Security

Microsoft Dynamics CRM 2011

Microsoft Dynamics CRM Online

Using Encrypting File System and BitLocker to Protect Microsoft Dynamics CRM Data on Client Computers

White Paper

Date: November 2011

Acknowledgements

Initiated by the Microsoft Dynamics CRM *Engineering for Enterprise* (MS CRM E^2) Team, this document was developed with support from across the organization and in direct collaboration with the following:

Key Contributor	**Technical Reviewer**
Murali Puthanveetil (*Microsoft*)	Monika Borgaonkar (*Microsoft*)

The MS CRM E^2 Team recognizes their efforts in helping to ensure delivery of an accurate and comprehensive technical resource in support of the broader CRM community.

Note: This paper leverages content previously published in the white paper *Using Encrypting File System to Protect Microsoft Dynamics CRM Data on Windows XP and Windows Vista.*

MS CRM E^2 Contributors

Ahmed Bisht, Program Manager	Jim Toland, Sr. Content Project Manager

Feedback

To send comments or suggestions about this document, please click the following link and type your feedback in the message body:
http://go.microsoft.com/fwlink/?LinkID=230732

Important: The subject-line information is used to route your feedback. If you remove or modify the subject line, we may be unable to process your feedback.

Legal Notice

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

Table of Contents

Introduction

With Microsoft Dynamics CRM 2011 and Microsoft Dynamics CRM Online, Microsoft Dynamics CRM for Microsoft Office Outlook provides functionality that enables users to disconnect from the network and work offline. In certain business scenarios, users gather and input information for long periods of time before having the chance to connect to the network and synchronize their data with the Microsoft Dynamics CRM server.

In the interim, depending on the type of information being gathered, it may be advisable to secure the CRM data on the client computer to help prevent theft via remote access or limit exposure should the portable computer containing the data be stolen.

This white paper explains how to use Microsoft BitLocker Drive Encryption (BitLocker) and Encrypting File System (EFS) to protect Microsoft Dynamics CRM data stored on client computers running Windows 7 Service Pack 1 (SP1), Windows Vista Enterprise Service Pack 2 (SP2), or Windows XP Professional Service Pack 3 (SP3).

Important: Using BitLocker and EFS to protect data on mobile computers is a recommended security practice for a wide variety of business applications, including Microsoft Dynamics CRM 2011 and Microsoft Dynamics CRM Online.

Components of Microsoft Dynamics CRM for Office Outlook

Microsoft Dynamics CRM users working offline require local access to Microsoft Dynamics CRM web pages, as well as a mechanism for storing information that is gathered and entered for eventual synchronization with the Microsoft Dynamics CRM database.

- **Cassini**. Cassini is a full-featured web server from Microsoft that, by default, serves requests only from the localhost. Cassini allows Microsoft Dynamics CRM for Outlook to host the Microsoft Dynamics CRM web application pages when offline. The Cassini process (Microsoft.Crm.Application.Hoster.exe) starts with Outlook.
- **Microsoft SQL Server 2008 Express Edition**. The process of installing Microsoft Dynamics CRM for Outlook on a client computer also installs SQL Server 2008 Express Edition and creates a user instance ("CRM"). The SQL Server service runs under the credentials of NT AUTHORITY\Network Service. After installation, the system creates two databases (MSCRM and Metabase). When CRM users work offline, data that they enter is stored locally in these SQL Server Express databases.

BitLocker and EFS

BitLocker and EFS are independent technologies that can be combined to provide a strong overall solution for data security. Because BitLocker and EFS provide security against different classes of attacks, an encryption solution that uses a combination of technologies benefits from the per-computer encryption provided by BitLocker and the per-user encryption provided by EFS.

Note: For more information about using BitLocker and EFS in combination, on Microsoft TechNet, in *Data Encryption Toolkit for Mobile PCs: Security Analysis*, see "Chapter 4: BitLocker and EFS Together" at: http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/analysis/80c0d0af-2c2e-45d6-9b29-f850926296bb.mspx.

Microsoft Windows Support for Data Encryption

Microsoft Windows 7, Microsoft Windows Vista, and Microsoft Windows XP support data encryption as follows.

