Microsoft

2007 Microsoft® Office System Document Encryption

June 2007

Microsoft® Office

Table of Contents

Introduction

The Microsoft 2007 Office system is a complete suite of productivity and database software that will help you save time and stay organized. Powerful contact management features help you manage all customer and prospect information in one place. You can develop professional marketing materials for print, e-mail, and the Web, and produce effective marketing campaigns in-house. You can create dynamic business documents, spreadsheets, and presentations, and build databases with no prior experience or technical staff. You will learn new features rapidly using the Microsoft® Office Fluent™ user interface that presents the right tools when you need them.

New tools help you work faster and create more professional documents, spreadsheets, and presentations. The Microsoft 2007 Office system helps you quickly accomplish routine tasks so you can spend more time with your customers. New task-based menus and toolbars automatically display the commands and options you can use, making it faster and easier to find the software features you need. And the new Live Preview feature makes it easy to sample your changes before you apply them.

In addition to the robust productivity enhancements included with the Microsoft 2007 Office system are new security advances. The Microsoft 2007 Office system was built with security in mind, using Microsoft's new Security Development Lifecycle approach for software development which provides a comprehensive framework of design, production, and testing methods and tools to ensure that code meets and exceeds current and anticipated security demands. The Microsoft 2007 Office system represents the most secure version of Office yet.

Encryption is the basis of securing electronic information. This paper discusses improvements in document encryption found in the Microsoft 2007 Office system We will discuss scenarios in which document encryption is valuable to the user, technical information regarding the Microsoft 2007 Office system document encryption and how to encrypt Microsoft 2007 Office system documents.

Benefits of Document Encryption

Organizations of all kinds need to protect information stored in 2007 Microsoft Office documents. Word documents, Excel spreadsheets and PowerPoint presentations can all contain information that needs to remain private, with access provided only to authorized persons inside or outside the organization. In some instances, inappropriate release of information contained in files could lead to theft of trade secrets, exposure of confidential customer information, or loss of significant amounts of money and brand equity. Companies in regulated industries could even face legal action if sensitive information is inadvertently disclosed. Therefore, protecting information and intellectual property should be a high priority for any company.

Recognizing the importance of protecting the information in Microsoft 2007 Office system files, Microsoft provides a number of security technologies that can protect that information. Examples of these technologies include:

- **Internet Protocol Security (IPSec) network encryption** IPSec is the preferred method used to encrypt information while it is in transit over the network. Once the information reaches the destination, IPSec no longer protects the information.
- **Rights Management Services (RMS) and Information Rights Management (IRM)** Windows Rights Management Services enables end-to-end protection and control over who can read, print, change, forward or copy a document. Information Rights Management extends RMS to Microsoft 2007 Office system applications. Rights Management Services depends on a supporting infrastructure that includes Certificate Services (PKI), Windows Rights Management Services server(s), Internet Information Services, Microsoft Active Directory and SQL Server, along with RMS client software and RMS-enabled applications.
- **Encrypting File System (EFS)** EFS is a feature of the NTFS file system that enables users to encrypt files and folders while they're stored on disk. This protects the documents from other users when machines are shared. However, when these documents are sent over the network, such as over e-mail or during file copy

operations, EFS encrypted documents are unencrypted. Some other mechanism must be used to protect EFS encrypted documents as they move "over the wire".

- **NTFS File System** The NTFS file system enables users to set permissions on who can access documents on disk. Any user who does not have permission to open the file will not be able to view the document. This is especially useful in shared computer scenarios.
- **BitLocker** BitLocker is a whole volume encryption technology in Microsoft Windows® Vista™ that enables users to encrypt the contents of the entire disk volume on which the operating system is installed. Volume encryption protects all files and folders on the protected volume. BitLocker is especially effective at protecting disk contents from being retrieved by so-called "offline attacks" where the attacker might try to boot an alternate operating system to retrieve the disk contents.
- **Microsoft 2007 Office system Document Signing** 2007 Office System document signing enables users to digitally sign documents. The digital signature confirms electronically the author of the document and also informs readers of the document if it has been changed since the document is signed; this protects against attackers intercept private documents and attempt to change the contents to meet their objectives.
- **Microsoft 2007 Office system Document Encryption** 2007 Office System document encryption enables users to encrypt Word, Excel and PowerPoint documents with a password. Only users who have entered the correct password can subsequently open the document.

