# e-SPA

# User's Guide

Procedures for Electronic submittal
of Medicaid State Plan Amendments
using CKMfile

**Use CKMfile to:**
**Encrypt and electronically sign**
**Encrypt**
**Decrypt**
**Securely Delete**

October 3, 2002

Version 2.0

# Table of Contents

# Introduction

SPA submittal has historically involved mail or courier transmission of a hard-copy SPA document from the State to the HCFA/CMS Regional Office. Problems with the traditional process include the delays associated with mailing this time-sensitive material, as well as a limited ability to share SPA contents during the review. This process has endured in large part because of the absence of a secure method to transmit a SPA, and to convey a State official's legal signature on the form 179 cover sheet. We believe that alternative solutions to these barriers are now available, and we are now able to make available an electronic process.

This electronic process is not intended to change the basic legal requirements for SPA submittals, requests for additional information (RAIs) and SPA approvals. This process is intended to provide an alternative means of transferring the needed materials in a quick and secure manner to support the SPA process.

While this process offers the advantages of prompt transmission of time-sensitive SPA materials, it also implies a responsibility for both State and Federal parties to monitor their E-mail resources for receipt of SPA documents.

Prior to using this process, the required software and authorization must be obtained. The software used to encrypt and digitally sign, encrypt without digital signature, decrypt and securely delete files is the *CKMfile* software licensed by TecSec, Inc. This software is provided by CMS for use in the Electronic SPA (e-SPA) transmittal process. To request additional information about the e-SPA process; send an E-mail to ESPACO@cms.hhs.gov.

# Getting Started

*CKMfile* is a utility that is part of the *Constructive Key Management*® (*CKM*®) System. *CKMfile* is used for file encryption and decryption, electronically signing files, verifying and securely deleting one or more files. To use *CKMfile*, you must obtain the *CKM*® *Desktop Suite* and a Token from your administrator. You must register the Token using *CKM*® *Tokens* and be enrolled in a Domain.

*CKM*® *Desktop Suite* is the core of the CKM System and is comprised of a collection of software components that are required to utilize the CKM technology.

*A CKM Token* is a storage device for a member's Credentials and Certificates. You will receive your Token (as well as the Password for your Token) from a CMS Central Office e-SPA Administrator.

After the installation of the *CKM*® *Desktop Suite* and registration of your token, the functions of *CKMfile*, as related to the e-SPA process, are described in this document.

***Please note***: Refer to the **e-SPA Installation Guide** for instructions on the installation of the above required software.

## *Accessing CKMfile*

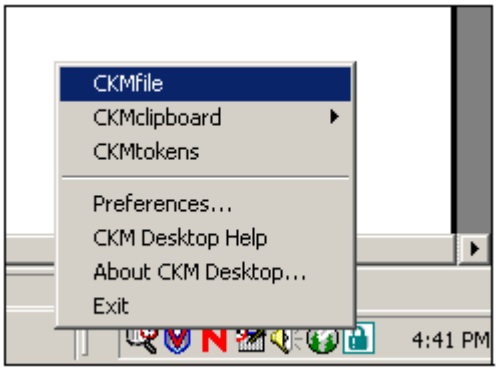
There are two methods in which to access *CKMfile*.

Accessing *CKMfile* from the ***Start Menu***

1. Select **Start** from your desktop.
2. Select **Programs** menu from the **Start** menu.
3. Select **TecSec** from the **Programs** menu.
4. Select the **CKMfile** command on the **TecSec** menu. This will launch *CKMfile*.

Accessing *CKMfile* from the ***CKM Desktop Icon***

1. Select or click the CKM Desktop tray icon.
2. Select *CKMfile* from the resulting menu. This will launch *CKMfile*.



## *CKMfile Toolbar*

After you start *CKMfile*, the *CKMfile* toolbar is displayed.


## *CKMfile Toolbar Buttons*

Each button on the *CKMfile* toolbar allows you to perform a different function.

***Please Note:*** For the purpose of the electronic SPA transmittals with the form 179, you will use the *Encrypt and Digitally sign files* (3rd button) and *Decrypt/Verify files* (4th button) options. Therefore, this User's Guide will give instructions on those options first. For other correspondence and RAI exchange you may or may not elect to use the *Encrypt file(s)* without a digital signature option (1st button).

**Encrypt file(s)** button – Allows you to encrypt one or more files.

**Digitally sign file(s)** – Allows you to electronically sign one or more files.

**Encrypt and digitally sign file(s)** – Allow you to encrypt and electronically sign one or more files.

**Decrypt/Verify file(s)** – Allows you to decrypt and/or verify one or more files.

**Securely delete file(s)** – Allows you to securely delete one or more files.

# Completing form 179 for Electronic Signature

Complete all sections of the form 179 as you normally would.

In the signature block enter: //Your Name - signature// For example: //Jane Smith - signature//

An example of a State Agency Official signature (block 12):

| | |
|---|---|
| ☐ NO REPLY RECEIVED WITHIN 45 DAYS OF SUBMITTAL | |
| 12. SIGNATURE OF STATE AGENCY OFFICIAL:<br>// Jane Smith – signature // | 16. RETU |
| 13. TYPED NAME: | |
| 14. TITLE: | |
| 15. DATE SUBMITTED: | |
| **FOR REGIONAL OFFICE USE** | |
| 17. DATE RECEIVED: | 18. DATE |

An example of a Regional Official signature (block 20):

| | |
|---|---|
| | |
| **FOR REGIONAL OFFICE USE ONLY** | |
| | 18. DATE APPROVED: |
| PLAN APPROVED – ONE COPY ATTACHED | |
| ATERIAL: | 20. SIGNATURE OF REGIONAL OFFICIAL:<br>// John Smith – signature // |
| | 22. TITLE: |
| | |

# Encrypting and Digitally Signing Files

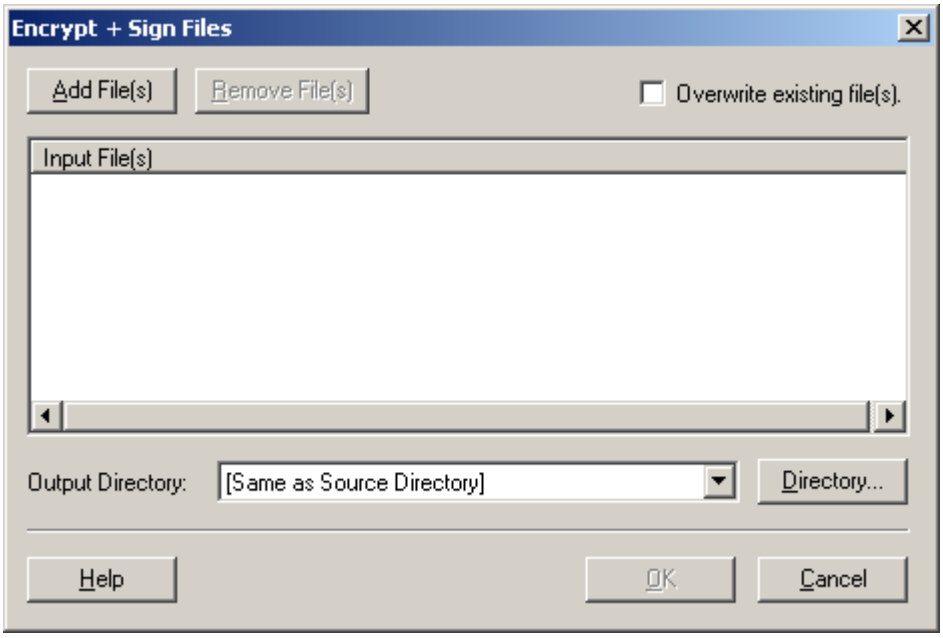
**For the purpose of the electronic SPA transmittals with form 179, you will use the *Encrypt and Digitally sign files* and *Decrypt/Verify files* options. Therefore, this User's Guide will give instructions on those options first.**

*CKMfile* allows you to encrypt AND digitally sign one or more files at a time. To do so, use the following steps:

1. Select the **Encrypt and digitally sign file(s)** button located on the *CKMfile* toolbar. This is the third button from the left.

This will bring up the **Encrypt + Sign Files** window. From this window, you will be able to select one or more files to be encrypted and digitally signed.