- ***Microsoft Windows 7 and Microsoft Windows Vista***. The Enterprise and Ultimate editions of both Windows 7 and Windows Vista support BitLocker, EFS, or a combined solution that offers both BitLocker and EFS protection.
    - Enable BitLocker to encrypt the operating system volume when Microsoft Dynamics CRM for Outlook is installed on that volume.
    - Implement EFS as the simplest means of encrypting CRM data on computers running Microsoft Dynamics CRM for Outlook.
    - For the greatest level of security (and defense in depth), use a combined solution. On the computer running Microsoft Dynamics CRM for Outlook, first enable BitLocker on the Windows 7 or Windows Vista operating system volume, and then implement EFS to encrypt Microsoft Dynamics CRM-specific files.
- ***Microsoft Windows XP***. Windows XP supports only EFS for encryption of data on computers running Microsoft Dynamics CRM for Outlook.

BitLocker Drive Encryption

BitLocker is a data protection feature that is available in the Enterprise and Ultimate editions of both Windows 7 and Windows Vista (as well as Windows Server 2008 and Windows Sever 2008 R2. BitLocker addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned personal computers by providing a closely integrated solution.

BitLocker helps prevent unauthorized access to data on lost or stolen computers by combining two major data-protection procedures:

- Encrypting the entire Windows operating system volume on the hard disk.
- Verifying the integrity of early boot components and boot configuration data.

The most secure implementation of BitLocker leverages the enhanced security capabilities of a Trusted Platform Module (TPM) version 1.2. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer running Windows Vista has not been tampered with while the system was offline.

On computers that do not have a TPM version 1.2, BitLocker can still be used to encrypt the Windows operating system volume. However, this implementation requires the user to insert a USB startup key to start the computer or resume from hibernation. In addition, it does not provide the pre-startup system integrity verification offered by BitLocker working with a TPM.

Important: BitLocker can be implemented to encrypt the operating system volume either before or after installation of Microsoft Dynamics CRM for Outlook.

Note: For more information about BitLocker, see the TechNet article *BitLocker Drive Encryption Technical Overview* at: http://technet2.microsoft.com/WindowsVista/en/library/ce4d5a2e-59a5-4742-89cc-ef9f5908b4731033.mspx?mfr=true.

Hardware, Firmware and Software Requirements

BitLocker can only be used on computers that meet or exceed BitLocker system requirements. In addition, be sure to consider the following requirements:

- For BitLocker to leverage the system integrity check provided by a TPM, the computer requires a TPM version 1.2. Without one, enabling BitLocker requires saving a startup key to a removable USB device such as a flash drive.
- The system BIOS (for TPM and non-TPM computers) must support the USB mass storage device class, including reading small files on a USB flash drive in the pre-operating-system environment.
- The hard disk must be partitioned with at least two volumes:
    - The operating system volume (or boot volume) contains the Windows operating system and its support files; it must be formatted with the NTFS file system. BitLocker is enabled on this volume.
    - The system volume contains the files that are needed to load Windows after the BIOS has booted the platform. BitLocker is not enabled on this volume. For BitLocker to work, the system volume must not be encrypted, must differ from the operating system volume, and must be formatted with the NTFS file system. The system volume should be at least 1.5 gigabytes (GBs).

  Note: In Windows 7, drives are automatically prepared for use by BitLocker; there is no need to create separate partitions before turning on BitLocker.

System Recovery while Using BitLocker

A recovery process can be triggered by a number of scenarios, for example:

- Moving the BitLocker-protected drive into a new computer.
- Installing a new motherboard with a new TPM.
- Turning off, disabling, or clearing the TPM.
- Updating the BIOS.
- Upgrading critical early boot components that cause system integrity validation to fail.
- Forgetting the PIN when PIN authentication has been enabled.
- Losing the USB flash drive containing the startup key when startup key authentication has been enabled.

An administrator may also trigger recovery as an access control mechanism, for example, during computer redeployment. In addition, an administrator may decide to lock down an encrypted drive and require that users obtain BitLocker recovery information to unlock the drive. If BitLocker enters recovery mode, the data in the encrypted volume can be recovered through a process that requires minimal setup.

Note: For more detail, see the *Windows BitLocker Drive Encryption Step-by-Step Guide* at: http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true.

