



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gsna>

Auditing PGP Options and Associated Policies: An Auditor's Perspective

Matthew Chalmers

September 2002

GSNA Assignment 2.1

Abstract. This paper details a security audit of the options set for a commercial version of PGP encryption software and associated usage policies. The paper explores risks, control objectives, and the current state of practice before formulating an audit checklist, performing an actual audit, and reporting the findings. The style and structure of this paper are meant to conform to the standards set forth for GIAC certification practical assignments [15].

Table of Contents

<u>1 Research in Audit, Measurement Practice, and Control</u>	1
<u>1.1 Object of Audit: PGP Options and Associated Policies</u>	1
<u>1.1.1 What is PGP?</u>	1
<u>1.1.2 How is PGP Used?</u>	1
<u>1.2 Risk Evaluation and Security Control Objectives</u>	2
<u>1.2.1 Evaluating the Risks to the System</u>	2
<u>1.2.2 Control Objectives</u>	4
<u>1.3 Current State of Practice</u>	24
<u>2 Audit Checklist</u>	25
<u>2.1 Guide to Reading the Checklist</u>	25
<u>2.2 Blank Table for One Checklist Item</u>	25
<u>2.3 The Audit Checklist</u>	25
<u>3 Audit Evidence</u>	33
<u>3.1 Conducting the Audit</u>	33
<u>3.2 Measuring Residual Risk</u>	45
<u>3.3 Evaluating the Audit</u>	45
<u>4 Audit Report</u>	47
<u>4.1 Executive Summary</u>	47
<u>4.2 Audit Findings</u>	47
<u>4.3 Background/Risk</u>	49
<u>4.4 Audit Recommendations</u>	50
<u>4.5 Costs</u>	51
<u>4.6 Compensating Controls</u>	51
<u>5 References</u>	53

1 Research in Audit, Measurement Practice, and Control

1.1 Object of Audit: PGP Options and Associated Policies

This paper will detail an audit of the options in PGPmail 7.1 for Windows, an enterprise email and file encryption client from Network Associates¹. The audit will also cover certain security policies associated with the use of PGP, the relevance of which will be evident as they arise throughout this paper. Specifically out-of-scope are other add-ons to PGP such as PGPdisk, PGPfire, PGPvpn, etc., and the PGP Keyserver software.

1.1.1 What is PGP?

PGPmail is one of the many commercial versions of the software that is generally known simply as PGP. Other commercial titles based on PGPmail (hereafter “PGP”) include PGP Corporate Desktop from NAI and PGP Personal Security from McAfee. PGP, which stands for Pretty Good Privacy, is used to encrypt files and email with public-key (asymmetric) cryptography, password-based symmetric cryptography, or within password-protected “self-decrypting archives,” and PGP is also used to digitally sign email and files for non-repudiation [1]. There are millions of PGP users world-wide [5].

1.1.2 How is PGP Used?

The simplest way PGP can be used in an organisation is by encrypting single emails or files as needed when transmitting or storing confidential data. PGP can be used in complex ways, however, including as the basis of an organisation’s Public Key Infrastructure, even with the use of smartcards [1]. Clearly PGP can be considered part of an organisation’s critical infrastructure depending on the extent to which it is used. For the purpose of this audit, it is assumed PGP is the organisation’s sole application-level [6] encryption product for end-user email and files.

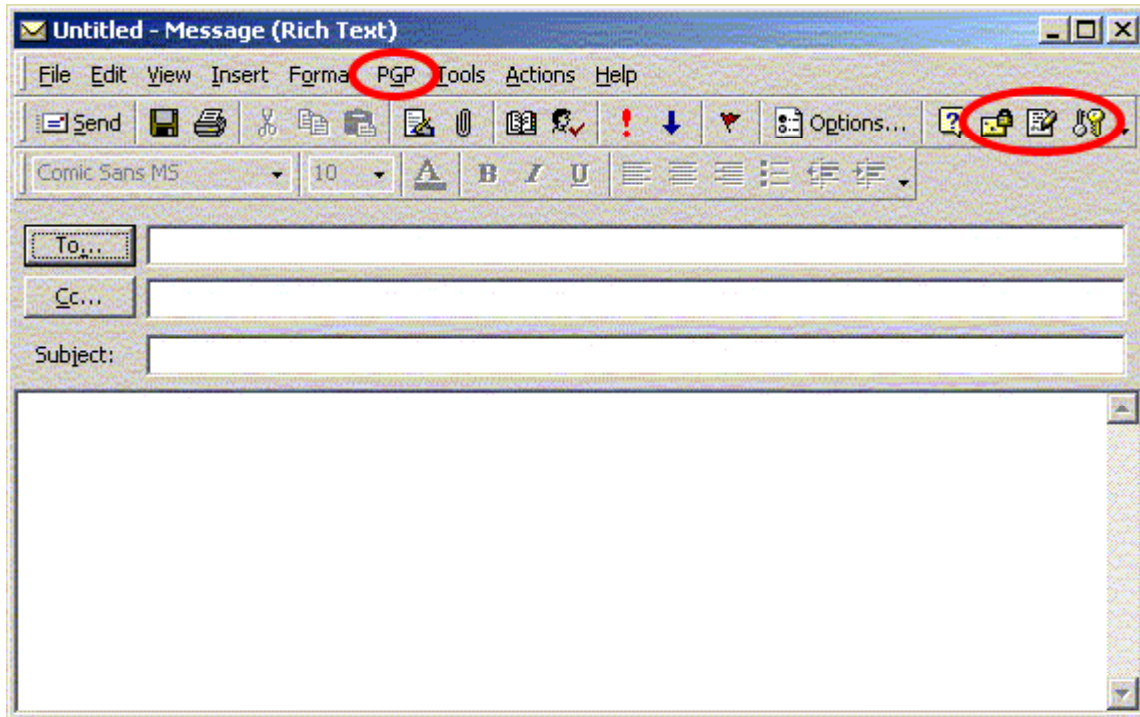
Many people mistakenly think PGP is a stand-alone application with a Graphical User Interface (GUI) used to perform encryption and decryption. While something like that is available (PGPtools) it is not typically how PGP is used on a system. Instead, PGP is usually more transparent, accessed either via toolbar buttons integrated into email clients such as Microsoft Outlook (Figure 1-1) or via the contextual menu in Windows Explorer or My Computer. PGP takes a file or the Clipboard’s contents as input and outputs to a file or the screen after performing its operation (encryption, decryption, signature verification, etc.). Plugins and background services make these functions transparent to the user.

¹ The rights to PGPmail as well as most other PGP offerings from NAI were purchased by the start-up PGP Corp in the summer of 2002 [4]. The last version of PGP released by NAI and the most recent version at the time of this writing is 7.1.2.

PGP was originally created by Phil Zimmermann [7].

© SANS Institute 2000 - 2005, Author retains full rights.

Figure 1-1, the PGP buttons and menu in an Outlook message window.



1.2 Risk Evaluation and Security Control Objectives

1.2.1 Evaluating the Risks to the System

In order to fully understand the risks one must know and understand the options available in PGP. Only certain options are available to end-users; others are set by the administrator in the organisation, who uses the PGPadmin client to configure and create a custom installer for users [3]. First high-level risks will be discussed.

The main questions to ask here are “what can go wrong...how likely is it to actually go wrong [and] what are the consequences if it does go wrong” [8]. Note that the concern is not with the operation of PGP. For example, it is not a concern whether PGP might fail to properly encrypt a confidential document. Concerns regard the options set in PGP and what can go wrong if they are set improperly. Also while external factors may pose risks, such as the OS’s protection of the PGP private keyring, these things also do not fall directly into the scope of the audit (but some will be considered).

The primary goal of the audit is to ensure good security-related options are set, and users cannot change PGP options in such a way as to weaken security. A secondary goal is to ensure good policies for PGP administration exist.

1.2.1.1 Weak Keys and Ciphers

For those familiar with PGP or public-key cryptography, the most obvious concern is the length of an encryption key. “The larger the [key], the greater the security, but also the slower the...algorithm operations.” [9] PGPadmin can be used to set a minimum key length or a specific key length. Readers may be aware that a method has been proposed which may significantly reduce the effort required to “break” RSA public keys [10] however one must keep in mind that there are different algorithms for public-key cryptography, and PGP supports the Diffie-Hellman type to which this attack may not apply. Also, NIST says in [11] that a 1024-bit RSA key should be sufficient to protect data until the year 2015. Additionally, one must remember that the data encrypted with the public key in PGP is actually a symmetric session key [1], so if the public key is stronger than the session key the point is moot. Symmetric algorithms used by PGP will be discussed later.

So, one can see right away that if the PGP options for public key size and symmetric cipher choice are poor, cryptanalytic or brute-force attacks may be plausible. The consequence, obviously, is disclosure of confidential data or loss of trust in the property of non-repudiation. How likely is the shortest key or weakest cipher in PGP to be exploited? Not very. As mentioned above, NIST believes the 1024-bit RSA key to be able to protect data until 2015, and that is the weakest public key PGP allows. And since the public key algorithm, while computationally intensive, only operates on the symmetric session key, there seems to be little incentive to use anything other than the longest available public key.

1.2.1.2 Man in the Middle (MIM) Attack

Another high-level risk that may be apparent is in the “web of trust” [2]. PGP keys are in fact certificates—essentially digitally signed public keys—but they are usually not signed, as are ecommerce web site SSL keys. When a user gets a PGP public key from another user, how can he or she tell it’s actually the valid public key, and not some bogus one created by a nefarious man in the middle? Perhaps an organisation’s users may, by policy, only use keys signed by a trusted organisational signing key. The holder of the signing key would be responsible for determining whether the public key in question is legitimate. Or if a user has a working relationship with another user, the two can exchange key fingerprints over the telephone to confirm each has the other’s correct public key. These policies and settings will be explored later.

If steps are not taken to reduce the risk of introducing an untrusted key, again, disclosure of confidential data or loss of trust in the property of non-repudiation can occur. How likely is this? Depending on the circumstances it could be very likely. If a company employee must exchange confidential data via email with an employee of another company, and the email traverses the Internet between

them, it is quite possible for a man in the middle to intercept public keys as they are sent for exchange, replace them with his own, and send them on to the recipients. By intercepting all the encrypted messages between the two employees the man in the middle can decrypt all their data then re-encrypt it and send it back on its way.

1.2.1.3 Local Attacks

Yet another risk to the system is the local attacker. If the PGP option to cache the passphrase (password) is turned on, then the user is at risk for having his or her confidential data disclosed or having messages sent digitally signed—if, for example, the user left his or her computer unattended and unlocked (e.g. with a password-protected screen saver) and an attacker happened upon it while the PGP passphrase was cached.

Another local attack would have to do with stealing a user's private key if it were not sufficiently protected. The user's PGP passphrase is the only thing standing between an attacker and the private key if an attacker copied the private key.

1.2.2 Control Objectives

The PGP software as a system is fairly easy to control. Once the PGAdmin tool is used to configure a custom installer, that installer is deployed in whatever specific way the organisation will use it to push the software to end users. End users are required to use the options set for them, and can only change those that were not locked. Since there is a potential for a lot of damage to be done, for example in the case of disclosure of confidential data, it makes sense to take the trivial amount of time necessary to create a custom installer with the inexpensive PGAdmin tool in order to minimise the risks.

The administrator's goal should be to set the PGP options in such a way as to prevent the use of weak keys or ciphers and prevent the end user from setting security-relevant options dangerously (such as setting an unlimited time on the passphrase cache) and it will be the auditor's job to determine if this is so as objectively as possible. Also, the organisation should have reasonably secure policies and procedures in place surrounding the use of the software. For example, it may be acceptable for internal email to be unencrypted even if confidential but confidential email sent outside the company's network should be encrypted with PGP. Therefore when dealing with persons outside the company's network, reasonable assurance is needed that the public key received for the external party is indeed that party's key. Blocking employee access to public key servers may be warranted, as PGP can be set to automatically search these when attempting to encrypt a file or email to a recipient whose key the user does not have.

Thus our overriding control objectives are to ensure good PGP options are set,

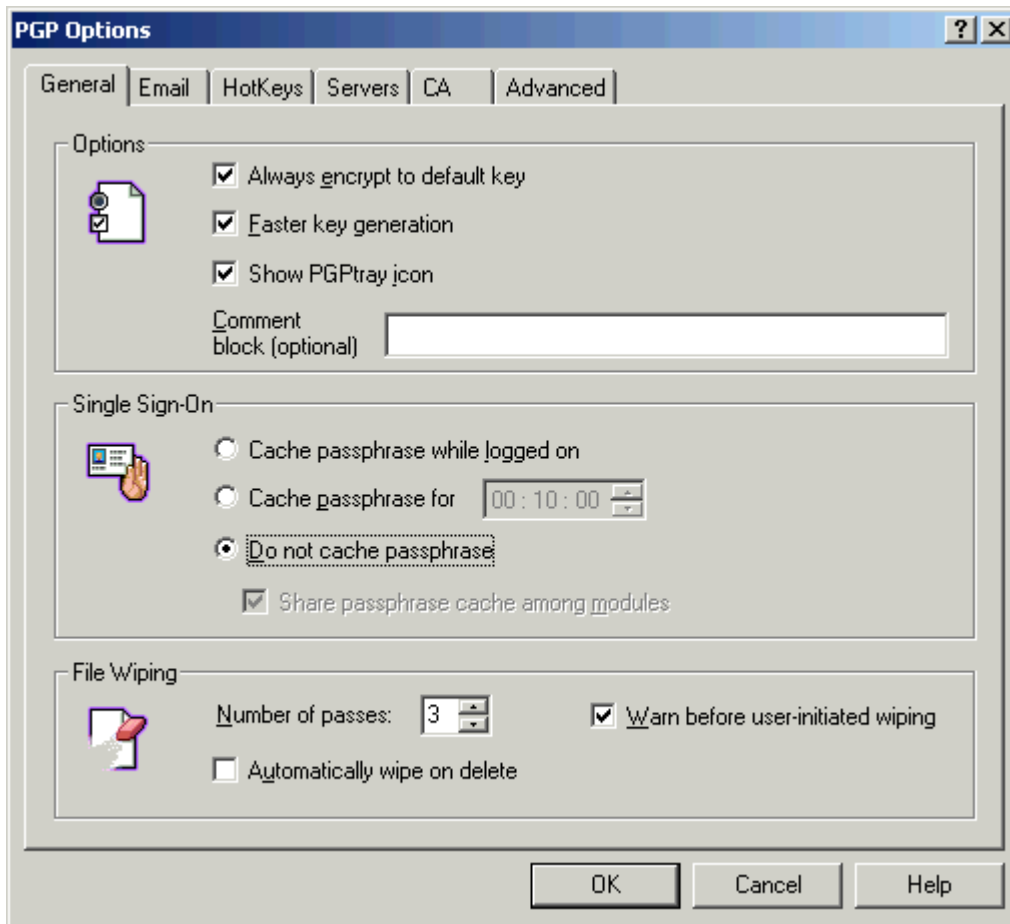
to ensure users cannot change PGP options in such a way as to degrade security, and to ensure good policies exist so overall security of the infrastructure is not threatened. We will also look at ancillary details like the protection afforded private keys, which is neither a PGP option nor a policy, but a technological control.

1.2.2.1 PGP User Options

Following is a list of the PGP user options with brief notes about security for each if applicable. For some options, there may be a “paranoid” versus “reasonable” justification for setting the option one way or another. This section is intended as a brief introduction to the PGP user options, and will translate into an audit checklist quite nicely later. In PGPmail 7.1, user options are segregated into six tabs.

A seventh tab called Files is where PGP is told to find the public and private keyrings and the random seed file. These values cannot be set with the PGPadmin tool but there are security implications. If the private keyring is stored in a shared directory the private key can be copied and attacked easily. There are also cryptanalytic attacks possible if an attacker could modify the random seed.

1.2.2.1.1 General



Always encrypt to default key is somewhat relevant to security. As long as the user has his or her own key set as the default, it keeps the user from having to copy himself or herself on encrypted emails so that he or she can read it later. However, as pointed out in [19] using this option exposes the sender and receiver to a certain form of traffic analysis whereby a man in the middle intercepting the message may be able to tell who sent it and who it's meant for, and also get a list of keys used to encrypt it.

