Users Guide
Professional Data Security (PDS)

http://crypto.brettlee.com

CONTENTS:

==========

1. Install the Application

==========

You have two choices:

- Manual installation (Recommended)
- Java Web Start (JWS) installation.

Manual: Download the Zip file and extract the contents to disk. If you plan on running the PDS from a thumbdrive, copy the file "pds.jar" to your thumbdrive. Do not execute the application (JAR) from the Zip file. While the application will "work" from a Zip file, you will lose portability between systems. Please see the Release Notes -> Known Issues for additional details.

Java Web Start: Ensure that JWS is installed on your system and select the appropriate JWS link to install PDS using JWS. Two types of JWS installs are provided: one to install a specific release and run that version only; another to install the latest release and have JWS periodically check for and install newer releases. Note that:

- JWS installs performed on disparate systems often define application directories differently, thus making interoperability slightly more difficult. The application provides the ability to default application directories; that and familiarity with the application resolve these issues.
- JWS doesn't appear to be the most dependable component of Java. For that reason, many people have given up delivering applications with JWS.

2. Initial Configuration

On startup, PDS creates directories for both KeyStores and Encrypted Files. These directories are .../mydata/mykeys and .../mydata/myfiles. If you used the manual installation, these directories are relative to the application (pds.jar). If you used the JWS installation they also may be in your home directory or your desktop. If you are using Windows, they also might be in C:\ or in you "Documents and Settings" folder; thanks JWS. :)

If you prefer, you may redefine these directories by selecting Tools -> Options from the drop down menu (or use the Accelerator Key F8). The first tab of the Options menu provides this ability (see Figure 1 below).

* For a complete list of Accelerator Keys, see Help -> Help Topics (or F1).

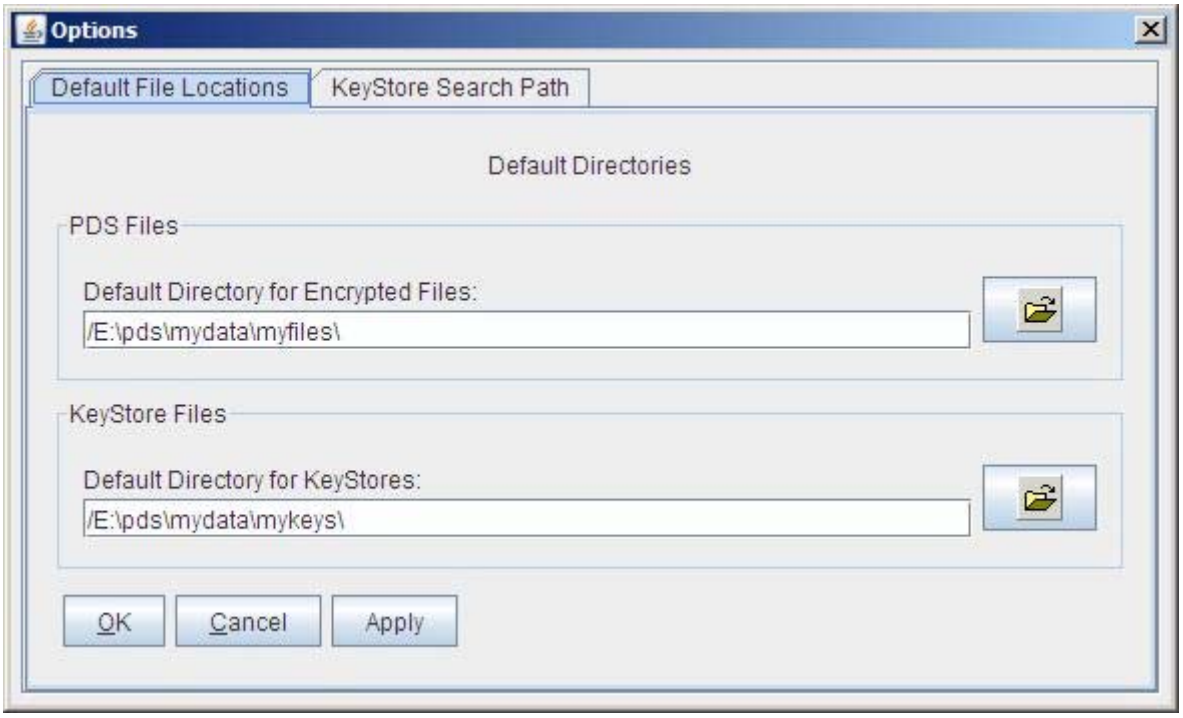

Figure 1 - Define Default PDS Directories

When creating or editing a file, the absolute path to the location of the KeyStore/Key is saved as metadata within the file. The next time the file is decrypted PDS searches for the KeyStore in the last known location. If you are using PDS from multiple computers, or you have an advanced PDS configuration, you may have KeyStores in several locations. To have PDS search several locations for the correct, add these search paths to the second tab

of the Options menu (see Figure 2). If the key is not found in the original location but is found in one or more locations in the alternate paths, you may then select the path you wish to use. Note that if the key is not found in either of these, you will be provided a dialog to browse for the KeyStore.

