# Global Information Assurance Certification Paper

Ewa Zurawska
GSEC Practical v1.4b
June 4, 2003

# Corporate PGP: A review of security controls

## 1. Abstract

Protecting a company's sensitive data these days is of paramount importance. PGP is popular cryptographic software that provides encryption to data in transfer and in storage. Acquiring PGP software and distributing it among corporate users is not sufficient. The default software configuration does not meet the security demands of corporate, multi-user implementation and must be restricted prior to distribution. In order to serve its purpose, the PGP tool must be used wisely. Distributing PGP without proper user training may create a false sense of security throughout the company, leading to data exposure.

This paper reviews various security measures that should be applied by the PGP administrator and users of corporate PGP in order to provide safe data encryption. A short introduction to cryptography is followed by characteristics of PGP encryption. Then, the components and features specific to multi-user PGP implementation (Keyserver, Admin tool, corporate keys) are introduced. This provides the foundation for a review of PGP configuration, that consists of two major sections: Keyserver configuration and PGP Desktop configuration (the latter via Admin tool). Last but not least, instructions and recommendations for PGP users are discussed.

## 2. Introduction to Cryptography

We may have security measures and tools to prevent intruders from getting into our network. However, that is no longer enough - sensitive data should be encrypted. Encryption is encoding, or scrambling data so that no undesired individual can read it even if they do find it.

Encryption involves three components: data to be encrypted (plaintext), the mathematical function that performs encryption/decryption (cipher) and a large number (key) that the function uses. If the same key is used for both encryption and decryption, we have conventional or symmetric cryptography. While symmetric cryptography is very fast, both the sender and the recipient must share the same key. Key distribution is a major challenge of symmetric cryptography. Asymmetric cryptography uses two different keys for encryption and decryption. The keys are computationally correlated; thus, they are called a keypair. The text encrypted with a public key can only be decrypted by corresponding private key. It is not feasible to deduce the private key from the corresponding public key. Asymmetric cryptography is slower than symmetric cryptography, but it solves the problem of key distribution (public keys are available to everyone).

Along with asymmetric cryptography comes the concept of digital signature. Digital signature certifies the integrity and authenticity of a message and provides non-repudiation mechanism. A digitally signed document is encrypted with the private key of the owner. To reduce the size of the signature, the document is first passed through a one-way hash function that produces short fixed-length output called message digest (160-bit or 128-bit). Then, the message digest is encrypted with the private key of the signer. To verify the signature, the recipient decrypts the digest with the signer's public key, re-computes it and compares both results.

## 3. Introduction to PGP

PGP encryption software applies both symmetric and asymmetric cryptography, taking advantage of both cryptosystems. In PGP, the message is encrypted with a symmetric, randomly generated key, called the session key that is used only once. Then, this session key is encrypted with the public key of the recipient. Both the message (encrypted with the symmetric key) and the symmetric key (encrypted with the asymmetric key) are sent to the recipient. Decryption works in the reverse way. Symmetric keys are smaller, faster and stronger than the public keys. To provide similar encryption strength, the asymmetric key must be significantly bigger than the symmetric key. Since the vast majority of PGP encryption is done using small symmetric keys, the process is fast. Application of public key encryption allows convenient and secure distribution of the symmetric key.

PGP compresses data prior to encryption. Compression speeds up data transmission, saves disk space and hides the pattern of the encrypted data, reducing exposure to the data pattern-based cryptanalysis.

The strength of encryption depends strictly on the power of the algorithm used. PGP supports two asymmetric key algorithms, Diffie-Hellman/DSS and RSA (also Legacy RSA), and five symmetric key algorithms, AES, CAST, Twofish, Triple-DES and IDEA.

Asymmetric Algorithms

RSA and Diffie-Hellman/DSS algorithms have similar encryption strength. Currently, both algorithms support digital signature (initially, Diffie-Hellman did not). Originally, RSA was the PGP standard. However, Diffie-Hellman/DSS offered better support for symmetric and hashing algorithms (for instance, the RSA PGP certificates used to support only one type of symmetric key – IDEA, and only MD5 hashing algorithm). Now the Diffie-Hellman/DSS is the standard for PGP. New RSA supports all PGP features, however it is fully compatible only with PGP versions 7.0 and above.

Both RSA and DH/DSS support the 1024, 1536, 2048 and 3072-bit keys, and the custom size key. The size of the DSS key is constant - 1024 bits. RSA Legacy can be 1024-bit, 1536-bit, 2048-bit or custom size.