Faster key generation is also somewhat relevant to security. It uses a table of pre-calculated primes to generate Diffie-Hellman keys, and both [19] and [2] warn the extremely security conscious against using this. Since key generation is not done often it seems sensible to turn this off, however [2] indicates there is no known cryptanalytic attack for this so it is optional. Using this option drastically reduces key generation time. If using a slower machine (Pentium II @ <500MHz) you can literally go out for coffee and return to find the sub-key is still being calculated.

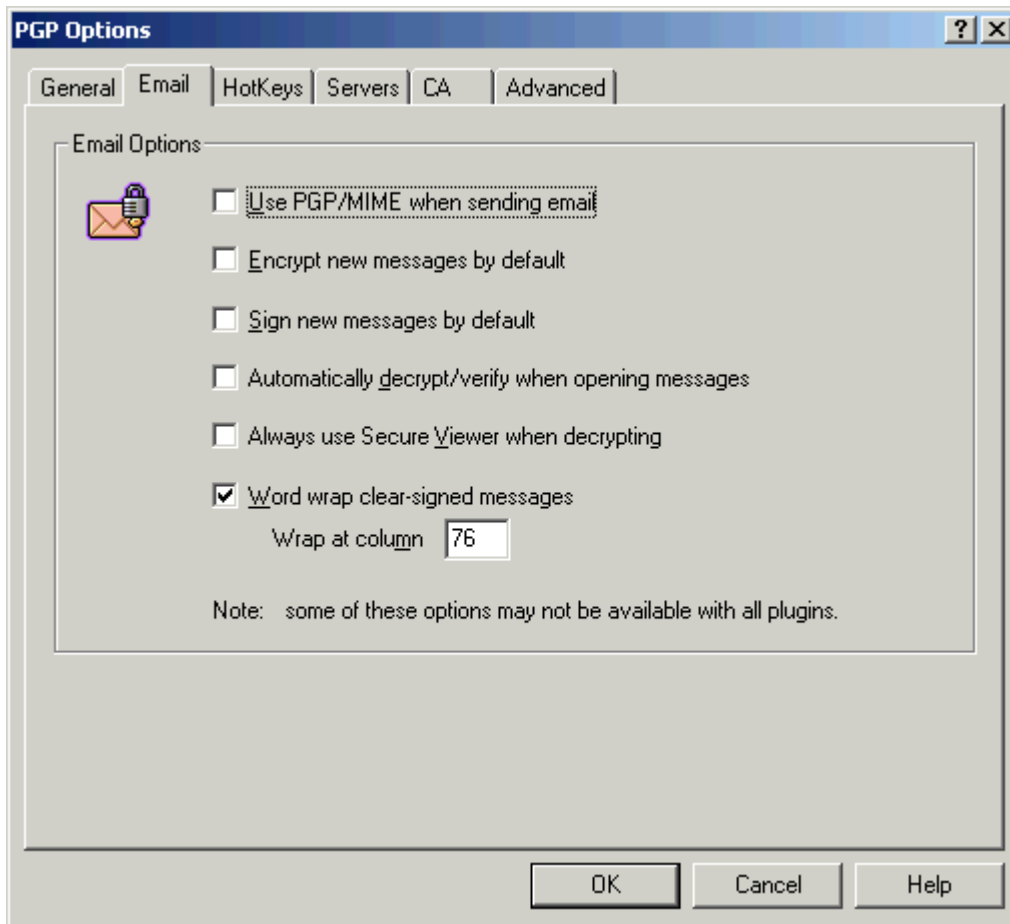
Show PGPTray icon is not really relevant to security. It puts a quick-access icon/menu in the Windows System Tray. However the paranoid might say this gives away to shoulder surfers the fact that the user probably has a PGP key.

Comment block is not terribly relevant to security. It allows an organisation to put a custom comment, such as the organisation's name or web address, in ASCII-Armoured blocks. However the paranoid might say putting the organisation's name or web address in the comment could be flagged by attackers who sniff network traffic if they are interested in the company's correspondence.

Cache passphrase is probably security-relevant. If the user is allowed to cache his or her passphrase indefinitely after the first entry, it becomes very easy for someone who walks by the user's PC while he or she is away from the desk to decrypt data and digitally sign data or emails. Caching should probably be disabled.

Number of passes for file wiping is important if users are allowed or expected to securely erase data from their disks. The more passes, the more secure the erasure, but the longer it takes to complete. Most organisations will not really need a secure erasure feature, however, the government or military might. PGP should probably not be relied upon for true secure erasure, as it seems to be the case that no matter how many times data is overwritten, a determined adversary can still recover all or most of the data from magnetic media [12]. The **warn before** checkbox is not really security-relevant. It is interesting to note that a bug was discovered [13] with the **automatically wipe** feature in combination with the Microsoft Windows 2000 Encrypting File System (EFS) whereby when this feature is turned on and an EFS-encrypted file is deleted, a decrypted copy in a hidden temporary file remains undeleted.

1.2.2.1.2 Email



Use PGP/MIME is not security-relevant, it is meant for users of the Eudora email client [2].

Encrypt new messages is probably not likely to be set in any organisation because, chances are, users will not need to encrypt all of their email, rather only those that contain confidential data or are being sent outside the company.

Sign new messages is also not likely to be set because unless the PGP passphrase is cached users will have to type them in every time an email is sent. (It may help to cut down on unnecessary use of email though!)

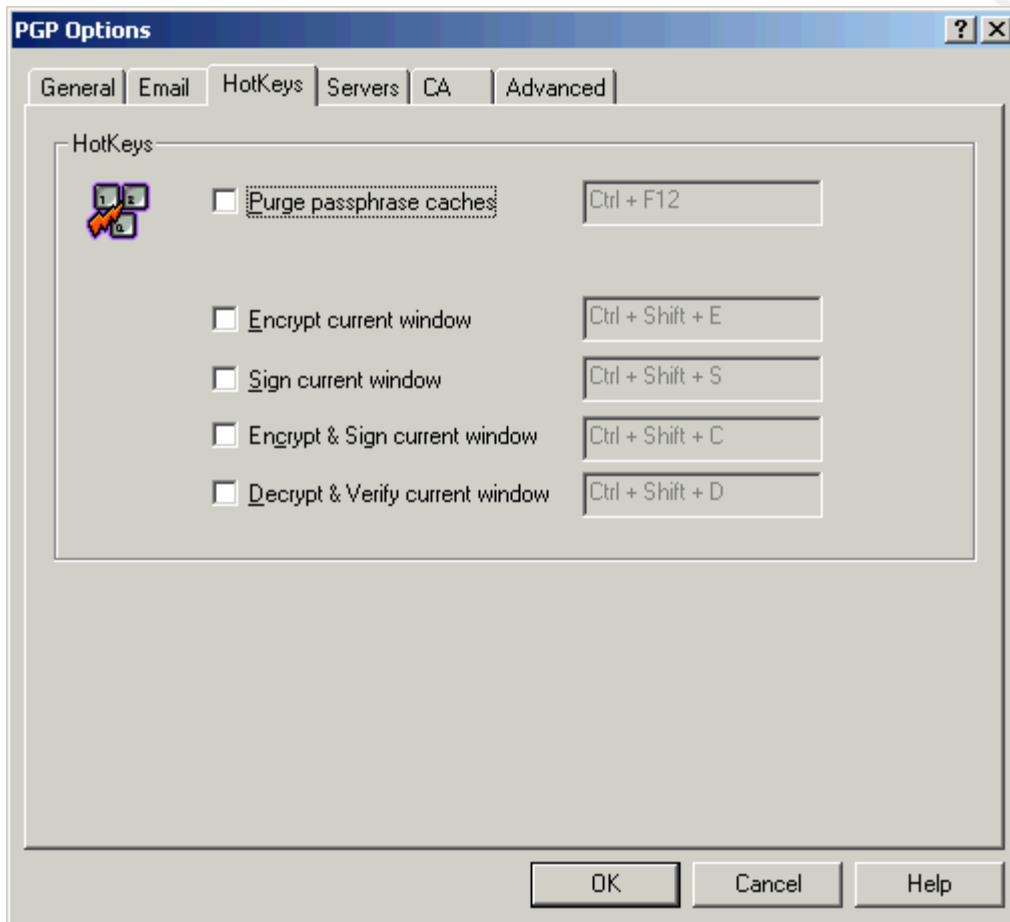
Automatically decrypt can be thought of as security-relevant mostly because of the likely behaviour of users, like saving changes on decrypted messages (which will cause a decrypted copy to be saved on the mail server in some instances as with Microsoft Exchange). There was also a bug prior to 7.1.1 [14] that caused a decrypted copy to automatically be saved to the server when replying to an automatically decrypted message.

Always use secure viewer is a great way to keep decrypted copies of messages from being saved, however, it prevents users from copying & pasting

too. Functionality and productivity go way down with this option checked.

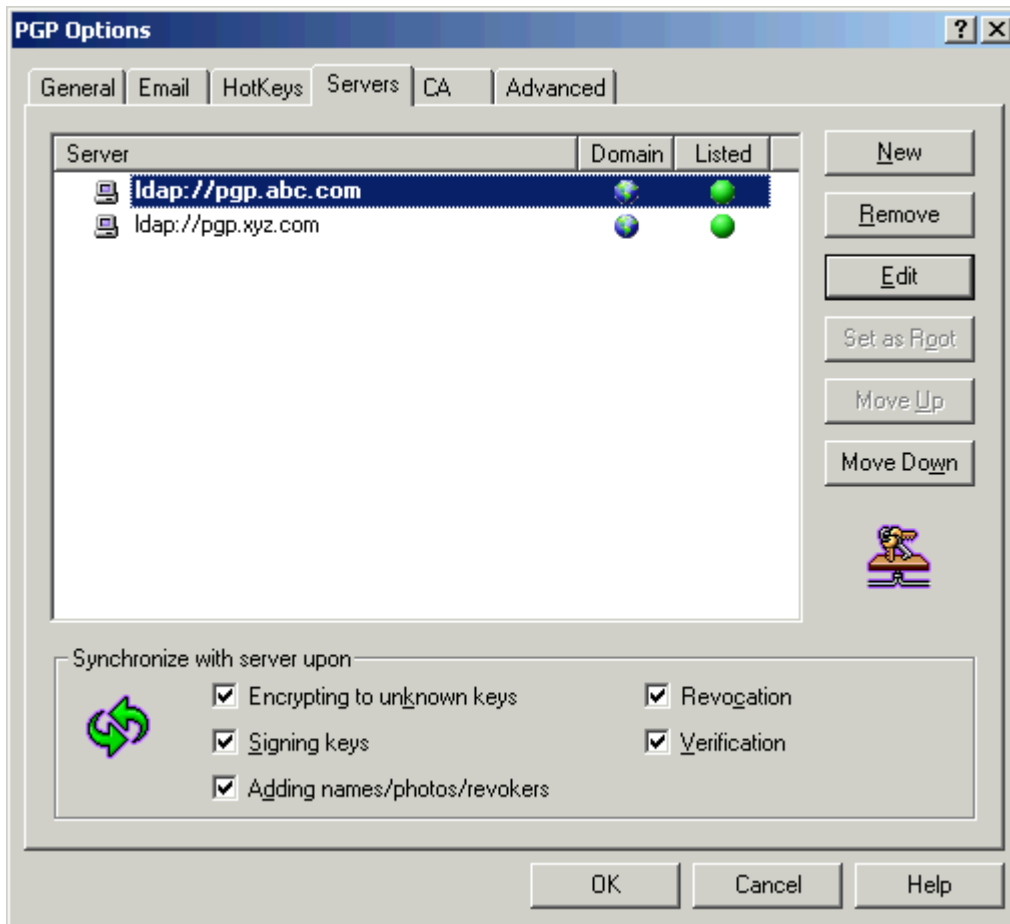
Word wrap is not really security-relevant.

1.2.2.1.3 Hotkeys



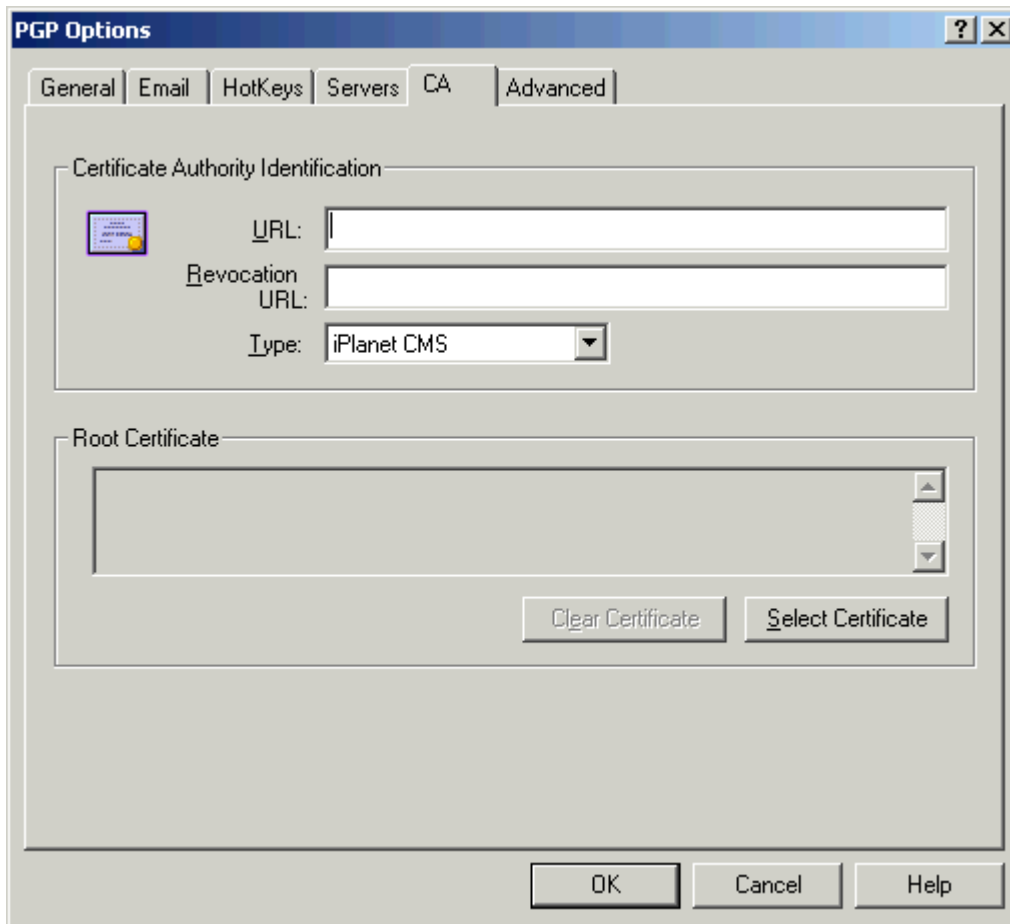
It may be possible for a Trojan to intercept hotkeys to either capture the user's passphrase or keep it from being purged from cache memory. Of course malicious code could theoretically be written to do this even if no hotkeys are set.

