GlobalCerts

PRODUCT OVERVIEW:

The GlobalCerts™ SecureMail Gateway™

Automatic encryption and decryption is unique to the SecureMail Gateway.

The GlobalCerts SecureMail Gateway is based on a network server appliance that automatically encrypts outgoing Internet email whenever possible. It also decrypts incoming encrypted Internet email automatically and delivers it to the existing mail infrastructure. The SecureMail Gateway even allows users to send encrypted email to people who have nothing more sophisticated than a basic web browser. It installs with a minimum of effort and requires no software to install on user desktops or corporate mail servers. It is standards-based, using X.509 compatible public key certificates with standard email formats and protocols..

GlobalCerts™ SecureMail Gateway™

The GlobalCerts email security solution is based around a network appliance, the GlobalCerts SecureMail Gateway. This appliance is installed on the enterprise network and is configured to encrypt and decrypt email that goes out to or comes in from the Internet. Automatic encryption and decryption is unique to the SecureMail Gateway.

To perform its automatic encryption and decryption, a SecureMail Gateway manages X.509 compatible public key certificates for each email user. It stores both the public key and the private key securely inside the appliance. The Gateway can be configured to always encrypt outbound email, or to only encrypt it when sent by selected users. If the recipient has an X.509 certificate that is discoverable by the gateway, mail is always encrypted using the public key in that certificate.

Even when the email recipients have no cryptography software and no SecureMail Gateway of their own, they can receive secure email from SecureMail Gateway users. Furthermore, the messages are protected by the same high-quality public key cryptography that protects normal encrypted email. This is the SecureMessenger™ feature described on page 4.

GlobalCerts has also made the SecureMail Gateway as unobtrusive as possible. Users keep the same desktop email software they have always used, their email addresses stay the same, and they continue to use any groupware (such as Novell® GroupWise®, Microsoft® Outlook, or Lotus Notes®) normally. The primary change they will notice is the presence of cryptography summaries at the bottom of email messages, indicating whether or not the message was encrypted in transit.

There is nothing to configure on users' desktops.

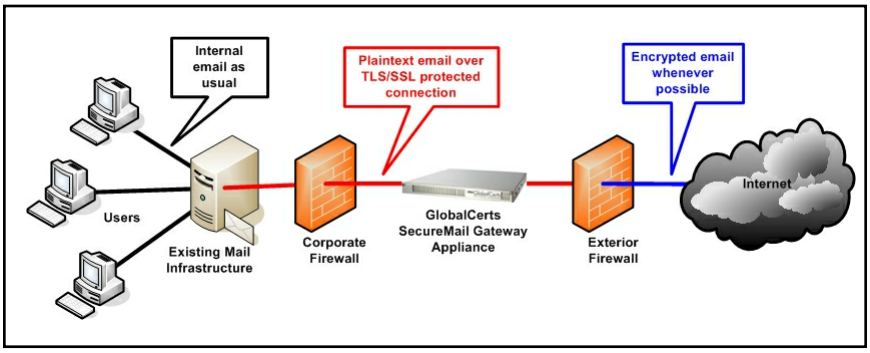

Figure 1: Overview of the Architecture

Email Security Architecture

A Proxy Architecture

The SecureMail Gateway provides a variety of email security services and features. It provides these features by working as a proxy between mail servers, or between external recipients and the organization.

The SecureMail Gateway's role as a proxy gives us maximum flexibility to accommodate your needs, without disrupting your business.

Standard Features: For Gateway Users

Automatic Encryption: When it is configured to always encrypt, the SecureMail Gateway, using standard S/MIME encryption, automatically encrypts messages for all recipients who have certificates that it can discover, as well as all recipients who have a SecureMessenger template. When it encounters a recipient who has neither, it prompts the sender to create a SecureMessenger template for that recipient.

Our simple installation means that your organization gets a substantial new service, but your IT staff does not get a substantial new burden.

Automatic Decryption: Encrypted email is decrypted automatically as it arrives at the organization. This feature allows for maximum compatibility with existing mail servers and mail filtering systems like virus scanners and keyword-based policy systems.

Transparent Operation: The SecureMail Gateway automatically creates users and their associated key pairs when they first send mail through the gateway. Alternatively, an administrator can designate which users will have their mail encrypted.

Compatibility means you keep your existing infrastructure and make just enough changes to add email security to it.

Simple Installation: The SecureMail Gateway is a network appliance and is installed in the network near the mail firewall. It requires very little work to install or configure. The SecureMail Gateway can be installed without making a single change to a user's desktop computer. No software is needed, no settings are altered, and no email addresses change.

