VeriSign™

White Paper

VeriSign® OnSite℠ and Microsoft® Windows® 2000

VeriSign® OnSite℠ and Microsoft® Windows® 2000

I. Introduction

Windows 2000 provides enterprise customers with a scaleable platform for managing PKI services and integrating them with mission-critical applications. VeriSign services enable these enterprises to leverage their Windows 2000 investment to quickly and cost-effectively set up and manage interoperable PKI services, enabling trusted business e-commerce and communications solutions.

This paper describes how VeriSign OnSite integrates with and leverages Windows 2000 PKI services. It includes an overview of VeriSign OnSite, a discussion of Windows 2000 PKI services and how they relate to OnSite, and application examples of how VeriSign's services integrate with Active Directory and PKI-enabled applications such as browsers and secure e-mail.

(For information on VeriSign's Gateway Service, which allows you to issue trusted interoperable VeriSign certificates from a Microsoft Certificate Server, please see the white paper "VeriSign Gateway Services for Microsoft Certificate Server" at http://www.verisign.com/products/gateway/index.html.)

II. Overview: VeriSign OnSite Integrated PKI Services

VeriSign OnSite is a fully integrated enterprise Public Key Infrastructure (PKI) service designed to secure intranet, extranet, Virtual Private Network, and e-commerce applications by providing maximum flexibility, performance, and scalability with the highest availability and security. OnSite allows you to quickly and cost-effectively establish a robust PKI and Certificate Authority (CA) with total control over security policy, PKI hierarchy, authentication models and certificate lifecycle management, linked to VeriSign's robust, high-availability certificate processing services.

The OnSite solution accelerates deployment and cuts operating costs while providing an open platform based on industry standards that can be easily integrated with off-the-shelf solutions, including all PKI-enabled Microsoft® applications and platforms. With VeriSign OnSite, enterprises can quickly and easily deploy a PKI while relieving themselves of the high expense of designing, provisioning, staffing, and maintaining a PKI backbone.

Key OnSite features include the following:

- **Certificate Authority**. VeriSign OnSite provides advanced Web-based configuration wizards, administration and support tools, report generators, and application integration modules to give an enterprise full control over its PKI and to provide the critical link to VeriSign's process centers. OnSite's capabilities provide full support for end-user registration and certificate renewal with end-user screens customized to an organization's look and feel for a particular application.

- **Registration Authority**. The centralized OnSite control center gives you full control of the registration and authentication process, allowing you to easily

manage the lifecycle process for enrolling, approving, and revoking certificates. With OnSite, you can also distribute RA functions such as certificate approval, revocation, audit and day-to-day management to an unlimited number of administrators, each with a unique role—from configuration to approval to read-only capabilities. Distributing points of control for defining, approving and revoking user keys and certificates minimizes the risk of security breaches. OnSite also provides customers with extensive audit trails and reporting capabilities along with auditable security practices—all features, which support non-repudiation of, certificate based-transactions.

- **Key Management**. OnSite Key Manager and Key Recovery Service enables centralized key generation, private key backup and distributed key recovery to ensure maximum security for your private keys. Key Manager and Key Recovery Service also includes dual key pair generation and usage, which allow the issuance and back-up of encryption key pairs. The OnSite Key Recovery Service provides a unique two-step process with the highest level of security for storing and recovering private keys.

- **The Automated Administration Module** allows transparent authentication and revocation of users or devices directly from pre-existing administrative systems, databases or directories, rather than requiring manual authentication for each certificate application.

- **The Directory Integration Toolkit** enables you to automatically insert certificates and certificate-revocation lists into LDAP-compliant directories. In a Windows 2000 environment the Active Directory can be used to authenticate users and as a central repository for certificates and related data.

III. Integrating OnSite and Windows 2000 Security Services

Windows 2000 security services include the following components:

- Active Directory
- Secure Channel (IIS SSL Client Certificate Mapping & Active Directory)
- Encrypting File System
- Roaming Profiles
- IPSec Client/Server
- Smartcards and Logon Certificates
- Revocation Services
- Security Management Tools
- Key Management Services

A. Active Directory

Active Directory is now the main certificate repository for enterprises. The Exchange Global Address List (GAL) has served as the primary Enterprise Directory for many organizations, but now the next release of Exchange (Exchange 2000) will incorporate Active Directory.

OnSite 4.51 fully supports the Windows 2000 Active Directory using LDAP both to publish certificates and to authenticate users. For example, browser certificates used to access your Extranet services are now published to the Active Directory and are automatically associated with the corresponding Windows 2000 user account, also managed in Active Directory.

