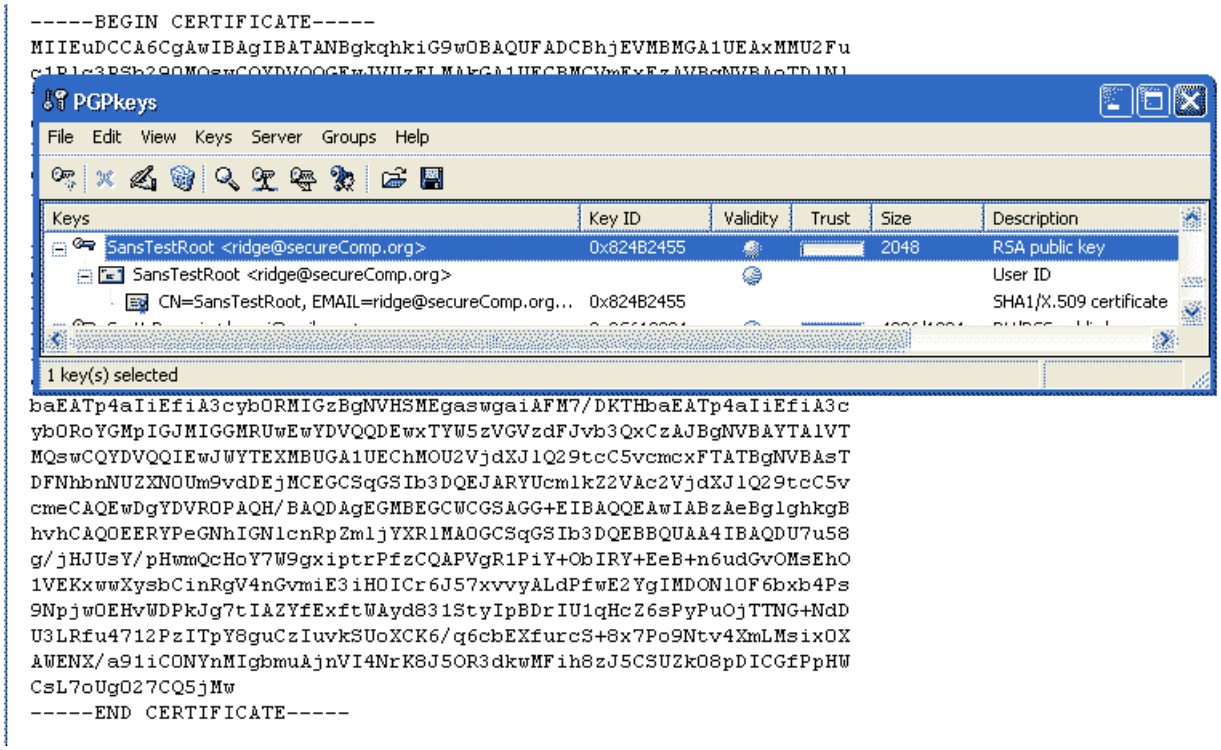
X509 digital certificates have been accepted into PGPKey manager *as* a cert since PGP v 6.01(?) or 6.51. Also the trust chain is imported intact. The whole PKI chain is marked trusted if you mark the signing Root cert as a "Trusted Introducer"
This works if the certificates are from a private PKI or through a known CA like Thawte.

Pre PGP6.....and with GPG, the x509s are seen as RSA v3 keys (which they are) and the trust chain is not imported into the key ring. GPG chokes on the signatures as the cert is not self signed . there is an easy work around. Then one has to manually rebuild the trust chain relationships.

