



CKM[®] SecryptM
Version 2.40
User's Guide



Enhancing Security Technologies

© TecSec[®], Incorporated 2007. All rights reserved.

Constructive Key Management and CKM are registered trademarks of TecSec, Incorporated. CKM Enabled, the TecSec logo and the CKM logo are trademarks of TecSec Incorporated. All other names are trademarks of their respective owners.

This product is protected by one or more of the following U.S. patents, as well as pending U.S. patent applications and foreign patents: 5,369,702, 5,369,707, 5,375,169, 5,410,599, 5,432,851, 5,440,290, 5,680,452, 5,787,173, 5,898,781, 6,075,865, 6,229,445, 6,266,417, 6,490,680, 6,542,608, 6,549,623, 6,606,386, 6,608,901, 6,684,330, 6,694,433, 6,754,820, 6,845,453, 7,016,495, 7,069,448, 7,079,653, 7,089,417, 7,095,851, 7,095,852, 7,111,173, 7,131,009, 7,178,030, 7,212,632.

TABLE OF CONTENTS

CKM SECRIPTM	4
CKMTM	4
CKMSECRIPTMSHUTDOWN.....	4
CHGPASS.....	4
CKMSECRIPTMFILER.....	4
CKM_SECRIPTM_GENERATOR	4
CKMSECRIPTMENCRIPTOR.....	4
CKMSECRIPTMLISTER.....	4
SYSTEM REQUIREMENTS	5
TECHNICAL SUPPORT	5
READER'S KEY	6
CKM-SPECIFIC TERMS	6
SPECIAL NOTES.....	8
CKMTM	9
COMMAND OPTIONS	9
CKMSECRIPTMSHUTDOWN	11
CHGPASS	12
COMMAND OPTIONS	12
CKMSECRIPTMFILER	14
COMMAND OPTIONS	14
TEMPLATE SPECIFICATION	15
CKM_SECRIPTM_GENERATOR	17
COMMAND USAGE	18
CKMSECRIPTMENCRIPTOR	19
COMMAND OPTIONS	19
CKMSECRIPTMLISTER	20
COMMAND USAGE	20
TSREGISTER	21
COMMAND USAGE	21
SAMPLE DEPLOYMENT	22

CKM SecryptM

CKM SecryptM is a product and its associated applications that provides for the mandatory encryption of files. It does this in a manner that is invisible to the user. To accomplish this, the IT Administrators have to configure the environment for each user. The following applications are included in the CKM SecryptM product to allow for this administration.

CKMtm

This command line utility is used to configure the CKM Applications and user Tokens for use in the CKM SecryptM system.

CKMSecryptMShutdown

This utility is used to cleanly shut down the CKM SecryptM system just before un-installation.

Chgpass

This command line utility is used to change the password on a CKM User Token.

CKMSecryptMFiler

This command line utility is used to unconditionally encrypt or decrypt data in a manner that is compatible to CKM SecryptM, but is not restricted to the CKM SecryptM configuration.

CKM_SecryptM_Generator

This command line utility is used in the configuration of CKM SecryptM.

CKMSecryptMEncryptor

This command line utility is used to scan one or more directories and will apply the CKM SecryptM configuration to encrypt the files.

CKMSecryptMLister

This command line utility is used to audit a directory structure to see what files exist, and whether or not the files are encrypted, decrypted, or excluded.

System Requirements

You must be an administrator on your machine to install CKM SecryptM.

- Pentium II or higher microprocessor (or equivalent)
- 20 MB of free disk
- 128 MB of RAM
- Operating Systems:
 - Microsoft® Windows XP Professional
 - Microsoft® Windows XP Professional with Service Pack (SP) 1
 - Microsoft® Windows® 2000 Professional with SP2+, or
 - Microsoft® Windows® 2000 Server with SP 2+, or
 - Microsoft® Windows 2000® Advanced Server with SP 2+,
- Microsoft® Internet Explorer 5.00+



Reference: For specific hardware requirements, please see Microsoft's requirements for each operating system.



Very Important: The software and hardware elements included in this list have been tested for compatibility with the CKM System by Quality Assurance professionals at TecSec. Newer versions, service releases or other upgrades of these elements that do not appear on this list may also be compatible with the system, but have not yet been tested for that purpose.