1.2.2.1.4 Servers



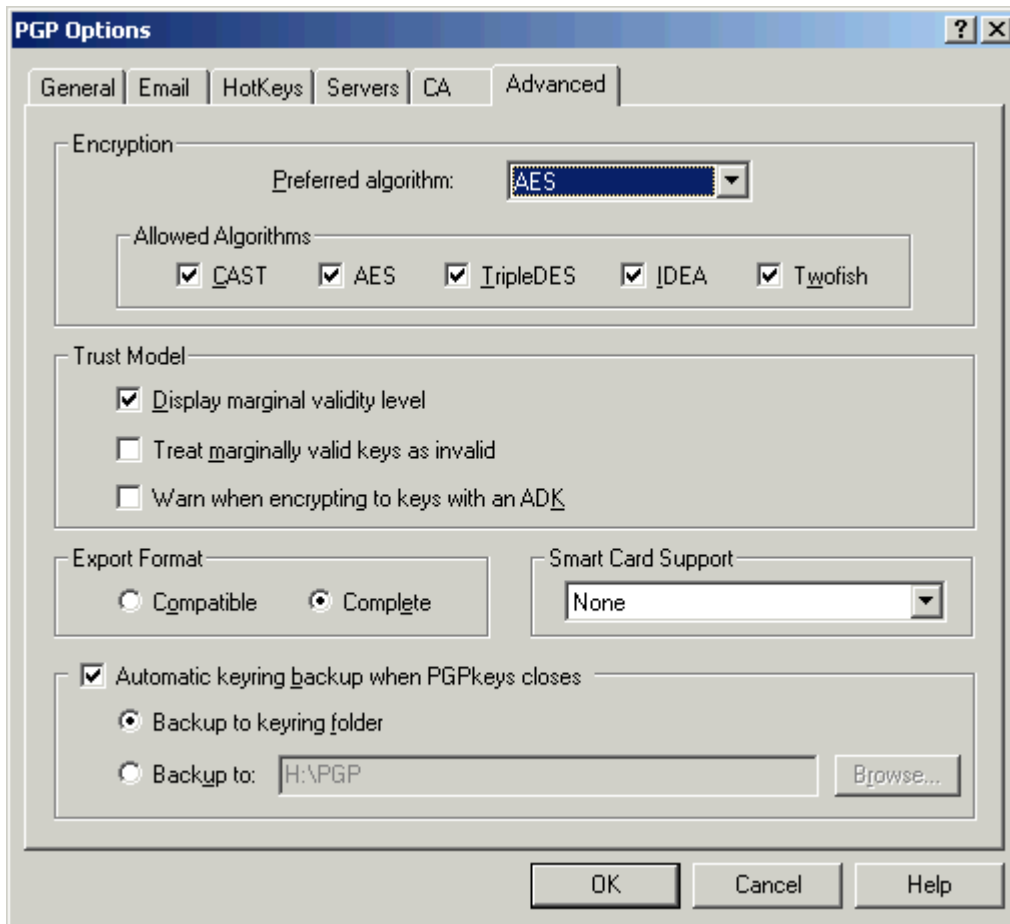
As previously mentioned, it could be a good idea to block users from reaching public PGP servers so as not to introduce untrusted keys or publicise information about the organisation which can be found in public keys. It might also be a good idea to set up an internal key server to store trusted keys. If that is the case, any of the **synchronisation** options may be relevant depending on other PGP settings or company policies. PGP requires at least one server to be defined.

1.2.2.1.5 CA



If the organisation is going to use PGP in a Public Key Infrastructure (PKI) in conjunction with a Certificate Authority (CA), this tab will be important. For this paper it is assumed no CA is used and there is no reason to audit these options.

1.2.2.1.6 Advanced



Preferred algorithm. As there has not yet been any contestation to the Advanced Encryption Standard (AES) algorithm it is probably the best choice for a preferred algorithm [11, 18]. If it is known that users will need compatibility with outside PGP users, at least one of the other algorithms should also be selected as **allowed**. Note that CAST, IDEA, and 3DES are the only algorithms supported by many older versions of PGP so if backward compatibility is desired, one of these must be checked. There is nothing inherently wrong with any of the supported ciphers, and no implementation flaws have been noted in this version of PGP. (The “vulnerability” in PGP described by Jallad, Katz, and Schneier in [17] is actually an implementation of a cryptanalytic attack called adaptive chosen-ciphertext, which exploits the OFB (Output Feedback) mode of operation of certain ciphers used in PGP. PGP actually contains “Manipulation Detection Code” (MDC) to thwart this attack, however, it appears to be turned off in this version of PGP according to Werner Koch [18]. PGP also compresses data before encryption, also foiling this attack.)

Display marginal validity level is not really security-relevant. It may serve as a quick reference for savvy users but is not essential.

Treat marginally valid keys as invalid can be used in a strict environment to

keep users from being able to work with keys that are not completely valid. Validity has to do with the aforementioned “web of trust.”

Warn when encrypting to keys with an ADK (Additional Decryption Key) is not really security-related, it only warns users when they choose to encrypt to a key with an ADK attached, as many corporate keys will have.

Export format is not security-related; it is for compatibility with old versions of PGP.

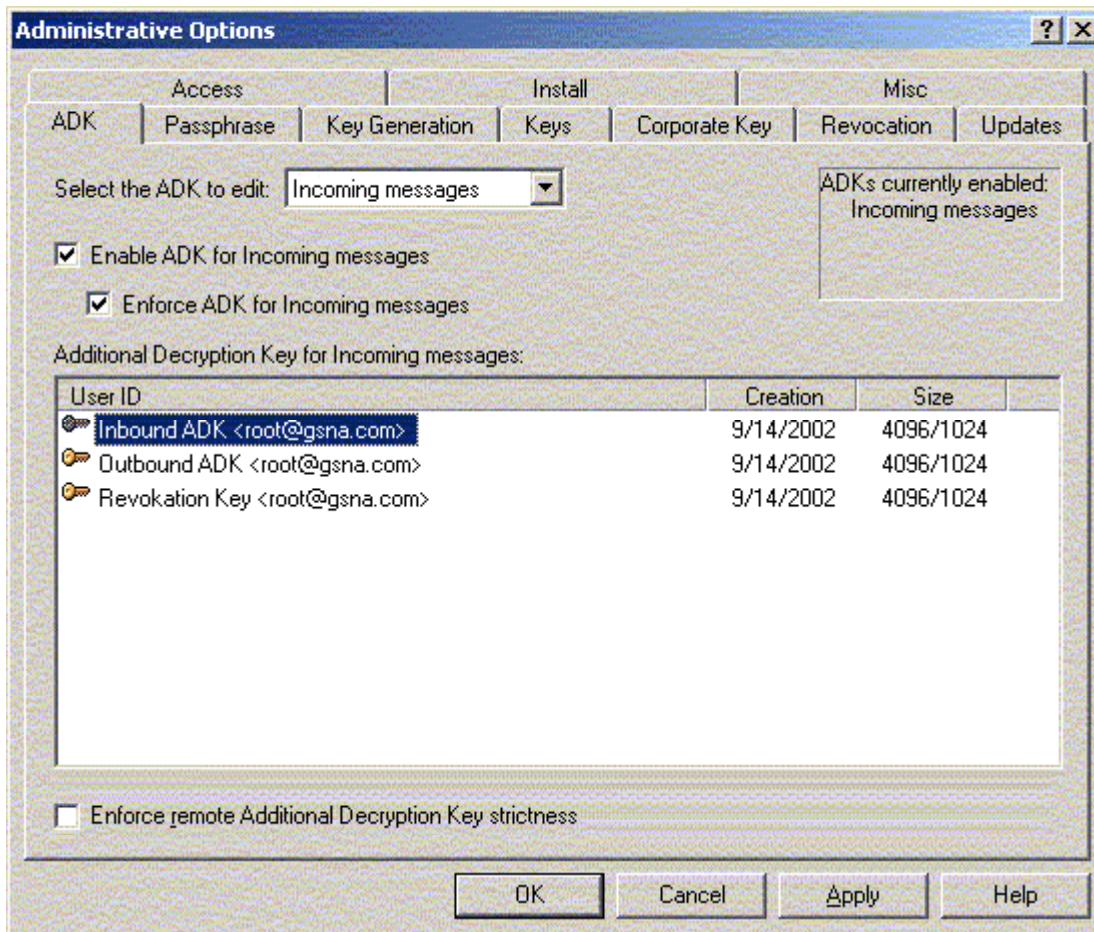
Smartcard support is only needed for environments using smartcards, obviously, and for this paper it is not relevant.

Automatic keyring backup should be considered if a default location is set in a public area. For example if an organisation has a shared network drive, keyrings should not be automatically backed up there as everyone with access will have access to all the private keys there and can guess at their passphrases. If this feature is used the location should be as secure as the main keyring location.

1.2.2.2 PGP Admin Options

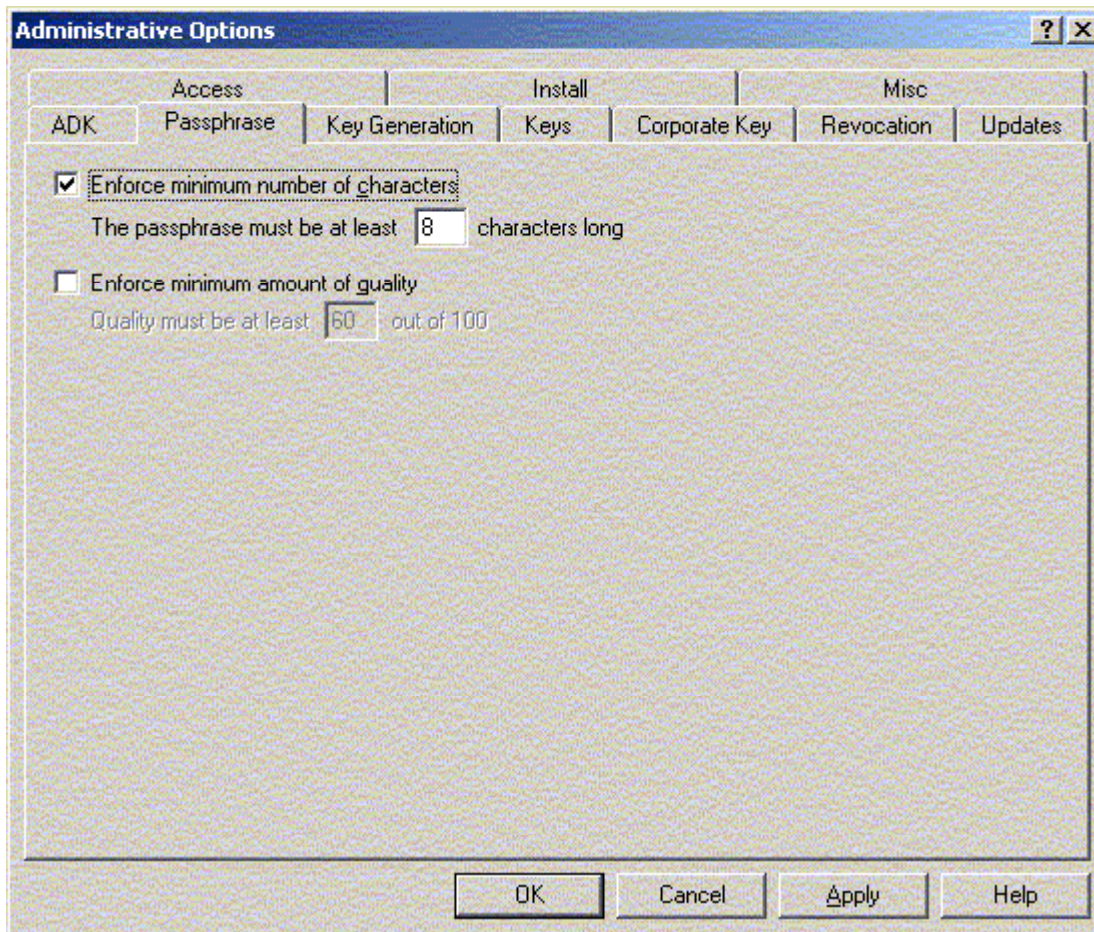
Following is a list of the PGP administrative options with brief notes about security for each if applicable. For some options, there may be a “paranoid” versus “reasonable” justification for setting the option one way or another. This section is intended as a brief introduction to the PGP administrative options, and will translate into audit checklist items quite nicely later. In PGPmail 7.1, administrative options are segregated into 10 tabs.

1.2.2.2.1 ADK



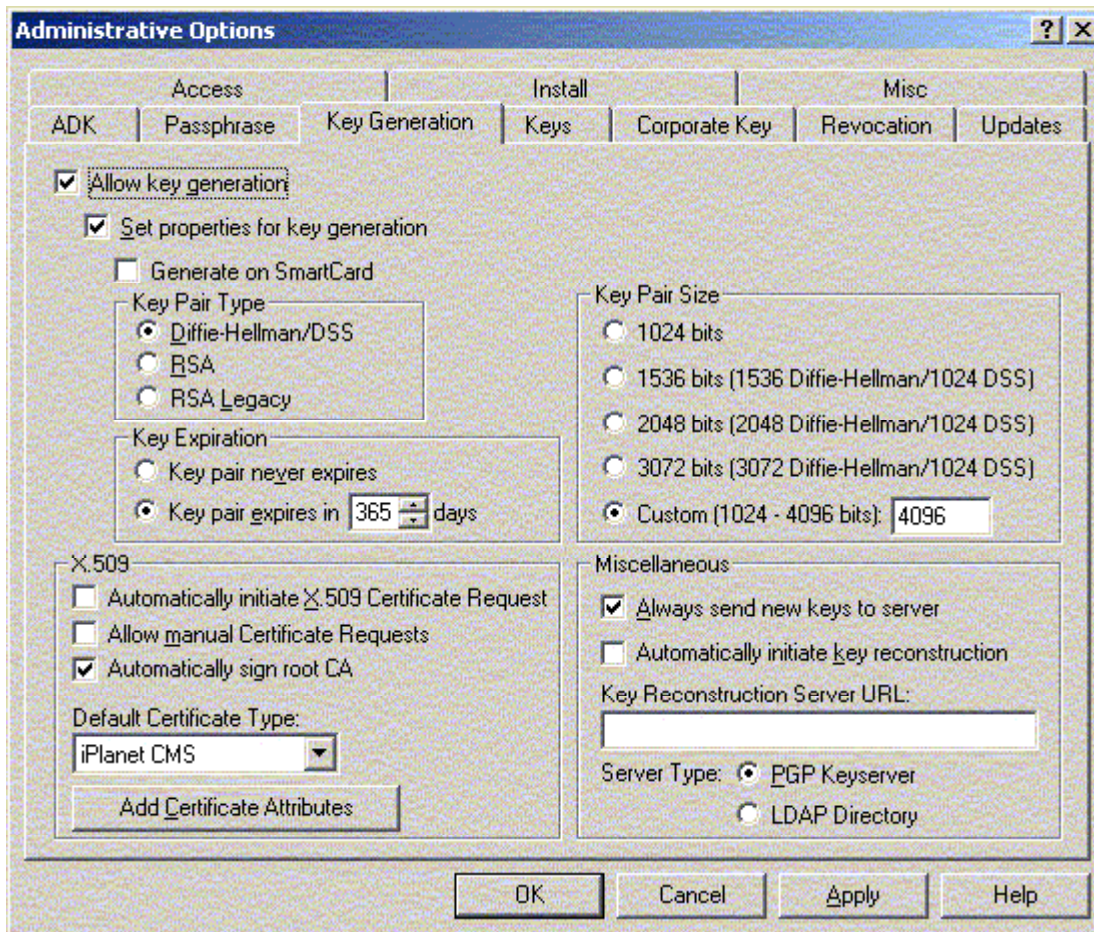
An ADK can be used to encrypt messages to and from the organisation's users. This is recommended over key escrow to preserve the property of non-repudiation. If ADKs are used they should probably be enforced, however, remote ADKs (those of other companies) should not necessarily be enforced.