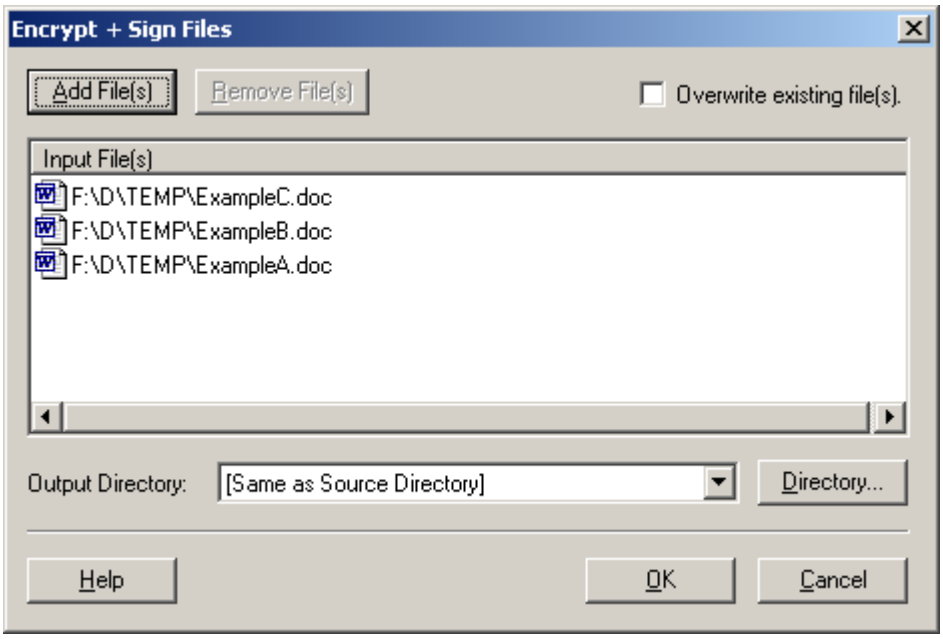
***Important:*** All files to be transmitted for a SPA (i.e., form 179 cover sheet and all related SPA files) should be selected for encryption and digital signature.




2. Select the **Add Files(s)** button located on the **Encrypt + Sign Files** window and navigate to the location of the file(s) to be encrypted and digitally signed.

3. The file(s) you selected to be encrypted and digitally signed will be listed in the **Encrypt + Sign Files** window under *Input File(s)*. The location of the encrypted and digitally signed file(s) will default to the drive and/or directory of the original unencrypted file(s) as illustrated in the *Output Directory* area as "Same as Source Directory". The filename(s) of the encrypted and digitally signed file(s) will have a new extension of .ckm added to the end of the original filename(s).

   ***Please note:*** You may change the *Output Directory* location by selecting the **Directory…** button next to *Output Directory.*



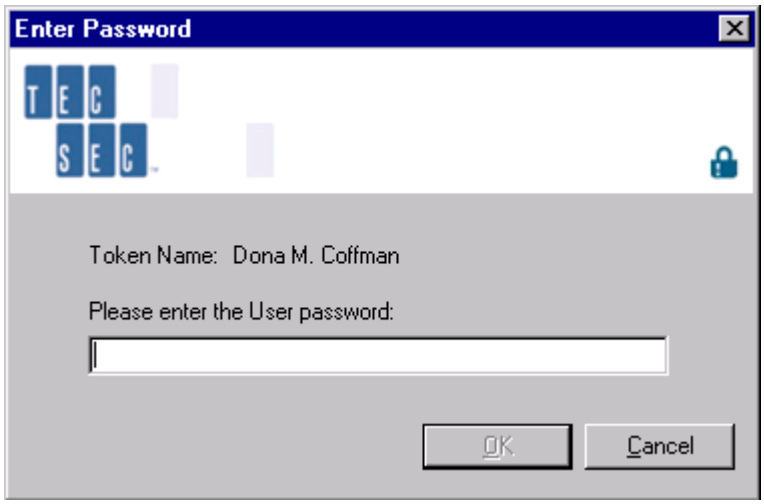

   ***Tip:*** If you decide not to encrypt and sign any of the file(s) listed in the **Encrypt + Sign Files** window, you may select the file(s) and select the **Remove File(s)** button. This will remove the file(s) from the **Encrypt + Sign Files** window and the file(s) will not be encrypted nor signed.

   ***Please Note:*** If there is a filename conflict, the filename(s) will be shown in RED and you will not be able to encrypt and sign any of the files listed. This usually occurs when the file already exists as an encrypted or encrypted and signed file (i.e., the same file name already exists with a .ckm extension). To continue you may 1) change the drive and/or directory of the output; 2) remove the file(s) from the list of files to encrypt and sign; or 3) click on *Overwrite existing file(s).*

4. Select the **OK** button on the **Encrypt + Sign Files** window to encrypt and digitally sign the selected file(s).

5. You will be prompted to enter the Password for your Token. On the **Enter Password** window, enter your Password and select the **OK** button. This is the Password from your CMS Administrator.

   ***VERY IMPORTANT:*** Your Password is case sensitive.

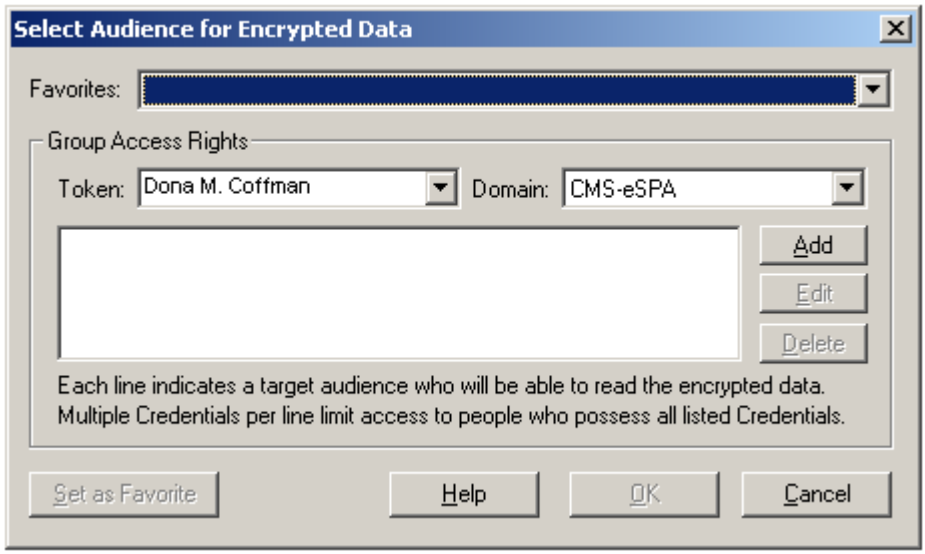



   ***Important*:** Once you have entered your Token Password AND "Encrypted and Sign", "Decrypt", "Encrypt" or "Delete" file(s), you do not need to re-enter your password again as long as *CKMfile* stays open. However, *CKMfile* and your Credentials are not secure if you leave your desk. It is recommended that you close *CKMfile* when not in use.

   ***Important:*** PASSWORDS CANNOT BE RESET. If you change your password and then cannot remember what you changed it to, a new token will have to be issued to you. The re-issuance of tokens will take 2-3 working days.

   ***Please note:*** You will be prompted to log in for most operations performed with *CKMfile*.

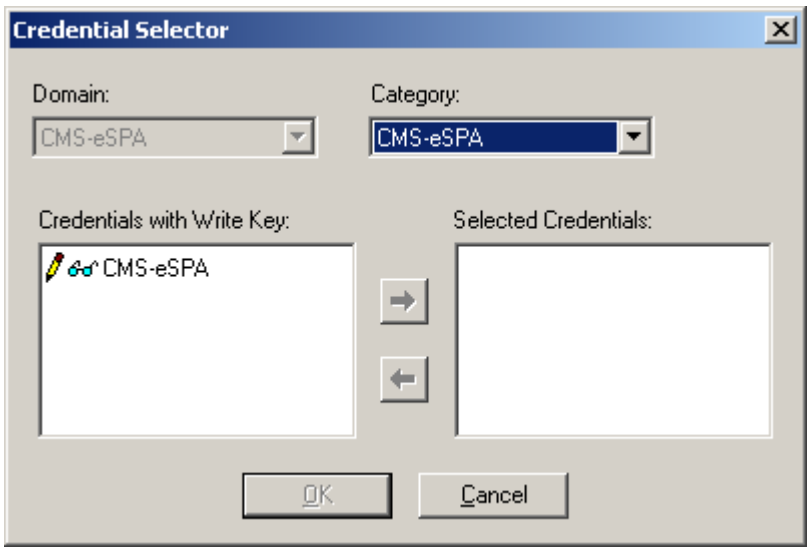
6. The **Select Audience for Encrypted Data** window will now appear allowing you to indicate the desired settings for encrypting and digitally signing your file(s).




7. On the **Select Audience for Encrypted Data** window, ensure that the **Token** is set to *YOUR NAME* (i.e., the name of the person who the software is registered to) and the **Domain** is set to *CMS-eSPA* under the **Group Access Rights** area. If they are not, use the drop-down arrow to select them.