X509 public keys can be exported from several applications in several formats. The ones that PGP handle best are base 64 .der also called .pem When opened in a .txt reader , they look like below.

```
-----BEGIN CERTIFICATE-----
MIIEuDCCA6CgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBhjEVMBMGA1UEAxMMU2Fu
c1Rlc3RSb290MQswCQYDVQQGEwJVUzELMAkGA1UECBMCVmExFzAVBgNVBAoTDlNl
Y3VyZUNvbXAub3JnMRUwEwYDVQQLEwxTYW5zVGVzdFJvb3QxIzAhBgkqhkiG9w0B
CQEWFHJpZGdlQHNlY3VyZUNvbXAub3JnMB4XDTA0MDkxMDE3MDUwMloXDTA0MTAx
MDE3MDUwMlowgYYxFTATBgNVBAMTDFNhbnNUZXN0Um9vdDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAlZhMRcwFQYDVQQKEw5TZWN1cmVDb21wLm9yZzEVMBMGA1UECxMM
U2Fuc1Rlc3RSb290MSMwIQYJKoZIhvcNAQkBFhRyaWRnZUBzZWN1cmVDb21wLm9y
ZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANXxPuL80rlPdbf3vmZE
F3msnd0dHYnksqUPWwaocCLyD+HAJSsMe/GWOMq7ayhwUbIDQHohjb8cTYaATIgd
9jcHaDmHAJ5yx7izCYmpqRu+mF+Oad233dUiaWLOEu17lDeV5xPB4V+Zv6JgM+CR
R7+aNrtH7qWkk6w3a+VxJQg+WB/duZTcCObxjfxXOtnbfsCAd5ghdwL3jsysLUJO
KnYSVfwsG4CJ63cCAitbTMzIuFj7udkAOEEe9w/BWVWV5SEfGDaTstC78392rojz
X31Qi5wRrqrZuSadr+Gs+H8c0MTXQpbxyedo0CmjQYUD3SonbtKCxCdg4ZV03IJL
JFUCAwEAAaOCAS0wggEpMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM7/DKTH
baEATp4aIiEfiA3cyb0RMIGzBgNVHSMEgaswgaiAFM7/DKTHbaEATp4aIiEfiA3c
yb0RoYGMpIGJMIGGMRUwEwYDVQQDEwxTYW5zVGVzdFJvb3QxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJWYTEXMBUGA1UEChMOU2VjdXJlQ29tcC5vcmcxFTATBgNVBAsT
DFNhbnNUZXN0Um9vdDEjMCEGCSqGSIb3DQEJARYUcmlkZ2VAc2VjdXJlQ29tcC5v
cmeCAQEwDgYDVR0PAQH/BAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIABzAeBglghkgB
hvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0GCSqGSIb3DQEBBQUAA4IBAQDU7u58
g/jHJUsY/pHwmQcHoY7W9gxiptrPfzCQAPVgR1PiY+ObIRY+EeB+n6udGvOMsEhO
1VEKxwwXysbCinRgV4nGvmiE3iH0ICr6J57xvvyALdPfwE2YgIMDONl0F6bxb4Ps
9Npjw0EHvWDPkJg7tIAZYfExftWAyd831StyIpBDrIU1qHcZ6sPyPuOjTTNG+NdD
U3LRfu4712PzITpY8guCzIuvkSUoXCK6/q6cbEXfurcS+8x7Po9Ntv4XmLMsix0X
AWENX/a91iC0NYnMIgbmuAjnVI4NrK8J5OR3dkwMFih8zJ5CSUZk08pDICGfPpHW
CsL7oUg027CQ5jMw
-----END CERTIFICATE-----
```

By copying to Clipboard then, opening PGPKey manager: Edit>Paste, you can import this key block into the PGP key store in its original format..



Once it is in PGPKey manager, right click the public key and go to "Sign" Sign with a private key in the local PGP Key store. Clicking "More Choices in the signing window gives you the option of Meta-Introducer or Trusted Introducer The PGP 6.58 Windows User's Manual defines them as this-

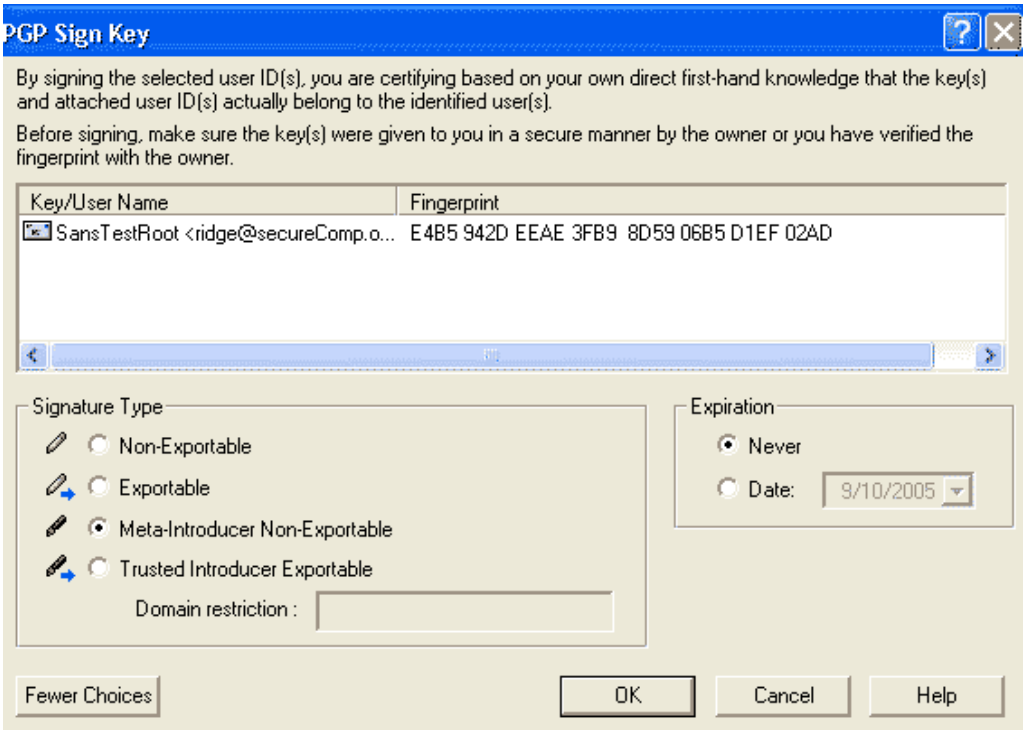
What is a trusted introducer?

