GlobalSign Enterprise Solutions

Secure Email & Key Recovery

Using GlobalSign's Auto Enrollment Gateway (AEG)

Table of Contents

Introduction

Many organizations, both large and small, face difficult choices when considering secure data transfer between stakeholder groups. Virtual teams made up of internal colleagues, outside partners and even potential clients find a need to collaborate effectively and securely, requiring cost effective ways to authenticate the integrity of data they receive but also the need to maintain confidentiality.

Now more than ever, data protection is one of the biggest concerns for CISOs and heads of security with solutions needed to cover the encryption of data either at rest or during transmission to other parties. Within this solution guide we will be highlighting the use of S/MIME certificates as a solution, providing a way to maintain confidentiality, as well as proving the integrity and origin of emails and their authors, how GlobalSign's Auto Enrollment Gateway makes provisioning S/MIME certificates easy for the Enterprise and how Key Recovery helps maintain the level of usability for the end-user.

The Benefits of Secure Email

The benefits of digitally signing and encrypting email communications includes:

- Prevent tampering of email content
- Prove message origin
- Prevent exposure of email content
- Flexible and secure communication
- Easy to implement

For further details on the benefits of digitally signing and encrypting email communications please view the GlobalSign Website – Secure Email.

GlobalSign's S/MIME Certificates

GlobalSign's PersonalSign Certificates use S/MIME technology to allow users to digitally sign and encrypt email.

- **Digitally signing** emails protects the origin and authenticity of an email. A digital signature (different from a "message signature" or customizable salutation) adds a unique code to a message which only comes from the Digital ID of the original sender. It also confirms that the content of the email has not been altered in transit.

- **Encrypting** email ensures message privacy. Encrypting email converts the message into (scrambled) ciphertext. Only the intended recipient (who is the owner of the corresponding private key*) can "unlock" the message and view the content in clear text.

  **Both the sender and the recipient must have a digital certificate to use email encryption.*

Secure Email is achieved using GlobalSign's Digital Certificate solution called PersonalSign. PersonalSign Certificates are cryptographic signing certificates that bind your verified, physical identity to the certificate so recipients of email messages can verify that the email actually came from you.

Figure 1 - Digitally Signed Email

Figure 2 - Encrypted Email

Support for Secure Email

GlobalSign's PersonalSign Certificates employ the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol to digitally sign or encrypt emails. S/MIME or Secure/Multipurpose Internet Mail Extensions is the industry standard for public

key encryption for MIME based data. S/MIME Encryption provides Message integrity, authentication, privacy via data encryption and non-repudiation via digital signatures. S/MIME is a standard tracked by IETF and now defined by several RFC's 3851, 3850, 3370, and 3369. S/MIME works by using a data envelope to surround the data entity which is inserted into a PKCS7 MIME Entity (when encrypting).

Most mail clients support S/MIME, such as Microsoft Outlook, Thunderbird, Apple Mail, Lotus Notes, and Mulberry Mail. For a detailed summary of S/MIME compatibility between email clients, please see our S/MIME White Paper.

