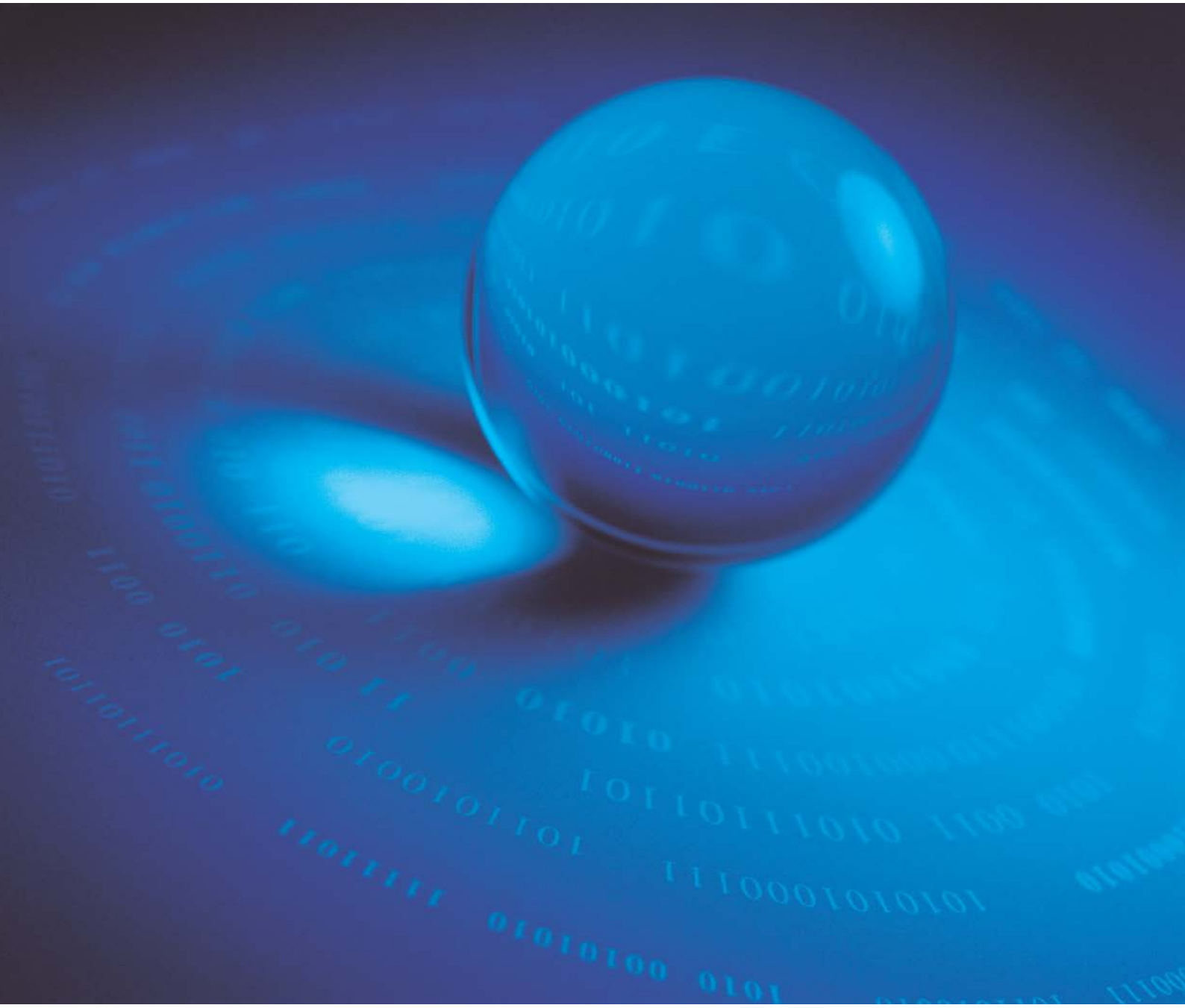
Application of EnterSafe Minidriver for EFS

V1.0



http://www.EnterSafe.com

EnterSafe will do their best to keep the content of this document as accurate as possible. But EnterSafe will not take the responsibilities for any direct or indirect loss that may be caused by this document. The content of this document will be amended along with the updating of the product without notification.