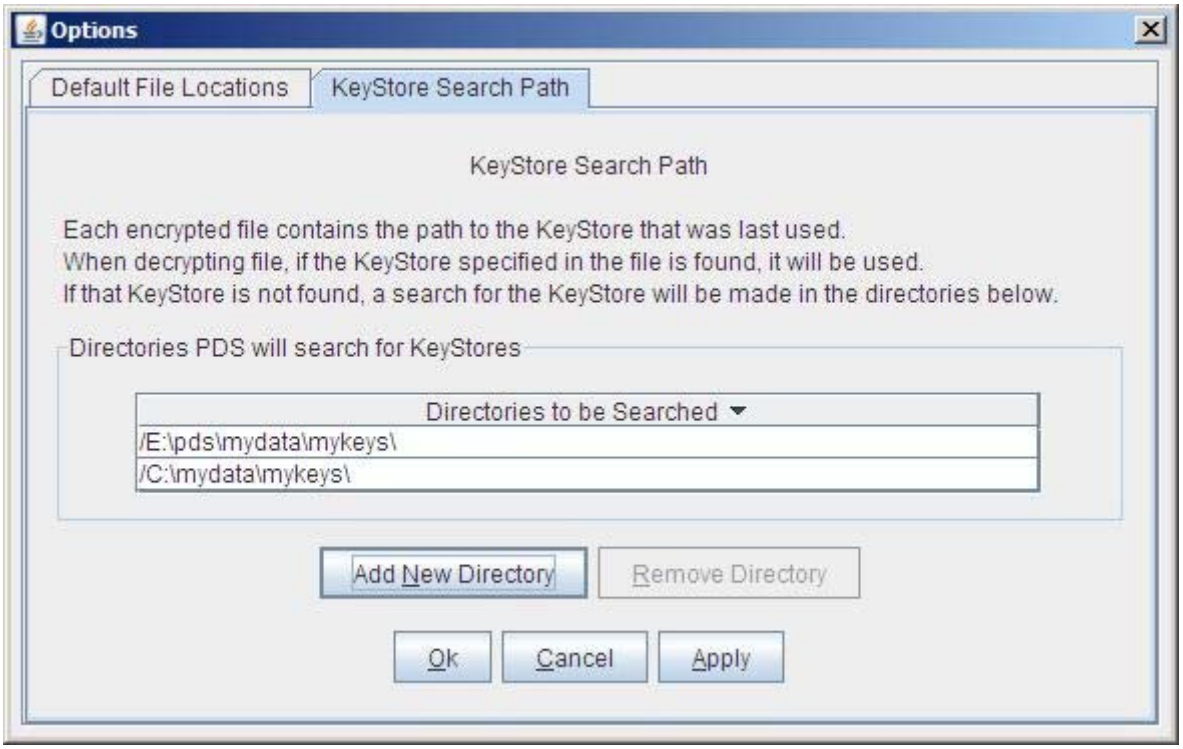

Figure 2 - Define Alternate KeyStore Search Paths

3. Create a KeyStore
==========

Now that we have our default file locations defined, it is time to create a KeyStore.

Select File -> New -> KeyStore (see Figure 3)

Figure 3 - Create a KeyStore

The Create New KeyStore dialog will pop-up (Figure 4).

- If you will be creating the KeyStore in the default directory, type in the name of the new KeyStore. Otherwise, click the Folder icon to navigate to the location where the KeyStore will be created and then provide the name.
- Type in the passphrase and confirmation passphrase and select Create to create the new KeyStore.

Should you wish to edit the passphrase of a KeyStore, the File -> Edit -> KeyStore -> Change Passphrase option provides this ability. Please see below for details.

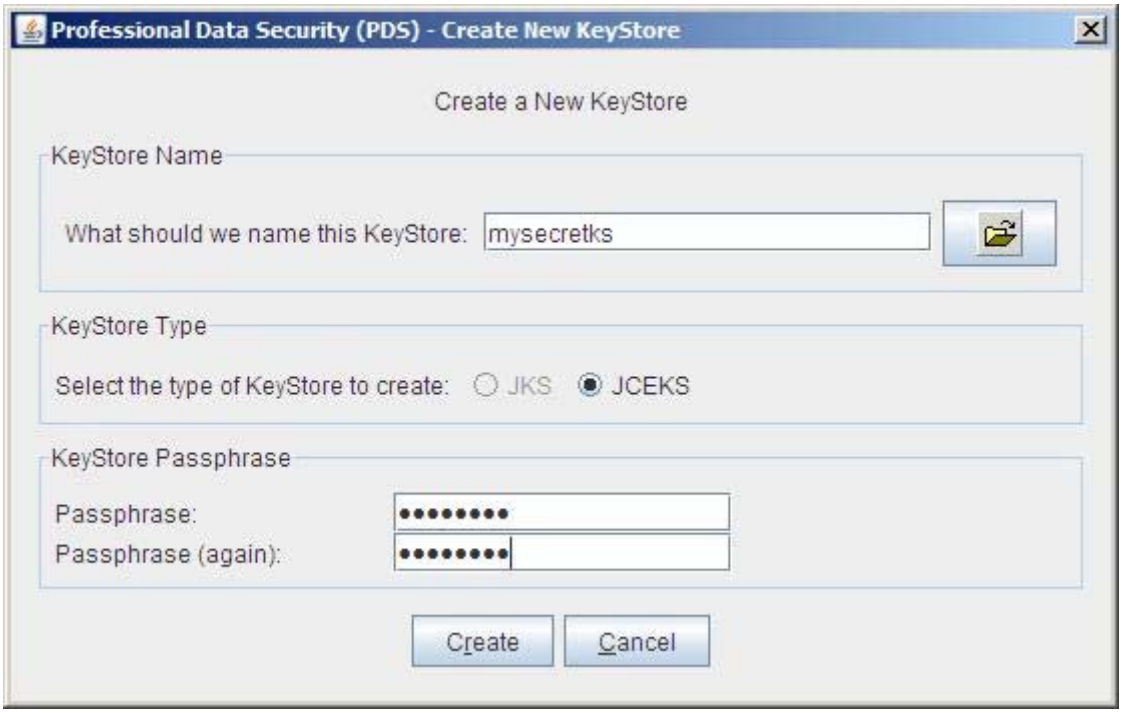

Figure 4 - Create new KeyStore dialog

4. Create a Key
==========
Now that we have a KeyStore created, it is time to create an Encryption Key.

Select File -> New -> Key (see Figure 5)