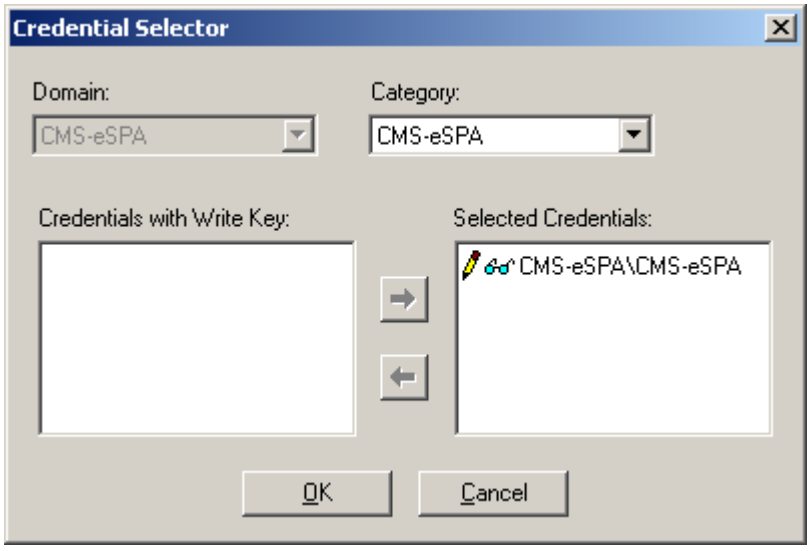
8. To select the Credentials for your target audience, select the **Add** button in the **Group Access Rights** area. The **Credentials Selector** window is displayed.

9. On the **Credential Selector** window, ensure that the Category is set to *CMS-eSPA*. If it is not, use the drop-down arrow to select it. All of the Credentials in the Selected Category are displayed in the **Credential with Write Key:** box.

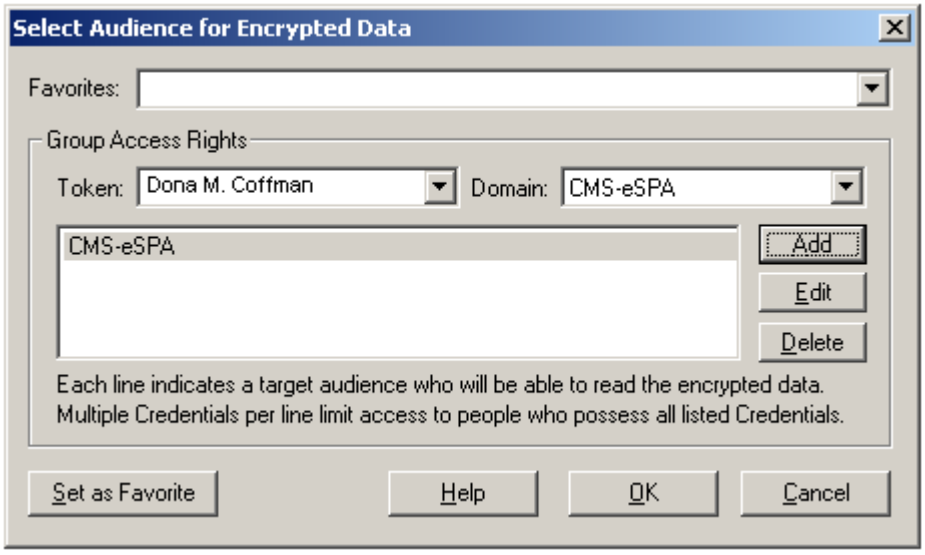



10. Select the **CMS-eSPA** Credential from the **Credential with Write Key:** box.

    Use the  arrow button to move the Credentials to the **Selected Credentials** box.



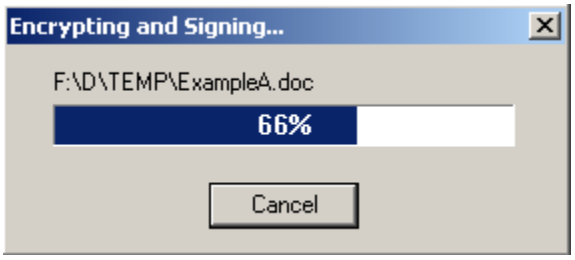
11. When you have finished making your selection, select the **OK** button. This takes you back to the **Select Audience for Encrypted Data** window, which displays the Credentials you selected. See example below.



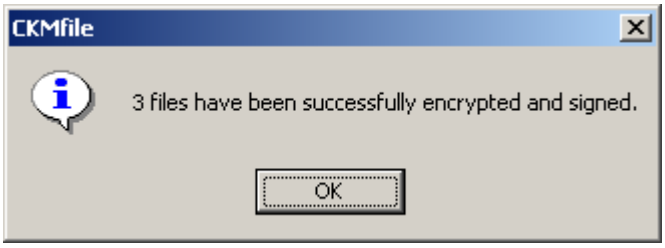

***Tip:*** To save time, you may set up a *Favorite* that will allow you to pre-define the audience for future encryption operations. Favorites will save the *Token*, *Domain* and *Credentials for your target audience* (steps 7, 8, 9, 10 and 11 above). See the section on Creating Favorites.

12. Once all your selections on the **Select Audience for Encrypted Data** window have been completed, select the **OK** button.

13. A progress dialog window will be displayed (as shown below) during the encryption and digital signing process.



14. Once your files have been successfully encrypted and digitally signed, a message box will be displayed on your screen. Select **OK** to continue.




15. The file(s) are now ready to be E-mailed to the appropriate person(s).

16. Using GroupWise (CMS) or other Internet E-mail software, locate the encrypted and digitally signed file(s) [they will have a .ckm extension] and attach them to the E-mail. Send the file(s) to the pre-defined Federal or State E-mail destination (see below). The Federal E-mail boxes established for SPA receipt will automatically send a response acknowledging receipt of the SPA package.

    ***Very Important:*** During testing of the e-SPA process it was discovered that sometimes if there is no text entered into the body/message area of the E-mail, the attached .ckm file(s) was pulled into the body/message area of the E-mail. Therefore, please enter text into the body/message area of the E-mail. Sample text: "*Attached is SPA XX-XXX cover letter, form 179 and amended pages.*" or "*Attached is our response to your request for additional information relating to SPA XX-XXX.*"

    **Federal E-mail destinations**:
    Effective July 1, 2002, all IR-SPAs should be submitted directly to the National Institutional Reimbursement Team (NIRT) at NIRT@cms.hhs.gov and the appropriate CMS Regional Office e-SPA E-mail address.

    Non-Institutional Reimbursement SPAs should be submitted to the CMS Regional Office e-SPA E-mail address. These addresses are as follow:

| | |
|---|---|
| Region 1 | ESPA1@cms.hhs.gov |
| Region 2 | ESPA2@cms.hhs.gov |
| Region 3 | ESPA3@cms.hhs.gov |
| Region 4 | ESPA4@cms.hhs.gov |
| Region 5 | ESPA5@cms.hhs.gov |
| Region 6 | ESPA6@cms.hhs.gov |
| Region 7 | ESPA7@cms.hhs.gov |
| Region 8 | ESPA8@cms.hhs.gov |
| Region 9 | ESPA9@cms.hhs.gov |
| Region 10 | ESPA10@cms.hhs.gov |

    **E-SPA Technical Assistance:**
    An ESPA E-mail address has been established to provide technical assistance and answer technical questions (ESPAtech@cms.hhs.gov). This E-mail address is not intended to answer program or policy questions.

    ***Please note:*** For CMS users, GroupWise does NOT provide for a permanent storage of the transferred document. A separate directory or storage medium must be established for the storage and/or archiving of these documents.

