Air Force Research Laboratory

Trusted End Node Security (TENS) Encryption Wizard (EW) User's Guide

Version 3.5.3 – 28 Aug 2018

TABLE OF CONTENTS

TABLE OF FIGURES

1 Quick Start

- If needed, download and install Oracle JRE from http://java.com.

  Most computers already have Java installed. Encryption Wizard is a standalone application and does not run inside a web browser, so you may disable or otherwise restrict Java's operation inside a web browser as you see fit.

- Download Encryption Wizard from https://www.tens.af.mil/download.htm.

  Many web browsers will not be able to form a secure connection to Department of Defense websites due to certificate issues ("unknown issuer" or "invalid certificate"). For details and solutions, see www.getTENS.online.

- Open the .zip file and extract the contents.

  Simply "browsing" inside the .zip file is convenient for quick examination, but is not recommended for operation.

- Double-click the .jar file or type on a command line "**java –jar EW-*-3.5.x.jar**" to start (using the appropriate exact filename).

- Optionally, in Windows click "**Install**" under the Tools menu to make Encryption Wizard more user-friendly.

- Drag-and-drop files/folders into the Encryption Wizard window.

- Select "**Encrypt**" for individual files or "**Archive**" for a many-to-one, compressed, and encrypted file.

- Enter your passphrase(s), smartcard*, or certificates(s) and optionally enter metadata.

- Your file is now encrypted.

- To decrypt, drag the .wzd / .wza file into Encryption Wizard and select "**Decrypt**". Or, if the Install step has been performed, you may double-click the encrypted file outside of the Encryption Wizard window to launch decryption mode.

** Smartcards supported in 64-bit Windows with Java 8 and later due to Java 7's lack of PKCS#11 support (see Sections 2 and 6).*

2 General Information

Encryption Wizard (EW) is a cryptographically-strong, fast, easy-to-use file and folder encryption program for protecting sensitive information (such as CUI, PII, SBU, FOUO, Privacy Act, personal, contractual, analytical, financial, and other data you are required to protect). EW encrypts all file types for data-in-transit and data-at-rest protection with drag-and-drop simplicity. Encryption Wizard is a simple, GOTS, certified, AES-128/AES-256, Java application. EW can be installed and executed without administrator rights on Windows, Mac, Linux, and Solaris computers with standard Java 1.8 or later.

EW can significantly increase an organization's security posture at little to no cost by protecting sensitive data in transit (e.g. email, FTP) and at rest (e.g. removable media).

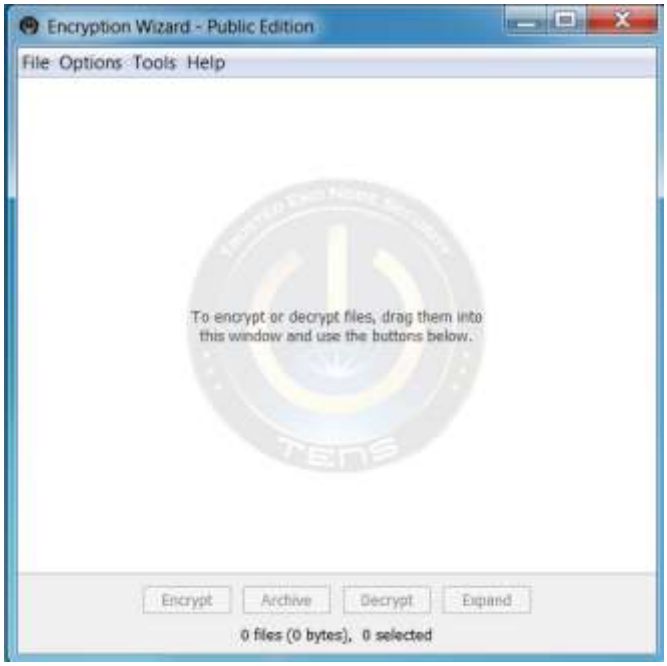


Figure 1 - Encryption Wizard Main Window

Encryption Wizard comes in multiple fully compatible and look-alike editions. Encryption Wizard - Public Edition (EW-Public) is free for everyone (and is also found within TENS-Public). Encryption Wizard - Government FIPS Edition (EW-Govt) is for the entire US Federal Government and its contractors, and contains a FIPS 140-2 validated cryptography module licensed from RSA Security. EW-Govt is accredited by the US Air Force and US Army. Encryption Wizard - Unified Edition (EW-Unified) is free for everyone, and contains a FIPS 140-2 validated cryptography module provided by The Legion of the Bouncy Castle.

2.1 System Requirements

- Java Runtime Environment 1.8 (March 2014) or newer. (Many PCs already have Java. The Oracle JRE at java.com is the recommended version. Installing Java usually requires administrative privileges; the "Server JRE" packages do not come with an installer utility but do not require elevated privileges.)
- 3 to 12 MB disk drive space depending on the edition used.
- [Optional] To unlock 256-bit keys, most JREs prior to 1.9 require replacement jurisdiction policy files to be installed. These are dependent on the country; for the Oracle JRE, the appropriate policy files are available at www.oracle.com/technetwork/java/javase/downloads/index.html

2.2 Recommended Use

Air Force Research Laboratory recommends Encryption Wizard for the protection of all sensitive data in transit or at rest. EW-Public and EW-Unified are for everyone while EW-Govt is licensed only for U.S. Federal Government employees and their contractors. The environment where Encryption Wizard is running should have security commensurate for the unencrypted data. EW offers no protection before/during encryption or during/after decryption - only encrypted data is protected. A few possible uses of Encryption Wizard include:

- Protecting Controlled Unclassified Information (CUI, SBU, FOUO, etc.) on laptops, CDs, thumb drives, and other portable media.
- Contractors, subcontractors, customers, and Contracting Officers may trade financials, contracts, and deliverables with the same tool.
- Communities can technically enforce Need-To-Know on shared drives.
- Military leaders may send FITREPs (EPRs) securely to sailors' (soldiers') webmail.
- NCOs can distribute alert rosters to soldiers' home email accounts.
- Users at home can safely store banking, investment, and credit card information.
- Reserve units can trade forms and paperwork with their "at-home" troops.
- Lawyers maintain attorney-client confidentiality by sharing only protected files.
- Software developers use EW's command line interface to add certified en/decryption to their systems.
- HR offices can securely send private, financial, and employee files to employees.
- Multi-agency organizations (e.g. DoD and DoE) can share files and information despite incompatible enterprise encryption solutions.

2.3 Installation and Setup

Encryption Wizard requires no installation or setup process. Assuming that a recent version of Java is installed on a user's system, Encryption Wizard may be executed simply by double-clicking on the executable, **EW-xxx-3.5.x.jar**. On Microsoft Windows, there are user convenience features that associate the Encryption Wizard file types with the tool and a Send To context menu as well (see Section 7.8 Optional 'Install' in Windows, for details).

2.3.1 Uninstallation

On Microsoft Windows computers, if you have used the file-type association features described in "Optional 'Install' in Windows," then you should use the "**Uninstall**" action (described in the same section) to remove the associations and related files.

As for the software as a whole, Encryption Wizard has no system-wide uninstallation process, as this would require administrative privileges. Simply delete the **EW-*.jar** file originally used to run the program.

2.4 What's New

Starting in version 3.4, Encryption Wizard permits the use of 256-bit AES keys. Prior to Java 9, this typically requires *unlimited strength jurisdiction policy files* to be installed; see Section 2.1, "System Requirements". The command-line interface has been completely rewritten, for more robust and featureful scripting. Microsoft Windows users can view file hashes by right-clicking on their files and using the appropriate "**Send To**" link, and securely delete their files by holding down the **Shift** key when right-clicking. Later releases of 3.4.x added a tool for generating public/private X.509 keypairs, and for MIME "wrapping" arbitrary files in Base64 encoding.

Version 3.5 introduces the Unified edition, providing FIPS 140-2 validated crypto to users of the Public edition.

2.5 Known Issues

Depending on the version of Java in use, Encryption Wizard may not be able to access CAC/PIV cards on Windows x64 editions for the purpose of encryption, decryption, or key export. Oracle Java 7 and earlier does not support the smart card interface through native PKCS#11 libraries on Microsoft Windows 64-bit systems due to the lack of available native libraries. These capabilities are available in Java 8, released in Q1 2014. However, support in Java 8 comes and goes depending on the exact combination of JRE version and smartcard middleware version; this is expected to settle down as user feedback percolates through vendors.

2.6 Launch Encryption Wizard

Encryption Wizard can be launched:

- By double-clicking **EW-*impl*-3.5.x{-FIPS}.jar** where ***impl*** is **Govt**, **Public**, or **Unified**, depending on the edition used (or its shortcut),
- If installed In Windows, by double-clicking a **.wzd, .wza,** or **.wzk** file; by selecting Encryption Wizard on a file/folder's Context Menu (found by right-clicking a file); by clicking the Encryption Wizard shortcut in the Windows Start Menu.
- By the command line (see Section 7.3).

2.7 Licensing

U.S. Government Edition

The EW-Govt edition contains a FIPS 140-2 validated cryptographic module licensed from RSA Security, LLC®. This edition may only be used by US Government employees or contractors under contract with the US Government. It may only be distributed by the Air Force Research Laboratory and by designated distribution authorities. Users may NOT examine code contained in the RSA licensed cryptographic module contained in this edition.

RSA's FIPS 140-2 validation is denoted by CMVP certificates 2468 and 2469, viewable at https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2468 and 2469.

Unified Edition
The EW-Unified edition contains a FIPS 140-2 validated cryptographic module provided by The Legion of the Bouncy Castle. This edition may be used by any party eligible to use the Public edition.

The Bouncy Castle FIPS 140-2 validation is denoted by CMVP certificates 2768 and 3152, depending on the version of Encryption Wizard. For EW-Unified 3.5.0 through 3.5.2, certificate 2768 is applicable:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2768
For EW-Unified 3.5.3 and later, certificate 3152 is applicable:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3152

Public Edition
The EW-Public edition has no specific restrictions on who may use it or how it is used. However, users are still subject to any licenses or agreements governing the use of their local Java Runtime Environment. EW-Public may be freely distributed via electronic or other means. Users may examine the executable code contained in the .jar file. Users may NOT re-purpose the executable code contained in the .jar file or distribute modified versions of its code or the .jar file without the prior written consent of the Air Force Research Laboratory.

All Editions
Any nation in the *Export Administration Regulations 740-1 Country Group E:1* is prohibited from using Encryption Wizard. As of December 2016, this excludes Iran, North Korea, Sudan, or Syria. Cuba is no longer on E:1 but is now on E:2, which may be equally prohibitive. Readers are cautioned that this status may change unpredictably, and are advised to obtain proper legal counsel.

Some of the non-cryptographic components of Encryption Wizard are third-party modules with their own varying licenses. None of those licenses impose additional restrictions on use or redistribution; the license texts are not included here to save space, but are hyperlinked below and are also available upon request. The Encryption Wizard team expresses our gratitude to the authors for making their tools available:

- The command-line parsing makes use of the Getopt port distributed along with GNU Prolog for Java, under the GNU Library General Public License v2. (The bulk of Prolog for Java is released under v3 of that license, but the Getopt port has its own licensing.)
- Part of the console portability routines use McDowell's TextDevice hierarchy, under the MIT License.
- The logging subsystem makes use of SLF4J, under the MIT License; Logback, under the GNU Library General Public License v2.1; and for certain builds, SysOutOverSLF4J, under the MIT License.
- The keypair generation utility makes use of the Bouncy Castle Crypto API, under the standard license of the Legion of the Bouncy Castle.

