

CyProtect Key Administration

Key Administration for 512 Bit Polymorphic Cipher

Version 1.3

Documentation

July 22, 2004

Copyright © 2004 CyProtect AG. All rights reserved.

Contents

1	Introduction.....	3
1.1	Example of use: file encryption.....	3
1.2	Example of use: drive encryption.....	3
1.3	MD5.....	4
1.4	Admin / User Mode.....	4
2	Installation.....	5
3	Licensing.....	6
4	Using CyProtect Key Administration.....	7
4.1	Key – New.....	8
4.2	Key – Import.....	9
4.3	Key – Export.....	9
4.4	Key – Delete.....	9
4.5	Key – Copy (>>>).....	9
4.6	Password.....	10
4.7	Group – New.....	10
4.8	Group – Rename.....	10
4.9	Group – Delete.....	10
4.10	iKey – Open.....	10
4.11	iKey – Close.....	10
4.12	iKey – Delete.....	11
4.13	iKey – Copy (<<<).....	11
4.14	Log file.....	11
5	Version history.....	12
5.1	Version 1.0 (October 15, 2003).....	12
5.2	Version 1.1 (November 05, 2003).....	12
5.3	Version 1.2 (November 18, 2003).....	12
5.4	Version 1.3 (July 22, 2004).....	12
6	Contact.....	13

1 Introduction

With *CyProtect Key Administration* you can generate keys and put them on a SafeNet iKey. These keys can be used instead of a usual password in the CyProtect products:

- **CyProtect File Encryption**
- **CyProtect Drive Encryption**

A key is a sequence of random bytes addressed by a unique name.

With random numbers instead of an entered password you get the full advantage of the current 512 bit Polymorphic Cipher. In order to create a „real“ 512 bit (= 64 bytes) key the input of 64 characters is not sufficient because the possible range of values for one byte (0 – 255) is not used even if some special characters are entered. Such password must either be much longer or internally extended. With the use of random numbers as „password“ these disadvantages can be avoided.

1.1 Example of use: file encryption

Imagine a company with executives who want to exchange documents or save them on a server in a secure encrypted way. In order to avoid the need of remembering a lot of passwords SafeNet iKeys should be used. A trustworthier administrator should have access to the documents in case of an emergency (e.g. lost or damaged iKey).

With *CyProtect Key Administration* in cooperation with *CyProtect File Encryption* this can be done as follows: The administrator installs *CyProtect Key Administration* on his (secure) PC and gets the SafeNet iKeys. Now he generates a new key (e.g. „Management“) and copies this key on all the iKeys for the executives. The iKeys are protected by a default pin code which can easily be changed by the executives.

Before exchanging or saving a document it is encrypted with the *CyProtect File Encryption* using the key „Management“ from the iKey. Everyone who wants to decrypt those documents need an iKey with the appropriate key.

If one of the executives loses his iKey but needs access to some encrypted documents urgently then the administrator can export this key from his key database into a file (optionally encrypted with a simple password) and send this file to the executive. If he has installed the *CyProtect Key Administration* (in user mode, see below) on his PC he can import this key into his private key database and immediately has access to the encrypted documents.

With a log file the administrator is able to create a new iKey with exactly the same keys on it if an iKey is lost or damaged.

1.2 Example of use: drive encryption

Field managers are provided with notebooks with sensitive data on them. These data should reside on an encrypted virtual drive secured by an SafeNet iKey.

CyProtect Drive Encryption is installed on each notebook. The keys for the virtual encrypted drives were generated with the *CyProtect Key Administration*, copied to SafeNet iKeys and handed to the

field managers.

Similar to the above mentioned setting the administrator is responsible for generating, saving and distributing the keys. The user must remember only the pin code for his iKey and in case of an emergency the administrator can always help because he has all the utilized keys.

1.3 MD5

When exporting a key into a file you can encrypt it with a password and optionally save a part (last byte) of the so called MD5 digest (hash code) of the password. This gives the user who imports this key file into his database the opportunity to check the password while entering. Caution: Because only a part of the MD5 is saved it is possible to enter a „wrong“ password that is accepted anyhow. So this check byte is only usefull to avoid common mistakes entering a password (upper and lower case, character swap).

Today's state of science does not give you an opportunity to compute the original password or key from the given hash code. But you have to keep in mind that the convenience this feature offers may cause a security hole. So we recommend not to use this feature for those users who attach great importance to security.

1.4 Admin / User Mode

CyProtect Key Administration is able to operate in two different modes depending on your license key:

- **Admin Mode:** This mode provides the unrestricted functionality to the administrator.
- **User Mode:** This mode may be usefull for end users. With this software an user is able to import keys as a files into his own key database and to copy a key from the key database to an iKey.

Following features are disabled in user mode:

- x Key – New
- x Key – Export
- x All functions refering to groups

2 Installation

Please consider the following installation requirements:

- Microsoft Windows 98, ME, NT (service pack 6 or above), 2000 or XP
- Pentium compatible PC
- 64 MB RAM
- 25 MB disk space free
- 800x600 screen resolution, at least 256 colores

Please start the setup program and follow the instructions shown on the screen.