Hashing Algorithms

PGP 8.0 (the newest version of PGP) supports three hashing algorithms: SHA-1 (160-bit), MD5 (128-bit) and RIPEMD-160. The SHA-1 algorithm is considered to be an extremely well designed hash function. 128-bit MD5 is regarded as not being secure enough. PGP includes it for compatibility with RSA signatures. RIPEMD-160 is intended to replace 128-bit hash functions.

"While MD5 is not considered broken, it is possible that two different, but closely related messages could hash to the same value. While this may not seem a big deal, changing a "1" to a "9", a change of only 1 bit, might give the same hash value if circumstances are right." (Yaw)

Symmetric Algorithms

AES, the default PGP algorithm, uses variable key length (128, 192, 256) and variable block length (128, 192, 256). It is smallest and fastest of the symmetric algorithms and is very easy to implement.

CAST is a 128-bit key that operates on a 64-bit block. It is very fast, free and well studied. It has a reputation as a very strong key that successfully resists cryptanalysis. It contains no weak or semi-weak keys.

Twofish uses a 128, 192 or 256-bit key with a 128-bit block size. It has good reviews but is relatively new.

Triple DES, an extension of DES is a 168-bit key (effective strength of 112-bit key). It operates on 64-bit blocks and is considered to be very strong and well documented. Therefore, it might be safer than the newer keys such as CAST or IDEA. However, it is slower.

IDEA, originally the default algorithm in PGP, is a 128-bit key that operates on 64-bit blocks. It is resistant to cryptanalysis. Although it has a large class of weak keys, the chance of getting a weak key is very small. Currently, IDEA is patented and requires a license for commercial use.

PGP encryption works with various data formats: single files, PGPdisks, and electronic mails. PGPdisk designates a portion of the computer hard drive to store multiple files (even entire applications) in encrypted format. End-to-end e-mail encryption protects email messages when they are in storage (on client or server machine) or as they travel over the network. All three forms - file, disk and email encryption - can use a single encryption key. Other useful security features of PGP are wiping (used with files and freespace to remove traces of deleted files from the computer) and secure viewer (prevents Tempest attack). All these components are combined into one software package called PGP Desktop.

## 4. Corporate PGP

PGP can be used by individual or by corporate users. Corporate PGP implements a pre-configured and pre-built user Desktop image. Various parameters are set and locked in the image prior to distributing it to the users. Changes are made via PGP Admin tool. PGP administrator selects settings for the corporate Desktop based on business-specific security policies. Some options are locked to prevent users from making changes.

Typically, public keys of all corporate users are stored in a central key repository called Keyserver. The primary function of Keyserver is distribution of public keys. Besides key distribution, Keyserver is also used for PGP policy management and policy enforcement in the organization. Key restrictions and enhancements set on the server apply to all corporate users. Keyserver also stores configuration of the corporate Desktop created via PGP Admin tool. Any update to the configuration may be automatically sent to all corporate users without having to re-install the Desktop.

Some PGP features implemented via Admin and Keyserver software are specific to the corporate, multi-user setting only, in which mechanisms are needed for secure key exchange between users, data and key recovery, revocation of keys etc. Many of these mechanisms are based on corporate keys. The corporate keys perform special security functions in corporate PGP. Initially generated as regular keys, they are promoted via configuration settings to the status of Corporate Signing Key (CSK), Additional Decryption Key (ADK) or Revocation Key. All three keys are very useful. Thus, PGP administrator should consider implementing them all.

Corporate Signing Key (CSK)

The most important corporate key is the Signing Key. This key is used to confirm the validity of other keys in the organization and to identify the organization to the outside world. Before encrypting sensitive data to the public keys of other users, it should be verified that the keys are valid. Corporate keys are trusted because an authorized person validates them before signing them with the CSK. The CSK signature attached to a key proves that the key has not been tampered with and that it belongs to the purported owner. Key tampering is the biggest challenge of public key cryptosystems.

Additional Decryption Key (ADK)

Information encrypted with a specific public key can only be decrypted with the corresponding private key. However, the required private key may be lost or the owner of the key may not be available. ADK is an emergency decrypting key. Without ADK, data that cannot be decrypted by the owner is lost, since no one else can decrypt it. When ADK is implemented, any information encrypted to the corporate user's key is automatically encrypted to ADK.