2.8 Certification and Accreditation

EW-Govt is certified for the Global Information Grid (e.g. NIPRNet, SIPRNet, and Constellation Net). EW-Govt is on the Air Force Evaluated/Approved Products List (AF EPL and see the EW-Govt package) and holds an Army Certificate of Networthiness (Cert # 201008395). EW-Govt is used by many non-DoD federal organizations and has/is seeking other certifications/approvals. Contact AFRL for its current certification status and/or to seek support in obtaining certification in your enterprise.

2.9 Custom Edition Changes

Users in Federal organizations may have a customized edition of Encryption Wizard (see https://www.tens.af.mil/ewizard_govt.htm). For those users, the appearance and behavior of your version of EW may differ slightly from that described in this manual. Typical changes include, but are not limited to:

- *Automatic use of recovery escrow keys during encryption*
  These keys are not shown in the key list (Section 8.2). Information about escrow keys will be displayed in the About dialog (Section 7.7). The main EW window will include a reminder warning that escrow keys are in use.

- *Enforcing password complexity requirements*
  When encrypting with a password (Section 3.2.1), all requirements will initially be listed. As the user types, individual requirements will be removed from the list as they are satisfied. If the passphrase generator tab (Figure 5) is used, the generator settings will initially be those to meet the requirements, but may be altered by the user. If a password is then generated which would not meet the requirements, the "**Add**" key will be disabled. Hovering the mouse over the disabled key will show a tooltip with the unmet requirements. Finally, if the user saves the altered settings as the default, then when EW starts up, any settings not meeting the requirements will be raised to the minimums (but can still be changed by the user). You can see whether this happens in the current log (after starting the generator, view **Help -> Log**).

- *Changing the defaults and/or removing some of the options described in Section 7.9*
  A smart user will check which options are toggled before starting any cipher operations to avoid surprises.

The first point of contact for support with custom builds will be listed in the About dialog (Section 7.7).

2.10 Information, Support, and Improvements

Information about Encryption Wizard is found in its Help Menu, in this manual, and the many documents (including whitepapers) found within https://www.tens.af.mil/ewizard.htm. The Air Force Research Laboratory offers additional information about Encryption Wizard upon request.

AFRL provides Tier 2 "Advanced" and Tier 3/4 "Development" support for EW-Govt and limited Tier 1 "Help Desk" support via email for all editions (as resources allow). R&D services may be cost-reimbursed.

We welcome suggestions from improving all forms of Encryption Wizard.

Developer
Air Force Research Laboratory
Website: https://www.TENS.af.mil
Program Management Office: TENS@us.af.mil
Help Desk: Wright-PattersonAFRL.RYW_ATSPI_Outreach@us.af.mil

3 Encrypt a File

To encrypt a file (see Figure 2), simply move the file into EW, select "**Encrypt**", and provide a key (passphrase or certificate).

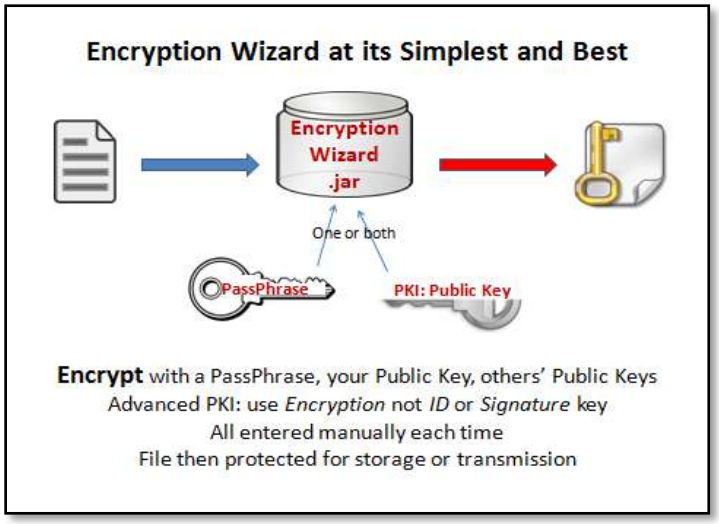


Figure 2 - Encryption Process

3.1 Select File(s) to Encrypt

To encrypt a file(s) and create a .wzd file, open Encryption Wizard and add the file(s) to the main file list in one of the following ways:

- Drag and drop file(s) to the file list window (see Figure 3)
- Use the menu to select "**Add File**", choose file(s) from the file selection dialog
- Press "**a**" to bring up the file selection dialog

- If installed in Windows, you may right-click a file, and select "**Send To…**" then "**Encryption Wizard**".

Once the file(s) is in the file list, select the file(s) to encrypt and click the "**Encrypt**" button in the bottom tool bar or press "**e**". If no files in the file list are selected, all files in the file list will be used. Each file selected will be encrypted as an individual .wzd file.

Figure 3 - File List Window

3.2 Provide the Keys

To add a key, select the tab for the intended key type (passphrase, CAC/PIV, or Cert File). Enter your key(s), as detailed in the following sections, and select "**OK**". Once added, they appear in the white "ready" box near the bottom of the window (see Figure 4). Users may enter multiple passphrases, smart card certificates, or soft certificates for use in the encryption process. Any one of the added keys will then be able to decrypt the file(s).To remove a key, select the key and select "**Remove**". After at least one key is added, select "**Next**" to continue.

The following sections describe how to add each key type.

3.2.1 Encrypt with a Passphrase

The Passphrase option uses a symmetric key - the same passphrase is used to encrypt and decrypt the file. Simply enter by typing (or copy/paste) the passphrase, confirm it by entering it again, then select "**Add**" or press **"Enter"** (see Figure 4.

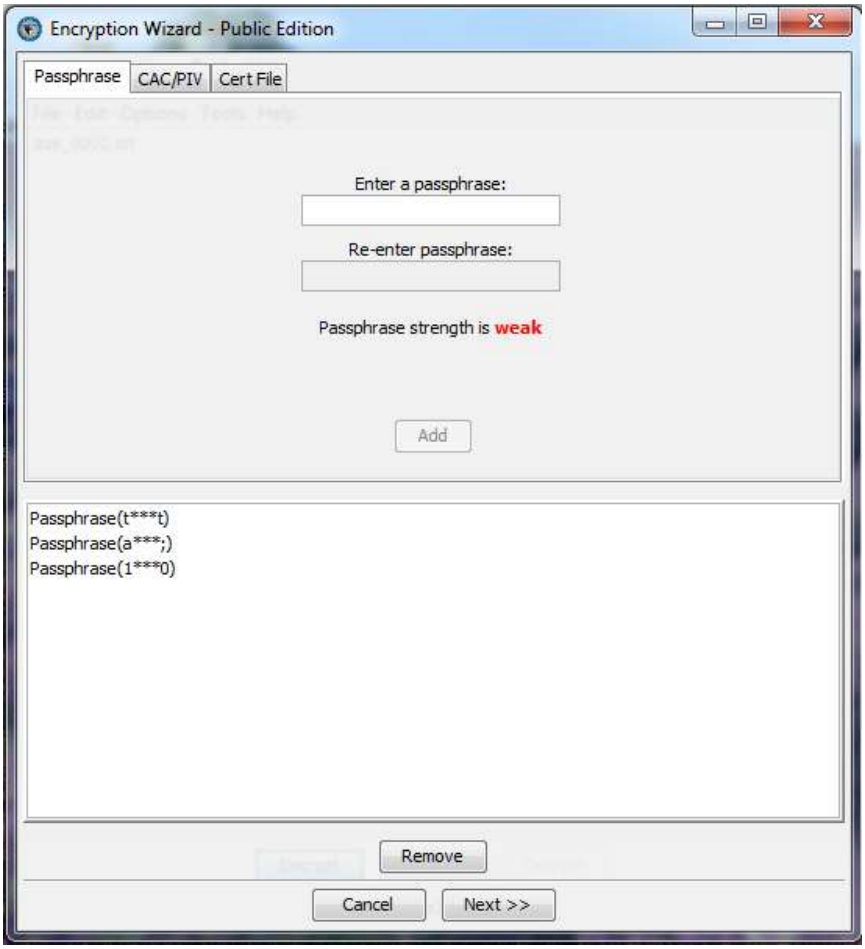


Figure 4 - Passphrase Entry Tab

Encryption Wizard accepts all characters. As you type, a strength estimator with a dictionary word check evaluates your passphrase and displays the strength of the current passphrase. Once added, EW will display the first and last letter of the passphrase while hiding the rest from prying eyes (and screen-capture malware).

Be sure to select a memorable passphrase or record it out-of-band (e.g. write it down and put it in a safe place). If you hold a public key or smartcard, we recommend also encrypting with it as backup to a lost password. If the passphrase is lost, forgotten, or mistyped, the data cannot practically be decrypted.

If you would like a computer generated random password, Encryption Wizard provides a tab with the ability to create a passphrase using parameters set by the user (see Figure 5). Set your parameters as described in Section 5, select "**Generate Passphrase**", and select "**Add**" when you get a passphrase you would like to use.

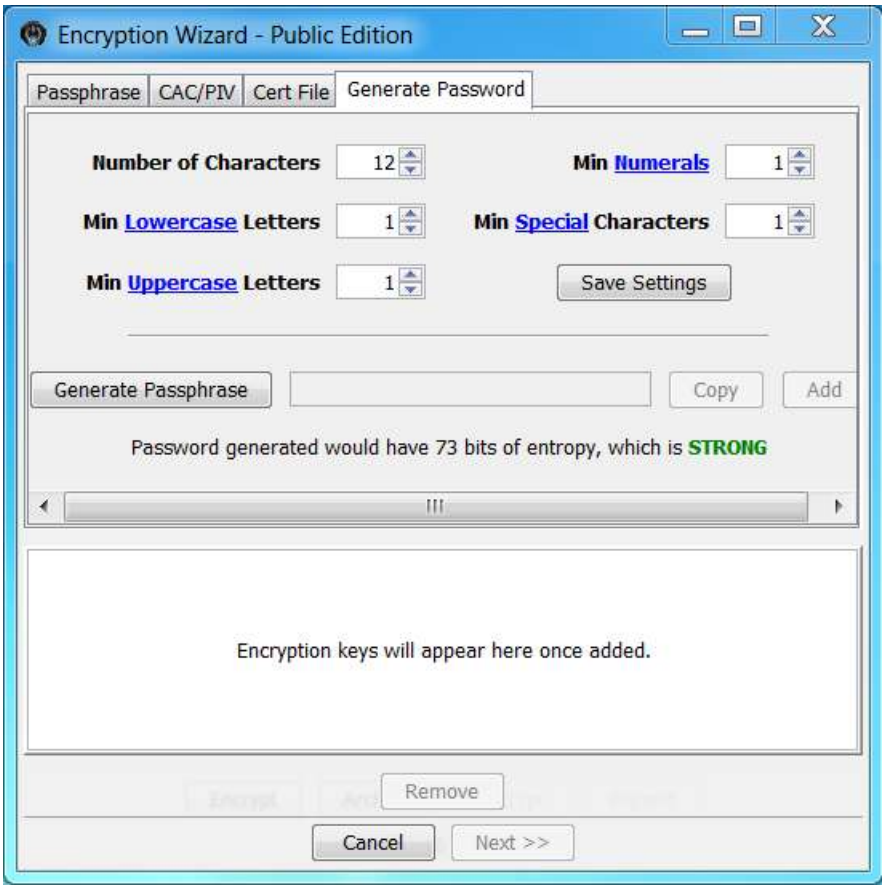


Figure 5 - Generate Password Tab

3.2.2 Encrypt with a CAC/PIV Card

Encryption Wizard may encrypt with a person's public certificate and decrypt with a person's private certificate. Certificates may be soft (a file in your computer, as in the next section) or embedded in a separate device, like a smartcard (e.g. CAC or PIV Card). This section only explains how to encrypt a file with your smartcard's public certificate, but we recommend reading the next section also.

