

USER MANUAL
POINTSEC MEDIA ENCRYPTION
SOFTWARE (VERSION 2.6)

PREPARED BY: IFMC
NOV 2007

DOCUMENTATION CONTROL

DOCUMENT PURPOSE

This guide explains how to use Pointsec ME to protect information stored on your workstation, removable media, external hard drives, floppy disks, and CDs/DVDs. This guide includes some of the most commonly used options to protect information.



TABLE OF CONTENTS

1.0	PURPOSE	1
1.1	Pointsec ME	1
1.2	Encrypting Data.....	1
1.3	Two options for encrypting information	Error! Bookmark not defined.
2.0	PASSWORD MANAGEMENT	2
2.1	Assigning Passwords to Encrypted/Protected Files and Devices	2
2.2	Passwords and Encrypted Data	2
3.0	CREATING AN ENCRYPTED PACKAGE - BEST FOR SENDING PHI TO A RECIPIENT.....	3
4.0	ACCESSING DATA – FROM AN ENCRYPED PACKAGED	6

LIST OF TABLES

Table 1—Examples of Acceptable Password Communication.....	2
Table 2—Creating an Encrypted Package.....	3
Table 3— Accessing Encrypted Data from an encrypted package.....	6

1.0 PURPOSE

The Centers for Medicare and Medicaid Services (CMS) requires employees to encrypt all agency data contained on mobile computers and devices. Encryption is the process of protecting stored or transmitted information with a password (key) so that it is indecipherable until the intended recipient uses the password to access it. When Pointsec software has been deployed, you will find it by clicking on **Start, Programs, Pointsec, Pointsec Media Encryption**, and finally **About**.

1.1 Pointsec ME

Pointsec ME is designed for Windows notebooks and laptops, desktops with USB drives, writeable CD/DVD drives, floppy drives, and external hard drives. It allows you to create encrypted information packages for easy and secure storage.

1.2 Encrypting Data

Pointsec ME recognizes all CDs as Read-Only devices. You should encrypt the data on your workstation hard drive. For example, at **C:\Pointsec**, before copying or it to a CD with Roxio. Once a CD/CD-RW CD has been encrypted, files cannot be written to the CD or modified. You must decrypt the file(s) and save the file(s) to a different location in order to modify them.

2.0 PASSWORD MANAGEMENT

This section explains how passwords should be assigned and how to get a password to a recipient of an encrypted package.

2.1 Assigning Passwords to Encrypted/Protected Files and Devices

Passwords assigned to protected files and devices must be at least 8 characters in length and alphanumeric with one number and a one uppercase letter. An example of a **good password** is **Cmsifmc1** A unique password should be used for each encryption transmission.

Passwords should not travel with the data; they should be provided separately to the recipient

2.2 Passwords and Encrypted Data

If you send out encrypted data, the password cannot travel with the data. See the table below for examples of acceptable password communication.

Table 1—Examples of Acceptable Password Communication

Data Travels By	Password Conveyed By	Acceptable Not Acceptable
CERTIFIED USPS MAIL (Signature required)	Phone to End User or Email	Acceptable
FedEx	Phone to End User or Email	Not Acceptable
Email	Phone to End User or Email	Not Acceptable
Encrypted data and password should never travel together.		

No provision is made for a lost password. If a password is forgotten the encrypted information must be recreated from its source.