Server Compatibility: The SecureMail Gateway is compatible with Microsoft® Exchange, Novell® GroupWise®, IBM® Lotus Domino®, and all standards-based (SMTP, POP, IMAP) mail software. The Gateway inter-operates with all components of the existing infrastructure, including advanced features like web access to email, anti-virus scanning, and content filtering.

If you have made an investment in PKI technology, you can choose to continue to use that technology in conjunction with the SecureMail Gateway.

Standards Compatibility: Each SecureMail Gateway appliance generates X.509 v.3 compliant digital certificates for their users. However, users can replace these certificates with X.509 certificates issued by other certificate authorities, for encryption and decryption operations. SecureMail Gateway appliances automatically detect and harvest new certificates for future use when they are attached to incoming email messages.

SecureMail Gateway™ Sending Securely to Certificate Holders

It's simple for anyone to initiate a secure message to someone else. They just type the email address a little differently.

All SecureMail Gateway appliances publish the certificates of their users in SecureTier™, GlobalCerts' global certificate management system. When a GlobalCerts SecureMail Gateway receives an outgoing message that is prepended with secure-, it looks for the recipient's certificate in SecureTier. If it finds it, it retrieves the certificate, validates it, and then encrypts the message using the public key contained in the certificate. If the certificate cannot be found in SecureTier, the SecureMail Gateway then checks its local certificate-harvesting repository to see if the certificate can be found there.

If the recipient's certificate is found, the Gateway uses the public key in that certificate to encrypt the email. Thus the Gateway can discover certificates in one of two ways.

If certificates can be found for the recipient, the SecureMessenger™ feature is not used. Instead, the recipient gets secure mail as usual.

1. If the certificate belongs to a user of a SecureMail Gateway, it will be published in SecureTier, and any other SecureMail Gateway will automatically and transparently discover it by looking it up in SecureTier using the recipient's email address;

2. If the certificate does not belong to a user of a SecureMail Gateway (i.e. it is not published in SecureTier) any gateway that encounters it will place it in its harvested-certificate repository. Thus when a SecureMail Gateway looks for a certificate, it first checks in SecureTier, and then looks for it in its local harvested-certificate repository.

SecureMessenger™: Sending Securely to Everyone

SecureMessenger™ is a feature integrated into the SecureMail Gateway, which allows users to easily and automatically encrypt email messages sent to recipients that don't have a certificate, or don't have a certificate that is discoverable by the SecureMail Gateway. SecureMessenger™ makes it safe to send sensitive information by email—customer financial information, PHI (Personally- identifiable Health Information) records or data, confidential legal documents, etc. Now information can be sent securely to any recipient in the world, even if they have nothing more sophisticated than a basic web browser.

If the gateway is configured to send all messages securely, and the recipient doesn't have a discoverable certificate, SecureMessenger is automatically invoked.

The SecureMail Gateway can be configured to always send these messages securely, or to only do it when the message is prepended **by secure-**.
Here's how it works, step-by-step, when encryption is optional:

1. 1. You prepend **secure-** to the recipient's email address, or place **[secure]** in the Subject line. For example, if your recipient's address were fredsmith@example.com, you would need to type **secure-fredsmith@example.com** into your To: field;

2. The SecureMail Gateway stores the message you're trying to send and immediately sends back to you a secure email message with a URL link to your own local SecureMail Gateway appliance;

A SecureMessenger template can be reused as often as required.

3. You connect to your SecureMail Gateway, over an SSL-secured Web connection, in order to enter a clue and a passphrase for your recipient. They will later use that clue to determine the passphrase, allowing them to read the email message. You can also request to be notified when the message is retrieved, and establish a lifetime for the message. After this lifetime has expired, the message is destroyed. Lastly, you can save these values in a template, as standard values you'll use every time you communicate with this recipient. You are then only prompted for the clue and passphrase once per recipient, when you initially create the template. After you submit this information, the SecureMail Gateway creates a temporary key pair, encrypts the message with the public key, and encrypts the private key with the passphrase.

