, serves as a comprehensive platform for O₂'s customers. It contains essential information related to mobile communication and mobile phone use, advantageous offers, and other attractive services. On this portal, customers can manage their contract data, view their invoices, and send e-mail and SMS text messages, as well as access the new O₂ Music Shop which has a huge selection of songs and other services.

Many O₂ customers take online services for granted. Since the applications are so user-friendly and intuitive, most users have no visibility or understanding of the complexity that lies behind them. O₂ strive to ensure their online services are available to users at all times, while continually improving them through innovation.

+ Security is a Complex Topic

For O₂, security is a top priority. This applies not only to O₂'s mobile telephone offers, but also to the entire array of services offered through their online portal. Customers access sensitive personal information, which beyond being important to protect, also means that O₂ have legal obligations to meet. Under the German Telecommunications and Data Protection Act, telecommunication providers are required to provide adequate protection for customer data through appropriate technical and administrative



measures. To help safeguard customers' sensitive data during communication over the Internet, O₂ rely on Secure Sockets Layer (SSL) Certificates from VeriSign. As the leading SSL Certification Authority (CA), VeriSign offers o2online-portal users the strongest encryption available to them. The certificates enable encryption between client browser and Web server, and thereby protect the data exchange between customers and the portal. O₂'s head of security for their online portal, Daniel Stricharz, explains their use of VeriSign SSL Certificates, "our customers expect their data to be comprehensively protected, and therefore SSL encryption is extremely important."

O₂ take security very seriously, and extend their use of SSL Certificates not only to their consumer portal, but also into other areas. Their certificates also encrypt email data when customers access their email through Outlook at O₂. They also maintain a continuous Internet connection with sales partners, such as Tchibo. Here, too, SSL Certificates are used to safeguard data transmission. In addition, O₂ use SSL Certificates for internal purposes – e.g. for encryption during transfer of confidential business and customer data between the central administrative office and O₂ shops or shops of business partners.

+ VeriSign – A Trustworthy Partner

"We rely on VeriSign and their depth of knowledge in the Internet, communication, and security space", Stricharz notes when describing their partnership with VeriSign. VeriSign's authentication and verification procedures are based on years of practical experience, and now with Extended Validation Certificates established by the CA/Browser forum – VeriSign is at the forefront of the next generation of SSL. More than a half-million companies, including 40 of the largest banks in the world and 93% of Fortune 500 companies, put their trust in VeriSign's authentication procedures. With its SSL Certificates, VeriSign offers its customers reliable protection during data transmission over the Internet, as well as increased protection against online crime, such as identity theft and phishing.

+ SSL Helps Assure Maximum Security

The SSL Certificates used at O₂ combine powerful authentication with strong encryption technology benefiting the service provider in three basic ways:

VeriSign relies on extensive procedures to authenticate the identity of a business and the legitimacy of a customer before an SSL Certificate is issued. As in the past, the three-tier authentication procedure remains the standard for secure, appropriate authentication of a company's identity. All major browsers automatically accept SSL Certificates issued by VeriSign as a Certification Authority (CA). With these certificates, O₂ can assure their customers that their data is transmitted in a secure manner and is kept safe from perpetrators of fraud.

Secondly, VeriSign offers modern encryption techniques that prevent unauthorised people from capturing and viewing confidential data. VeriSign uses Server-Gated Cryptography (SGC) technology so that it can offer strong 128-bit SSL encryption to the greatest possible number of users. Without an SGC-enabled Certificate, visitors using certain older browsers and many using older Windows 2000 operating systems



are limited to 40- or 56-bit encryption when visiting Internet sites.

Finally, VeriSign safeguards message integrity. In Internet communications between client browser and server, SSL protects message content from alteration by third parties. Customers can be sure that O₂ will receive the exact data they have entered.

+ Efficient Management of SSL Certificates

Initially, O₂ used SSL Certificates from a variety of Certification Authorities (CAs) for safeguarding their portal and other applications. This was a manual process with SSL Certificates being requested and issued on an individual basis. O₂'s IT department had to maintain lists of certificates' expiry dates and each time a certificate had to be applied for, purchasing and accounts had to be involved, slowing the process down even further. Under these circumstances, their IT staff couldn't review the overall status of their current certificates in a timely manner nor guarantee a uniform management of their costs. They needed a way in which they could manage their SSL Certificates in an efficient manner across several servers in different locations.

In order to meet this challenge, O₂ chose VeriSign's Managed Public Key Infrastructure for SSL (MPKI for SSL). "The purchase price of SSL Certificates was not the only attractive aspect of this service. Efficient management of SSL across server sites and server types, and increased visibility for administrators were hugely decisive factors", notes Daniel Stricharz on their decision to use VeriSign's MPKI for SSL. This service facilitates O₂'s purchasing, installation, administration, and settling of accounts for SSL Certificates. As a result, it simplifies and significantly speeds up the protection of O₂'s Web servers. With VeriSign's MPKI for SSL, customers including O₂ obtain the certificates they need quickly and easily.

Web-based certificate administration via VeriSign's Control Centre provides O₂ with a Web based interface which gives them the ability to obtain a complete overview of their certificate inventory at any time, as well as issue, renew, replace and revoke certificates. "It used to take us days to set up a new SSL certificate", Stricharz notes. "With VeriSign's MPKI product, we only need an hour to do this, no matter what day of the week it is or time of day."

+ Security and Trust Bring Success

"VeriSign's MPKI has exceeded our expectations", says Stricharz summarising performance to date. VeriSign has simplified the management of O₂'s SSL Certificates, as well as lowered the cost of acquiring and administering them. VeriSign's Certificates fit very well into O₂'s existing security plan. This applies not only to the secure transmission of customer data, but also to the effective safeguarding of the business's internal data traffic. "VeriSign has earned a position of trust with our customers, and by using their SSL Certificates, we are showing them how seriously we take their security", Stricharz adds. In addition to these issues, VeriSign's excellent support and prompt response to questions and problems have proven second to none for O₂.

Additional information can be found on our website www.verisign.co.uk.

© 2007 VeriSign UK Ltd. All rights reserved. VeriSign, the VeriSign logo, the checkmark circle, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other brand names are the property of the respective owners.

00024107
ML070580