While IPSec, RMS, EFS and BitLocker all provide support for a defense in depth plan for Microsoft 2007 Office system document protection, Microsoft 2007 Office system document encryption can be used in a greater variety of environments and provide protection for Office documents when the supporting infrastructure for these other technologies is not available, and can provide an added layer of protection in conjunction with these technologies as part of a multi-layered security strategy.

The following scenarios highlight some advantages of Microsoft 2007 Office system document encryption:

- An accountant in a small accounting firm needs to send financially sensitive information over the Internet to her clients. She must protect this private information from being intercepted and read by anyone other than the clients. The accountant uses Microsoft 2007 Office system document encryption to set a password on the spreadsheets and calls the clients to provide them with their passwords.
- Managers of a large hedge fund need to communicate with a number of partners about an upcoming merger. There are Word documents, Excel spreadsheets and PowerPoint presentations that must be shared. While the hedge fund managers have recently put together a Rights Management Solution for their organization, they haven't yet extended the solution to include partners outside the local network. Hedge fund executives use Microsoft 2007 Office system document protection to ensure that documents can only be opened by trusted partners.
- Road warriors for an insurance firm are instructed to upload expense reports to a directory on an FTP server. The traveling salespeople encrypt their expense report spreadsheets to prevent them from being from being read should they be intercepted over the unsecure FTP protocol.

As these scenarios illustrate, Microsoft 2007 Office system document encryption is a vital part of a secure Office document defense in depth strategy. Microsoft 2007 Office system enables you to use passwords to help prevent other people from opening or modifying Microsoft Office Word 2007 documents, Microsoft Office Excel 2007 workbooks, Microsoft Office OneNote 2007 notebooks and Microsoft Office PowerPoint 2007 presentations. This password protection is easy for users to implement and doesn't require any complex infrastructure changes; all it requires is that users have the Microsoft 2007 Office system installed on their computers.

Microsoft 2007 Office system Document Encryption Improvements

Password protection is not a new concept in the Microsoft 2007 Office system, but it has been made stronger and easier to use. Previous versions of Microsoft Office used an RC4 stream cipher with a key length of up to 128 bits. The problem with this approach was that when changes are made to the encrypted document and the document is saved, the initialization vector (IV) remains unchanged and the same keystream is used to encrypt subsequent versions of the encrypted document. This weakness in the implementation of the RC4 encryption algorithm made it possible for hackers compare two versions of a password-protected file to discover the contents and allow unauthorized users to read its contents. A number of software companies took advantage of these limitations to make "password recovery utilities" that could decrypt RC4-protected documents. Obviously, it was time to move to a now a new means of encrypting documents.

Microsoft 2007 Office system document encryption is a significant improvement. The encryption information block is the same as in previous versions of Office, but the Microsoft 2007 Office system uses the Advanced Encryption Standard (AES) encryption, which is the strongest industry-standard algorithm available and was selected by the National Security Agency (NSA) to be used as the standard for the U.S. Government, AES has a default 128-bit key (which can be increased to 256-bit via the Windows Registry) and uses SHA-1 hashing. In addition, The Microsoft 2007 Office system improves the algorithm of converting passwords into keys: 50,000 SHA-1 sequential iterations are performed.

Some key facts about Microsoft 2007 Office system document encryption:

- Only Microsoft Word 2007 documents, Microsoft Excel 2007 workbooks, and Microsoft PowerPoint 2007 presentations can be encrypted using the built-in Microsoft 2007 Office system encryption feature.
- The default encryption algorithm is AES 128-bit. This value can be increased to AES 256-bit via a Registry entry, local security policy, or domain Group Policy.