ADK allows information recovery, but not key recovery. No one besides the key owner should have access to the private key. If other users have access to the private key, the key owner can deny signing information with the key.

Revocation Key

Compromised keys should be revoked. Revocation prevents other users from encrypting to the revoked key, but all information encrypted to the key prior to revoking can still be decrypted. By default, only the key owner can revoke the key. In order to do so, he must know the key passphrase and/or key reconstruction data. If the key owner cannot revoke the key (e.g. he has lost the passphrase and key reconstruction data, or he is not available), the key will look valid to other users and they will continue to encrypt to it. If the key is compromised, encrypting to it creates security exposure. Revocation key is the key designated to revoke keys of others on behalf of their owners.

Security of corporate keys is critical. If corporate keys are not secure, having them can cause more harm than good. Corporate keys must be protected both physically and electronically. If any of the keys are ever compromised, the integrity of the corporate PGP is lost. Compromised corporate keys can easily be used to tamper other keys within the organisation or to get unauthorised access to sensitive data. The following are basic security guidelines for handling of the corporate keys:

- The keys should be generated and used in the presence of at least two custodians. No single person should have full control over the corporate keys.
- In order to implement shared custody over the keys, they should be split into shares. (PGP supports Blakely-Shamir splitting technique). Splitting minimises the risk of key misuse. The minimum number of shares necessary to use the key must be set.
- Shares of the corporate keys and their backup copies should be locked in a safe. Contingency copies should be stored offsite.
- Access to the keys and their shares should be restricted and logged.
- If shares are collected over the network using TLS, the shareholders' fingerprints must be verified.
- All operations that use the corporate keys should be executed on a physically secure system.
- The size of the corporate keys should be set at minimum 2048 bits.
- The key passphrase should be exceptionally strong. It is advised that non-printable ASCII characters be included, since these cannot be cracked by dictionary attack.
- Using key reconstruction data is not recommended.

The administrator may consider generating the corporate keys on smart cards. However, keys stored on smart cards cannot be split, because the private key is non-exportable from the smart card.

## 5. Configuring the Keyserver

Corporate PGP is based on three interdependent software components: Keyserver, Admin Tool and client Desktop. Configuration of these components determines the quality of the corporate PGP service. Secure PGP is a desirable data protection tool. Poorly implemented PGP creates a false sense of security, which may lead to unexpected data exposures.

Keyserver is the central point of the corporate PGP. It has a range of configurable parameters that control the behavior of the entire PGP. Configuration of Keyserver is set via Keyserver Configuration Wizard (few initial settings) and the Web Console. The wizard creates a server administrative account (which is later use to log in to Web Console) and sets the protocol for the Web Console connection. Using the http protocol (port 80) is unsafe. The connection should be established over https (port 443). The http should be allowed only if it is necessary for backward compatibility. Otherwise, it should be disabled. An important step of wizard configuration is generation of Keyserver secure key. The key and the X.509 certificate are used to establish secure communication between web clients and the server. The key is stored in the server local keyring along with other important keys (e.g. CSK).

Typically, all other parameters are set via Web Console. Direct editing of server configuration files (pgpcertd.conf, httpd.conf) should be avoided. However, some settings are not available on the Console and can be set only directly in the files. For instance, to restrict the Web Console access to a specific IP/host (the default access in unrestricted), the httpd.conf file must be edited manually. However, this is only an exception.

Set Secure Mode (LDAPS)

By default, Keyserver listens for client requests on LDAP (port 389). However, the server also supports Secure Mode, which is based on TLS protocol. TLS listens on LDAPS (default port 636). Using the Keyserver secure key, which is generated during initial server configuration, Secure Mode provides encrypted and authenticated communication. Secure Mode is recommended for some administrative tasks such as key deletion. In Secure Mode, Keyserver will not start without successful authentication. Secure Mode parameter can be set to one of the following: disabled, optional or required. It is recommended to select the required mode.

Restrict access to specific IP, host, key, user ID/password

One of the server settings (**Default Access**) defines the level of permissions granted to all users by default (none, read, add, delete, admin). The default level of users' permissions should be restricted. However, certain users may require special permissions other than default. These permissions may be granted to a specific IP, host or key using the **Allow Access By** parameter (options: **Allow IP, Allow Host, Allow KeyID**). Some operations on the server (delete or admin)

require two authentications – by IP/host and by key ID. High-level administrative operations, such as uploading Desktop preferences to the server, additionally require an administrator ID/password.