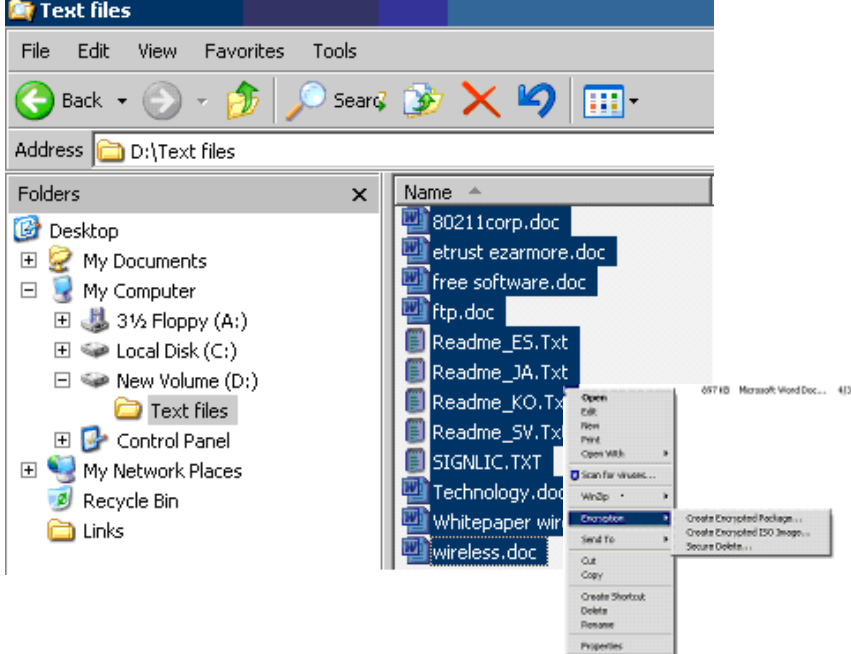
3.0 CREATING AN ENCRYPTED PACKAGE - BEST FOR SENDING PHI TO A RECIPIENT

The following section explains how to use Pointsec Media Encryption to pack files into encrypted packages. Encrypted packages can be used to transfer and store information securely on a CD, DVD or other device.

You may find it easier to manage the Pointsec encrypted files by creating a Pointsec folder on your workstation, for example “C:\Pointsec”, to save encrypted and decrypted files.

This section explains how to create an encrypted package for recipients who do not have Pointsec ME software as well as for recipients who do have Pointsec ME software.

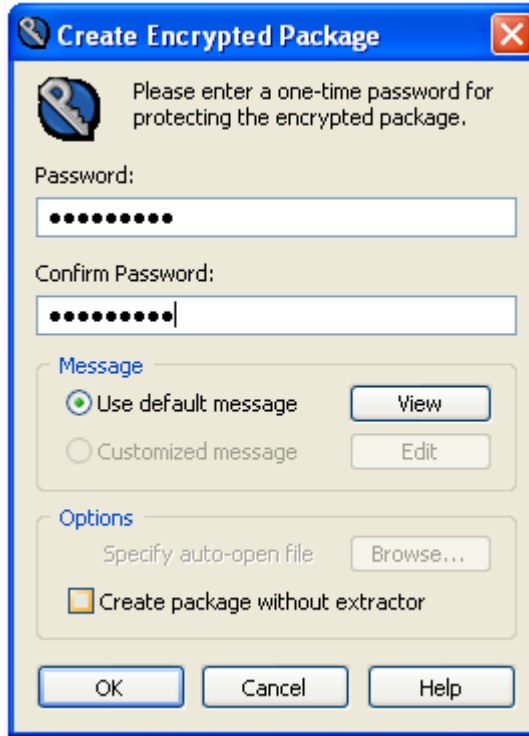
Table 2—Creating an Encrypted Package

<p>1. Open Windows Explorer and highlight and select the file(s) for encryption.</p> <p>2. Right click on the highlighted file(s) and click on Encryption. Then click on Create Encrypted Package.</p> <p>Note: Do not use the Create Encrypted ISO Image</p>	
--	---

3. Enter a password for protecting the encrypted package.

Passwords must be at least **8 characters** in length and alphanumeric With one Uppercase letter. An example of a good password would be **Cmsifmc1**