1.2.2.2.2 Passphrase



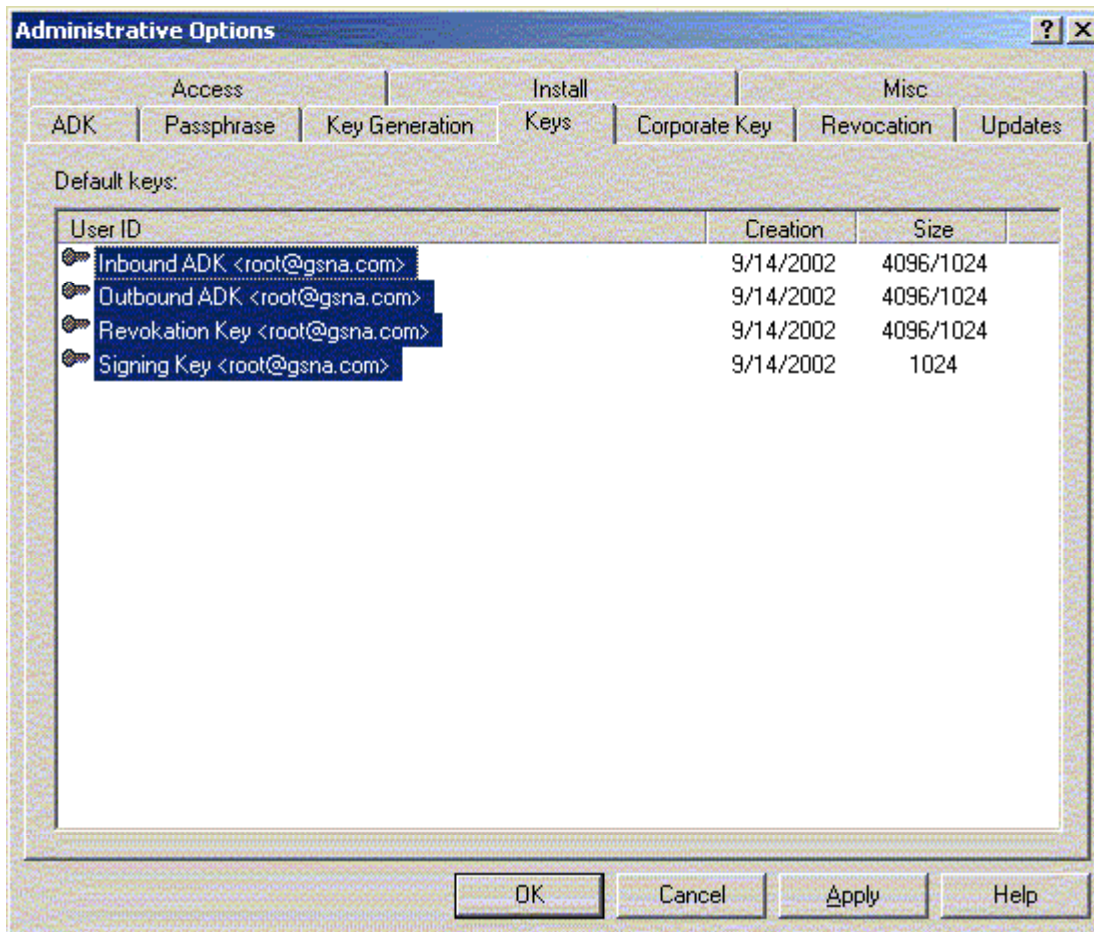
Instead of researching the effectiveness of PGP's built-in passphrase quality measurement, a minimum length is enforced. In [16] AusCERT estimates the cracking time for an eight-character password to be one year, versus one week for a seven-character password.

1.2.2.2.3 Key Generation



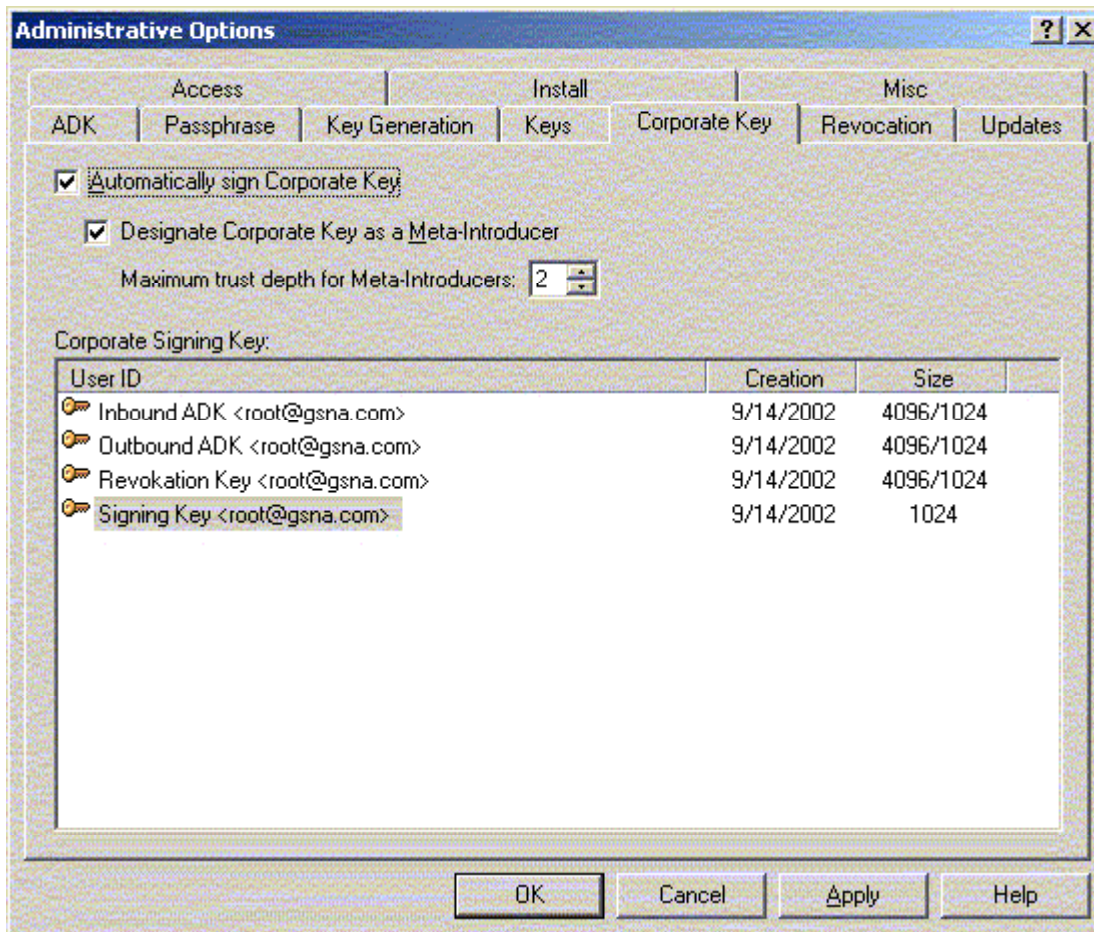
Allowing users to create their own keys may decrease infrastructure complexity. The key properties will be controlled, however, using good practices such as the largest size, a one-year expiration, etc.

1.2.2.2.4 Keys



The ADKs and other corporate keys are automatically added to each user's keyring.

1.2.2.2.5 Corporate Key

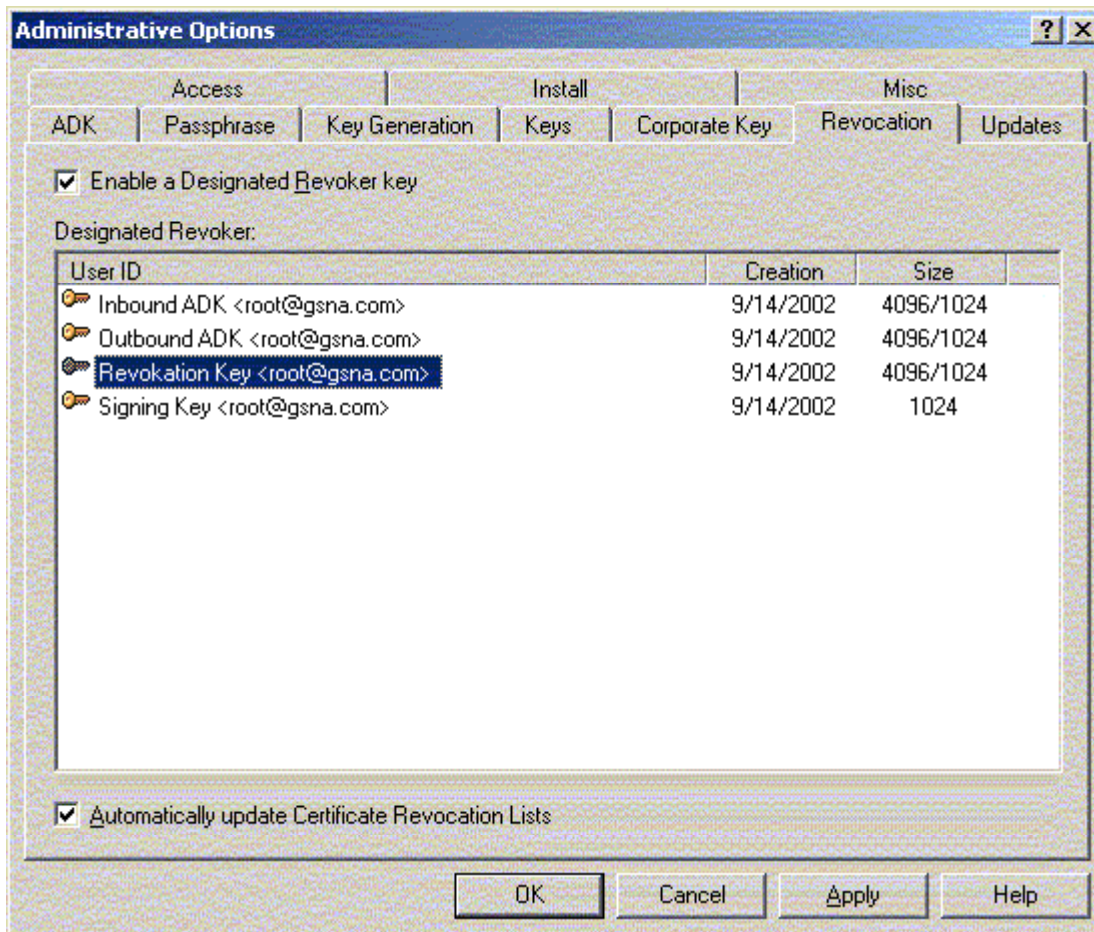


One key is designated the corporate signing key and a “meta-introducer” which can then designate other keys as trusted introducers [3]. When configured this way, any key signed by the corporate key automatically appears as valid to users, and the corporate key can designate other keys to work this way as well.

Think of it hierarchically. The root certificate in the organisation is the meta-introducer, the corporate signing key. Users can trust that any key signed by this key has been validated. This key can also designate other keys as trusted introducers, and users can trust any key signed by those keys as well.

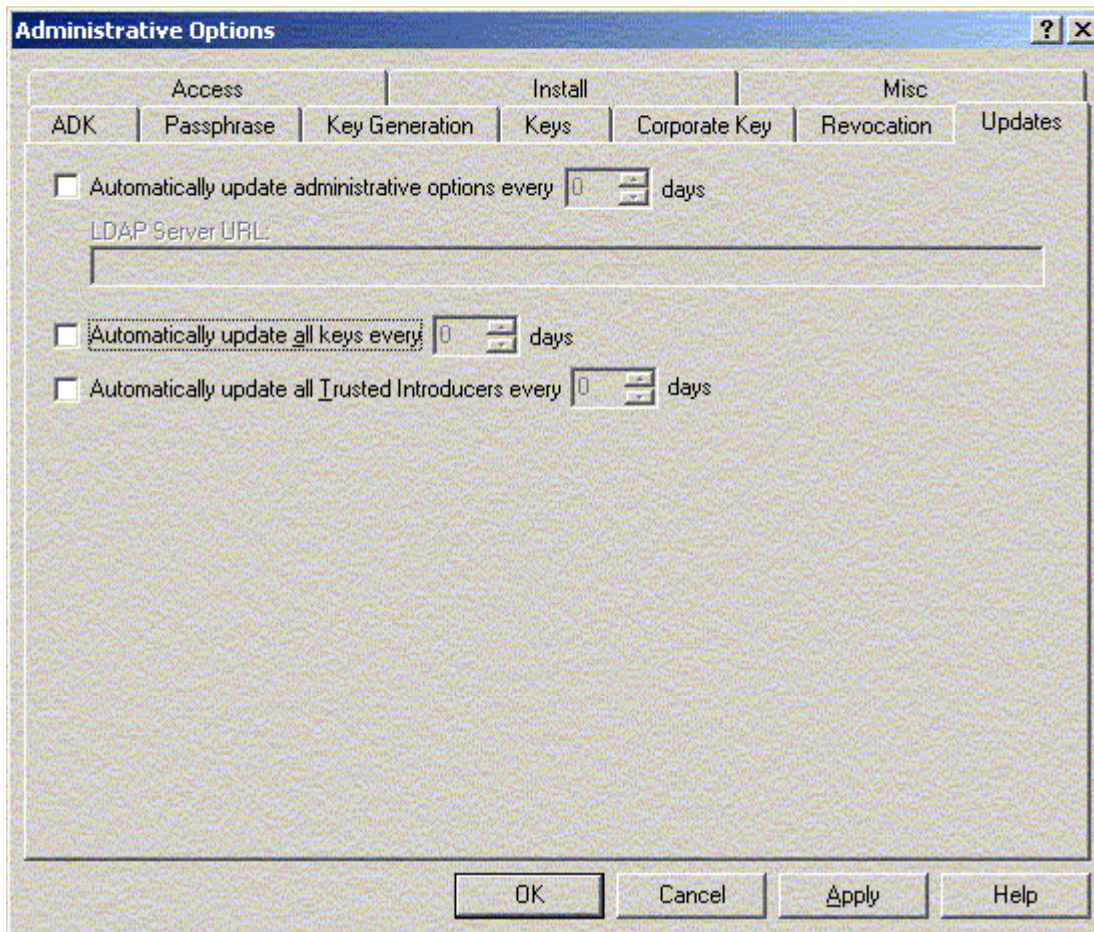
Obviously this implies the corporate signing key must be well protected.

1.2.2.2.6 Revocation



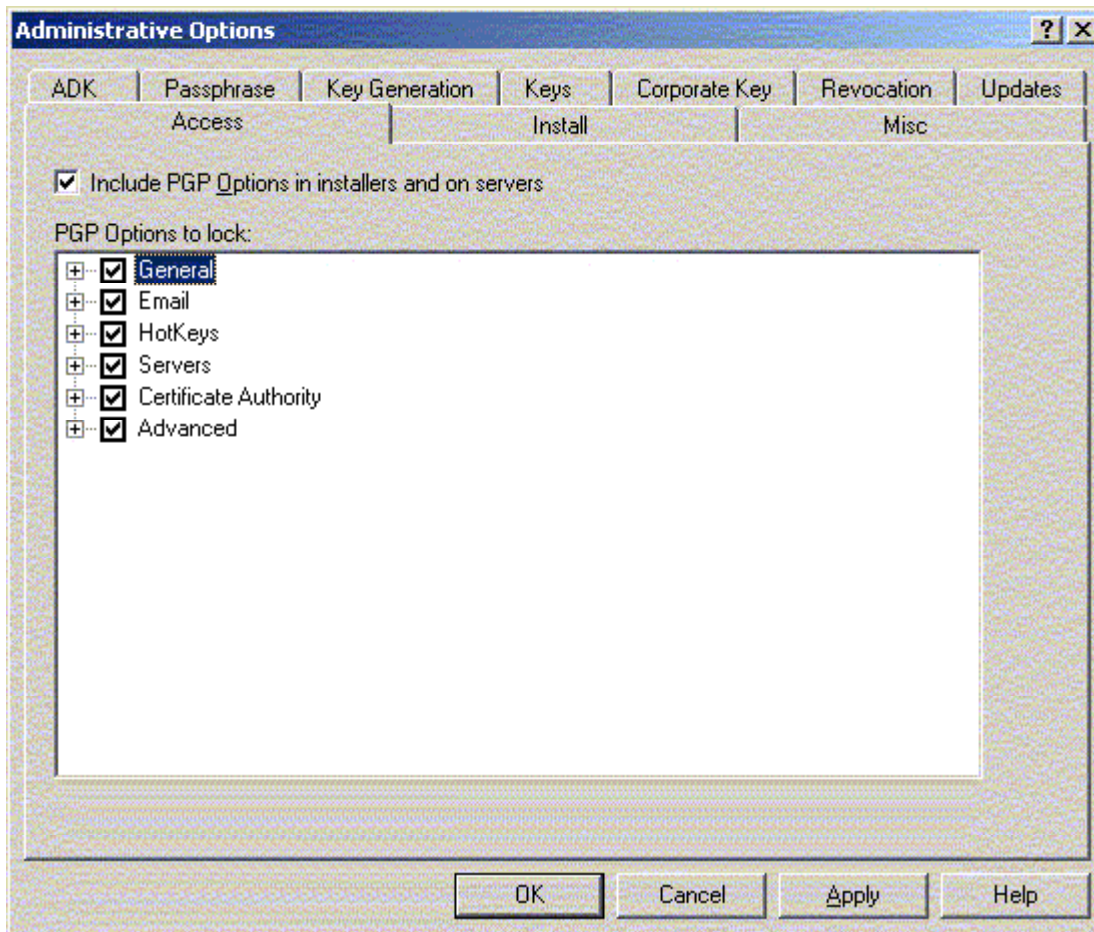
A designated revocation key simply allows the organisation to revoke users' keys (certificates) when necessary. There are many reasons to revoke a user's key: if the employee quits or is fired, if the user forgets his or her passphrase, if the user's only copy of the private key is destroyed, if the user's private key is compromised or the passphrase is revealed or discovered, etc.

