Comodo Secure Email Certificates

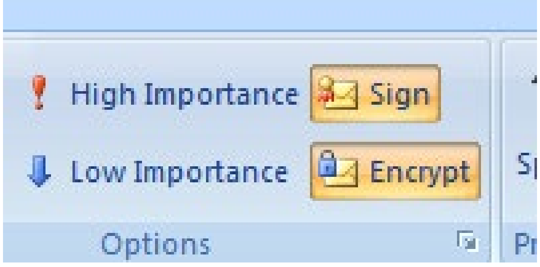
Secure communications for home and business users

Unsecured email messages are rather like sending a postcard written in pencil. They can be intercepted, read or edited by any moderately skilled hacker or nosy mail server admin long before they reach their intended recipient. While this isn't an issue if your email consists of 'Wish you were here', it poses a problem if you are sending anything remotely confidential.

To avoid this, every message sent should be encrypted and signed using a digital certificate. Encrypting your message means that nobody else can read it apart from your intended recipient. Digitally signing the mail proves to your recipient that the mail was genuinely sent by you (and not an impersonator). Signing also means that it is impossible for anyone to alter the contents of your email without the recipients being alerted.

After downloading and installing a Comodo email certificate, you will be able to use the 'Sign' and 'Encrypt' buttons on your favorite mail client:

Sign and Encrypt buttons in Outlook 2010



How they work in detail

When you apply for an email certificate, two types of encryption keys are generated by your operating system. These are called the 'Private Key' and the 'Public Key'. Messages encrypted with the private key can only ever be decrypted with the corresponding public key and vice-versa. Private keys are used to digitally sign your outgoing mails and will never be shared with anybody. They will never leave your computer and are known only to you. Public keys are used to encrypt your outgoing mails and are intended to be shared with everybody and anybody with whom you wish to exchange secure communications. Because your public key is actually in your email certificate, you can pass your public key to a contact by simply sending them a signed email.

When you sign and encrypt an email, you guarantee three elements:

- **Authenticity.** Messages signed with your private key can only be decrypted with your public key – nothing else can decrypt them. You have already sent your public key to your contacts so that they can do this decryption. If your recipient can decrypt the digital signature attached to your mail with your public key then the email must have come from you. This is because you are the only person that has access to your private key and are therefore the only person that could have encrypted it. Digitally signing therefore proves to your recipient that the message and attachments really came from you and not someone masquerading as you.

- **Integrity.** When you digitally sign your mail, your mail client will run the message through a computer algorithm to calculate a 'hash' of the entire message contents. This hash is completely unique to the message you have just created and is sent as an attachment. When your recipient's mail client receives your mail, it does a parallel calculation on your message to produce its own hash. Then it compares the hash attached to your mail with the hash it has just calculated. If the two match, then the contents of the mail have not been altered since you pressed the 'send' button. If the two hashes differ then your recipient will be alerted as somebody may have tampered with your mail.

- **Privacy.** Unlike digital signing, which is done with your private key, email is encrypted with the public keys of your contacts. As explained above, you should have exchanged public keys with all your contacts beforehand (this can be done by simply sending them a signed email). A mail encrypted with someones public key can only be decrypted with their private key. This means only the person you encrypted for can read the mail because they are the only person in the world with access to the private key. Your email cannot be intercepted and read by anybody else.

Comodo SecureEmail Certificates take only a few minutes to install, provide the highest levels of messaging security and are trusted by 99.9% of all email clients, including:

- Microsoft® Outlook Express
- Microsoft® Outlook®
- Microsoft® Entourage
- Apple Mail
- Mozilla Thunderbird
- Or any other S/MIME compliant software

Next Steps

Comodo offers secure email certificates for both corporate and home users.

Home users can download a free email certificate at
http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html

Corporate email certificates are available at different price points depending on the term and the number of certificates required. Corporate email certificates are available through Comodo Certificate Manager and Enterprise PKI Manager.

Enterprises can purchase Comodo email certificates directly from
http://www.enterprisessl.com/ssl-certificate-products/addsupport/secure-email-certificates.html

More information about Comodo Certificate Manager can be found at
http://enterprise.comodo.com/security-solutions/digital-certificates/certificate-manager/

To speak directly with a Comodo representative about Secure Email certificates, please contact us at the following:
Email: sales@comodo.com
Telephone - US: +1 (888)- 266-6361, International: +1 (703)- 581-6361

About Comodo

Comodo provides the highest level of security at competitive prices. As the second largest provider of business-validated certificates, Comodo ensures that millions of transactions are safely performed everyday. We are always looking for new ways to enhance online trust and security. Comodo is bringing online trust, security, and compliance solutions to a new higher standard.

Comodo Group Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester
M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

Tel : +1.888.266.6361
Tel : +1.703.581.6361
www.instantssl.com
Email : sales@comodo.com