# Decrypting and/or Verifying Files

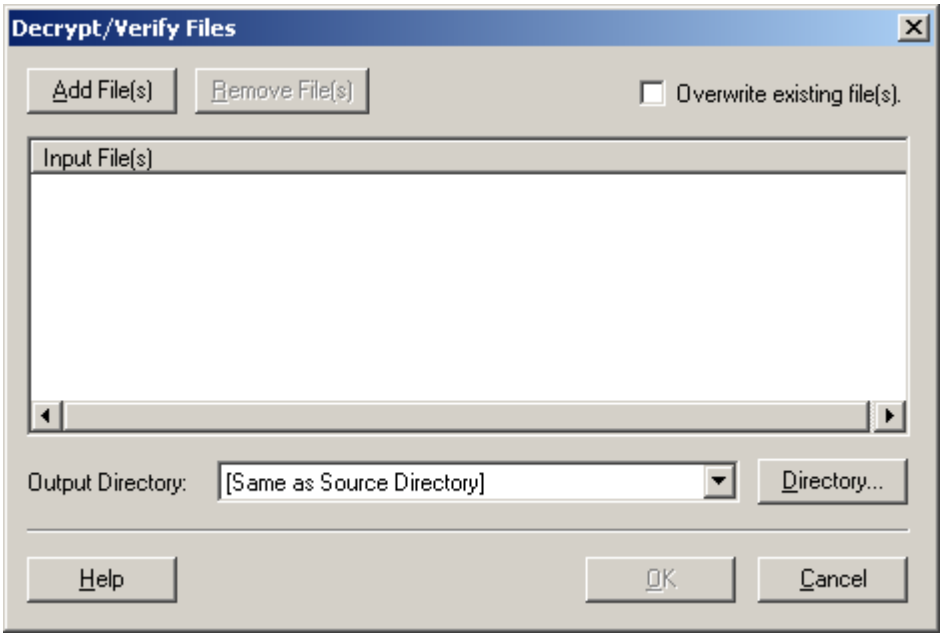
**For the purpose of the electronic SPA transmittals with form 179, you will use the *Encrypt and Digitally sign files* and *Decrypt/Verify files* options. Therefore, this User's Guide will give instructions on those options first.**

*CKMfile* allows you to decrypt and/or verify one or more files at a time. To do so, use the following steps:

***Please note:*** Ensure that the file(s) to be decrypted and/or verified has been saved to your PC. You CAN NOT decrypt/verify an encrypted file(s) directly from your E-mail.

1. Select the **Decrypt/Verify file(s)** button located on the *CKMfile* toolbar. This is the fourth button from the left.

This will bring up the **Decrypt/Verify Files** window. From this window, you will be able to select one or more files to be decrypted and/or verified.

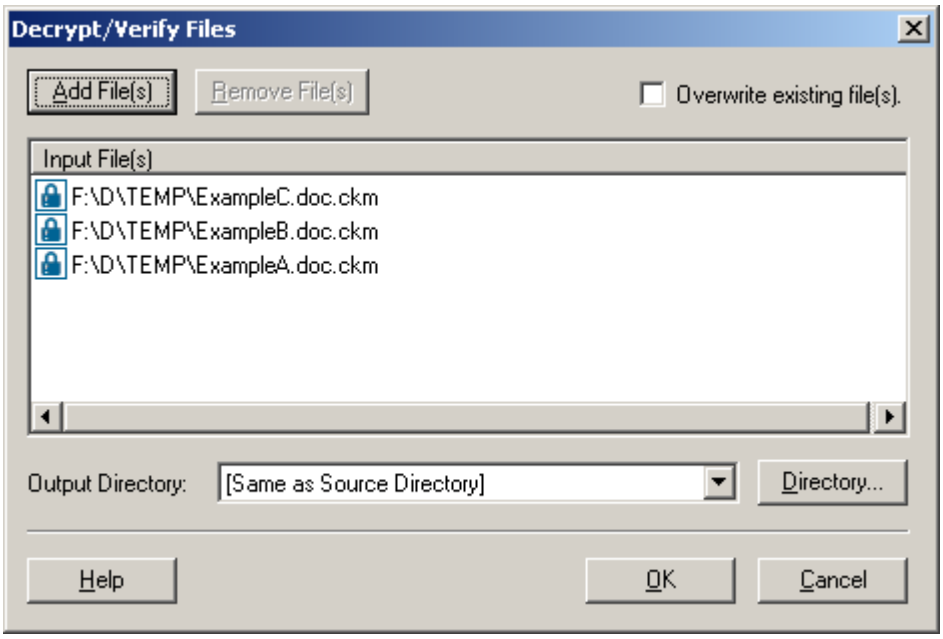



2. Select the **Add File(s)** button located on the **Decrypt/Verify Files** window and navigate to the location of the file(s) to be decrypted and/or verified. The file(s) to be decrypted and/or verified will have the .ckm extension and an icon that looks like a pad-lock.

   ***Important:*** File(s) must be saved on your PC. The file(s) CAN NOT be decrypted/verified from your E-mail.

3. The file(s) you selected to be decrypted and/or verified will be listed in the **Decrypt/Verify Files** window under *Input File(s)*. The location of the decrypted and/or verified file(s) will default to the drive and/or directory of the original encrypted and digitally signed file(s) as illustrated in the *Output Directory:* area as "Same as Source Directory". The filename(s) of the decrypted and/or verified file(s) will be the same as the encrypted and digitally signed filename(s) but without the .ckm extension.

   ***Please note:*** You may change the *Output Directory* location by selecting the **Directory…** button next to *Output Directory.*



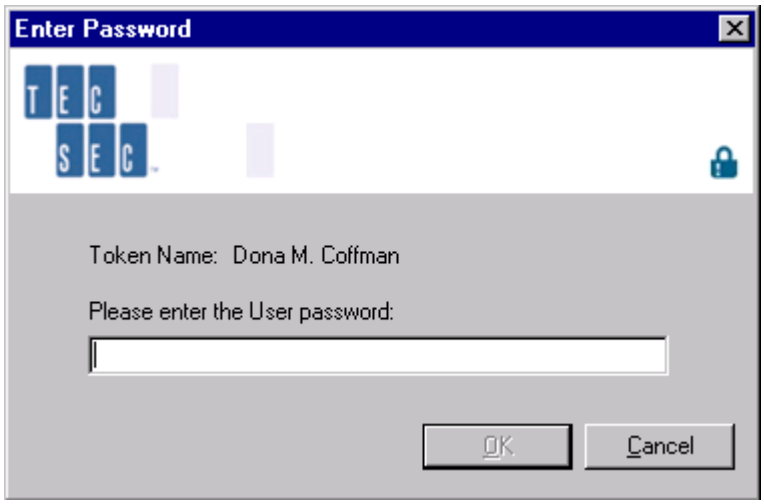

   ***Tip:*** If you decide not to decrypt and/or verify any of the file(s) listed in the **Decrypt/Verify Files** window, you may select the file(s) and select the **Remove File(s)** button. This will remove the file(s) from the **Decrypt/Verify Files** window and the file(s) will not be decrypted nor verified.

   ***Please Note:*** If there is a filename conflict, the filename(s) will be shown in RED and you will not be able to decrypt and and/or verify any of the files listed. This usually occurs when the file already exists as a decrypted and/or verified file (i.e., the same file name already exists without the .ckm extension). To continue you may 1) change the drive and/or directory of the output; 2) remove the file(s) from the list of files to decrypt and/or verify; or 3) click *Overwrite existing file(s)*.

4. Select the **OK** button on the **Decrypt/Verify Files** window to decrypt and/or verify the selected file(s).

5. You will be prompted to enter the Password for your Token. On the **Enter Password** window, enter your Password and select the **OK** button. This is the Password from your CMS Administrator.

   ***VERY IMPORTANT:*** Your Password is case sensitive.

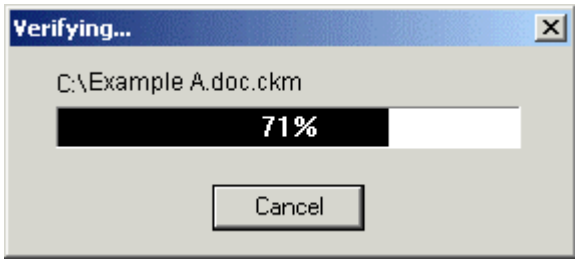



   ***Very Important:*** Once you have entered your Token Password AND "Encrypted and Sign", "Decrypt", "Encrypt" or "Delete" file(s), you do not need to re-enter your password again as long as *CKMfile* stays open. However, *CKMfile* and your Credentials are not secure if you leave your desk. It is recommended that you close *CKMfile* when not in use.

