



White Paper

Secure Messaging for Your Enterprise E-mail

Secure Messaging for Your Enterprise E-mail

I. Introduction: VeriSign® Go Secure!SM for Microsoft® Exchange

E-mail is the virtual nervous system on which enterprises and organizations of every size and description rely to communicate internally with colleagues and co-workers, and externally with business partners and customers.

Businesses, governments, and institutions depend on e-mail to transmit all types of communications—often, extremely sensitive information. Within organizations, this may include human resources, payroll, and other confidential data. And externally, we routinely send sensitive information such as pricing data, design specifications, legal documents, and purchase orders over the Internet to and from remote employees, other divisions, business partners, suppliers, legal counsel, and customers.

Imagine the risk of having your competitor access and monitor all e-mail communications with your top customers. Imagine the risk of hackers modifying the contents of sales proposals or legal documents. Imagine the risk of disgruntled employees intercepting payroll related communications.

These risks are real. *In a recent security survey, 68 percent of companies surveyed characterized messaging misdemeanors as widespread, with losses estimated at \$3.7 million per company a year¹.*

Although it may seem that sending a message through your company's intranet or over the Internet is secure enough, it isn't. Programs designed to intercept messages are readily available on the Web. Even many office LANs run through insecure public areas on the Internet at some point during transmission. And often, as with most frauds, computer crimes are carried out by insiders. Security by obscurity does not work.

So why don't more companies secure their messages? There have been several barriers to deployment:

- Lack of standards support by key messaging vendors
- Solutions that are difficult to deploy, support, and use
- Lack of interoperability between different e-mail clients
- Scalability of vendors' security solutions

¹ "How Safe are Your Business Secrets?", Lee Bruno, *Data Communications Magazine*

Fortunately, things have changed:

- All major enterprise e-mail platforms (Microsoft® Exchange 5.5 SP1 and later, Lotus® Notes R5, Groupwise 5.5, and Netscape) now support the S/MIME standard.
- VeriSign has introduced Go Secure!SM for Microsoft Exchange, a new secure messaging solution that:
 - Makes it easy to deploy, support, and use secure messaging with your existing Microsoft Exchange infrastructure
 - Is completely interoperable across different extranet recipient e-mail clients
 - Enables very scaleable deployments and usage within enterprises as well as with external customers, suppliers, and business partners

Go Secure! for Microsoft Exchange works with existing Microsoft Outlook 98 and 2000 desktop clients and supports Exchange 5.5 server (SP1) or later. Certificate requests are automatically approved using the users' Windows NT® logon credentials. This seamless process makes it easy for administrators to deploy Exchange security to a large number of users. Go Secure! allows automatic publishing of digital certificates issued via the VeriSign OnSiteSM managed service to the existing Exchange global directory, and the automatic retrieval of certificates for encrypting and signing sensitive e-mail messages. It also includes tailored support and implementation services, administrator set-up guides, and end-user tutorials. Combined with VeriSign's highly scalable OnSite service for digital certificates, the Go Secure! Service ensures quick and easy deployment of secure e-mail.

According to a recent review by PC Week² of VeriSign's Go Secure! For Microsoft Exchange:

- "Go Secure! proved easy to implement and tightly integrated with Exchange."
- "The service obviates costly infrastructure and maintenance outlays and can be more quickly deployed than an in-house scheme."
- "The service addresses one of the biggest complaints administrators have about implementing a PKI system, namely client deployment. There are no new applications or plug-ins to deliver to desktop PCs and users can perform activation."
- "The benefit to Go Secure is ease of administration."
- "For companies that need secure Exchange e-mail, VeriSign's Go Secure! for Microsoft Exchange service fits the bill. Less expensive than setting up and

² "VeriSign Service Eases Exchange Security", *PC Week* 8/99

maintaining an in-house PKI, the product also affords tight integration with Exchange.”