You can use *CyProtect Key Administration* basically without SafeNet iKeys but in this case the benefit is quite limited.

Presently the following versions of SafeNet iKey are supported:

- 10xx (1000 and 1032)
- 20xx (2000 and 2032)
- 3000

Attention: Each version of SafeNet iKey requires a separate version of this software. You will not be able to use different versions of SafeNet iKeys with one version of *CyProtect Key Administration*.

3 Licensing

In order to unlock the software you need a key file (cykey.key) which you will get after registration (source see chapter). The you have to copy this file into the installation directory of the software or

C:\Program files\Common files\CyProtect.

4 Using CyProtect Key Administration

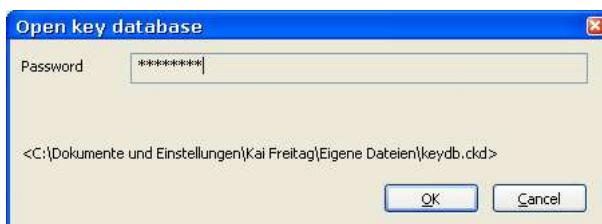
Starting the software for the first time, a new empty key database is created. The key database consists of only one file so backups can be easily done.

In order to encrypt this new key database you can enter a password:



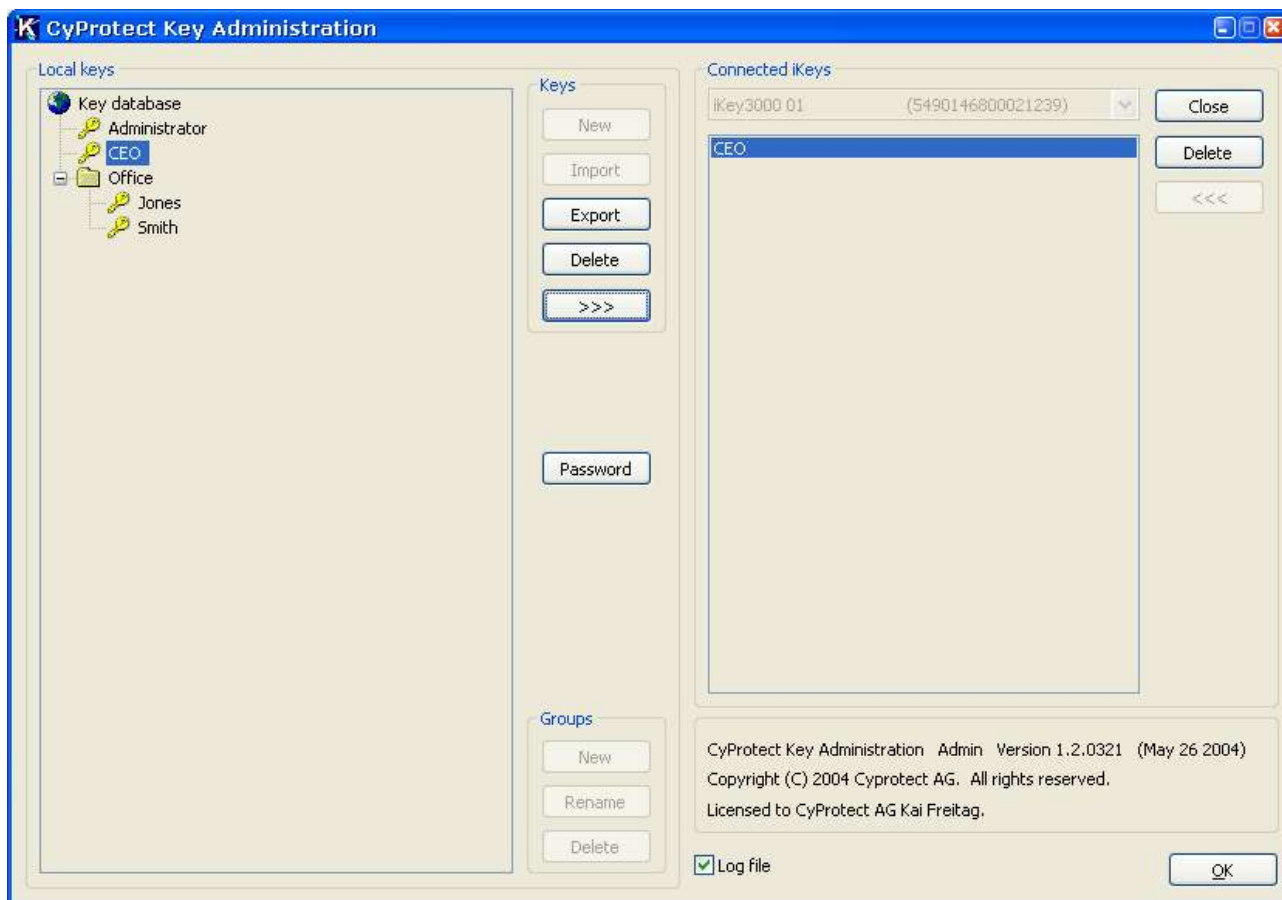
You can use an empty password as well but then please keep in mind that the key database with all the keys is saved as plaintext on your harddisk. We do recommend using a good password here!