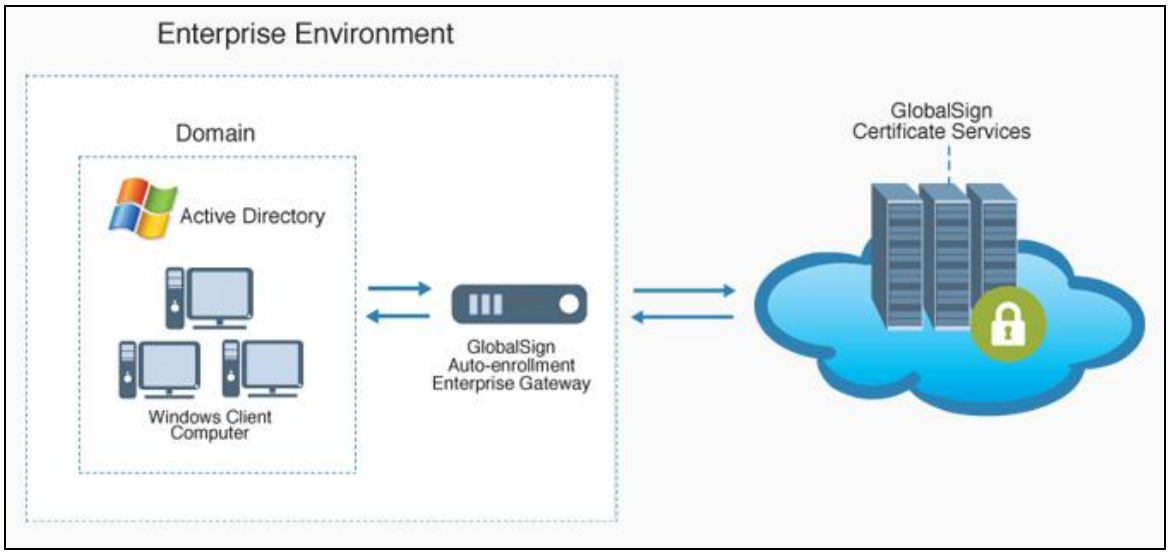
Enterprise Solutions for Secure Email

If your organization is looking to implement an enterprise-wide secure email solution, you are able to use either an internal CA or an external CA depending on your requirements, however using an internal CA to generate a self-signed certificate is not recommended for security reasons. So it is recommended to use an external CA, such as GlobalSign, which has two methods to issue and manage S/MIME certificates.

- **Manually - Enterprise PKI (EPKI):** Enterprise PKI (EPKI) is a cloud-based managed PKI service to issue and manage GlobalSign Client Certificates. The EPKI web portal / APIs provide administrators with a cost effective and easy to use solution to simplify PKI deployments and eliminate the need to host your own Certificate Authority. For more information about EPKI please visit: https://www.globalsign.com/enterprise-pki/
- **Automatically - Auto Enrollment Gateway (AEG):** This is the preferred method for any organization running a Windows environment and Active Directory. AEG is a software service that acts as a proxy between GlobalSign's SaaS certificate services and an organization's Windows environment, simulating aspects of an on-premise Certificate Authority (e.g. Microsoft CA) while forwarding all certificate enrollment requests to GlobalSign. GlobalSign manages the security, high availability, and CA operations, while organizations retain control of users and policies. The gateway can be used to enroll and issue certificates to all types of Active Directory Objects, including users, servers, desktops, laptops, and Domain Controllers.

The remainder of this solution guide will go over the simplicity that AEG introduces to providing secure email.

AEG – How it Works



To understand how AEG works please view this brief video of the solution: https://www.globalsign.com/auto-enrollment-gateway/how-it-works.html#auto-enrollment-diagram.

Example: Sending and Receiving Secure Email

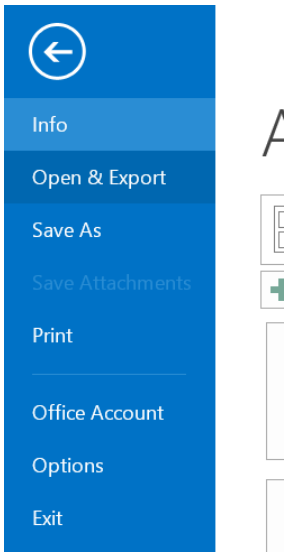
Now that AEG has provisioned the S/MIME certificate to the user's device they will be able to install the certificate into the email client and sign and encrypt email messages. For the following example, this has been demonstrated in Microsoft Outlook 2013. For a complete understanding of email clients and S/MIME compatibility please view the S/MIME white paper.