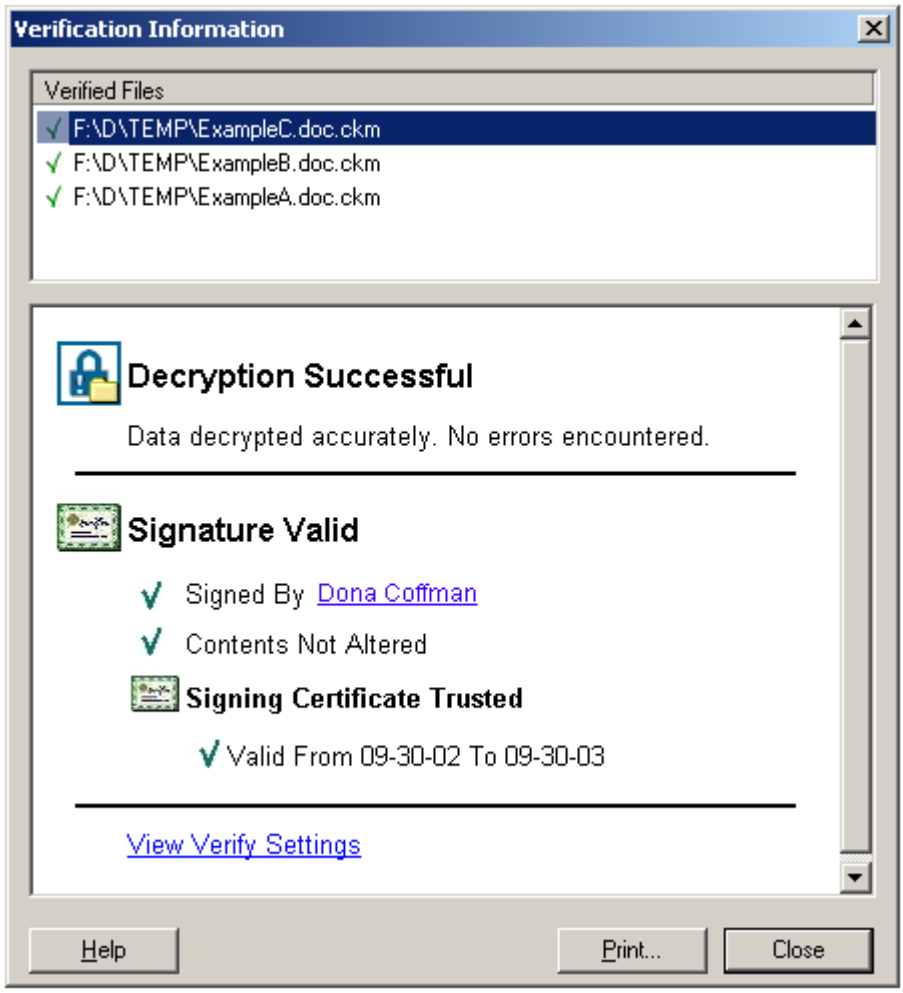
   ***Important:*** PASSWORDS CANNOT BE RESET. If you change your password and then cannot remember what you changed it to, a new token will have to be issued to you. The re-issuance of tokens will take 2-3 working days.

   ***Please note:*** You will be prompted to log in for most operations performed with *CKMfile*.

6. A progress dialog will be displayed during the verification and decryption process.



7. After your file(s) have been successfully decrypted and/or verified, a message box will be displayed on your screen. This screen informs you what files were verified, whether the decryption was successful or not, who digitally signed the document, and whether the signature is valid or not. If the signature is not valid, the reason why it is not valid is displayed on the screen.




***Note:*** Each file decrypted and/or verified will has it's own Verification Information. You must select each file name in the *Verified Files* area to view each files verification information.

To Print a hard copy of the verification information, select the **Print…** button on the *Verification Information* window. When the standard *Print* window appears, select (highlight) the printer you wish the verification information to be printed to and select the **Print** button.

***Note:*** Each files verification information must be printed separately. You must select each file and perform the print procedures described above.

8. Select the **Close** button on the *Verification Information* window to continue, once you are finished printing the verification information.

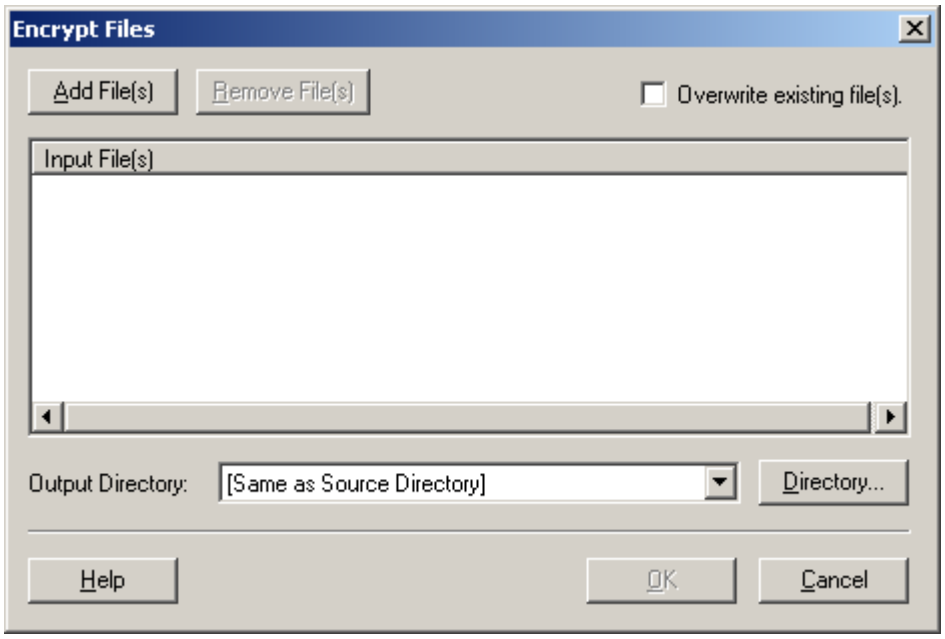
# Encrypting Files without Digitally Signing

**For the purpose of the electronic SPA transmittals WITH form 179, you will use the *Encrypt and Digitally sign files* and *Decrypt/Verify files* options. However, *for other correspondence and RAI exchange you may or may not elect to use the Encrypt file(s) option.***

*CKMfile* allows you to encrypt without digitally signing one or more files at a time. To do so, use the following steps:

1. Select the **Encrypt file(s)** button located on the *CKMfile* toolbar. This is the first button on the left.

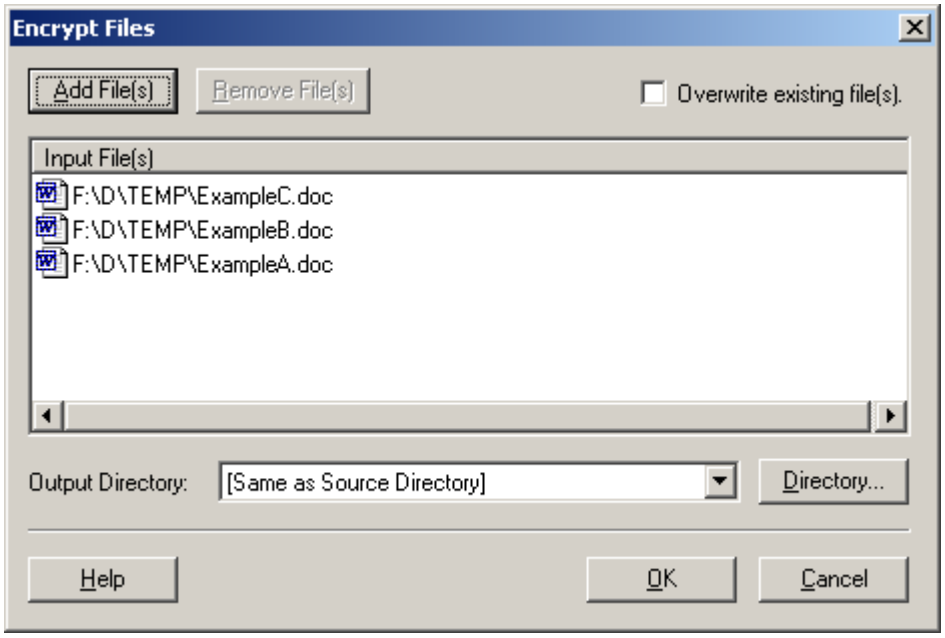
This will bring up the **Encrypt Files** window. From this window, you will be able to select one or more files to be encrypted.




2. Select the **Add File(s)** button located on the **Encrypt Files** window and navigate to the location of the file(s) to be encrypted.

3. The file(s) you selected to be encrypted will be listed in the **Encrypt Files** window under *Input File(s)*. The location of the encrypted file(s) will default to the drive and/or directory of the original unencrypted file(s) as illustrated in the *Output Directory* area as "Same as Source Directory". The filename(s) of the encrypted file(s) will have a new extension of .ckm added to the end of the original filename(s).

   ***Please note:*** You may change the *Output Directory* location by selecting the **Directory…** button next to *Output Directory*.