Encrypting File System

EFS is a built-in feature in Windows operating systems (Windows 7, Windows Vista, Windows XP, Windows 2000, Windows Server 2003, and Windows Server 2008) that provides for file- and folder-level encryption on NTFS file systems. Use EFS to protect confidential, sensitive data from people who have physical access to a computer. If an attacker obtains a mobile computer, file- or folder-level permissions (access control list) and authentication mechanisms are of little help. However, if the user account password is weak (for example a dictionary word) and were cracked, EFS would be defenseless. This scenario emphasizes the fact that there is no substitute for a strong password.

To *encrypt* a file, EFS uses a symmetric key, known as the File Encryption Key (FEK). The FEK uses the Advanced Encryption Standard (AES) algorithm with a 256-bit key. This FEK is then further encrypted with an asymmetric (RSA) key pair. The FEK is encrypted with the public key of the user who initiated the encryption, and the encrypted FEK is stored in the file header.

To *decrypt* the file, the file system requires the private key of the user to first decrypt the FEK. After the FEK is decrypted, the file system uses the FEK to decrypt the actual contents of the file. The operation is executed by the operating system and therefore transparent to the user.

Note: Users implementing EFS should always create a back up copy of the private key and store it in a secure location. Should the operating system be reinstalled or the hard disk be transferred to another mobile computer, data within encrypted files will remain inaccessible to users without the private key. For more detail about EFS, see *The Encrypting File System*: http://www.microsoft.com/technet/security/guidance/cryptographyetc/efs.mspx.

Important: In Windows 7 and Windows Server 2008 R2, the architecture of EFS has changed to incorporate elliptic curve cryptography (ECC). This enables EFS to be compliant with Suite B encryption requirements as defined by the National Security Agency to meet the needs of United States government agencies for protecting classified information. For more detail about these changes in EFS, see the TechNet article *Changes in EFS* at: http://technet.microsoft.com/en-us/library/dd630631(WS.10).aspx

Considerations for Implementing EFS

Before implementing EFS, be sure to review the factors described in the following table.

Consideration	Description
Compressed Drives	EFS cannot encrypt compressed drives, files, or folders. Compression and encryption are mutually exclusive. Encrypted files are decompressed.
FAT File System	Windows does not support EFS with FAT file system.
Private Keys and DPAPI	While a user is logged on, the users' private keys use Data Protection API (DPAPI). DPAPI uses derivatives of a user's logon credentials to protect data. This reemphasizes the usage of strong passwords.

Consideration	Description
Using Data Recovery Agent	Data recovery is a major concern if user keys are lost and cannot be retrieved. The data recovery process encrypts data for multiple entities. Typically, two entities are involved, the user initiating the encryption and a designated Data Recovery Agent (DRA) entity, such as an administrator within your domain. DRA keys are shadow keys in that data that is encrypted with the user's key is also encrypted with a copy of the DRA key. If the user's key is lost, DRA can apply its key to decrypt the data, which can then be re-encrypted with a new private key by the user. DRA does not guarantee private key recovery.
Using Key Archival and Recovery	With a key recovery mechanism, a certification authority (CA) within an enterprise is required to copy the user's private key and store the same key securely in the CA database. Auto-enrollment of user keys is also possible. If a user's private key is lost, then the CA administrator retrieves the user's private key from the database, eliminating the need for a DRA. However, using a DRA even in place of key recovery is useful in large organizations and is a recommended best practice. **Note:** For more information about data and key recovery, see the following resources: ▪ *How Do You Want to Recover BitLocker-Protected Drives?* http://technet.microsoft.com/en-us/library/ee706519(WS.10).aspx ▪ *Encrypting File System in Windows XP and Windows Server 2003*: http://technet.microsoft.com/en-us/library/dc261d01-f76c-dd44-94f5-2a5e027fdfa7.aspx. For more information about adding an EFS recovery agent, see the following resources: ▪ *Create a recovery certificate for encrypted files* http://windows.microsoft.com/en-US/windows7/Create-a-recovery-certificate-for-encrypted-files ▪ *How to add an EFS recovery agent in Windows XP Professional*: http://support.microsoft.com/kb/887414.
Windows System Files and Folders	Windows prevents encryption of system files and folders and everything under %SYSTEMROOT%
Sharing Files Encrypted with EFS	To learn about sharing files that are encrypted with EFS, see the topic *Share encrypted files* at: http://windows.microsoft.com/en-US/windows7/Share-encrypted-files.
Copying or Moving Encrypted Files	In general, copying encrypted files will result in the files inheriting the encryption properties of the target location. If files are moved instead, the files will not inherit the encryption properties of the target location