Installing a S/MIME Certificate – Microsoft Outlook 2013

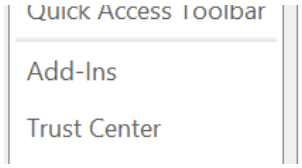
After AEG has installed the S/MIME certificate it will be available for use in Outlook 2013. To use the certificate in Outlook 2013, the user will need to do the following:

1. Open Outlook 2013 and click on **File**.

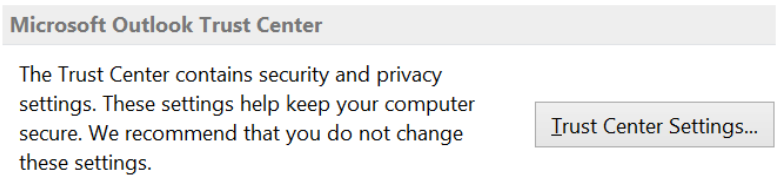
2. Click **Options**.



3. With the Options window open click **Trust Center** in the left-hand menu.

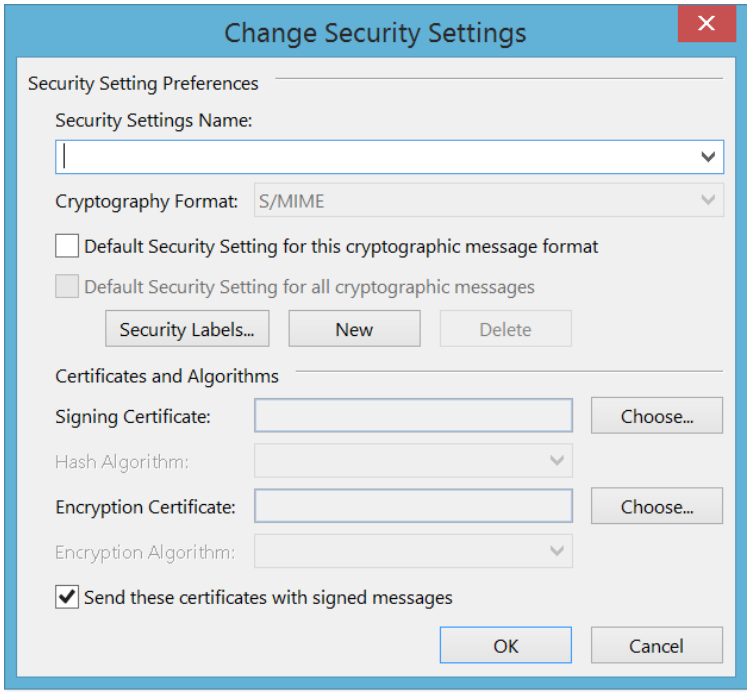


4. Click **Trust Center Settings…**



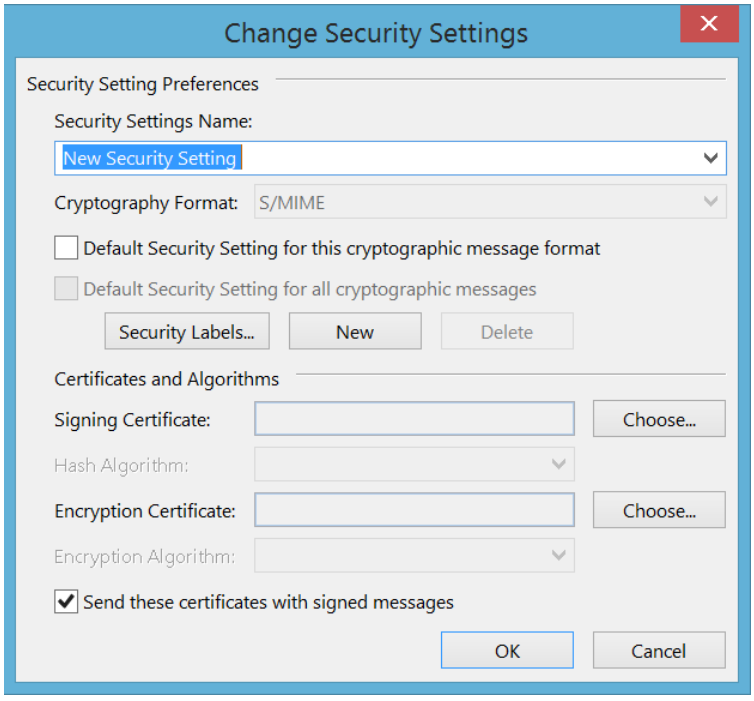
5. Click **E-mail Security** from the left-hand menu.

