

SOPHOS

SafeGuard® PrivateCrypto 2.40 Hilfe

Stand: September 2009



Inhalt

1	Einleitung	2
2	Installation.....	4
3	SafeGuard PrivateCrypto Benutzeranwendung	5
4	SafeGuard PrivateCrypto Explorer-Erweiterungen	14
5	Mindestlänge von Kennwörtern	19
6	SafeGuard PrivateCrypto Command Line-Schnittstelle.....	20
7	SafeGuard PrivateCrypto OLE Automations-Schnittstelle	22
8	Technischer Support.....	28
9	Copyright.....	29

1 Einleitung

SafeGuard PrivateCrypto bietet einen benutzerfreundlichen Weg zur Datenverschlüsselung. Eine oder mehrere Dateien und komplette Verzeichnisse können verschlüsselt werden. Die Struktur des Verzeichnisses bleibt nach der Verschlüsselung erhalten. Zusätzlich bietet SafeGuard PrivateCrypto die Möglichkeit, die verschlüsselten Dateien zu komprimieren.

1.1 Archive

Die Verschlüsselung und Komprimierung mehrerer Dateien und Verzeichnisse (Archive) wird unterstützt. Es ist möglich, einzelne Dateien zu einem Archiv ganz einfach hinzuzufügen oder aus einem solchen zu entfernen.

SafeGuard PrivateCrypto 1.x kann Archive, die mit der Version 2.x oder neuer erzeugt wurden, nicht öffnen.

SafeGuard PrivateCrypto 2.x kann Archive, die mit der Version 1.x erzeugt wurden, öffnen, kann diese jedoch nicht verändern.

Die Integration in den Windows Explorer erlaubt die Verschlüsselung von Dateien, indem man sie im Windows Explorer mit der rechten Maustaste anklickt und ein Kennwort eingibt.

Um eine Datei zu entschlüsseln, reicht ein Doppelklick auf ein Archiv und die Eingabe eines Kennworts oder der Besitz des verwendeten Schlüssels. Um Benutzern, die SafeGuard PrivateCrypto nicht installiert haben, die Entschlüsselung zu ermöglichen, können selbst-extrahierende Programme erstellt werden. Solche Dateien können durch die Eingabe des Kennworts entschlüsselt werden.

Innerhalb der SafeGuard PrivateCrypto Benutzeranwendung ist es dem Benutzer möglich, Archive zu erstellen und zu verwalten (Dateien hinzufügen/löschen). Dateien können ganz einfach zu einem Archiv hinzugefügt werden, indem man sie in die SafeGuard PrivateCrypto Dateiliste in der Benutzeranwendung zieht. Dort können auch Voreinstellungen für die Verschlüsselung/Entschlüsselung (z. B. Standardordner für verschlüsselte Dateien) festgelegt werden (Dialog SafeGuard PrivateCrypto Optionen).

1.2 Schlüssel aus dem SafeGuard Enterprise Schlüsselring

SafeGuard PrivateCrypto erlaubt es, neben der Verschlüsselung durch Eingabe eines Kennworts auch Schlüssel aus dem SafeGuard Enterprise Schlüsselring für die Verschlüsselung zu verwenden. Ist SafeGuard Enterprise auf dem Computer installiert, können alle Schlüssel im Schlüsselring des Benutzers (von SafeGuard Enterprise zentral erzeugte oder auf dem SafeGuard Enterprise Client lokal erzeugte Schlüssel) verwendet werden.

So können SafeGuard PrivateCrypto Archive einfach zwischen SafeGuard Enterprise Benutzern ausgetauscht werden. Zur Entschlüsselung des Archivs muss der zur Verschlüsselung verwendete

Schlüssel auf dem Computer vorhanden sein. Voraussetzung dafür ist, dass auf beiden Computern die Version 2.30 oder höher von SafeGuard PrivateCrypto verwendet wird.

Hinweis: Bitte beachten Sie, dass auf beiden Computern derselbe Schlüssel vorhanden sein muss (z. B. ein SafeGuard Enterprise Gruppenschlüssel). Wenn Sie einen SafeGuard Enterprise Schlüssel verwenden, der nicht im Schlüsselring des Empfängers enthalten ist, kann dieser das Archiv nicht entschlüsseln.

Wenn Sie lokal erzeugte SafeGuard Enterprise Schlüssel verwenden, müssen Sie dem Empfänger die Passphrase des Schlüssels mitteilen. Der Empfänger wird beim Öffnen des Archivs automatisch zur Eingabe dieser Passphrase aufgefordert.

1.3 Protokollierung (Kennwort-Historie)

Es ist möglich, eine Protokollierungsdatei zu erzeugen, in der das Kennwort, der Dateiname, das Datum der Verschlüsselung und (optional) ein Kommentar gespeichert werden. Diese Kennwort-Historie wird mit Hilfe eines zusätzlichen Kennworts oder eines SafeGuard Enterprise Schlüssels gesichert.

Das Kennwort müsste zusätzlich bei jeder Verschlüsselung eingegeben werden und kann deshalb gespeichert werden. Dabei ist zu beachten, dass dies ein Sicherheitsrisiko darstellt, weil die Speicherung des Kennworts nicht auf einem sicheren Weg erfolgen kann!

Wird ein SafeGuard Enterprise Schlüssel zur Sicherung verwendet, erfolgt das Abspeichern der Kennwörter ohne Benutzerinteraktion, wenn der verwendete Schlüssel im Schlüsselring des Benutzers vorhanden ist.

1.4 Verschlüsselte E-Mail-Anhänge

SafeGuard PrivateCrypto bietet die Möglichkeit, Dateien via E-Mail in einem Vorgang zu verschlüsseln und zu senden (siehe [Verschlüsseln & Senden](#) auf Seite 14). Nach der Verschlüsselung und der optionalen Komprimierung wird der E-Mail Client gestartet, und die Datei wird automatisch angehängt.

2 Installation

Um SafeGuard PrivateCrypto für PC zu installieren, starten Sie das Setup-Programm durch einen Doppelklick auf pccrypt_german.msi oder pccrypt_german.exe.. Ein Installationsassistent begleitet Sie durch den weiteren Installationsvorgang. Bitte folgen Sie den Anweisungen.

