



Secure Messaging for Your Enterprise E-mail

[Go Secure! for Exchange Solution Description](#)

Trusted Internet Services from the Sign of Trust on the 'net.

VeriSign Go Secure! for Microsoft Exchange Solution Description

Introduction:

Imagine trying to operate your business without email, as we all have on occasion when our company email systems are down temporarily for one reason or another. Email is the virtual nervous system with which we communicate internally with fellow employees and externally with our business partners and customers.

Businesses, governments, and institutions depend on email for all types of communications, and at times use it to transmit extremely sensitive information. Internally, this may include human resource, payroll, and other confidential data. And externally, we routinely send sensitive information (such as pricing information, design specifications, legal documents, and purchase orders) over the open internet to and from remote employees, other divisions within our companies, business partners, suppliers, legal counsel, and customers.

Imagine the risk of having your competitors access and monitor all email 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.

The risk is real. ***In a recent security survey, 68% of companies characterized messaging misdemeanors as widespread, with losses estimated at \$3.7 million per company a year*.***

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 public, insecure areas at some point or another. And regardless, as with most fraud, computer crimes are often 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 have been difficult to deploy, support and use.
- Lack of interoperability between different email clients.
- Scalability of vendors' security solutions.

Fortunately, things have changed:

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

Go Secure! for Exchange works with existing 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 for automatic publishing of OnSite issued digital certificates to the existing Exchange global directory and the automatic retrieval of certificates for encrypting and signing of sensitive email 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 email.

According to a recent review by PC Week** of VeriSign's Go Secure! for Microsoft Exchange:

- "GoSecure 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 PC’s and users can perform activation.”
- “The benefit to Go Secure is ease of administration.”
- “For companies that need secure Exchange email, VeriSign’s Go Secure for Microsoft Exchange service fits the bill. Less expensive than setting up and maintaining an in-house PKI, the product also affords tight integration with Exchange.”

Solution Overview:

VeriSign’s Go Secure! for Microsoft Exchange is a 7x24, enterprise-class digital certificate service which 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 email 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

Go Secure! for Microsoft Exchange service components include:

Exchange Subscriber Enrollment:

- HTML and scripts to control user enrollment process.
- Flexibility to customize to fit your corporation’s look and feel.
- Automatically populates users’ enrollment forms with their Exchange certificate content, greatly reducing the chance for enrollment errors.

Exchange Directory Integration:

- Search utility retrieves user’s name, email address and organizational information from the GAL during enrollment.
- Automatically publishes end-user certificates to the GAL.

NT AutoAuthentication:

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

Exchange Certificate Policy Manager:

- Conforms certificate content to meet Exchange directory formatting requirements.
- Certificates are interoperable with non-Microsoft S/MIME client recipients.
- Issues certificates linked to the VeriSign Trust Network, eliminating the need for you to set up explicit trust relationships with your external business partners, suppliers, or customers. Your certificates will automatically be trusted by recipients with any major S/MIME compliant email client.
- Enforces uniform policy for all end-user enrollments including certificate content, key usage, and VTN directory publishing.

Documentation:

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

7 X 24 Global Operations Center:

- High availability data centers with full redundancy and disaster recovery.
- Proven scalability to millions.
- Maximum-security facilities, built using DOD specifications.
- Binding Service Level Contracts.

VeriSign's Go Secure! Service for Microsoft Exchange is continuously upgraded to ensure 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.

End-User Experience:

Go Secure! is easy to deploy, support and easy to use. As mentioned earlier, one of the deployment barriers with previous secure messaging solutions has been ease of use. Go Secure! was designed to make the end-user enrollment process very simple, and also make it very easy for end-users to send secure messages without having to understand PKI.

A typical enrollment process would be as follows:

1. Exchange or Security administrator sends an email to users with instructions and a URL to start the enrollment process. The user clicks on the embedded URL, which takes him/her to the enrollment pages.
2. The user is prompted to enter their NT log-on credentials (NT username and password) for purposes of authentication. The enrollment server uses the NT credentials to find their entry in the GAL, and their friendly name, email 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. AutoAuth will then automatically approve the certificate request, pass the certificate request on to key manager to generate the key-pair, and then the approved certificate request and user 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 their client.
4. The user's certificate is published to the Exchange GAL, making it easy for other users within the organization to access their certificate (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 email.