For most smartcard users, Encryption Wizard will find the proper public certificate on your smartcard, assuming your system has a reader and the underlying software/middleware necessary to access the reader. Select the "**CAC/PIV**" tab, insert the smartcard into the reader, select "**Access**", and enter your Personal Identification Number (PIN) (also called the Master Key) if asked for it. EW usually chooses the best Encryption certificate (if multiple ones are presented) but you can select another. Select "**Add**". EW automatically pulls and adds the smartcard's public certificate (see Figure 6).

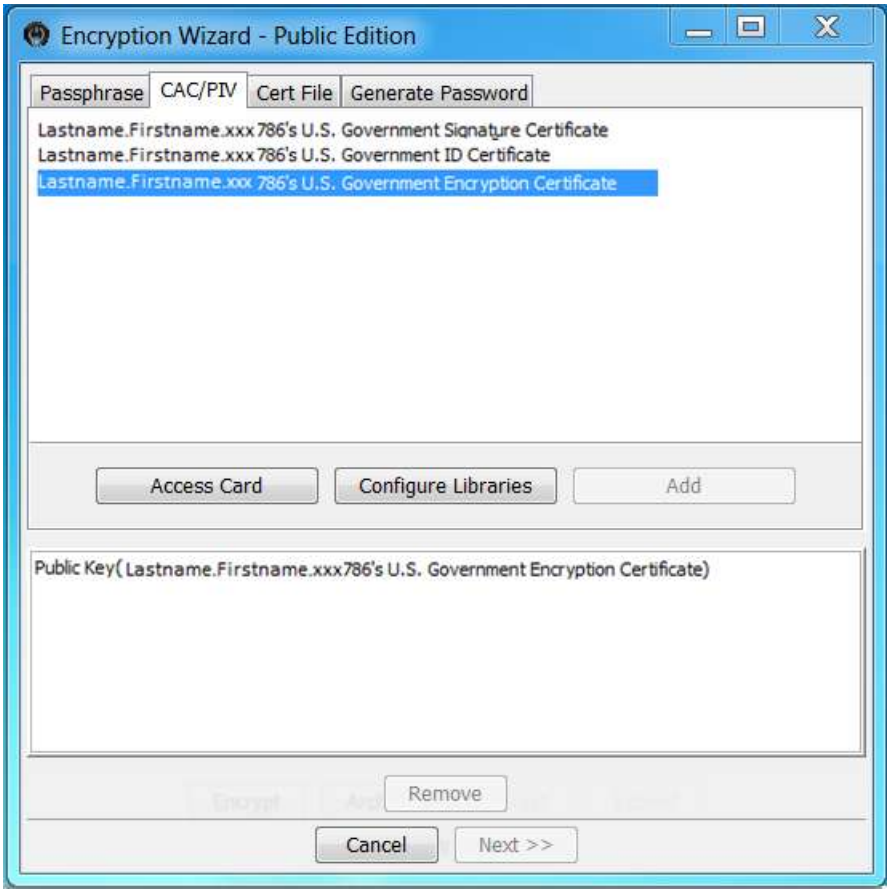


Figure 6 - Smartcard (CAC/PIV) Selection Tab

3.2.3 Encrypt with a Certificate File (Public Key, Certificate)

You may trade public certificates via email, a public fileshare site, posting it on a webpage or Facebook page, etc. Encryption Wizard's Keychain (see Section 7.2) makes managing others' public certificates easier.

In Encryption Wizard, select the **Cert File** tab, browse to the soft certificate file's location and select "**Add**" (See Figure 7). You may also drag-and-drop the certificate into the window.

Figure 7 - Certificate File Tab

A few cautions when using Public Keys:

- Never share your private key or the PIN / password to access your private key.
- When using the DoD CAC, **always use the Encryption Certificate** - this is the only certificate that is kept in escrow by DISA for later retrieval. EW usually selects this key by default. If you encrypt your data with any other certificate, you may not be able to decrypt the file if you have been issued a new CAC.
- If files are encrypted with only a third party's PKI certificate, then ***only*** the holder of that private key will be able to decrypt them. For example, if a file is encrypted with only the PKI certificate of the Secretary of Defense and you delete the original file, then only the Secretary of Defense will have access to that file. If you want to also be able to decrypt the file, you will need to add your own public key as well.

3.3 Add File Metadata

After selecting your key(s), Encryption Wizard optionally requests searchable metadata about the encrypted file. The user-supplied metadata (see Figure 8) is stored inside the encrypted file's header in plaintext so that it may be indexed by enterprise search tools (or read by humans). If you have installed Encryption Wizard, you may configure Encryption Wizard to suppress the display of the metadata dialog under the **Option** menu (see Section 7.9).

Figure 8 - Metadata Entry Window

3.4 Save or Delete the Original File

Finally, the user will be asked if they wish to delete the original file (see Figure 9). Generally we recommend keeping the original, unless you are on an untrustworthy (e.g. public) computer. Within the **Options** menu, you may set EW to "**Always Keep**", "**Always Delete**", or "**Ask**" (see Section 7.3.4.5).

Figure 9 - File Deletion choices

The newly created .wzd file will appear in the EW window in blue text (see Figure 10) and in the directory of the original file. Your file is now protected.

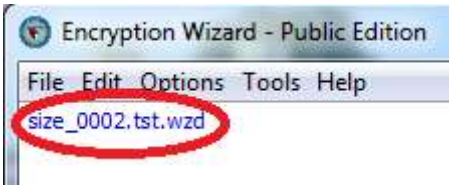


Figure 10 - Encrypted File Displayed

4 Decrypt a File

The process for decrypting a file with Encryption Wizard is similar to the process for encrypting it (see Figure 11). Simply add an Encryption Wizard file (a file with the extension .wzd or .wza) to the file list by dragging and dropping it, selecting "**Add File**" from the File menu, or pressing "**a**".

In Windows, if Encryption Wizard was "installed" you may also double-click on the file and proceed directly to the decryption key window.

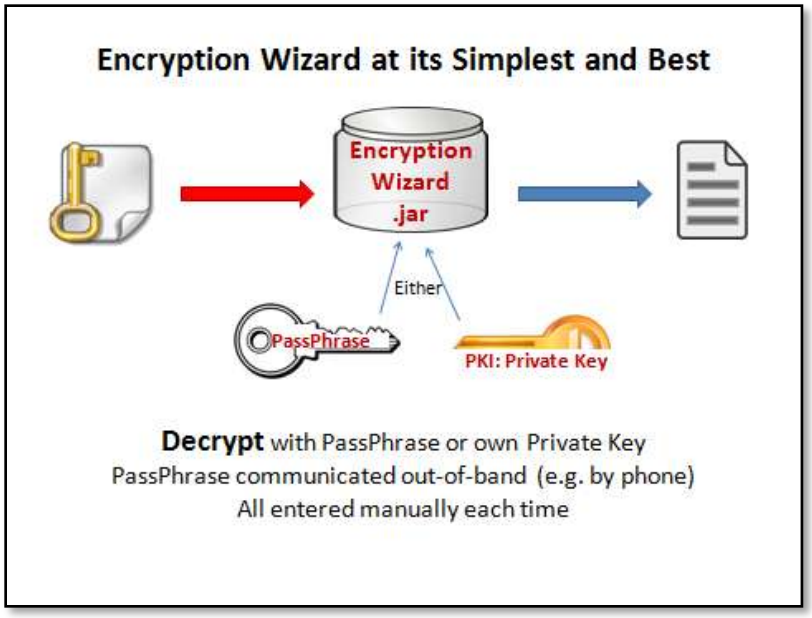


Figure 11 - Decryption Process

4.1 Enter a Decryption Key

Once the file is in the Encryption Wizard file window, select the encrypted .wzd or .wza file and select the "**Decrypt**" button or press "**d**". **Encryption** Wizard will ask for the keying material that was used to encrypt the file. If encrypted with multiple passphrases and/or certificates, only one of those is needed to decrypt the file; use the decryption method that is most convenient. Next:

- If the file was encrypted with a passphrase, enter the passphrase, and select "**OK**" or press **"Enter"** (see Section 3.2.1 for instructions on a similar interface).
- If the file was encrypted with your public key, select the "**CAC/PIV**" tab, select "**Access**" to read your card, select a certificate (typically the Encryption Certificate), and enter your PIN (see Section 3.2.2 for instructions on a similar interface).
- If the file was encrypted with some other public certificate, find the file by selecting "**Location**", browse to the .pfx or .pkcs12 file, and follow the prompts to find and unlock the private key file (see Section 3.2.3 for instructions on a similar interface).

The original file will be decrypted and restored to the original filename and extension. If you decrypt a file and there is a file with the same name within the same folder, you will be asked to overwrite the original file or cancel. The file will appear in black text in EW's file list window and in the directory of where the .wzd file existed.

5 Generate Passphrase

Encryption Wizard is able to generate strong, random passphrases that can be used within Encryption Wizard or for other accounts and software. To generate a passphrase, use "**Generate Passphrase**" under the Tools menu, press "**G**", or use the **Generate Passphrase** tab within the key selection page of the encrypt/archive file wizard. Provide the parameters you desire and select the "**Generate Passphrase**" button (see Figure Figure 12) to display the passphrase in the text box. The generated passphrase can be copied to the clipboard to be pasted into a keychain or text document for remembering using the "**Copy**" button next to the displayed passphrase.

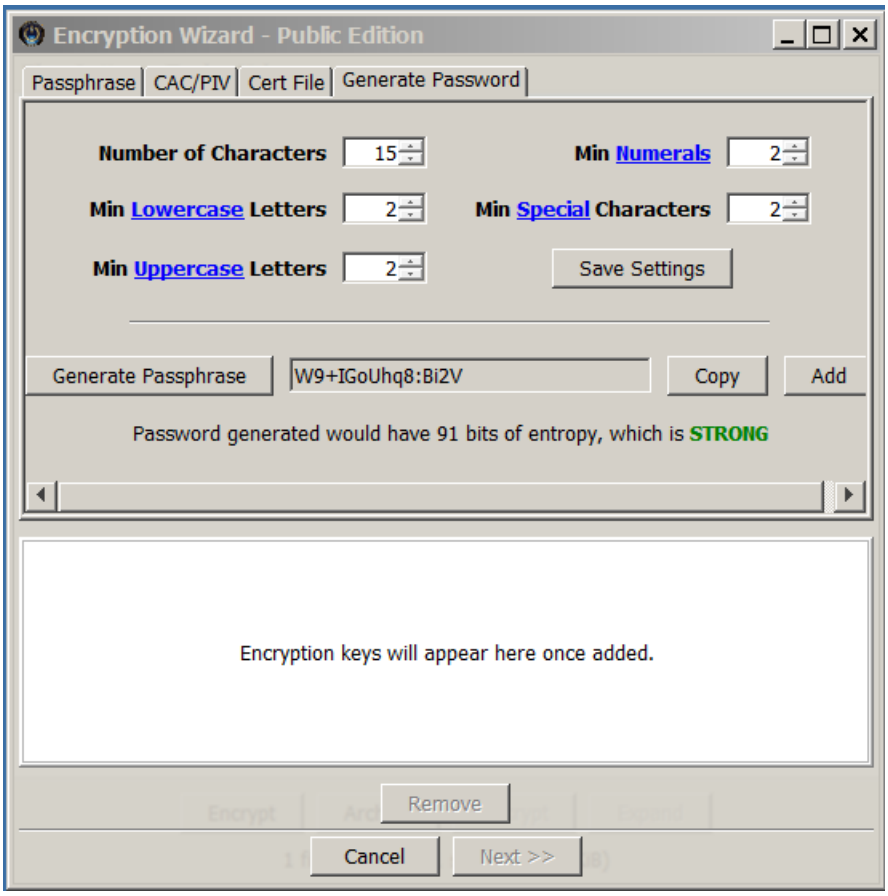


Figure 12 - Generate Passphrase Dialog

Encryption Wizard's password generator can be configured to create passphrases up to 100 characters in length with only the specified character sets. To change the desired length of the passphrase and to specify the minimum number of each character set within the passphrase, type new numbers or select the up/down arrows on the boxes next to the character set's description. **If**

the minimum number of a character set is set to "0", the passphrase will not contain any characters from that set.