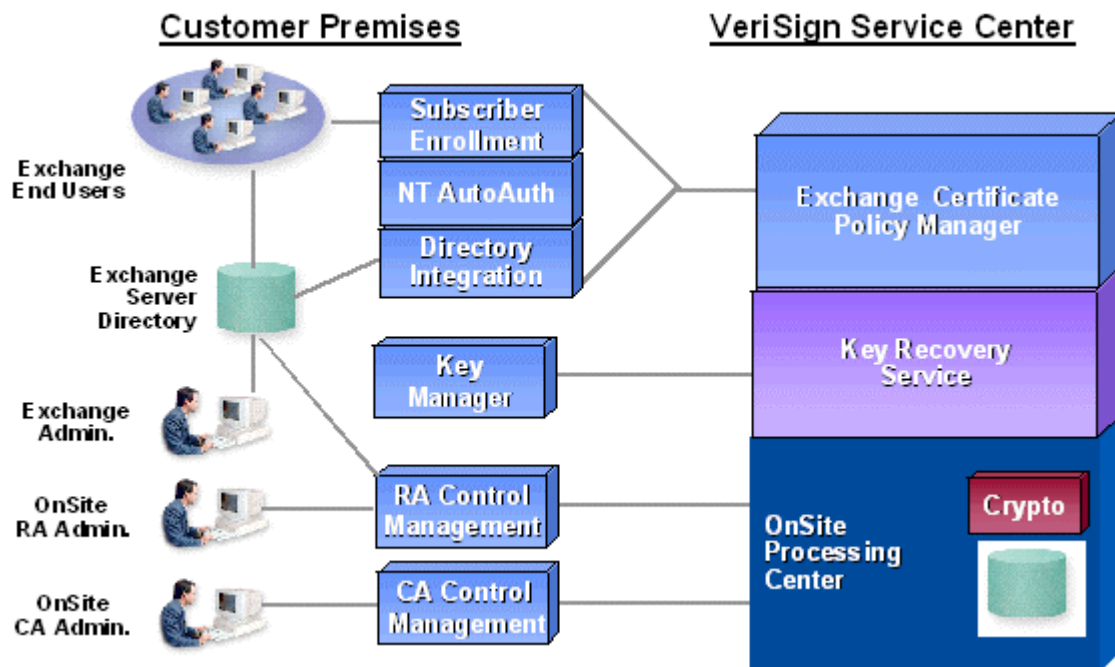
II. Solution Overview

VeriSign’s Go Secure! for Microsoft Exchange is a 24x7, enterprise-class digital certificate service that enables universal secure messaging using Microsoft Exchange and VeriSign’s global digital certificate services. Go Secure! 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. Typical implementation time is no more than several days. This is in sharp contrast to other secure e-mail alternatives that require installation of additional and proprietary client, server, and directory software.

Go Secure! for Microsoft Exchange service components include:

- Exchange Subscriber Enrollment
- Exchange Directory Integration
- NT AutoAuthentication
- Exchange Certificate Policy
- Technical Documentation
- Customer Service and Quality Assurance

The following diagram illustrates a typical implementation. Base certificate lifecycle services are provided by the VeriSign OnSite service, key management and recovery services are delivered by VeriSign’s Key Management Service, and Exchange server and client integration is accomplished with Go Secure! for Microsoft Exchange.



A. Exchange Subscriber Enrollment

- Use HTML and scripts to control the user enrollment process.
- Flexibly customize the Exchange Subscriber Enrollment to fit your corporation's look and feel.
- Enable users to automatically populate users' enrollment forms with their Exchange certificate content, greatly reducing the chance for enrollment errors.

B. Exchange Directory Integration

- This search utility retrieves users' names, e-mail addresses, and organizational information from the GAL during enrollment.
- The Exchange Directory Integration function automatically publishes end-user certificates to the GAL.

C. NT AutoAuthentication

- Certificate requests are automatically approved using users' Windows NT logon credentials and Exchange directory information.
- AutoAuthentication works across single, multiple, or geographically dispersed Exchange domains.
- AutoAuthentication works with the OnSite AutoAdministration kit.