- AES encryption is supported for Open XML formats used in previous versions of Microsoft Office when those documents are created in an Microsoft 2007 Office system application. However, documents saved in the older Office binary formats can only be encrypted using RC4 to maintain compatibility with older versions of Microsoft Office.
- AES support is a function of the operating system's cryptographic services providers (CSPs). AES encryption is supported on Windows Server 2003, Windows XP SP2 and Windows Vista.
- The level of protection provided by the AES encryption is related to the strength of the password used to protect the document. You should use complex passwords that include upper and lower case letters, numbers and symbols and that are at least 8 characters long.
- Password complexity cannot be enforced for Microsoft 2007 Office system encryption. Users should be encouraged to use complex passwords during training.
- There are no administrative settings that force users to encrypt documents

It's important to note that there are two options to add a password in Microsoft 2007 Office system documents. One option enables you to encrypt the document using a password; this is referred to as a **Password to open**. The second option does not use any encryption. It is designed so you can collaborate with content reviewers you trust, but is not designed to help make the file more secure. This is referred to as the **Password to modify**. These two options appear in Figure 1.

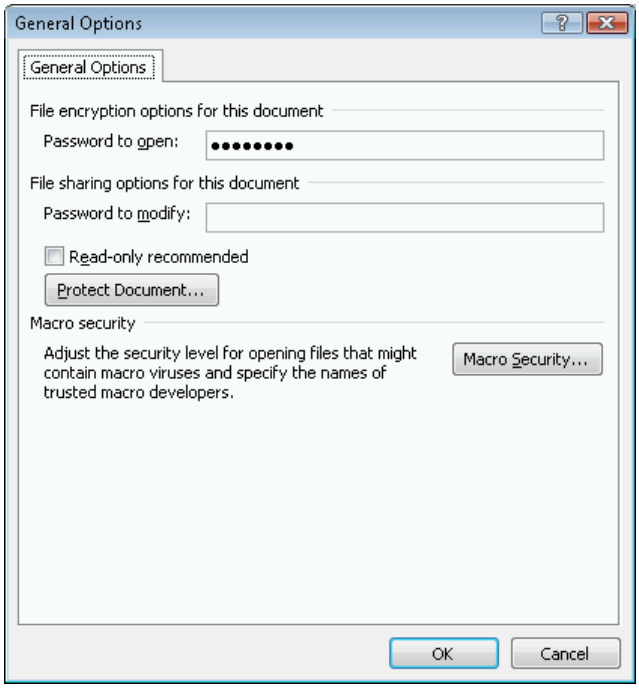

Figure 1: Setting passwords to open and modify an Microsoft 2007 Office system document.

Compatibility is always a concern among administrators planning a rollout of a new version of Microsoft Office. In a scenario where users need to share Microsoft 2007 Office system documents with others who have previous versions of Microsoft Office, document encryption can still be enforced with the help of the **Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats** which can be downloaded at http://www.microsoft.com/downloads/details.aspx?FamilyId=941B3470-3AE9-4AEE-8F43-C6BB74CD1466&displaylang=en

The Compatibility Pack enables users with Microsoft Office XP or Office 2003 to enter a password and read Microsoft 2007 Office system encrypted documents *if* the user is running an operating system supporting the AES encryption algorithm. Thus, in order for Office XP or Office 2003 users using the Compatibility Pack to open a Microsoft 2007 Office system encrypted document, they must be using Windows Server 2003, Windows XP SP2 or Windows Vista as their operating system.

End-User Microsoft Office Document Encryption

Encrypting a Microsoft 2007 Office system Word, Excel or PowerPoint document is easy. Users can use one of two ways to encrypted an Office document: from the **Office Button** or from the **Save As** dialog box.