PGP uses the concept of a trusted introducer, someone who you trust to provide you with keys that are valid. This concept may be familiar to you from Victorian novels, in which people gave letters of introduction to one another. For example, if your uncle knew someone in a faraway city with whom you might want to do business, he might write a letter of introduction to his acquaintance. With PGP, users can sign one another's keys to validate them. You sign someone's key to indicate that you are sure that their key is valid, which means that it truly is their key. There are several ways to do this. When a trusted introducer signs another person's key, you trust that the keys they sign are valid, and you do not feel that you must verify their keys before using them.

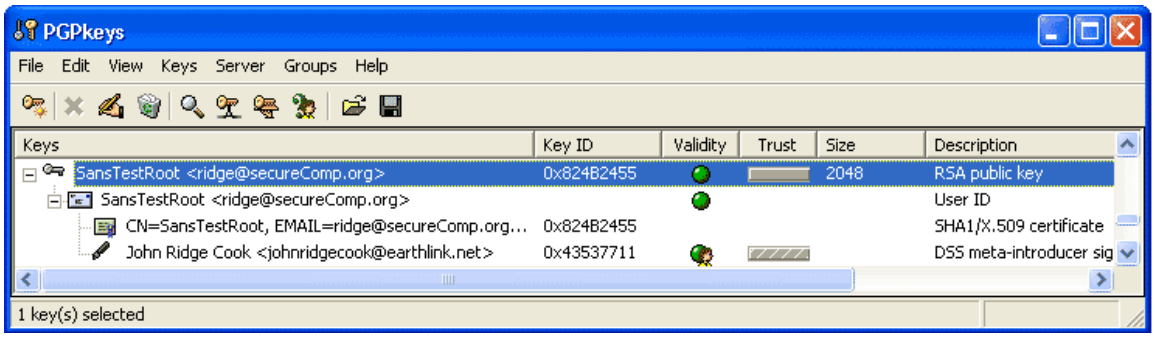
What is a meta-introducer

PGP also supports the concept of a meta-introducer--a trusted introducer of trusted introducers. If you work in a very large company, you might have a regional security officer, a trusted introducer, who would sign users' keys. You could trust that these keys were valid because the regional security officer had performed the actions to ensure validity. The organization may also have a head security officer who works with the local security officers, so that a person in a West Coast office could trust a person in an East Coast office, because both their keys had been signed by their respective regional security officers, who in turn had their keys signed by the head security officer, who is a meta-introducer. This allows the establishment of a trust hierarchy in the organization.

Since the Root Certificate can authenticate other Intermediary certificates, act as a Bridge Certificate between different CAs, and be the final authentication for User certs, pick Meta-Introducer. If you want to export your signature, then pick Trusted Introducer.