Redirect keys to the pending area for verification

Typically, PGP keys generated by corporate users are automatically sent to the Keyserver. By default, the server accepts all keys without screening them. PGP users trust that the public keys available on Keyserver are valid. Maintenance of this trust is vital for the functioning of corporate PGP. To prevent the broadcast of invalid keys (tampered, accidentally generated, etc.), all keys must be verified before being posted. In order to temporarily hold keys for verification, the PGP administrator sets the **Required Signature** policy. When this policy is enforced, keys that are missing the signature of CSK cannot be posted on the server. (Since the submitted keys are initially not signed by CSK, all of them fail the policy.) The PGP administrator may redirect the failing keys to the pending area by setting **Action on Key Policy Failure** parameter. Then, the keys in the pending area are verified. Valid keys are signed with the CSK and resubmitted to the server. Invalid keys are deleted.

Keys are verified by checking their fingerprints (hash calculated on the key, its signature(s), and some user data). The fingerprint is displayed as a unique hexadecimal number or series of words. To verify the fingerprint, the administrator must contact the owner of the key (usually by telephone) and confirm that the fingerprint of the submitted key and the one provided by the key owner match.

Besides the fingerprint, the PGP administrator should verify other attributes of the submitted key before posting it to the Keyserver. For instance, a key may be generated with a bogus timestamp. The key generation date and time are based on the computer clock. A dishonest user may change the clock to generate a key with a wrong date trying to defeat non-repudiation. Keys with erroneous data should be rejected.

The PGP administrator may turn on the setting **Remove Unallowed Signatures**. When this setting is on, only the signatures specified as **Required Signatures** or **Allowed Signatures** will be accepted on the server.

Accept key reconstruction data

"One of the most common problems with a large-scale PGP deployment is that users sometimes forget their passphrases or even lose their private keys. This leads to help desk calls, which can be costly for organization." (Price, p.2)

The owner of the lost key faces two major challenges – notifying other users about the loss (otherwise, they will continue encrypting data with the lost key) and decrypting the data already encrypted with the key. The corporate Revocation Key and the Additional Decryption Key, when implemented, solve both problems. However, the lost key itself is irrecoverable and must be replaced with a new key. Although it is possible, re-encryption of the data can be a very tedious and

frustrating task. To solve the problem of lost keys, some PGP implementations store copies of all users' keypairs on a backup system. This approach violates non-repudiation, thus should not be used.

An alternative solution, the key reconstruction feature, seems like a better option, although it also carries some risks. When the key reconstruction is enabled, users may recover their lost keys and passphrases themselves without intervention of the administrator. The only ting they need is to have access to their public keys (these are publicly available to everyone on Keyserver) and know at least three of five answers to the personal questions created during key generation. These five questions and answers are called key reconstruction data. Key reconstruction uses Blakely-Shamir key splitting technology. The five answers work similarly to the shares of a split key. Key reconstruction data is stored on the Keyserver, under ID of the key. To enable key reconstruction, the PGP administrator must turn on **Accept Key Reconstruction Data** setting.

The main problem with the key reconstruction data is that guessing three of five answers gives the attacker full control over the key. For comparison, guessing a passphrase without having access to the private key creates exposure but does not allow the attacker to act as the key owner. When the key reconstruction data is stored on Keyserver, users of corporate PGP can see the personal questions of all other users. If the questions are weak, they can help an attacker gain access to the key. If the key reconstruction data is stored in the LDAP directory instead, it is protected with the user ID and password. This means that users are able to see only their own data. However, upon successful authentication, both questions and answers are sent to the user in one data block. Successful attack on the LDAP password gives the attacker access to the entire data block. To avoid the risks of both alternatives, extremely secure PGP implementations do not use key reconstruction at all.

Send key reconstruction data over LDAPS

If the reconstruction data is implemented, all communication with the key reconstruction server must use LDAPS.

Configure Keyserver log

Keyserver registers in a log file all operations requested on the server, such as type of request, the session ID that links all operations performed in one connection, time, duration, client IP, etc. The **AccessLog File** parameter specifies the name and location of the log. The setting of the **AccessLog Details** parameter defines the level of registered information (none, bind, unbind, abandon, add, modify, search, delete, ldap, or all). By default, the access log is not archived and may grow unlimited. To prevent very large logs, the PGP administrator may schedule daily or weekly archiving of the access log by specifying cycling parameters (day, time, number of archives to keep).