Revision History:

Date	Version	Description
January 2008	1.0	1st Edition

EnterSafe

SOFTWARE DEVELOPER'S AGREEMENT

This Software Developer's Agreement ("SDA") is a legal agreement between you (either an individual or a single entity) and EnterSafe Corporation for the software that accompanies this SDA, which includes computer software and may include associated media, printed materials, "online" or electronic documentation, and Internet-based services ("Software").**YOU AGREE TO BE BOUND BY THE TERMS OF THIS SDA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.**

1. GRANT OF LICENSE. EnterSafe grants you the rights described in this SDA provided that you comply with all terms and conditions of this SDA.

1.1 EnterSafe grants you a limited, nonexclusive license to use the Software, and to make and use copies of the Software, for the purposes of designing, developing and testing your software applications.

1.2 EnterSafe grants you to merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may revise, reverse engineer, decompile, disassemble, enhanced or otherwise modified the Software, except only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

3. NO RENTAL OR COMMERCIAL HOSTING. You may not rent, lease, lend or provide commercial hosting services with the Software.

4. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that you might incur for any reason whatsoever (including, without limitation, all damages referenced herein and all direct or general damages in contract or anything else), the entire liability of EnterSafe and any of its suppliers under any provision of this SDA and your exclusive remedy hereunder shall be limited to the greater of the actual damages you incur in reasonable reliance on the Software up to the amount actually paid by you for the Software.

5. DISCLAIMER OF WARRANTIES. to the maximum extent permitted by applicable law, EnterSafe and its suppliers provide the Software and support services (if any) AS IS AND WITH ALL FAULTS, and hereby disclaim all other warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the Software and the provision of or failure to provide support or other services, information, software, and related content through the Software or otherwise arising out of the use of the Software. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

6. RESERVATION OF RIGHTS AND OWNERSHIP. EnterSafe reserves all rights not expressly granted to you in this SDA. The Software is protected by copyright and other intellectual property laws and treaties. EnterSafe own the title, copyright, and other intellectual property rights in the Software.

7. TERMINATION. This SDA is effective until terminated. Upon any violation of any of the provisions of this SDA, rights to

use the Software shall automatically terminate and the Software must be returned to EnterSafe or all copies of the Software destroyed. You may also terminate this SDA at any time by destroying all copies of the Software in your possession or control. If EnterSafe makes a request via public announcement or press release to stop using the copies of the Software, you will comply immediately with this request. The provisions of paragraphs 2, 3, 4, 5 and 6 will survive any termination of this SDA.

CE Attestation of Conformity

The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test report No. 70407310011
Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

FCC certificate of approval

This Device is conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

USB

This equipment is USB based.

WEEE

Dispose in separate collection.

Contents

1 Overview

1.1 What's Encrypted File System

The Encrypting File System (EFS) is a file system driver with filesystem-level encryption available in Microsoft Windows (2000 and later) operating systems, except Windows XP Home Edition, Windows Vista Basic, and Windows Vista Home Premium. The technology transparently allows files to be encrypted on NTFS file systems to protect confidential data from attackers with physical access to the computer.

1.2 Preparing for EnterSafe Minidriver

Before use EFS with EnterSafe Minidriver, the following requirements should be satisfied:

1. Install EnterSafe Minidriver;
2. Certificate installation on the EnterSafe Minidriver Token;
3. Folder creation;
4. Folder encryption.

2 Infrastructure Configuration

2.1 Architecture

The general infrastructure needed is:

- Windows Client on an NTFS partition, Windows Vista as an example.
- Active Directory
- Certificate Authority

2.2 Microsoft Encrypted File System

2.2.1 Prerequisite

In order to successfully accomplish the following use case, you need a computer running Windows Vista and a user account with administration rights.