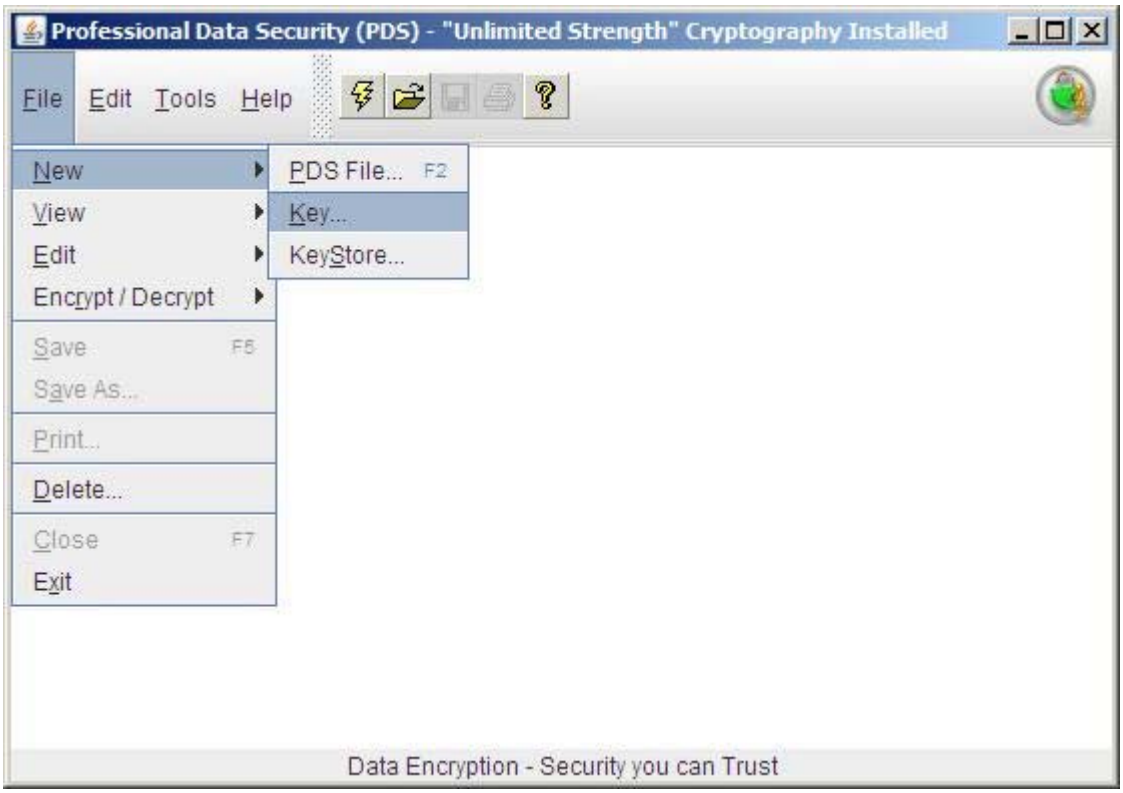

Figure 5 - Create a Key

The Create New Encryption Key dialog will pop-up (Figure 6).

- Type in the Key Alias that will refer to the new Key.
- Click to select the type and strength of the new Key.
- Type in a passphrase and confirmation passphrase for the new key. Note that the Key passphrase may be the same as the KeyStore passphrase. This simplifies things greatly, but it is also less secure.
- Associate the Key with a KeyStore by clicking the File Chooser in the KeyStore Association area. Provide the passphrase for the KeyStore.
- You may make this key the default key. Having a default key simplifies the creation and encryption of files.
- Select Create. Your KeyStore now holds one Encryption Key.

Should you wish to edit certain properties of your keys, the File -> Edit -> Key option allows you to redefine the default key, change the passphrase of a key, and also delete a key. Please see below for details.

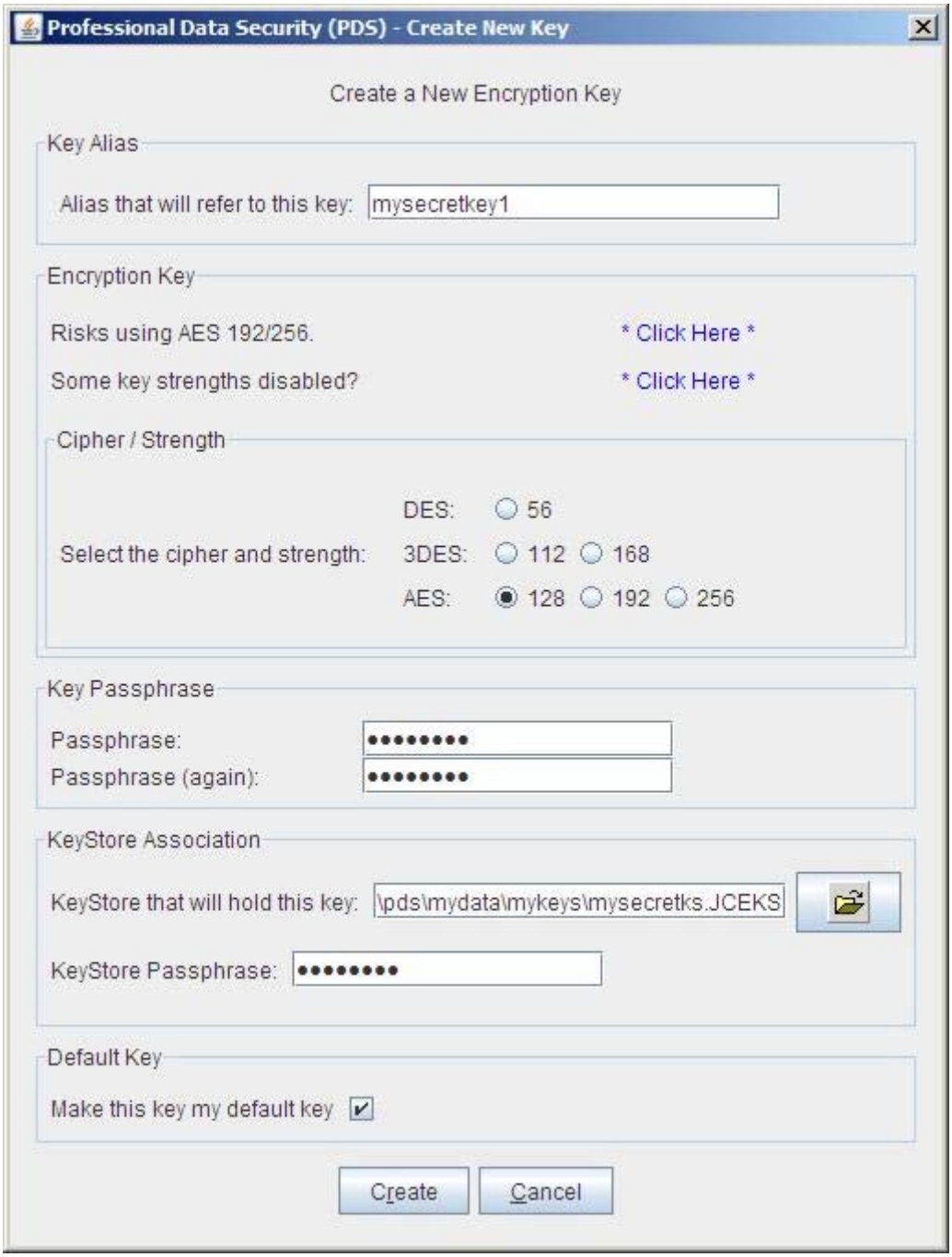

Figure 6 - Create new Encryption Key dialog

5. Create a PDS File
==========

Select File -> New -> File from the menu. Note that you may also use the Accelerator Key F2 or select the Lightning Icon from the toolbar.

