

PGP TrustCenter is a provider of digital certificates which can be used for digital signatures, authentication and encryption purposes. If you do not already have a digital certificate, please visit PGP TrustCenter's website at <http://www.pgptrustcenter.com/digital-certificate-solutions> to obtain a "TC Personal ID" or "TC Business ID".

By obtaining a digital certificate, you now possess a pair of cryptographic keys; a **public key** and a **private key**. The private key should be kept secret and is stored in a secure location on your computer when you install your certificate. On the contrary, your public key can be widely distributed. Messages are encrypted with the recipient's public key and can **only** be decrypted with the corresponding private key. If you plan to use digital certificates for encrypted email, below are a few notes to help get you started:

1. **Your email client must be S/MIME compliant.** Most web-based emails are not S/MIME compliant (i.e., hotmail and yahoo) and therefore cannot make use of certificates for encryption or signing purposes. Common email clients that support S/MIME are Microsoft Outlook, Apple Mail, Mozilla Thunderbird and Lotus Notes to name a few.
2. **BOTH parties must have a digital certificate.** By obtaining a digital certificate for yourself, you can use this certificate for authentication or digital signatures. But when it comes to encryption, having a certificate actually only allows others to send encrypted email to **you**. If you (the sender) wants to send encrypted email to someone else (the recipient), you are actually not using "your" certificate to encrypt the email; you will need to encrypt the email with the "recipient's" public key. This ensures that the encrypted email can only be decrypted by the holder of the corresponding private key, which would be the recipient. And if you want to send an encrypted email to multiple recipients, you would need to have every recipient's public key or else the email client will not let you send the email message as encrypted.
3. **Exchanging public keys.** How do you actually obtain someone's public key so that you can send them an encrypted email? There are traditionally several ways to distribute your public key. While a **private** key is never distributed, a **public** key can be freely distributed. In order to send encrypted messages over the Internet, you need to exchange certificates with the recipient. You can do this in a number of ways:
 - **Digitally sign your emails.** By placing a digital signature on your emails, you can also freely distribute your public key to all recipients. When the recipient receives your email, they can save your contact details. Email clients such as Outlook will automatically save any associated certificates. From then on, this person can then send you encrypted emails.
 - **Public certificate lookup.** Many public CAs, such as PGP TrustCenter, provide a free web-based lookup of public keys. If PGP TrustCenter has issued the

certificates, you can perform a search for a user's public key:

<http://www.pgptrustcenter.com/certificate-services>

- **Send an e-mail message with your .cer file attached.** Once you have a certificate, it is possible to export the certificate from your web browser as a .cer file. Note that when you export your certificate for distribution purposes, you should never include the option to export your private keys. The recipient can then import the .cer file into your contact card or into their certificate store (such as Internet Explorer).
- **Create a contact card with your .cer file, and send the contact card.**
- **Publish your certificate to an LDAP Directory or another directory that is available to the other person.**
- **Post the certificate on a share that is available to the other person.**

Please visit our website to view our latest product configuration guides using certificates. These guides provide instructions on using digital certificates with many email clients, as well as importing and exporting certificates using popular web browsers:

<http://www.chosensecurity.com/digital-certificate-support>