D. Exchange Certificate Policy Manager

- This component conforms certificate content to meet Exchange directory formatting requirements.
- Certificates are interoperable with non-Microsoft S/MIME client recipients.
- Certificates are linked to the VeriSign Trust Network (VTN), eliminating the need for you to set up explicit trust relationships with your external business partners, suppliers, or customers. Recipients using any major S/MIME-compliant e-mail client can automatically trust certificates issued via OnSite and Go Secure!.
- The Policy Manager enforces a uniform policy for all end-user enrollments, including certificate content, key usage, and VTN directory publishing.

E. Documentation

- The Administrator Implementation Guide provides detailed steps on planning, integrating, and implementing OnSite with Exchange.
- An online self-help reference guide walks end-users through Outlook certificate installation and usage.

F. 24x7 Global Operations Center

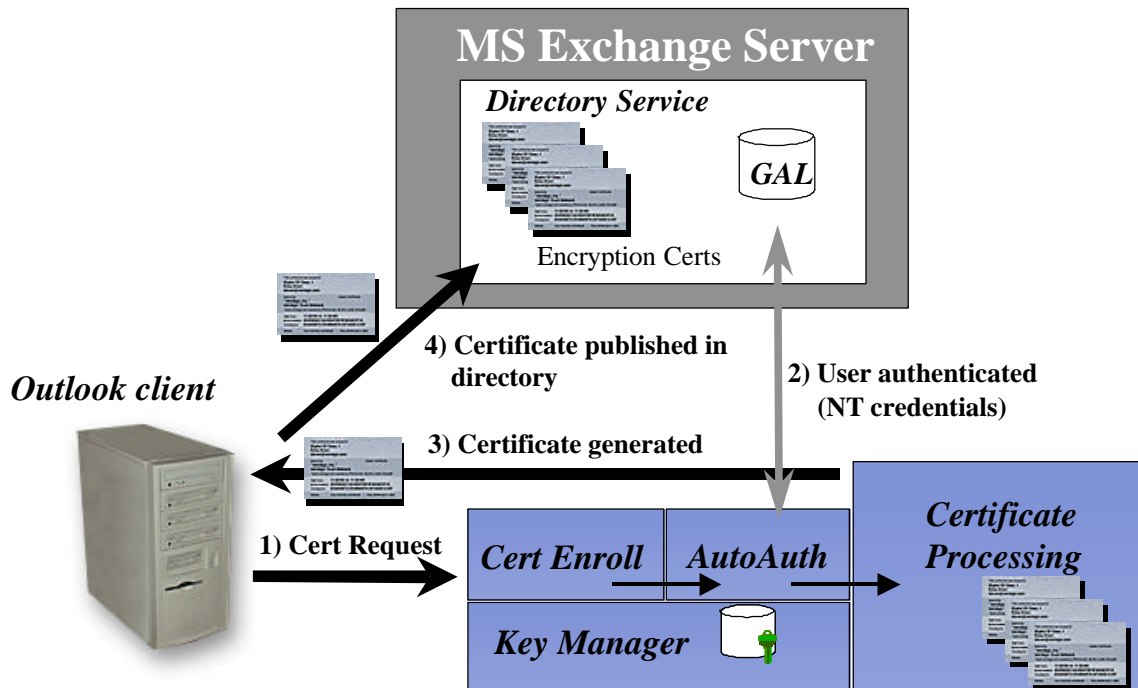
- VeriSign’s high-availability data centers are armed with full redundancy and disaster recovery capabilities.
- VeriSign has proven the scalability of its services to millions of certificates.
- VeriSign’s maximum-security facilities are built using U.S. Department of Defense security specifications.
- VeriSign provides your business with binding, service-level contracts.

VeriSign’s Go Secure! Service for Microsoft Exchange is continuously upgraded to ensure that your secure messaging investment is always up to date, even as you deploy upgrades such as Windows 2000 and Exchange 2000. With Go Secure!, you can be confident that VeriSign’s PKI services will always work seamlessly with your existing and future Exchange/NT infrastructures.