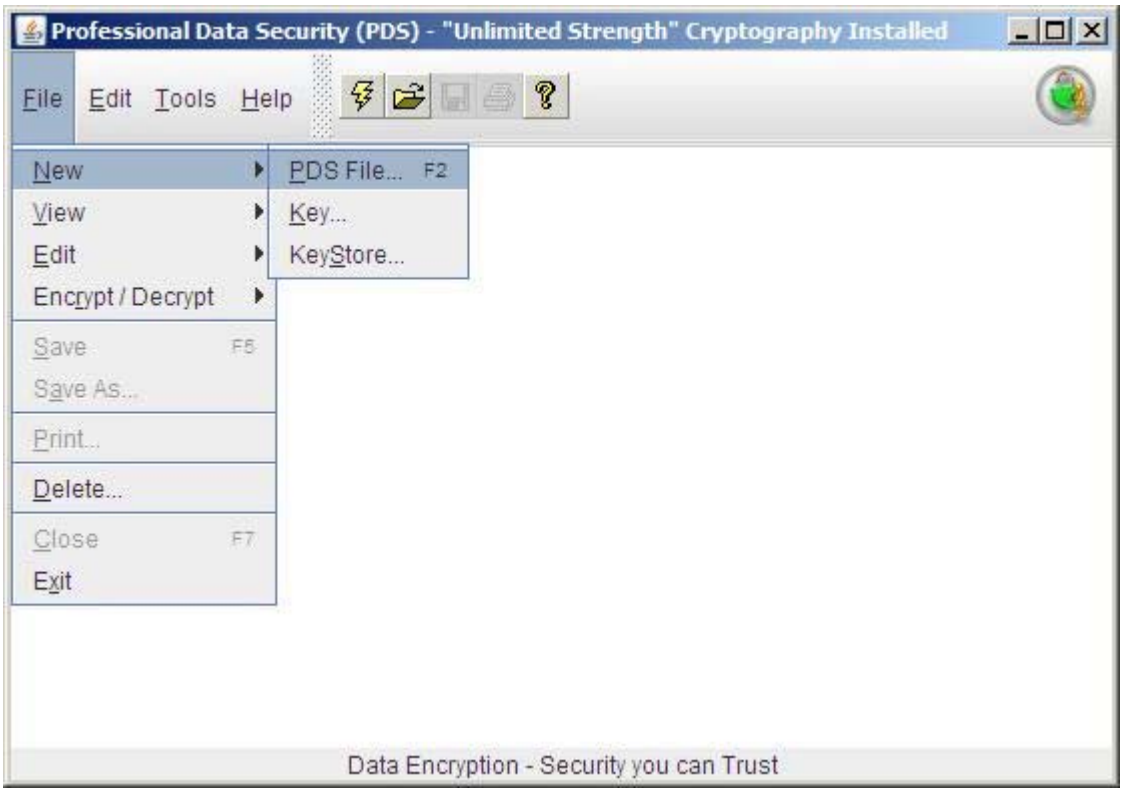

Figure 7 - Create a PDS File

The Create New PDS File dialog will pop-up (Figure 8).

- Type in the name of the new file.
- If you are using the default key, select Create. Otherwise, ensure that the "Use My Default Key" is not selected, use the Folder icon to navigate to the KeyStore, provide the passphrase for the KeyStore, and finally select the Key. You will then return to this menu with the new KeyStore and Key Alias fields populated; click Create to create the new file.
- An authentication dialog (Figure 9) will pop up. Provide your credentials and select Accept.

Figure 8 - Create new PDS File dialog

Figure 9 - Authentication dialog

Congratulations!!! You have created a PDS file (Figure 10). You may now enter your confidential data into this file and securely save it to disk.

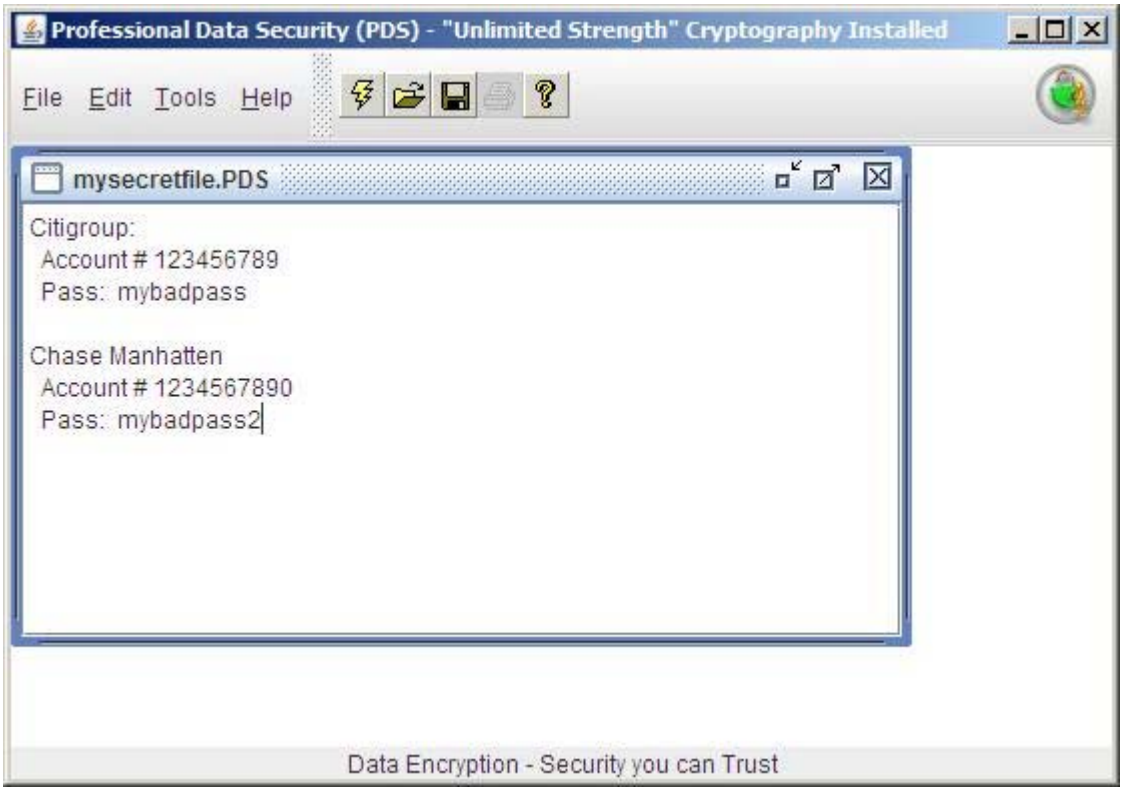

Figure 10 - Our new PDS file.