Configure system log

Every operating system has its own logging mechanism. For instance, Unix records information in the syslog file, and Windows use the Event Viewer. The level of information registered in the system log can be set via the **LogLevel** parameter to one of the following: error, warning, info, or verbose. The Keyserver error log lists only the events from the last server start/restart. The system log also lists the events preceding the last start.

When setting the parameters for both logs, the PGP administrator must remember that the amount of collected data is very important for tracking security incidents.

Other general security principles must be applied when setting the Keyserver:

- The Keyserver must be installed on the dedicated, hardened system.
- It must be set behind a firewall in a room with restricted access.
- Only the necessary firewall ports should be open (LDAP, LDAPS, HTTPS, SSH).
- Regular backups of the entire system should be maintained.
- Logs should be monitored.

## 6. Configuring the Desktop (Admin tool)

The PGP Admin tool is used to configure the PGP client installer. Restrictions set in the client installer affect all PGP users. The Admin tool sets two types of options:

1) PGP options – user's personal settings, such as: passphrase caching, location of local keyrings, URL of Keyserver, encryption algorithms, PGPdisk options, wipe options, smart cards options
2) Administrative options – corporate settings, such as: corporate keys, passphrase restrictions, URL of reconstruction server, automatic updates

PGP users have no access to the administrative options (the second group) – these can be set only via the Admin tool. On the other hand, PGP options (the first group) are not restricted by default. PGP users can see the options and, if they wish to, can change their values. However, the administrator can use the Admin tool to lock all or selected PGP options and prevent users from modifying them. Locked options are greyed out in the user's Desktop. The following four PGP options are more critical than others – PGP administrator should consider locking them:

Do not cache passphrase

PGP Desktop includes four passphrase caching options. Users can cache passphrase in computer memory for a specific time or until logoff, share the passphrase cache among modules or not cache the passphrase at all. Since it is convenient to enter the passphrase only once for all PGP operations, users may

decide to cache their passphrases. From the security perspective, passphrase caching creates exposure and, as such, should be disabled.

Enable automatic keyring backup
If this option is enabled, PGP creates automatic backup of the local keyring when the PGPkeys window is being closed. This option prevents users' keys from being accidentally lost. Therefore, it is safe to turn the option on and lock it to disable re-setting.

Do not allow forcible and auto-unmount
When a PGPdisk containing open files is forcibly or auto-unmounted data on the disk may be lost. PGPdisk configuration allows unmounting of the disk without warning. To prevent users from accidental data loss, it is safe to disable all options related to forcible and auto-unmounting. When these options are disabled, the PGPdisk containing open files cannot be automatically unmounted.

Select Corporate Keyserver
Since all key operation in the corporate PGP should point to the corporate Keyserver, it is recommended to remove other public servers from the list and lock the option to disable re-setting.

The second group of options, the administrative options, includes many critical settings. Some of the selections in this group will depend on the Keyserver configuration. PGP administrator should consider setting the following options:

Set Corporate Signing Key
CSK proves the validity of all keys deployed in the corporate PGP – it is beneficial and highly recommended to have it implemented. CSK is selected from the Corporate Key panel of the Admin tool. Selecting the **Automatically sign corporate key** option makes all new keys automatically sign the CSK.

Set and enforce ADK(s)
The ADK(s) is important emergency decryption tool in the corporate PGP. PGP supports three types of ADK: incoming, outgoing and PGPdisk. The incoming ADK is permanently attached to public keys of all corporate users. Data encrypted to public keys of corporate users is automatically encrypted to the incoming ADK, (regardless of where the data is coming from - from within or outside of the organization). The outgoing ADK is used with messages sent outside of the organization. PGPdisk ADK is added to all new disks created by PGP users.

ADK can be enabled (added to the recipient list by default) and enforced (user cannot remove it from the list). It is recommended that the incoming ADK be enforced. ADK(s) are enabled and enforced from the ADK panel of the Admin tool.

Set corporate Revocation key

Compromised keys must be revoked. Otherwise, other corporate users will continue to encrypt to them. The corporate revocation key is an emergency tool used in situations when users cannot revoke their own compromised or lost keys themselves. Having the key in the corporate PGP is critical. The Revocation key is selected from the Revocation panel of the Admin tool.