3 SafeGuard PrivateCrypto Benutzeranwendung

Um SafeGuard PrivateCrypto zu starten, klicken Sie auf **Start > Programme > Sophos > SafeGuard PrivateCrypto** (bzw. den Ordner, den Sie während der Installation ausgewählt haben). Neben den SafeGuard PrivateCrypto Explorer-Erweiterungen bietet SafeGuard PrivateCrypto die Möglichkeit, Archive über die SafeGuard PrivateCrypto Benutzeranwendung zu erzeugen und zu verwalten.

Dort können Dateien hinzugefügt und gelöscht sowie einzelne Dateien aus einem vorhandenen Archiv extrahiert werden.

Dateien (und Verzeichnisse!) können vom Windows Explorer in die PrivateCrypto-Dateiliste verschoben werden. Diese Dateien werden dann zur aktuellen Dateiliste hinzugefügt.

Die Dateiliste der SafeGuard PrivateCrypto-Benutzeranwendung zeigt alle Änderungen, die am aktuell ausgewählten Verschlüsselungsarchiv vorgenommen wurden:



Die Datei ist bereits Teil des Archivs und bleibt unverändert.



Die Datei wird zum Verschlüsselungsarchiv hinzugefügt.



Die Datei wird aus dem Verschlüsselungsarchiv herausgenommen.

Bitte beachten Sie, dass Änderungen in den Verschlüsselungsarchiven nur erfolgen, wenn die Datei gespeichert wird.

Unter Nutzung der Schaltfläche **Auspacken** oder dem Menü-Befehl **Datei > Entschlüsseln** können eine oder mehrere Dateien des Verschlüsselungsarchivs in der Liste ausgewählt und vom Archiv extrahiert (entschlüsselt) werden. Die verschlüsselten Versionen der Dateien bleiben innerhalb des Verschlüsselungsarchivs erhalten. Wenn keine Datei ausgewählt wird, extrahiert der Befehl **Entschlüsseln** standardmäßig alle Dateien des Archivs.

Werden ganze Verzeichnisse verschlüsselt, wird der entsprechende Pfad unter *Pfad* in der Listenansicht der SafeGuard PrivateCrypto Benutzeranwendung angezeigt.

3.1 SafeGuard PrivateCrypto-Optionen

Im Dialog SafeGuard PrivateCrypto *Optionen* (**Extras > Optionen**) können Voreinstellungen für Verschlüsselung/Entschlüsselung und die Kennwort-Historie festgelegt werden. Dies gilt für die SafeGuard PrivateCrypto Benutzeranwendung und für die Microsoft Windows Explorer-Erweiterungen. Die Einstellungen können auf Wunsch auch in den Dialogen *Verschlüsselt*

Speichern und *Entschlüsseln* (Klicken Sie auf die Schaltfläche **Optionen**) für die aktuelle Operation einmalig geändert werden. Die Voreinstellungen selbst können nur innerhalb des Dialogs *Optionen* geändert werden. Der Dialog *Optionen* besteht aus drei Seiten:

3.1.1 Verschlüsselung

Voreinstellungen nach der Installation:

- **Standardordner:** leer [Gleich wie Quelldatei]
- **Erzeuge ein selbst-extrahierendes Programm:** nicht aktiviert
- **Sicheres Löschen der Quelldateien nach der Verschlüsselung:** nicht aktiviert

Komprimiere Daten: aktiviert Wenn diese Einstellungen geändert wurden, können Sie durch Drücken der Schaltfläche **Standard** wiederhergestellt werden.

Die hier getätigten Einstellungen gelten für alle Verschlüsselungsoperationen, die entweder mit der SafeGuard PrivateCrypto Benutzeranwendung oder über die Explorer Erweiterungen durchgeführt werden. Sie können **temporär für eine einzige Verschlüsselungsoperation** im Dialog *Verschlüsseln* überschrieben werden.

Das Anklicken von **OK** speichert die Einstellungen und schließt den Dialog *Optionen*.

3.1.2 Entschlüsselung

Voreinstellungen nach der Installation:

- **Standardordner:** leer [Gleich wie Quelldatei]
- **Sicheres Löschen des Archivs nach dem Entschlüsseln aller Dateien:** nicht aktiviert

Wenn diese Einstellungen geändert wurden, können Sie durch Drücken der Schaltfläche **Standard** wiederhergestellt werden.

Die hier getätigten Einstellungen gelten für alle Entschlüsselungsoperationen, die entweder mit der SafeGuard PrivateCrypto Benutzeranwendung oder über die Explorer Erweiterungen durchgeführt werden. Sie können **temporär für eine einzige Entschlüsselungsoperation** im Dialog *Entschlüsseln* überschrieben werden.

- **Standardordner:**
Standardmäßig werden alle Dateien in dieses Verzeichnis entschlüsselt. In der Drop-Down-Liste können dasselbe Verzeichnis wie jenes der Quelldatei und der Ordner *Eigene Dateien* ausgewählt werden. Ein weiteres Verzeichnis kann durch das Anklicken der Schaltfläche [...] ausgewählt werden.

- **Sicheres Löschen des Archivs nach dem Entschlüsseln aller Dateien:**
Wenn diese Option ausgewählt ist, wird das verschlüsselte Dateiarchiv nach der Entschlüsselung aller Dateien gelöscht (und kann daher nicht wiederhergestellt werden).

Das Anklicken von **OK** speichert die Einstellungen und schließt den Dialog *Optionen*.

3.1.3 Kennwort-Historie

Es ist möglich, eine Protokollierungsdatei zu erzeugen, in der das Kennwort, der Dateiname, das Datum der Verschlüsselung und (optional) ein Kommentar gespeichert werden. Diese Kennwort-Historie wird mit Hilfe eines zusätzlichen Kennworts oder eines SafeGuard Enterprise Schlüssels gesichert.

Das Kennwort müsste zusätzlich bei jeder Verschlüsselung eingegeben werden und kann deshalb gespeichert werden. Dabei ist zu beachten, dass dies ein Sicherheitsrisiko darstellt, da die Speicherung des Kennworts nicht auf einem sicheren Weg erfolgen kann!

Die Anzeige der Protokollierungsdatei ist nur über den Befehl **Kennwort-Historie** aus dem Menü *Extras* möglich.

Voreinstellungen nach der Installation:

- **Kennwort-Historie einschalten:** deaktiviert
- **Datei für Kennwort Historie:** keine
- **Kennwort für Historie in der Registry speichern:** deaktiviert

Wenn diese Einstellungen geändert wurden, können Sie durch Drücken der Schaltfläche **Standard** wiederhergestellt werden.