Technical Support

If you need immediate assistance while using *CKM Desktop*, contact Technical Support at support@tecsec.com or call 703-506-9069 and select option 2 from the main greeting.

Reader's Key

CKM-Specific Terms

Algorithm – A formalized set of rules for carrying out a computation or solving a problem in a finite number of steps. A cryptographic Algorithm is a method for transforming information, so that is not readable until it is decrypted.

Please see the topic entitled **Error! Reference source not found.** for a description of the Algorithms supplied with CKM Desktop.

Category – A logical groupings of Credentials. Categories are not associated with any cryptographic values.

CKM Desktop – A collection of software components required if using CKM technology. CKM Desktop is installed with all CKM administration and desktop products.

Constructive Key Management (CKM) – CKM is TecSec's standards-based and patented cryptographic key management technology. It provides secure knowledge management and access management based on rules and roles enforced through cryptography.

Credential – A Credential is one of many items in a Category. Behind the scenes, each Credential is associated with a cryptographic value. Access to information is limited by giving certain Members certain Credentials.

Decryption – The process of turning encrypted text (cipher text) into readable information (plaintext).

Digital Certificate - Contains a public key and identifying information (i.e. a subject, an issuer, and usage information). Each Certificate is used to identify a single user or entity. The owner of a Certificate will also hold the private key associated with the Certificate's public key.

The most common use of a Digital Certificate is to verify that data sent in a message has not been altered, and to provide the receiver with the means to encode a reply. Certificates can also be used for non-repudiation. The standard Certificate format used by Windows 2000 Certificate-based processes is X.509v3. CKM supports X.509v3 Certificates.

Digital Signature - A digital code that can be attached to an electronic file and uniquely identifies the sender. Digital Signatures provide Authentication and Non-Repudiation.

Domain – A group of objects and entities that are administered as a whole with common rules and procedures. Domains are established using TecSec's large-scale administrative tool, *CKM Enterprise Builder*.

Encryption - The process of turning readable information also referred to as clear text or plaintext, into unreadable information, also referred to as cipher text.

Enterprise – An Enterprise is an organization containing at least one Domain, at least one Organizational Unit, and with at least one Member. A secure Enterprise is established using *CKM Enterprise Builder*, TecSec's large-scale administration tool.

Organizational Unit (OU) - Organizational Units are groupings of Members with common attributes.

Read Access – The ability to decrypt, but not encrypt protected information.

Read-and-Write Access – The ability to both encrypt and decrypt protected information.

Roles - In the CKM System, Members are assigned to roles. These roles can be created to reflect existing roles within an organization. Each role is associated with specific Credentials and other enterprise information.

Skins – Skins allow you to change the appearance of your application window using different pre-set themes.

Token – A storage device for a Member's Credentials and Certificates. You receive your Token (as well as the Password for your Token) from your Administrator.

Token Provider – The entity that issues your Token.

Write Access - The ability to encrypt, but not decrypt protected information.

Special Notes



Please Note: Indicates that a certain action must be carried out in order to perform an operation correctly. This may also indicate an important fact that should be taken into consideration while performing an operation.



Example: Contains a demonstration of how an operation should be performed.



Very Important: Warns that a certain action or missing information could cause the application or your computer to perform poorly.



Tip: Contains helpful hints, shortcuts or alternate ways of performing an operation.



Reference: Indicates that further information may be found in another section.

CKMtm

This command line utility allows the user to register Tokens and associate a token to a CKM Enabled Application like CKM SecryptM. This utility is part of the core CKM System.

The CKM System uses the concept of CKM Enabled Applications to specify which token to use when that application is running. If an application uses the CKM System and does not have an associated token, the CKM System will look at the special application called "Default" and use the associated token if it has been specified.

Command Options

The following table describes the command line options for CKMtm.