6. To define your security settings and to specify which certificate you wish to use you need to define your default security settings. To do so, click the**Settings** button. You will then see the following screen:

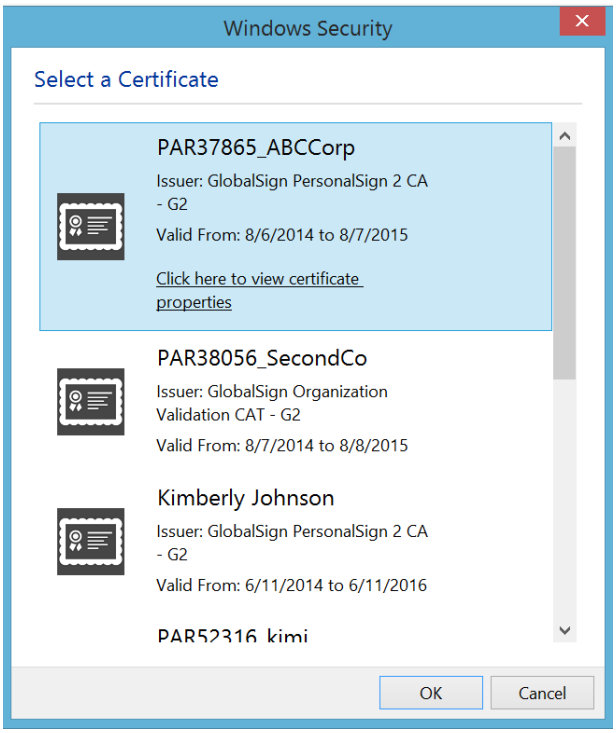


7. You can create different security settings and give these separate names. You can define the following settings:
   - Secure Message Format (type of e-mail)
   - Digital Signature Settings
   - Encryption Settings
   - Security Setting Preferences (setting defaults)

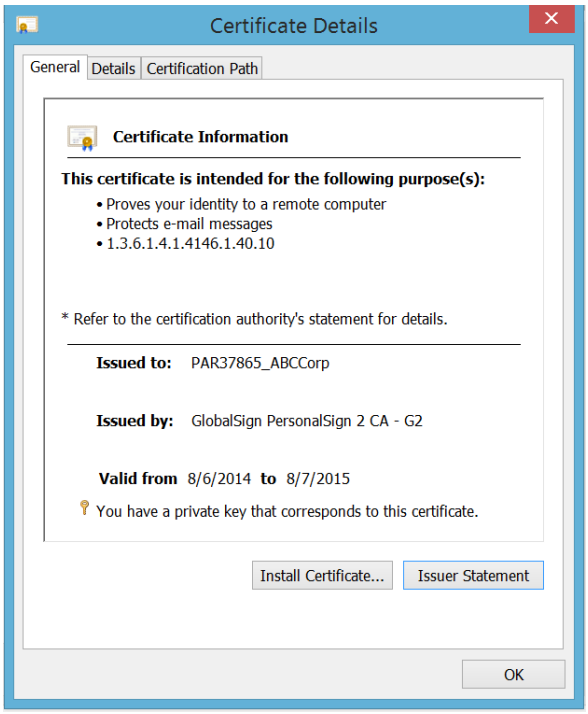
8. The first step is to give your setting a name which you can choose yourself.



9. The **Digital Signature** settings allow you to choose the certificate you wish to use for signing your emails. If you click the **Choose** button you will be presented with a list of your personal certificates.