In order to support the Encrypted File System, the File System Type must be set to NTFS. This is done when installing the Widows operating system.

2.2.2 Widows Vista Properties

To activate the EFS using the EnterSafe Minidriver Token, you must proceed as follows:

1. On the Windows Vista Control Panel, select **Administrative Tools**.
2. Click on **Local Security Policy** (you must be a member of the Administrator Group).
3. On the Public Key Policies, right-click on **Encrypting File System** and select **Properties**. The Encrypting File System Properties dialog appears as shown in Figure 1:

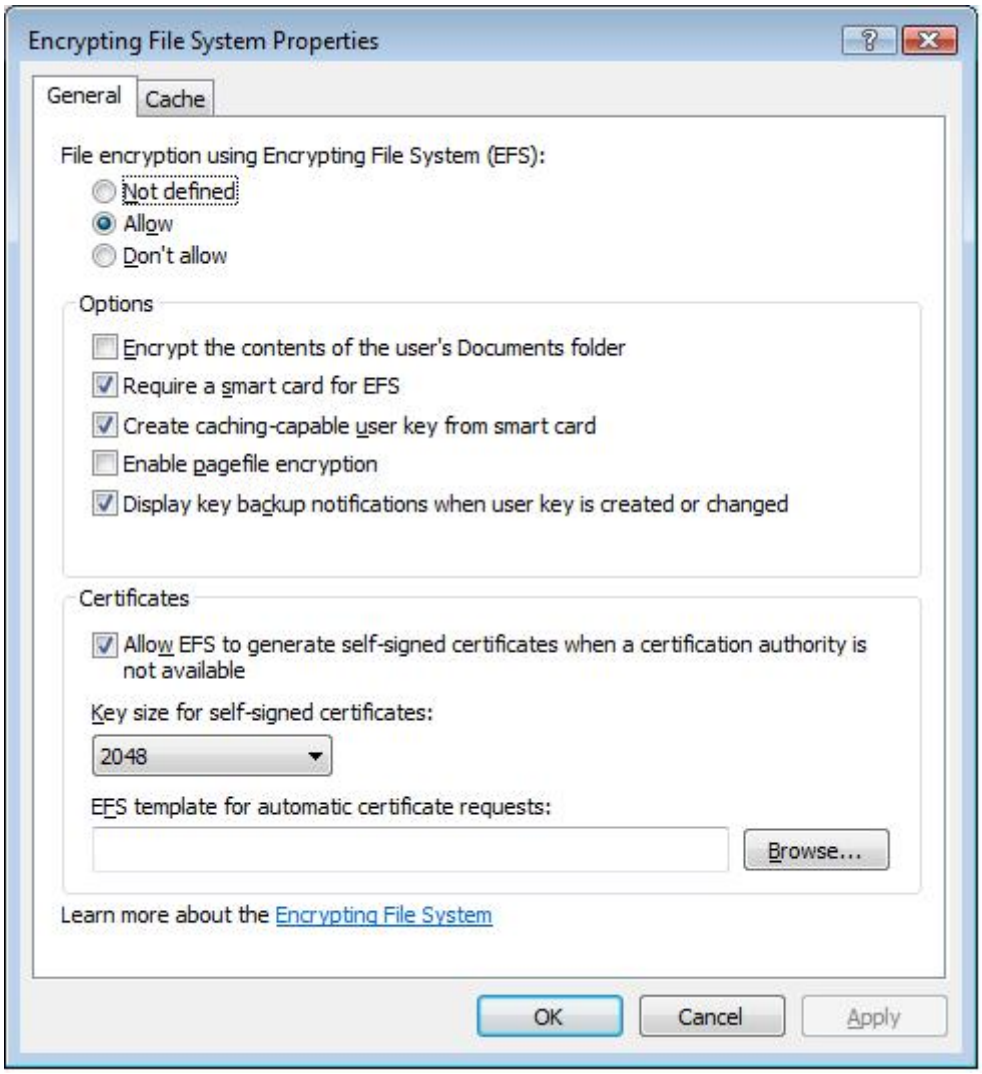


Figure 1 Encrypting File System Properties-General