Consideration	Description
Event Logs and Dynamics CRM Events	Microsoft Dynamics CRM events are logged in event logs, which are by default created under System32\Config and cannot be encrypted. As a result, there is a possibility of some Microsoft Dynamics CRM data leakage on the hard disk.
Microsoft Dynamics CRM Tracing and EFS	If CRM tracing is enabled, the tracing folder should be encrypted, too. You can enable tracing using the client diagnostic tool distributed with Microsoft Dynamics CRM for Outlook. If tracing is enabled, the trace logs get written to the AppData\Microsoft\MSCRM\Traces.
Data Protection over the Network	EFS does not protect data while it is in transit over the network. For protection, configure the Microsoft Dynamics CRM server with HTTPS. **Note**: For information about how to set up HTTPS on Microsoft Dynamics CRM web servers, see the topic *Make Microsoft Dynamics CRM client-to-server network communications more secure* in the Microsoft Dynamics CRM Implementation Guide. **Important**: For on-premises deployments, you can further protect intra-domain communication by using IPSec. ▪ For details about configuring IPSec on computers running Windows 7, Windows Server 2008, and Windows Server 2008 R2, see the following resources: ○ *IPSec* http://technet.microsoft.com/en-us/network/bb531150 ○ *IPSec Tunneling* http://technet.microsoft.com/en-us/library/cc811544(WS.10).aspx ○ *Connection Security Rules* http://technet.microsoft.com/en-us/library/cc772017(WS.10).aspx ▪ For details about configuring IPSec on computers running Windows XP, see *Using Microsoft Windows IPSec to Help Secure an Internal Corporate Network Server* at: http://www.microsoft.com/downloads/details.aspx?familyid=A774012A-AC25-4A1D-8851-B7A09E3F1DC9&displaylang=en.

Preparing to Implement EFS for Microsoft Dynamics CRM Files

Before implementing EFS on mobile computers containing Microsoft Dynamics CRM data, be sure that you know the set up requirements for EFS, the specific folders and files that require encryption, and which applications and services to stop to ensure that EFS sets up successfully.

Assumptions

For the purposes of this white paper, mobile computers on which EFS will be configured are assumed to be running:

- Windows 7 SP1, Windows Vista Enterprise SP2, or Windows XP Professional SP3
- Microsoft Dynamics CRM for Outlook (default installation on drive C)
- Microsoft Office 2010, 2007, or 2003

In addition, it is assumed that the mobile computer user that will configure EFS is a:

- User of the installed Microsoft Dynamics CRM for Outlook application
- Member of the Local Administrators group on the mobile computer

Files and Folders to Encrypt

With a default installation on drive C, use EFS to encrypt the following files and folders:

- The Microsoft Dynamics CRM binaries that appear under:
  %PROGRAMFILES%\Microsoft CRM
- Microsoft Dynamics CRM Data under the user profile folder:
  AppData\Local\Microsoft\MSCRM

  This folder also contains the:
  - Database files MSCRM_MSDE.mdf and MSCRM_MSDE_log.ldf
  - Traces folder

    Note: Even with tracing enabled, it is not necessary to encrypt any folder separately.

Applications and Services to Stop before Implementing EFS

Prior to implementing EFS, be sure to perform the actions detailed in the following table.

Action	Detail
Shutdown Outlook	No instances of Outlook should be running.
Stop Cassini	Start Task Manager, and then on the **Processes** tab, look for Microsoft.Crm.Application.Hoster.exe; if it is listed, end the process manually.
Stop Indexing Services	Run services.msc, select **Indexing Services**, and then stop the service.
Change the SQL Server Service logon account to match the user account that is primarily using Microsoft Dynamics CRM for Outlook and has initiated encryption.	Run services.msc, select **SQL Server (CRM)** service, and then stop the service. On the **LogOn** tab, enter the appropriate logon credentials, and then click **OK**. The user account chosen will be granted Log On as a service right. On the **General** tab, start the service.

Note: If any file is in use, the encryption task will fail with an error. Use Process Explorer (http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx) to find the application that is locking the file that was reported as inaccessible.

Configuring EFS for Microsoft Dynamics CRM Folder and Files

Encrypting Folders and Files

▶ To encrypt Microsoft Dynamics CRM data by using EFS, perform the following procedure:

1. In Windows Explorer, navigate to %PROGRAMFILES%, right-click the **Microsoft CRM** folder, and then click **Properties**.
2. In the **Properties** dialog box, click **Advanced**.

