PGP TrustCenter
A DIVISION OF PGP CORPORATION

Using PGP TrustCenter's Digital Certificates with Google Gmail for FireFox

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".

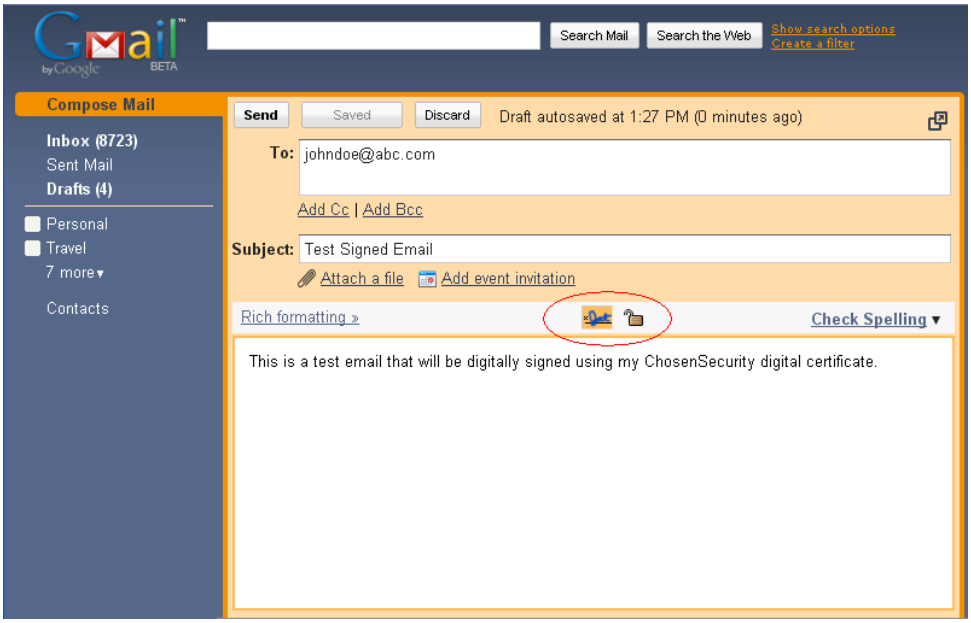
At this time, to use any of the security features in Gmail, only Mozilla's FireFox is currently supported. To use this feature, you will need to install the "Gmail S/MIME" add-on. We tested version 0.4.1 with FireFox v3.5. Gmail S/MIME provides Firefox users with S/MIME support for Gmail. S/MIME support is integrated directly into Google's Gmail web interface. Reading and sending of encrypted mail is supported. Signing of messages is supported as of version 0.2.0. Verification of signatures is not supported in the current version. Version 0.2.0 onwards has also addressed several interoperability problems with support for most major mail clients. Also note that the S/MIME add-on does not currently work with a Google Apps business email account.

Configuring Google Gmail using Mozilla FireFox

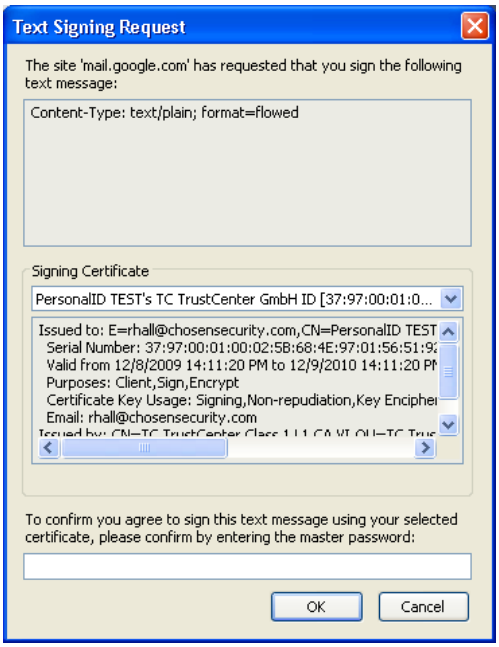
After you have your digital certificate with private keys installed in Mozilla, you will need to configure Gmail with S/MIME support in order to use the certificate:

1. From Mozilla's Add-Ons for FireFox website, download the Gmail S/MIME add-on: https://addons.mozilla.org/en-US/firefox/addon/592
2. Install the S/MIME add-on and restart FireFox.
3. You may also need to install TC TrustCenter's Universal or Class 2 Root CAs into Mozilla if using an older version. Depending on which certificate you have ordered from PGP TrustCenter, you can install the following (accept all trust options during installation):
   TC Personal ID: http://www.trustcenter.de/media/Universal_CA-I.der
   TC Business ID: http://www.trustcenter.de/media/class_2_ii.der
4. Emails can now be digitally signed and/or encrypted by clicking on the "sign" and "padlock" icons.
5. After clicking on "Send", Gmail displays a Text Signing Requests dialogue box and will ask for a "Master Password". You can leave this blank and just click OK. See screenshots on next page.
6. Next Gmail will display a message dialogue that says "Authentication Required". Here you should enter your Gmail email password.

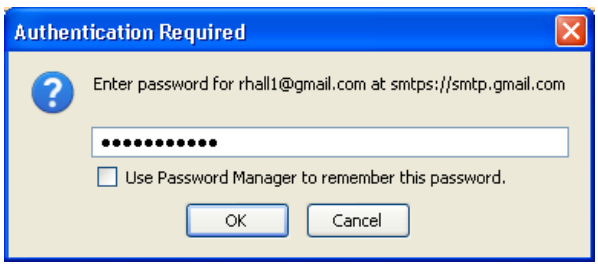
Please see the corresponding screen shots on the next page.



Note the two new icons added to Gmail for Digital Signatures and Encryption



Leave this “Master Password” blank and press OK.



Enter your Gmail email password and press OK.

Digitally Signing Emails

By digitally signing a message, you apply your signature to the message. The digital signature includes your certificate (certificate: A digital means of proving your identity. When you send a digitally signed message you are sending your certificate and public key. Certificates are issued by a certification authority, and like a driver's license, can expire or be revoked.) and public key (public key: The key a sender gives to a recipient so that the recipient can verify the sender's signature and confirm that the message was not altered. Recipients also use the public key to encrypt (lock) e-mail messages to the sender.). This information proves to the recipient that you have signed the contents of the message and not an imposter, and that the contents have not been altered in transit. This is done within Gmail by selecting the "signature" icon:

Encrypting Emails

Encrypting an e-mail message protects the privacy of the message by converting it from readable plaintext into ciphered (scrambled) text. Only the recipient who has the private key (private key: The secret key kept on the sender's computer that the sender uses to digitally sign messages to recipients and to decrypt (unlock) messages from recipients. Private keys should be password protected.) that matches the public key (public key: The key a sender gives to a recipient so that the recipient can verify the sender's signature and confirm that the message was not altered. Recipients also use the public key to encrypt (lock) e-mail messages to the sender.) used to encrypt the message can decipher the message.

In order to encrypt emails in Gmail, you must first choose a recipient and then select the "padlock" icon:

In order to send encrypted messages over the Internet, the recipient of your email must also possess a digital certificate. It is important to note that emails are encrypted using the ***recipient's*** certificate and ***not your own*** certificate. You will need to exchange certificates with the recipient prior to sending encrypted emails. You can do this in a number of ways:

- Exchange Digitally Signed emails. The recipient receives your certificate from the signed email.
- 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.

- If the certificates have been issued by PGP TrustCenter / TC TrustCenter, the certificates may have been published to our public lookup service. This is available online at: http://www.pgptrustcenter.com/certificate-services.