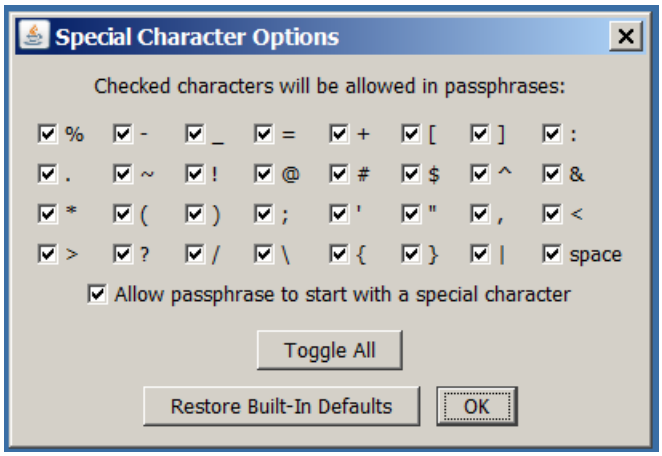


Figure 13 - Special Character Option Dialog

In addition to removing the whole character set, specific characters from each set may be included or removed by selecting the hyperlinked word in the character set's description. A dialog box (see Figure Figure 13) will open showing the options for that character set. Those characters that have a check in the check box will be used while those not checked will be excluded from any passphrases generated. You will also have the option to allow passphrases to start with special characters within the special character options dialog[1]. If you plan to use the current parameters often, you may want to save them by selecting "**Save as Default**". The settings will be used each time Encryption Wizard is used from then on.

5.1 Communicating Passphrase Safely

Sharing a passphrase-encrypted file that you intend others to view obviously requires sharing the passphrase as well. But the secrecy of your encrypted information can be compromised if the passphrase is trivial to obtain. We give here some advice for communicating a passphrase in a safe and secure manner.

- The most important idea is that the passphrase must be communicated out-of-band, that is, using a different means of communication than that used for sharing the encrypted files. For example, if you send an encrypted file as an email attachment, do not put the plaintext passphrase in the same email.
- It's best to not use the same email systems for sending the passphrase as you used for the encrypted data. Specifically, avoid using the same sender account or the same recipient account, as a compromise of either account would mean that both data and passphrase are stolen at the same time.

[1] Even with the appropriate boxes checked, space characters are not used for the first nor last positions in the generated password, because that would just be asking for trouble.

- A common method of sharing a passphrase is a telephone conversation, if you can positively identify the person on the other end. We recommend using a good phonetic alphabet to avoid misunderstandings caused by background noise or telephone static.
- Prior agreements reached in face to face meetings are good ways of setting up a passphrase or passphrase scheme.
- Ideally, encrypt the passphrase itself, if the parties involved have an existing avenue of secure communication.

Some example scenarios of sharing a passphrase safely:

- An encrypted file is sent via Gmail to somebody with a government-issued CAC. The passphrase is encrypted using the CAC certificate and sent over a different system.
- Files shared among an in-house contracting team are encrypted with a passphrase built from the relevant contract number combined with a shared "secret".
- Project data passed between Team X at Company A and Team Y at Company B is encrypted with a passphrase agreed upon at the program kickoff meeting.

6 Encryption Wizard Archives

Archives simply place many files/folders into one encrypted file. Encryption Wizard archives are similar to WinZip or other file archive utilities, except that they are secured by strong encryption and reveal nothing about the files they contain. An Encryption Wizard archive is good for preserving folder structure, creating backups, sending many files, or when you need to reduce file size.

6.1 Select Files for an Archive

To encrypt files/folders into one archive (.wza) file, open Encryption Wizard and add files and/or directories to the main file list (see Section 3.1).

6.2 Create an Archive

Once the files are in the file list, select the file(s) to archive and click the "**Archive**" button in the bottom of the main window or press "**c**". Name the archive by entering a filename; a user may also select a path and filename for the archive using the "Choose File" button. If no location is given, the .wza file will be created on the Desktop (or your system's default location). Compression is enabled by selecting the "**Compress**" checkbox (see Figure Figure 14). The archive file is given a ".wza" file extension (e.g.: filename.wza).

Figure 14 - Archive File Name

6.3 Finish Archive

Keying material for Encryption Wizard Archives are selected in the exact same manner as other Encryption Wizard files (see Section 3.2). Likewise one may optionally add file metadata about the archive file (see Section 3.3).

There are several differences in creating an archive (.wza) over individual (.wzd) files. The archive file creation process does not give you the option to delete the original files. Once the archive is created, a simple "**Success**" window appears. The original files will remain listed in the EW file list window; the newly created archive file will not appear in EW's file list window.

6.4 Expand an Archive

To expand and decrypt an archive (.wza) file, open Encryption Wizard, select the file to expand, and select the "**Expand**" button or press "**x**". (In Microsoft Windows if "Installed" double-clicking the .wza file will take you through these steps.)

Next, specify the directory in which to expand the archive. The archive will be expanded to the specified directory while retaining the original file/folder organization (see Figure Figure 15).

You will then be asked to provide the keying material. The key material selection is the same as for decrypting a .wzd file (see Section 8.2). You will see a Success window when expansion and decryption is complete.

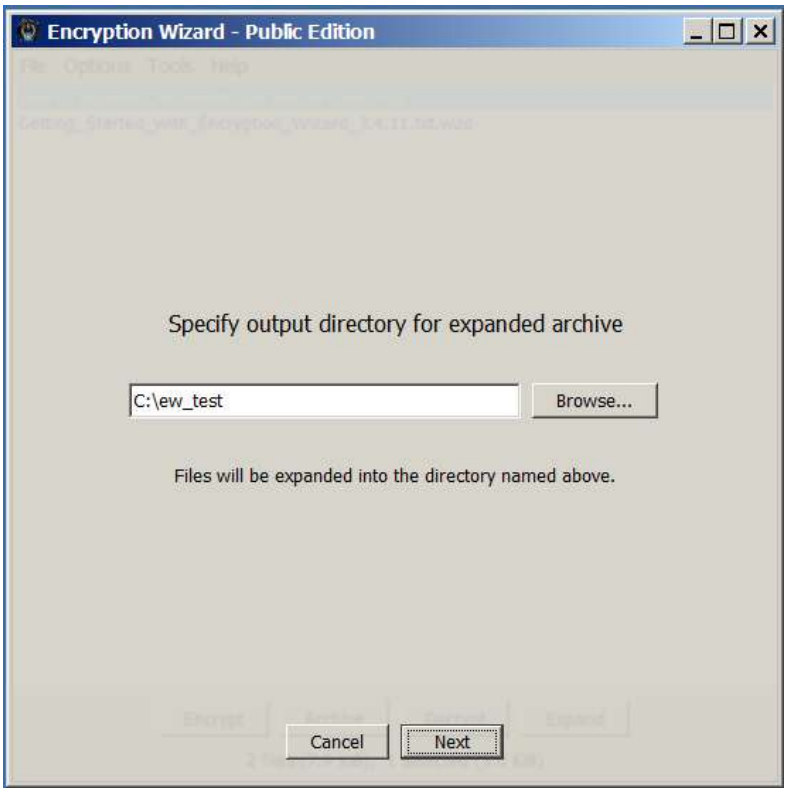


Figure 15 - Archive Expansion Location

7 Advanced Features

7.1 Upgrading Encryption Wizard Installations

If you have used the file-associated features on a Microsoft Windows computer (see section 7.8, "Optional 'Install' in Windows"), then we recommend that the tools be re-installed when a new edition of Encryption Wizard is placed on your computer. Running "Uninstall" on the older version, followed by "Install" on the newer version, is ideal. If the older version is no longer available, then simply run "Uninstall" and "Install" on the newer version, waiting for the confirmation popup in between. You may find shortcuts to the older version remaining in, for example, the Start Menu; these can easily be right-clicked on and deleted.

Before performing the "Install" step, we also recommend running the Encryption Wizard JAR file from its unpacked distribution folder, that is, the folder created when you unpacked the original .zip file. If the "Install" process finds a copy of the User Manual in the same folder as the JAR file, then the manual will also be installed and reachable via the Windows **Start Menu**.

7.2 Keychain

Keychains are a feature where users can securely store, neatly organize, and quickly access passphrases, public certificates, plus network and online account passwords. The Keychain stores this information within an encrypted file, the same way your own information is protected, and can be easily shared between people and organizations.

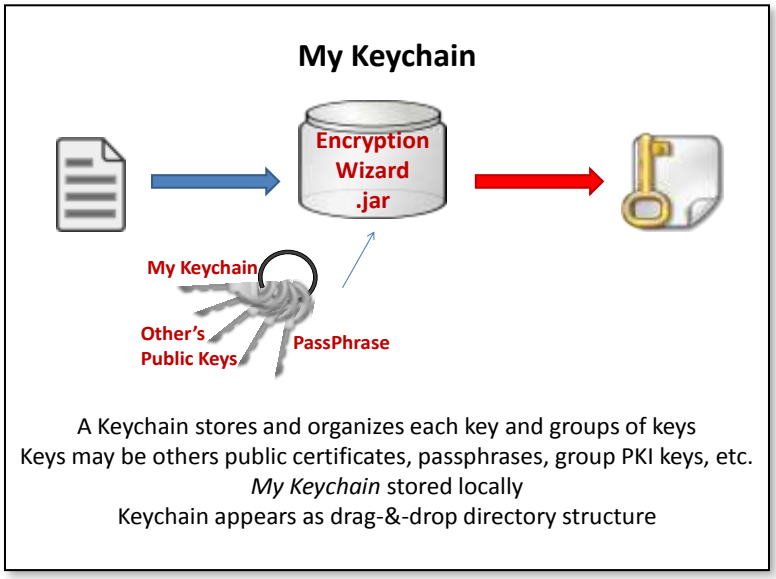


Figure 16 - Keychain Creation Process

7.2.1 Create a Keychain

Under the Tools menu, select "**Create a Keychain**" and then enter the name of your new Keychain (see Figure 16). You may create and use multiple Keychains simultaneously. Keychain names must be unique; EW cannot load two same-named Keychains.

