

How-To Backup Your Decryption Key

Date issued:	April 2008	Written for:	SecureZIP® for Windows® desktop users
Effective date:	Immediate	Products affected:	SecureZIP for Windows Standard Edition SecureZIP for Windows Enterprise Edition PKZIP® for Windows Standard Edition** PKZIP for Windows Enterprise Edition**
Technical Support Ticket ID:	N/A	Author:	JPeterson

Introduction to Product/Feature: SecureZIP for Windows supports the use of digital certificates and associated public/private key pairs. Users who elect to use such key pairs must take steps to backup at least one copy of their private key in order to protect against loss due to file corruption or disk failure. This document provides a step-by-step illustration for backing up and recovering a private key.

In order to backup your private key, you must meet the following requirements:

- Have access to the machine on which your private key and digital certificate are located (this will typically be the system on which you use SecureZIP).
- Have Internet Explorer installed
- Have a reliable backup system using removable media, such as a USB drive or writeable CD or DVD drive

Step-by-Step Description: To complete the backup of your key, you will perform the following steps:

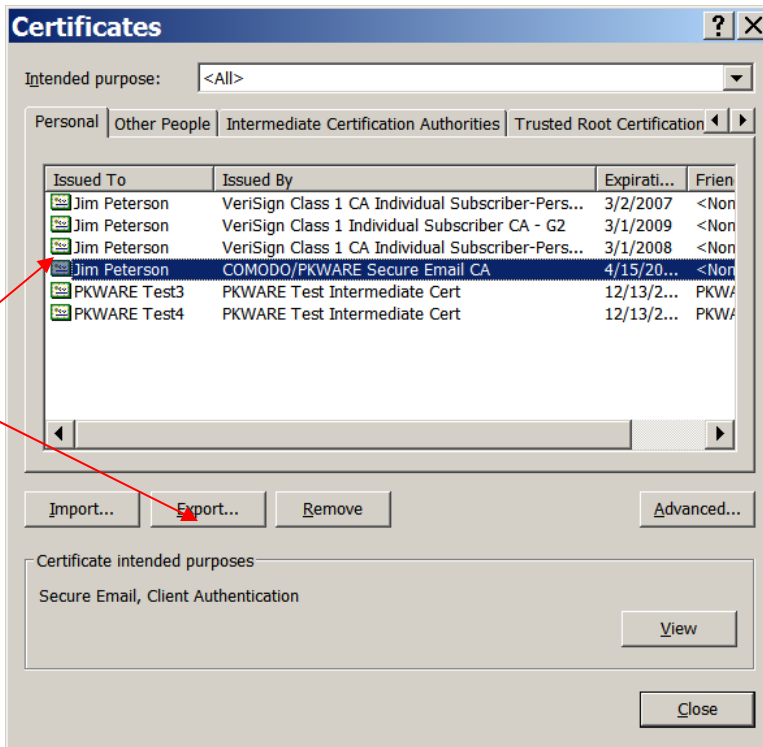
1. Use the Microsoft Certificate Export Wizard to write your Digital Certificate and private key to a secure file.
2. Assign a private password to protect your key while it is stored on your backup media.
3. Write the secure file to your backup device.

Visual Examples: Follow these instructions to export your private key to a secure file:

1. Open Internet Explorer and select Internet Options from the Tools menu.
2. Choose the Content tab and click on the Certificates button.
3. The Certificates window will open displaying your Digital Certificate; choose the Personal tab. If you have more than one key in the list that appears, you should complete these steps for each key to ensure you retain all keys in use on your machine.
4. To backup your SecureZIP key, highlight the key that is “Issued By” COMODO/PKWARE Secure Email CA.
5. Press the button labeled Export to start the export Wizard

