

The User-friendly Way to Exchange Secure Data

SafeGuard[®] PrivateCrypto

Help

Version 2.31



Document date: April 2009



Contents

CHAPTER 1	Introduction.....	1
	1.1 Archives	1
	1.2 Keys from the SafeGuard Enterprise key ring	2
	1.3 Logging (Password History).....	2
	1.4 Encrypted E-mail attachments	2
	1.5 Algorithms	3
CHAPTER 2	Installation	4
CHAPTER 3	SafeGuard PrivateCrypto User Application	5
	3.1 SafeGuard PrivateCrypto Options	7
	3.2 Encryption	7
	3.3 Decryption.....	8
	3.4 Password History	9
	3.4.1 SafeGuard PrivateCrypto Password History.....	10
	3.5 Creating new archives	12
	3.6 Save Encrypted.....	13
	3.7 Opening existing archives	14
	3.8 Adding files to an archive.....	15
	3.9 Removing files from an archive.....	15
	3.10 Decrypting files and archives	15
CHAPTER 4	SafeGuard PrivateCrypto Explorer extensions.....	17
	4.1 Encrypting files.....	18
	4.2 Decrypting files	20
	4.3 Creating self-extracting executables	21
CHAPTER 5	Minimum password length.....	23
CHAPTER 6	SafeGuard PrivateCrypto Command Line Interface	24
CHAPTER 7	SafeGuard PrivateCrypto OLE Automation Interface	26

Contents

7.1 Example Script.....	28
Technical Support	32
Copyright	33

1 Introduction

SafeGuard PrivateCrypto offers a user-friendly way for encrypting data. Single and multiple files as well as entire directories can be encrypted. The directory structure is preserved after decryption. Additionally, files can be compressed after encryption.

1.1 Archives

Encryption and compression of multiple files (archives) is also supported and it is possible to add and extract single files from an archive easily.

SafeGuard PrivateCrypto 1.x cannot open archives created with SafeGuard PrivateCrypto 2.x and later versions.

SafeGuard PrivateCrypto 2.x can open archives created with SafeGuard PrivateCrypto 1.x but not modify them.

Integration in Windows Explorer allows encryption of files by right-clicking on them in Windows Explorer and entering a password.

To decrypt a file, you only have to double-click an archive and enter a password or the key used for encryption has to be available to you. If a user, who should be able to decrypt the file, does not have SafeGuard PrivateCrypto installed, self-extracting executables can be created. To decrypt these files, you have to enter the password.

With the SafeGuard PrivateCrypto User Application the user can create and administrate (adding/remove files) archives. Files can be added to archives by just dragging them into the SafeGuard Private Crypto file in the user application. Default values for encryption/decryption (e.g. default folder for encrypted files, etc.) can be set there as well (SafeGuard PrivateCrypto Options dialog).

1.2 Keys from the SafeGuard Enterprise key ring

In addition to encrypting files by entering a password, SafeGuard PrivateCrypto also offers the usage of keys from the SafeGuard Enterprise key ring for encryption. If SafeGuard Enterprise is installed on the computer, all keys from the user's key ring (keys created centrally by SafeGuard Enterprise and keys created locally on the SafeGuard Enterprise client) can be used.

Thus, SafeGuard PrivateCrypto archives can simply be exchanged between SafeGuard Enterprise users. For decrypting the archive, the key used for encryption has to be available on the computer. A prerequisite for this procedure is that SafeGuard PrivateCrypto Version 2.30 or higher is used on both computers.

HINT:

Please note that the same key has to be available on both computers (e.g. a SafeGuard Enterprise group key). If you use a SafeGuard Enterprise key, which is not contained in the recipient's key ring, the recipient cannot decrypt the archive.

If you use locally generated SafeGuard Enterprise keys, you have to communicate the passphrase to the recipient. The recipient will be automatically prompted to enter the passphrase when opening the archive.

1.3 Logging (Password History)

It is possible to generate a log file where password, file name, date of encryption and optionally a comment is saved. This log file is encrypted using an additional password or a SafeGuard Enterprise key. As the password has to be entered additionally for each encryption procedure, it can be saved in the registry to make the process more user friendly. However, please note that this represents a security risk, since there is no possibility to save the password in a secure way!

When using a SafeGuard Enterprise key for encryption, the passwords are saved without any user interaction, if the key used is included in the user's key ring.

1.4 Encrypted E-mail attachments

Using SafeGuard PrivateCrypto you can encrypt and send files via E-mail in a single procedure ([see "Encrypt & Send", page 17](#)). After encryption and optional compression the E-mail client is launched and the file is attached automatically.

1.5 Algorithms

SafeGuard PrivateCrypto uses the "Rijndael" algorithm that is defined as the new Advanced Encryption Algorithm (AES). The Utimaco implementation uses the "Rijndael" algorithm with a key length of 256 bit to encrypt data. For compression the BZIP2 library is used. The keys for encryption operations are derived from entered passwords using the PKCS#5 password based cryptography standard.