Um Pfad und Namen, Kennwort, Datum der Erstellung und Anmerkungen für ein Archiv in einer separaten Datei zu speichern, muss die Option **Kennwort-Historie einschalten** aktiviert werden.

In einem zweiten Schritt können Name und Verzeichnis der Datei für die Kennwort-Historie spezifiziert werden.

Der Einfachheit halber kann das Kennwort für die Historie-Datei gespeichert werden. Es muss sonst jedesmal eingegeben werden, wenn ein Archiv erzeugt wird und das Kennwort in der Kennwort-Historie abgespeichert werden soll. **Beachten Sie bitte, dass dies ein Sicherheitsrisiko darstellt!**

Das Anklicken von **OK** speichert die Einstellungen und schließt den Dialog *Optionen*.

Funktionsweise

Ein Benutzer hat die Möglichkeit, seine Kennwörter in einer separaten Datei zu protokollieren. Falls der Benutzer beschließt, die Kennwörter in einer Datei zu protokollieren (was als solches ein Sicherheitsrisiko darstellt), gibt es folgende Möglichkeiten, diese Datei zu sichern:

Hinweis: Einstellungen zur Protokollierung in einer Kennwort-Historie haben bei der Verwendung von SafeGuard Enterprise Schlüsseln keine Auswirkung. Dementsprechend wird auch keine Aufforderung zur Eingabe eines Kennworts angezeigt, solange Sie SafeGuard Enterprise Schlüssel zur Verschlüsselung Ihrer Archive verwenden.

- Eine Möglichkeit ist, ein Kennwort (das für die Verschlüsselung der Kennwort-Historie benutzt wird) für jede gewünschte Protokollierung einzugeben. Dies ist zwar sicher, aber nicht sehr benutzerfreundlich, da immer zwei Kennwörter eingegeben werden müssen; eines für das Archiv und das Kennwort für die Kennwort-Historie.
- Die zweite Möglichkeit ist es, einen SafeGuard Enterprise Schlüssel für die Sicherung der Kennwort-Historie zu verwenden. Die Datei wird ohne Benutzerinteraktion verschlüsselt, wenn auf den Schlüssel im persönlichen Schlüsselring des Benutzers zugegriffen werden kann.
- Eine weitere Möglichkeit ist, das Kennwort für die Kennwort-Historie abzuspeichern. Nur wenn der Benutzer die Kennwort-Historie einsehen will, muss dieses Kennwort nochmals eingegeben werden. In diesem Fall gibt es keinen sicheren Weg, das Kennwort und somit die Kennwort-Historie und alle enthaltenen Passwörter zu schützen!

Die eingestellte Datei für die Kennwort-Historie kann im Dialog Optionen eingesehen und geändert werden (Seite *Kennwort-Historie*).

Das Einsehen der Kennwort-Historie ist nur über den Befehl **Kennwort-Historie ansehen** aus dem Menü *Extras* möglich.

Pfad und Name, das Kennwort, das Datum der Erstellung und optional ein Kommentar für das Archiv werden in einer Liste angezeigt. Über die Schaltfläche **Kopieren** lässt sich der Inhalt der Kennwort-Historie in die Z Wischenablage zu kopieren. Von dort aus kann der Inhalt für Archivierungszwecke in Textverarbeitungsprogramme übertragen werden.

Hinweis: Bitte stellen Sie sicher, dass die Zwischenablage geleert wird, nachdem sie für das Kopieren der Kennwort-Historie benutzt wurde!

3.2 Kennwortprüfung

SafeGuard PrivateCrypto prüft beim Festlegen eines Kennwortes die Sicherheit des Kennwortes direkt bei der Eingabe. Über dem Eingabefeld wird die Sicherheitsstufe des eingegebenen Kennwortes angezeigt (Sehr gering, Gering, Mittel, Hoch, Ausgezeichnet).

Besonders durch Buchstaben/Zahlenkombinationen und die Verwendung von Sonderzeichen erhöhen Sie die Sicherheit eines Kennwortes,

3.3 Neue Archive erzeugen

Neue Archive können mit SafeGuard PrivateCrypto auf folgende Weisen erzeugt werden:

1. Wählen Sie die Dateien bzw. Verzeichnisse im Windows Explorer aus.
Klicken Sie mit der rechten Maustaste und dann auf das **PrivateCrypto** Kommando im Kontextmenü *SafeGuard PrivateCrypto*. Daraufhin wird die SafeGuard PrivateCrypto Benutzeranwendung geöffnet.
Die ausgewählten Dateien werden in der Dateiliste der SafeGuard PrivateCrypto Benutzeranwendung angezeigt. Wenn ein Verzeichnis ausgewählt war, wird der Verzeichnisname unter *Pfad* angezeigt.
Wählen Sie **Speichern**.
Sie haben nun die Möglichkeit, ein Kennwort einzugeben oder einen SafeGuard Enterprise Schlüssel auszuwählen.
Kennwort:
Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **OK**. Das Archiv wird im voreingestellten Zielordner für verschlüsselte Archive erzeugt:
Voreinstellungen (Zielverzeichnis, Optionen usw.) können im Dialog *Optionen* vorgenommen werden.
Schlüssel:
Sie können jeden beliebigen Schlüssel aus Ihrem SafeGuard Enterprise Schlüsselring auswählen.
Beachten Sie bitte den Unterschied zwischen automatisch erzeugten SafeGuard Enterprise Schlüsseln (Gruppenschlüssel, ...) und lokal erzeugten.
Wenn Sie einen automatisch erzeugten Schlüssel auswählen, kann das Archiv von jedem Benutzer, der diesen Schlüssel auch in seinem Schlüsselring hat, geöffnet werden.
Wenn Sie lokal erzeugte Schlüssel verwenden, kann ein Benutzer an den Sie dieses Archiv möglicherweise weitergeben wollen, das Archiv durch Eingabe der Passphrase für diesen Schlüssel öffnen.
Voraussetzung für beide Fälle ist, dass vom Empfänger die Version 2.30 oder höher von SafeGuard PrivateCrypto verwendet wird.
2. Öffnen Sie SafeGuard PrivateCrypto.
Fügen Sie Dateien durch Drag&Drop (Ziehen vom Explorer in die Dateiliste von SafeGuard PrivateCrypto) zur Dateiliste hinzu. Wenn Sie ein Verzeichnis hinüberziehen wird das ganze Verzeichnis hinzugefügt und die Verzeichnisstruktur wird ebenfalls mit abgespeichert.
Geben Sie ein Kennwort ein oder wählen Sie einen Schlüssel aus, bestätigen Sie es und drücken Sie auf **OK**. Das Archiv wird im voreingestellten Zielverzeichnis für verschlüsselte Archive erzeugt:
Voreinstellungen (Zielverzeichnis, Optionen usw.) können im Dialog *Optionen* vorgenommen werden.

