VeriSign®
The Value of Trust℠

VeriSign® Go Secure!℠ for Web Applications

Secure extranet and intranet applications virtually overnight

Enterprises are relying on cost-cutting, timesaving extranets and intranets for exchanging information with customers, partners, and employees through applications such as ERP, supply-chain management, and online banking and trading. It's vital to ensure that only legitimate users have access to potentially sensitive information and that transactions are protected from hacking and tampering. But easily guessed, frequently lost user names and passwords are insecure, and more thorough security measures can be complicated to implement. Now VeriSign has the solution. Go Secure! for Web Applications, with VeriSign's Managed Public Key Infrastructure (PKI) service, enables your enterprise to secure the Web interfaces to applications for a million or more users virtually overnight, implementing digital certificates and digital signatures to authenticate users and protect transactions.

Make digital certificates easy to obtain and use

Go Secure! lets you streamline the end user experience of obtaining and using digital certificates (and that means lower customer support costs!). Certificates enable you to limit access to sensitive extranet and intranet data only to authenticated users. They also enable end users to digitally sign online forms. Once you've deployed Go Secure! and decided the rules for certificate use, users can be automatically prompted to obtain certificates and even to renew or revoke them. The Personal Trust Agent makes certificates easily available in the same easy-to-use Web interface for users of both Microsoft® Internet Explorer and Netscape® Communicator browsers, and now includes support for the VeriSign Roaming service (available separately). The Roaming Service gives end users the ability to access their certificates from anywhere without the cost associated with distributing and supporting hard tokens and readers. And by capturing and verifying digital signatures, the Personal Trust Agent enables non-repudiation. Deploy the Password Migration module to convert all your users from user names and passwords to digital certificates and almost automatically: users can access your application as usual, and then receive a digital certificate to use in place of passwords. Go Secure! for Web Applications lets you make digital certificates readily available to all your users, and control how they are used to access your Internet, extranet and intranet applications.

Deploy Go Secure! quickly

Go Secure! for Web Applications consists of plug-and-play components that accelerate the process of securing new or existing applications across your enterprise. It leverages your existing IT infrastructure, integrating smoothly with standard browsers and applications without requiring proprietary client software. Deploying it is easy: Start by configuring your application servers and controlling security policy by

Key Benefits

Fast and easy to deploy: Designed to let enterprises secure extranet and intranet applications with digital certificates overnight.

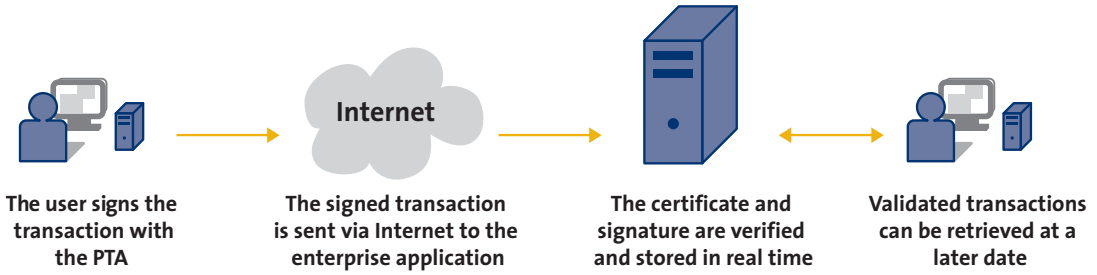
Fast and easy to use: Integrate the Personal Trust Agent (PTA) into your applications to enable users to easily obtain and manage digital certificates. The PTA supports digital signatures and client authentication, as well as the VeriSign Roaming service (available separately), allowing end users to access their certificates from any computer terminal.

Secure: Digital certificates ensure that only legitimate users can access potentially sensitive data on your extranet or intranet, and enable users to encrypt and digitally sign online transactions.

Globally interoperable: Digital certificates enable users of your extranet and intranet to communicate securely with anyone.

Scalable: VeriSign's PKI service, together with Go Secure!, grows with your enterprise, issuing as many digital certificates as you need without requiring incremental investments in hardware, database administration, customer support, or physical security.

The Digital Signature Process



deciding when and how your extranet users interact with certificates. The Certificate Parsing module lets you tailor access privileges, and the Certificate Validation module enables server-side revocation checking based on CRL or OCSP technology, ensuring that holders of revoked certificates cannot access sensitive information. Then configure the Web-based UI, customized with your own branding, for certificate issuance and management.

Components of Go Secure! for Web Applications

- *The Personal Trust Agent* for user-friendly certificate management, client authentication, and digital signatures that can be integrated with a Microsoft or Netscape browser without requiring a proprietary desktop client, and now including support for the VeriSign Roaming Service (available separately)
- *The Digital Signature Platform* that includes components that generate and validate signed transactions in text or HTML.
- *The Certificate Parsing Module* that lets you tailor access privileges to extranet and intranet resources based on customized end user identification certificates
- *The Certificate Validation Module* that enables server-side revocation checking of client certificates, ensuring that holders of revoked certificates cannot access sensitive information
- *The Password Migration Module* that enables you to replace user names and passwords with digital certificates virtually overnight
- *The Digital Notarization Tool* creates a proof of an electronic document's state at a particular point in time.
- *The File Encryption Tool* that protects confidential information by encrypting files on your computer
- *A 400+ page step-by-step Implementation Guide* that makes deployment fast and easy

About Go Secure! Services

Go Secure! for Web Applications is part of a suite of managed services designed to dramatically accelerate the way enterprises secure mission-critical applications and transactions for intranets, extranets, Web sites, and networks. Go Secure! services plug into your existing IT infrastructure without requiring you to change your network or desktops, and together with VeriSign Managed PKI Services, give you everything you need to quickly incorporate digital certificate-based security into your applications. Other Go Secure! services include Go Secure! for Microsoft Exchange and Lotus Notes, for securing enterprise e-mail messaging, and Go Secure! for Virtual Private Networks, for securing VPNs that extend intranets connecting remote users, offices, partners, and customers via the Internet.

System Requirements

Web Servers: *Microsoft IIS 4.0 (Windows NT® only), Microsoft IIS 5.0 (Windows 2000 only), Netscape Server 3.0 or later (for Windows NT, Sun Solaris, or HP-UX) or, iPlanet 4.0 or later (for Windows NT, Windows 2000, Sun Solaris, or HP-UX)
Application Servers: IBM Web Sphere Application Server, BEA System's Web Logic
Single Sign-on Servers: Netegrity SiteMinder

For More Information

For more information about VeriSign Managed PKI and Go Secure! services or for a free test-drive of Managed PKI, visit www.verisign.com/products/onsite/index.html. To contact a VeriSign Sales Representative, call 650.426.5115, or send an e-mail message to verisales@verisign.com.

VeriSign® The Value of Trust℠

©2003 VeriSign, Inc. All rights reserved.
VeriSign, the VeriSign logo, Network Solutions, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.
DS 046 0103