At all further starts of the software you will be prompted for the password of the key database:



The path of the key database is displayed for your information.

Now you can see the main dialog:



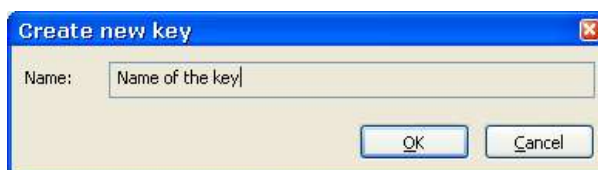
On the left you see the content of the key database.

In the upper right corner you see the currently connected iKeys. This list is permanently updated so you can connect new iKeys to your PC and will see them after a few moments in this list.

In the lower right corner the license data and some version information is shown.

4.1 Key – New

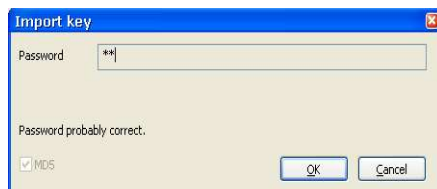
If a group or the root element is selected you can generate a new key within this level:



Please enter the name of the new key. Every key name is unique in the key database. The random content of the key will be generated automatically. In order to calculate these random numbers every user action (mouse move or click, keyboard) and some other data (like processor speed) is used.

4.2 Key – Import

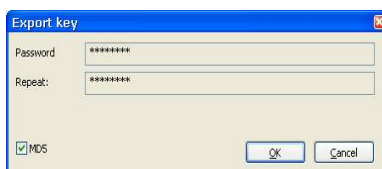
In order to put a key into your database that you have as a file, please select the desired group or the root element on the left and click „Import“. Then you have to select the (exported) key file and enter the appropriate password.



In the example above you see the checked „MD5“ meaning that the key file was encrypted with a password and a part of the MD5 digest of this password was stored as well. As long as the MD5 digest of the entered password does not match the stored value the button „OK“ stays disabled. If no MD5 digest was stored the button „OK“ is always enabled.

4.3 Key – Export

If a key is selected in the left part of the dialog you can export this key into a file. Choose a filename and decide whether you want the key file to be encrypted:



The key is saved as plaintext if no password is entered.

4.4 Key – Delete

The currently selected key can be deleted after a confirmation. Caution: This action cannot be undone! It may be reasonable to delete a key in the database if you want to have your keys only on your iKey.

4.5 Key – Copy (>>>)

You can copy a selected key from the database to an already opened iKey. If there is already a key with the same name on the iKey, this action is rejected. Key names must be unique on the iKey as well as in the key database.

4.6 Password

Here you can change the password of your key database:



4.7 Group – New

Below the root element or another group you can create new groups in order to arrange your keys. The name of a group can only consist of numbers, characters and some special characters. Every name of a group can only be used once in a key database.

4.8 Group – Rename

Unlike key names it is possible to rename groups.

4.9 Group – Delete

If you want to delete a group you can decide whether you also want to delete all sub elements (groups and keys) or to move these elements to the root element.

4.10 iKey – Open

After selecting one of the connected iKeys you can open this iKey by entering the appropriate pin code. Only after opening the keys on the iKey become visible and the button „Open“ becomes „Close“.

4.11 iKey – Close

Because there can only be one open iKey at any time, these open iKey must be closed in order to open another one.

4.12 iKey – Delete

Delete the currently selected key on the open iKey after confirmation request.

4.13 iKey – Copy (<<<<)

Copy the currently selected key from the iKey to the active group or the root element (key database) in the left part of the dialog. This can only be done if there is no other key with the same name in the key database.

4.14 Log file

You can log all basic user actions with the checked „Log file“. In the file „logfile.txt“ you can see for example which keys have been copied to a specific iKey (identified by serial number or name). If this iKey is lost or damaged you can easily create a new iKey with the same content using the information in this log file..

5 Version history

Legend:

- [+] Additional functionality
- [*] Changed functionality
- [-] Bugfix

5.1 Version 1.0 (October 15, 2003)

First release version (only for internal use).

5.2 Version 1.1 (November 05, 2003)

- [+] Detection of iKeys connected/disconnected after program start.
- [-] Deleting last key on iKey now works.

5.3 Version 1.2 (November 18, 2003)

- [+] Distinction between admin and user mode.

5.4 Version 1.3 (July 22, 2004)

- [-] Fixed bug deleting keys from iKey.

6 Contact

For orders, questions, prais, criticism and hints please contact:

CyProtect AG
A company of IT & More GmbH
Schatzbogen 58
D-81829 Munich
Germany
Tel.: +49-(0)89-420447-0
Fax: +49-(0)89-420447-79
E-Mail: info@cyprotect.com
Internet: www.cyprotect.com