3. Wählen Sie die Dateien bzw. Verzeichnisse im Windows Explorer aus.
Klicken Sie mit der rechten Maustaste und dann auf das Kommando **Verschlüsseln** im Kontextmenü *SafeGuard PrivateCrypto*.
Geben Sie ein Kennwort ein oder wählen Sie einen Schlüssel aus, bestätigen Sie es und drücken Sie auf **OK**. Das Archiv wird im voreingestellten Zielverzeichnis für verschlüsselte Archive erzeugt:
Voreinstellungen (Zielverzeichnis, Optionen, usw.) können im Dialog *Optionen* vorgenommen werden.

3.4 Verschlüsselt speichern

Um ein neues Archiv zu speichern

1. Klicken Sie auf die Schaltfläche **Speichern** in der SafeGuard PrivateCrypto Benutzeranwendung.
Der Dialog **Verschlüsselt Speichern** wird angezeigt.
2. Sie haben nun die Möglichkeit, ein Kennwort einzugeben oder einen SafeGuard Enterprise Schlüssel auszuwählen.
Kennwort:
Geben Sie ein Kennwort ein, bestätigen Sie es, und drücken Sie auf **OK**. Das Archiv wird im voreingestellten Zielordner für verschlüsselte Archive erzeugt:
Voreinstellungen (Zielverzeichnis, Optionen usw.) können im Dialog *Optionen* vorgenommen werden.
Schlüssel:
Sie können jeden beliebigen Schlüssel aus Ihrem SafeGuard Enterprise Schlüsselring auswählen.
Beachten Sie bitte den Unterschied zwischen automatisch erzeugten SafeGuard Enterprise Schlüsseln (Gruppenschlüssel, ...) und lokal erzeugten.
Wenn Sie einen automatisch erzeugten Schlüssel auswählen, kann das Archiv von jedem Benutzer, der diesen Schlüssel auch in seinem Schlüsselring hat, geöffnet werden.
Wenn Sie lokal erzeugte Schlüssel verwenden, kann ein Benutzer an den Sie dieses Archiv möglicherweise weitergeben wollen, das Archiv durch Eingabe der Passphrase für diesen Schlüssel öffnen.
Voraussetzung für beide Fälle ist, dass vom Empfänger die Version 2.30 von SafeGuard PrivateCrypto verwendet wird.
3. Das voreingestellte Zielverzeichnis (spezifiziert im Dialog *Optionen*) wird im Eingabefeld **Archivdatei** angezeigt.
Falls erforderlich, ändern Sie es. Das neue Zielverzeichnis ist nur für diesen einen Vorgang gültig.

4. Als Name für das Archiv wird standardmäßig der Name der ersten Datei auf der Dateiliste vorgeschlagen. Die Dateierweiterung .uti wird automatisch hinzugefügt.
Der Dateiname kann geändert werden.

Hinweis: Bitte lassen Sie die Dateierweiterung unverändert!

5. Klicken Sie auf OK.

Um ein Archiv zu speichern, können auch die Befehle **Verschlüsselt speichern** und **Verschlüsselt speichern unter** aus dem Menü *Datei* der SafeGuard PrivateCrypto Benutzeranwendung benutzt werden.

3.5 Öffnen vorhandener Archive

Um ein vorhandenes Archiv zu öffnen, genügt ein Doppelklick auf das Archiv im Windows Explorer.

Die SafeGuard PrivateCrypto Benutzeranwendung wird automatisch gestartet.

- Ist die Protokollierung der Kennwort-Historie aktiviert und die Datei mit einem Kennwort gesichert, werden Sie zuerst aufgefordert, das Kennwort für die Kennwort-Historie Datei einzugeben. Anschließend müssen Sie das Kennwort für das Archiv eingeben. Danach wird der Inhalt des Archivs angezeigt.
- Ist die Protokollierung der Kennwort-Historie aktiviert und die Datei mit einem SafeGuard Enterprise Schlüssel gesichert und der Schlüssel in Ihrem Schlüsselring vorhanden, wird das Archiv automatisch geöffnet.

Sie können auch den Befehl **Öffnen** aus dem Menü *Datei* der SafeGuard PrivateCrypto Benutzeranwendung oder die Schaltfläche **Öffnen** verwenden, um ein Archiv zu öffnen.

Um ein vorhandenes Archiv zu entschlüsseln, kann auch der Befehl **Entschlüsseln** aus dem SafeGuard PrivateCrypto Kontextmenü des Windows Explorers benutzt werden. Das Archiv wird dann sofort entschlüsselt. Abhängig von der gewählten Verschlüsselungsart (Kennwort oder ein Schlüssel aus dem SafeGuard Enterprise Schlüsselring), muss das Kennwort eingegeben werden oder der verwendete Schlüssel muss vorhanden sein-

3.6 Dateien einem Archiv hinzufügen



Um Dateien zu einem existierenden Archiv hinzuzufügen, benutzen Sie die Schaltfläche +. Wenn Sie die Schaltfläche anklicken, öffnet sich ein Dateiauswahldialog, in dem Sie die Dateien auswählen können, die Sie hinzufügen wollen.

Ebenso kann man aus dem Menü *Bearbeiten* die Kommandos **Hinzufügen** oder **Verzeichnis hinzufügen** benutzen, um Dateien oder Verzeichnisse zu einem Archiv hinzuzufügen.

Noch komfortabler ist es, Dateien oder Verzeichnisse vom Explorer in SafeGuard PrivateCrypto hineinzuziehen.

Neu hinzugefügte Dateien werden in der Dateiliste mit einem grünen + angezeigt. Sie werden zum verschlüsselten Archiv hinzugefügt, wenn man auf die Schaltfläche **Speichern** in der Symbolleiste klickt.

3.7 Dateien aus einem Archiv entfernen



Um Dateien aus einem vorhandenen Archiv zu entfernen, benutzen Sie die Schaltfläche -. Wählen Sie die zu entfernenden Dateien im PrivateCrypto Hauptfenster aus und klicken Sie auf die Schaltfläche -.