7.2.2 Populate a Keychain

Keychains can be populated with eight different types of information or objects: Group, Person, Network, Computer, Website, Username, Passphrase, and Certificate (Cert). Each one may or may not contain the others to create a hierarchical tree. The active buttons at the bottom of the Keychain window as well as the context menu items generated by right clicking on an item will show which types can be added to that item. Objects in your keychain can be modified by using "**Edit**" and deleted using "**Delete**. All items in the Keychain window may be copy-pasted or dragged into different locations/objects or other active keychain windows.

Figure 17 - Keychain Creation Dialog

7.2.2.1 Group

Groups are used to represent organizations and communities (e.g. Alpha Flight, F22 Contract Review, ISR-4a Study Team, RYWA, and Skeet Team as shown in Figure Figure 18). Each Group may possess any other type of object except Username including sub-Groups (e.g. the RYWA Group has Testers and Developers). To add a Group, select "**Add Group**" from the Organizational menu or press "**G"** and enter the Group's name. To add a sub-Group, select the Group, select "**Add Group**", and enter a name.

Figure 18 - Keychain With Groups And Persons

7.2.2.2 Person

Persons are contacts that can be by themselves or be included in a Group. A Person can have a X.509 public certificate or a passphrase associated to it (see Figure Figure 18). To add a Person select a Group or the root and click "**Add Person**" under the Organizational menu or press "**P**". The contact information dialog box will appear. Enter the person's name, call sign, or nickname within the Name box and optionally fill in the other boxes. When done, click **"OK"**. These values can be viewed anytime by hovering the mouse pointer over the person in the Keychain window or by clicking edit on that person.

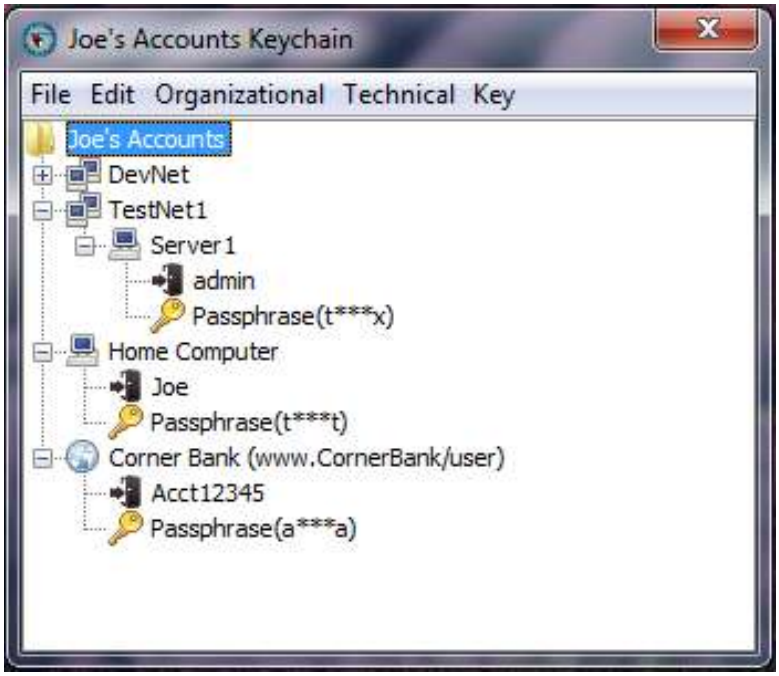


Figure 19 - Keychain With Network, Computer and Website Accounts

7.2.2.3 Network Account

A network account can be used to represent a single sign-on for a specific network or it can be used to group a number of computer accounts on the same network. A network can have a computer account, username, and/or passphrase associated with it (see Figure 19). To add a Network Account, select a Group or root and click "**Add Network Account**" under the Technical menu or press "**N**". A dialog will appear asking you to enter the name of the network that the account resides on. When done, click "**OK**".

7.2.2.4 Computer Account

A computer account is similar to a Network account. A computer account can have a username and/or passphrase associated to it (see Figure 19). To add a Computer Account, select the root, a group, or a network account and click "**Add Computer Account**" under the Technical menu or press "**O**". A dialog will appear asking you to enter the name or designation given to the computer that the account resides on. When done, click "**OK**".

7.2.2.5 Website Account

A website account can be used to store a website's name and URL to access it. A website account can have a username and/or passphrase associated to it (see Figure 19). To add a Website Account, select the root or group to add it to and click "**Add Website Account**" under the Technical menu or press "**W**". A dialog will appear asking you to enter the name of the website and the URL to access it. When done, click "**OK**". The URL can easily be copied so that it can be pasted into a browser window by selecting the website account and pressing **"Ctrl-c**" or right clicking and selecting "**Copy**".

7.2.2.6 Username

A username is the username or a reminder for a network, computer, or website account. To add a username, select a network, computer, or website and click "**Add Username**" under the Technical menu. Type the username or reminder in the dialog. Just like the website account the username can be copied by selecting the username and pressing **"Ctrl-c**" or right clicking and selecting "**Copy**".

7.2.2.7 Passphrase

Passphrases can be used to assign a passphrase to a group or person that can be quickly accessed when you wish to encrypt/decrypt a file or as the passphrase for a network, computer, or website account. To add a passphrase, select the type you want to associate a passphrase with, select "**Add Passphrase**" from the Key menu or press "**A**", and enter the passphrase in the passphrase dialog box. Upon selecting "**OK**", the Passphrase will appear with the passphrase obscured (e.g. first and last letter and remaining text replaced with 3 asterisks). To view the full passphrase, enable **Show keychain passphrases** under the **Options** menu (see Section 7.9.7). Even though the full passphrase is not shown, you may still copy it and paste it into a passphrase box and it will contain the whole passphrase.

7.2.2.8 Certificate (Cert)

To associate a certificate, select the Group or Person and click "**Add Cert**" from the Key menu, press "**C**", or right-click and select "**Add Certificate**". A dialog box will ask for a "**File**" (a soft certificate with a .cer or .x509 extension) or "**CAC/PIV**" to read your local smartcard.

Select "**File**" when working with Groups and Persons other than you. Browse to and add that certificate file. (To obtain other's certificates, see Section 3.2.3). The "**CAC/PIV**" button requires a smartcard and its owner and exports only the smartcard's public key to the Keychain.

7.2.3 Save a Keychain

When complete, save your Keychain. Select "**Save**", enter a filename, and then select the encryption key(s) (see Section 3.2). If this is your first time saving, Encryption Wizard will ask if you would like to make the key(s) your default keys. This allows you to save in the future without supplying a filename and encryption key(s) each time. To change the filename of your keychain or use different keys, simply select the "**Save As**" button to save your keychain. When successful, a dialog box will appear. If you have a smartcard, we recommend using both a complex passphrase and your CAC/PIV for keys. Only use others' certificates or share your passphrase if you want others to have access to your Keychain. If you attempt to close Encryption Wizard you will be warned of unsaved changes in each Keychain.

7.2.4 Share Keychains

You can create and share Keychain (.wzk) files with others. Generally, a .wzk file should be created for a group containing public certificates used by members of the group, members' own certificates, and mutually-known passphrases. Keychains with personal information should not be shared. The recipient should place the new .wzk file in the folder with their other .wzk file(s).

7.2.5 Use the Keychain to Encrypt File(s)

Once a Keychain (or several) are created, the keys they contain may be used to encrypt files/archives. To use a Keychain, select a file(s) to encrypt (see Section 3.1) or to archive. When the user has one or more opened, they will appear as tabs after the Cert File tab in the Key Selection window (see Figure 21). Select a tab, drill down through the Keychain directory until you find the certificates/passphrases of your chosen Group(s) or Person(s). Click on the certificate/passphrase you wish to use then select "**Add**". To add all of the subordinate certificates/passphrases within that Group or Person, select the Group (or Person) and select "**Add All**". You may select multiple certificates/passphrases by holding the **Ctrl key** as you select each one and then "**Add**" all of them at the same time.

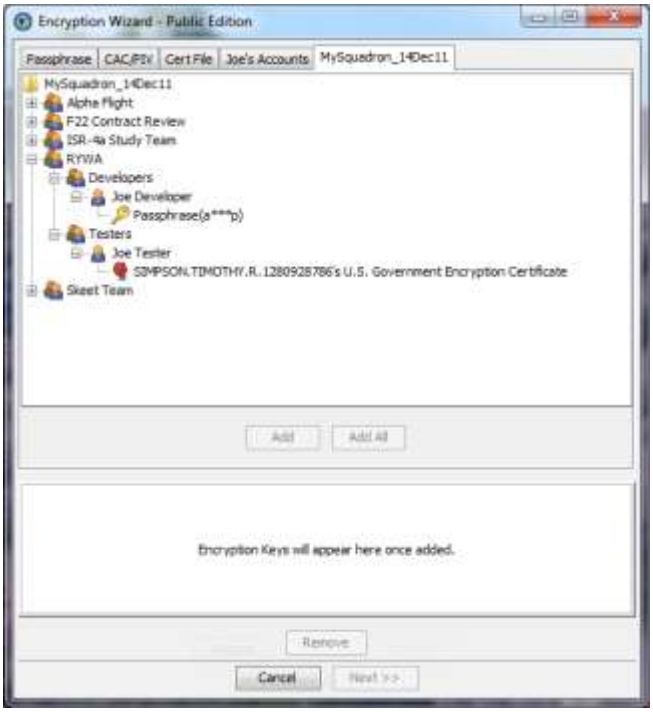


Figure 21 - Keychain Tab Within Key Selection Window

7.2.6 Open a Keychain

Upon start-up, Encryption Wizard will ask the user to open all Keychains (.wzk files) it finds in the same directory as the .jar file. To open a saved Keychain within another directory, select "**Open Keychain**" under the "**Tools**" menu (see Figure Figure 21), browse to the desired file, "**Open**", and enter a key to decrypt and load the Keychain. Your Keychain will appear in a new window and be available as a tab when you encrypt/decrypt.

7.2.7 Manage a Keychain

Under the **Tools** Menu, rollover **Manage Keychain** then select one of the listed, opened Keychains (see Figure Figure 21). The Keychain window will appear and you may add, delete, and edit its content. To retain changes, the user must "**Save**" and add the encryption keys again. All opened or created Keychains appear in the **Tools > Manage Keychains** menu until EW is closed. Closing the Keychain window itself does not close the Keychain.

7.2.8 Sort a Keychain

Each Keychain has the ability to be sorted. The default sort used is by object type. This sorts each level by its type thereby grouping all like objects together. If you would like to have your tree sorted alphabetically select the Alphabetical choice from the Sort menu under the Edit menu. This will sort each object in a level alphabetically by its displayed information.

7.3 Command Line

Encryption Wizard has command line counterparts for most GUI operations, allowing EW to be scripted, integrated into larger systems, or otherwise automated. Basic interaction is still supported, for actions like prompting for PINs or filenames. As a rule, only one primary action is allowed per command line session.