Note that the above type of file may be referred to as a PDS file, an internal file or a native file. Files of this sort are limited in size and are meant to support only ASCII bytes. Further, these files are written with an ASCII header followed by the encrypted bits encoded as Base64. These are the only types of files that the PDS editor currently supports. The clarification above is brought up because PDS may also be used to encrypt any existing files that you have. PDS refers to existing files as "external" files.

When working with internal files, the overhead of converting 128-bit ASCII to Base64 is negligible due to the limited size of the files. However, when encrypting external files there are no known application limits to the type and size of files that PDS supports. For this reason, the default option when encoding encrypted external files is not Base64 but Binary. Like the internal files, external files also have a ASCII header.

Note that should you wish, you may encode an external file using Base64. While not

practical for large or binary files, encoding a plain text file as Base64 and then carefully editing the header will allow the PDS editor to support the file as an internal (size limitations).

Similarly, internal files may be decrypted to simple ASCII files using the decryption option for external files.

6. Encrypting and Decrypting External Files

Select File -> Encrypt / Decrypt -> "Encrypt or Decrypt" (see Figure 11).

Note that when encrypting or decrypting an external file, the source is never modified or deleted. Also, a confirmation prompt will be issued prior to overwriting any files.

Figure 11 - Encrypt / Decrypt Files and Directories

The Encrypt an Existing File dialog (Figure 12) follows a similar format as the previously reviewed dialogs. The differences are the destination for the encrypted file (four options) and the encoding format (discussed previously). Note that the option to write to tape is not

supported on Windows; appending is supported only via a non-rewinding device file.

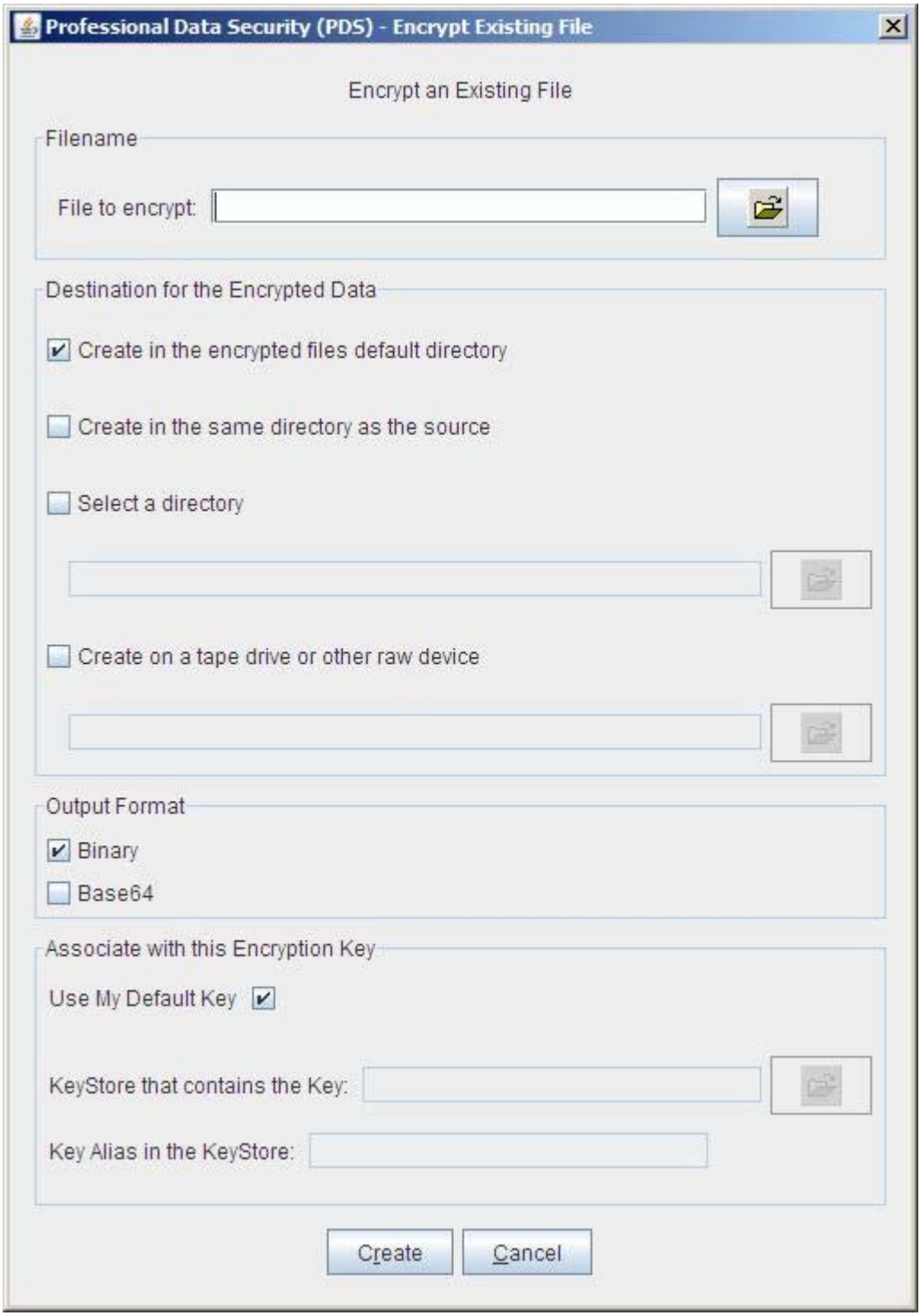

Figure 12 - Encrypt an Existing File.

The Decrypt a PDS File dialog (Figure 13) follows a similar format as the previously reviewed dialogs.