Option	Description
-H	Present command line option help
--help	Present command line option help
-L	Display a list of the registered tokens
-A "Path and filename"	Add a soft token. This command is used to register the path and file name of a soft token. Once a soft token is registered, it can then be used by CKM SecryptM
-E "App name"	Adds the name of a CKM Enabled Application to the system. You must be a local administrator to use this command.
-R "TecSec Soft Token" xx	Removes the registration of a soft token from the system. This command removes the registration but does NOT delete the actual token. Once the registration information for a soft token has been removed, the system no longer can use the token. The first parameter is the name of the token provider. For CKM SecryptM it will be "TecSec Soft Token". The second parameter is the slot number of the token to unregister. This slot number is visible in the -L list, and was displayed when the token was registered.
-S "App Name" "TecSec Soft Token" xx	This command is used to tell the system to use a specific token whenever the specified CKM Enabled Application uses the CKM System. The first parameter is the name of the CKM Enabled application, or "Default". The second parameter is the name of the token provider. For CKM SecryptM it will be "TecSec Soft Token". The third parameter is the slot number of the token to unregister. This slot number is visible in

	the –L list, and was displayed when the token was registered.
-U “App name”	This option is used to remove any token association from the CKM Enabled application that is specified.
-P	This option displays a list of the CKM Enabled Applications.
-C “TecSec Soft Token” xx	<p>This option is used to interactively change the password for the specified token. The system will prompt the user for the current password, the new password, and a confirmation of the new password. If all of these are entered correctly, the password for the indicated token will be changed.</p> <p>The first parameter is the name of the token provider. For CKM SecryptM it will be “TecSec Soft Token”. The second parameter is the slot number of the token to unregister. This slot number is visible in the –L list, and was displayed when the token was registered.</p>
-I “TecSec Soft Token” xx	<p>This option is used to display the details for the indicated token. The system will prompt the user for the password. If the password is entered correctly, both public and private information will be displayed. Otherwise only public information will be displayed.</p> <p>The first parameter is the name of the token provider. For CKM SecryptM it will be “TecSec Soft Token”. The second parameter is the slot number of the token to unregister. This slot number is visible in the –L list, and was displayed when the token was registered.</p>



Please Note: Command line options are case insensitive.

CKMSecretMShutdown

This utility is used to cleanly shut down the CKM SecryptM system just before un-installation. This command has no parameters and should only be used just before uninstalling the CKM SecryptM program.



Please Note: This application is not included in the installation. It is intended to be used in the deployment system and is provided separately.

Chgpass

This command line utility is used to change the password on a CKM User Token. This application has two modes of operation: Interactive and command line.

In the interactive mode, the token information is provided on the command line and a windows dialog is presented to the user. This dialog will allow the user to change the password.

Both modes of operation use the same set of command line options to control the operation of the application.

Command Options

The following table describes the command line options for Chgpass.

Option	Description
-A "App Name"	This option is used to indicate the CKM Enabled Application that is to be used to specify which token to use. Once the token is specified, the Chgpass application can perform its functionality.
-P "Provider"	This option is used to specify which token provider is used to access the token that is to have a new password. For CKM SecryptM, this option will have the value of "TecSec Soft Token". This option is used with the -S option to fully specify the token to change.
-S xx	This option is used to specify the slot number of the token to change. This option is used with the -P option to fully specify the token to change.
-PASS "password"	This option is used to auto fill in the current token password. This option is normally used in deployment situations where the token is created with a "standard" password and the user is forced to change the password on first use. It is also used in the command line mode to specify the current password of the Token.
-RANDSSO	This option is used to generate a random password for the token and store the random password into a Single Sign On system. The Chgpass application is run in the command line mode when this option is used. This option also requires the use of the -PASS option.



Please Note: Command line options are case insensitive.



Please Note: You will use either the `-A` option OR the `-P` and `-S` options to specify the token to use. If neither set of options are specified, or if an error occurs while attempting to access the Token, an error will be presented and Chgpass will exit.

CKMScryptMFile

This command line utility is used to unconditionally apply the file level encryption to a single file, a single directory of files, or all directories and files from a specified directory.

This application is a standalone application that will use the same encryption techniques that CKM ScryptM uses to allow for the encryption of files can be dynamically changed. Other CKM utilities like CKMfile are used to create encrypted archives of files. CKM ScryptM is used to create protected files that can be dynamically changed.



