



CASE STUDY

Visibly Secure Online Banking

A proactive security policy and the latest encryption technology are set to increase customer confidence in online banking.

“No bank can afford to be red, yellow or even white. When our customers transact online, a green address bar is the best indication that they are on the real Postbank site and not a phishing site. The additional authentication required to gain the green bar is vitally important for a bank such as ours!”

Michael Heinen
Divisional Director, Postbank.



Extended Validation SSL Certificates

Extended Validation (EV) SSL allows visitors using the latest generation of browsers to clearly see a business' official company name in the display to the right of the URL. For example, if you use Internet Explorer (IE) 7 to access a secure page on Postbank's website, the URL address bar will turn green because their website is secured with an EV SSL Certificate. This proves that it is a truly authenticated website. Furthermore, as with all sites secured by EV Certificates, the display next to the green bar will toggle between the company name listed on the certificate and the Certificate Authority that issued the certificate.



+ Overview

With 14.6 million customers, close to 25,000 employees, and 4,500 financial advisors, Postbank Group is one of the largest financial service providers in Germany. However, their primary focus is retail banking. The services they offer to their customers range from payment transactions, commercial banking, bonds, investment funds, insurance policies, and building society accounts. Since their inception, Postbank has endeavoured to offer the highest level of flexibility to their customers. This is why their customers can bank with them at branches across Europe, as well as over the telephone and online. On request, financial advisors will even make home visits!

+ Postbank - The Pioneer in Home Banking

Postbank has 23 years of experience in telephone and online banking. Back in 1983, when they were still part of the German Federal Postal Service, they pioneered home banking by offering their "Btx-Postgiro" service in Germany. Even in those early years, Postbank understood how important security was for home banking to succeed. They joined forces with other banks in Germany to develop a security platform that offered the basis for secure online banking which remains unchanged to this day. Login is accomplished with an account number and an online PIN (personal identification number). Every transaction, such as a transfer or a standing order, is enabled with a transaction number (TAN), a token that is valid only once. In 2005, Postbank enhanced the TAN functionality making it an indexed TAN (iTAN) or mobile TAN (mTAN). The mTAN has since been tested by the Rhineland TÜV (Technical Supervisory Board) and has been certified as secure.

PIN and TAN enabled Postbank to provide customer account access over the Internet. When they took this step in 1998, Postbank was the first bank in Germany to move their customers to strong 128-bit SSL (Secure Sockets Layer) encryption. SSL security is managed via the web server and browser which means that Postbank customers do not need to install any additional software to achieve the benefits of encryption so Postbank customers can rest assured that banking online with Postbank is not only fast and simple, but most importantly it is secure.

Postbank is the market leader in online banking, operating the most frequently visited banking website in Germany, www.postbank.de (2.6 million unique users in Oct. 2006. Source: Nielsen/NetRatings). The growth in the number of Postbank's online customers clearly shows a willingness to bank online. Yet, before trying online banking, many customers still worry about the security of both their transactions and their personal data. To counter these fears, Postbank relies on VeriSign Secure Site Pro SSL Certificates with Server Gated Cryptography, and they have done so ever since the introduction of their Internet banking service. The certificates encrypt, and thereby protect, the exchange of data between Postbank and their customers. However, "VeriSign SSL Certificates also assure our online users that they are accessing a valid and legitimate banking portal", confirms Michael Heinen, Divisional Director at Postbank. SSL Certificates work independently of the operating system, browser type, and browser version. "We needed to implement a solution that guaranteed secure online-banking for our customers without passing the expense of additional software onto them."

+ VeriSign, a Dependable Partner for Secure Online Banking

Michael Heinen explains Postbank's reasons for working with VeriSign: "With VeriSign, we have an experienced online banking partner with comprehensive expertise in Internet security." VeriSign's authentication and verification procedures are based on years of practical experience. Currently used to secure more than a half-million web servers, including those of the 40 largest banks in the world and 93% of Fortune 500, companies put their trust in VeriSign's authentication procedures. Now with Extended Validation Certificates mandated by the CA/Browser Forum - VeriSign is at the forefront of the next generation of SSL Certificates. This new standard has significantly improved the validation process, further reassuring Postbank's customers and Internet users worldwide that they really can trust websites that are protected by Extended Validation SSL Certificates.

