SafeNet Authenticators for VeriSign’s Certificate-based VPNs

SOLUTION BRIEF

Benefits

- End-to-end solution, with best-of-breed products, provided by a single system integrator.
- High-level security for VPN solutions, users’ private credentials and digital certificates, resulting in reduced risk of unauthorized access.
- Strong two-factor authentication, encryption, signing and decryption for a variety of electronic transactions, ensuring a high level of security through reliance on a hardware-based USB device.
- VeriSign keys and certificates and VPN passwords can be securely created and stored on the SafeNet authenticator, operating transparently with any standard browser or email client.
- Flexible and portable authentication device.

SafeNet Authenticators for VeriSign Digital Certificates

VeriSign's digital certificate services enable trusted and secure electronic commerce and communications over IP networks. Utilizing SafeNet's certificate-based authenticators allows users of VeriSign's PKI systems to generate and store private keys and digital certificates inside the token, creating a secure environment and allowing full portability and ease of use. SafeNet certificate-based authenticators' support for standard security interfaces enables complete PKI-based authentication. SafeNet certificate-based authenticators can also perform sensitive on-chip encryption operations, ensuring that user keys are never exposed to the PC environment.

SafeNet Authentication for VPN Systems

A Virtual Private Network (VPN) is a private data network that maintains privacy through the use of a tunneling protocol and security procedures. SafeNet authenticators store VPN access details and authentication credentials, ensuring that users have secure and easy network access.

SafeNet Authentication and Certificate-based VPNs

SafeNet authentication solutions and certificate-based VPNs integrate multiple vendor technologies — the SafeNet authenticator, a VeriSign digital certificate, and a third-party VPN client (such as Cisco or Check Point) — in a single package. It ensures strong two-factor authentication, providing customers with a comprehensive solution, increased network security and reduced infrastructure costs and connection charges. Users simply insert a personal SafeNet authenticator and enter their unique SafeNet authenticator password. Users can take all their authorization details with them wherever they go, making remote access to VPN systems a cinch.

Features

- SafeNet eToken PRO
  - Highly secure smart card chip; Common Criteria certified
  - Secure storage and robust file system
  - Hardened tamper-evident and water-resistant shell
  - Standard USB interface
  - On-board RSA 1024-bit and 2048-bit authentication, DES, 3DES (triple DES), SHA1
  - Support for crypto API, including PKCS#11 and CAPI
  - Certifications: FIPS 140-2 Level 2 & 3
  - SAM (SafeNet Authentication Manager) for managing token deployment and lifecycle

- SafeNet and Certificate-based VPNs
  - Certificate-based VPNs
  - Portable certificates and strong two-factor authentication
  - Certification and registration authority services
  - x509 certificate support

Benefits

- End-to-end solution, with best-of-breed products, provided by a single system integrator.
- High-level security for VPN solutions, users’ private credentials and digital certificates, resulting in reduced risk of unauthorized access.
- Strong two-factor authentication, encryption, signing and decryption for a variety of electronic transactions, ensuring a high level of security through reliance on a hardware-based USB device.
- VeriSign keys and certificates and VPN passwords can be securely created and stored on the SafeNet authenticator, operating transparently with any standard browser or email client.
- Flexible and portable authentication device.
PKI, Digital Signatures and Certificates

Organizations authenticate the identity and validity of users accessing information on computer networks through Public Key Infrastructure (PKI), a system providing solutions for secure eCommerce and network services. A PKI consists of protocols, services, and standards supporting applications of public key cryptography. In a PKI, every user is assigned a cryptographic key pair consisting of a public key and private key that are mathematically related. The public key is published, while the private key is kept secret.

Digital Certificates

Digital certificates are electronic credentials that tie a public key to an individual, and help prevent someone from using a phony public key to impersonate someone else. A basic certificate will contain a public key and an individual’s name. Common certificates also include an expiration date, the name of the Certificate Authority (CA) that issued the certificate, and a serial number. Most importantly, it contains the digital signature of the CA.

Virtual Private Networks

VPNs utilize the public telecommunication infrastructure and maintain privacy through tunneling protocol and security procedures. These procedures normally include VPN servers that require all users be authenticated before allowing them access. With a VPN, organizations have the same capabilities as they would with a framework of lines owned or leased for private use, at much lower cost.

SafeNet Authentication and VeriSign — Making Strong VPNs Work for You

Together with VeriSign digital certificates and a third-party VPN client solution, SafeNet’s certificate-based authenticators enable remote access to secured VPNs. Information stored on the SafeNet authenticator can include site access combinations, each containing the user name, site, and authentication password, as well as PKI keys and certificates.

For more information on VeriSign, visit www.VeriSign.com.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers’ most valuable assets, including identities, transactions, communications, data and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies and in over 100 countries trust their information security needs to SafeNet.