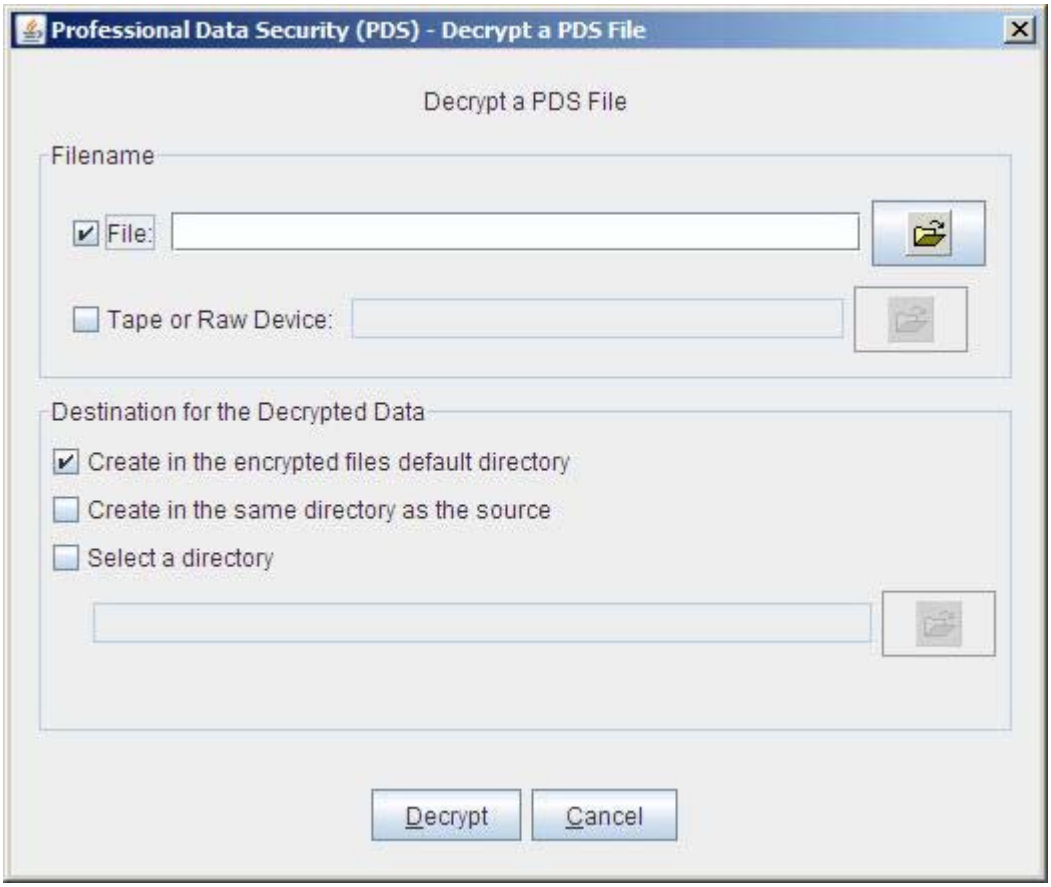

Figure 13 - Decrypt a PDS file.

The Encrypt an Existing Directory dialog (Figure 14) follows a similar format as the previously reviewed dialogs. The difference here is that a level of compression may be selected. When encrypting a directory, the contents are packaged in ZIP format, optionally compressed, and then encrypted.

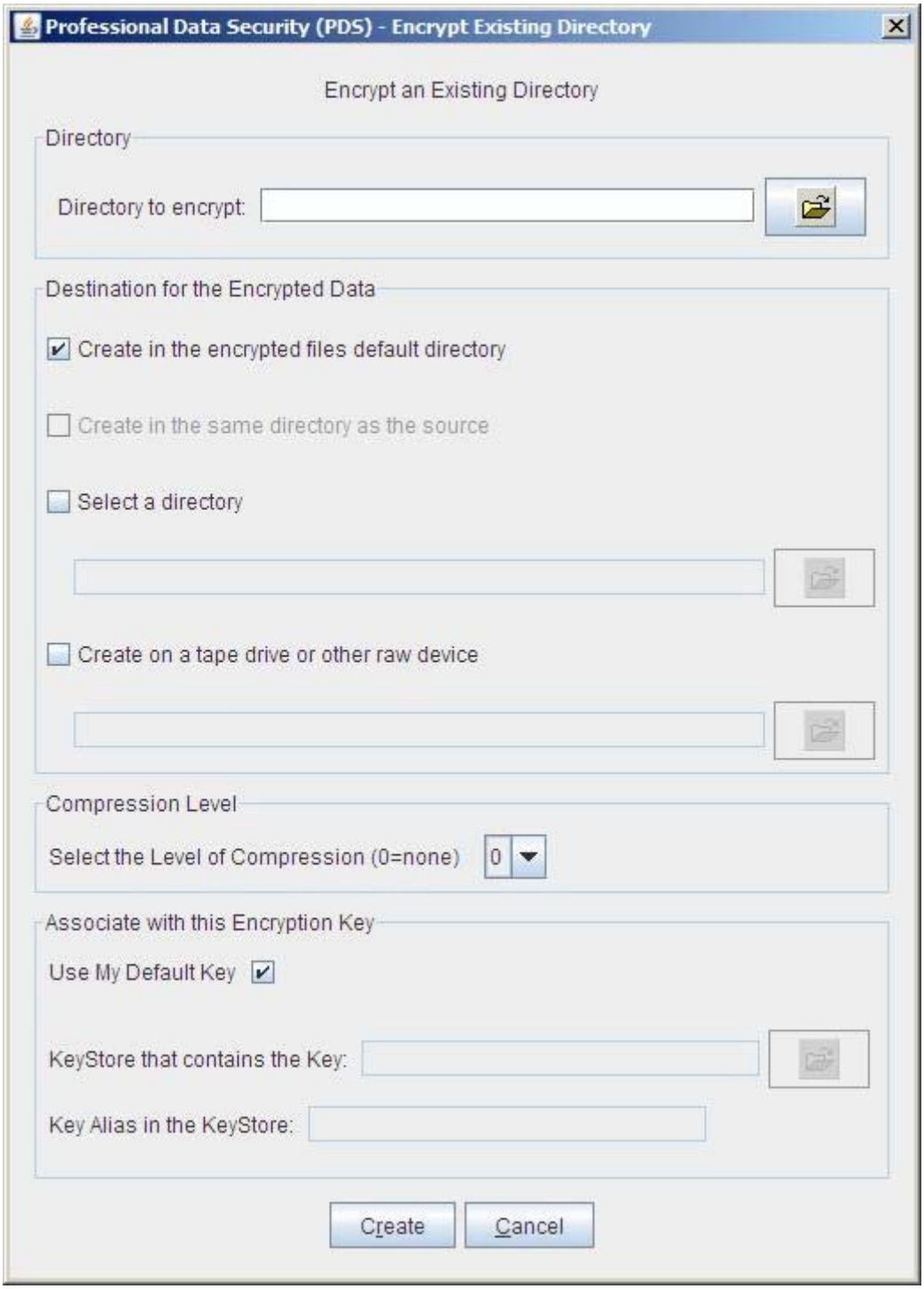

Figure 14 - Encrypt an Existing Directory.

The Decrypt a PDS Directory (Figure 15) follows a similar format as the previously reviewed dialogs. The difference is that the Encrypted Directory may either be decrypted

and written with the directory structure recreated, or it may be decrypted and written written as a single ZIP file that maintains the directory structure and can be extracted some time in the future.