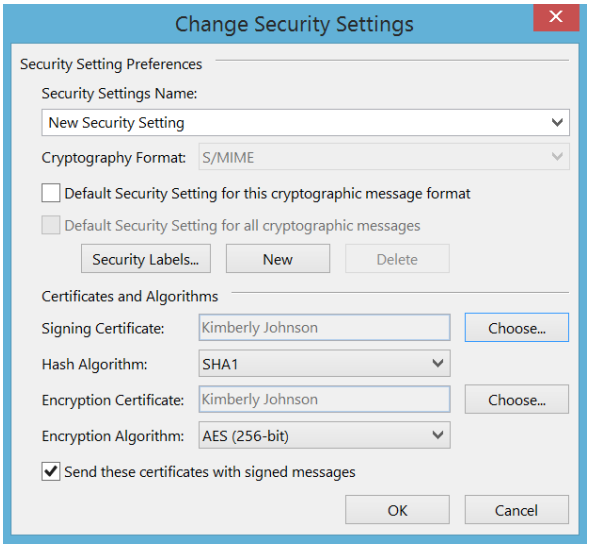


You can view a certificate by selecting it and clicking **Click here to view certificate properties**.



When you find the certificate you want to use select it and click **OK**.

10. The certificate will be added to both the **Signing Certificate** and **Encryption Certificate** box.

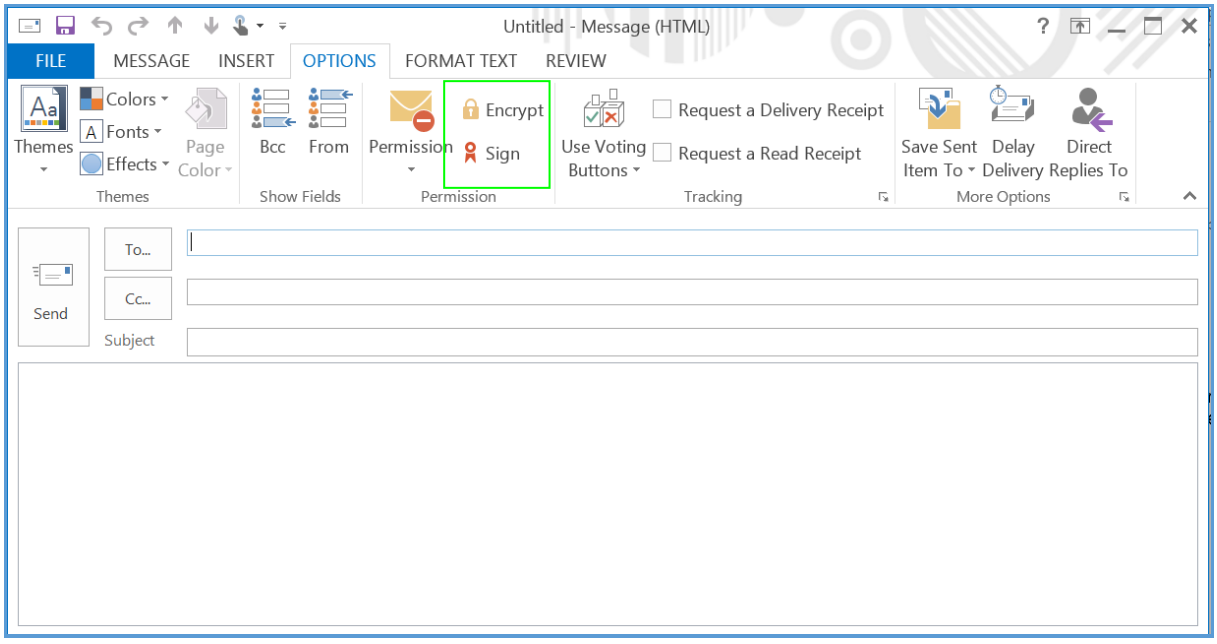


Note, if you wish to change your Encryption Certificate you can do so by clicking **Choose** next to **Encryption Certificate**.

11. Both the **Signing Certificate** and the **Encryption Certificate** settings sections allow you to define which type of hashing algorithm you want to use for the creation of your signatures (SHA-1, MD5, 3DES, etc).