1.2.2.2.7 Updates



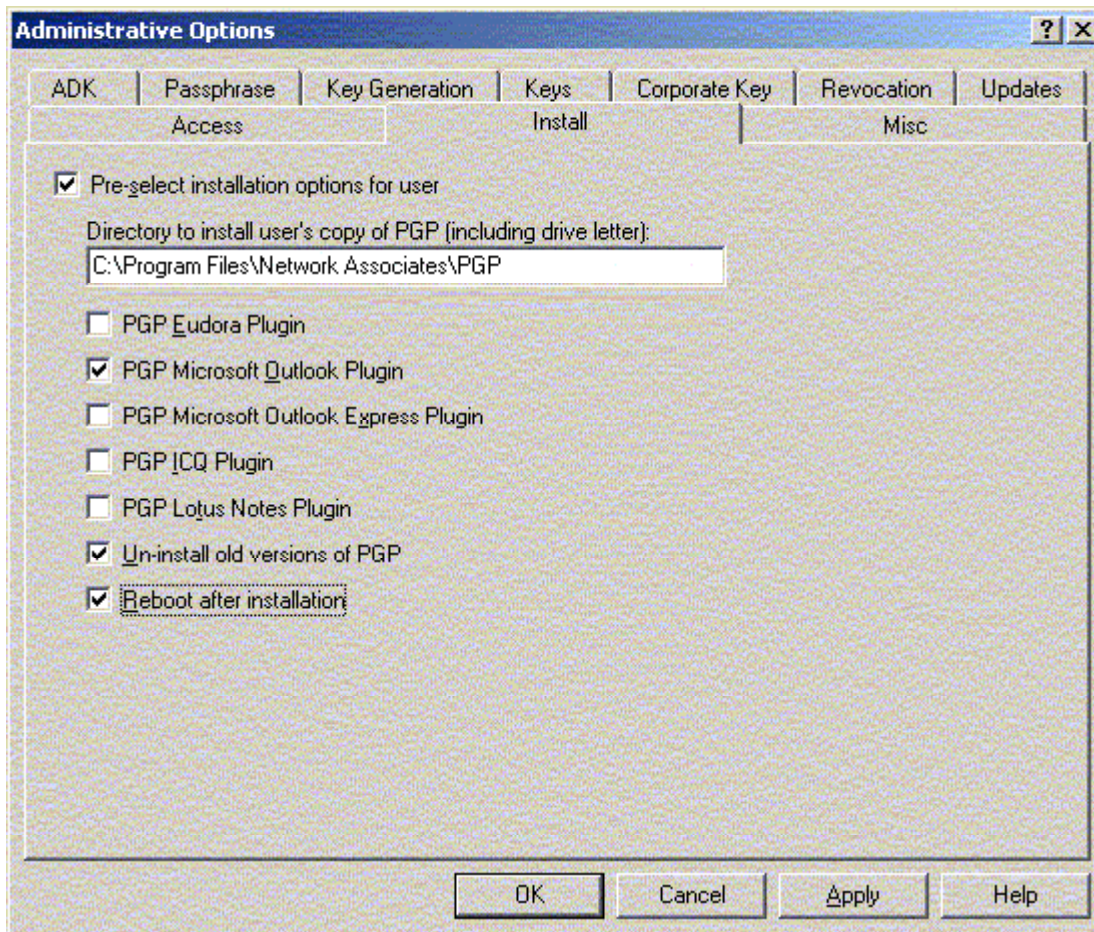
If a key server is used, options can be set to automatically update the administrative options in case they are changed, automatically update all the user's keys in case there are revocations or new signatures, and automatically update the trusted introducers. These are good options to use and all of them enhance security, but they can introduce potential problems such as network congestion, significant load on the key server, extra help desk calls when users get error messages about the operations failing or the server not responding, and extra administrative overhead. As long as the relevant infrastructures are in place these are probably acceptable risks for enhanced security, but not essential.

1.2.2.2.8 Access



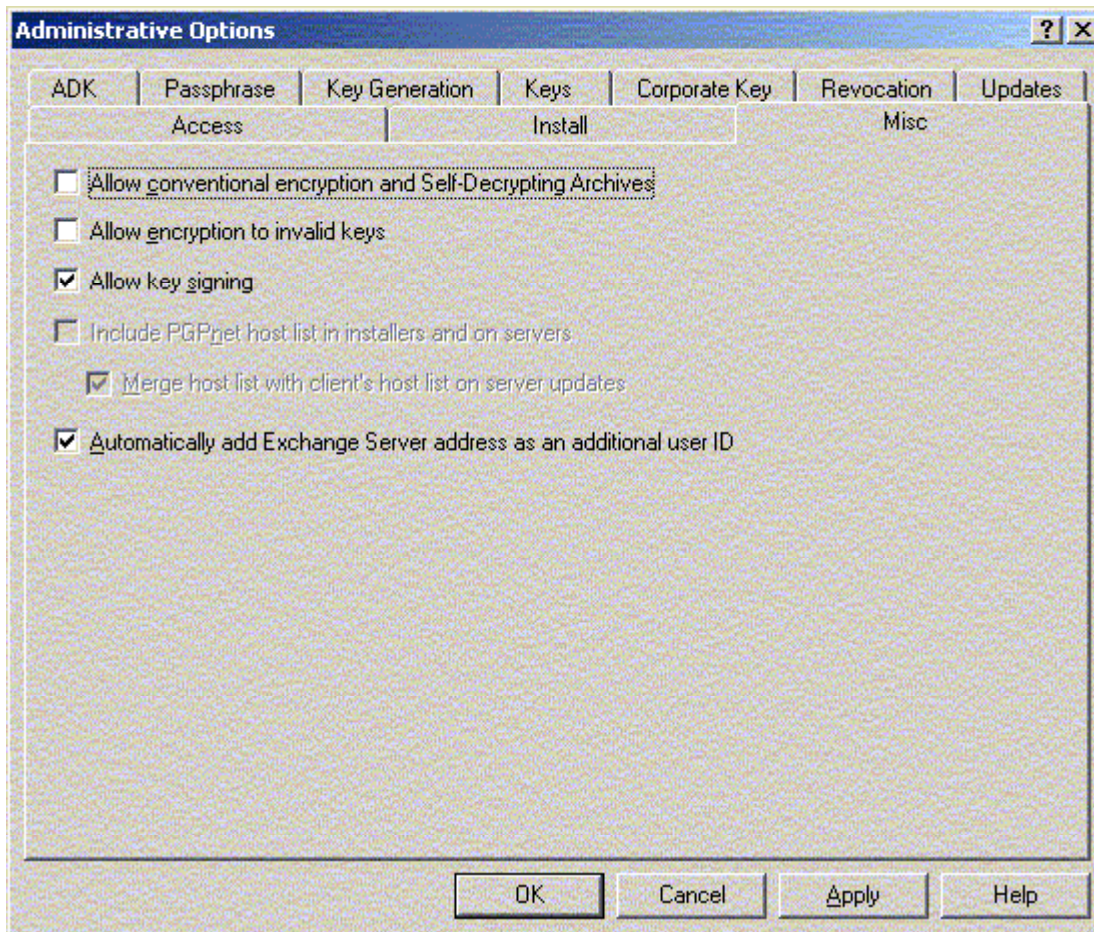
All of the PGP user options can be locked so that users cannot modify them. Locking certain options is important to security, such as the preferred algorithm, but most others only need to be locked to prevent the user from “shooting himself in the foot” by changing something and ending up with undesirable results (e.g. the option to always encrypt to default key), or to prevent users from doing silly things like adding their own inappropriate comment block.

1.2.2.2.9 Install



Pre-selecting installation options for the user makes for a consistent software deployment—administrators will always know where the application is installed and only those features needed (e.g. plug-ins for email clients) will be installed. These options do not directly affect security though.

1.2.2.2.10 Miscellaneous



Allowing conventional encryption and creation of self-decrypting archives (SDAs) may be one of the most important security mistakes that can be made in setting PGP options. In the author's experience, users are more confused about these features and have more trouble with them than anything else about PGP.

Allowing conventional encryption and SDAs creates a password-sharing issue. While users will be forced to choose a password based on the administrative setting (above) of minimum length or quality, users often use their private key passphrase, and/or use the same password for every SDA they create, thoroughly degrading security. If, for example, a user always uses the same password for SDAs and sends them to recipients outside the company, the files can be intercepted by attackers who can try passwords continuously until cracked—and since all the SDA passwords are the same, the attacker will be able to decrypt all SDAs intercepted.

Allowing key signing probably cannot hurt. If untrusted keys are allowed to be introduced into the organisation (difficult to prevent since keys can be imported from email messages), users can sign them and share them. Users can also set the trust level on another user's key basically making that user a trusted introducer. However these will tend to be isolated cases. User education about

checking for the corporate signature will help.

Automatically adding the Exchange Server address is a helpful feature for organisations using Exchange, as it helps PGP to determine which key to use when encrypting email. However more info is added to public keys, possibly leading to information leakage to attackers.

1.2.2.3 Associated Policies

In addition to the user and administrative options summarised above, the audit must look at certain related policies governing the use of PGP in the organisation. These will be detailed in the audit checklist later, but some examples would be: how trusted introducers are assigned, how data recovery with ADKs is done, etc.

1.3 Current State of Practice

No audit checklists for PGP seem to exist, nor do any tools for analysing PGP options for security, as indicated by a fair number of Google [20] web searches for relevant keywords. The best resources for evaluating PGP options seem to be the *PGP Administrator's Guide* and *PGPmail User's Guide*, although they are hardly audit checklists. If a checklist of any kind does exist, it either is not published on the Internet or is quite obscure and difficult to find.

Is it worth it to audit PGP options? The author thinks it is if PGP is used in an enterprise or really any commercial environment where confidential data is valued, as some PGP options when set poorly can lead to disclosure or loss of non-repudiation. Organisations that use PGP as an email PKI or that go to the extent of using it in conjunction with smartcards for authentication certainly need to pay careful attention to how the product is configured.

In the next section an audit checklist will be created from scratch based on the user and administrative options summarised above in Section 1.2.2.1 and Section 1.2.2.2, respectively. The audit checklist will not be a simple list of PGP options with the optimal setting for each; it is a better use of resources to focus on the control objectives: ensure the user cannot change options to degrade security, ensure policies are such that the security of the infrastructure is not threatened, and ensure other protections exist if not covered by a PGP option or policy (e.g. technological control over storage of the private key).

2 Audit Checklist

2.1 Guide to Reading the Checklist

Option/Policy	(#) What is being evaluated.
Objective	What is to be achieved.
Risk(s)	What can go wrong.
Likelihood	How likely it is to go wrong (high, medium, low).
Consequence(s)	What happens if it does go wrong.
Residual or Obverse Risk(s)	Remaining risk if any, or the risk involved with meeting the objective, if any.
Test(s)	How to test for compliance, whether it's an observation or stimulus-response, and whether objective/subjective.
Compliance	Whether the system is compliant and how you know.
Resource(s)	[From what source(s) came the info to decide on this objective.]

2.2 Blank Table for One Checklist Item

Option/Policy	()
Objective	
Risk(s)	
Likelihood	
Consequence(s)	
Residual or Obverse Risk(s)	
Test(s)	
Compliance	
Resource(s)	[]

2.3 The Audit Checklist

Note that there is not a one-to-one correspondence of checklist entries to PGP options. Not all options are critical to security, so the administrator is free to set them as he or she sees fit depending on the needs of the organisation. The auditor should still look at all the options not on the checklist and see if they have been set to peculiar values, as altogether they could present some risks that a thorough auditor could point out even if the risks are not to security. An example of one PGP option that does not really need to be audited is first in the list. The reader should be able to see how a knowledgeable auditor could help a less knowledgeable administrator in interpreting the pros and cons of options such as this.

Also some options such as the certificate authority tab in user options will only be used in certain organisations, but if used they must be audited. Options not used by the organisation being audited for Section 3 of this paper are not included in the checklist.

For the purpose of the audit checklist's "reference" line item, the reference number 99 serves to indicate the item in question is drawn from the author's own experience.

Option/Policy	(1) Always encrypt to default key should be ON.
Objective	Help keep users from locking themselves out of their own data.
Risk(s)	Users could send encrypted messages without encrypting to their own keys.
Likelihood	High. Users do not typically copy themselves on emails.
Consequence(s)	Users would not be able to read their own sent messages, which could lead to help desk calls or requests for data recovery.
Residual or Obverse Risk(s)	If no default key is set this option doesn't help and PGP will warn the user every time encryption is performed that there is no default key. If high secrecy is necessary, encrypting to the originator's key can reveal the source of a message in traffic analysis.
Test(s)	View option's checkbox. Objective.
Compliance	If checkbox is checked.
Resource(s)	[2, 19]

Option/Policy	(2) Faster key generation should be OFF.
Objective	Use most secure method of generating keys.
Risk(s)	A cryptanalytic attack against pre-calculated primes.
Likelihood	Low. No such attack as of yet.
Consequence(s)	Disclosure of confidential data, possible loss of non-repudiation.
Residual or Obverse Risk(s)	Slower key generation.
Test(s)	View option's checkbox. Objective.
Compliance	If checkbox is unchecked.
Resource(s)	[2, 19]

Option/Policy	(3) Comment block is blank.
Objective	Do not reveal info in ASCII-armoured files.
Risk(s)	Operationally confidential data can be revealed.
Likelihood	High. All emails are sent ASCII-armoured.

Consequence(s)	Attackers sniffing traffic can see the comment block.
Residual or Obverse Risk(s)	None.
Test(s)	View comment block entry box. Objective.
Compliance	If comment block entry box empty.
Resource(s)	[22]

Option/Policy	(4) Do not cache passphrase.
Objective	Prevent local attacks due to cached passphrase.
Risk(s)	If passphrase is cached, malicious user does not need it.
Likelihood	Medium. Victim must leave PC unattended.
Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	Inconvenient to users who decrypt/sign data frequently.
Test(s)	View radio button. Objective.
Compliance	If radio button for do not cache is selected.
Resource(s)	[2]

Option/Policy	(5) Internal key server(s) listed, no external key servers listed.
Objective	Use only trusted certificate repositories.
Risk(s)	Company keys sent to public key server, untrusted keys imported to user's keyring.
Likelihood	High or medium depending on other settings.
Consequence(s)	Information leakage, MIM attack.
Residual or Obverse Risk(s)	Inconvenience if all key exchanges done manually.
Test(s)	View server tab. Objective. Note: If servers are not locked in Admin options, users can add/delete/modify servers, so additional controls like firewall rules may be warranted.
Compliance	Only authorised server(s) listed.
Resource(s)	[2, 99]

Option/Policy	(6) Preferred algorithm is AES.
Objective	Use the best symmetric algorithm available as default.
Risk(s)	If an older/weaker algorithm is chosen it may be easier to break encrypted messages. Other algorithms are slightly slower.
Likelihood	Low. All ciphers in PGP are very good.
Consequence(s)	Disclosure of confidential data.
Residual or Obverse Risk(s)	There may be unknown implementation flaws in certain algorithms.
Test(s)	View preferred algorithm selection. Objective.
Compliance	If AES selected as preferred algorithm.