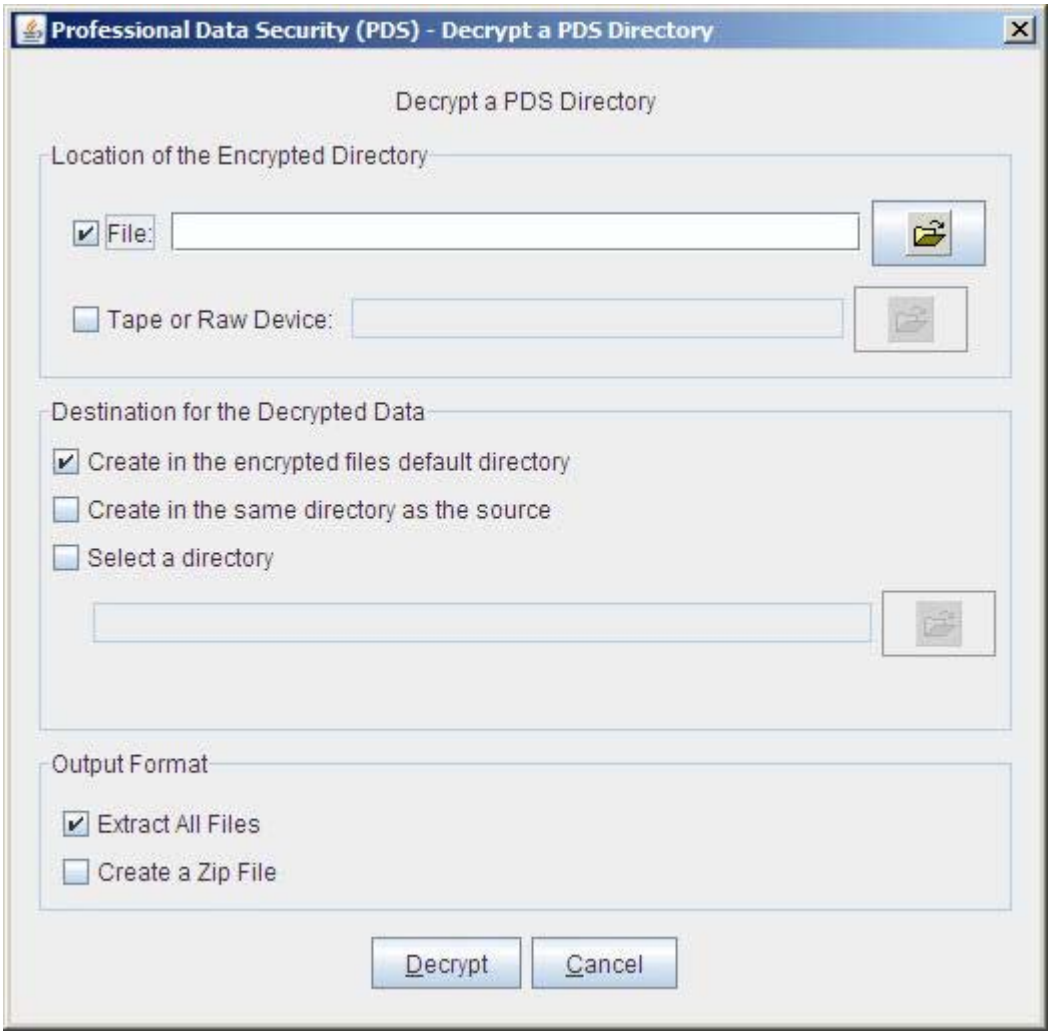

Figure 15 - Decrypt a PDS Directory.

7. Modify KeyStore Passphrase.
==========

Select File -> Edit -> KeyStore -> Change Passphrase (see Figure 16).

Figure 16 - Change the Passphrase of a KeyStore.

Acknowledge that you have a backup of the keystore (see Figure 17).

Figure 17 - Acknowledge the risk.

Select the KeyStore to modify. Provide the current passphrase as well as the new and confirmation passphrase. Then select Modify (see Figure 18).

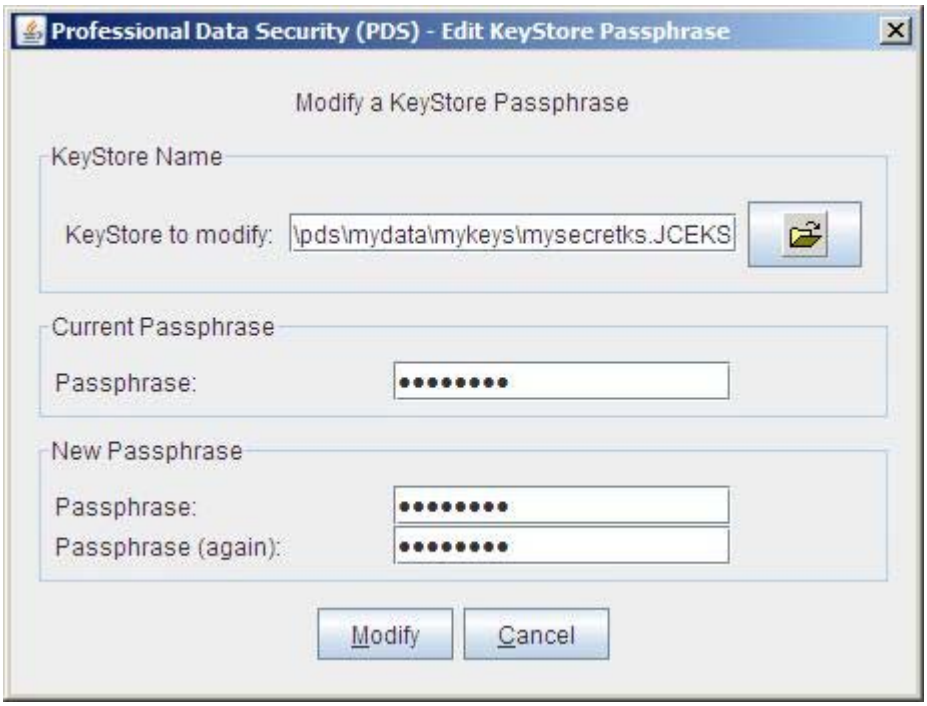

Figure 18 - Modify the KeyStore Passphrase.

8. Edit Encryption Key Properties.
==========

Properties include:

a. Set a key to be the default key
b. Change a key passphrase
c. Delete a key

Select File -> Edit -> Key (see Figure 19).