   The **Advanced Attributes** dialog box displays attribute options for compression and encryption. This dialog box also includes archive and indexing attributes.

3. Select the **Encrypt contents to secure data** check box, and then click **OK** to close the **Advanced Attributes** dialog box.

   If the folder contains files, a **Confirm Attribute Changes** dialog box appears.
4. To encrypt all the contents of this folder, click **Apply changes to this folder, subfolders, and files**, and then click **OK**.
5. Repeat the previous steps to encrypt all the files and folders specified previously in the “Files and Folders to Encrypt” section.

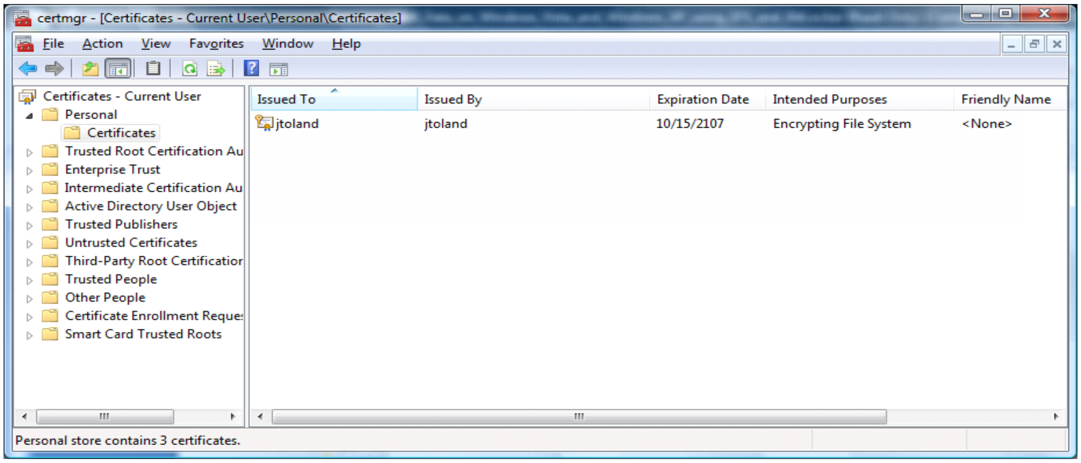
At this point, a self-signed certificate is created for EFS purposes. Ideally, the next step is to back up the private keys to a secure storage.

Backing up Private Keys

▶ To back up the private keys, perform the following procedure:

1. Log on to the mobile computer using the credentials provided when the data originally was encrypted.
2. In the Microsoft Management Console Certificates snap-in, run Certmgr.msc, and then, in the Console Root tree, navigate to the Certificates – Current User / Personal / Certificates folder.
3. Select the certificate that displays the name of the current user in both the **Issued To** and **Issued By** columns.

   Matching values in these columns indicate a “self-signed certificate.”
4. Ensure that the **Intended Purposes** column reads “Encrypting File System.”

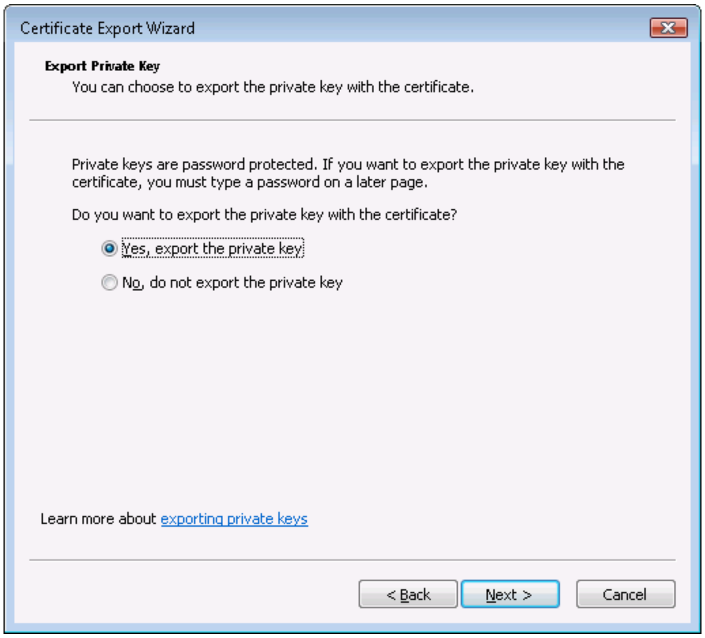

certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Other People
Certificate Enrollment Reque:
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
jtoland	jtoland	10/15/2107	Encrypting File System	<None>

Personal store contains 3 certificates.