In einem ersten Schritt wird die Datei mit einem roten - markiert. Wirklich aus dem Archiv entfernt wird die Datei erst, wenn Sie auf die Schaltfläche **Speichern** in der SafeGuard PrivateCrypto Benutzeranwendung klicken.

Anstelle der Schaltfläche - können Sie auch den Befehl **Löschen** aus dem Menü *Bearbeiten* der SafeGuard PrivateCrypto Benutzeranwendung oder die Taste Entfernen der Tastatur benutzen.

3.8 Dateien und Archive entschlüsseln

Zum Entschlüsseln von Dateien und Verzeichnissen

1. Wählen Sie die gewünschten Dateien in der Dateiliste der SafeGuard PrivateCrypto Benutzeranwendung aus.
2. Klicken Sie auf die Schaltfläche **Auspacken** in der Symbolleiste.
Der Dialog *Entschlüsseln* wird angezeigt.
3. Falls erwünscht, ändern Sie das Zielverzeichnis und wählen Sie die Option *Sicheres Löschen des Archivs* nach dem Entschlüsseln aller Dateien.
4. Klicken Sie auf **OK**.
Alle ausgewählten Dateien werden nun entschlüsselt und im Zielverzeichnis gespeichert.

Hinweis: Um ein ganzes Archiv zu entschlüsseln, ist es auch möglich, es im Windows Explorer auszuwählen und Entschlüsseln im Kontextmenü SafeGuard PrivateCrypto anzuklicken. Lediglich das Kennwort muss eingegeben werden. Wurde zum Verschlüsseln ein SafeGuard

Enterprise Schlüssel verwendet, wird das Archiv automatisch entschlüsselt, wenn der verwendete Schlüssel verfügbar ist. Einzelne Dateien können nicht ausgewählt werden.

4 SafeGuard PrivateCrypto Explorer-Erweiterungen

Die Erweiterungen zum SafeGuard PrivateCrypto Explorer bieten einen einfachen Weg, Dateien und Verzeichnisse zu verschlüsseln. Zusätzlich erlauben sie es dem Benutzer, Dateien/Verzeichnisse zu verschlüsseln und diese direkt vom Windows Explorer aus per E-Mail zu versenden.

Wird mit der rechten Maustaste auf Dateien/Verzeichnisse geklickt, öffnet sich ein Kontextmenü mit dem Untermenü **SafeGuard PrivateCrypto**. Dieses enthält folgende Kommandos:

- **Verschlüsseln**

Zum Verschlüsseln von Dateien/Verzeichnissen direkt im Windows Explorer.

- **PrivateCrypto**

Startet die SafeGuard PrivateCrypto Benutzeranwendung. Die ausgewählten Dateien/Verzeichnisse werden in der Dateiliste der Benutzeranwendung angezeigt. Dies gibt dem Benutzer die Möglichkeit, bestimmte Dateien hinzuzufügen oder zu löschen.

- **Verschlüsseln & Senden**

Verschlüsseln von Dateien und Verzeichnisse und direktes Senden via E-Mail Client. Nachdem die Verschlüsselung abgeschlossen ist, wird der E-Mail Client gestartet und das verschlüsselte Archiv wird automatisch angehängt.

Hinweis: Das Senden von Archiven via E-Mail erfordert ein entsprechend konfiguriertes E-Mail-Programm auf Ihrem System!

SafeGuard PrivateCrypto benutzt die Windows-Funktion MAPI (Mail Application Program Interface) für die Kommunikation mit Ihrem E-Mail-Programm. Diese Standard-Schnittstelle erlaubt es SafeGuard PrivateCrypto und anderen Anwendungen, Ihr E-Mail-Programm zu kontrollieren (z. B. Verfassen einer Nachricht oder Dateien anhängen). Um eine angemessene Funktionalität zu gewährleisten, muss Ihr System folgende Anforderungen erfüllen:

- Ihr E-Mail-Programm muss ein MAPI-kompatibles Mail-System sein.
 - Ihr E-Mail-Programm muss die "Simple MAPI"-Schnittstelle unterstützen, die für SafeGuard PrivateCrypto erforderlich ist.
 - Das E-Mail-Programm ist als Standard Mail Client ("primary MAPI client") konfiguriert.
- **Sicheres Löschen**
Ermöglicht das sichere Löschen von Dateien, sodass sie nicht wiederhergestellt werden können.

4.1 Dateien verschlüsseln

Verschlüsselung von Dateien mit SafeGuard PrivateCrypto:

1. Wählen Sie die Dateien im Windows Explorer aus.
2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Dateien.
Das Kontext-Menü mit dem Eintrag *SafeGuard PrivateCrypto* wird angezeigt.
3. Klicken Sie auf **Verschlüsseln**.
Der Dialog **Verschlüsselt Speichern** wird angezeigt.
4. Sie haben nun die Möglichkeit, ein Kennwort einzugeben oder einen SafeGuard Enterprise Schlüssel auszuwählen.

Kennwort:

Geben Sie das Kennwort (höchstens 32 Zeichen) im Eingabefeld **Kennwort** ein und bestätigen Sie es im Eingabefeld **Bestätigung**.

Schlüssel:

Sie können jeden beliebigen Schlüssel aus Ihrem SafeGuard Enterprise Schlüsselring auswählen.

Beachten Sie bitte den Unterschied zwischen automatisch erzeugten SafeGuard Enterprise Schlüsseln (Gruppenschlüssel, ...) und lokal erzeugten.

Wenn Sie einen automatisch erzeugten Schlüssel auswählen, kann das Archiv von jedem Benutzer, der diesen Schlüssel auch in seinem Schlüsselring hat, geöffnet werden.

Wenn Sie lokal erzeugte Schlüssel verwenden, kann ein Benutzer an den Sie dieses Archiv möglicherweise weitergeben wollen, das Archiv durch Eingabe der Passphrase für diesen Schlüssel öffnen.

Voraussetzung für beide Fälle ist, dass vom Empfänger die Version 2.30 von SafeGuard PrivateCrypto verwendet wird.

Archivdatei

Unter *Archivdatei* wird das voreingestellte Zielverzeichnis für verschlüsselte Archive, das im Dialog *Optionen* der SafeGuard PrivateCrypto Benutzeranwendung, ausgewählt wurde, angezeigt. Als Name für die verschlüsselte Datei/das Verzeichnis wird der Name der ersten Datei des Archivs vorgeschlagen. Standardmäßig wird die Dateiendung **.uti** an die verschlüsselte Datei angehängt. Wird die Dateiendung geändert, kann das Archiv unbrauchbar werden.