SafeGuard PrivateCrypto is available for Windows 2000, Windows XP and Windows Vista. SafeGuard PrivateCrypto is available as freeware and can be downloaded from the SafeGuard PrivateCrypto home page (www.utimaco.com/PrivateCrypto.com) for personal use.

2 Installation

To install SafeGuard PrivateCrypto for PC, start the setup program by double-clicking on `sgpc231.exe` or `sgpc231.msi` (resp. `sgpc231_u.exe` or `sgpc231_u.msi` for the unlicensed version). An installation wizard will guide you through the rest of the installation procedure.

3 SafeGuard PrivateCrypto User Application

To start SafeGuard PrivateCrypto, click **Start > Programs > SafeGuard PrivateCrypto** (resp. the folder you have selected during installation) > **SafeGuard PrivateCrypto**.



Besides the SafeGuard PrivateCrypto Explorer extensions SafeGuard Private Crypto offers the possibility to create and administrate archives using the Safeguard Private Crypto User Application.

There, files can be added and removed from archives and single files can be extracted from an existing archive.

Files (and directories!) can be dragged from Windows Explorer to the PrivateCrypto file list. These files are then added to the current file list.

The file list of the SafeGuard PrivateCrypto User Application shows all changes made to the encryption archive currently selected:



The file is already part of the archive and will remain unmodified.



The file will be added to the encryption archive.



The file will be removed from the encryption archive.

Please note that changes to encryption archives are only done when saving the file.

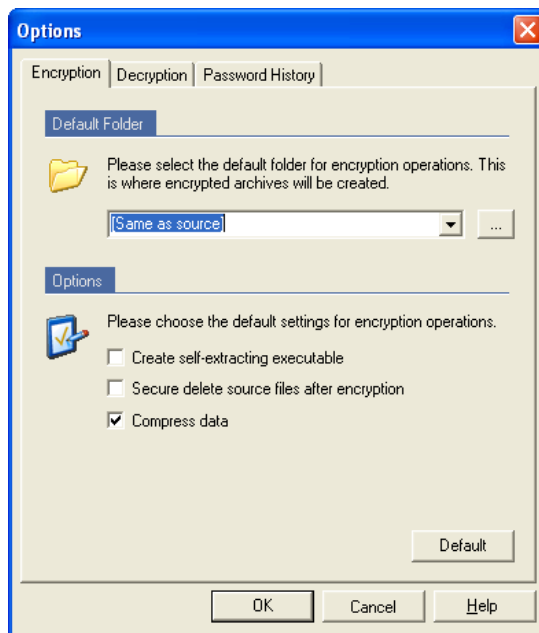
Using the **Decrypt** button or menu command (**File > Decrypt**) one or more files of the encryption archive can be selected in the list and extracted (decrypted) from the archive. The encrypted versions of the files remain within the encryption archive. If no file is selected, the **Decrypt** command extracts all files of the archive by default.

In case entire directories are to be encrypted, the corresponding path is displayed under *Path* in the list view of the SafeGuard PrivateCrypto User Application.

3.1 SafeGuard PrivateCrypto Options

In the SafeGuard PrivateCrypto *Options* dialog (**Tools > Options**) default values for encryption/decryption and password logging operations can be defined. They apply to both, the SafeGuard PrivateCrypto User Application and Windows Explorer Extensions. If required, these can be changed in the *SafeGuard PrivateCrypto - Save Encrypted* and *SafeGuard PrivateCrypto - Decrypt* (click **Options**) dialogs. The default settings can only be changed within the **Options** dialog. The **Options** dialog consists of three tabs:

3.2 Encryption



Default settings after installation:

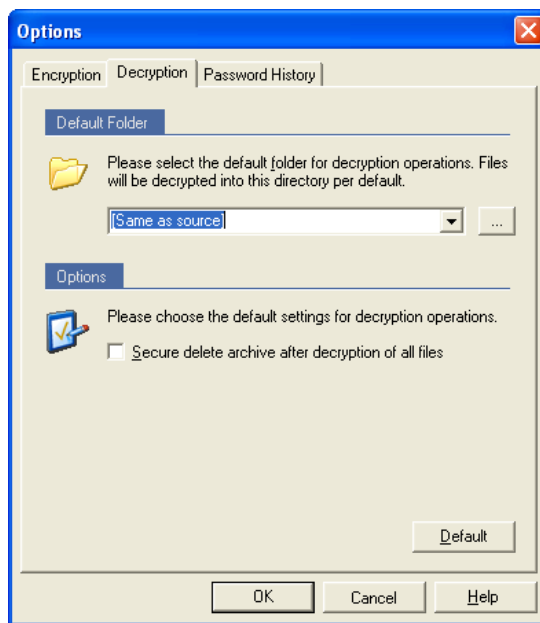
- **Default Folder:** empty [same as source]
- **Create self-extracting executable:** deactivated
- **Secure delete source file after encryption:** deactivated
- **Compress data:** activated

If these settings have been changed, they can be restored by clicking the **Default** button.