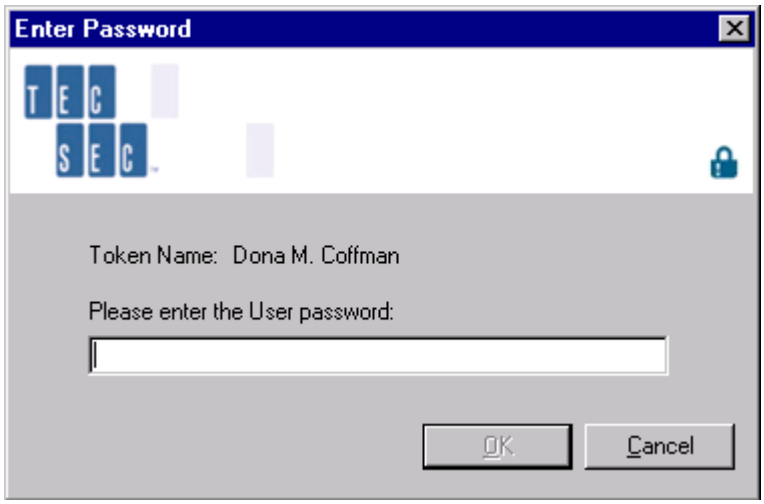

   ***Tip:*** If you decide not to encrypt any of the file(s) listed in the **Encrypt Files** window, you may select the file(s) and select the **Remove File(s)** button. This will remove the file(s) from the **Encrypt Files** window and the file(s) will not be encrypted.

   ***Please Note:*** If there is a filename conflict, the filename(s) will be shown in RED and you will not be able to encrypt any of the files listed. This usually occurs when the file already exists as an encrypted file (i.e., the same file name already exists with a .ckm extension). To continue you may 1) change the drive and/or directory of the output; 2) remove the file(s) from the list of files to encrypt; or 3) click on *Overwrite existing file(s)*.

4. Select the **OK** button on the **Encrypt Files** window to encrypt the selected file(s).

5. You will be prompted to enter the Password for your Token. On the **Enter Password** window, enter your Password and select the **OK** button. This is the Password from your CMS Administrator.

   ***VERY IMPORTANT:*** Your Password is case sensitive.

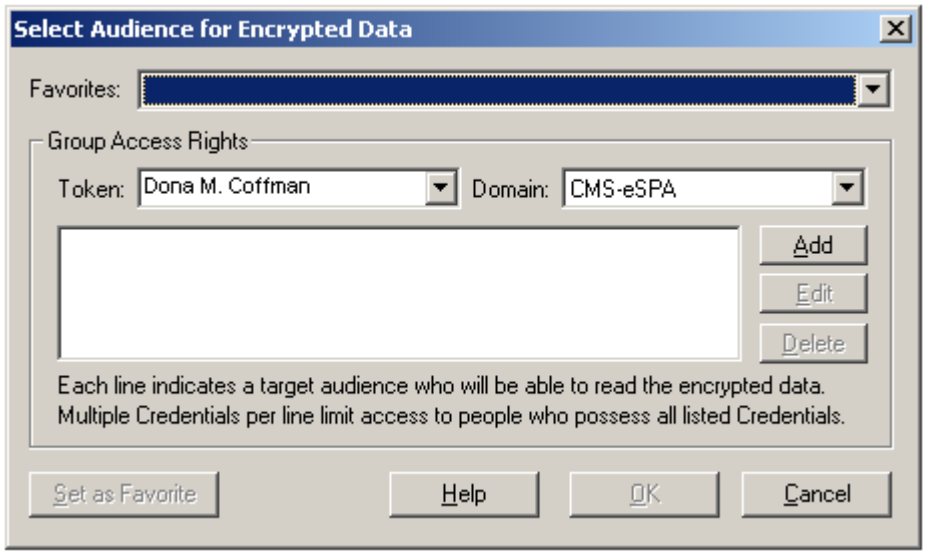



   ***Important*:** Once you have entered your Token Password AND "Encrypted and Sign", "Decrypt", "Encrypt" or "Delete" file(s), you do not need to re-enter your password again as long as *CKMfile* stays open. However, *CKMfile* and your Credentials are not secure if you leave your desk. It is recommended that you close *CKMfile* when not in use.

   ***Important:*** PASSWORDS CANNOT BE RESET. If you change your password and then cannot remember what you changed it to, a new token will have to be issued to you. The re-issuance of tokens will take 2-3 working days.

   ***Please note:*** You will be prompted to log in for most operations performed with *CKMfile*.

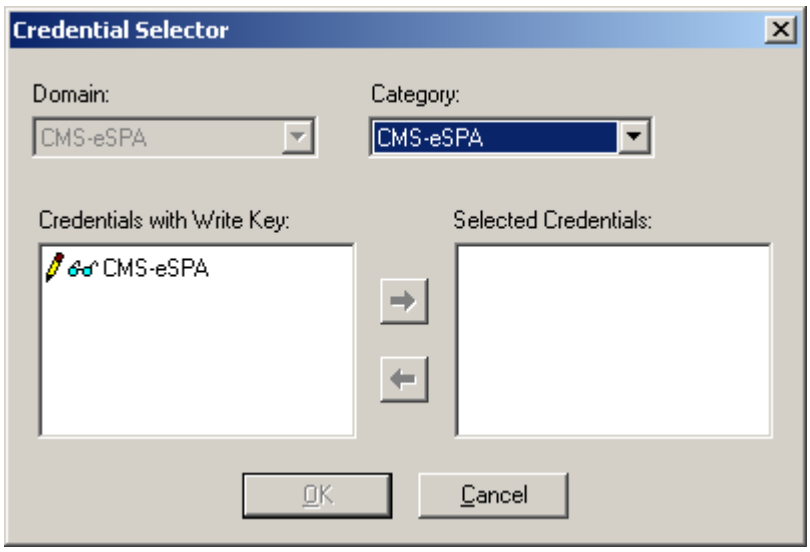
6. The **Select Audience for Encrypted Data** window will now appear allowing you to indicate the desired settings for encrypting your file(s).




7. On the **Select Audience for Encrypted Data** window, ensure that the **Token** is set to *YOUR NAME* (i.e., the name of the person who the software is registered to) and the **Domain** is set to *CMS-eSPA* under the **Group Access Rights** area. If they are not, use the drop-down arrow to select them.

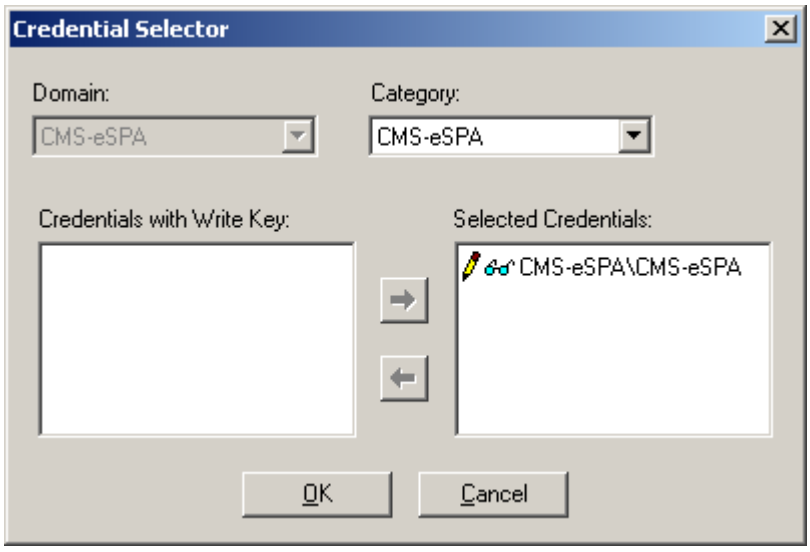
8. To select the Credentials for your target audience, select the **Add** button in the **Group Access Rights** area. The **Credentials Selector** window is displayed.

9. On the **Credential Selector** window, ensure that the Category is set to *CMS-eSPA*. If it is not, use the drop-down arrow to select it. All of the Credentials in the Selected Category are displayed in the **Credential with Write Key:** box.

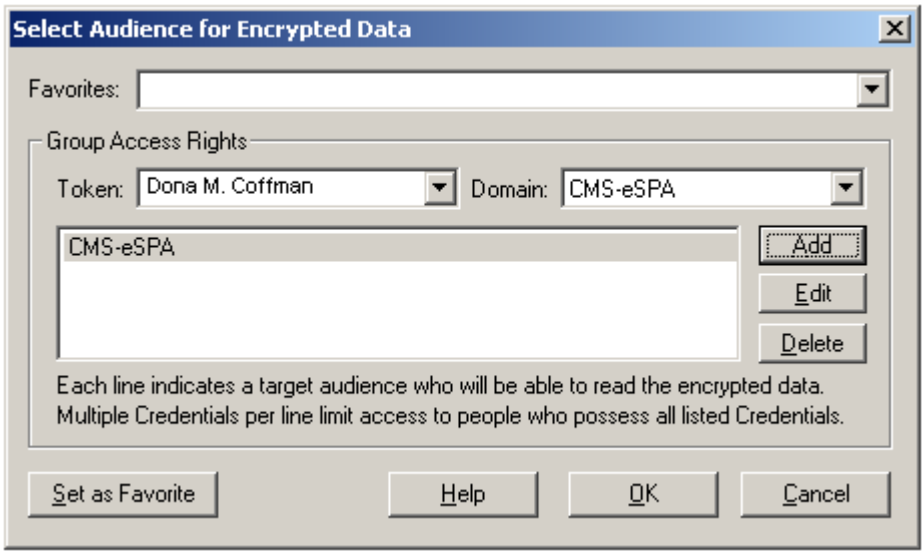



10. Select the **CMS-eSPA** Credential from the **Credential with Write Key:** box.

    Use the  arrow button to move the Credentials to the **Selected Credentials** box.