For existing users of certificates and to provide a seamless transition for Exchange users, Microsoft has implemented a proxy approach to maintain backwards-compatibility with currently deployed clients.

For example, when Outlook users want to find an individual within their organization, they would normally search the Global Address List (GAL), which aggregates all messaging recipients in the enterprise. Because Exchange 2000 servers no longer host their own directory service, all data is now retrieved from the Global Catalog servers in Active Directory.

Because a Global Catalog server can support the Messaging Application Programming Interface (MAPI) protocol as well as Lightweight Directory Access Protocol (LDAP), Outlook clients can communicate with Active Directory using the same protocol employed by the Exchange Server 5.5 Directory Service.

To make Exchange 2000 compatible with the existing MAPI client base, an Exchange 2000 server proxies any MAPI DS requests to a local Global Catalog server on the network. The DS Proxy process on the Exchange 2000 server accomplishes this task. The proxying process is simply a forward of the packet; it does not change the request into (Lightweight Directory Access Protocol) LDAP. Active Directory supports a number of protocols, including LDAP and MAPI DS, so an Outlook directory request is completely valid, even directly against an Active Directory server.

B. Secure Channel: IIS SSL Client Certificate Mapping & Active Directory

Certificate mapping is a Windows 2000 feature that associates a certificate with a Windows 2000 user account stored in Active Directory. Internet Explorer and IIS 5.0 can be used to authenticate a user to an account stored in Active Directory based on the name information in a certificate. The account that the certificate maps determines the user's access rights on the server.

For example, you can create customer accounts in the Active Directory and then issue certificates via OnSite to their browsers. When users log onto your site using their certificates, IIS verifies their account privileges against the Active Directory and then logs them in. The benefit of this solution is that no additional database is required for authentication or management of external users.

C. Encrypting File System

OnSite can issue certificates for use by the Windows encrypting file system (EFS) if the certificate profile selected by the OnSite Administrator contains the enhanced key usage extension for EFS. This gives the Administrator control of which user certificates can be used to encrypt local files.

An additional benefit of the OnSite Key Management Service is that it enables the recovery of user's lost encryption keys. Windows 2000 has no native key recovery system and handles encrypted file recovery by encrypting everything with a single system admin key. The disadvantage of this method is that this single key can decrypt every file in your company, so if it is cracked, stolen, or misused, the security of your entire organization can be jeopardized.

D. Roaming Profiles

Roaming profiles enable mobile users to log into workstations within the enterprise and still access their VeriSign certificates. Because Windows 2000 stores user certificates and keys in users' profile in an encrypted form, users with roaming profiles (not mandatory profiles, which are read-only) can access VeriSign Personal certificates and keys anywhere within a Windows 2000 domain environment. For a more robust extranet solution to roaming Certificates, VeriSign offers an additional roaming service.

E. IPSEC Client/Server

OnSite can issue certificates for use by the Windows 2000 IPSec client for Virtual Private Networks. OnSite allows the Administrator to choose a certificate profile that contains both the Enhanced key usage and IPSec AltSubjectName Extension required by the Microsoft client. In addition, OnSite offers enterprise customers a comprehensive and mature IPSec solution that supports not only Windows 2000 but also solutions from Cisco, Checkpoint, and many other clients, firewalls, and routers.

F. SmartCards and Logon Certificates

VeriSign has worked closely with manufacturers to ensure that its services work smoothly with a variety of cryptographic hardware devices. All OnSite enrollment pages support alternative CSP (cryptographic service providers) that may be used to generate and store keypairs and certificates. Any Smartcard that has a Microsoft CSP and sufficient memory to store the certificate (such as those from Gemplus and Litronic) can be used. The flexible OnSite Administrator's Policy Wizard allows the OnSite Administrator to either force the user to enroll using a particular hardware CSP or allow the user to choose a software CSP if no hardware is available. You can ensure that a Smartcard is always used for key protection in high-security environments, while also providing support for mixed environments in which Smartcards have not been fully deployed.

G. Revocation Services

Windows 2000 supports revocation checking across all supporting Microsoft applications through the use of CRL Distribution Points (CDPs). A CRL Distribution Point is an extension in the certificate that points to the location of the CRL (Certificate Revocation list) maintained by the CA. Both OnSite certificates and VeriSign's public client certificates already contain these CDP extensions. Some Microsoft applications such as Outlook

Express already enable revocation checking by default. Other applications such as Internet Explorer support revocation checking, but require that it be enabled by switching it on in the application or Windows registry.