III. The End-User Experience

One of the deployment barriers for previous secure messaging solutions has been ease of use. Go Secure! is designed to make the end-user enrollment process as simple as possible. It also makes it very easy for end-users to send secure messages without having to understand the complexities of Public Key Infrastructure (PKI).

The following figure illustrates the user enrollment process:



The process of enrolling for a digital certificate works as follows:

1. The organization's Microsoft Exchange or Security administrator sends an e-mail to users with instructions and a URL to start the enrollment process. The user clicks on the embedded URL, which links to the enrollment Web pages.
2. The user is prompted to enter NT log-on credentials (NT username and password) for purposes of authentication. The enrollment server uses the NT credentials to find the user's entry in the GAL, and their friendly name, e-mail address, and organization name. This information is pre-published in the user enrollment form, so all the user has to do is review the information and accept. AutoAuthentication then automatically approves the certificate request and passes the certificate request on to Key Manager to generate the key pair. Then the approved certificate request and the user's public key is securely transmitted to VeriSign's certificate processing center.
3. VeriSign's processing center automatically issues the user certificate and downloads it to the enrollment server, which automatically installs the certificate in the user's client certificate store. Key Manager also automatically installs the user's private key on his or her e-mail client.
4. The user's certificate is published to the Exchange GAL, making it easy for other users within the organization to access the certificate in order to send encrypted messages.

At the end of the user enrollment process—which takes about a minute—a self-guided tutorial is presented on the user's client with detailed instructions and screen shots showing how to send digitally signed and encrypted e-mail.

The user interface for sending signed and encrypted e-mails from Outlook 98 or 2000 includes icons for digital signatures and encryption, which are added to the Outlook toolbar. When a user selects the signature icon, the message is encrypted with the user's own private key, thus ensuring to the recipient that the message really came from the user (authentication and non-repudiation) and was not tampered with en route (message integrity). The sender's certificate is linked to the VeriSign Class 2 public roots, which are embedded in tens of millions of installed S/MIME-compatible clients, so that the signed messages will automatically be trusted by the recipient's S/MIME client (even if they recipient is not a VeriSign user).

The user can also ensure the confidentiality of a message by encrypting the message with the recipient's public key, which Outlook automatically obtains from the recipient's certificate in the GAL (if an internal employee) or the sender's local contacts folder (for external recipients). To encrypt the e-mail, the user needs only to click on the encryption icon on the toolbar.

If the sender does not have an external recipient's certificate, he or she can search for and retrieve it from VeriSign's public certificate directory if the recipient has a VeriSign issued certificate. Otherwise, the user can simply have the external recipient send a

signed e-mail, and then add the recipient's certificate to the recipient's entry in the Contacts folder by simply right-clicking on the address field.

IV. Key Management Architecture

The approved enrollment form requesting the certificate is sent to the Key Manager, which generates the key pair and sends the public key to VeriSign. Then, the signed certificate is returned to the Key Manager, and the Key Manager sends the private key and certificate to the user in PKCS#12 format via an automated import into IE and the MS CAPI cert store.

Just before the private key and certificate are sent to the end user, the private key is copied to the database for backup (if this fails, the end user does not get the certificate—the end-user never gets it unless it is first escrowed).

VeriSign Key Manager generates a unique 168-bit random triple DES key to encrypt each private key. Each private key has a unique 3DES key to go with it. The system also encrypts the triple DES key with a public key from VeriSign, and then these 2 encrypted keys (the encrypted private key and the encrypted 3DES key), called the Key Recovery Block, are stored in the database along with the name of whomever it belongs to. This results in an extremely secure solution: if someone steals the database, he or she would have to crack a different 3DES key for EACH private key.

For a key recovery operation, the administrator retrieves the user record from the database and sends the key recovery block to VeriSign. VeriSign verifies that the request is authorized (signed by the Administrator's certificate), decrypts the key recovery block using the VeriSign private key, and returns the unique 3DES key, which is used to decrypt the private key. VeriSign never sees the user's private key, but to recover it, VeriSign has to approve the transaction by providing the 3DES key.