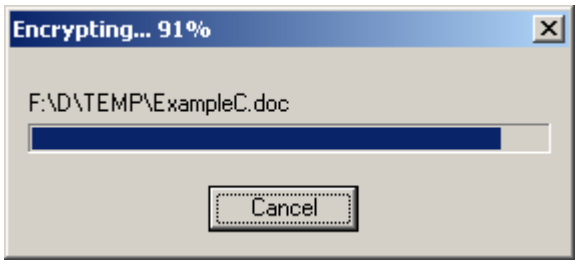
11. When you have finished making your selection, select the **OK** button. This takes you back to the **Select Audience for Encrypted Data** window, which displays the Credentials you selected. See example below.



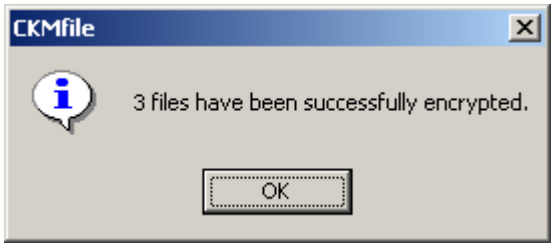

***Tip:*** To save time, you may set up a *Favorite* that will allow you to pre-define the audience for future encryption operations. Favorites will save the *Token*, *Domain* and *Credentials for your target audience* (steps 7, 8, 9, 10 and 11 above). See the section on Creating Favorites.

12. Once all your selections on the **Select Audience for Encrypted Data** window have been completed, select the **OK** button.

13. A progress dialog window will be displayed (as shown below) during the encryption process.



14. Once your files have been successfully encrypted, a message box will be displayed on your screen. Select **OK** to continue.




15. The file(s) are now ready to be E-mailed to the appropriate person(s).

16. Using GroupWise (CMS) or other Internet E-mail software, locate the encrypted file(s) [they will have a .ckm extension] and attach them to the E-mail. Send the file(s) to the pre-defined Federal or State E-mail destination (see below). The Federal E-mail boxes established for SPA receipt will automatically send a response acknowledging receipt of the SPA package.

    ***Very Important:*** During testing of the e-SPA process it was discovered that sometimes if there is no text entered into the body/message area of the E-mail, the attached .ckm file(s) was pulled into the body/message area of the E-mail. Therefore, please enter text into the body/message area of the E-mail. Sample text: "*Attached is SPA XX-XXX cover letter, form 179 and amended pages.*" or "*Attached is our response to your request for additional information relating to SPA XX-XXX.*"

    **Federal E-mail destinations**:
    Effective July 1, 2002, all IR-SPAs should be submitted directly to the National Institutional Reimbursement Team (NIRT) at NIRT@cms.hhs.gov and the appropriate CMS Regional Office e-SPA E-mail address.

    Non-Institutional Reimbursement SPAs should be submitted to the CMS Regional Office e-SPA E-mail address. These addresses are as follow:

| | |
|---|---|
| Region 1 | ESPA1@cms.hhs.gov |
| Region 2 | ESPA2@cms.hhs.gov |
| Region 3 | ESPA3@cms.hhs.gov |
| Region 4 | ESPA4@cms.hhs.gov |
| Region 5 | ESPA5@cms.hhs.gov |
| Region 6 | ESPA6@cms.hhs.gov |
| Region 7 | ESPA7@cms.hhs.gov |
| Region 8 | ESPA8@cms.hhs.gov |
| Region 9 | ESPA9@cms.hhs.gov |
| Region 10 | ESPA10@cms.hhs.gov |

**E-SPA Technical Assistance:**
An ESPA E-mail address has been established to provide technical assistance and answer technical questions (ESPAtech@cms.hhs.gov). This E-mail address is not intended to answer program or policy questions.

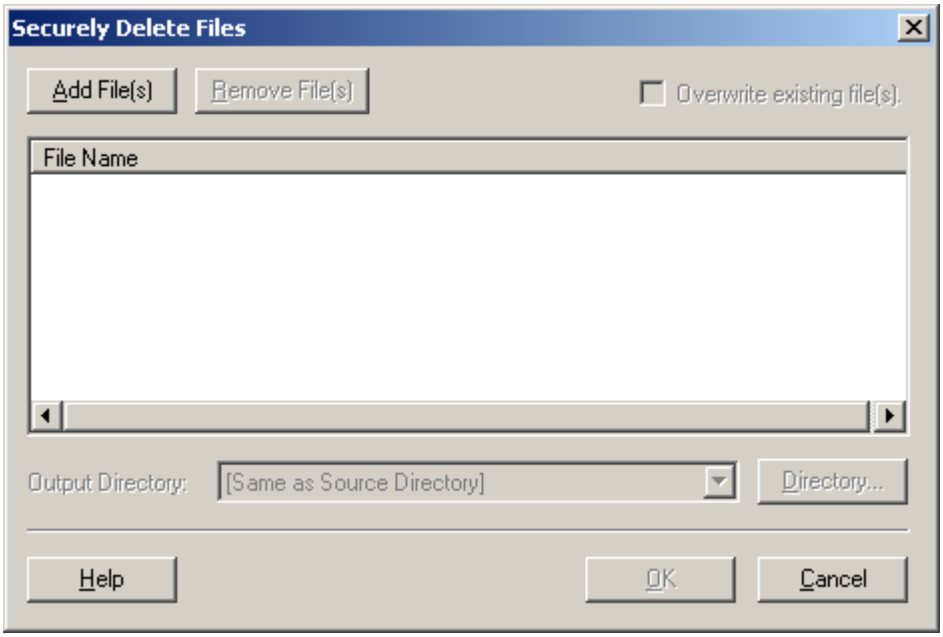
***Please note:*** For CMS users, GroupWise does NOT provide for a permanent storage of the transferred document. A separate directory or storage medium must be established for the storage and/or archiving of these documents.

# Securely Deleting Files

*CKMfile* allows you to securely delete one or more files at a time. To do so, use the following steps:

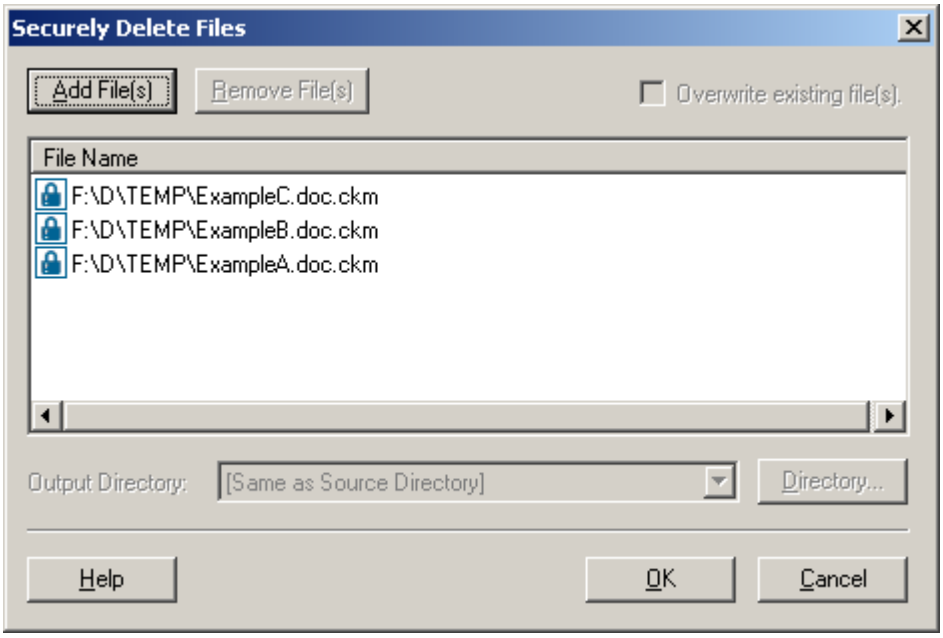
1. Select the **Securely delete file(s)** button located on the *CKMfile* toolbar. This is the last button on the right.