**PKZIP products use digital certificates and keys for decryption only.

*** Proprietary and Confidential to PKWARE, Inc. ***



6. On the Welcome dialog, press Next.



7. Check the option “Yes, export the private key” and press Next.



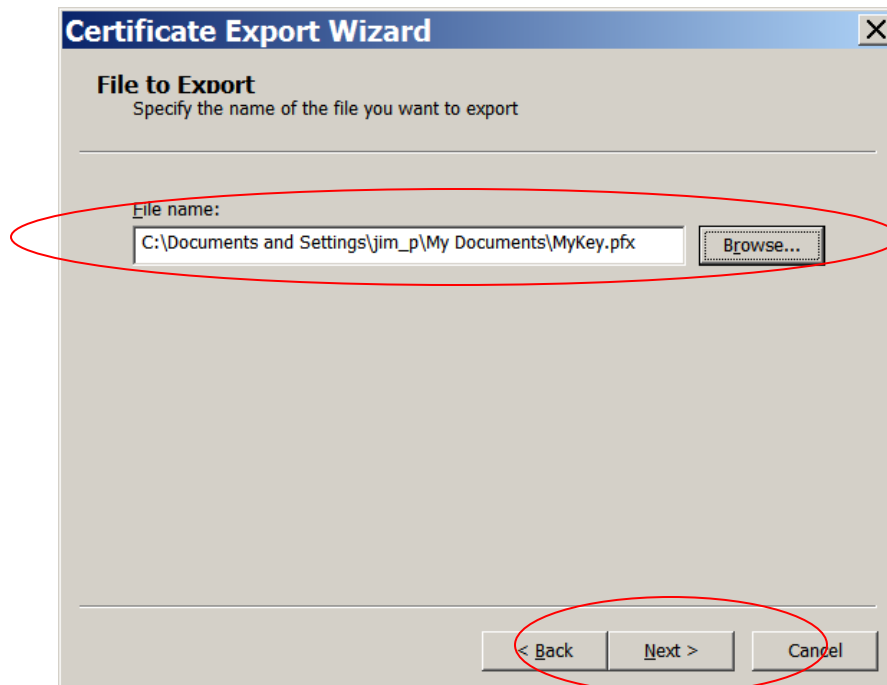
8. Choose the option “Personal Information Exchange – PKCS #12” and also check the boxes “Include all certificates in the certification path” and “Enable strong key protection.” DO NOT check the box to “Delete the private key if the export is successful.” Press Next to continue.



9. Enter a password that will be used to protect your key while it is stored on your backup media. Make sure you record this password; you will need it in the event you ever need to restore your private key.



10. Enter the name for the secure file that will store your private key. Use the Browse button to select a location to save your file.



*** Proprietary and Confidential to PKWARE, Inc. ***

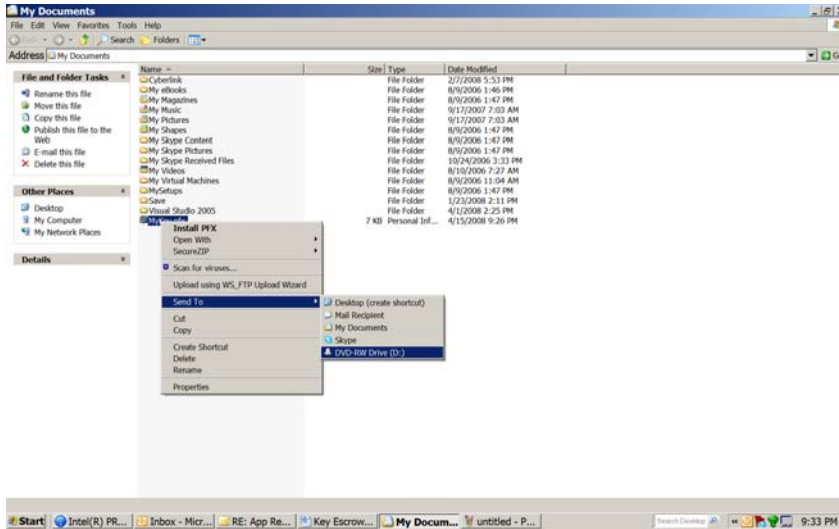
11. Press Finish to complete the export of your key.



12. The Export Wizard will display the following message when the export has completed successfully. After this message appears, you can copy the file to your storage media.