The user interface for sending signed and encrypted emails from Outlook 98 or 2000 is done through signing and encryption icons which are added to the Outlook toolbar. When a user selects the signing icon, the message is encrypted with their own private key, thus ensuring to the recipient that the message really came from them (authentication and non-repudiation) and was not tampered with (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, which means the signed messages will automatically be trusted by the recipient's S/MIME client (even if they are not VeriSign users themselves).

Confidentiality can be accomplished by encrypting the message with the recipient's public key, which Outlook will automatically obtain from the recipient's certificate in the GAL (if an internal employee) or the sender's local contacts folder (for external recipients). All the user has to do to encrypt the email is to click on the encryption icon on their toolbar.

If the sender does not have an external recipient's certificate, then they can search 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 them a signed email, and the user can then add the certificate to the person's entry in the Contacts folder by simply right-clicking on the address field.

Key Management Architecture:

With VeriSign's Key Manager, the approved enrollment form requesting the certificate is sent to the Key Manager which generates the key pair, sends the public key to VeriSign, and then the signed certificate is returned to the Key Manager, and the Key Manager sends the private key and certificate to the user. This is provided to the end 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 first escrowed).

The 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 in that if someone steals the database, they would have to crack a different 3DES key for EACH private key.

For a key recovery operation – the Administrator goes to the database and retrieves the user record, sends the key recovery block to VeriSign, VeriSign verifies that this is an authorized request (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 okay the transaction by providing the 3DES key.

The administrator must be authorized to do key recovery AND every key recovery transaction is audited by VeriSign, so if you suspected there was a compromise (e.g. by a rogue Administrator) you could review which keys were recovered by that Administrator and simply revoke and reissue those. There is no possible way for an Administrator to cover his/her tracks. Finally, VeriSign can even monitor the system and if there is an unusual level of activity, can notify a contact at the customer site, for example, there are normally an average of 5 recoveries per week and then one day there are 100 requests. VeriSign could send an alert to a different point of contact asking for confirmation.

In summary, having a product solution versus this type of recovery service, is like the difference between having a really strong safe with a good combination (but if someone guesses the combination, and gets into the safe they have access to everything in the safe), and having a safety deposit box within a trusted bank, which only grants access if I am authorized, where you need the bank to grant access, but they can't see anything in the safe. (With Key Manager, the safe isn't even at VeriSign, it's at the customer site.) Only by adding this service piece do you get truly reliable key recovery.

One of the considerations in setting up a secure messaging solution is whether to implement dual key or single key-pair certificates. In the case of dual key, 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 there is no question of authenticity for signed messages). The issue with dual key implementations is that most non-Microsoft email clients (e.g. Netscape) do not support dual key, and therefore will not be able to receive dual key signed messages. Thus, imposing dual key greatly restrains 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, because 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 a unique capability that is only available with VeriSign's Key Recovery Service, and ensures that extranet interoperability with a variety of S/MIME email clients is possible.

Overview of Implementation Steps

At a high level, the implementation steps are 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 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 cert 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 pair, 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. Auto auth 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 Auto Auth
 - 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. Email enrollment URL to users

Features and Benefits Summary:

- **Directory integration:** OnSite certificates published directly to the Exchange Global Address List
 - Don't have to setup, synchronize, and support another directory for S/MIME certs
 - Certificate retrieval for encrypting is automated using Outlook
- **Client:** Integrates with Outlook 98 or later
 - Minimizes desktop deployment, support and end-user training requirements
- **Interoperability:** Leverages VeriSign public hierarchy
 - No root deployment issue to worry about, does not require administering and supporting explicit trust relationships or cross-certification in order to have external trust.
 - Enables very scaleable secure extranet messaging solution.
- **Authentication options:** NT user name and password and/or additional database (e.g. pin or HR database)
 - Simplifies end-user roll-out.
- **Flexible key management options:** Single or dual key
 - Non-repudiation supported with both options
 - Single key allows broadest extranet interoperability

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 users to send each other encrypted messages. It also integrates natively with Outlook 98 or 2000, so there's no new client software required – which greatly simplifies deployment, support and end-user training. And Go Secure! leverages VeriSign's roots that are embedded in millions of email clients and browsers, which means your certificates will automatically be trusted by your external partners, suppliers, and customers.