Resource(s)	[11, 18]
--------------------	----------

Option/Policy	(7) Automatic keyring backup not set to shared directory.
Objective	Do not disclose PGP keys.
Risk(s)	Private key compromise.
Likelihood	High. If keyring saved in a shared folder, it is compromised.
Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	None.
Test(s)	View automatic backup location if any, then view security policy for the automatic backup location to determine if shared. Objective.
Compliance	If automatic backup location not shared.
Resource(s)	[99]

Option/Policy	(8) Enable & enforce inbound & outbound ADK.
Objective	Provide means to recover employee data without key escrow.
Risk(s)	If users are allowed to encrypt data without an ADK or escrowed key—in the latter case especially if users create their own keys—then data loss could result.
Likelihood	High. If nothing else, users forget passwords frequently.
Consequence(s)	Data loss.
Residual or Obverse Risk(s)	Slightly greater chance of disclosure of confidential data as more keys are used for encryption, meaning there are more keys available for decryption—and security is only as good as the weakest link.
Test(s)	A test whereby the auditor would ask a user to encrypt something to see what keys were used would be required. To test inbound ADK, the auditor would need the public key of a user and try to encrypt something to it. For outbound ADK, the “enforce” option is tested by attempting to remove the ADK from the PGP dialog where keys are confirmed. Objective; stimulus-response.
Compliance	If the tests described above yield desired results. “Partial compliance” is acceptable for inbound ADK because it is not enforceable.
Resource(s)	[3, 23]

Option/Policy	(9) Enforce minimum of eight characters in passphrase.
Objective	Try to keep users from selecting poor passphrases.
Risk(s)	A poor passphrase is more easily guessed.
Likelihood	High. Users have many passwords to remember and often do things to make it easier, leading to poor passwords.

Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	A minimum length does not guarantee a good passphrase; more helpdesk calls to recover lost data—PGP passphrases cannot be “reset” like many other passwords.
Test(s)	A user’s client must be used to either create a new key or change the passphrase on an existing key. If a passphrase less than the minimum length is given PGP should refuse it. Objective; stimulus-response.
Compliance	If a passphrase less than the minimum cannot be chosen.
Resource(s)	[16, 23]

Option/Policy	(10) Key generation is allowed and key properties are set according to company policy or best practice.
Objective	Allow users to generate keys to ensure privacy and reduce work of administrator. Set properties such that good keys are created.
Risk(s)	If users do not generate their own keys, it is possible that a copy could be left on the machine used to generate users’ keys, or in the case of electronic transfer they could be intercepted. Weak keys could be created without set properties.
Likelihood	Medium. Depends on other factors like key transport method.
Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	Users can generate multiple keys and confuse themselves or never get old keys properly revoked.
Test(s)	Use a user’s client to generate a new key. If key can be generated, ensure properties of resulting key are correct. Objective; stimulus-response.
Compliance	Key can be generated and has correct properties.
Resource(s)	[3]

Option/Policy	(11) Corporate key is set as meta-introducer.
Objective	Designate a root certificate for the “web of trust.”
Risk(s)	Web of trust is weaker without a meta-introducer.
Likelihood	Low. A meta-introducer is not necessarily required as long as users know to trust keys signed by the designated corporate key.
Consequence(s)	Web of trust weaker, user confusion, more administrative overhead.
Residual or Obverse Risk(s)	PGP “web of trust” does not work as seamlessly as a real PKI with a root CA. Also, having a meta-introducer requires extra precautions to be taken due to the added authority.

Test(s)	Add a new user key to another user's keyring and observe if the new key is automatically validated due to being signed by the meta-introducer. Objective; stimulus-response.
Compliance	If the key that is supposed to be the meta-introducer is the meta-introducer.
Resource(s)	[3]

Option/Policy	(12) Revocation key is set.
Objective	Corporate key used to revoke user keys as necessary.
Risk(s)	Inability to revoke user keys.
Likelihood	High.
Consequence(s)	Confusion due to users continuing to use an old or compromised key.
Residual or Obverse Risk(s)	External parties that cannot connect to internal key server, or users who do not synchronise with key server will not know a key is revoked. Key can be misused to revoke keys illegitimately.
Test(s)	Create a new key with a user's client and observe the Revokers tab in Key Properties. Ask the administrator to revoke a test key. Objective; stimulus-response (if key revoked, but could be verified by observing key IDs).
Compliance	If keys are created with revocation key attached and revocation key can in fact be used to revoke keys.
Resource(s)	[3]

Option/Policy	(13) All security-critical PGP options (those mentioned in this checklist) are locked so users cannot change them.
Objective	Do not allow user to change options that can degrade security.
Risk(s)	Users could change PGP options and degrade security.
Likelihood	Medium. Depends on the option.
Consequence(s)	Numerous, depending on option.
Residual or Obverse Risk(s)	Possible user inconvenience.
Test(s)	Look at all options in a user client and try to change each one. Note which are changeable. Objective
Compliance	If the security-critical options (which in itself may be subjective) are unchangeable.
Resource(s)	[3, 19, 99]

Option/Policy	(14) Allow conventional encryption & SDAs set according to company policy.
Objective	Disallow these features if possible due to password sharing and weaker security.

Risk(s)	Users may pick poor passwords, and data protected this way is significantly more vulnerable to attack.
Likelihood	High.
Consequence(s)	Unintentional disclosure of user PGP passphrases (and possible loss of non-repudiation), disclosure of confidential data.
Residual or Obverse Risk(s)	If SDAs are not allowed, users will be unable to securely communicate with people who do not have PGP.
Test(s)	Attempt to create an SDA with a user's client. Objective; stimulus-response.
Compliance	If company policy allows SDAs and SDAs can be created; if company policy disallows SDAs and SDAs cannot be created.
Resource(s)	[3, 99]

Option/Policy	(15) Do not allow encryption to invalid keys.
Objective	Lessen the extent to which MIM attack can be performed.
Risk(s)	Users may encrypt confidential data using a key that should not be trusted.
Likelihood	Medium. Depends on user education and other compensating controls.
Consequence(s)	Disclosure of confidential data.
Residual or Obverse Risk(s)	Users may still be able to make invalid keys valid to bypass this restriction. Disallowing encryption to invalid keys is a minor inconvenience.
Test(s)	Import an invalid key to a user's client and attempt to encrypt data to it. Objective; stimulus-response.
Compliance	If encryption fails.
Resource(s)	[3, 99]

Option/Policy	(16) Do not automatically add Exchange Server address to keys.
Objective	Avoid revealing confidential info.
Risk(s)	Internal user IDs and other info can be revealed.
Likelihood	High.
Consequence(s)	Attackers who come across public keys (which are usually not treated as sensitive) can discover bits of info about the company's network and processes. The fact that Exchange is used will be known, and user IDs may be seen and can be used to help break into systems.
Residual or Obverse Risk(s)	Adding the Exchange Server ID to keys usually makes it easier to send PGP-encrypted messages to other employees on the same network, but this probably isn't necessary.

Test(s)	Create a key with a user's client and see if the Exchange ID is automatically added. Objective; stimulus-response.
Compliance	If Exchange ID not added to key when created.
Resource(s)	[99]

Option/Policy	(17) A policy exists for validating new user keys.
Objective	Employee keys should be signed by the corporate key so users know it is trusted.
Risk(s)	User confusion, inability to encrypt depending on other options.
Likelihood	Medium. Depends on many factors.
Consequence(s)	Users may not be able to use PGP because keys are invalid, users may become accustomed to trusting invalid keys.
Residual or Obverse Risk(s)	Policy may not be adhered to.
Test(s)	Ask administrator for documentation and to describe process. If an internal key server is used, policy should state service level agreement (SLA) for validating new user keys as best practice. Subjective. A stimulus-response test could be done, wherein a new user key is created to see if the SLA for validating the key is met.
Compliance	Policy exists.
Resource(s)	[3, 99]

Option/Policy	(18) Private keyrings are kept by default in a folder only the owner can access.
Objective	Prevent compromise of private keys.
Risk(s)	Private key compromise can lead to confidential data disclosure or loss of non-repudiation.
Likelihood	Medium. Compensating control is passphrase.
Consequence(s)	Confidential data disclosure, loss of non-repudiation.
Residual or Obverse Risk(s)	Administrators can always access all data on company-owned information systems. User is responsible for integrity of his or her own private keyring and any backups.
Test(s)	Install a new copy of PGP and note where private keyring is automatically created. Observe OS controls on the location. Objective.
Compliance	If default location for private keyring is not shared or given permissions for other users to access.
Resource(s)	[99]

Option/Policy	(19) A policy exists for data recovery using ADKs.
----------------------	--

Objective	An administrator with access to the ADKs can essentially read anyone's encrypted email and files so there should be a policy for proper use.
Risk(s)	Rogue administrator who gets access to encrypted data could decrypt it. Random user who gets access to encrypted data could request administrator decrypt it even though it does not belong to him/her.
Likelihood	Low. Administrator would probably not also have access to user's email at least. In the case of a user requesting data recovery of someone else's data, Administrator should know by seeing which keys were used whether he or she is dealing with the right user.
Consequence(s)	Disclosure of confidential data.
Residual or Obverse Risk(s)	Policy may not be followed.
Test(s)	Ask administrator for documentation and to describe policy. There may be an SLA, which could be tested. Subjective.
Compliance	Policy exists.
Resource(s)	[99]

Option/Policy	(20) Policy exists for revocation of terminated users.
Objective	Minimise potential for terminated employee to use key.
Risk(s)	Terminated user could send signed messages containing orders for work to be done, requesting info, etc., to employees who do not know sender was terminated).
Likelihood	Medium. Depends on organisation.
Consequence(s)	Disclosure of confidential data, other consequences depending on circumstances.
Residual or Obverse Risk(s)	Policy may not be followed; depending on key/CRL update frequency there may still be a window of opportunity.
Test(s)	Ask administrator for documentation and to describe policy. There should be an SLA, which could be tested. Subjective.
Compliance	Policy exists.
Resource(s)	[99]

3 Audit Evidence

3.1 Conducting the Audit

A complete audit based on the checklist in Section 2 above was performed. Ten of the tests, five of which are stimulus-response tests, were taken from the completed checklist and are presented in this section.

Checklist tables are copied, and the Compliance cell is turned green, yellow, or

red to indicate compliance level. Comments and evidence appear after each table. When one screenshot serves as evidence for multiple checks, only one screenshot follows all the tables and comments to which it applies.

Option/Policy	(2) Faster key generation should be OFF.
Objective	Use most secure method of generating keys.
Risk(s)	A cryptanalytic attack against pre-calculated primes.
Likelihood	Low. No such attack as of yet.
Consequence(s)	Disclosure of confidential data, possible loss of non-repudiation.
Residual or Obverse Risk(s)	Slower key generation.
Test(s)	View option's checkbox. Objective.
Compliance	If checkbox is unchecked.
Resource(s)	[2, 19]

"Faster key generation" checkbox was observed to be unchecked and locked in a user installation. (See Figure 3-1.)

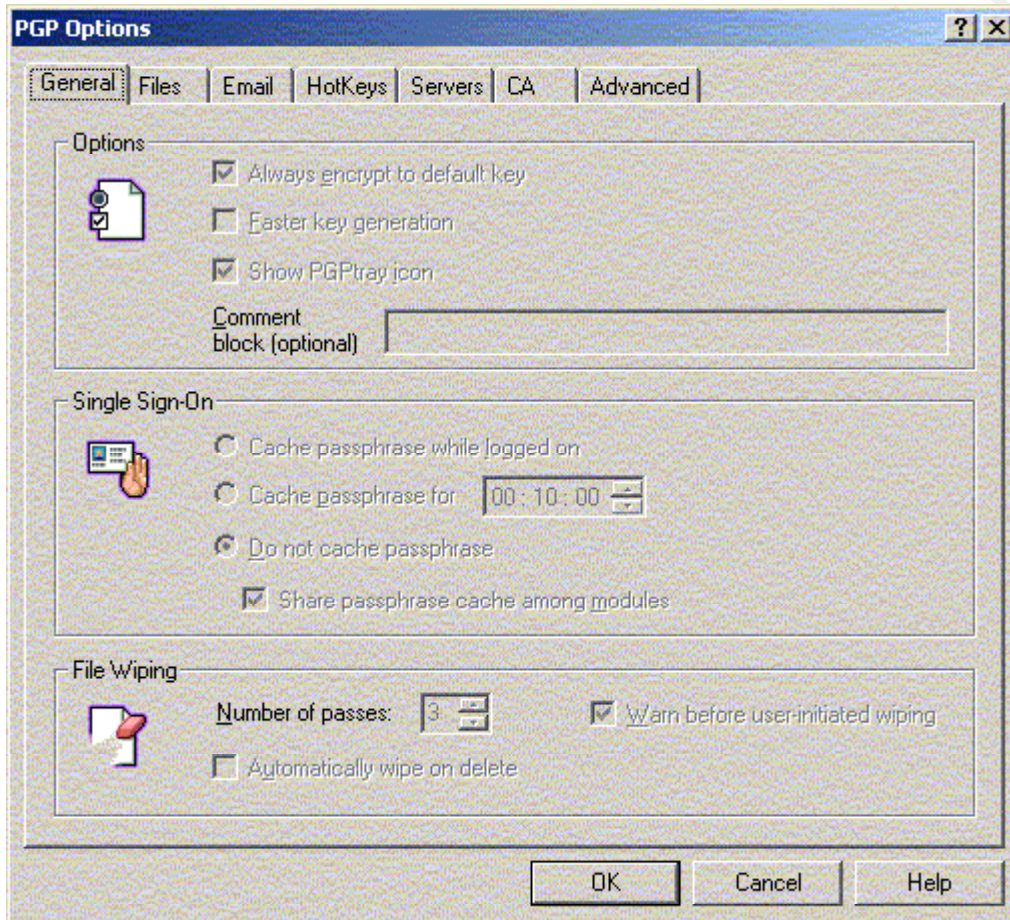
Option/Policy	(3) Comment block is blank.
Objective	Do not reveal info in ASCII-armoured files.
Risk(s)	Operationally confidential data can be revealed.
Likelihood	High. All emails are sent ASCII-armoured.
Consequence(s)	Attackers sniffing traffic can see the comment block.
Residual or Obverse Risk(s)	None.
Test(s)	View comment block entry box. Objective.
Compliance	If comment block entry box empty.
Resource(s)	[22]

"Comment block" entry box was observed to be blank and locked in a user installation. (See Figure 3-1.)

Option/Policy	(4) Do not cache passphrase.
Objective	Prevent local attacks due to cached passphrase.
Risk(s)	If passphrase is cached, malicious user does not need it.
Likelihood	Medium. Victim must leave PC unattended.
Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	Inconvenient to users who decrypt/sign data frequently.
Test(s)	View radio button. Objective.
Compliance	If radio button for do not cache is selected.
Resource(s)	[2]

“Do not cache passphrase” radio button was observed to be selected and locked in a user installation. (See Figure 3-1.)

Figure 3-1, audit evidence for General options.



Option/Policy	(8) Enable & enforce inbound & outbound ADK.
Objective	Provide means to recover employee data without key escrow.
Risk(s)	If users are allowed to encrypt data without an ADK or escrowed key—in the latter case especially if users create their own keys—then data loss could result.
Likelihood	High. If nothing else, users forget passwords frequently.
Consequence(s)	Data loss.
Residual or Obverse Risk(s)	Slightly greater chance of disclosure of confidential data as more keys are used for encryption, meaning there are more keys available for decryption—and security is only as good as the weakest link.

Test(s)	A test whereby the auditor would ask a user to encrypt something to see what keys were used would be required. To test inbound ADK, the auditor would need the public key of a user and try to encrypt something to it. For outbound ADK, the “enforce” option is tested by attempting to remove the ADK from the PGP dialog where keys are confirmed. Objective; stimulus-response.
Compliance	If the tests described above yield desired results. “Partial compliance” is acceptable for inbound ADK because it is not enforceable.
Resource(s)	[3, 23]

Account with user installation was used to encrypt an email to an external address (non-company key) and an internal address (company key). PGP Recipient Selection dialog showed Outbound ADK selected and locked. Outbound ADK used, from local keyring, has the correct key ID. Therefore Outbound ADK is enabled and enforced properly. Dialog showed Inbound ADK selected but not locked and it was able to be removed as expected. (See Figure 3-2.)

Test was done to encrypt to a company key from a non-company account. Inbound ADK was selected but able to be removed, because the configuration does not honour remote ADK enforcement. (See Figure 3-3.)

Figure 3-2, showing locked outbound ADK, originator is a company install.