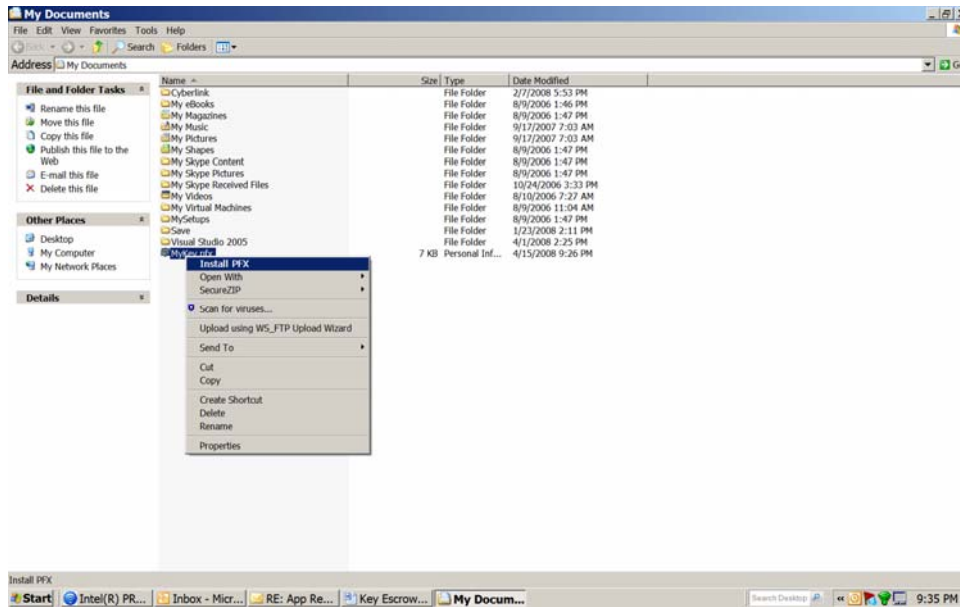
13. The steps to copy your secure file to your storage media will vary depending on the type of storage used for your backups. One example is illustrated below. Using Windows Explorer, locate the secure file created with the Export Wizard. Use the right-click menu in Windows Explorer to write the file to CD/DVD media.



14. When the copy completes, store the media in a secure location.

Follow the steps below for restoring your private key from the secure file:

1. Should it ever be necessary to restore your digital certificate, insert your backup media and highlight the secure file that holds your key. Using the right-click menu in Windows Explorer, select the option Install PFX.



2. The Certificate Import Wizard will start. Follow the steps to install your key.

Conclusion: Backing up one or more copies of your decryption (private) key is imperative to ensure you will have the means to recover data you've encrypted using SecureZIP. This document shows that making such a backup requires only a few, easy-to-complete steps that provide a necessary safeguard against corruption of the private key file or failure of your PC hard disk.

Background: SecureZIP protects your files and messages using data encryption and a key. A key can be either a passphrase you define and/or public keys from recipients you allow to access the files. Once encrypted, this information can only be accessed using the key. As long as you need to access the data you have protected, you will need to ensure you retain a copy of the key. If you lose the key, you will lose access to your data.

Encrypting using digital certificates provides for easier management of keys over time and provides a higher level of data protection than using a passphrase. In enterprise environments, use of the SecureZIP contingency key feature ensures encrypted data can be recovered by an appropriate data professional in your organization. A contingency key serves as an extra key in addition to any other keys you may use for normal access to your protected data.

If your organization is not using the contingency key feature of SecureZIP, or if you are using SecureZIP at home *and* using a digital certificate with associated public/private key pair, you will need to ensure you make a backup of your decryption (private) key. For a more detailed discussion, please see http://en.wikipedia.org/wiki/Private_key.

*** Proprietary and Confidential to PKWARE, Inc. ***

Proprietary Information: N/A

* If you need any further information, please contact PKWARE Product Support at <http://www.pkware.com/support/desktop>.

Copyright © 2008 PKWARE, Inc. All rights reserved.

PKWARE, the PKWARE Logo, SecureZIP, and PKZIP are registered trademarks of PKWARE, Inc. Trademarks of other companies mentioned in the document appear for identification purposes only and are the property of their respective companies.