4. In File encryption using **Encryption File System (EFS)** area, select **Allow**.
5. In **Options** area, check **Require a smart card for EFS**.
6. In Certificates area, clear **Allow EFS to generate self-signed certificates when a certification authority is not available**.
7. In the Encrypting File System Properties area click on the **Cache** tab. By checking the **User locks workstation**, you clear the encryption session key cache when the workstation is locked, as shown in Figure 2:

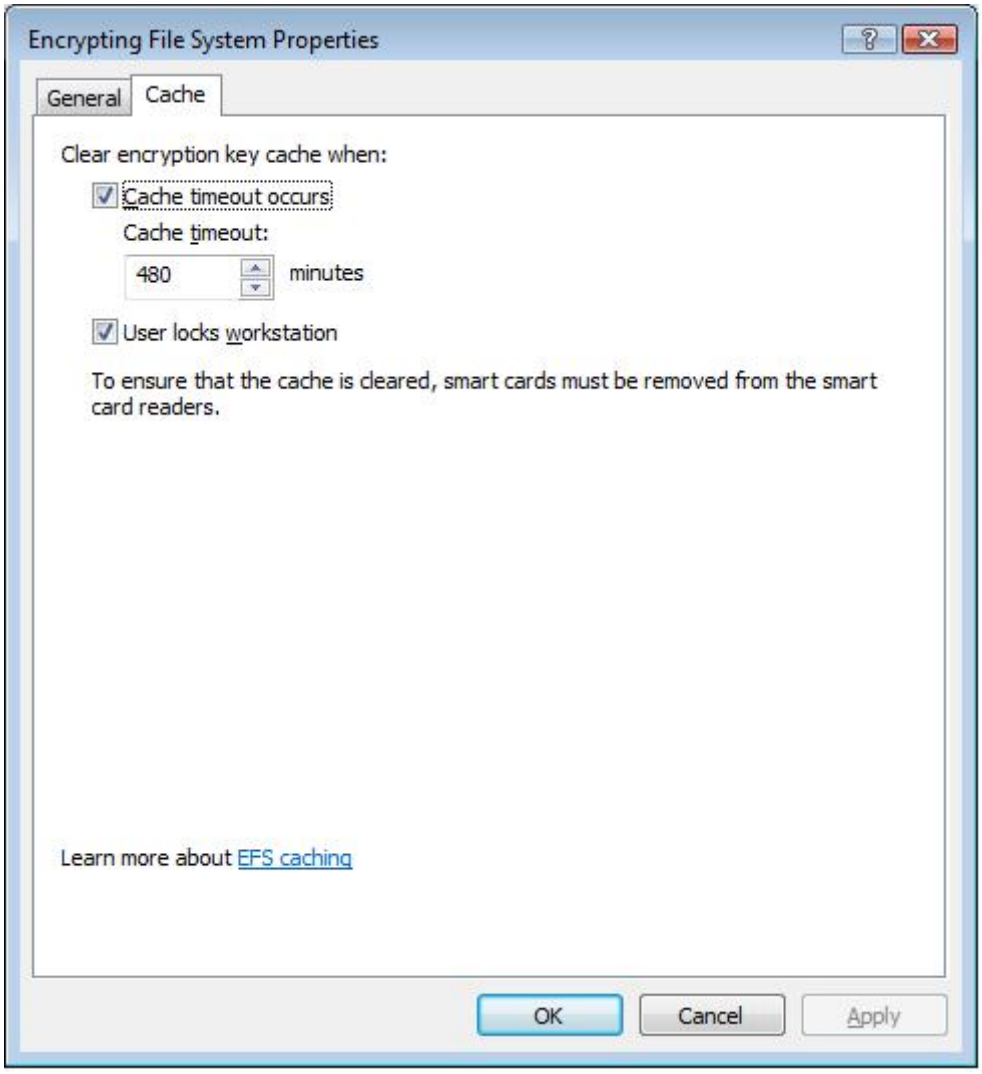


Figure 2 Encrypting File System Properties-Cache

Note:The procedure is not necessary for operating systems earlier than Windows Vista.