In order to incorporate the CSK, ADK and Revocation keys in the default keyring of each PGP user, the keys must be selected in the Keys panel of the Admin tool.

Select key generation settings

The details related to key generations are set from the Key Generation panel of the Admin tool.

The PGP administrator may generate keys for all corporate users. This approach violates non-repudiation, and thus, should be avoided. It is recommended that users be allowed generate their own keys.

RSA and Diffie-Hellman/DSS have similar encryption strength and both support digital signature. However, some other factors may have to be considered when deciding between both keys. For instance, some VPN gateways with X.509 certificate support only the RSA-based certificates. Smart cards do not support the Diffie-Hellman/DSS keys. On the other hand, RSA is not fully compatible with any PGP version lower than 7.0. For communication with users running older versions of PGP it may be necessary to use RSA Legacy.

Deriving the private key from the correspondent public key is extremely difficult, but possible. Larger keys are harder to crack, but operations performed with larger keys require more time. The lowest acceptable key size in recent PGP is 1024-bit key. The recommended minimum key size is 2048-bit (default).

If key reconstruction is implemented, the URL of the reconstruction server must be provided. It is critical to communicate with the key reconstruction server using LDAPS.

New keys can be automatically sent to the Keyserver if the option **Always send new keys to server** is enabled. This setting is very useful in corporate PGP.

Keys can be generated on smart cards. Keys generated on smart cards are not exportable – the private portion of the key never leaves the smart card. All operations that use the private key, such as decryption and signing, take place directly on smart card. Thus keys generated on the smart cards are more secure. However, they cannot be backed up, so the smart card is lost the key is lost too. The option can only be used if the corporate environment supports smart cards (users have the devices and the smart card software installed).

Set restrictions on key passphrase

Passphrase is considered to be the weakest point of PGP. Forcing users to use long and high-quality passphrases prevents passphrase cracking. By default, there are no restrictions on passphrase length. If a passphrase is shorter than 8 characters, the user receives a warning, but the passphrase is still accepted (even if it is as short as 1 character). The PGP administrator should use the Admin tool's Passphrase panel to set minimum length for passphrases. The quality of a passphrase depends on the variety of characters used (different case letters, numbers, punctuation, spaces). PGP supports extended, non-printable ASCII characters - these cannot be cracked by dictionary attacks, and thus significantly improve the quality of passphrase.

Schedule automatic updates of configuration

Over time, the PGP administrator may need to change some settings of the client Desktops. The PGP Admin tool supports automatic Desktop updates. The frequency of updates is set in the Updates panel of the Admin Tool. The automatic update is very convenient, as the changes are downloaded to all corporate users transparently without generating a new installer. LDAPS is the recommended update protocol; it provides data encryption and authentication.

Allow conventional encryption and SDA

The conventional encryption and the Self-Decrypting Archives use passphrases instead of PGP keys. This type of encryption is less secure, but may be useful for exchanging encrypted information with someone who has no PGP.

Allow encryption to invalid keys

Encryption to invalid keys is allowed by default. PGP implementations with higher security standards should disallow it.

## 7. Users training (do's and don'ts)

The PGP administrator might put a lot of effort to secure corporate PGP, but, if users do not follow good security practices, the effort is wasted. Users need to be instructed how to use the software. Software-specific security policies will help users to understand PGP risks and enforce good habits. The following are some guidelines for PGP users:

Protect your passphrase and key reconstruction data

Having access to the private key and its passphrase gives the attacker full control over the key and allows for acting on behalf of the key owner. It is critical to protect passphrases from exposures. Forcing minimum length and minimum quality of passphrase helps but does not eliminate all risks. Users should be given the following instructions:

- It is critical to choose a strong passphrase; thus, it should not be chosen on the spur of the moment. It should be something that is easy for the key owner to remember but difficult for others to guess.

- A passphrase should not consist of a single word – single-word passphrases can be discovered by the dictionary attacks. Various non-alphabetic characters should be included in the passphrase.
- A passphrase should not be written down - it should be memorized. If it must be written down, it should be inaccessible to others (e.g. stored in encrypted format).
- A user should always use the **Hide Typing** option when typing the passphrase in the presence of others. It is important to make sure that no one is watching the keystrokes.
- A passphrase should be changed regularly, and always when suspected of having been compromised. If it has been compromised, it should be changed, and the backup keyrings and freespace should be wiped to prevent usage of the old passphrase.