The settings defined here are valid for all encryption operations, performed either in the SafeGuard PrivateCrypto User Application or using the Explorer Extensions. They can be overwritten temporarily for a **single encryption operation (Options** in the *Save Encrypted* dialog).

Click **OK** to save the settings and close the *Options* dialog.

3.3 Decryption



Default settings after installation:

- **Default Folder:** empty [same as source]
- **Secure delete archive after decryption of all files:** deactivated

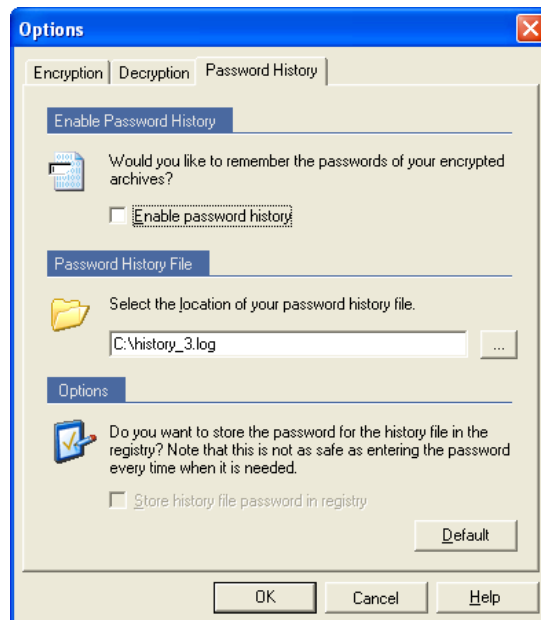
If these settings have been changed, they can be restored by clicking the **Default** button.

The settings defined here are valid for all decryption operations, done either in the SafeGuard PrivateCrypto User Application or using the Explorer Extensions. They can be overwritten temporarily for a **single decryption operation** in the *Decrypt* dialog.

- **Default Folder:**
Files will be decrypted into this directory by default. In the drop-down list, the same directory as the source file and the My Documents folder can be selected. Another directory can be selected clicking the [...] button.
- **Secure delete archive after decryption:**
If activated, the encrypted archive will be wiped (and thus can not be restored) after decryption of all files.

Click **OK** to save the settings and close the *Options* dialog.

3.4 Password History



It is possible to generate a log file in which password, file name, date of encryption and optionally a comment can be saved. This password history is secured with an additional password or a SafeGuard Enterprise key. This password can be saved in the registry as it has to be entered for each encryption process. However, please note that this represents a **security risk** as the password cannot be saved in a secure way.

Viewing the password log file is only possible using the **View Password History** command from the *Tools* menu.

Default settings after installation:

- **Enable password history:** deactivated
- **Password History File:** none
- **Store history file password in registry:** deactivated

If these settings have been changed, they can be restored by clicking the **Default** button.

To store path and name, password, date of creation and comments for an archive in a separate file, the **Enable password history** option has to be checked. The name and the path of the history file can be specified in a second step.

For convenience reasons the password for the history file (it has to be entered anytime an archive is created and the password is to be logged in the password history) can be stored in the Windows registry. **Please note that this represents a security risk!**

Click **OK**, to save the settings and close the **Options** dialog.

3.4.1 SafeGuard PrivateCrypto Password History

Users have the possibility to log their passwords in a separate file. If the user decides to log the passwords in a file (which as such represents a security risk), there are the following possibilities for securing this file:

HINT:

Settings for logging a password history do not have any effect when using SafeGuard Enterprise keys. Thus, the user will not be prompted to enter a password, if SafeGuard Enterprise keys are used for encrypting archives.

- A secure method is to enter a password (used for encryption) for the log file for each required logging procedure. It is more secure but not user friendly because always two passwords have to be entered; one for the archive and one for the log file.
- Alternatively, you can use a SafeGuard Enterprise key for securing the password history. The file will be encrypted without any user interaction, if the key can be accessed in the user's personal key ring.
- The password for the log file can also be stored in the registry. This password will be used for logging. If the user wants to view the log file, this password has to be entered again. However, there is no secure way to protect the password (and therefore the log file) in this case!

Password history has to be enabled in the *Options* dialog (**Password History** tab).

The content of the password history file can only be viewed using the **View Password History** command from the **Tools** menu in the SafeGuard PrivateCrypto User Application.

Path and name, password, date of creation and optionally a comment for the archive are displayed in a list. The **Copy History to Clipboard** button can be used to copy the content of the history file to the clipboard from where it can be pasted into word processors for archiving concerns.