The command line interface (CLI) is completely rewritten with EW 3.4. Nearly all of the option letters/spellings are maintained from previous releases. Options consist of either a single hyphen and individual letters ("short options") or a double hyphen and a keyword ("long options"); users familiar with most CLI software installed on a typical Linux system will find this familiar. The generic CLI invocation looks like

```
java jvm_arguments -jar path/to/EW-xxx-3.x-xxx.jar EW_arguments
```

in which EW_arguments consists of options and/or filenames. (Here, "filenames" is used in the general Unix sense, including names of folders. A folder or directory on the command line will be expanded to include all its files.) Filenames and options may be interspersed, allowing command lines to be built up programmatically. Usually, EW can figure out which is which, but you can force it to stop looking for options and treat all following arguments as filenames with a double hyphen by itself, e.g.,

```
java -jar EW.jar -e -p mypass -- -this-filename-is-very-odd
```

If a filename starts with an @ character, it is treated as a "command file":

```
java -jar EW.jar [...] @more_args [...]
```

The contents of the command file (here, the file named "**more_args**") are treated as additional arguments to EW. The additional arguments take the place of the @file argument, and may be options, file/directory names, or even more command files (which will be recursively read and replaced). The arguments inside a command file are separated by whitespace. Whitespace characters can be included in an argument by quoting the argument with single or double quotes; any character can be passed through by prefixing it with a backslash. Note that on Windows, paths listed in a command file will typically need all their backslashes doubled (or replaced with forward slashes).

On a Linux system, the "**Tools**" menu includes an option to generate a wrapper script for CLI use. The script will invoke Encryption Wizard using the same Java JRE and EW jar file as was used to create the script[2]. In that case, invocation looks like

```
name_of_script  arguments
```

Nearly all options have both a short and a long form. They are synonyms as far as runtime behavior is concerned; use whichever spelling you prefer. Generally, short options are faster to type when you're using EW "by hand," while long options are self-documenting and can be useful reminders when you're running EW from an enclosing piece of software.

7.3.1 Note on Manual Text

For readability, this manual uses both short and long forms when naming options, and short options in examples. To save space, we use a plain "**ew"** as shorthand for CLI invocation. This should be understood to mean either a wrapping script or the complete "**java ... -jar ..."** form, described above. A dollar sign is used as a shell prompt and must not be typed as part of the command.

7.3.2 Options Listing

-a --archive[=ARCNAME]	Create an encrypted archive (in ARCNAME.wza ifgiven, or specified by **-t** if not)
-c --compress	Use compression for encryption and archiving
-d --decrypt	Decrypt files individually
-e --encrypt	Encrypt files individually
-G --genpass[=COUNT]	Print **a** (or **COUNT**) random password(s), then exit
-H --hash[=TYPE]	Print **TYPE** checksum for each input file
-h --help	Print this help and exit. Use **"-v"** before "**-h**" to see extended help for each option as well as additional/obscure options.
--help-explain	Print explanations and examples of using options and exit
-k --x509=FILE	Read X.509 certificates from **FILE**
-m --meta=FILE	Read/store file metadata in **FILE**
-o	Overwrite existing files unconditionally

[2] Advanced users or system administrators can edit the script to adjust the hardcoded paths or arguments. For example, suppressing the splash logo during startup.

-p --pass=PASSWORD	Specify a passphrase
-P --pin=PASSWORD	Specify a PIN/passphrase for unlocking private X.509 certificates
-q --quiet	Turn off all console output not strictly requested
-r --secure-delete[=HOW]	Controls secure file deletion; for details use: **--secure-delete=help**
-s --smart	Let the Wizard GUI decide what to do based on the input file names, then exit after completion
-t --output=PATH	Override default output location
--version	Print version information and exit
-v --verbose	Turn on additional output for whatever else is happening
-x --expand[=PATH]	Expand an archive (to **PATH** if given, or specified by **-t** if not)
-y --keychain=KEYCHAIN	Load KEYCHAIN during startup

7.3.3 Built-In Help

The most common options are described in **-h/--help** output, along with a few words of explanation. A full[3] listing of options is printed with the addition of the **-v/--verbose** option, and the explanatory text for some options is expanded as well:

```
ew -vh
ew -v -h
ew --verbose --help
...etc, etc
```

Some examples and additional notes about the CLI are displayed with:

```
ew --help-explain
```

It is recommended reading if you are new to the Encryption Wizard CLI.

7.3.4 Special Options

Most options map to GUI operations, and should be self-explanatory in conjunction with the rest of this manual. Those are not discussed further. Some options are unique to the CLI or offer more specific control than the GUI, as described below.

7.3.4.1 File Hashes

The **-H/--hash** option causes EW to calculate a file's checksum and then exit without doing anything else. This option may be repeated, specifying different algorithms; they will be printed in the same order as you gave them on the command line. Adding more **-v**'s adds more formatted output:

$ ew -Hsha512 -Hmd5 file*
file1: 44FFF39A19D4E2D...
file1: 8DD612CE4C15669...

[3] There are a very few options left undocumented, as they are meant for diagnosing EW itself; their exact spelling and behavioiur change often. End users may be directed by TENS personnel to pass these options.

file2: 5807F43726E34B2...
file2: A640423BFAA2429...
file3: 1D5A0CA83CFB565...
file3: DFEC1EE1A8CC696...

$ ew -Hsha512 -Hmd5 file* -v
file1 [SHA-512]: 44:FF:F3:9A:19:D4:E2:D...
file1 [MD5]: 8D:D6:12:CE:4C:15:66:9...
file2 [SHA-512]: 58:07:F4:37:26:E3:4B:2...
file2 [MD5]: A6:40:42:3B:FA:A2:42:9...
file3 [SHA-512]: 1D:5A:0C:A8:3C:FB:56:5...
file3 [MD5]: DF:EC:1E:E1:A8:CC:69:6...

$ ew -Hsha512 -Hmd5 file* -vv
/absolute/path/to/file1 [SHA-512]: 44:FF:F3:9A:19:D4:E2:D...
/absolute/path/to/file1 [MD5]: 8D:D6:12:CE:4C:15:66:9...
/absolute/path/to/file2 [SHA-512]: 58:07:F4:37:26:E3:4B:2...
/absolute/path/to/file2 [MD5]: A6:40:42:3B:FA:A2:42:9...
/absolute/path/to/file3 [SHA-512]: 1D:5A:0C:A8:3C:FB:56:5...
/absolute/path/to/file3 [MD5]: DF:EC:1E:E1:A8:CC:69:6...

The available hash algorithm names are listed with **-vh** or **-Hhelp/--hash=help** and are case-insensitive. As of this writing, they include MD5, SHA-1, and most SHA-2 variants; the SHA-3 algorithm (Keccak) has been recently specified by NIST but its support in Encryption Wizard depends on the version and edition. A special "algorithm" choice of 'user' (**-Huser/--hash=user**) may be given as a shortcut specifying a preconfigured list in the GUI.

When the hash output bytes are formatted into text, the choices of uppercase versus lowercase and which separator character (if any) is printed between bytes both default to the settings stored in the GUI. They may be overriden per invocation by **--hash-case** and **--hash-sep** options.

By default, **-H/--hash** assumes CLI text output. If using **-u/--usermode** to force GUI output, you will instead see popup dialogs containing the checksums. This is in fact how the "**EW File Hashes**" entry in MS-Windows "**Send To**" menus is implemented, and can be used on any platform.

7.3.4.2 Choosing Files By Pattern Matching

Certain shell environments are limited in their abilities to launch EW with a long list of input files. For example,

```
$ ew [options_or_actions] *.pdf
$ ew [options_or_actions] long/path/to/a/location/*.pdf
```

In a limited shell, the first command may fail if sufficiently many PDF files are present. The second command will fail earlier, at a lower threshold number of files, as each expanded path takes up more of the shell's permitted resources for argument capacity.

If you are launching the GUI with an initial list of files, one workaround is simply to name directories instead of files (e.g., "**long/path/to/a/location**"), allow EW to recursively expand the files, and then remove extraneous entries once the GUI is displayed. If this is infeasible, or if you are performing actions other than launching the GUI, then another possibility is to use the **-M/--match** option. This allows you to start EW within the limits of the shell, and EW will perform the expansion itself:

```
$ ew [options_or_actions] "-Mg:*.pdf"
$ ew [options_or_actions] "-Mg:*.pdf:long/path/to/a/location"
```

This example is fairly straightforward. The **"g"/"glob"** syntax should be familiar to most users. More complicated matching can be done with the "**r"/"regex"/"rexexp**" syntax, not described here.

Use **-Mhelp** or **--match=help** to see more information about syntax and restrictions.

7.3.4.3 Metadata

Rather than prompting for unencrypted metadata as the GUI is shown doing in Section 8.3, metadata on the CLI can be assembled ahead of time. The **-m/--meta** option takes a filename as its argument, and reads information from that file in a format based on Sun properties.

```
$ cat META.txt
# This line is a comment.
! So is this one.
title       This Is a Title
author = Mr. Equals Sign Is Optional, Esq.
comments:   as are colons
subject     How To Write Metadata
$ ew -e -p somepass -m META.txt example.dat
```

The filename argument can also be a specially-formatted expression of the form

```
{clause1 [; clause2; clause3...]}
```

where square brackets indicate optional clauses Each clause is of the form

```
X:value
```

and **X** is one of the following case-insensitive letters:

T Title field
A Author field
S Subject field
K Keywords field
C Comments field

The curly braces delimiting the expression will likely need special quoting or escaping to pass through your shell interpreter:

```
$ ew -e -p somepass -m "{T:Some Title; A:$USERNAME}" example1.dat
$ ew -e -p somepass -m '{C:Random keywords are funny}' example2.dat
$ ew -e -p somepass -m '{K:variable-speed corn muffins}' example3.dat
```

Whether from a file or the command-line directly, each of the metadata descriptors are optional, but at least one must be present (that is, the braces can't be empty and the file can't be blank).

7.3.4.4 Encryption With Random Passwords

When using **-e/--encrypt** or **-a/--archive**, an additional **option -g/--randper** can combine several steps of the GUI into one. The **-g** option takes an output filename as an argument. For each file being encrypted, EW will generate a random passphrase (Sections 12.4.6 and 14), add it as an encryption key (Section 8.2.1), and store the encrypted filename and corresponding passphrase in the output file.

For example, a professor with a PDF file intended for each of his dozen students could do:

```
   $ ew -e -g PASS.txt -k mycert.cer student*.pdf
   Loaded certificate from mycert.cer
   Encrypting 12 files
   Processing student01.pdf...
   == Success ==

   Processing student02.pdf...
   == Success ===

[10 more encryptions]

   $ cat PASS.txt
   9cxmBr[l     student01.pdf
   SZE5s%33     student02.pdf
[10 more passwords]
```

Now, the file student02.pdf.wzd could be decrypted by either the professor's own private key (the counterpart to the public half in mycert.cer) or by the passphrase "**SZE5s%33**". The encrypted files can each be transmitted over channels which are not necessarily secure (e.g., student email), and each student would need to obtain their own corresponding passphrase (hopefully by more than just a phone call to the department office, see Section 5.1).

If the **-k/--x509** option had not been used, nor the **-p/--pass** option to provide static passphrases, then each student's file would ONLY be recoverable with its random passphrase.

7.3.4.5 Secure Deletion

The secure deletion described in Section 7.9.4 is usable directly from the CLI with the **-r/--secure-delete** option. Specifying **-rexcl or --secure-delete=excl** will delete all the files listed on the command line using secure deletion, then exit without doing anything else.

Similar to the behavior of **-H** described above in File Hashes, you can use the **-u/--usermode** option to force a GUI popup dialog. This is how the "**Secure Delete**" action in MS-Windows shift-right-click menu is implemented, and can be used on any platform.

Use **-rhelp** or **--secure-delete=help** to see more information on the secure deletion technique.