5. Right-click the certificate to be exported, point to **All Tasks**, and then click **Export**.
6. On the first page of the Certificate Export Wizard, click **Next**.

7. On the **Export Private Key** page, under **Do you want to export the private key with the certificate**, select **Yes, export the private key**, and then click **Next**.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

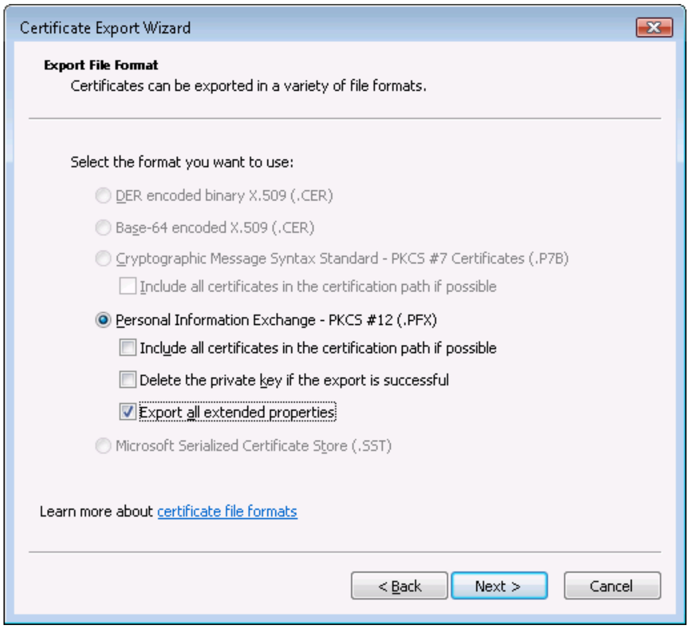
● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

8. On the **Export File Format** page, select the format of the exported key file. If the correct EFS key is selected for export, there will only be a single choice available, **Personal Information Exchange-r PKCS#12 (.PFX)**.

   There are three check boxes available for selection with this format.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

   □ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

   □ Include all certificates in the certification path if possible

   □ Delete the private key if the export is successful

   ☑ Export all extended properties

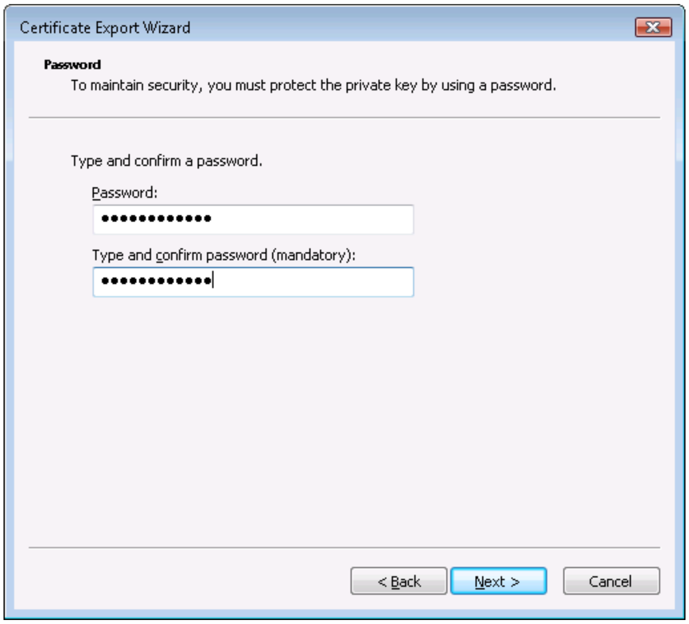
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

9. Select the **Export all extended properties** check box, and then click **Next**.

10. On the **Password** page, type and confirm the password with which you want the .pfx file to be encrypted.

    Provide a strong password that meets with your organization’s password policy.



Certificate Export Wizard

Password

To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password:

●●●●●●●●●●●●

Type and confirm password (mandatory):

●●●●●●●●●●●●

11. Click **Next**, and then specify a path and file name for the .pfx file.

    This should be a secure location mandated by key storage organization policies.