HINT:

Please be sure to empty the clipboard after using it for copying the content of the history file!

3.5 Creating new archives

New archives within SafeGuard PrivateCrypto can be created in the following ways:

1. Select the files resp. directory in Windows Explorer.

Right-click the files or the directory and click **PrivateCrypto** in the *SafeGuard PrivateCrypto* context menu.

The SafeGuardPrivateCrypto User Application opens.

The selected files are listed in the list view of the SafeGuard PrivateCrypto User Application.

If a directory was selected, the directory name is displayed under *Path*.

Click **Save**.

You can now enter a password or select a SafeGuard Enterprise key.

Password:

Enter a password, confirm it and click **OK**. The archive is created in the specified target directory: Default settings (target directory, options, etc.) can be set in the **Options** dialog of the SafeGuard PrivateCrypto User Application.

Key:

You can select any key from your SafeGuard Enterprise key ring.

Please note the difference between automatically generated SafeGuard Enterprise keys (group keys etc.) and locally generated keys.

If you select an automatically generated key, any user whose key ring also includes this key can open the archive.

If you use locally generated keys, a possible recipient can open the archive by entering the passphrase of this key.

A prerequisite for both cases is that the recipient uses SafeGuard PrivateCrypto Version 2.30 or a later version.

2. Open SafeGuard PrivateCrypto.

Add files by dragging them to the file list (dragging from Windows Explorer to the file list of SafeGuard PrivateCrypto). If you drag a directory, the entire directory will be added and the directory structure will also be saved.

Enter a password or select a key, confirm it and click **OK**. The archive is created in the specified target directory:

Default settings (target directory, options, etc.) can be set in the **Options** dialog of the SafeGuard PrivateCrypto User Application.

3. Select the files resp. directory in Windows Explorer.
Right-click the files or the directory and click **Encrypt** in *the SafeGuard PrivateCrypto* context menu.
Enter a password or select a key, confirm it and click **OK**. The archive is created as specified under Target of Encrypted Archive:
Default settings (target directory, options, etc.) can be set in the *Options* dialog of the SafeGuard PrivateCrypto User Application.

3.6 Save Encrypted

To save a new archive, proceed as follows:

1. Click the **Save** icon in the SafeGuard PrivateCrypto User Application. The **Save Encrypted** dialog is displayed.



2. You can now enter a password or select a SafeGuard Enterprise key.

Password:

Enter a password, confirm it and click **OK**. The archive is created in the specified target directory: Default settings (target directory, options, etc.) can be set in the **Options** dialog of the SafeGuard PrivateCrypto User Application.

Key:

You can select any key from your SafeGuard Enterprise key ring.

Please note the difference between automatically generated SafeGuard Enterprise keys (group keys etc.) and locally generated keys.

If you select an automatically generated key, any user whose key ring also includes this key can open the archive.

If you use locally generated keys, a possible recipient can open the archive by entering the passphrase of this key.

A prerequisite for both cases is that the recipient uses SafeGuard PrivateCrypto Version 2.30 or a later version.

3. The default target directory (specified in the *Options* dialog) is displayed in the **Target** field. Change it, if necessary. The new target directory is only valid for this single operation.
4. The name of the first file in the file list is suggested by default as a name for the archive. The file extension **.uti** is added automatically.
The file name can be changed.

HINT:

Please leave the file extensions unchanged!

5. Click **OK**.

To save an archive, also the **Save Encrypted** and the **Save Encrypted As** commands from the **File** menu of the SafeGuard PrivateCrypto User Application can be used.

3.7 Opening existing archives

To open an existing archive, just double-click it in Windows Explorer. The SafeGuard PrivateCrypto User Application is launched automatically.

- If password history logging is activated and the file is secured with a password, you will first be prompted to enter the password for the password history file. Afterwards, enter the password for the archive and the archive's content is displayed.
- If password history logging is activated and the file is secured with a SafeGuard Enterprise key included in your key ring, the archive will be opened automatically.

To open another archive, use the **Open** command from the **File** menu of the SafeGuard PrivateCrypto User Application.

To open an existing archive, the **Decrypt** command from the SafeGuard PrivateCrypto context menu in Windows Explorer can be also used. In this case, the archive will be decrypted immediately. Depending on the encryption type selected (password or key from the SafeGuard Enterprise key ring) the password has to be entered or the key used has to be available.

3.8 Adding files to an archive



To add files to an existing archive, use the **+** button. Clicking it opens an **Add Files** dialog where the files to be added can be selected.

To add files and directories to an archive, you can use also the **Add** and the **Add Directory** command from the *Edit* menu of the SafeGuard PrivateCrypto User Application.

You can also drag files or directories from Windows Explorer to SafeGuard PrivateCrypto.

Newly added files are marked with a green + symbol in the file list. They are added to the encrypted archive after clicking the **Save** symbol in the SafeGuard PrivateCrypto User Application.