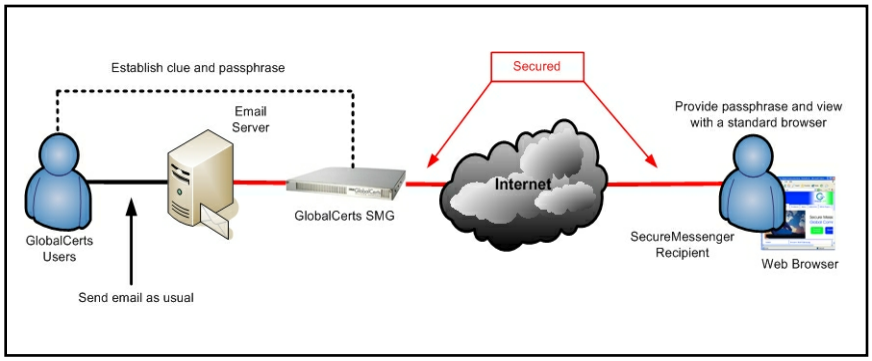

Figure 2: SecureMessenger™

4. The SecureMail Gateway immediately notifies your recipient that they have a secure message waiting for them. They receive a simple email message with a private Web link to a secure Web page hosted on the sender's SecureMail Gateway appliance;

You can communicate securely with colleagues as easily as adding 'secure-' to their email address.

5. The recipient clicks on the private Web link, establishing a secure Web connection (using SSL) to your SecureMail Gateway. They are prompted with the clue and asked for the passphrase;

6. When the recipient types the correct passphrase, their temporary private key is unlocked, the message is decrypted and displayed, and the recipient is easily able to download any attachments you included-all across the secure Web connection that has been initiated;

Your recipient uses a web-mail interface, but you always use your email software as usual.

7. Your recipient can also reply to you securely: they type their reply message in the Web browser window and upload any files to be sent. Their message and all of its attachments are then encrypted and sent securely to you, the original message sender. Until the original message expires, the recipient can reply to you as many times as they would like;

8. You receive their reply as a secure email message in your mailbox as usual. Any files they uploaded are attachments to the message. You don't have to do anything special to receive them.

The SecureMessenger is easy to use, and requires minimal user training. With GlobalCerts you spend your time in familiar email software. There's no special Web site for initiating or receiving these messages, and secure replies come to your regular email inbox in the usual way. For increased security, SecureMessenger™ messages are stored at all times on your Gateway, not with any third party. Your secure information flow does not depend on any other company, and the keys that decrypt messages are stored solely within your company's trusted intranet.

SecureTier™

DNS is fast, hierarchical and efficient. SecureTier solves the problem of finding public keys for encrypting messages.

Finding Public Key Certificates Quickly and Easily

Another standard feature of all SecureMail Gateway appliances is their connection to SecureTier™, GlobalCerts' global certificate management system. One of the biggest hurdles to using public keys to encrypt email is the problem of discovering public key certificates for all the recipients of email messages. The difficulty of finding certificates for email encryption is a major obstacle to large-scale adoption of email encryption systems, and GlobalCerts has created SecureTier™ specifically to overcome this barrier. In order to encrypt an email message, a certificate must be found for every intended recipient. If the recipient does not have a certificate that can be discovered, another secure delivery mechanism, (such as SecureMessenger) must be used.

SecureTier™ leverages DNS technology - the same fundamental Internet technology that resolves domain names into IP addresses - to provide a global public certificate discovery and retrieval system. SecureTier enables public key certificates to be found quickly and easily, based on the Internet email address of the recipient. No other technology is as fast, as scalable, or as robust.

Every SecureMail™ Gateway user certificate is published in SecureTier™, significantly simplifying inter-organizational secure communications, since knowledge of an email address is all that is required to discover the certificate of any SecureMail™ Gateway user. Any SecureMail Gateway can find the certificate of another SecureMail Gateway user via SecureTier™- and then use it to encrypt their email messages.

Because SecureTier™ is so fast and scalable; SecureMail Gateway appliances look for encryption certificates for all recipients of all messages all the time by default. This is a unique benefit that only GlobalCerts can offer. No other key distribution and discovery system is so efficient that key lookup can be performed on every message as a matter of course.

Compatibility with Existing PKI Technology

There are two fundamental ways in which the SecureMail Gateway utilizes certificates that are issued by other X.509-compliant secure email systems. It can encrypt messages using public keys harvested from incoming email messages that are received, and it can use key pairs generated by other X.509-compliant PKI software for its own internal users.

Using Recipients' Certificates Automatically

If your colleagues have certificates from another PKI vendor, they need only send you a message digitally signed with their certificate. The SecureMail Gateway harvests the certificate when it is first received. If the certificate successfully validates, it is stored in the SecureMail Gateway. The next time you (or any other user of your SecureMail Gateway) try to send that person email, the SecureMail Gateway automatically finds their certificate and uses it to encrypt your message. If the harvested certificate fails to validate, it is placed in a queue for administrative attention. The administrator can then inspect the certificate validation chain, and determine the appropriate action.