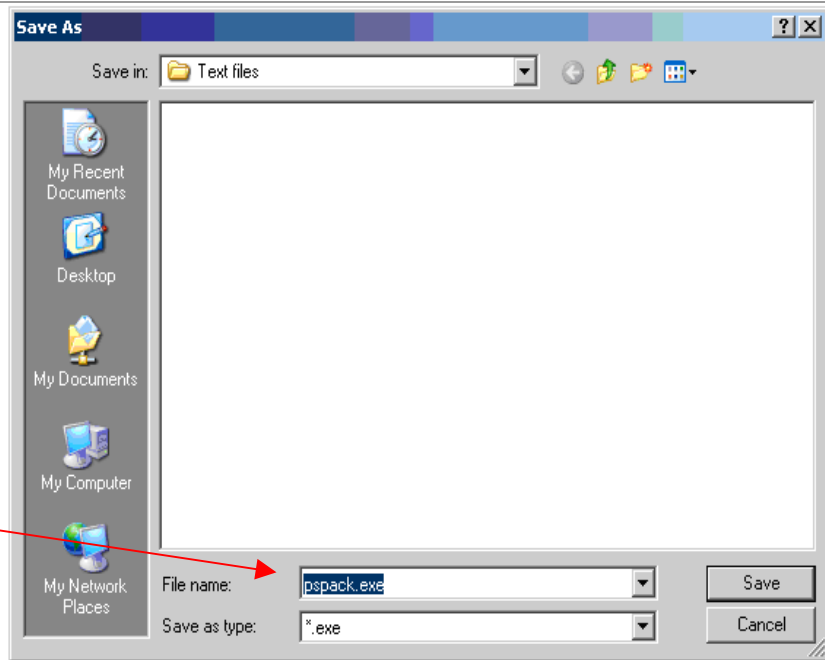
Accept defaults the select **OK**



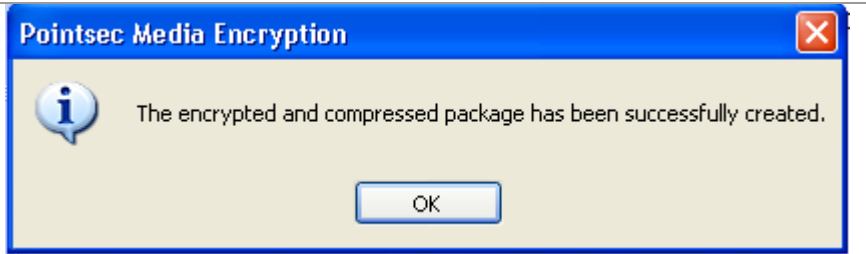
No provision is made for a lost password. If a password is forgotten the encrypted information must be recreated from its source.

4. Give the encrypted package a new file name and click on **SAVE**.

Tip: You should change the file name or the previous pspack.exe (the Pointsec default name for a self-decrypting file) will be overwritten if one already exists



5. This screen shows that a package was created. Click OK



6. This screen shows that a package, called **test.exe**, has been created.

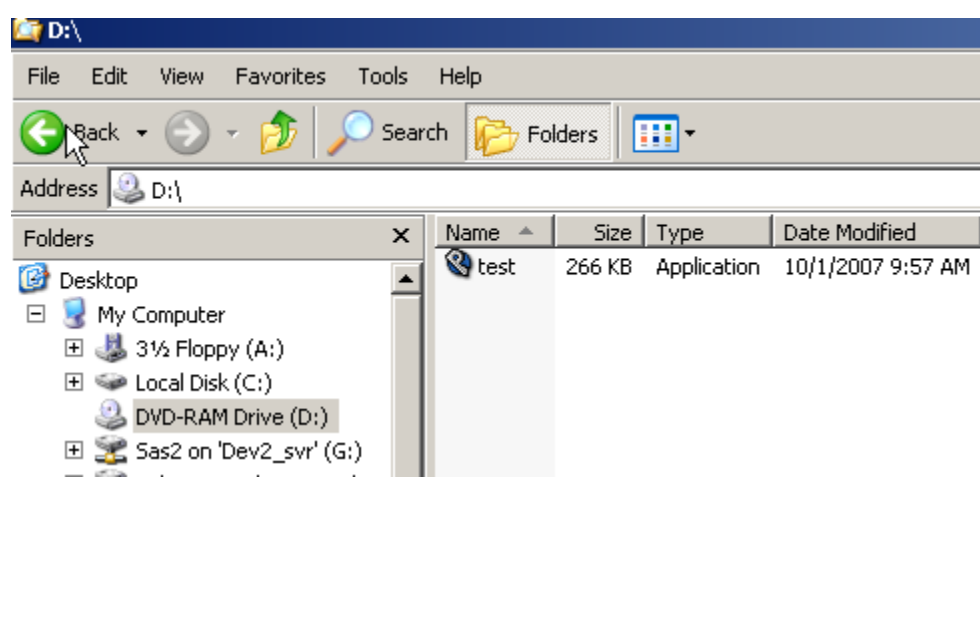
Name	Size	Type	Date Modified
80211corp.doc	279 KB	Microsoft Word Doc...	2/23/2004 10:37 AM
etrust ezarmore.doc	89 KB	Microsoft Word Doc...	12/1/2003 1:55 PM
free software.doc	95 KB	Microsoft Word Doc...	12/1/2003 11:39 AM
ftp.doc	87 KB	Microsoft Word Doc...	12/13/2005 8:17 AM
Readme_ES.Txt	35 KB	Text Document	3/2/2005 8:00 PM
Readme_JA.Txt	31 KB	Text Document	3/2/2005 8:00 PM
Readme_KO.Txt	32 KB	Text Document	3/2/2005 8:00 PM
Readme_SV.Txt	31 KB	Text Document	3/2/2005 8:00 PM
SIGNLIC.TXT	6 KB	Text Document	12/21/2004 4:40 AM
Technology.doc	352 KB	Microsoft Word Doc...	2/5/2004 4:05 PM
Whitepaper wireless 802.doc	157 KB	Microsoft Word Doc...	3/11/2003 4:56 PM
wireless.doc	897 KB	Microsoft Word Doc...	4/30/2003 11:04 AM
test.exe	1,344 KB	Application	12/4/2006 11:28 AM

- ❑ An encrypted package can be burned to a CD or DVD with Roxio or copied to a USB drive.
- ❑ Pointsec has a 2GB file size limit.