3.9 Removing files from an archive



To remove files from an existing archive, use the **-** button. Select the files to be removed in the PrivateCrypto main window and click the **-** button. In a first step the file is marked with a red -. It is removed after clicking the **Save** icon in the SafeGuard PrivateCrypto User Application.

To remove files from an archive, also the **Remove** command from the **Edit** menu of the SafeGuard PrivateCrypto User Application or the Remove key on the keyboard can be used.

3.10 Decrypting files and archives

To decrypt files and archives, proceed as follows:

1. Select the required file/files in the file list of the SafeGuard PrivateCrypto User Application.
2. Click the **Decrypt** icon in the toolbar.
The *Decrypt* dialog is displayed.
3. If required, change the target directory and/or select the **Secure delete archive after decryption of all files** option.
4. Click **OK**.
All selected files are decrypted and stored in the target directory.

HINT:

To decrypt an entire archive, you can also select in Windows Explorer and click **Decrypt** in the SafeGuard PrivateCrypto context menu. Only the password has to be entered. In case a SafeGuard Enterprise key was used for encryption, the archive will automatically be decrypted, if the key used is available. Individual files cannot be decrypted using this method.

4 SafeGuard PrivateCrypto Explorer extensions

The SafeGuard PrivateCrypto Explorer extensions offer an easy way to encrypt files and directories. Additionally, they allow users to encrypt files/directories and send them directly from Windows Explorer.

Right-clicking on files/directories displays a context menu with a **SafeGuard PrivateCrypto** submenu containing the following commands:

- **Encrypt**
To encrypt files/directories directly in Windows Explorer.
- **PrivateCrypto**
To start the SafeGuard PrivateCrypto User Application. The selected files/directories are displayed in the list view of the user application. Thus, the user can add resp. remove specific files from the selection.
- **Encrypt & Send**
To encrypt files directories and to send them via an e-mail client immediately.
After successful encryption, the E-mail client is launched and the encrypted archive is attached automatically.

HINT:

SafeGuard PrivateCrypto support of sending archives via E-mail requires a properly configured E-mail program on your system!

- SafeGuard PrivateCrypto uses a Windows function called MAPI (Mail Application Program Interface) to communicate with your E-mail program. This standard interface allows SafeGuard PrivateCrypto and other applications to control your E-mail program (e.g. to create a message or to attach a file). To guarantee proper functionality your system has to meet the following requirements:
 - Your E-mail program has to be a MAPI compatible mail system.
 - Your E-mail program has to support the "Simple MAPI" interface, which is required by SafeGuard PrivateCrypto.
 - The E-mail program is configured as standard mail client (or "primary MAPI client").
- **Secure delete**
To delete files securely so they cannot be restored anymore.

4.1 Encrypting files

If you want to encrypt files using SafeGuard PrivateCrypto:

1. Select a file in Windows Explorer.
2. Right click the selected file.
A context menu with a *SafeGuard PrivateCrypto* entry is displayed.
3. Click **Encrypt**.
The SafeGuard PrivateCrypto - Save Encrypted dialog is displayed.



4. You can now enter a password or select a SafeGuard Enterprise key.

Password:

Enter a password (maximum: 32 characters or digits) in the **Password** field and confirm it in the **Confirm** field.

Key:

You can select any key from your SafeGuard Enterprise key ring.

Please note the difference between automatically generated SafeGuard Enterprise keys (group keys etc.) and locally generated keys.

If you select an automatically generated key, any user whose key ring also includes this key can open the archive.

If you use locally generated keys, a possible recipient can open the archive by entering the passphrase of this key.

A prerequisite for both cases is that the recipient uses SafeGuard PrivateCrypto Version 2.30 or a later version.

5. If you want to create a self-extracting program, activate the **Create Self-Extracting Executable** option.

Target

In filed **Target**, the default target for encrypted archives specified in the *Options* dialog of the SafeGuard PrivateCrypto User Application is displayed. The name of the first file in the archive is suggested as a name for the encrypted file/archive the name of file resp. The file extension **.uti** is added to a SafeGuard PrivateCrypto encrypted file by default. If you change the file name extension, the file may become unusable.

Using the [...] button beside the field another folder in which the encrypted source file is stored, can be specified (the new path can also be entered directly in the edit field).

If you click the **Options** button, SafeGuard PrivateCrypto offers the following additional options:

Secure delete source files after encryption:

If this option is activated, the source file is wiped (and thus cannot be restored). Only the encrypted version of the file remains on the system.

Compress data:

Compresses the selected file/archive. Please be aware of the fact, that compression may lead to an increased file size, if it is used with very small files or with files that have already been compressed. Creating an archive requires a considerably longer processing time if compression has been activated.

Log Password to password history:

The password is stored in the password history.