Benutzt man die Schaltfläche **Durchsuchen** neben dem Eingabefeld, kann ein anderer Ziellordner für die verschlüsselte Quelldatei angegeben werden (der neue Pfad kann auch direkt im Eingabefeld für die Archivdatei eingegeben werden).

Wenn Sie auf die Schaltfläche **Optionen** klicken, bietet SafeGuard PrivateCrypto weitere Optionen an:

Selbst extrahierendes Programm erzeugen

Ist diese Option aktiviert, wird ein selbst extrahierendes Programm erzeugt.

Sicheres Löschen der Quelldateien nach der Verschlüsselung:

Ist diese Option aktiviert, wird die Quelldatei auf eine Art und Weise gelöscht, dass sie selbst mit entsprechenden Programmen nicht wiederhergestellt werden kann. Nur die verschlüsselte Version der Datei bleibt im System.

Daten komprimieren:

Komprimiert die ausgewählte Datei/ das Verzeichnis.

Bitte beachten Sie, dass die Komprimierung die Datei eventuell vergrößert, wenn sie auf sehr kleine Dateien, oder auf Dateien, die bereits komprimiert wurden, angewendet wird. Die zur Archiverstellung benötigte Zeit ist bedeutend länger, wenn die Komprimierung aktiviert ist.

Kennwort in der Kennwort-Historie merken:

Das verwendete Kennwort wird in der Kennwort-Historie gespeichert.

Hinweis: Die Voreinstellungen für diese Optionen sind im Dialog Optionen der SafeGuard PrivateCrypto Benutzeranwendung festgelegt. Werden sie im Dialogfeld geändert, werden die vorgegebenen Einstellungen nur für diesen Verschlüsselungsvorgang außer Kraft gesetzt.

5. Klicken Sie auf OK.

4.2 Dateien entschlüsseln

Zum Entschlüsseln von Dateien mit SafeGuard PrivateCrypto:

1. Wählen Sie das Archiv im Windows Explorer aus.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Archiv.
Das Kontextmenü mit einem *SafeGuard PrivateCrypto* Eintrag wird angezeigt.
3. Klicken Sie auf **Entschlüsseln**.
Der Dialog *Entschlüsseln* wird angezeigt.
 - Wurde das Archiv mit einem Kennwort verschlüsselt, werden Sie aufgefordert, dieses einzugeben.
Nach dem Klicken auf **OK** wird das Archiv entschlüsselt.

Hinweis: Wenn Sie ein falsches Kennwort eingeben, verlängert sich die Wartezeit nach jedem Versuch.

Wenn Sie auf die Schaltfläche **Optionen** klicken, bietet SafeGuard PrivateCrypto folgende

zusätzlichen Optionen an:

Archivdatei

Unter Archivdatei wird das voreingestellte Zielverzeichnis für verschlüsselte Archive, das im Dialog Optionen der SafeGuard PrivateCrypto Benutzeranwendung ausgewählt wurde, angezeigt. Benutzt man die Schaltfläche **Durchsuchen** neben dem Eingabefeld, kann ein beliebiger Ordner, in dem die verschlüsselte Datei gespeichert werden soll, spezifiziert werden (der neue Pfad kann auch direkt im Eingabefeld angegeben werden).

Sicheres Löschen des Archivs nach dem Entschlüsseln aller Dateien

Ist diese Option aktiviert, wird das Archiv nach dem Entschlüsseln aller Dateien sicher gelöscht (und kann nicht wiederhergestellt werden). Nur die entschlüsselte Dateien bleiben im System.

Hinweis: Diese Optionen sind im Dialog Optionen der SafeGuard PrivateCrypto Benutzeranwendung voreingestellt. Werden sie im Dialogfeld geändert, werden die vorgegebenen Einstellungen nur für diesen Entschlüsselungsvorgang außer Kraft gesetzt.

- Wurde das Archiv mit einem SafeGuard Enterprise Schlüssel verschlüsselt und der Schlüssel ist in Ihrem Schlüsselring vorhanden, wird das Archiv automatisch entschlüsselt.

4.3 Selbst-extrahierende Programme erzeugen

SafeGuard PrivateCrypto erlaubt Ihnen, selbst-extrahierende Programme zu erzeugen. Der Vorteil von selbst-extrahierenden Archiven liegt darin, dass sie auch von Benutzern entschlüsselt werden können, die SafeGuard PrivateCrypto nicht installiert haben. Um sie zu entschlüsseln, benötigt man lediglich das Kennwort oder die Passphrase für einen lokal erzeugten SafeGuard Enterprise Schlüssel.

SafeGuard PrivateCrypto kann auch selbst-extrahierende Programme unter der Verwendung von lokal erzeugten SafeGuard Enterprise Schlüsseln erzeugen. Diese .exe Dateien können auch auf Computern ohne SafeGuard PrivateCrypto und ohne SafeGuard Enterprise entschlüsselt werden. Beim Starten eines solchen Programms wird der Benutzer aufgefordert, die Passphrase des lokalen Schlüssels einzugeben. Diese muss dem Empfänger vorher bekanntgegeben werden.

Die Passphrase wird beim Erzeugen eines lokalen Schlüssels für SafeGuard Enterprise festgelegt.

Um ein selbstextrahierendes Archiv mit SafeGuard PrivateCrypto zu erzeugen:

1. Wählen Sie eine Datei im Windows Explorer aus.
2. Klicken Sie mit der rechten Maustaste auf die ausgewählte Datei.
Ein Kontextmenü mit dem Eintrag *SafeGuard PrivateCrypto* wird angezeigt.
3. Wählen Sie **Verschlüsseln** aus.
Der Dialog *Verschlüsselt Speichern* wird angezeigt.

4. Sie haben nun die Möglichkeit, ein Kennwort einzugeben oder einen SafeGuard Enterprise Schlüssel auszuwählen.

Kennwort:

Geben Sie das Kennwort (höchstens 32 Zeichen) im Eingabefeld Kennwort ein und bestätigen Sie es im Eingabefeld *Bestätigung*.