Using A Certificate from Another CA

If you have a certificate from another CA, such as Digital Signature Trust Company or Verisign®, you can upload that certificate and its corresponding private key, and the SecureMail Gateway will use that key pair automatically. Email messages you send encrypted will be digitally signed with that private key, and any incoming email will be encrypted using the public key contained in the matching certificate.

Encrypted messages generated by the SecureMail Gateway are compatible with existing S/MIME standards. All X.509 certificates issued by SecureMail Gateway appliances are X.509 version 3 compliant, with support for extensions popular in modern browsers and email software.

Compatibility with Existing E-mail Infrastructure

This kind of compatibility sets the GlobalCerts Email Security Solution apart.

GlobalCerts actively tests its products with many well-known email software products and platforms to assure support and interoperability. GlobalCerts also complies with standards such as S/MIME, X.509, and RSA Security's PKCS series of standards. Since no software is installed on the desktop computers or mail servers, the SecureMail Gateway is compatible with many email software products that are standards-compliant, but may not have significant market presence. The following page contains a list of major commercial software that has been formally tested with the GlobalCerts SecureMail Gateway.

E-mail Server Software

- Novell® GroupWise® 1
- Lotus® Notes™
- Microsoft® Exchange
- UNIX® send mail
- SMTP-based mail servers
- UW IMAP and POP servers

E-mail Client Software

- Novell® GroupWise®
- Lotus® Notes™
- Netscape™
- Microsoft® Outlook™
- Microsoft® Outlook Express™
- Eudora

SecureMessenger™ has been tested with Netscape, Internet Explorer, the AOL® web browser, the EarthLink™ web browser, and several text-only web browsers (such as those used by the visually impaired).

Implementing Email Security

This is the baseline configuration. There are a variety of options available to meet special needs, but this covers the essentials.

The GlobalCerts SecureMail Gateway thoroughly protects your organization's email messaging. It requires very little, if any, reconfiguration of your email environment.

Inbound Email

Inbound mail passes through the SecureMail Gateway first.

The SecureMail Gateway must be the inbound mail exchanger (MX) for the organization. This means that when email comes in from the outside world, it will pass through the SecureMail Gateway before being delivered to any other email servers. This allows the SecureMail Gateway to provide seamless, automatic decryption of encrypted email. If your organization uses a virus scanner or other mail filter software, the SecureMail Gateway can send the decrypted mail to that system for filtering and scanning..

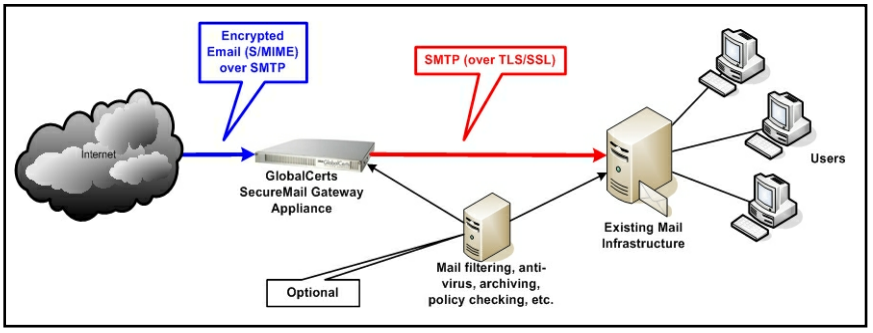

Figure 3: Inbound Mail Flow

The SecureMail Gateway is compatible with virus scanners and all other mail filtering software.

If your organization uses any kind of mail filtering software, such as an anti-virus scanner or mail archiving server, it will continue to operate normally. Messages are decrypted prior to being scanned. No other approach to automatic email encryption exists that can so easily accommodate virus scanners and mail filtering systems.

Outbound Email

Outbound mail passes through the SecureMail Gateway last.

The SecureMail Gateway must be the last stop for email outbound to the Internet. This means that if you already have an email server (such as Lotus® Domino™ or Microsoft® Exchange), you must direct it to send all outbound email to the Gateway for final delivery to the Internet. The messages, not yet encrypted, can be protected by SSL communications as they travel between your existing mail server and the SecureMail Gateway. After the SecureMail Gateway performs encryption operations, the messages are released to the Internet using SMTP as usual.