H. Security Management Tools

Windows 2000 includes a number of tools for managing the Windows 2000 environment implemented as Microsoft Management Console (MMC) snap-ins that allows Windows administrators to manage users throughout the enterprise. For Windows Administrators who wish to administer OnSite through the same mechanism, VeriSign provides an OnSite MMC that enables administrators to view users' OnSite certificates, as well as to enroll, renew and revoke existing users.

The MMC communicates with OnSite using the well-established CRS protocol. Microsoft and VeriSign are working closely together within the IETF on a new revision of CRS protocol now known as CMC. It is expected that all future Management interfaces to Windows 2000 as well as to future Microsoft clients will support the upgraded CMC protocol once it has been finalized.

I. Key Management Services

Windows 2000 currently contains no native Key Management services but does allow third parties to provide such services. Key recovery provides obvious benefits for users of services such as EFS (see section IIIC above) and Email. The OnSite Key Recovery Service provides a unique two-step process with the highest level of security for storing and recovering private keys. With VeriSign's Key Management Service, private keys are individually encrypted and stored in a local database. VeriSign Key Manager generates a unique 168-bit random triple DES key to encrypt each private key. The system then encrypts the triple DES key with a VeriSign public key. Then these two encrypted keys (the encrypted private key and the encrypted 3DES key), called the Key Recovery Block, are stored in the database. This is an extremely secure solution because if the database is cracked, the hacker would then have to crack a different 3DES key for *each* private key.

For a key recovery operation, the Administrator sends the key recovery request to VeriSign. VeriSign then verifies that the request is authorized (signed by the Recovery Administrator's certificate), decrypts the key recovery block using the VeriSign private key, and returns the unique 3DES key, which is then used by the Key Recovery server to decrypt the private key. It is important to note that with this architecture, VeriSign never sees the user's private key; to recover it, VeriSign must authorize the transaction by providing the recovery key.

The benefits of the service are that the Administrator must be authorized to perform key recovery, and that VeriSign audits every key recovery transaction. Therefore, if you suspect that a key has been compromised (e.g. by a rogue Administrator) you could determine which keys were recovered by the Administrator and simply revoke and reissue them. There is no possible way for an Administrator to conceal the compromise. Finally, VeriSign can even monitor the system for unusual activity levels and notify a contact at the customer site if the number of recovery requests increases sharply or suddenly. VeriSign could then alert an alternative point of contact asking for confirmation.

VeriSign's Key Recovery Service is unique in that it also supports non-repudiation with single key pairs. If a private key is compromised by a rogue administrator, then the audit logs at VeriSign can be checked to determine whether or not users' private keys were ever recovered, and if so, when and by whom. This unique capability is available only with VeriSign's Key Recovery Service, and ensures that extranets interoperate with a variety of S/MIME e-mail clients.

IV. Windows PKI Application Integration Examples

The following overview describes how the integration of VeriSign OnSite and the Windows 2000 PKI affects information flow and the user experience, focusing on Microsoft Exchange as the best application example of how PKI will be implemented in enterprises.

A. Corporate Extranet

Digital certificates in conjunction with existing Web clients ensure that only authorized users can access potentially sensitive data on your extranet or intranet, Certificates also enable users to encrypt and digitally sign online transactions for non-repudiation.

Using OnSite Web enrollment, users of SSL-enabled clients such as Internet Explorer or Netscape Communicator can obtain certificates that contain their account names via OnSite. Earlier versions of Windows required an explicit mapping in IIS to map a user certificate to a specific NT account. In Windows 2000, IIS works in conjunction with Active Directory to provide a more flexible and scalable certificate mapping solution for extranet users.

The new functionality of IIS allows it to match users' names in certificates with their accounts in the Active directory. Windows Administrators no longer must maintain a separate authentication and access control database for extranet users.

If a certificate must be revoked and replaced, no new mapping in IIS is necessary: OnSite automatically places the correct certificate in the Active Directory when it issues the new certificate. When IIS authenticates the user, it will do so against the Active Directory rather than against hard-coded mapping as before. Thus for the first time, both internal and external users can be managed using regular Windows Admin tools. Permissions and rights can be changed dynamically and will be reflected automatically the next time the user logs in.

Customers enroll for a certificate by requesting it on the extranet. Depending on the authentication method used to identify the enrollee, OnSite can either issue the certificate automatically, the OnSite Auto Authentication Module checking against the Active Directory in order to approve the request, or the request can go into a pending queue for later manual authentication and issuance by an OnSite Administrator. When OnSite issues the certificate, it is sent to the end user and published automatically into the Active directory.