Schlüssel:

Für selbst extrahierende Programme können Sie einen lokal erzeugten SafeGuard Enterprise Schlüssel verwenden. Um die Datei zu entschlüsseln, muss der Empfänger die Passphrase für diesen Schlüssel eingeben. Die Passphrase wird beim Erzeugen des Schlüssels in SafeGuard Enterprise festgelegt.

5. Klicken Sie auf **Optionen>>** und aktivieren Sie die Option **Selbst-extrahierendes Programm erzeugen**.

Archivdatei

Unter *Archivdatei* wird das voreingestellte Zielverzeichnis für verschlüsselte Archive, das im Dialog *Optionen* der SafeGuard PrivateCrypto Benutzeranwendung ausgewählt wurde, angezeigt. Als Name für die verschlüsselte Datei/das Verzeichnis wird der Name der ersten Datei des Archivs vorgeschlagen. Standardmäßig wird die Dateiendung **.uti** an die verschlüsselte Datei angehängt. Wird die Dateiendung geändert, kann das Archiv unbrauchbar werden.

Benutzt man die Schaltfläche [...] neben dem Eingabefeld, kann ein anderer Zielordner für die verschlüsselte Quelldatei, angegeben werden (der neue Pfad kann auch direkt im Eingabefeld für die Archivdatei eingegeben werden).

Wenn Sie auf die Schaltfläche *Optionen* klicken, bietet SafeGuard PrivateCrypto folgende weitere Optionen an:

Sicheres Löschen der Quelldateien nach der Verschlüsselung:

Ist diese Option aktiviert, wird die Quelldatei auf eine Art und Weise gelöscht, dass sie selbst mit entsprechenden Programmen nicht wiederhergestellt werden kann. Nur die verschlüsselte Version der Datei bleibt im System.

Daten komprimieren:

Komprimiert die ausgewählte Datei/ das Verzeichnis.

Bitte beachten Sie, dass die Komprimierung die Datei eventuell vergrößert, wenn sie auf sehr kleine Dateien angewendet wird, oder auf Dateien, die bereits komprimiert wurden. Die zur Archiverstellung benötigte Zeit ist bedeutend länger, wenn die Komprimierung aktiviert ist.

Kennwort in der Kennwort-Historie merken:

Das verwendete Kennwort wird in der Kennwort-Historie gespeichert.

6. Klicken Sie auf **OK**.

5 Mindestlänge von Kennwörtern

SafeGuard PrivateCrypto bietet die Möglichkeit, eine Mindestlänge für Kennwörter festzulegen. Dazu kann der DWORD Eintrag PasswordLengthMin unter folgendem Schlüssel in der Windows-Registrierung abgelegt werden:

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

64 Bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UTIMACO\SGPC

Legen Sie einen Wert für PasswordLengthMin fest, der die Mindestlänge für Kennwörter definiert (in Zeichen).

6 SafeGuard PrivateCrypto Command Line-Schnittstelle

Die Command Line Syntax für SafeGuard PrivateCrypto ist wie folgt (rufen Sie `pcrypt` vom Installationsverzeichnis von SafeGuard PrivateCrypto auf):

```
pcrypt [Pfad und Name der Quelldatei] [Optionen]
```

Optionen:

-e<Archiv>	Erstellt das vorhandene Verschlüsselungsarchiv. Wird kein Archiv angegeben, wird der Name der ersten Datei benutzt (und die Endung <code>.uti</code>).
-d<Archiv>	Entschlüsselt das vorhandene Archiv.
-a<Archiv>	Fügt die gegebenen Dateien zu einem vorhandenen Archiv hinzu. Falls das Zielarchiv noch nicht existiert, wird es erstellt.
-x<Archiv>	Erstellt ein selbst-extrahierendes Programm.
-o<Verzeichnis>	Output Verzeichnis (nur für Entschlüsselung)
-p<Kennwort>	Kennwort für Verschlüsselung/Entschlüsselung
-l<Kennwort>	Kennwort für Kennwort-Historie
-m	Senden des Archivs nach der Verschlüsselung.
-n	Verbirgt die Benutzerschnittstelle, zeigt jedoch Fehlermeldungen an.
-q	Verbirgt die Benutzerschnittstelle und Fehlermeldungen.
-c[+ -]	Komprimiert Daten während der Verschlüsselung.
-s[+ -]	Löscht die Quelldatei(en) nach der Verschlüsselung/Entschlüsselung
-t[+ -]	Überschreibt vorhandene Zieldateien.
-h	Zeigt die Commandline Syntax an
-w	Löscht Dateien. Kann nicht mit Verschlüsselung und Entschlüsselung kombiniert werden.
-aes256	Verwendet den AES-256 Algorithmus. Gilt nur für neue Archive. Default wie in den SafeGuard PrivateCrypto Optionen voreingestellt.

@<file>	Dateinamen, die mit "@" beginnen, werden als Kontrolldateien verstanden, die zusätzliche Dateinamen und Optionen enthalten können. Dies erlaubt das Übertragen großer Command Line Strings, das normalerweise aufgrund der Restriktion der Größe der Command Lines nicht möglich wäre.
---------	--

Beispiele:

```
pcrypt sophos.txt -e -oC:\Encrypted\Sophos_Enc.txt -p12345678 -n  
-s
```

Die Datei `sophos.txt` wird verschlüsselt und als `Sophos_Enc.txt.uti` (die Dateiendung `.uti` wird automatisch angehängt) im Verzeichnis `C:\Encrypted` abgespeichert. Das Kennwort für das Entschlüsseln der Datei lautet 12345678. Weil `-n` spezifiziert wurde, wird keine Benutzerschnittstelle angezeigt (z. B. um ein Kennwort einzugeben). Die Quelldatei, die sich im selben Verzeichnis befindet, aus dem `pcrypt` aufgerufen wurde, wird nach der Verschlüsselung gelöscht (`-s`).

Erstellen eines Archivs mit zwei Dateien:

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

Hinzufügen einer dritten Datei und eines Verzeichnisses, das Dateien enthält (unter Zurückgreifen auf das obere Archiv):

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

Dateien von einem Archiv extrahieren:

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

7 SafeGuard PrivateCrypto OLE Automations-Schnittstelle

SafeGuard PrivateCrypto enthält einen OLE Automations-Server, der für den programmatischen Gebrauch von SafeGuard PrivateCrypto innerhalb aller Anwendungen, die mit dem Windows-Scripting kompatibel sind, benutzt werden kann. Dies schließt den Windows Scripting Host (unterstützt Visual Basic Scripting, JavaScript, Perl, ...) genauso wie Microsoft Office Anwendungen, Web-Seiten und Programmierumgebungen wie Visual Basic, Visual C++ und viele andere mehr, ein.