Please Note: The CKMScryptMFile application does not use the configuration information for the CKM ScryptM product. All configuration information is passed on the command line. This means that you can encrypt files that could make the machine not bootable.

Command Options

The following table describes the command line options for Chgpas.

Option	Description
-SPEC "specification"	This option is used when encrypting data to specify the template that is to be used in the key management.
-APP "App Name"	This option is used to specify the CKM Enabled Application name that is to be used to gain access to the Token. See the CKMtm command for more information on CKM Enabled Applications.
-AS "filespec"	This option is used to specify the filename or file spec (a file name with wild cards of * or ?). All files that match this specification in each directory searched will be processed. This option can be specified more than once to process multiple file specs in all directories processed.
-AF "full path"	This option is used to process a single file. The full path and file name must be specified. The use of wild cards are not allowed on this option.
-AD "full path"	This option is used to specify a single directory that is to be processed. All file specs (from the –AS option) will be searched in the specified directory. The full path to the directory should be specified.
-AR "full path"	This option is used to specify a directory and all of its sub-directories that are to be processed. All file specs (from the –AS option) will be searched in the specified directory and all of its sub-

	directories. The full path to the directory tree should be specified.
-D	This option specifies that decryption is to be performed on all –AF, -AD and –AR options that follow.
-E	This option specifies that encryption is to be performed on all –AF, -AD and –AR options that follow. This option is the default. Also, this option requires the use of the –SPEC option.
-DISPLAY	This option is used to specify that the progress of the application be displayed in a window. When the application is finished, the window will wait until the user presses Enter. If you want to run the application in the background, then do not specify this option.

Template Specification

The specification of the template has the following format:

DomainGuid~xx~AccessGroupList

DomainGuid is the full guid for the domain to use. It shall be formatted as follows:

{999999999-9999-9999-9999-999999999999}

Xx is the number of access groups specified. Each access group is a complete specification of what is needed to acquire the key used in this encryption. The relationship between access groups is OR. This means that you must have all of the information for at least one access group.

AccessGroupList is the list of access groups. Each access group has the following format:

Type~parameters~

Currently, only one type is supported. This type is “cred”. The parameters for cred are a list of credential ids that are separated by commas.

The following spec is an example of the use of a single access group using a single credential:

```
{99999999-9999-9999-9999-9999999999999999}~1~cred~1~
```

The following spec is an example of the use of two access groups. The first group uses one credential. The second group uses two credentials.

```
{99999999-9999-9999-9999-9999999999999999}~2~cred~1~cred~2,4~
```

In this example, the user must have either credential 1 or both credentials 2 and 4 in the indicated domain to access this information.



Please Note: When encrypting information, the user must have all of the credentials specified. When decrypting information, the user only has to have the information for at least one access group.

CKM_ScryptM_Generator

This application is used to specify the template that is to be used for a given path and its sub-directories. The CKM ScryptM application uses the concept of drive types to provide flexibility to the administrators in how they protect data. Currently CKM ScryptM has defined the following drive types:

Drive Type	Description
Boot	The drive that the operating system used to boot up. The boot drive typically has additional requirements that can affect the encryption process. Therefore the boot drive has its own list of parameters. Any directory specifications are relative to the root directory of the boot device/partition.
Fixed	This drive type is any non-removable storage media attached to the computer. It may be a partition of a hard drive, a USB hard drive, or some other non-removable media. Any directory specifications are relative to the root directory of the device/partition.
Removable	This drive type includes all USB thumb drives except for those that are in the TrustedRemovable list. Any directory specifications are relative to the root directory of the device/partition.
TrustedRemovable	This drive type is a subset of Removable list. Currently the thumb drives from MXI Security are in this list as they provide hardware level encryption of the contents. Any directory specifications are relative to the root directory of the device/partition.
Network	All network locations are in this subset. Any directory specifications are relative to the root directory of the device/partition.
CD	This option is currently not implemented. Any directory specifications are relative to the root directory of the device/partition.
Global	This option is not directly mapped to a drive type. It allows for the specification of specific paths (including server for UNC or drive letter for mapped or local drives) as well as global settings. Any directory specifications must be full path including the full UNC or local drive letter.