3 EnterSafe Minidriver Token Use Cases

3.1 Performing EFS Operations With An Existing Certificate

Before using the EnterSafe Minidriver Token for EFS, the Token should contain a smart card logon certificate. And the certificate must have the EFS attribute.

After you log on to the workstation, please create a folder for the EFS, for example, named EFS_example. And create a file in the folder.

To encrypt the folder and its files, proceed as follows:

1. Right-click on the EFS_example folder and then click on **Properties**, as shown in Figure 3:

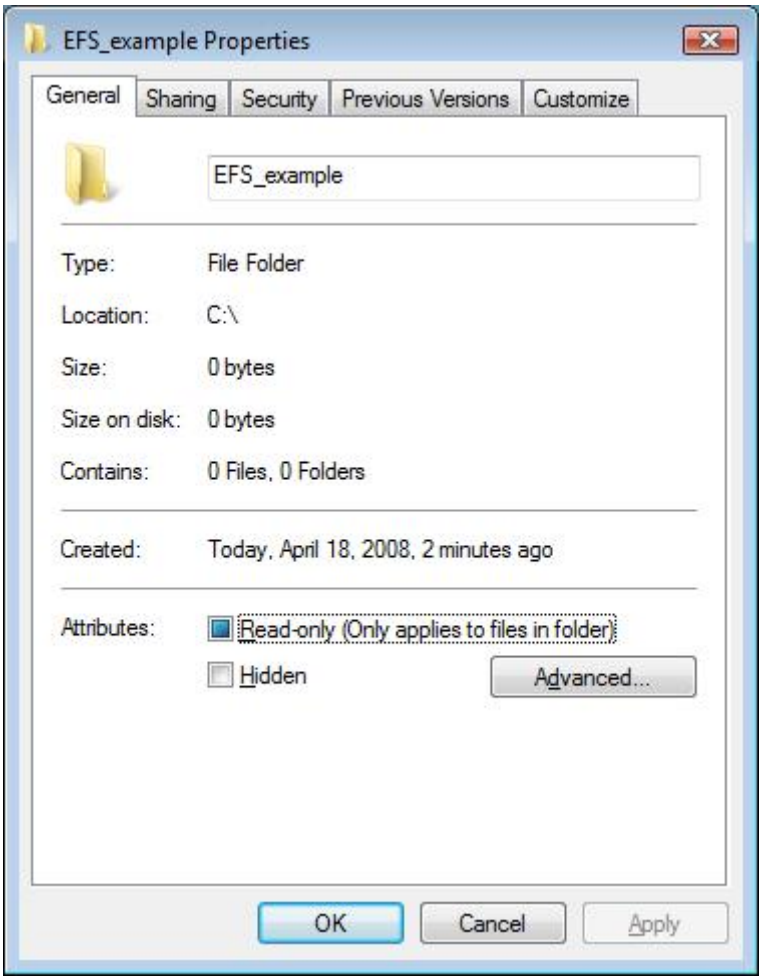


Figure 3 EFS folder Properties

2. Click on **Advanced**, as shown in Figure 4:

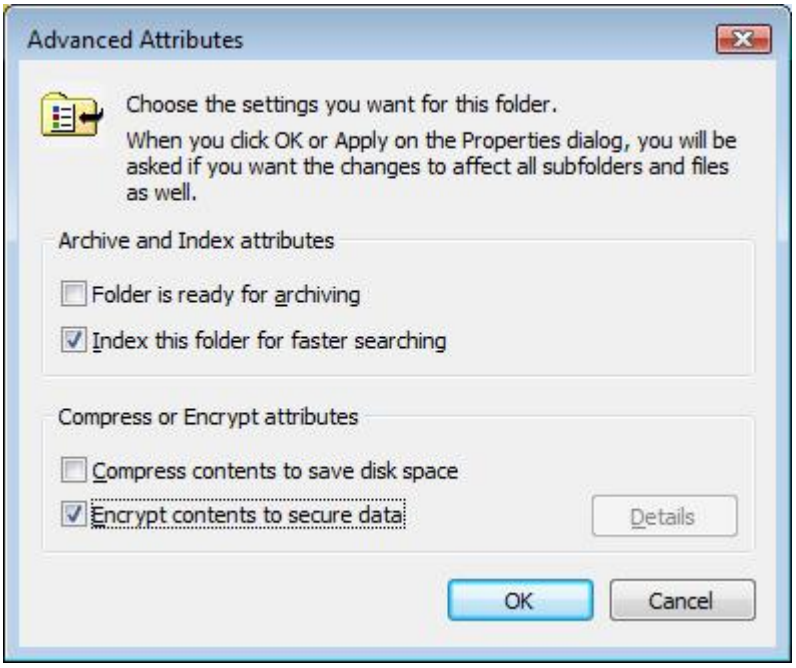


Figure 4 Advanced Attributes