Safety principles similar to those for the passphrase should be applied to key reconstruction data. Access to key reconstruction data gives an attacker full control over the key. A user should make sure that key reconstruction data is extremely strong. The personal questions must not be able to lead the attacker to the answers. Users may consider leaving the questions blank.

Protect access to your private key

By default, the private key and its backup reside on the PC of the key owner. The following protection methods for the private key should be considered:

- The key owner should always have full control over the private key. It is safe to store the key on a write-protected floppy disk. The private portion of the key is not exported by default – thus, the key owner must remember to include it. If the key is stored on a computer, changing the default name and location of the keyring can increase security of the key. It is not safe to store the key on a remote computer because remote access can be eavesdropped on.
- If the key resides on the computer, the computer should never be left unlocked. It is recommended to have a password-protected screen saver. If the key resides on a floppy disk, the floppy disk should always be removed from the computer drive immediately after use and stored in a secure location.
- A key exported for sharing with others should never include the private portion.
- It is important to have a backup copy of the key. However, if the computer that stores the PGP key is on a network, the key owner must ensure that the key files are not automatically included in a system-wide backup. The key backup should be stored in a secure location, not on a system that can be accessed by other users.
- All key changes should be updated on the Keyserver.

Protect public keys from being tampered with

Public key cryptosystems are vulnerable to public key tampering. Validating keys before posting them on the corporate Keyserver ensures that the keys belong to

their real owners. When a PGP key cannot be obtained from Keyserver, it should be obtained directly from its owner or from a trusted third party. To secure one's own local keyring from tampering, it may be signed with the PGP key.

Protect your PGPdisk

- It is important to protect access to the computer containing the PGPdisk, as anyone with access to the computer can delete the file that controls the disk. If the file is deleted, the data is permanently lost.
- A PGPdisk should be unmounted when not in use – only an unmounted disk is encrypted. When a PGPdisk is mounted, anyone with local or remote access to the computer can access the data on the disk. Unmounting makes the disk invisible to others. A user must make sure that the mounted PGPdisk cannot be seen from the network.
- It is better to encrypt PGPdisk volume with a key (versus a passphrase). Passphrase protection is less secure. In addition, key encryption allows a single PGPdisk to be encrypted with multiple keys – the disk is shared without the passphrase being shared.
- It is recommended to have a backup copy of the PGPdisk – if the original disk is lost, the data can be recovered from the backup. However, the PGPdisk should not be backed up when it is mounted, as the backup copy of the disk will be decrypted. Backup of the PGPdisk to remote systems is not recommended.
- PGPdisk can be shared. If a user of the shared disk is removed, the disk should be re-encrypted (this changes the disk encryption key). It is difficult, although possible, to get the old encryption key from the computer's memory and continue accessing the disk. The re-encryption should be applied to all copies of the disk.
- PGP supports nested PGPdisks – nesting increases security of the stored data.

Useful encryption option

Of all the encryption options offered in PGP, two options are particularly useful for securing files:

- Wipe Original – when this option is selected, the original file is overwritten with its encrypted version. PGP users may not be aware that the files being encrypted are not overwritten with their encrypted version by default. By default, the encrypted data is stored in a new file, leaving the original clear text file untouched.
- Secure Viewer – the viewer uses a TEMPEST font that prevents special electronic equipment from remotely reading files based on their radiation. Selecting this option sets restrictions on displaying files upon decrypting. The files cannot be opened or edited with a regular editor - they can be opened only in the Secure Viewer. Also, they cannot be saved in the decrypted format. This option is recommended for extremely confidential documents.

Wipe your files

Deleted files are not completely removed from the hard disk. Usually, only the file name is deleted, but the data stays on the disk until it is overwritten by another application. There are tools that can retrieve the data from deleted files. To prevent this, the data must be made irrecoverable. This can be done by multiply overwriting free space on the disk. This process is called wiping. PGP wipe utility can be applied to any file on the computer. Wiping does not send the file to the Recycle Bin. This option should be used to permanently delete sensitive files from the system. PGP provides the option of automatically wiping the files being deleted.

Wipe your freespace

Computer users may not be aware of the fact that many applications create temporary copies of the files being processed. The files are deleted when the applications close, but the data is left on the disk. Users also rarely know that some operating systems (for instance the NTFS) keep a filesystem journal with copies of everything that is written to a disk. Regular file wiping does not remove these files; they can be removed only with the PGP Free Space Wiper. Computers that store sensitive data should be wiped frequently to ensure that their hard drives do not keep residual data (10 wipe passes are recommended for commercial data). However, this option cannot be used on boot partition.