7.3.4.6 Password Generation

The random password generator described in Section 14 is usable directly from the CLI with the **-G/--genpass** option. The generation parameters default to the same as those used in the GUI, including any changes saved by the user. The defaults may be overridden by using the **--genpass-param** option, passing either a file or a brace-enclosed expression as described in the **--help-explain** text:

```
$ ew -G --genpass-param=path/to/special/passgen.conf
BL:k%H5Rg
$ ew -G --genpass-param='{14,3,3,2,2}'
HiNzq_R0l0H=Nz
$ ew -G3
%XQtIs7:
6[M_w8Q4
L8Hp1qp=
```

7.3.4.7 Reading a Password From a File

Some situations in which **-p/--pass** would ordinarily be employed may preclude its use. In long-running operations on a multiuser system, it may be unwise to leave a plaintext passphrase visible in the process table. Different shells treat different characters as special, leading to surprising errors if you forget to quote the option or escape the individual characters. In circumstances like these, consider using the **--pass-file** option instead. The first line of the specified file is extracted, any leading and trailing whitespace is removed, and the resulting text is treated as if it had been passed using **-p/--pass**.

7.3.4.8 Platform Specific Actions

The operations specific to a particular platform (for example, the convenience features on MS-Windows in Section 7.8 and the Linux wrapper script generation in the introduction to Section 7.3) are also available for the command line using the **--run-platform** option. Barring permission errors, these will run entirely without interaction. Use **--run-platform=help** to see the available actions and their spellings for the current platform.

7.4 File Info (Hash)

You may obtain the MD5[4], SHA-256, or potentially other hashes of a file from the File Info option. EW provides other basic file information including name, size, created date and, if available, a .wzd and .wza file's unencrypted metadata (see Figure Figure 22 - File Info Dialog). To use, select a file and then right-click (or select **File Info** in the **File** Menu), or double-click a file. Because calculating hashes (checksums) is a cryptographic process, the windows may take several seconds to show those values.

[4] MD5 is still commonly used although it's been broken. AFRL recommends using SHA-256 hashes or better.

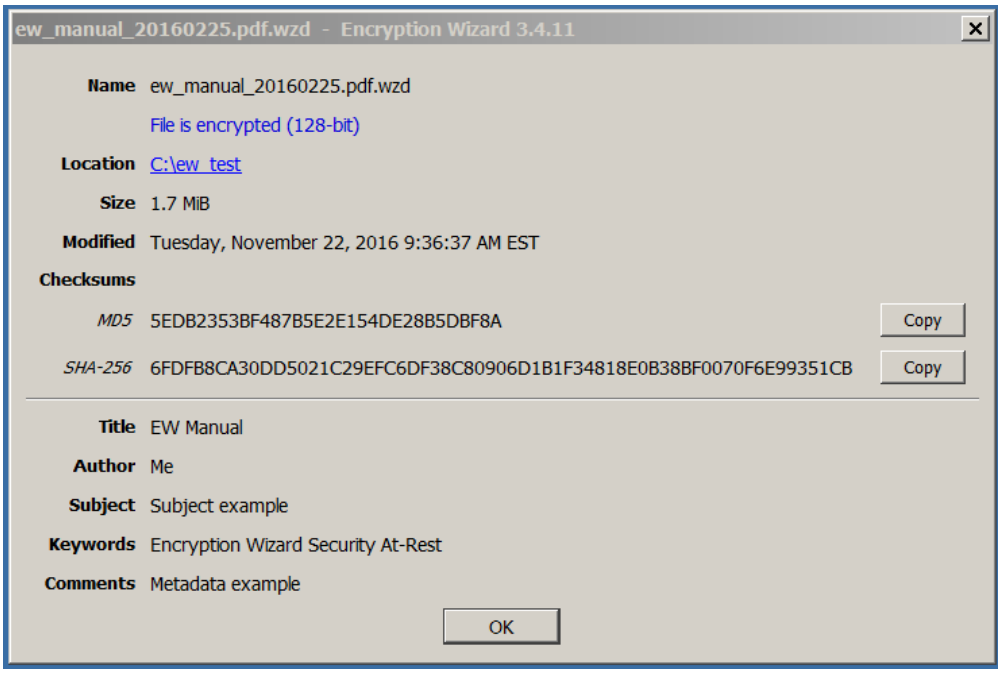


Figure 22 - File Info Dialog

Any of the information shown may be highlighted with the mouse for copying to the clipboard. The hashes may also be easily copied with the "**Copy**" buttons, as highlighting very long strings can be tedious and error-prone.

If you are running on MS-Windows and have performed the optional "Install" step, then this window is also reachable by right-clicking a file in Windows Explorer, opening the **Send To** menu, and selecting "**EW File Hashes**". Which hash algorithms are used may be configured in the Advanced Options.

7.5 Export CAC/PIV Certificate

If you have a smartcard, a smartcard reader, and necessary middleware installed, you may export your smartcard's public certificate using the **Tools** menu's "**Export CAC/PIV certificate**" option. (You would do this to share your public certificate with someone who would encrypt a file that only you may open.) To save the public certificate, select the option, enter one's PIN or Master Key, select a certificate from the card, pick a location, and Save with a filename with a .cer extension (e.g. Firstname_Lastname_Encryption.cer).

Encryption Wizard makes no attempt to export any private keys from smartcards, as this is typically prohibited by the middleware in any case.

7.6 Hotkeys

Hotkeys provide a quick way to access the main features of Encryption Wizard. To use a hotkey, simply type the hotkey while the Encryption Wizard window is the active window. Hotkeys are underlined in menus. Not all hotkeys work on all operating systems.

a	Add files to the file list

c	Archive the selected files in the list
d	Decrypt selected encrypted files in the file list
e	Encrypt selected unencrypted files in the file list
g	Generate passphrase
i	Open File Info (hash) window
l	Access the Encryption Wizard log
q	Quit
F5	Refresh list
s	Open System Information Window
x	Expand the selected file in the list
Del	Remove selected file(s) from the file list (except on Mac)
F1	Access the help system
Ctrl-A	Select all the files in the file list
Esc	Deselect all files in the file list

This list is not exhaustive; additional hotkeys will typically appear in menus as they are displayed (but this is specific to the OS and window manager).

7.7 About Window

The About window describes your specific version/build (see Figure 23). It is found under **Help** on the main window's menu bar. In all builds, the program office logo background is retained here.

Figure 23 - About Dialog

The exact content of the window can vary quite a bit for custom editions. Escrow keys, the FIPS module, specific helpdesk or contact information, can all appear here.

7.8 Optional 'Install' in Windows

The following features are limited to Microsoft Windows.

EW supports an "Install" feature that sets up file associations, creates an Encryption Wizard directory with a copy of EW-xxx.jar, and adds a "**Send To**" feature. A new EW folder and shortcut are added to the Windows **Start Menu**. If the User Manual is present in the same folder as the JAR file (that is, the file you double-clicked to start the copy of EW performing the install), then the manual will also be copied and its own **Start Menu** shortcut created.

These changes apply only to the current user's account. Although not yet observed, this feature may require administrator rights on some configurations.

To "Install" Encryption Wizard in Microsoft Windows select "**Tools**" from the toolbar and select "**Install**" (see Figure 24). To "Uninstall" Encryption Wizard select "**Tools**" and select "**Uninstall**".

Each time a new Encryption Wizard version is obtained, it should be re-Installed. This is easily done by opening the newest version of Encryption Wizard, selecting "**Uninstall**", waiting for a confirmation, selecting "**Install**", and again waiting for a confirmation.

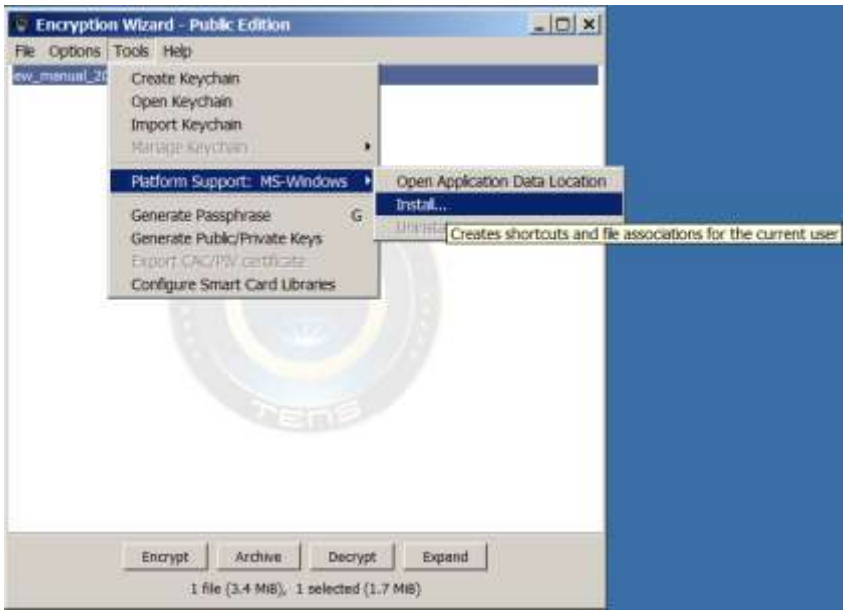


Figure 24 - Install/Uninstall Menu Options

7.9 Options

Encryption Wizard includes a number of configuration options that will be stored in the user's application preferences directory (see Figure 25).

Figure 25 - Configuration Menu Items

7.9.1 Show Name Only

When selected, the files listed will not show the directory structure. For example, with "**Show Name Only**" unchecked a file within a directory structure might appear as "**MyFolder\Files\Text.txt**". If "**Show Name Only**" was checked it would show "**Text.txt**".

7.9.2 Ask/Keep/Delete Files

Versions of Encryption Wizard prior to 3.1.1 would encrypt and decrypt files "in place" - if a file was encrypted, the original unencrypted file was deleted; conversely, if a file was decrypted, the originally encrypted file was deleted. This option was added to permit the user to select one of three options:

- Always delete the original form of the file (default behavior for versions < 3.1.100)
- Always keep files
- Always ask about removing the original form of the file (default behavior for versions > 3.1.100)

7.9.3 Show Encrypted First

This option changes the order of files presented within EW's primary window. If selected, first all encrypted blue files and then all black unencrypted files will be shown. If not selected, files will be shown in alphabetical order.

7.9.4 Secure Delete - Selecting Delete Behavior

Versions of Encryption Wizard >=3.2.4 include the option for performing a more secure delete. The method consists of overwriting all file locations three (3) times: first time with a character, second time with its complement, and the third time with a random character. Only advanced technical (laboratory) means *might* be able to recover files after a secure delete.

If you are running on MS-Windows and have performed the optional "Install" step, this may be performed on any file outside of the encryption/decryption process. Holding the **Shift key** while right-clicking on a file in Windows Explorer will allow "**Secure Delete**" directly.

7.9.5 Disabling the Metadata Request Dialog

Encryption Wizard version 3.2.9 and later disables the metadata request dialog (see Section7.3.4.3) unless you check this option.

7.9.6 Ask For Output Location

When files are encrypted by Encryption Wizard, the default behavior is to create a file in the same file location with a .wzd or .wza extension added to the original filename. When a file is decrypted by Encryption Wizard, it removes the .wzd or .wza extension from the filename and places the new file in the same file location as the encrypted file. This poses a problem when the original file is in a location that the user does not have write access to such as a finalized CD/DVD or when the user does not wish to have the file have the same filename. Encryption Wizard allows the user to select the new file's location and filename by toggling the "**Ask for output location**" option. When a user encrypts or decrypts a file, a file location window will appear in the wizard that will allow the user to enter a directory and/or filename for the new file. If a directory is entered for a file(s) then Encryption Wizard will still add/remove the .wzd extension to the original filename. *(Versions of Encryption Wizard prior to 3.3.6 labeled this option* "**Ask About File Saves**".*)*

7.9.7 Show Keychain Passphrases

When enabled, the user will be able to see the full passphrases stored within the Keychain (see Section 7.2.2.7). By default, these are obscured as to mitigate shoulder-surfing and screen-capture malware.