+ SSL Encryption Safeguards Online Banking

The SSL Certificates currently used at Postbank combine powerful authentication with strong encryption technology. Postbank uses VeriSign's Server Gated Cryptography (SGC) technology to offer strong 128- or 256-bit SSL encryption to their online banking customers. Without SGC-enabled Certificates, visitors using older browsers, and many using Windows 2000, are limited to a relatively weak 40- or 56-bit encryption. This low level of encryption is insufficient to access Postbank's online banking service as Postbank's servers are configured to automatically end any session where a customer's encryption level doesn't meet prerequisites.

+ New Challenges - Protection from Phishing

Reports of phishing attacks and identity theft make banking customers feel increasingly wary and insecure. At Postbank, SSL Certificates provide a foundation for secure online banking. Nevertheless, an increasing number of customers want to know how their identity will be protected and how they can tell if the website they are visiting is legitimate and not in any way manipulated. Postbank are constantly tasked with ensuring their security measures match customer expectations. To address fears of phishing, in 2005 increased security measures were introduced, establishing nationwide iTANs and mTANs, Internet fund transfer limits, as well as e-mail encryption for customers.

+ Increased Security from Next Generation SSL

To provide advanced security features and visible protection for their customers, Postbank relies on VeriSign's Extended Validation SSL Certificates. The CA/Browser Forum worked together with Certificate Authorities, including VeriSign, to design Extended Validation Certificates for the next generation of browsers, such as Internet Explorer 7. Now it's much simpler and easier for users to know whether they are on a legitimate Internet site. "The Introduction of Extended Validation Certificates is an additional step towards making online banking an even more secure channel to reach our customers", comments Michael Heinen on Postbank's extra security measures.

Next generation browsers, such as IE7, use background colours in the address bar to identify SSL sessions that are secured with Extended Validation Certificates. If an Internet site is protected with a VeriSign Extended Validation Certificate, the address bar will turn green in Internet Explorer 7. "No bank can afford to be red, yellow or even white. When our customers transact online, a green address bar is the best indication that they are on the real Postbank site and not a phishing site. The additional authentication required to gain the green bar is vitally important for a bank such as ours!" The green colour in the address bar means that VeriSign has checked the legitimacy of the organisation in question and their right to use the domain name secured by the SSL Certificate.

Further to this, a display next to the URL address bar toggles between the organisation's name and the Certificate Authority that issued the SSL Certificate. When customers visit Postbank's website using a browser such as IE7, they will see all of these security features and a new padlock icon to the right of the address bar. By clicking on the padlock, users can access information detailing the validity of the certificate as well as the name of the issuing authority.

+ Security Pays for Itself

For companies with a high degree of recognition, like Postbank, the use of Extended Validation SSL is a sensible additional defence against online fraud. When Postbank customers see the green bar, they know they can bank online with peace of mind. "We use Extended Validation SSL Certificates to provide our customers with the greatest possible protection", Michael Heinen states. "Security information must be available to our customers quickly and easily when banking online. Only then will they frequently use online banking with real confidence, and benefit from the advantages of e-banking." Postbank customer surveys show that increased exposure to online banking, together with a policy of actively providing the right information, will help customers see online banking in a very positive light. With comprehensive security consisting of Extended Validation SSL, PINs, iTANs or mobile mTANs, Postbank will continue to provide reliable protection for their customers now and in the future.

+ Why VeriSign

VeriSign is the leading supplier of intelligent infrastructure services. Unparalleled experience in the Internet, telecommunications, and the security environment allows VeriSign to help companies, agencies, and individuals achieve operational efficiency. VeriSign is the leading Secure Sockets Layer (SSL) Certificate Authority enabling secure e-commerce and communications for websites, intranets, and extranets. VeriSign continues to lead the SSL Certificate industry as a member of the CA/Browser Forum, a standards-making body focused on Extended Validation SSL Certificates.

Additional information about Extended Validation SSL and VeriSign can be found on our website www.verisign.ch.