CKM ScryptM will look for the template to use for the encryption of new files in the following order. The first successful match defines the template to use.

- The specific paths in Global are searched first. If any specific path in global matches the path in question, or is a parent to the path in question, then the template associated to the specific path is used.
- The drive type of the path in question is then determined. If the relative path of the path in question is specified in the list of paths for that drive type, or is a child of any of the paths in that drive type, then the associated template is used.
- Lastly, the global default template is used.

CKM_ScryptM_Generator is a command line program that has the following usage.

Command Usage

The following table describes the command line parameters for CKM_ScryptM_Generator.

CKM_ScryptM_Generator	DriveType	Path	Template
-----------------------	-----------	------	----------

DriveType is one of the items from the above table. This parameter must match one of the items in the table.

Path is the relative or full path of with the drive type. The drive type table specifies if full or relative path is required. If an empty parameter is specified (by using ""), then the specification is the default for that drive type. This means that if no specific path in the drive type matches, then the default will be used.

Template is the specification of the encryption template. This is defined above in Template Specification. If the specification is the empty parameter (by using ""), then the specified path and its sub-directories shall not be encrypted.

CKMScryptMEcryptor

This application is used to encrypt data that either existed either before CKM ScryptM was installed or before the latest set of changes to the configuration.

This application was designed to run in the background. It does however have the option to display the progress of its operation. It is also a batch processing application. Each time the user logs into the machine, this program is automatically started with the -RUN option. It then checks to see if there are any unprocessed batches and if so it processes them. By default this application is used to specify the batches that will be run on the next login.

Here is the list of the command options for this application:

Command Options

The following table describes the command line options for CKMScryptMEcryptor.

Option	Description
-AF "filename"	This option specifies that the specified file is to be processed. The processing will be either encrypt or decrypt based on the prior use of the -E or -D options.
-AD "path"	This option specifies that the specified directory is to be processed. The processing will be either encrypt or decrypt based on the prior use of the -E or -D options.
-AR "path"	This option specifies that the specified directory and all of its sub-directories are to be processed. The processing will be either encrypt or decrypt based on the prior use of the -E or -D options.
-D	Decrypt the files specified by the options that follow this option on the command line.
-E	Encrypt the files specified by the options that follow this option on the command line. This is the default option.
-RUN	Run all existing batches plus the batch specified on this command line immediately.
-DISPLAY	Display the progress of the batch processing. This option internally also forces the -RUN option.

CKMSEcryptMLister

This application is used to create a file listing that indicates the file name, and the encryption status of the file. The file status is one of the following:

Status	Description
Yes	The file is encrypted
No	The file is not encrypted
Excluded	The file is not encrypted and has been specifically excluded from encryption.

This application is a command line application with the following usage:

Command Usage

The following table describes the command line parameters for CKMSEcryptMLister.

CKMSEcryptMLister Path OutputFile

Path is the full path specification for the directory (and its sub-directories) that is to be scanned.

OutputFile is the full path and file name of the file that is to contain the results of the file scan.



Please Note: The path does not and cannot point to a file. It also cannot have any wildcards.

TSRegister

This application is used to register this installation to the corporation that purchased the license.



Please Note: The serial number and install code SHALL be kept confidential to that corporation. Any disclosure of the serial number or install code to people other than employees of the corporation and their affiliates (if allowed in the End User License Agreement), or TecSec shall be a violation of the TecSec End User License Agreement.

Command Usage

The following table describes the command line parameters for TSRegister.

TSRegister SerialNumber,InstallCode

The serial number and install code are issued by TecSec to each corporation or agency that purchases our products.

Sample Deployment

For this sample deployment, we are making the following assumptions:

- The user profiles (the information in Documents and Settings) is on the boot drive.
- The boot drive is C:
- Tokens have been created and are located on \\TokenServ\Tokens
- Each user has a Token.
- Each Token was built using a default password of 1111.
- Only the files in “Documents and Settings” are to be encrypted.
- SMS will be used to push packages that contain a batch file and the associated documents
- The path to the package shall either be mapped as a user drive letter, or be copied to the user’s computer before being applied.
- Only one CKM Token has or will be registered on the user’s computer for each user of the computer.
- Each user must have their own token registered before they can access the encrypted files.
- The user does not need to know or remember the password to their token
- IT can replace the user token if needed.