3. In the **Advanced Attributes** dialog, you must check **Encrypt contents to secure data** and then click on **OK** twice.

4. In the **Confirm Attribute Changes**, select **Apply changes to this folder, subfolder and files** and then click on OK.

Figure 5 Confirm Attribute Changes

5. In the Encryption File System dialog, select **Use an existing smart card certificate**, as shown in Figure 6:

Figure 6 Select an existing smart card certificate

6. Select the user certificate and then click on OK, as shown in Figure 7:

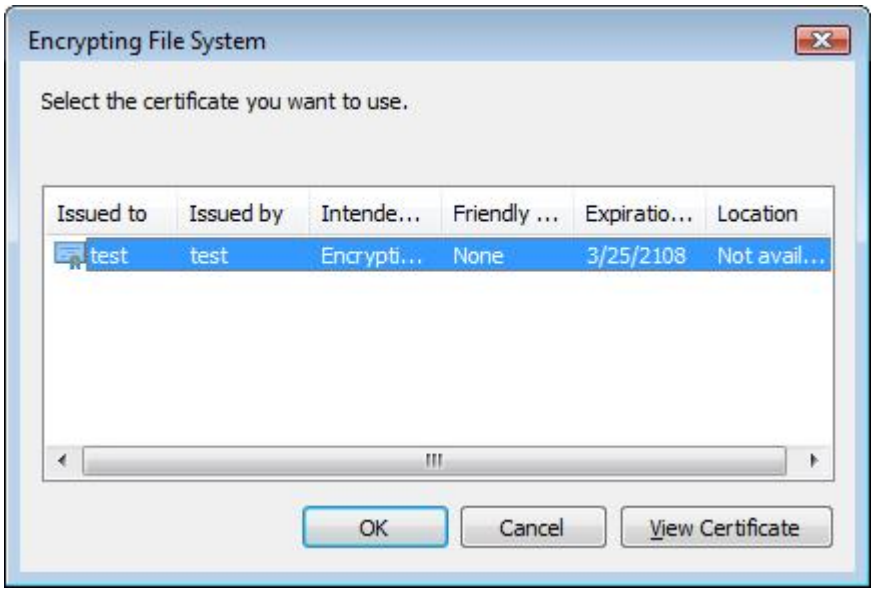


Figure 7 Select a certificate

7. Then the PIN dialog pops up. Enter your PIN code and then click on OK, as shown in Figure 8:

Figure 8 PIN dialog

The EFS_exmaple folder is now encrypted.