© SANS Institute 2000 - 2005

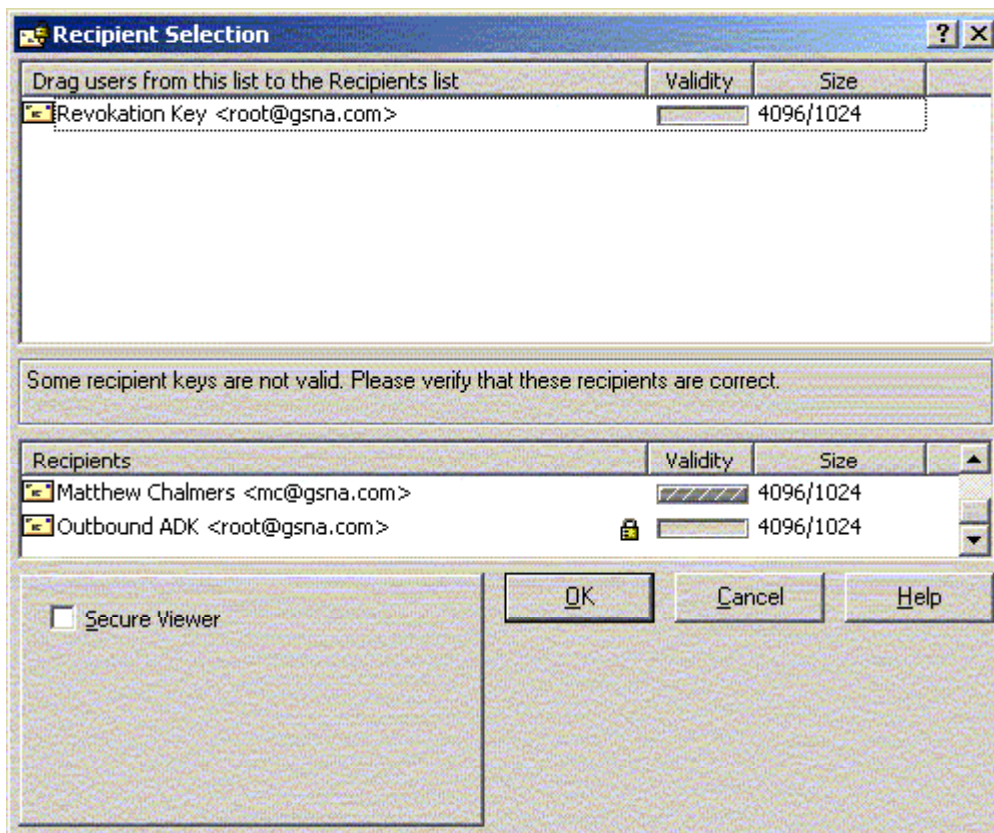
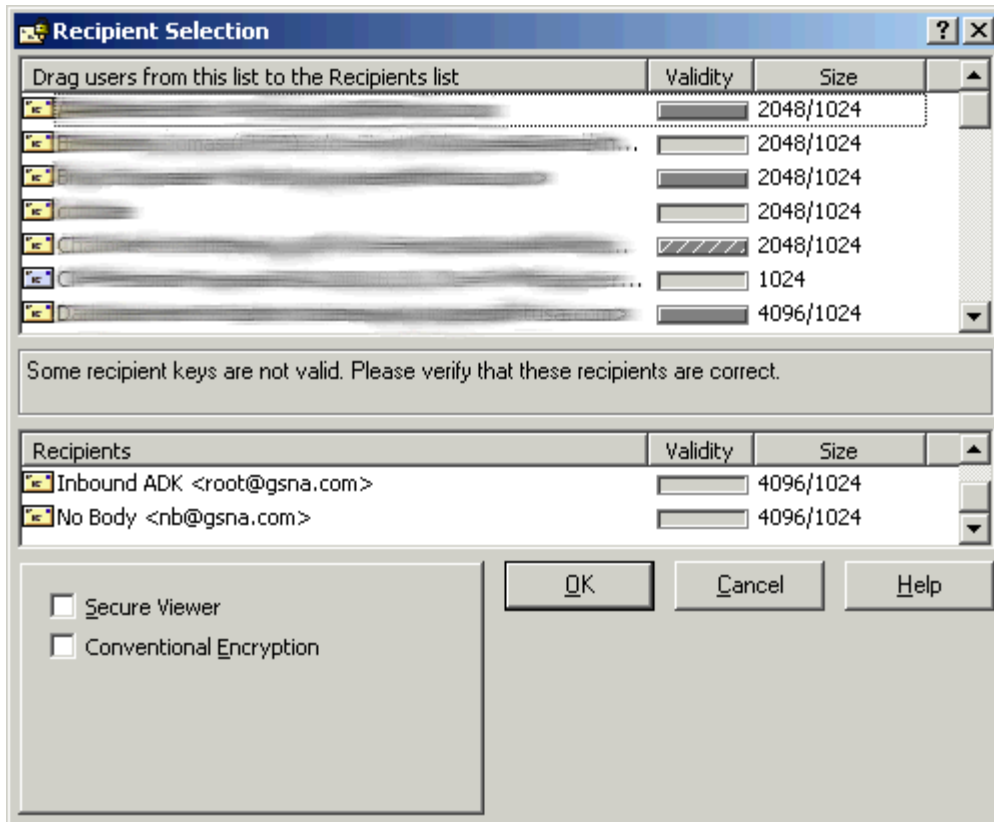


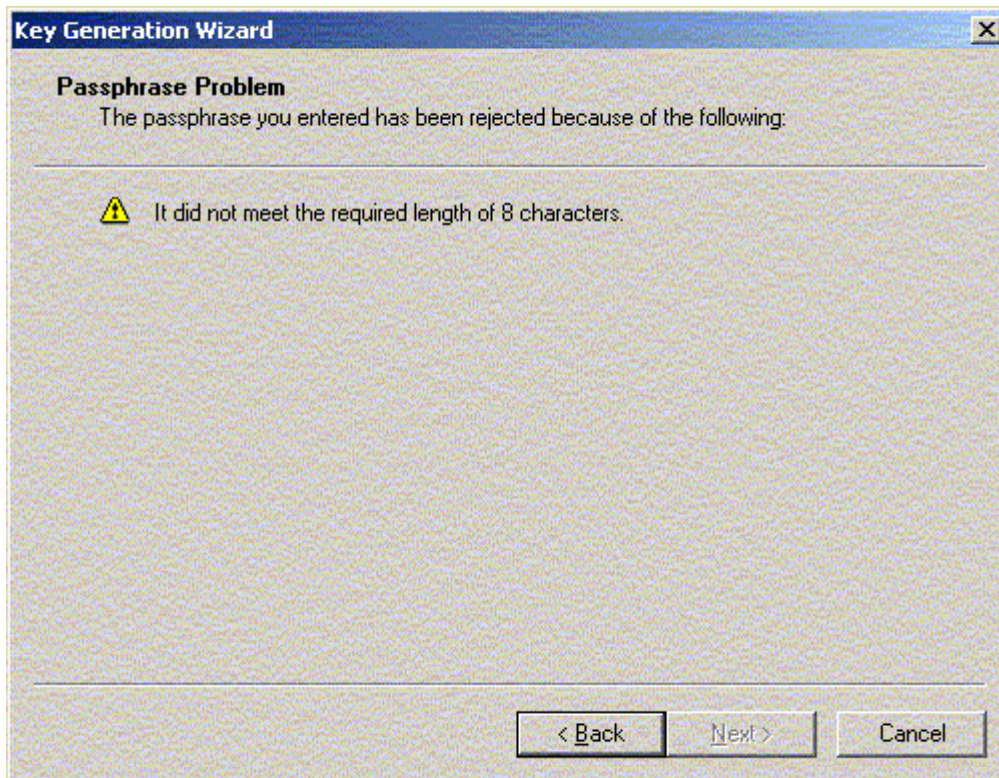
Figure 3-3, showing inbound ADK selected. Sensitive info has been smudged.



Option/Policy	(9) Enforce minimum of eight characters in passphrase.
Objective	Try to keep users from selecting poor passphrases.
Risk(s)	A poor passphrase is more easily guessed.
Likelihood	High. Users have many passwords to remember and often do things to make it easier, leading to poor passwords.
Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	A minimum length does not guarantee a good passphrase; more helpdesk calls to recover lost data—PGP passphrases cannot be “reset” like many other passwords.
Test(s)	A user’s client must be used to either create a new key or change the passphrase on an existing key. If a passphrase less than the minimum length is given PGP should refuse it. Objective; stimulus-response.
Compliance	If a passphrase less than the minimum cannot be chosen.
Resource(s)	[16, 23]

A key was created with a user installation, and PGP would not allow the process to proceed when a passphrase of less than eight characters was chosen. Note disabled Next button. (See Figure 3-4.)

Figure 3-4, showing error message from PGP regarding passphrase length.

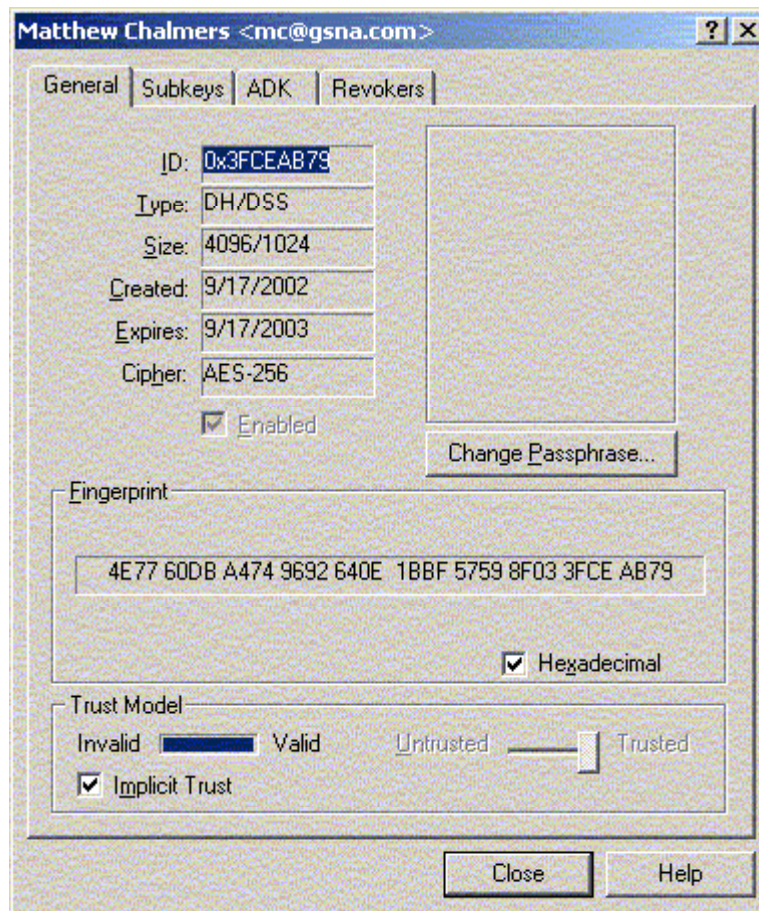


Option/Policy	(10) Key generation is allowed and key properties are set according to company policy or best practice.
Objective	Allow users to generate keys to ensure privacy and reduce work of administrator. Set properties such that good keys are created.
Risk(s)	If users do not generate their own keys, it is possible that a copy could be left on the machine used to generate users' keys, or in the case of electronic transfer they could be intercepted. Weak keys could be created without set properties.
Likelihood	Medium. Depends on other factors like key transport method.
Consequence(s)	Disclosure of confidential data, loss of non-repudiation.
Residual or Obverse Risk(s)	Users can generate multiple keys and confuse themselves or never get old keys properly revoked.
Test(s)	Use a user's client to generate a new key. If key can be generated, ensure properties of resulting key are correct. Objective; stimulus-response.
Compliance	Key can be generated and has correct properties.
Resource(s)	[3]

A key was generated with a user installation (evidencing key generation ability) and the properties thereof were displayed, showing the key meets requirements:

type, minimum length, maximum life, preferred cipher, ADK and designated revoker. (See Figure 3-5.)

Figure 3-5, showing properties of a user-generated key.

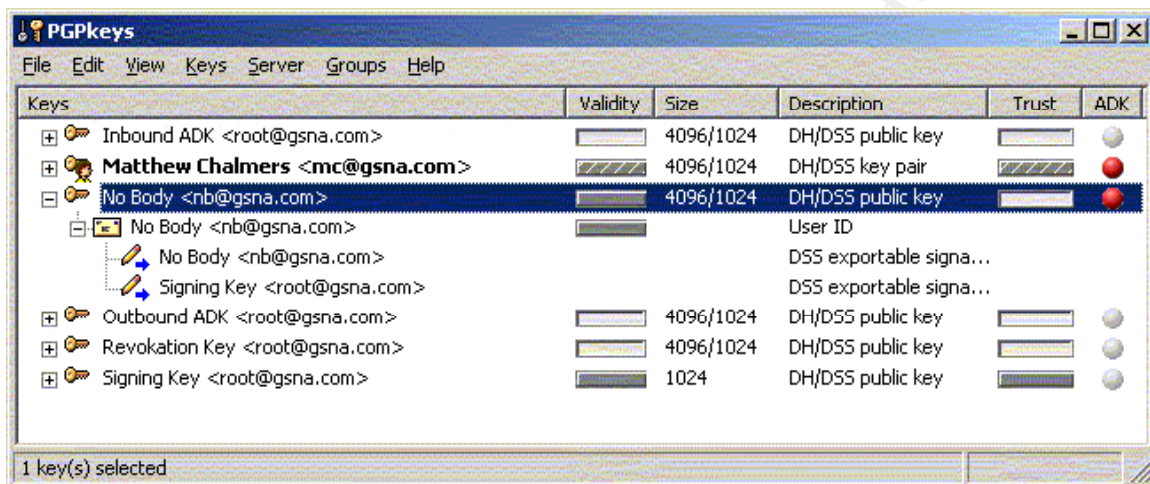


Option/Policy	(11) Corporate key is set as meta-introducer.
Objective	Designate a root certificate for the “web of trust.”
Risk(s)	Web of trust is weaker without a meta-introducer.
Likelihood	Low. A meta-introducer is not necessarily required as long as users know to trust keys signed by the designated corporate key.
Consequence(s)	Web of trust weaker, user confusion, more administrative overhead.
Residual or Obverse Risk(s)	PGP “web of trust” does not work as seamlessly as a real PKI with a root CA. Also, having a meta-introducer requires extra precautions to be taken due to the added authority.
Test(s)	Add a new user key to another user’s keyring and observe if the new key is automatically validated due to being signed by the meta-introducer. Objective; stimulus-response.

Compliance	If the key that is supposed to be the meta-introducer is the meta-introducer.
Resource(s)	[3]

A public key signed by the corporate key was imported to another user's keyring. It was marked valid by PGP even though the user did not sign it. (See Figure 3-6.)

Figure 3-6, showing a public key marked valid without the user's signature.



Option/Policy	(15) Do not allow encryption to invalid keys.
Objective	Lessen the extent to which MIM attack can be performed.
Risk(s)	Users may encrypt confidential data using a key that should not be trusted.
Likelihood	Medium. Depends on user education and other compensating controls.
Consequence(s)	Disclosure of confidential data.
Residual or Obverse Risk(s)	Users may still be able to make invalid keys valid to bypass this restriction. Disallowing encryption to invalid keys is a minor inconvenience.
Test(s)	Import an invalid key to a user's client and attempt to encrypt data to it. Objective; stimulus-response.
Compliance	If encryption fails.
Resource(s)	[3, 99]

An external public key was imported to a user's keyring, and then an attempt was made to encrypt an email to that invalid key (unsigned by the user or corporate key, or any key the user trusts). PGP displayed an error message indicating this operation could not be performed. (See Figure 3-7.)

Figure 3-7, an error message indicating inability to encrypt to invalid keys.