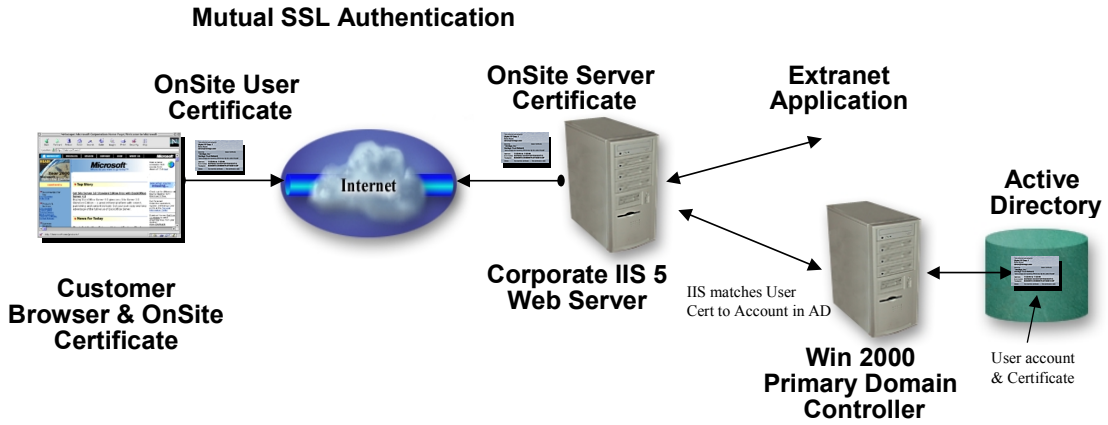

Figure 2: Mutual SSL Authentication

For example, you can create customers' accounts in the Active Directory and then issue SSL certificates for client authentication to customers' browsers. When users log onto your site with their certificates, IIS verifies their account privileges against the Active Directory and then logs them in. The benefit of this solution is that no additional database is required for authentication or management of external users. An additional benefit of issuing server certificates through OnSite is that the certificates are automatically trusted by virtually all browsers, eliminating the cumbersome process of distributing root keys to all your partners.

B. Exchange PKI Solution Overview

VeriSign's Go Secure! service integrates VeriSign's managed security services directly into your existing Exchange environment, making it easy to deploy, administer, and use secure messaging anywhere in the world—with no additional changes to your IT infrastructure. Go Secure! implementation typically takes no more than a few days, unlike other secure e-mail alternatives that require installation of additional proprietary client, server, and directory software.

Go Secure! for Microsoft Exchange service components include:

Exchange Subscriber Enrollment

- Exchange Subscriber Enrollment includes HTML and scripts to control the user enrollment process.

- It gives you the flexibility to customize the user interface to fit your corporation's look and feel.
- Exchange Subscriber Enrollment automatically populates users' enrollment forms with their Exchange certificate content, greatly reducing enrollment errors.

Exchange Directory Integration

- This is a client-side search utility that determines which directory (Win 2000 Active Directory or the Exchange 5.5 GAL) to use to retrieve the user's name, e-mail address and organizational information during enrollment.
- Exchange Directory Integration automatically publishes end-user certificates to the correct directory.

NT Auto Authentication

- Certificate requests are automatically approved using users' Windows NT logon credentials and directory information.
- NT Auto Authentication works across single, multiple, or geographically dispersed Exchange domains.
- It also works with the OnSite Auto Administration kit for additional authentication checks as required by the customer.

Exchange Certificate Policy Manager

- The Exchange Certificate Policy Manager conforms certificate content to meet Exchange and Active directory formatting requirements.
- Certificates are interoperable with non-Microsoft S/MIME client recipients.
- The Exchange Certificate Policy Manager issues certificates linked to the VeriSign Trust Network, eliminating the need for you to set up explicit trust relationships with each of your external business partners, suppliers, or customers. Your certificates will be trusted automatically by recipients with any major S/MIME compliant e-mail client.
- The Exchange Certificate Policy Manager enforces a uniform policy for all end-user enrollments including certificate content, key usage, and VeriSign Trust Network directory publishing.