Please Note: These assumptions and the resulting scripts are for example purpose only. They shall not be used to dictate the proper use of the system. They are simplified for illustration, and are therefore not enforcing the proper security that should be enforced in a live deployment.

The following script could be used to install or upgrade the CKM SecryptM application. It shall be run with local admin rights.

```
----- BEGIN UPGRADE.BAT -----  
  
@echo off  
  
rem  
rem Preparing to uninstall the system.  
  
CKMSecryptMShutdown.exe  
  
echo Removing any prior versions of CKM SecryptM  
start /wait msixexec /x {F7C17873-ED3D-4DEA-BAA0-BA92DD65A7BD} /qn
```

22

```

echo Installing CKM SecryptM
start /wait msisexec /i "TecSec-CKMSecryptM_v2.40.msi" /log "%SystemDrive%\install.log" /qn

rem
rem This command is used to register the serial number and install code for the corporation.
rem
"c:\Program Files\TecSec\CKM\TSRegister" xxxxxxxx, yyyyyyyyyy

rem import additional exclusions into the registry
reg import CKMex.reg

if errorlevel 1 goto BadInstall

echo Establishing the working parameters
rem Now make sure that the windows\system32 folder is not encrypted
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Global "\SystemRoot" ""

rem The TecSec logs also should not be encrypted.
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Global "%SystemDrive%\TecSec\Logs" ""

rem In order to uninstall the product, this directory must not be encrypted.
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Global "%SystemDrive%\Config.Msi" ""

rem
rem And set up the default encryption for all drives and UNC paths
rem

rem Specify that all files on non-boot fixed drives shall be encrypted
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Fixed "" {99999999-9999-9999-9999-999999999999}~1~cred~1~

rem By default, the boot drive is not encrypted
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Boot "" ""

rem but documents and settings is to be encrypted
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Boot "\Documents and Settings" {99999999-9999-9999-9999-999999999999}~1~cred~1~

rem Network drives are not to be encrypted in this sample
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Network "" ""

rem Removable drives are to be fully encrypted
"%programfiles%\tecsec\ckm\ckm_secryptm_generator" Removable "" {99999999-9999-9999-9999-999999999999}~1~cred~1~

rem Register the service as we are now ready to start
"%programfiles%\tecsec\ckm\ckmsecryptmservice" -Service

rem And start the service
net start ckmscryptmservice

```

----- END UPGRADE.BAT -----

Now that the CKM SecryptM product is installed and configured, the computer should be rebooted.

The second step is to configure the user as they log in so that they have the Token and the Token is registered for use by the system.

This batch file shall be configured to run as the user logs in and does not require any elevated rights.

----- BEGIN USERCONFIG.BAT -----

```

Rem
rem Remove any pre-existing token registration
rem
"%programfiles%\tecsec\ckm\ckmtm" -u Default > NUL 2<&1

```

```
"%programfiles%\tecsec\ckm\ckmtm" -u "CKM Secure" > NUL 2<&1
"%programfiles%\tecsec\ckm\ckmtm" -u "CKM SecryptM" > NUL 2<&1
"%programfiles%\tecsec\ckm\ckmtm" -r "TecSec Soft Token" 0 > NUL 2<&1
rem
rem The token has been unlinked, so get it and register it now.

md "%USERPROFILE%\Tokens" > NUL 2<&1
del "%USERPROFILE%\Tokens\%username%.tok" > NUL 2<&1
copy \\TokenServ\Tokens\%username%.tok "%USERPROFILE%\Tokens"

"%programfiles%\tecsec\ckm\ckmtm" -a "%USERPROFILE%\Tokens\%username%.tok"
"%programfiles%\tecsec\ckm\ckmtm" -s Default "TecSec Soft Token" 0

rem And change the password, which also allows for the setting of SSO
"%programfiles%\tecsec\ckm\chgpass" -a Default -pass 1111 -randss0
----- END USERCONFIG.BAT -----
```