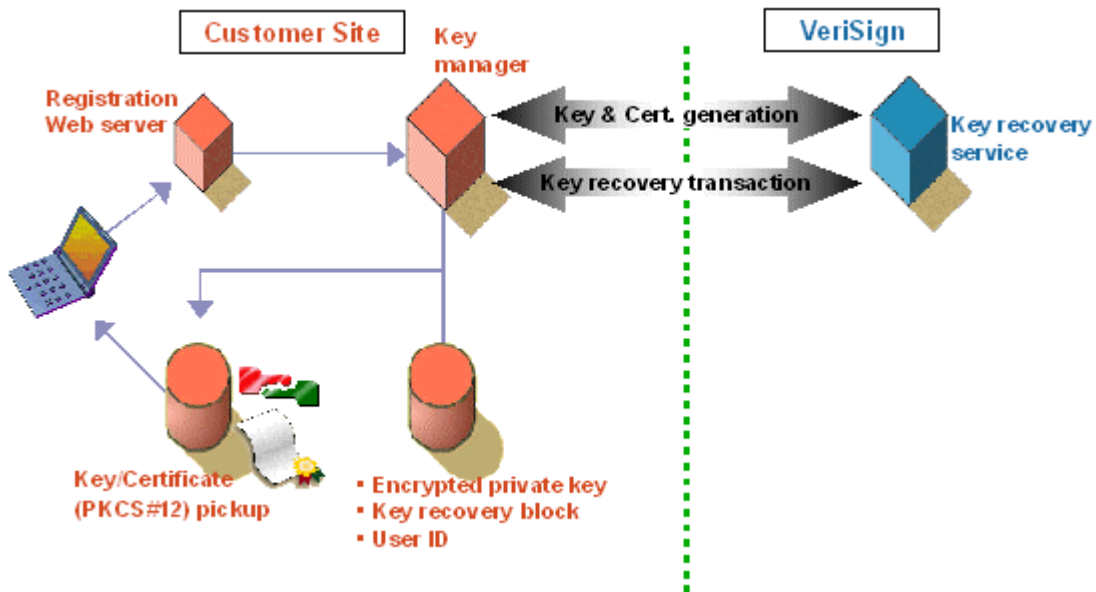
The administrator must be authorized to execute key recovery, and every key recovery transaction is audited by VeriSign. If you suspected a compromise (such as one by a rogue Administrator) you could review which keys were recovered by that Administrator and simply revoke and reissue them. There is no way for an Administrator to cover his or her tracks. Finally, VeriSign can monitor the system for unusual levels of activity and notify a contact at the customer site if unusually high numbers of requests are detected. VeriSign could send an alert to a different point of contact asking for confirmation.

The difference in security between a recovery service such as that used by Go Secure! and a product-based solution is like the difference a safety deposit box within a trusted bank and a safe with a combination lock. The bank grants access to the safety deposit box only to authorized account holders, and does not know what is in the box, maximizing the security of its contents. But if someone guesses the combination to the safe, he or she gains access to everything in the safe. Only by adding this service component do you get truly reliable key recovery.

An important consideration in setting up a secure messaging solution is whether to implement dual-key or single key-pair certificates. In the case of dual keys, separate key-

pairs and certificates are issued for signing and encrypting. The encryption private key is stored in the key recovery database, while the signing private key stays on the user's client (and nowhere else). That way, the administrator can access the user's encryption private key (in case it is lost), but never sees the signing private key (thereby ensuring that there is no question of authenticity for signed messages). However, in dual-key implementations, most non-Microsoft e-mail clients (such as Netscape) do not support dual keys and therefore are not able to receive dual-key signed messages. Thus dual keys limit extranet interoperability.

The other approach, also supported by VeriSign's Key Recovery Service, is a single key-pair solution. In this case, the key manager centrally generates the key pair, stores the private key, and exports it to the user's client. One certificate is used for both signing and encrypting. VeriSign's Key Recovery Service is unique in that it can also support non-repudiation with single key-pairs. If there is every any question of a private key compromise by a rogue administrator, then the audit logs at VeriSign can be checked to determine whether or not the user's private key was ever recovered, when, and by whom. This is unique capability is only available with VeriSign's Key Recovery Service, and ensures that extranet interoperability with a variety of S/MIME e-mail clients is possible.