HINT:

These options are predefined in the *Options* dialog of the SafeGuard PrivateCrypto User Application. Changing them in this dialog overrides the default settings for this single encryption operation only.

6. Click **OK**.

4.2 Decrypting files

To decrypt files using SafeGuard PrivateCrypto, proceed as follows:

1. Select a file in Windows Explorer.
2. Right-click on the selected archive.
A context menu with a *SafeGuard PrivateCrypto* entry is displayed.
3. Click **Decrypt**.
The **Decrypt** dialog is displayed.
 - If the Archive was encrypted with a password, you will be prompted to enter it. After clicking OK the archive will be decrypted.

HINT:

If a wrong password is entered, the waiting period increases after each attempt.

If you click the **Options** button, SafeGuard PrivateCrypto offers the following additional options:

Target

In field **Target**, the default target for decrypted archives specified in the Options dialog of the SafeGuard PrivateCrypto User Application is displayed. Using the [...] button beside the field, another folder in which the encrypted source file is stored can be specified (the new path can also be entered directly in the edit field).

Secure delete archive after decryption of all files

If this option is activated, the encrypted archive is wiped (and thus cannot be restored). Only the decrypted version of the file remains on the system.

HINT:

These options are predefined in the Options dialog of the SafeGuard PrivateCrypto User Application. Changing them in this dialog overrides the default settings for this single decryption operation only.

- If the archive was encrypted with a SafeGuard Enterprise key included in your key ring, the archive will be decrypted automatically.

4.3 Creating self-extracting executables

SafeGuard PrivateCrypto offers the opportunity to create self-extracting executables. The advantage of a self-extracting executable is that they can also be decrypted from users, who do not have SafeGuard PrivateCrypto installed. For decrypting them only the password or the passphrase for a locally generated SafeGuard Enterprise key is needed.

SafeGuard PrivateCrypto can also create self-extracting programs using locally created SafeGuard Enterprise keys. These .exe files can also be decrypted on computers on which neither SafeGuard PrivateCrypto nor SafeGuard Enterprise is installed. Upon launching the program, the user is prompted to enter the passphrase of the local key. This passphrase has to be communicated to the recipient beforehand.

The passphrase is defined when creating a local key for SafeGuard Enterprise.

To create a self-extracting executable using SafeGuard PrivateCrypto:

1. Select a file in Windows Explorer.
2. Right click on the selected file.
A context menu with a *SafeGuard PrivateCrypto* entry is displayed.
3. Click **Encrypt**.
The *SafeGuard PrivateCrypto - Save Encrypted* dialog is displayed.
4. You can now enter a password or select a SafeGuard Enterprise key.

Password:

Enter a password (maximum: 32 characters or digits) in the **Password** field and confirm it in the **Confirm** field.

Key:

For self-extracting programs you can use a locally created SafeGuard Enterprise key. To decrypt the file, the recipient has to enter the passphrase for this key. The passphrase is defined when creating a local key for SafeGuard Enterprise.

5. Activate the **Create self-extracting executable** option.

Target

In field **Target**, the default target for encrypted archives specified in the *Options* dialog of the SafeGuard PrivateCrypto User Application is displayed. The name of the first file in the archive is suggested as a name for the encrypted file/archive. By default the file extension **.uti** is added to a SafeGuard PrivateCrypto encrypted file. If you change the file name extension, the file may become unusable.

Using the [...] button beside the edit field another folder in which the encrypted source file is stored, can be specified (the new path can also be entered directly in the edit field).

If you click the Options button, SafeGuard PrivateCrypto offers the following additional options:

Secure delete source files after encryption:

If this option is activated, the source file is wiped (and thus cannot be restored). Only the encrypted version of the file remains on the system.

Compress data:

Compresses the selected file/archive.

Please be aware of the fact, that compression may lead to an increased file size if it is used with very small files or with files that have already been compressed.

Log Password to password history:

The password is stored in the password history.

6. Click **OK**.

5 Minimum password length

SafeGuard PrivateCrypto offers the possibility to define a minimum length for passwords. Therefore the DWORD entry `PasswordLengthMin` under the key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\UTIMACO\SGPC
```

has to be added to the Windows registry. Define a value for `PasswordLengthMin` that defines the minimum length for passwords (in characters).

6 SafeGuard PrivateCrypto Command Line Interface

The command line syntax for SafeGuard PrivateCrypto is as follows (call pcrypt from the installation directory of SafeGuard PrivateCrypto):