12. Click **OK** to save your Security Settings. Continue to click **OK** to exit the Trust Center and Outlook Options and confirm your changes.

Digitally Signing an Email – Microsoft Outlook 2013



In a new email message, under the **Options** section you will see two mail security icons. The first is the encryption icon. Selecting it will encrypt your email. The second is the signing icon. Selecting this will sign your email with the certificate of your choice.

Note: You will need the public key of your recipient before you can encrypt your email.

Your digital signature enables the recipient of your message to verify that you actually sent the message. It also guarantees the message was not altered en route. Signing your email will also give your recipient your public key. This will allow your

recipient to send you encrypted emails in the future.

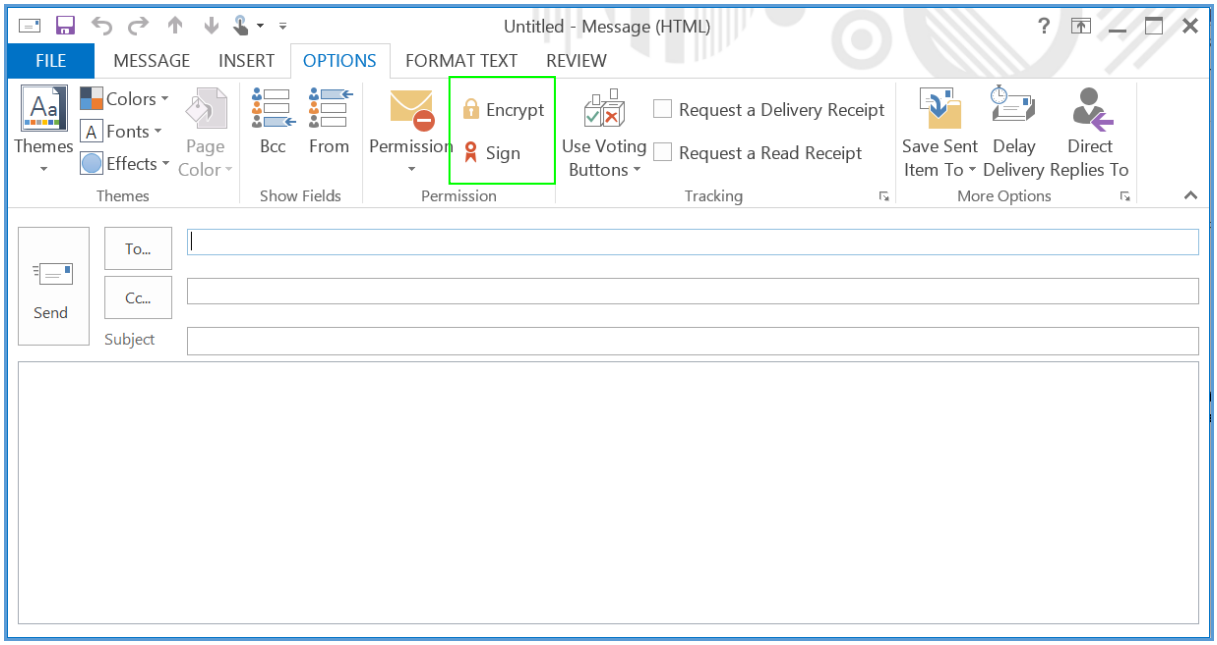
Signing a message does not automatically encrypt the message or prevent it from being intercepted. To ensure that only the recipient can read a message you must be sure to encrypt the message by exchanging public keys with the recipient and clicking the encrypting icon.

If the recipient of your signed message uses an S/MIME–enabled email package he or she can still read your message. In this case, your digital signature will show up as an attachment. The signed icon shows that the received message was signed.

The untrusted signature icon shows that the received message was signed by a certificate which was issued by a CA which you do not trust yet. This is either because you have not installed the CA's root certificate or it has been revoked. This icon looks like:

You can sign your messages each time you want to sign an email or you can configure your security settings (as described previously) to automatically sign using a specific certificate.