Protect your email

- Sensitive email and attachments should be saved in the encrypted format so that they remain secure. Attachments can be opened without decrypting the email message.
- When storing sensitive email in the outbox before sending it, a PGP user should ensure that the email application supports outbox encryption. If not, the messages can be encrypted using the Current Window option.
- When dealing with sensitive messages, misleading or blank subject lines can be used.

Keep your computer virus-free

PGP, or the operating system running PGP, may become subject to virus attacks. When this happens, sensitive data can be intercepted, the functionality of the software can be modified to suit the attacker needs, and the original PGP version can be replaced with a Trojan horse version. PGP has no built-in anti-virus protection. The risk of virus infection can be greatly reduced by installation of the anti-virus software. Digital signing of the PGP software ensures integrity of the code. The signature should be verified frequently.

Protect random seed file

PGP session keys are generated using seed file (randomseed.rnd). The seed file contains both random seed and random key materials. Though very difficult, it is possible to derive the next or previous session key from these materials. Thus,

the random seed material should be protected from disclosure. Only the owner of the computer should have access to the seed file (read-only). Other users should have no access at all. If these file restrictions are infeasible, access to the computer should be restricted (e.g. the computer should be locked) to prevent the copying of files.

Restrict virtual memory/swap files

New operating systems that run large applications use virtual memory and swap files. As a result of data swapping, sensitive information (keys, passphrases, decrypted files) may be moved to a swap file on the hard disk without the user's knowledge. Sensitive PGP data never stays in computer memory very long. Thus, although the probability of swapping it to the disk is very low, it does exist. Anyone with physical access to the computer can access the swap file. The administrators of extremely secure systems may consider turning off virtual memory features or installing software that overwrites swap files.

## 8. Conclusion

Having PGP Desktop installed on a computer does not guarantee security of the data on the system. In order to secure the data, the administrator must set configuration restrictions and create usage policies. Users must follow these policies - no encryption program provides protection against bad habits. Even when all participants follow good security principles, a security risk still exists, but is limited. A well-protected system requires great effort to break into and often discourages violation attempts.

## 9. References


Christoyannis, Costas. “An Overview of Cryptography.” 1998.
URL: http://www.securitypointer.com/encryption.htm
(15 May 2003)

[1] McCune, Tom. “Tom McCune’s PGP Questions and Answers”.
URL: http://www.mccune.cc/PGPpage2.htm (15 May 2003)

[2] PGP Corporation. “An Introduction to Cryptography”. Version 8.0.2. May 2003. URL:
http://www.pgp.com/products/whitepapers/pgp_introtocryptography.pdf
(15 May 2003)

[3] PGP Corporation. “PGP Keyserver Enterprise Edition: Administrator’s Guide” Version 7.0. November 2002. URL:
http://pgp2all.spb.ru/data/docs/v8/PGPKeyserverAdminGuide.pdf
(15 May 2003)

[4] PGP Corporation. “PGP 8.0: Administrator’s Guide”. November 2002.
URL: http://pgp2all.spb.ru/data/docs/v8/PGPAdministratorsGuide.pdf
(15 May 2003)

[5] PGP Corporation. PGP 8.0 for Windows: User’s Guide. Version 8.0.2. March 2003.

[6] PGP Corporation. Price, Will. “Inside PGP Key Reconstruction”. May 2003.
URL: http://www.pgp.com/products/whitepapers/PGPKeyRecon.pdf (15 May 2003)

[7] Ross, David E. “Pretty Good Privacy (PGP)”. May 2003.
URL: http://www.vcnet.com/~rossde/PGP/ (15 May 2003)

[8] Heath, Jim. “How electronic encryption works and how it will change your business”. 2002. URL: http://www.viacorp.com/crypto.html (15 May 2003)

[9] Williams, Randall T. “The passphrase FAQ”. Version 1.04. January 13, 1997. URL: http://www.stack.nl/~galactus/remailers/passphrase-faq.html#230
(15 May 2003)

[10] Yaw, David. “PGP: An Algorithmic Overview”. November 6, 2001.
URL: http://www.davidyaw.com/crypto/PGP.pdf (15 May 2003)