7.9.8 Configure Smart Cards

Encryption Wizard comes configured with a few standard PKCS#11 libraries for Windows, Linux, and Macintosh operating systems (see Figure 26). The location of these libraries is based upon the default install location or Air Force SDC location for that smartcard middleware.

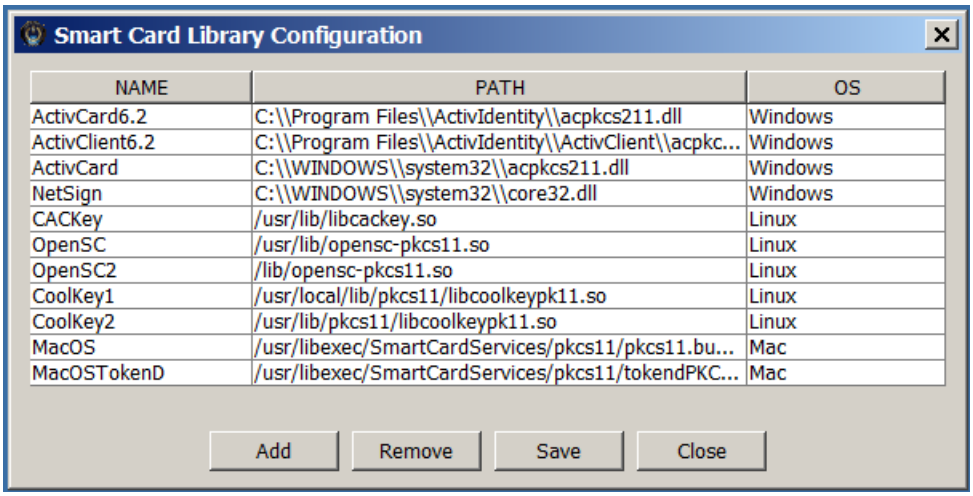


Figure 26 - Smartcard Configuration Dialog With Default Configuration

If the user's smartcard middleware was installed in a custom location or they are using a different PKCS#11 middleware library, Encryption Wizard allows the user to add that library to the current configuration and save it to the application directory. The saved configuration will then be loaded by Encryption Wizard during each startup. To do this, select "**Add**" and fill in a unique provider name, the operating system, and the filename of the PKCS#11 library (see Figure 27). You can either type this filename or "**Browse...**" to the file to select it. Select "**OK**" to add this library to the table and then select "**Save**" to save this configuration (see Figure 27).

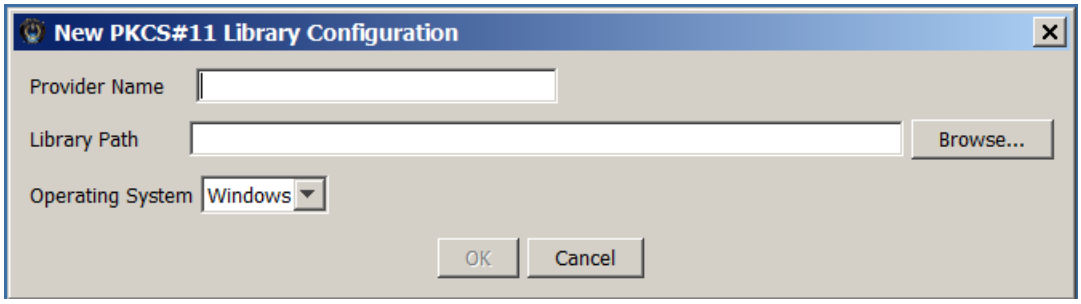


Figure 27 - Add PKCS#11 Library Dialog

Users can also delete libraries from the configuration that they don't want Encryption Wizard to use or check when looking for smartcards to access. To use, select the row in the configuration that you wish to remove and select "**Remove**" (see Figure 26). To go back to the default configuration, search for the smartcard.cfg in your application directory and delete it.

7.9.9 Using AES-256 or SHA3 Hashes

Some unusual features or obscure behavior can be adjusted through the "**Advanced Options...**" dialog. The choice of tabs in this window may change depending on the version and edition of Encryption Wizard, but typically users can choose to enable 256-bit encryption (if this has been previously unlocked, see Section 2.1), and select which hashing algorithms should be performed when displaying file info (see Sections 7.4 and 7.3.4.1).

Appendix A: Decrypting Files Encrypted With a Previous CAC

NOTE:	This documentation is supplementary and is not fully tested across the DoD

This document describes how to obtain expired or retired personal DoD PKI certificates from the escrow facilities at DISA, and use them to open files encrypted with the older PKI certificates with Encryption Wizard.

Summary of steps:

1. Obtain older PKI key from escrow
2. Prepare key for use with Encryption Wizard
3. Use with Encryption Wizard

1. Obtaining personal DoD PKI certificates

There is both an automated and manual process. Full instructions and assistance can be received from your agency/service PKI helpdesk. Follow directions here:
https://afpki.lackland.af.mil/html/keyrecovery.cfm

2. Preparing an escrow certificate for use with Encryption Wizard

- You must first import the escrow key into Internet Explorer, and then export it into PKCS#12 (".PFX") format to use with Encryption Wizard.

2.1. Follow the instructions provided by the Air Force PKI Office to import the certificate into Internet Explorer: https://afpki.lackland.af.mil/assets/files/CI-09-07-001_Automated_key_Recovery_v1230.pdf. These instructions are linked from the PKI page above.

There is one small but important change to the instructions:

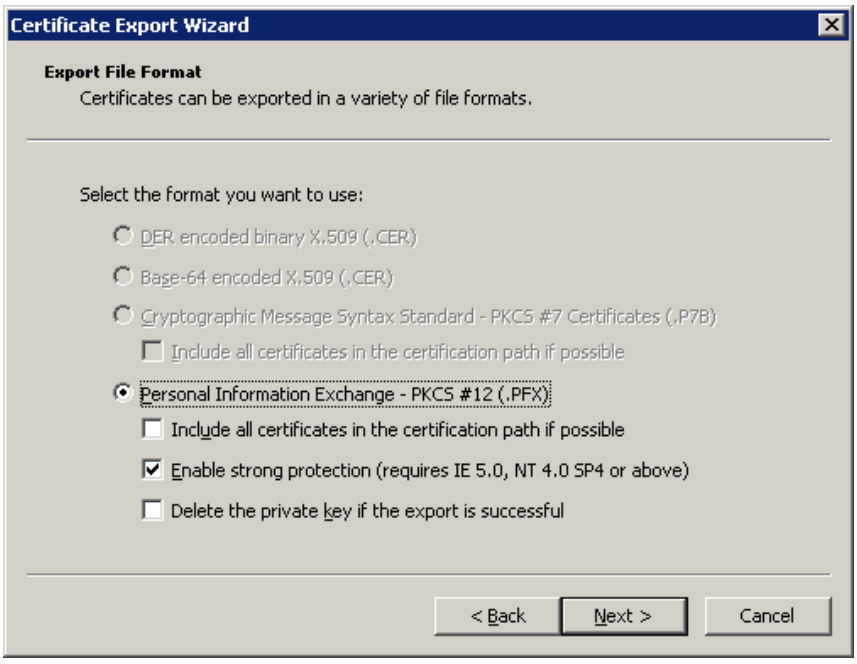
2.1.1. On page 26, you must enable the option of re-exporting the private key. (Which is the entire point of Appendix A.)

2.2. Export the Certificate from Internet Explorer to **PFX** format

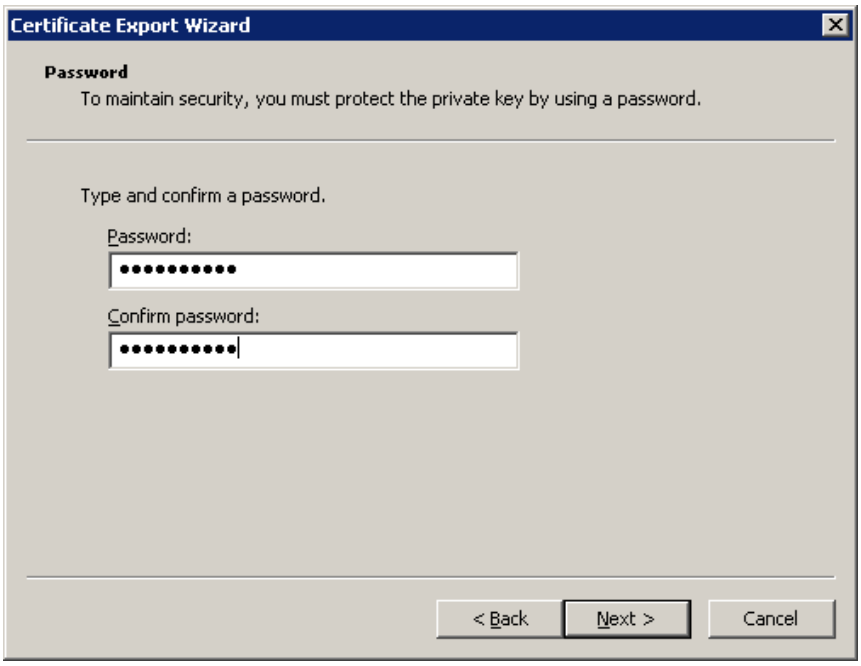
2.2.1. Open IE; Select **Tools->Internet Options**; click **Content** tab; click **Certificates**; Select escrowed certificate; Select **export**

2.2.2. Export Private Key? **YES**

2.2.3. Save as **PFX** file - use options as shown (the exact options will vary depending on your version of Windows)



2.2.4. Choose a password - this will be the password you use inside Encryption Wizard each time you decrypt using the recovered key. EW does not use the 16-character password generated by the DISA website, nor the password you created when importing the key into Internet Explorer. (You may of course reuse either of those passwords here.)



2.2.5. Choose a filename that makes sense

2.2.6. Click **Finish**

2.2.7. Next, use the passphrase you created back in Page 31 of the AF PKI guide (when importing the DISA certificate into Internet Explorer)

2.2.8. All Done

3. Use exported PFX key with Encryption Wizard

3.1. Open the file encrypted with the old PKI key in Encryption Wizard (see Section 4 for further help)

3.2. Select "**Decrypt**"; select "**Cert file**" tab; select "**Location**" (see Section 3.2.3 for further help).

3.3. Select the PFX file exported in step 2.2.5 above.

3.4. When prompted for a password/PIN, enter password you selected in step 2.2.4.

3.5. Select the private key (the name will be gibberish) and select "**OK**"

3.6. If prompted for a password/PIN again, re-enter the same password.

4. Cleanup and Reminders

If you do not need the recovered key other than for Encryption Wizard decryption, then it is best to remove it from the Windows/IE Certificate storage. The .pfx file you originally saved from the DISA website should also be deleted securely.

Don't confuse the passwords! Three are involved here:

- The 16-character DISA website password, used only during import.
- The password created during import, used during export. This is also used by Windows to read encrypted email.
- The password created during export, used by EW.