The folder is now accessible only for the EFS_exmaple. To access the files in this folder, you must log on as EFS_exmaple and use your smart card.

If another user logs on to your PC, he or she cannot open the EFS_exmaple encrypted folder, even if that user has administrative rights for the PC.

If you log on as EFS_exmaple without a smart card, you will be unable to access to the encrypted files. You will be resquested to attach the smart card, as shown in Figure 9:

Figure 9 Prompt to insert a smart card

3.2 Creating A New Certificate For EFS Operations

After you log on to the workstation, please create a folder for the EFS, for example, named EFS_example. And create a file in the folder.

To encrypt the folder and its files, proceed as follows:

1. Right-click on the EFS_example folder and then click on **Properties**, as shown in Figure 10:

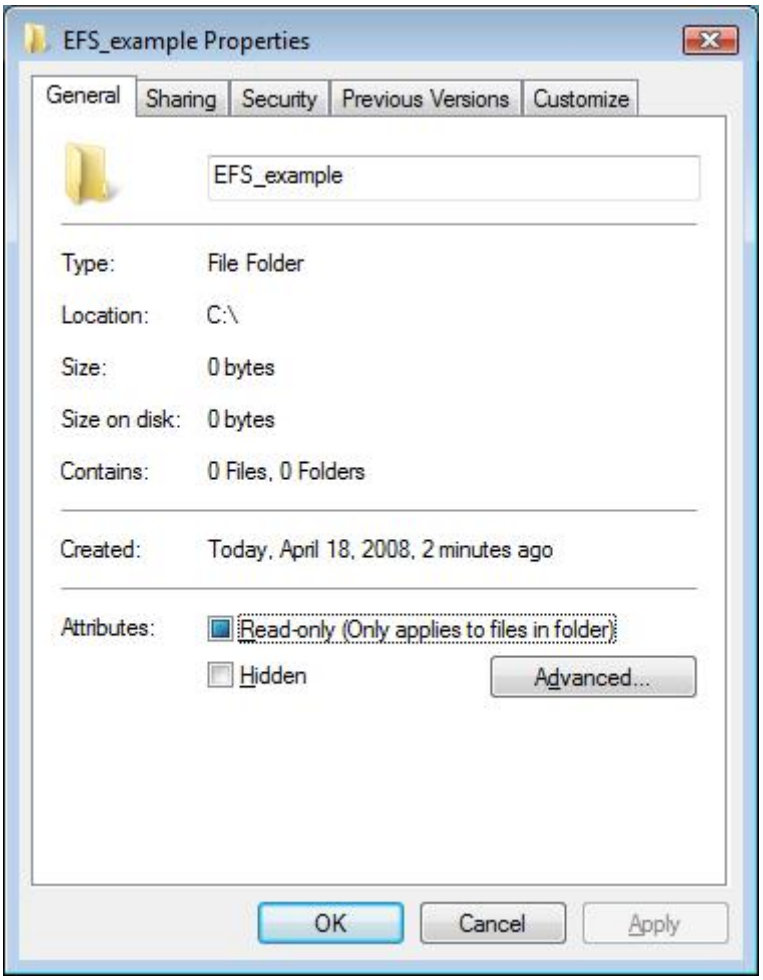


Figure 10 EFS folder properties

2. Click on **Advanced**, as shown in Figure 11:

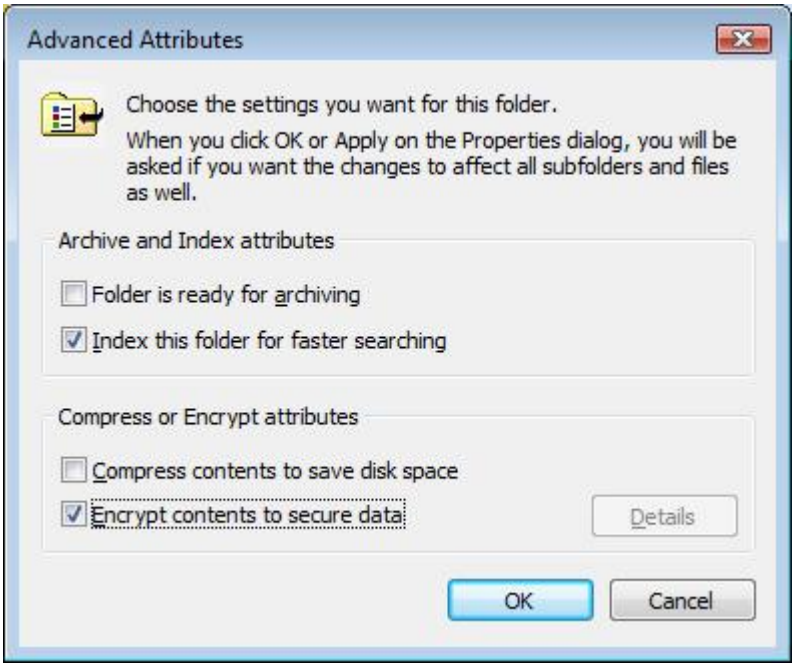