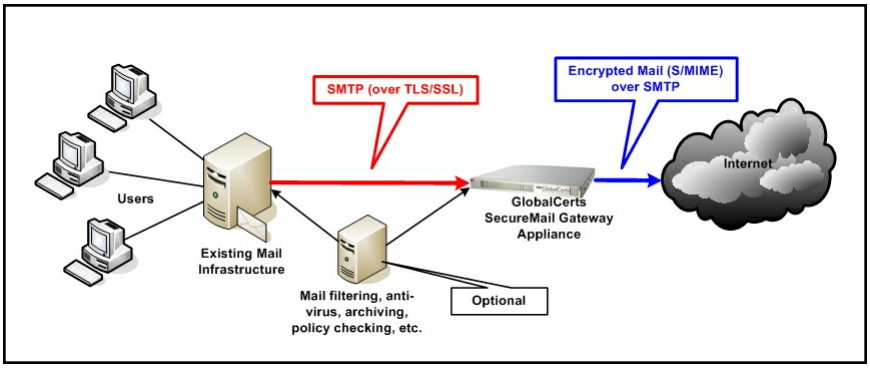

Figure 4: Outbound Mail Flow

Many companies employ an outbound mail scanner that enforces company policy, performs content filtering, scans for viruses, or perhaps archives all outbound messages. SecureMail Gateways are compatible with all such systems since SecureMail Gateways are involved only at the very last stage, when mail has been processed and is approved for release to the Internet.

On the Network

The SecureMail Gateway requires few local network accommodations. It needs DNS names, IP addresses and the ability to accept certain connections through the firewall. These firewall requirements are detailed in a separate checklist available from your GlobalCerts sales representative.

Managing the SecureMail Gateway™

SecureMail Gateway appliances are managed through a secure Web interface. Using a web browser, a user ID, and a passphrase, an administrator can manage all the functions of a SecureMail Gateway: users, their certificates, and the appliance itself. Accounts can be managed individually or in bulk, and various options can be modified and customized to make your SecureMail Gateway enforce the email policies and presentation style of your organization.

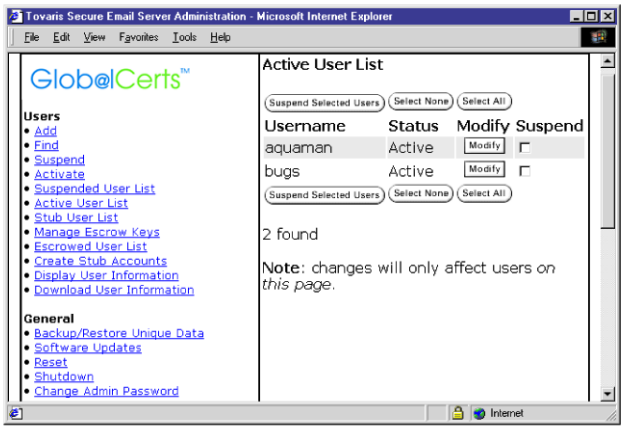

Figure 5: Web-based Administration

Advanced Options

Redundancy

GlobalCerts can provide hot spares so that encrypted email is always available.

Because email is a mission-critical communications service, GlobalCerts can provide redundant “hot spare” SecureMail Gateway appliances to make sure encrypted email is always available. One SecureMail Gateway is active as a master at all times and is providing email encryption services. The other is actively in contact with the master, ready to take over its duties in the event that it should fail.

It's easy, it's safe, and it works seamlessly with your existing systems.

Summary

The GlobalCerts SecureMail Gateway protects corporate email when it is most vulnerable—outside the corporate intranet. It is designed to minimize the disruption of existing workflow and mail infrastructure and protect as many email messages as possible, with strong, military grade encryption. Importantly, the integrated SecureMessenger™ feature, allows secure messages to reach every email recipient in the world through a simple Web-based interface. SecureTier™ provides scalable distribution of certificates and the fastest discovery of certificates for encryption.

Because the risks are too great to your business, and confidential communications can't be privately conducted using unencrypted email, the GlobalCerts SecureMail Gateway offers a cost-effective and complete solution to protect your email as it travels across the Internet.

Features

- Encryption and decryption performed in the Gateway
- Support for both S/MIME and SSL email links
- Transparent operation and key management
- Compatible with standard email clients
- Each user is provided with a separate x.509 certificate
- Can be deployed with content triggered encryption
- Utilizes SecureTier™ Certificate Management Infrastructure

Benefits

- Enables anti-virus and content filtering functions near the firewall
- Communicates securely with virtually anyone
- No user or administrator actions required
- No software to load on each user workstation
- Allows for end user digital signatures
- Failsafe mechanism for unsophisticated users
- Provides inter-organizational communication capability

100 South Street West
Charlottesville,Virginia 22902
434-245-5300
866-868-2747 (Toll Free)
www.globalcerts.net