Option/Policy	(18) Private keyrings are kept by default in a folder only the owner can access.
Objective	Prevent compromise of private keys.
Risk(s)	Private key compromise can lead to confidential data disclosure or loss of non-repudiation.
Likelihood	Medium. Compensating control is passphrase.
Consequence(s)	Confidential data disclosure, loss of non-repudiation.
Residual or Obverse Risk(s)	Administrators can always access all data on company-owned information systems. User is responsible for integrity of his or her own private keyring and any backups.
Test(s)	Install a new copy of PGP and note where private keyring is automatically created. Observe OS controls on the location. Objective.
Compliance	If default location for private keyring is not shared or given permissions for other users to access.
Resource(s)	[99]

Keyrings by default are stored under the user's profile in a folder called PGP within My Documents. While other non-administrator users on the local system are unable to view the keyrings there, it was found to be the case that by default the entire hard drive is shared in an unrestricted manner on the network, so any remote user, regardless of privilege level, without the victim user's password, can mount the hard drive and view all files in all folders on it. (See Figures 3-8 & 9.)

Figure 3-8, showing the share permissions for the hard drive.

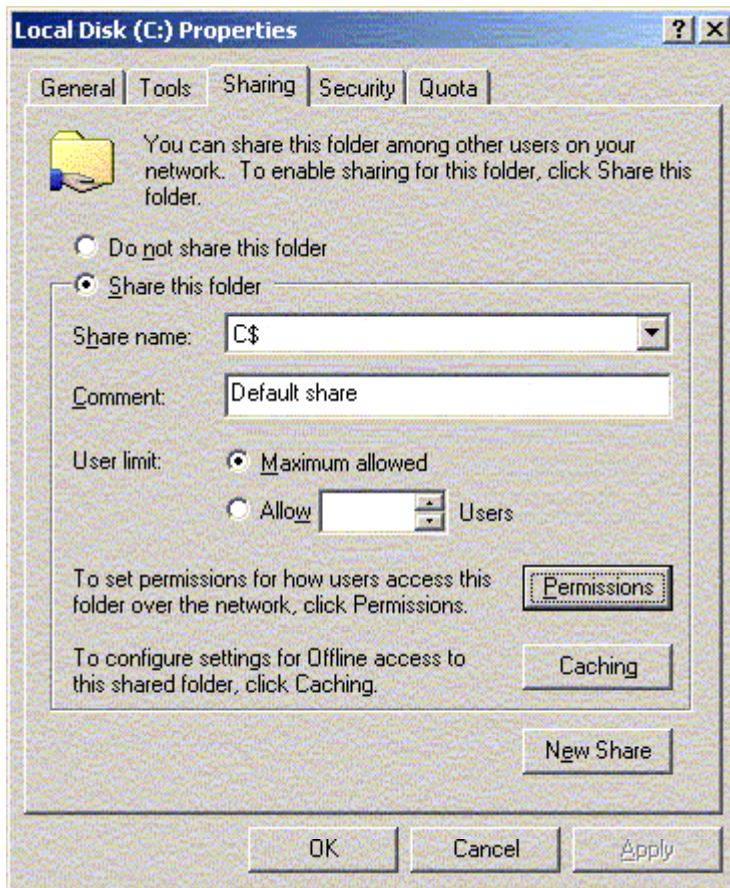
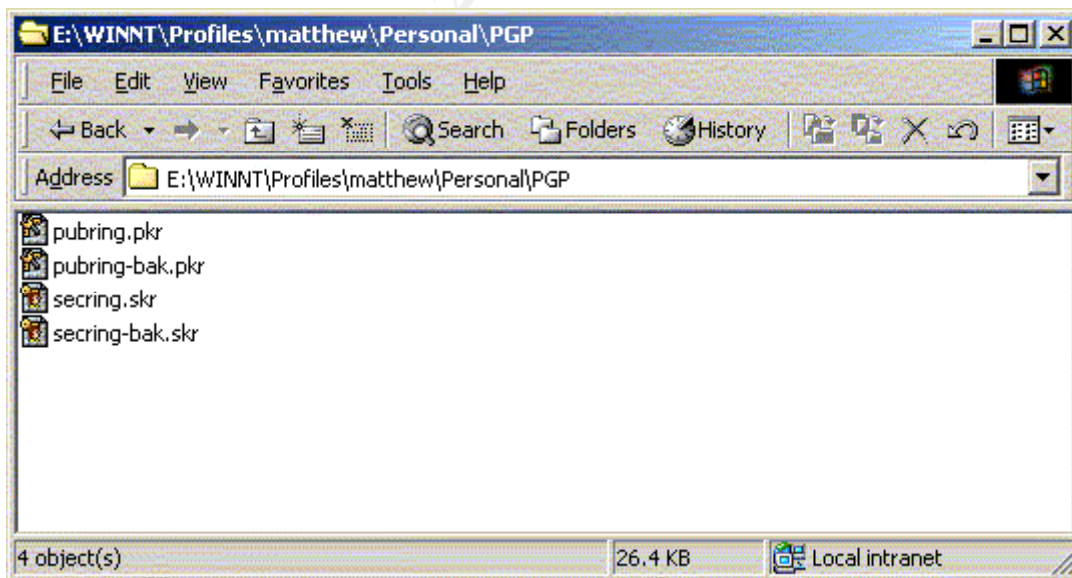


Figure 3-9, showing the keyrings found on the remote PC.




Option/Policy	(19) A policy exists for data recovery using ADKs.
----------------------	--

Objective	An administrator with access to the ADKs can essentially read anyone's encrypted email and files so there should be a policy for proper use.
Risk(s)	Rogue administrator who gets access to encrypted data could decrypt it. Random user who gets access to encrypted data could request administrator decrypt it even though it does not belong to him/her.
Likelihood	Low. Administrator would probably not also have access to user's email at least. In the case of a user requesting data recovery of someone else's data, Administrator should know by seeing which keys were used whether he or she is dealing with the right user.
Consequence(s)	Disclosure of confidential data.
Residual or Obverse Risk(s)	Policy may not be followed.
Test(s)	Ask administrator for documentation and to describe policy. There may be an SLA, which could be tested. Subjective.
Compliance	Policy exists.
Resource(s)	[99]

Administrator was asked to produce a documented policy for data recovery with ADKs. The Administrator showed the auditor an intranet page containing PGP user information, including a paragraph regarding forgotten passphrases. (See Figure 3-10.) However, the procedure is unclear and incomplete. After a thorough search by both Administrator and auditor, there also seems to be no corresponding back-end document such as Administrator instructions or procedures, or a true policy document containing any information about data recovery, key revocation, etc. While what does exist is a start, it is not considered compliant with the audit item.

Figure 3-10, showing the vague and incomplete procedure regarding ADKs.


[BACK TO TOP](#)

Trouble Shooting

User has forgotten passphrase.

- Ensure user doesn't have caps lock on.
- Warn user that anything he has encrypted with that key and passphrase will be lost if he can't remember his passphrase. (A business emergency request by an FVP or above is required to implement the ADK procedure for lost passphrases)
- If user insists he can't remember his passphrase refer to Information Security (████████████████████) to get his keys revoked.

3.2 Measuring Residual Risk

The control objectives, at a high level, for this audit were: to ensure good PGP options were chosen by the Administrator; to ensure users could not degrade security by changing options; and to ensure adequate policies were in place to support the infrastructure.

The audit certainly accomplished its objectives as far as determining what work remains to be done, and this remaining work translates into residual risk.

Specifically it was found that virtually all users on the network could map the drives of virtually all other users and gain access to their PGP keyrings. There may be advantages to configuring PCs this way by default, but PGP private keys are not things that should be shared at all. Non-repudiation, data confidentiality, and data integrity are all compromised. This cannot be viewed as an acceptable risk. This particular Local Area Network is configured such that each user has his or her own private network drive that other users cannot mount at all. If the hard drive sharing feature cannot be changed, perhaps users could be instructed to move their PGP keyrings to their private network drives. With good user education the cost would be minimal. Unfortunately the PGP installer cannot be forced to place the keyrings on the network drive by default, however, a bit of scripting costing little in resources could be done to take care of the situation at installation time.

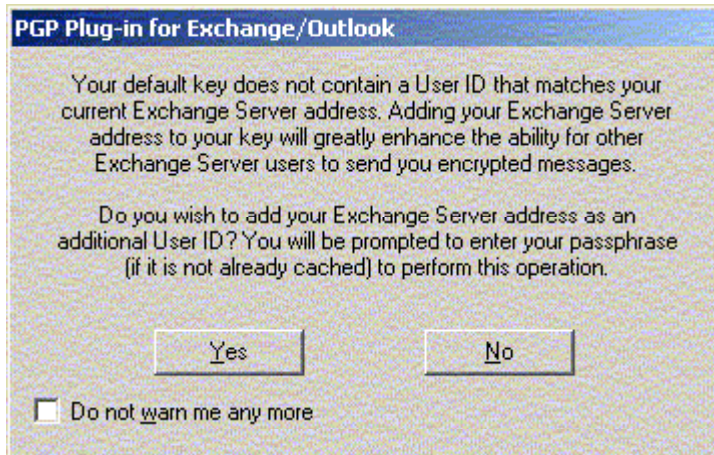
It was also found that policies governing the use of corporate keys are inadequate or not well documented. The “understood” policies need to be documented and approved by management, and any that affect users should be published in the user information intranet page that was brought to light in the audit. Fortunately the residual risk in this instance is not significant. It did seem the Administrator and Information Security in general are doing the right things; it is just that what they are doing is not formalized in documentation.

3.3 Evaluating the Audit

PGP options and related policies are certainly auditable. However, without detailed knowledge of certain options, one may incorrectly assume one choice is better than another by the sound of it. Many PGP options are readily checked through simple observation of the settings in a user’s software. Others must be tested by performing some operations to elicit responses from the software.

Unfortunately, there are some quirks about PGP that keep certain things from being strictly enforced. For example, the inbound ADK cannot be enforced, and the Exchange Server ID cannot be kept off keys (even though it can be set not to be automatically added when generating keys, PGP still gives the user the option of adding it later—see Figure 3-11). Also, PGP does not seem to be amenable to installing a newly configured client when another used to exist, i.e. some options cannot be “unset” by installing the software again without having the super-user find all PGP-related files and settings and eradicate them.

Figure 3-11, a PGP dialog giving the user the option of adding an Exchange ID.



4 Audit Report

4.1 Executive Summary

Overall the audit of PGP options and associated policies went well, with a final grade of B. Areas of strength include good choices for security-related settings and keeping them locked down so users cannot degrade security by changing them. Areas of weakness include insufficient protection of users' private keys, which is crucial to the overall effectiveness of the PGP infrastructure, and incomplete documentation of understood policies and procedures regarding administrative functions.

4.2 Audit Findings

1. **User private keys are not securely stored (Item #18).** PGP by default creates a new user's keyrings in a folder called "PGP" under the user's profile directory, which is not readable by other normal users on the local system. However it was found to be the case that all desktops by default are configured to share the entire C: drive without authentication (see Figure 4-1), and users are able to mount the drives of other users remotely and view any and all files (see Figure 4-2). The *only* thing protecting private keys given this situation is the passphrase chosen by the user, and unfortunately a nefarious insider could harvest private keys and brute-force the passphrases day and night until found.

Figure 4-1, showing the share properties of a user's C: drive.

© SANS Institute 2000 - 2005

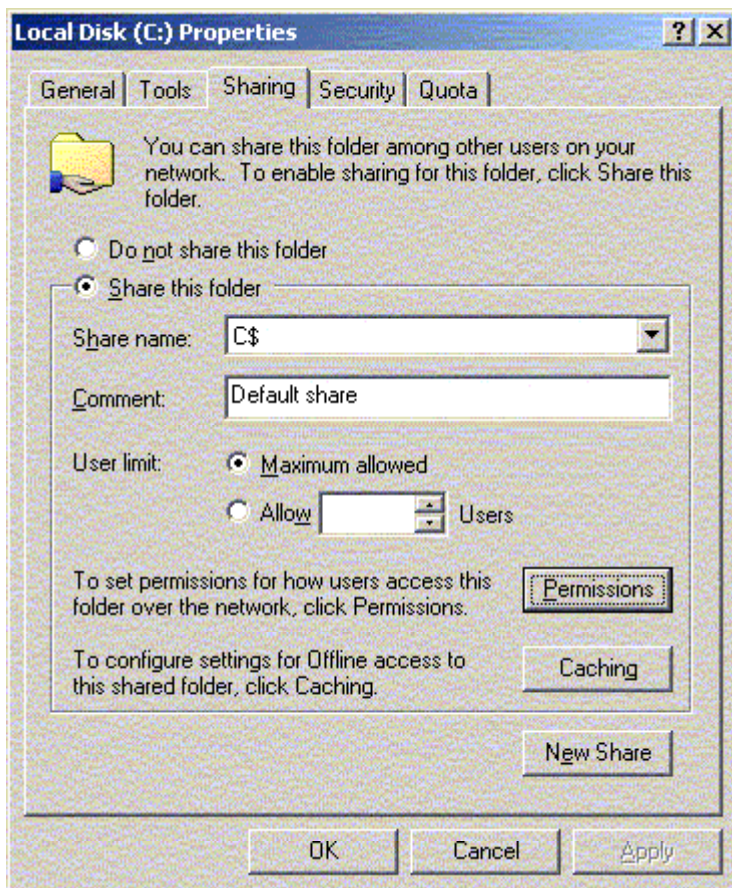
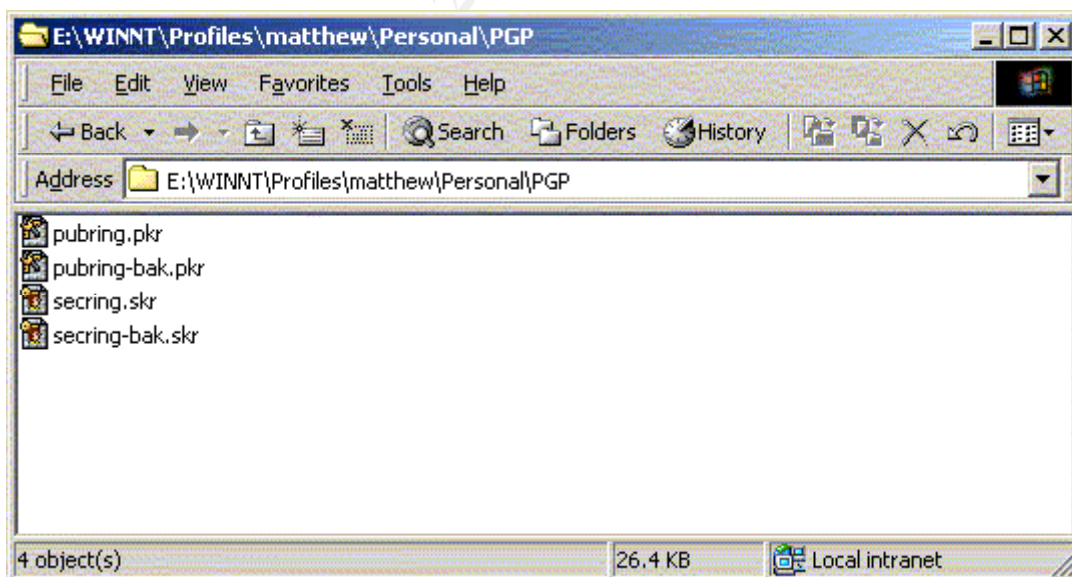


Figure 4-2, a listing of PGP keyrings on a user's system, mounted remotely.



2. **No documented policy exists for handling data recovery using ADKs (Item #19).** The only documentation that exists regarding the data

recovery process is a few bullets explaining trouble-shooting forgotten passphrases in a user information page on the corporate intranet (see Figure 4-3). While a procedure does seem to be understood by the Administrator, it is very important to have such formally documented since it concerns Additional Decryption Keys which are used in all encryption operations in the company. Everything encrypted by all users in the enterprise is encrypted with at least one ADK, so these keys should be well protected, as if they were the skeleton keys to every door in the office building.

Figure 4-3, showing the vague and incomplete ADK policy.

 [BACK TO TOP](#)

Trouble Shooting

User has forgotten passphrase.

- Ensure user doesn't have caps lock on.
- Warn user that anything he has encrypted with that key and passphrase will be lost if he can't remember his passphrase. (A business emergency request by an FVP or above is required to implement the ADK procedure for lost passphrases)
- If user insists he can't remember his passphrase refer to Information Security (k[REDACTED]) to get his keys revoked.

© SANS Institute 2000 - 2005