V. Overview of Implementation

Go Secure! for Microsoft Exchange is implemented as follows:

1. Ensure proper server and desktop configurations.
 - a. Server Requirements: 5.5 SP1 or later
 - b. Client Requirements: Outlook 98 or 2000 (with IE4 or IE5)
2. Identify naming conventions for setting up Certificate Authority (CA).
 - a. Maps to Exchange directory naming

- b. Naming in user's certificate matches Exchange server site name (OU) and domain name (O)
 - c. User certificate DN matches user's DN name in directory
- 3. Determine key recovery configuration
 - a. Single vs. dual key (note: dual-key configuration will limit extranet S/MIME interoperability as most non-Microsoft clients do not yet support dual key—see section on Key Manager architecture for further detail)
 - b. Non-repudiation is supported with single-key pairs because VeriSign's Key Recovery Service key access audit trail tracks who has accessed a user's key.
- 4. Enroll for OnSite CA.
- 5. Determine CDP location (customer-hosted).
- 6. Identify authentication model.
 - a. Authenticated Network log-on option (automatically authenticates and approves certificate request based on user NT credentials). This option is the default authentication packaged with Go Secure!.
 - b. AutoAuthentication against some other database (refer to OnSite documentation).
- 7. Install OnSite local hosting site kit.
 - a. Includes auto-configuration for your Exchange environment.
- 8. Set up enrollment Web server (IIS with NTLM authentication).
- 9. Set up AutoAuthentication.
 - a. Implement authentication model (see step 6).
- 10. Configure CRL retrieval and storage.
- 11. Set up Key Manager.
- 12. Set up HTML for user enrollment and acceptance pages.
- 13. E-mail enrollment URL to users.

VI. Features and Benefits Summary

- **Directory Integration:** OnSite certificates are published directly to the Exchange Global Address List
 - There's no need to set up, synchronize, and support another directory for S/MIME certificates.

- Certificate retrieval for encrypting is automated using Outlook.
- **Client Integration:** E-mail clients are integrated with Outlook 98 or later.
 - This minimizes desktop deployment, support, and end-user training requirements.
- **Interoperability:** Go Secure! for Microsoft Exchange leverages the VeriSign public hierarchy.
 - There are no root deployment issues to worry about. And Go Secure! does not require administering and supporting explicit trust relationships or cross-certification in order to have external trust.
 - Go Secure! enables very scalable secure extranet messaging solution.
- **Authentication Options:** Options include Windows NT user names and passwords and/or additional database (e.g. pin or HR database).
 - Multiple authentication options simplify end-user roll-out.
- **Flexible Key Management Options:** Options include single- or dual-key.
 - Non-repudiation is supported by both options.
 - Single-key allows broadest extranet interoperability.

VII. Summary

VeriSign Go Secure! for Exchange makes it easy to deploy and support secure messaging within your organization. It automatically publishes your end-users' certificates to your Exchange directory, making it easy for them to send each other encrypted messages. It also integrates natively with Outlook 98 or 2000, so there's no new client software required—streamlining deployment, support, and end-user training. And Go Secure! leverages the VeriSign roots that are embedded in millions of e-mail clients and browsers, which means that your certificates will automatically be trusted by your external partners, suppliers, and customers.

For more information about VeriSign Go Secure! for Microsoft Exchange, VeriSign OnSite services, and the entire family of VeriSign enterprise trust solutions, visit www.verisign.com. To learn more about VeriSign Authentication Services, contact a Sales Representative at 650-429-5115, or send an e-mail message to verisales@verisign.com.

VeriSign, Inc.
1350 Charleston Road
Mountain View, CA 94043
Phone: 650-961-7500
Fax: 650-961-7300

© 2000 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, OnSite, and Go Secure! are trademarks and service marks or registered trademarks and service marks of VeriSign, Inc. 4/00