C. End-User Experience

The user enrollment process follows these steps:

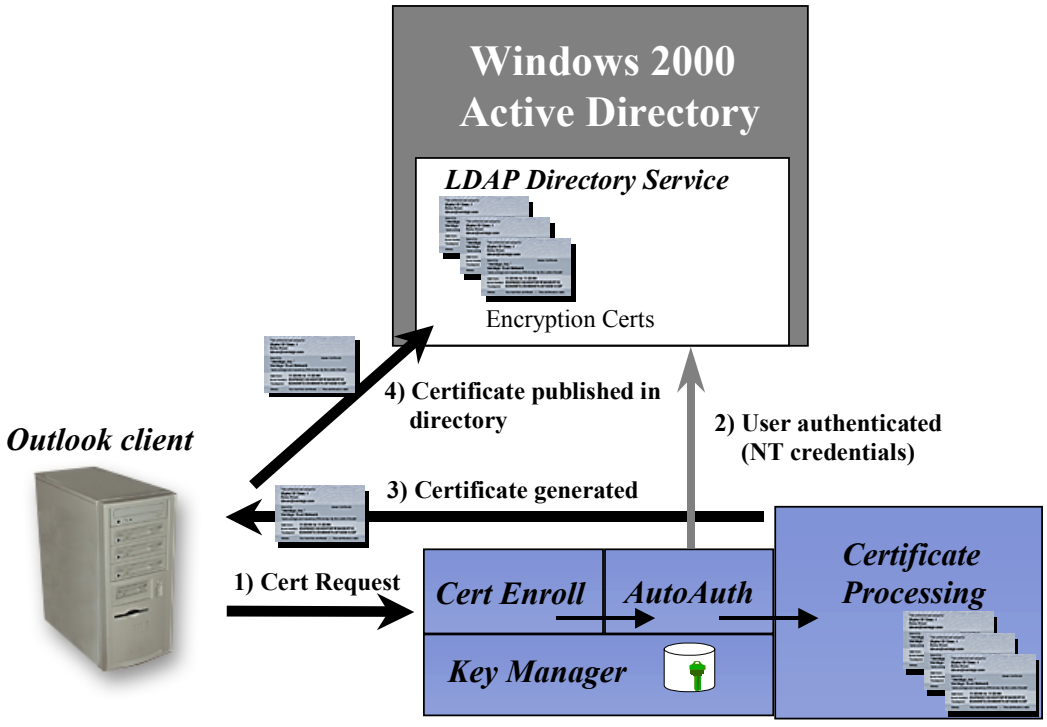

Figure 3: Certificate Enrollment Process in Windows 2000

The certificate is linked to VeriSign Class 2 public roots, which are embedded in tens of millions of installed S/MIME-compatible clients. This means that signed messages will automatically be trusted by the recipient's S/MIME client, even if the recipient does not use a VeriSign certificate.

If the sender does not have an external recipient's VeriSign-issued certificate, then the sender can search for and retrieve it from VeriSign's public certificate directory.

D. OnSite and Microsoft Exchange 2000

Microsoft Exchange 2000 uses the Active Directory as its authentication mechanism. This means that user accounts and certificates are now stored in the Active Directory rather than the Exchange GAL. For existing Outlook clients who will look to the GAL in order to find their certificates, this change is seamless due to the proxying mechanism deployed by Microsoft between the Exchange Server and the Active Directory.

OnSite integrates with the Windows NT Environment in three main ways:

- **Authentication:** Automatically verifying users' NT credentials against a PDC before issuing them a certificate

- **Subscription:** Retrieving users' attributes from the directory for inclusion into their certificates via LDAP

- **Publication**: Using LDAP to publish certificates to the Exchange or corporate X.500 Directory

In Windows 2000, Active Directory now provides the authentication mechanism for verifying user Logon credentials. This is a transparent transition that does not require OnSite to support any new interface to authenticate users. In addition, the VeriSign Auto Authentication module can also retrieve information from the Active directory to provide additional authentication for the enrollment request.

The existing ability in OnSite to retrieve account information and publish a certificate using LDAP and ADSI means that OnSite is already compatible with Active Directory. All that is required is for OnSite to identify which Directory in which to store the user certificate.

The OnSite Administrator can select the default Active Directory. In addition, for mixed environments in which customers may be running multiple directories concurrently (Exchange 5.5 and Exchange 2000, for example), the OnSite Administrator can enable a VeriSign control (hosted on the enrollment pages) to transparently and automatically detect which directory the applicant is currently using and then update accordingly.

In Windows 2000, users can encrypt local files using Microsoft's EFS. The OnSite Administrator can allow a user's certificate issued for Exchange to also be valid for EFS file encryption. This preference must be set in the OnSite Control Center prior to certificate issuance.