Encrypting an Email Message – Microsoft Outlook 2013



To encrypt your message you need to have a copy of the digital certificate of the intended recipient. When you receive a signed email, you can save the certificate of the sender in your Contacts List. You need to create an entry in the Contacts List if you want to send encrypted email to that person. You must also import his or her digital certificate into your Contacts List.

When you receive an email the encrypted icon indicates that the message has been encrypted. This icon appears in the lower right corner (blue padlock) of the address pane. The encryption process is done automatically.

You can encrypt your messages each time you want to encrypt or you can configure your security options so that your messages will be automatically encrypted every time the digital certificate resides in your address book.

When you receive an encrypted message the encrypted icon appears on the email window:

The user has now successfully installed their S/MIME certificate and has signed and encrypted email messages. For more of the benefits to sending and receiving secure emails please refer to the previous section **The Benefits of Secure Email**.

Now that you have a complete understanding of secure email, let's take a look at how Key Recovery can assist users if they are unfortunate enough to lose access to their private key.

What is Key Recovery?

When users lose their private keys, any information that was persistently encrypted with the corresponding public key is no longer accessible. Using key archival and recovery helps protect encrypted data from permanent loss if, for example, an operating system needs to be reinstalled, the user account to which the encryption key was originally issued is no longer available, or the key is otherwise no longer accessible.

Key archival and recovery are not enabled by default. This is because many organizations would consider the storage of the private key in multiple locations to be a security vulnerability. Requiring organizations to make explicit decisions about which certificates are covered by key archival and recovery and who can recover archived keys helps ensure that key archival and recovery are used to enhance security rather than detract from security.

Key Recovery Process Overview

Key archival can be performed either manually or automatically. Manual key archival requires users to export private keys and send them to a PKI or CA Admin who imports them to the protected CA database. Automatic key archival is performed during the certificate enrollment process when a certificate template is configured to require key archival. In AEG, during the certificate enrollment process, the private key is securely sent to the AEG server as part of the certificate request and is archived there. These archived keys never leave your system and are protected.

Note: A private key that is known or suspected to be compromised should be revoked as soon as possible.

Key recovery requires the use of an enterprise-level certificate template called Key Recovery Agent. For this reason, you cannot do key recovery on a standalone CA. Only Enterprise CAs have access to templates. Also, by default, only Domain Admins or Enterprise Admins have access to the Key Recovery Agent template. This is controlled by permissions on the template in Active Directory.

Here is how a Key Archival and Recovery process works:

1. Create a key recovery agent account: By default, the security groups that can enroll the Key Recovery Agent certificate template are Domain Admins and Enterprise Admins. If you would like to add another agent, this can be done through the security settings of the Key Recovery Agent template

2. Acquire the key recovery agent certificate: You need to enable and acquire a Key Recovery Agent Certificate for the purpose of recovering private keys

3. Create a new certificate template that allows key archiving: You can create a new certificate template that allows Key Archival in the Certificates Templates console. This will allow key recovery in the domain in the event that the private key is lost or corrupted

4. Acquire a user certificate that has an archived key: Once the User certificate templates have been configured to archive keys, you can use the CA (AEG) to automatically provision/install certificates with archive keys bit set.

5. Perform key recovery: The PKI Admin/CA Admin can perform Key Recovery using a few certutil commands

6. Import the recovered private key: This is the final step in the process where you import the recovered key into the certificate store of the user who lost their keys.

Conclusion

S/MIME certificates provide a way to maintain confidentiality, as well as proving the integrity and origin of emails and their authors. GlobalSign's Auto Enrollment Gateway makes provisioning S/MIME certificates easy for the Enterprise and its Key Recovery functionality maintains the level of usability for the end-user.

If you are interested in learning more about GlobalSign's AEG solution and how you can implement flexible and secure email communication within your organization please contact the **GlobalSign Sales Team** in your region.

GlobalSign Contact Information

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com