Die Exportklasse wird als "PrivateCrypto.Archive" bezeichnet. Für die Scripting-Kompatibilität exportiert sie eine Idispatch-Schnittstelle mit folgenden Befehlen und Eigenschaften:

Eigenschaften:

Die Eigenschaften der PrivateCrypto.Archive Objekte sind so voreingestellt, wie es in den Optionen von SafeGuard PrivateCrypto definiert ist. Werden die Eigenschaften eines Archivobjektes geändert, betrifft dies nur nachfolgende Vorgänge dieses einzelnen Objekts. Die Gesamteinstellungen werden jedoch nicht verändert.

CompressData	Boolean	Komprimierung an/aus.
DecryptDeleteSource	Boolean	Sicheres Löschen des Verschlüsselungsarchivs, nachdem alle Dateien extrahiert wurden. Dies geschieht nur, wenn alle Dateien des Archivs erfolgreich extrahiert wurden. Wird eine einzelne Datei extrahiert, wird dadurch nicht das gesamte Archiv gelöscht, selbst wenn es die einzige Datei des Archivs ist.
DecryptFolder	String	Zielordner des verschlüsselten Archivs.
EncryptDeleteSource	Boolean	Sicheres Löschen der Quelldateien, nachdem sie erfolgreich zum Verschlüsselungsarchiv hinzugefügt wurden.
EncryptFolder	String	Zielordner für Verschlüsselungsarchive.
EncryptAlgorithm	Integer	Verschlüsselungsalgorithmus für das neue Archiv. Default wie voreingestellt in den PrivateCrypto Optionen. Unterstützte Werte: 2=AES-256

NoGui	Boolean	Diese Option kann auf True gesetzt werden, wenn kein GUI gezeigt werden soll. In diesem Fall werden weder Dialoge noch Fehler oder Warnungen angezeigt. Standardmäßig wird diese Option auf False gesetzt. Daraus ergibt sich, dass nach Kennwörtern gefragt wird, wenn sie nicht bereits als Befehlsparameter angegeben sind. Wenn die "NoGui"-Eigenschaft auf True gesetzt wurde, aber eine Benutzer-Interaktion erforderlich ist (z. B. Eingabe eines Kennworts), wird der gesamte Vorgang gelöscht und ein entsprechender Fehlercode zurückgeschickt.
PasswordLogEnabled	Boolean	Soll das Kennwort in der Kennwort-Historie protokolliert werden, wenn ein Verschlüsselungsarchiv erzeugt wird.

Befehle:

Dies ist die Liste der Befehle, die für PrivateCrypto.Archive aufgerufen werden können. Die in Klammern gesetzten Parameter sind optional. Weiter unten finden Sie eine Beschreibung der einzelnen Parameter:

AddFiles archive, files, pwd, (logpwd), (comment)	Eine oder mehrere Dateien zu einem Verschlüsselungsarchiv hinzufügen. Wenn das Archiv nicht bereits existiert, wird es erzeugt.
CreateSFX archive, files, (pwd), (logpwd), (comment)	Erzeugen eines selbst-extrahierenden Programms, das eine oder mehrere Dateien enthält.
Decrypt archive, (files), (pwd)	Extrahieren von einer, mehreren oder aller Dateien aus einem Verschlüsselungsarchiv. Die Datei-Parameter können hier optional sein. In diesem Fall werden alle Dateien aus dem Archiv extrahiert.
Encrypt archive, files, (pwd), (logpwd)	Erzeugen eines neuen Verschlüsselungsarchivs, das aus einer oder mehreren Dateien besteht. Falls die Zielfeile bereits besteht, wird der Benutzer gefragt, ob sie überschrieben werden soll oder nicht.
RemoveFiles archive, files, (pwd)	Entfernen von einer oder mehreren Dateien aus einem Verschlüsselungsarchiv. Die Dateien sind nicht entschlüsselt, sondern werden einfach aus dem Archiv entfernt. Das Kennwort wird nur für Authentifizierungszwecke benutzt.

Parameter:

archive	Name des Verschlüsselungsarchivs. Dieser ist für alle Befehle erforderlich.
files	Darunter versteht man entweder einen einzelnen Dateinamen oder eine Reihe von Dateinamen. Weiter unten finden Sie ein Beispiel, wie man eine Reihe von Dateinamen spezifiziert.
pwd	Das Kennwort für das Verschlüsselungsarchiv. Wird ein neues Archiv erzeugt und ist die Kennwortprotokollierung aktiviert, wird das Kennwort für das Archiv in die Kennwort-Historie geschrieben. Wird kein Kennwort angegeben, wird der Benutzer nach dem Kennwort gefragt.
logpwd	Das Kennwort für die Kennwort-Historie. Soll ein Eintrag zur Kennwort-Historie hinzugefügt werden, wird das Kennwort für den Zugang zur Kennwort-Historie benötigt. Das Kennwort ist nicht erforderlich, wenn es in der Registrierung gespeichert ist.
comment	Der Kommentar für den Eintrag in der Kennwort Historie.

7.1 Beispiel-Skript

Hier ein Sample eines VBScript Codes, das die Verwendung aller unterstützten OLE Automatisierungsfunktionen demonstriert :

```
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
```

8 Technischer Support

Technischen Support erhalten Sie auf <http://www.sophos.de/support>.

Wenn Sie den technischen Support kontaktieren, halten Sie bitte zumindest folgende Angaben bereit:

- Die Versionsnummer(n) der Sophos Software
- Betriebssystem(e) und Patch-Level(s)
- Den genauen Wortlaut etwaiger Fehlermeldungen

9 Copyright

Copyright © 2009 Sophos Plc. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Sophos ist ein eingetragenes Warenzeichen der Sophos Plc, und SafeGuard ist ein eingetragenes Warenzeichen der Utimaco Safeware AG, einem Mitglied der Sophos Gruppe. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Alle SafeGuard Produkte unterliegen dem Urheberrecht der Utimaco Safeware AG, einem Mitglied der Sophos Gruppe oder, sofern anwendbar, ihrer Lizenzinhaber. Alle weiteren Sophos Produkte unterliegen dem Urheberrecht der Sophos Plc oder, sofern anwendbar, ihrer Lizenzinhaber.