12. Click **Next**, ensure the summary matches your selections, and then click **Finish** to export the EFS certificate and private key to the .pfx file.

Ensure that the exported private key is stored at a different location (other than your mobile computer) as per the cryptography key storage practices in your organization.

Deleting and Importing the Private Keys

Some organizations may mandate deleting private keys after usage and importing them only at the time of usage. This may be done to ensure that the private key is not stored on the mobile computer unless encrypted data is in use, which reduces the possibility of malicious software accessing the private keys.

Delete a key during export

Start the process of exporting keys as listed in the previous “Back up the private keys” section. In step 8, on the **Export File Format** page, select the option **Delete the private key if export is successful**. Continue through steps 8-12 to finish exporting.

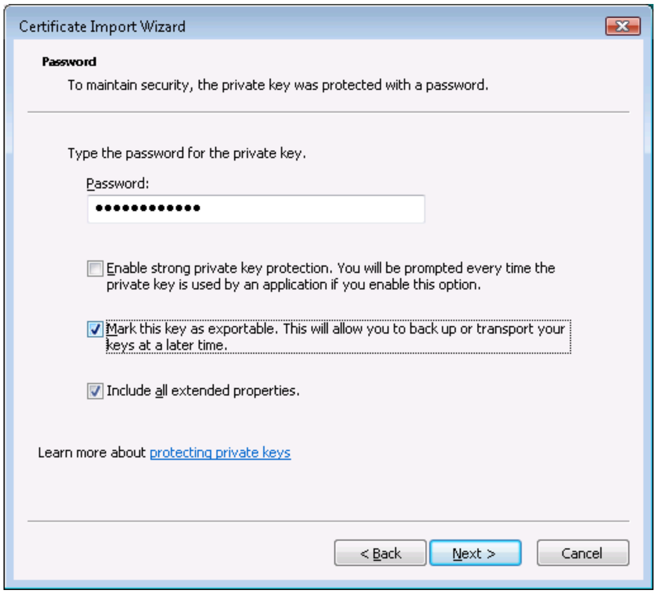
Import a private key

If an enterprise–wide private key recovery solution is provided, the user should follow the same. A user with physical access to the secure location storing the exported keys may import and use those keys.

Note that if the keys were previously deleted, the user must do a key import to ensure that the Microsoft Dynamics CRM for Outlook Compatibility Update starts without any errors. Because the keys for decryption must be available to the application before the data can be accessed, be sure to import them before starting Outlook.

- To import a private key, perform the following steps:

1. Log on to the mobile computer using the credentials that were provided when the data originally was encrypted, and then connect to the secure location storing the exported private key file.
2. Double-click the .pfx file to start the Certificate Import Wizard, provide the private key file name (.pfx file) and location, and then click **Next**.
3. On the **Password** page, provide the password used to lock the .pfx file during export, and then select the **Mark this key as exportable** check box.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●●●●●●●●●●

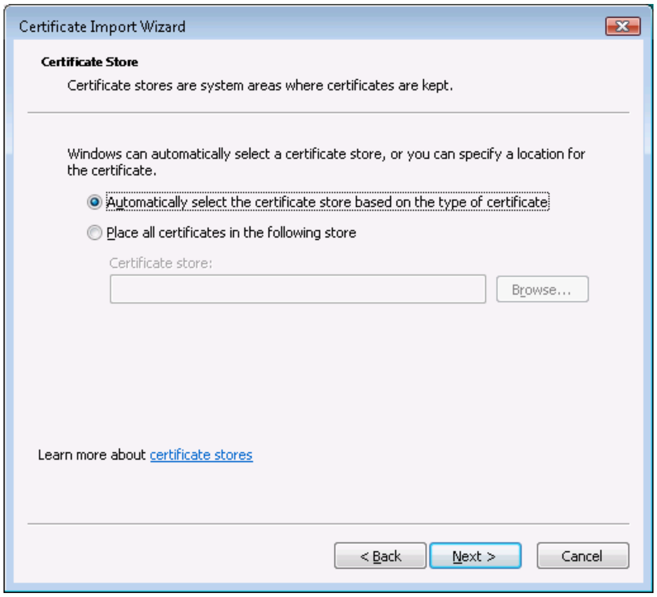
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

4. Click **Next**, and then on the **Certificate Store** page, ensure that **Automatically select the certificate store based on the type of certificate** is selected.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

5. Click **Next**, click **Finish** to complete the certificate import process, and then, in the **Import was successful** confirmation message, click **OK**.

