



VeriSign® Roaming Service

Extend your PKI security solution to mobile end users

VeriSign allows enterprises to secure their road warriors by enabling them to securely access private information and digitally sign critical transactions from any computer terminal, any time, anywhere. As an extension of Managed PKI Services, implementation of the Roaming Service easily transforms existing user name and password accounts into digital certificates, making access to a wide variety of Web-based information and services from any remote terminal fast, easy, and secure. Because the Roaming Service is software based, it avoids the high costs and limited portability of hardware based solutions such as smartcards. And all transactions are permanently stored, so that a record of the digital certificate's activity is always available in the form of a digital receipt.

Secure, high-value internet transactions accessible from anywhere

Typically, a digital certificate is downloaded and permanently stored on the hard drive of an end user's computer terminal, permitting access through only that terminal. But frequently, users require their digital certificates to conduct secure transactions from remote terminals or Internet kiosks. For example, doctors and nurses might need to access an intranet from numerous offices or patient rooms to digitally sign diagnosis and prescription forms. Financial services Web sites might need to offer customers the ability to digitally sign online transactions from home or work. State and federal governments could provide services and information that can be accessed from personal computers and public libraries.

The challenge is to provide certificate access for the mobile end user while preserving security, a permanent record of the transaction, and strong encryption. The VeriSign Roaming Service meets this challenge with the Personal Trust Agent (PTA), a browser plug-in that accesses the user's digital certificate in seconds from any terminal. Users need only enable the plug-in with one click and enter a formatted password. The PTA permits users to sign every Internet transaction with the digital certificate, securing the exchange and creating a permanent record.

Robust security

The fundamental problem with simple password protection for client-based data stored within browsers is that a password needs to be easily memorable (otherwise there is a strong tendency to write it down)—and that means an attacker can easily guess it. With the PTA, enterprises no longer have to rely on the browser to locally manage password configuration, but can remotely enforce their password policy. Also, a traditional credential server that verifies passwords presents a major single point of vulnerability to inside attacks, because private keys are stored on a single server. VeriSign Roaming Service

Key Benefits

Easy to Use—The Personal Trust Agent automatically replaces user names and passwords with digital certificates. The plug-in downloads in seconds and installs by itself, seamlessly integrating digital certificates with Netscape® and Internet Explorer® Web browsers.

Flexible—Client authentication and secure Internet transactions requiring a digital signature can be conducted from any terminal, any time, anywhere.

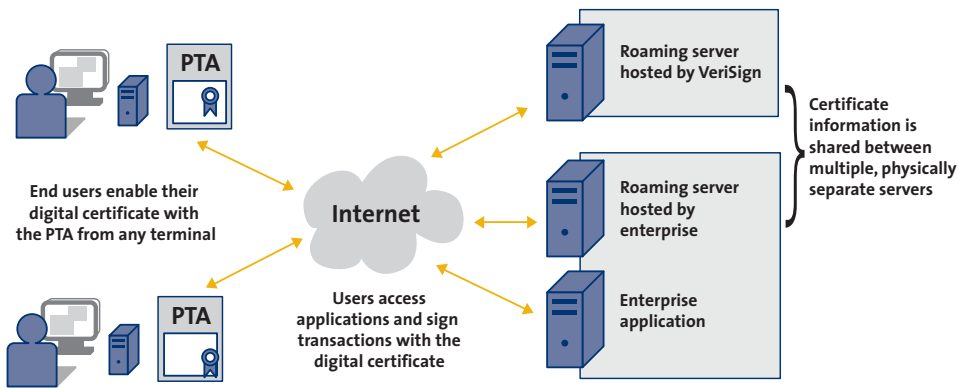
Cost-Effective—Because VeriSign Roaming Service is software based, it costs much less to implement than a smartcard or other hardware solution.

Secure—Key information stored on multiple physically separated servers protect the digital certificate from unauthorized access by both external and internal sources.

Quick to Deploy—VeriSign can have your enterprise roaming-enabled in a matter of days.

Irrefutable—Transactions are validated and stored so an electronic record of certificate use is always available.

The Roaming Process



employs multiple physical servers to store certificates and access information in multiple pieces. The pieces are later reassembled, so passwords are never revealed to back-end servers (only the user ever knows the password), ensuring that an intruder or a malevolent insider can't crack them.

When a digital certificate is downloaded to the user's terminal, it is not stored permanently on the hard drive of the terminal, but resides temporarily in the computer's memory. The certificate lasts only as long as you need it, ensuring that other users do not have access to your credentials. Customizable options let enterprises decide when and how frequently the certificate is erased from the computer.

Easy download and seamless integration for end users

- An end user visits an enterprise Web site, such as an online stock brokerage, offering the use of digital certificates to roaming users.
- The Web application automatically prompts the user to download the PTA. With just one click, the application downloads in seconds and automatically installs itself onto the browser. There is no need to reboot the computer or restart the Web browser.
- The user establishes a user name and password that is permanently linked to the certificate, even when it is downloaded to another computer terminal.
- The PTA instantly downloads the digital certificate to the computer's memory only for the duration of the Internet session. The digital certificate appears in the form of a membership card that displays the name and logo of the issuing enterprise, the name of the user, and the expiration date of the digital certificate.
- All transactions are signed and secured with the digital certificate.
- Subsequent interaction with a roaming-enabled Web site requires only the entry of the user name and strong password.

Effortless implementation for enterprises

Enterprises provide employee access and manage digital certificates with VeriSign Managed PKI Services. VeriSign Roaming Services seamlessly integrate with Managed PKI infrastructure, automatically migrating end user access from user names and passwords to digital certificates. There is no need to reconfigure each individual account. The standard configuration provides shared hosting of servers with VeriSign, with options for additional configurations.

For More Information

To learn more about VeriSign Roaming Services, go to <http://www.verisign.com/products/roaming>

To learn more about the VeriSign Managed PKI Services, go to <http://www.verisign.com/products/onsite>

To speak to a Sales Representative about Roaming Services, call 650.429.5115 or send e-mail to verisales@verisign.com.