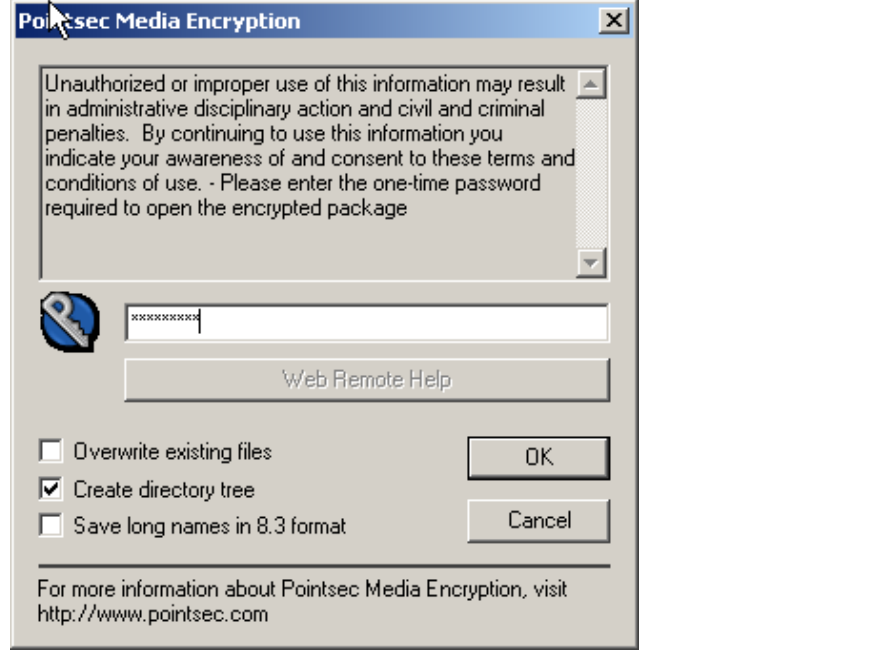
4.0 ACCESSING DATA – FROM AN ENCRYPED PACKAGED

When encrypted media is received, insert or attach the media to the workstation to access the data contained on the device. This section will explain how you will access encrypted package.

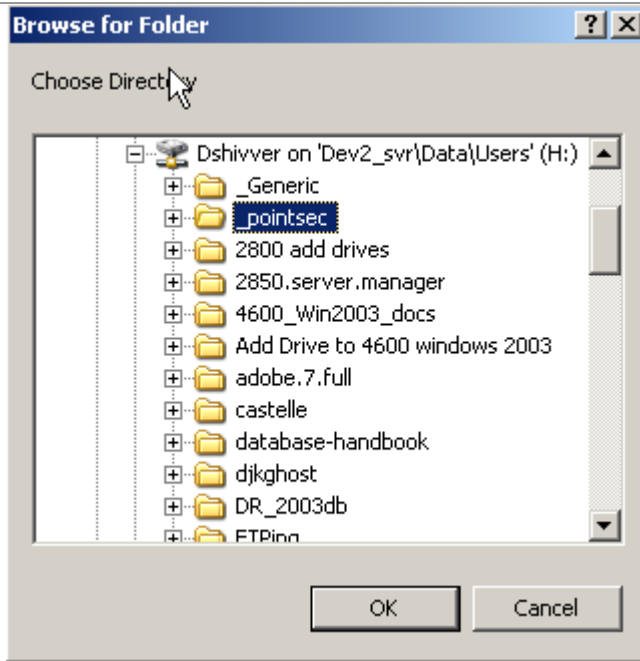
Table 3— Accessing Encrypted Data from an encrypted package.

<p>1. Open Windows Explorer and select the CD drive in order to display the contents of the encrypted CD. Double click on the test.exe application to start the decryption process.</p> <p>Note: This example is for a CD however these same steps can be followed for all portable media.</p>	
---	---

Note: No provision is made for a lost password. If a password is forgotten the encrypted information must be recreated from its source.

<p>2. Enter the password. Then click on OK.</p> <p>NOTE: No provision is made for a lost password. If a password is forgotten the encrypted information must be recreated from its source.</p>	
---	--

3. When the correct password is entered, the Pointsec Media Encryption Wizard starts. Browse to the drive and folder you want the files decrypted into. **OK** to continue.



Confidential/Sensitive information must be placed in a secure location like a network drive with access controls in place so that only people who have a need to see the data have access to it. Do not place files on an unsecured network share drive or the local C:\ drive if data are confidential in nature.

- ❑ Browse to the location specified – the files will be there and ready to access without entering a password.
- ❑ The contents on the CD remain encrypted and should be properly labeled and stored in a secure location. If the CD will not be needed, it should be properly destroyed, i.e., shredded.