This will bring up the **Securely Delete Files** window. From this window, you will be able to select one or more files to be securely deleted.




2. Select the **Add File(s)** button located on the **Securely Delete Files** window and navigate to the location of the file(s) to be securely deleted.

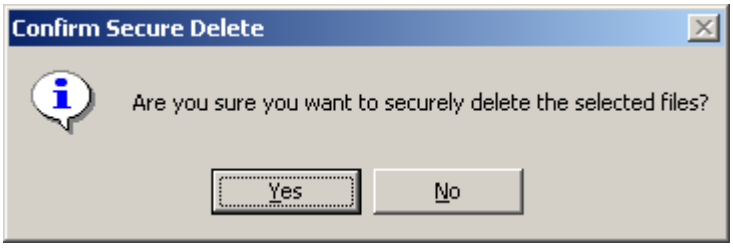
3. The file(s) that you selected to be securely deleted will be listed in the **Securely Delete Files** window.




***Tip:*** If you decide not to delete any of the file(s) listed in the **Securely Delete Files** window, you may select the file(s) and select **Remove File(s)** button. This will remove the file(s) from the **Securely Delete Files** window and the file(s) will not be deleted.

4. Select the **OK** button in the **Securely Delete Files** window to security delete the selected file(s).

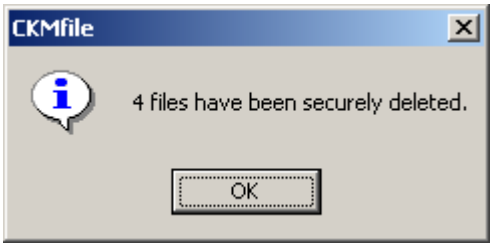
5. A message box will display for you to confirm the secure deletion operation.




6. Select **Yes** to continue.

7. A progress dialog window will be displayed during the secure deletion process.

8. After your files have been successfully and securely deleted, a message box will be displayed on your screen. Select **OK** to continue.



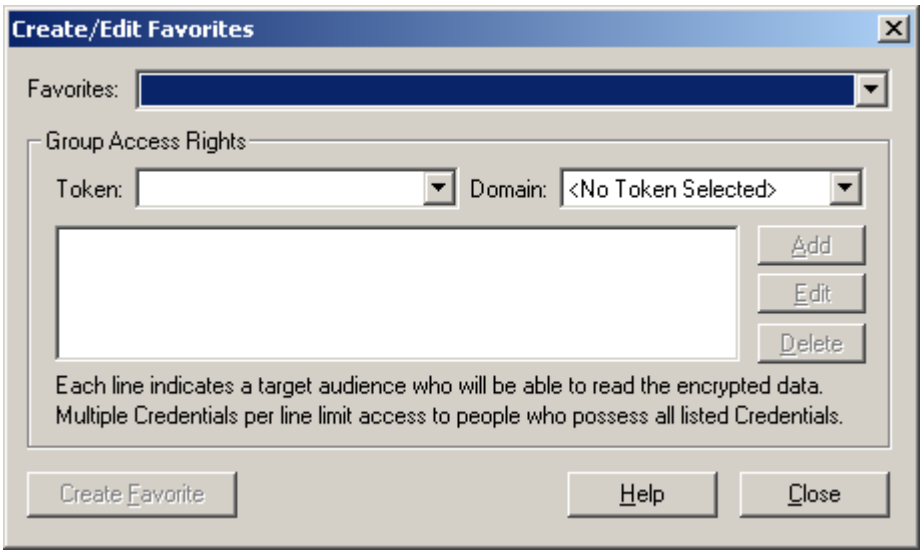
# Creating Favorites

*CKMfile* allows you to save frequently used encryption preferences called Favorites. Encryption preferences that can be saved include: Token, Domain, and Credentials for your target audience. Favorites allow you to save time by not needing to re-define the audience for future encryption operations. This will allow you to replace steps 7, 8, 9, 10 and 11 under ***Encrypting and Digitally Signing Files*** and ***Encrypting Files without Digitally Signing***. To do so, use the following steps:

1. From the *CKMfile* toolbar, select **File** menu.

2. Select the **Favorites** command from the **File** menu.

   The **Create/Edit Favorites** window will be displayed




3. Under the **Group Access Rights** area, from the **Token** drop-down list, select *YOUR NAME* (i.e., the name of the person who the software is registered to).

4. You will be prompted to enter the Password for your Token. In the **Enter Password** window, enter your Password and select the **OK** button.

   ***Please Note:*** You will only be prompted to enter your Password only if you have not previously logged in to *CKMfile*. If you are not prompted to enter your Password, please skip to Step 5.

5. Once you are logged in, the **Domain** should default to *CMS*, under the **Group Access Rights** area. If it is not, from the **Domain** drop-down list, select *CMS*.

6. To select the Credentials for your target audience, select the **Add** button in the **Group Access Rights** area. The **Credentials Selector** window is displayed.

7. On the **Credential Selector** window, ensure that the Category is set to *ESPA*. If it is not, use the drop-down arrow to select it. All of the Credentials in the Selected Category are displayed in the **Credential with Write Key:** box.

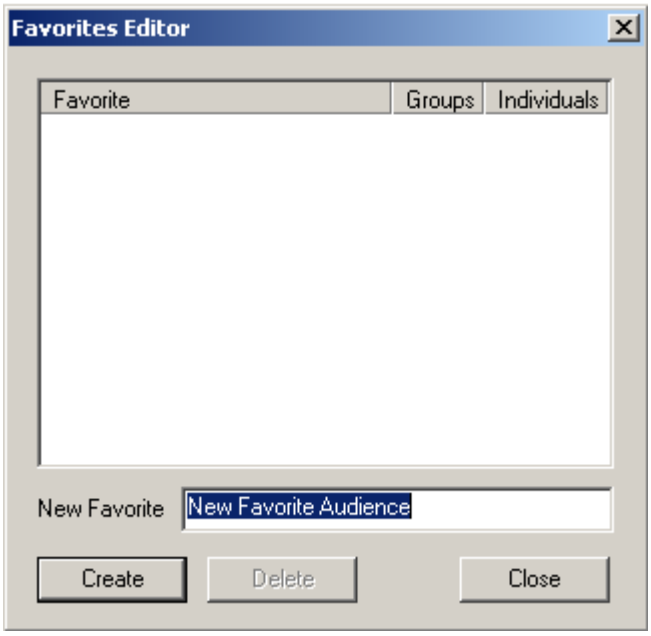
8. Select the **ESPA** Credential from the **Credential with Write Key:** box.

   Use the  arrow button to move the Credentials to the **Selected Credentials** box.

9. When you have finished making your selection, select the **OK** button. This takes you back to the **Create/Edit Favorites** window, which displays the Credentials you selected.

10. From the **Create/Edit Favorite** window, select the **Create Favorite** button.

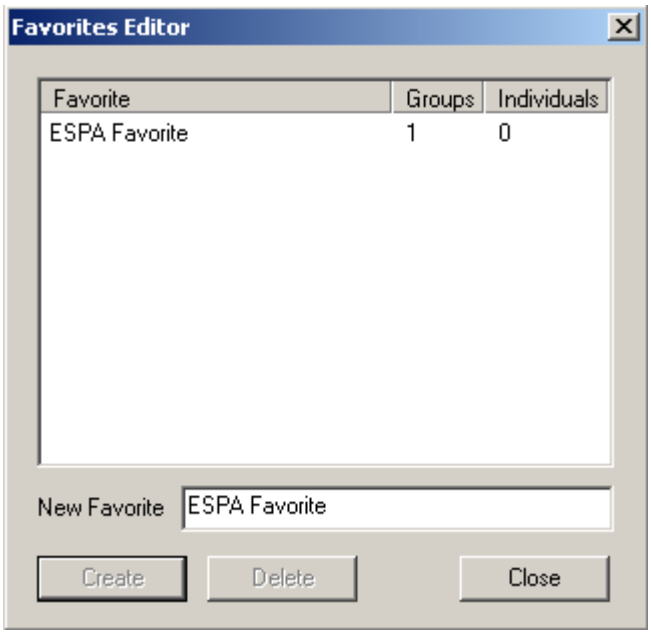
11. The **Favorites Editor** window will be displayed.




12. In the **New Favorite** field, enter the name for your Favorite. The name can be any combination of letters and numbers up to 35 characters long.

13. Select the **Create** button in the **Favorites Editor** window.

14. Your Favorite will now be listed in the **Favorite Editor** window.




When you are **Encrypting and Digitally Signing File(s)** or **Encrypting Files without Digitally Signing** and you get to the **Select Audience for Encrypted Data** window, using the Favorites drop-down list, select the Favorite you created. This replaces Steps 7, 8, 9, 10 and 11.