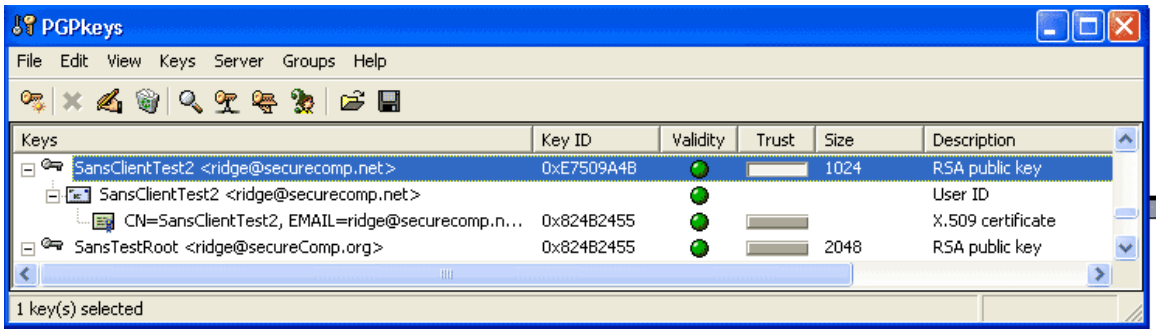


Click OK and enter the passphrase for the secret key you will use to authenticate this key. The Certificate will be entered into the PGPKey manager as a trusted and valid key.

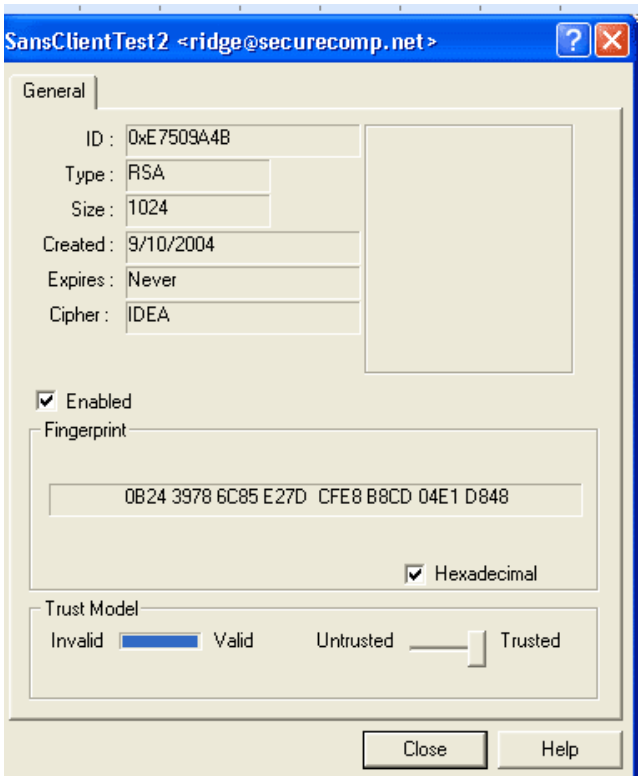


Repeat the process for another certificate signed by that Root, an Intermediary which is signed by that Root, or any other element of a PKI trust chain terminating with that Root.

In this instance, SansClientTest2 was opened in a .txt reader, copied to Clipboard, PGPKeys opened, then Edit>Paste. Importation was approved and the x509 appeared in the key list already marked "Valid". Why? Because it was signed by the Root , which was marked as an Introducer when signed by a local private key.



However, Trust has not been set, in a PGP sense for this particular key. The Root was trusted and PGP marked the Client2 key as valid, but not trusted. To do that, right click>Properties and move the slider over.



Repeat the same simple process for any other x509 certificate you wish to import. If you have a certificate with both the public and private key halfs (.p12 or ,pfx) they can be imported directly into PGP (Key>Import), though the passphrase protecting the private key will have to be entered.

The process above applies to Commercial CA's Roots and client x509s. Their Root certs are often on the key servers or their web sites. They can also be exported from the Internet Explorer or Mozilla certificate stores and brought into PGP. Thawte Freemail x509 certificates can be used for both S/MIME and PGP with the authenticated trust chain carried over in both applications.

Some question the wisdom of extending trust models across different applications, but PG P is quite capable of operating in a hierarchical PKI structure as well as the diffuse, Web of Trust model. This way, if one is sure of the authenticity of the Root and their practices, you can use PGP with a X509 certificate whose trust chain is also used for more critical networking authentication, code signing, etc……

This process does not extend to GnuGP. It does not accept a key that is not self signed . While creating X509s self signed is possible and is a "PGP" type of way to use S/MIME, it defeats the PKI logic. It can be worked around if you have both the public and private key-

> (Guy's Workaround)
> Import to PGP the key (including secret) with the X.509 certificate.
> On the keyring , delete the X.509 certificate and self sign the key
> with a exportable signature. Then re-import the key with the certificate
> attached. They will combine on the keyring.

Ridge Cook
9/10/04