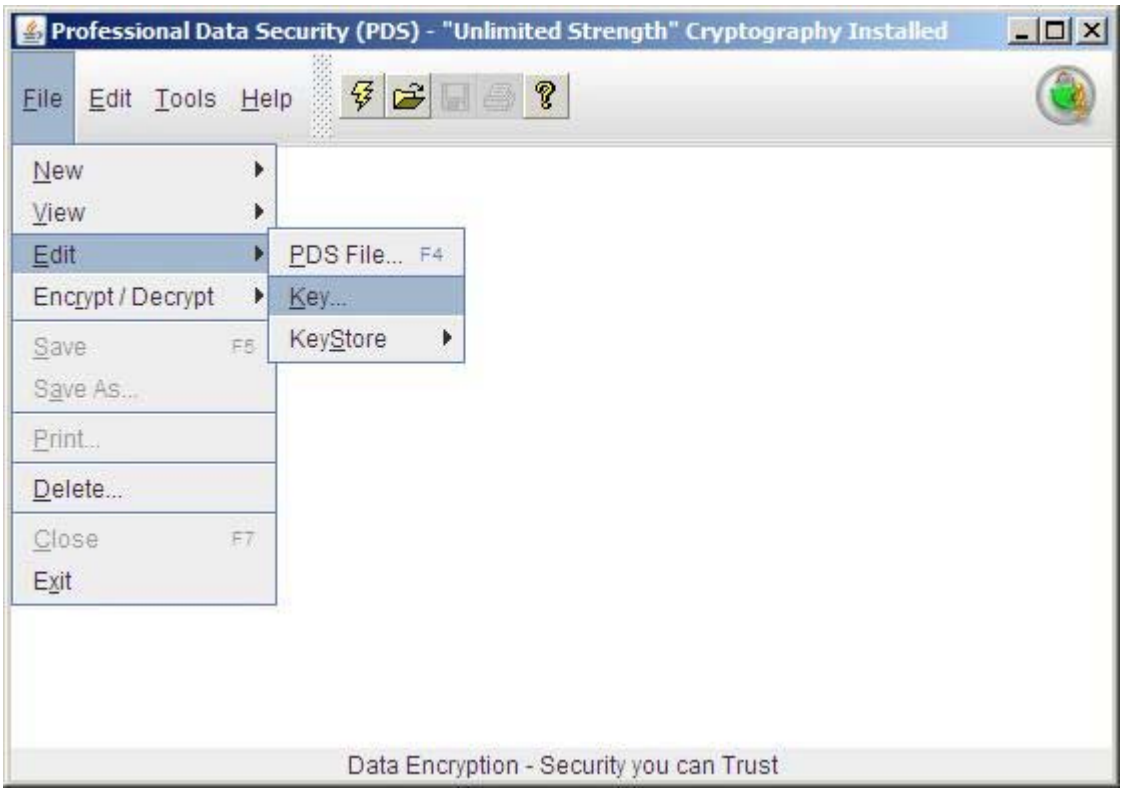

Figure 19 - Edit Encryption Key Properties.

Navigate to the KeyStore containing the Encryption Key (see Figure 20).

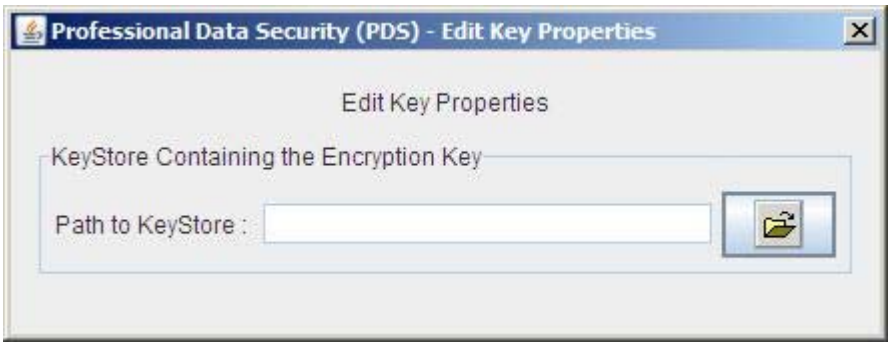

Figure 20 - Locate KeyStore dialog.

Provide the authentication credentials for the KeyStore (see Figure 21).

Figure 21 - Provide KeyStore Authentication Credentials.

Select the Encryption Key to modify, then select the desired form of modification. Follow the prompts to complete the action. (see Figure 22).

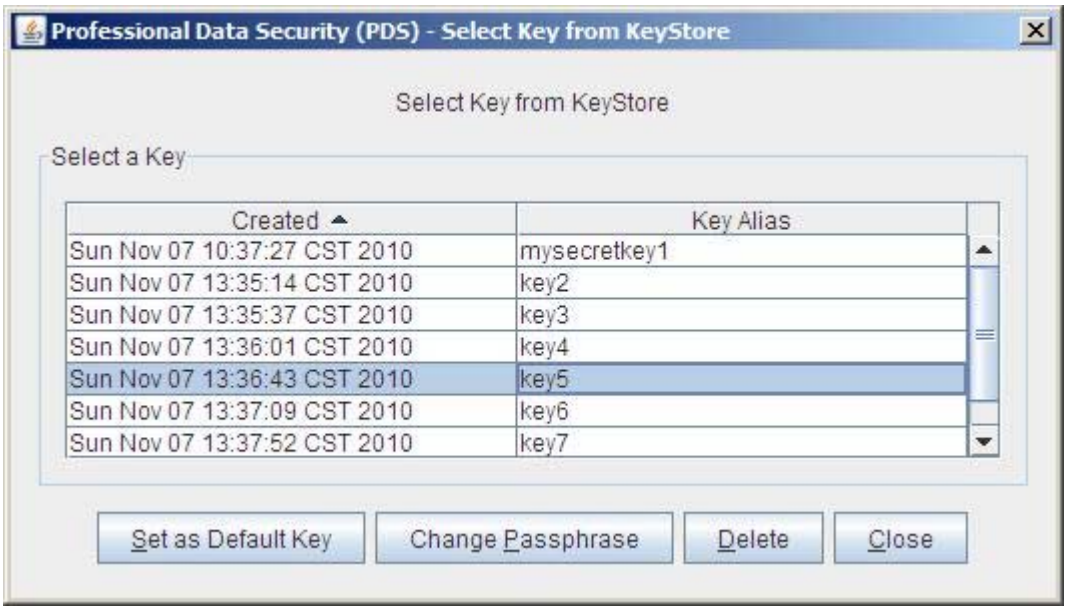

Figure 22 - Modify the Encryption Key.