Common Issues after a Restart or Private Key Deletion

If the private keys are deleted, the file system will not be able to decrypt your files the next time you start the mobile computer. To fix this, import the private keys from your secure location. If Microsoft Dynamics CRM for Outlook does not function correctly after the import, there are some known issues explained in the following scenarios.

Scenario A

Situation. Microsoft Dynamics CRM for Outlook was set to Offline mode. Outlook was closed. Private keys were deleted. The mobile computer was turned off. When you restart, the CRM toolbar is not loaded, and the Microsoft Dynamics CRM folders are not available in Outlook. This is caused because the Microsoft Dynamics CRM add-in for Outlook failed to load.

Resolution. If Microsoft Office 2010 is installed, on the **File** menu, click **Options**. In the **Options** dialog box, in the navigation pane, click **Add-Ins**, and then on the **Add and manage Office Add-ins** page, under **Add-ins**, remove and add Crmaddin.dll.

If Microsoft Office 2007 is installed, on the **Tools** menu, select **Trust Center**. In the **Trust Center** dialog box, in the navigation bar, select **Add-ins**, and then click **Go**. In the **COM Add-Ins** dialog box, select the **Microsoft Dynamic CRM Outlook Add-in** check box, click **Remove**, and then click **OK**. Restart Outlook, open the **COM Add-Ins** dialog box, and then click **Add** to include the add-in. Navigate to the install location for Microsoft Dynamics CRM for Outlook, select **Crmaddin.dll**, and then click **OK** twice. After it is included, the add-in should also start Cassini.

If Microsoft Office 2003 is installed, on the **Tools** menu, select **Options**. In the **Options** dialog box, click the **Other** tab, and then click **Advanced Options**. In the **Advanced Options** dialog box, click **COM Add-ins**. In the **COM Add-ins** dialog box, select the **Microsoft CRM Outlook Add-in** check box. Click **OK** to close all open dialog boxes, and then restart Outlook.

Scenario B

Situation. Microsoft Dynamics CRM for Outlook was set to Offline mode. Outlook was closed. Private keys were deleted. The mobile computer was turned off. When you restart and Outlook is started, Microsoft Dynamics CRM pages fail to load because the Cassini process failed to start.

Resolution. You must manually restart the Cassini process in this case. To do this, navigate to the Microsoft Dynamics CRM for Outlook installation folder, for example: %PROGRAMFILES%\ Microsoft CRM \Client\res\web\bin. Double-click **Microsoft.Crm.Application.Hoster.exe**.

Scenario C

Situation. Microsoft Dynamics CRM for Outlook cannot save any data in Offline mode, and you get an access denied message. This results from SQL Server being unable to write to the Microsoft Dynamics CRM databases.

Resolution. Ensure that the SQL Server service is running as the user account that encrypted the files.

Summary

In summary, when using BitLocker and EFS on a mobile computer running Microsoft Dynamics CRM for Microsoft Office Outlook:

- When used appropriately, the BitLocker and EFS features provided by Windows can be very secure.
- Data recovery and key recovery should be handled using any established PKI practices (such as DRA and private key recovery solutions) within an organization.
- Always remember to:
  - Use very strong passwords.
  - Maintain the safety and security of the BitLocker recovery key; it is the only means of booting the operating system in case of hardware failure or USB key loss.
  - Export the EFS private keys to a secure location.

Appendix A: Additional Resources

The following resources contain additional information about how to use BitLocker and EFS to protect Microsoft Dynamics CRM data that is stored on client computers running Windows 7 SP1, Windows Vista Enterprise SP2, or Windows XP Professional SP3.

- *BitLocker Drive Encryption in Windows 7: Frequently Asked Questions*
  http://technet.microsoft.com/en-us/library/ee449438(WS.10).aspx
- *Help protect your files using BitLocker Drive Encryption*
  http://windows.microsoft.com/en-US/windows7/Help-protect-your-files-using-BitLocker-Drive-Encryption
- *Windows BitLocker Drive Encryption Design and Deployment Guides*
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=18293
- *BitLocker Drive Encryption*
  http://msdn.microsoft.com/en-us/windows/hardware/gg487306.aspx