```
pcrypt [path and name of source file] [options]
```

Options:

-e<archive>	creates the given encryption archive. If no archive is given, the name of the first file is used (with extension changed to .uti).
-d<archive>	decrypts the given encryption archive.
-a<archive>	adds the given files to an existing archive. If the target archive does not already exist, it is created.
-x<archive>	creates a self-extracting executable
-o<directory>	output directory (only for decrypt)
-p<password>	password for encrypting/decrypting
-l<password>	password for log file
-m	send the archive after encryption
-n	hides user interface but displays error messages
-q	hides user interface and error messages
-c[+ -]	compresses data at encryption
-s[+ -]	deletes source file after encryption/decryption
-t[+ -]	overwrites existing target files
-h	displays the command line syntax
-w	wipes files. Cannot be combined with encryption and decryption.
-aes256	use the AES-256 encryption algorithm. This only applies to new archives. Default as predefined in the SafeGuard PrivateCrypto options.
@<file>	file names starting with "@" are interpreted as control files that may contain additional file names and options. This allows passing large command line strings that normally would not be possible because of command line size restrictions.

Examples:

```
pccrypt utimaco.txt -e -oC:\Encrypted\Utimaco_Enc.txt -p12345678 -n  
-s
```

The file `utimaco.txt` is encrypted and stored as `Utimaco_Enc.txt.uti` (the file extension `.uti` is added automatically) in the directory `C:\Encrypted`. The password to decrypt the file is `12345678`. Since `-n` was specified no user interface is displayed (e.g. for entering a password). The source file located in the same directory from where `pccrypt` was called is deleted after encryption (`-s`).

Creating an archive with two files:

```
Pccrypt test.txt test2.txt -etest.uti -psecret
```

Adding a third file and a directory including files (recursively) to the above archive:

```
Pccrypt test3.txt c:\winnt -atest.uti -psecret
```

Extracting some files from an archive:

```
Pccrypt -dtest.uti test.txt test2.txt -psecret
```

7 SafeGuard PrivateCrypto OLE Automation Interface

SafeGuard PrivateCrypto contains an OLE automation server, that can be used for programmatically using PrivateCrypto from within all applications compatible with Windows scripting. This includes the Windows Scripting Host (supporting Visual Basic Scripting, JavaScript, Perl, ...) as well as Microsoft Office applications, Web pages and programming environments like Visual Basic, Visual C++ and many more.

The class exported is named "PrivateCrypto.Archive". For scripting compatibility, it exports an IDispatch interface with the following commands and properties.

Properties:

The properties of PrivateCrypto.Archive objects are preset as defined in the PrivateCrypto options. Changing the properties of an archive object affects only subsequent operations on this single object but does not change the global settings.

CompressData	Boolean	Compression on/off.
DecryptDeleteSource	Boolean	Securely delete (wipe) the encryption archive after extracting all files. This is done only if all files of the archive have been extracted successfully. Extracting a single file does not cause deletion of the entire archive, even it is the only file of the archive.
DecryptFolder	String	Target folder of decrypted archive.
EncryptDeleteSource	Boolean	Securely delete (wipe) the source files after they have successfully been added to the encryption archive.
EncryptFolder	String	Target folder for encryption archives.
EncryptAlgorithm	Integer	Encryption algorithm for the archive. Default as predefined in the SafeGuard PrivateCrypto options. Supported values are: 2=AES-256

NoGui	Boolean	<p>This option can be set to True, if absolutely no GUI should be shown. In that case, neither dialogs nor message boxes will be displayed.</p> <p>By default this option is set to False, which results in asking for passwords if they are not already passed as command parameters and popping up message boxes with descriptive text in case of errors.</p> <p>If the "NoGui" property is set to True, but a user interaction is required (e.g. entering a password), the whole current operation is cancelled and an appropriate error code is returned.</p>
PasswordLogEnabled	Boolean	Log password in password log file in case of creation of new encryption archives.

Commands:

This is the list of commands that can be called for the PrivateCrypto.Archive object. Parameters in brackets are optional. See below for a description of the single parameters:

AddFiles archive, files, pwd, (logpwd), (comment)	Add one or more files to an encryption archive. If the archive does not exist yet, it will be created.
CreateSFX archive, files, (pwd), (logpwd), (comment)	Create a self-extracting executable, containing one or more files.
Decrypt archive, (files), (pwd)	Extract one, more or even all files from an encryption archive. The files parameter may be optional here. In that case, all files are extracted from the archive.
Encrypt archive, files, (pwd), (logpwd), (comment)	Create a new encryption archive, consisting of a single or more files. If the target file already exists, the user is asked if it should be overwritten or not.
RemoveFiles archive, files, (pwd)	Remove one or more files from an encryption archive. The files are not decrypted, they are simply removed from the archive. The password is used only for authorization purposes.

Parameters:

archive	Name of the encryption archive. This is necessary for all commands.
files	This specifies either a single file name or an array of file names. See the example below on how to specify an array of file names.
pwd	The password for the encryption archive. If a new archive is created and password logging is enabled, the password is written to the log file. This parameter may be left empty for all commands. In that case, the user is prompted for the password.
logpwd	The password for the password history file. If an entry has to be added to password log file, this password is used to access the log file. The password is not required if it is already stored in the registry.
comment	The comment for the password history entry.

7.1 Example Script

Here is a sample piece of VBScript code demonstrating the use of all supported OLE automation functions:

```
language = "VBScript"

'=====
'
' This script demonstrates the SafeGuard® PrivateCrypto OLE
automation object.
' During the demo, files are created in the "c:\demo" directory.
'
'=====

On Error Resume Next
'
' Define the name of the directory used by this demo.
' This will automatically be created, if necessary.
'
sFolder = "c:\demo"

'
' Create the necessary files for this demo
'
Call Install(sFolder)
```

```

'
' Declare and create our object for interfacing SafeGuard®
PrivateCrypto
'
Dim pc
Set pc = CreateObject ("PrivateCrypto.Archive")

'
' Set encryption options
'
pc.CompressData = True
pc.EncryptDeleteSource = False

'
' Create an encryption archive, holding all files from the "files"
subdirectory
'
If Not pc.Encrypt(sFolder & "\test.uti", sFolder & "\files",
"secret") then
    MsgBox pc.GetErrorText
End If

'
' Create a self-extracting executable from a given
' list of files. Note that if one of the given file names
' represents a directory, all files within this directory
' are used. Further, the optional log file password parameter
' is filled out here.
'
Dim arrayCreate(2)
arrayCreate(0) = sFolder & "\files"
arrayCreate(1) = sFolder & "\test.uti"

If Not pc.CreateSFX(sFolder & "\test.exe", arrayCreate, "secret",
"logpwd") then
    MsgBox pc.GetErrorText
End If

'
' Decrypt all files from an archive to a given location.
' Note that the empty files array parameter (par #2) specifies
' to extract all files.
'
pc.DecryptFolder = sFolder & "\decrypt"

```

```

If Not pc.Decrypt(sFolder & "\test.uti", ,"secret") then
    MsgBox pc.GetErrorText
End If

'
' Remove a list of files from an archive
'
Dim arrayRemove(2)
arrayRemove(0) = "files\test2.txt"
arrayRemove(1) = "files\test3.txt"

If Not pc.RemoveFiles(sFolder & "\test.uti", arrayRemove, "secret")
then
    MsgBox pc.GetErrorText
End If

'
' Add a single file to an encryption archive
'
If Not pc.AddFiles(sFolder & "\test.uti", sFolder &
"\files\test2.txt", "secret") then
    MsgBox pc.GetErrorText
End If

'
' Free the SafeGuard® PrivateCrypto automation object
'
Set pc = nothing

MsgBox "End of demo. Generated files can be found in folder " &
sFolder & "."

'
'-----
' Helper routine to set-up files used by the demo script
'-----
'
Sub Install (sFolder)

    On Error Resume Next

    Dim fso
    Dim file

    '

```

```
' Create a filesystem-object
'
Set fso = CreateObject("Scripting.FileSystemObject")

'
' Create directories used by the demo
'
fso.CreateFolder sFolder
fso.CreateFolder sFolder & "\files"

'
' Delete old files from earlier runs of this demo
'
fso.DeleteFile sFolder & "\test.uti"
fso.DeleteFile sFolder & "\test.exe"
fso.DeleteFile sFolder & "\decrypt\*.*"
fso.DeleteFile sFolder & "\decrypt\files\*.*"

'
' Create input files for the demo
'
Set file = fso.CreateTextFile(sFolder & "\files\
test1.txt", True)
file.WriteLine("This is a demo text file.")
file.Close

fso.CopyFile sFolder & "\files\test1.txt", sFolder &
"\files\test2.txt"
fso.CopyFile sFolder & "\files\test1.txt", sFolder &
"\files\test3.txt"

Set fso = nothing

End Sub
```

Technical Support

Online Documentation

Our knowledge database provides answers to many typical questions about the SafeGuard product range, including its functionality, implementation, administration and troubleshooting.

Link to support area: <http://www.utimaco.com/myutimaco>

To access the public area of the knowledge database you can logon as a guest user. To access the restricted area of the knowledge database you need a valid software maintenance agreement. Our support staff continually adds to the contents of both areas, and keeps them up to date on an on-going basis.

Advanced support services and telephone support

For customers with a valid maintenance contract, qualified support staff is available to provide advice and assistance. To receive a contract offer tailored to your specific needs, please contact your sales partner.

We hope you understand that some enquiries from customers without a maintenance agreement may require several working days to process. In urgent cases, please contact the sales partner from whom you bought your licenses or software subscription.

Copyright

Copyright © 2004 - 2009 Utimaco Safeware AG - a member of the Sophos Group.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

SafeGuard is a registered trademark of Utimaco Safeware AG - a member of the Sophos group.

This product includes software developed by Eric Young (eay@mincom.oz.au). Patents rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a Trademark of Ascom, Tech Ltd.

All other product and company names mentioned are trademarks or registered trademarks of their respective owners.