Figure 11 Advanced Attributes

3. In the **Advanced Attributes** dialog, you must check **Encrypt contents to secure data** and then click on **OK**

twice.

4. In the **Confirm Attribute Changes** area, select **Apply changes to this folder, subfolder and files** and then click on **OK**.

Figure 12 Confirm Attribute Changes

5. In the **Encryption File System** dialog, select **Create a new smart card certificate**, as shown in Figure 13:

Figure 13 Select an existing smart card certificate

6. Then you will be requested to enter the user PIN of the smart card, as shown in Figure 14:

Figure 14 PIN dialog

7. A new smart card certificate is created in your Token.

8. Select the created user certificate and then click on OK, as shown in Figure 15:

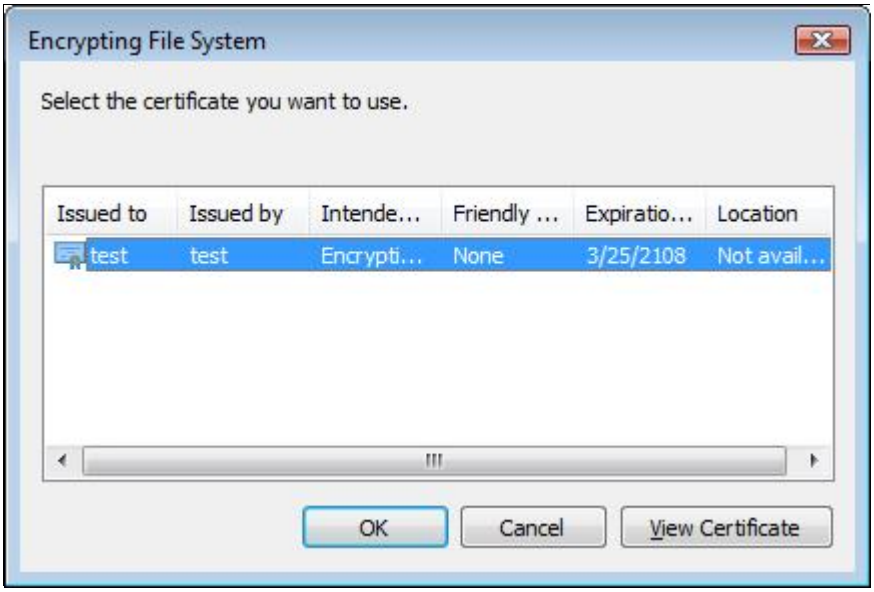


Figure 15 Select a certificate

9. Then you will be requested to enter the user PIN. Enter your PIN code and then click on OK, as shown in Figure 16:

Figure 16 PIN dialog

The EFS_example folder is now encrypted successfully.