Encrypting a Document using the Office Button

Perform the following steps to encrypt a document from the Office Button:

1. Click the **Office Button** and point to **Prepare**. Click **Encrypt Document**.

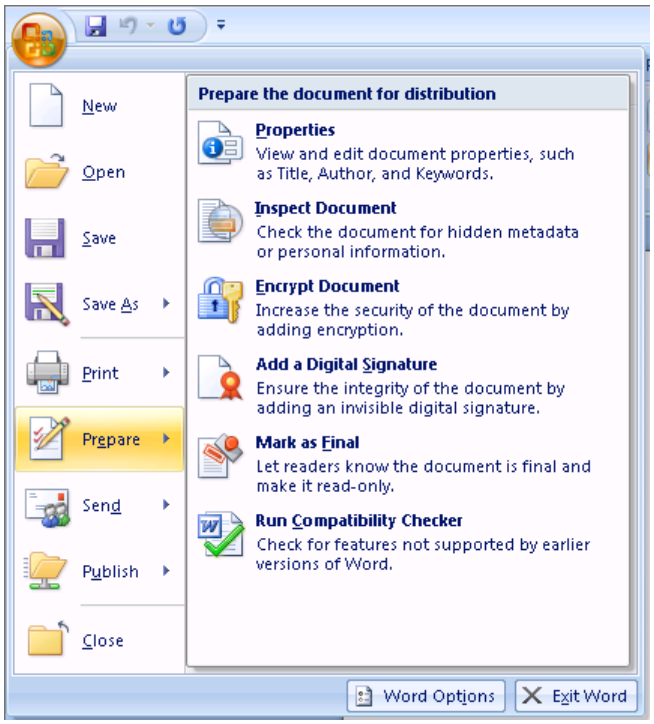

Figure 2: Selecting the Encrypt Document option from the Office Button

2. In the **Encrypt Document** dialog box, enter a password in the **Password** text box. Keep in mind that if you lose or forget the password, it cannot be recovered. Click **OK**.

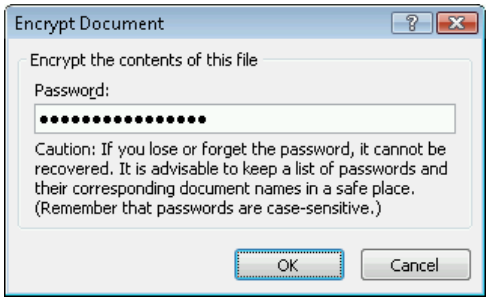

Figure 3: Entering a password to encrypt the document

3. In the **Confirm Password** dialog box, reenter your password in the **Reenter password** text box. Click **OK**.

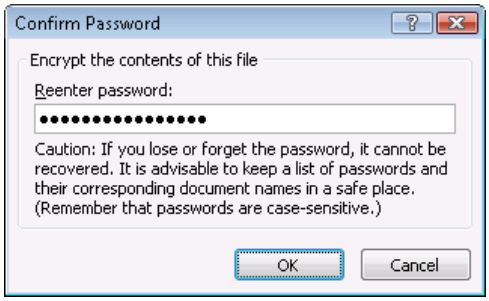

Figure 4: Confirming the encryption password

The document is now encrypted and no one will be able to view the document without entering the password.

Encrypting a Document from the Save As Dialog Box

You also have the option to encrypt a document with a password when saving the document.

Perform the following steps to encrypt the document during a Save As operation:

1. Click the Office Button and then click **Save As**.

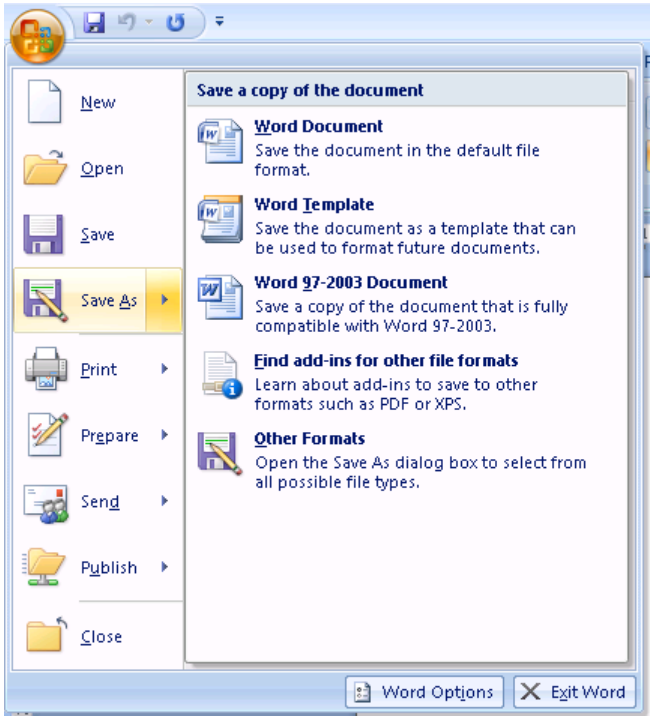

Figure 5: Using the Save As option to encrypt a document

2. In the **Save As** dialog box, enter a name for the document and then click the **Tools** button. Click **General Options** on the drop down list.

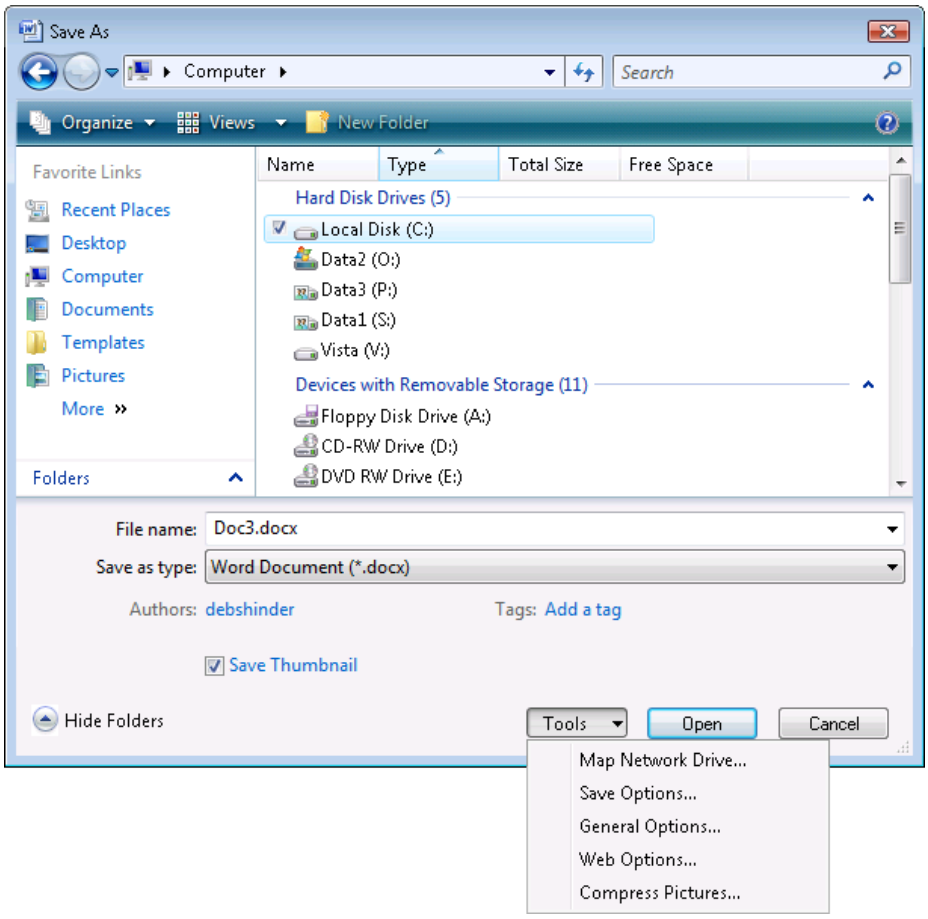

Figure 6: Using General Options to encrypt the document

3. In the **General Options** dialog box, enter a password to encrypt the document in the **Password to open** text box and then click **OK**.

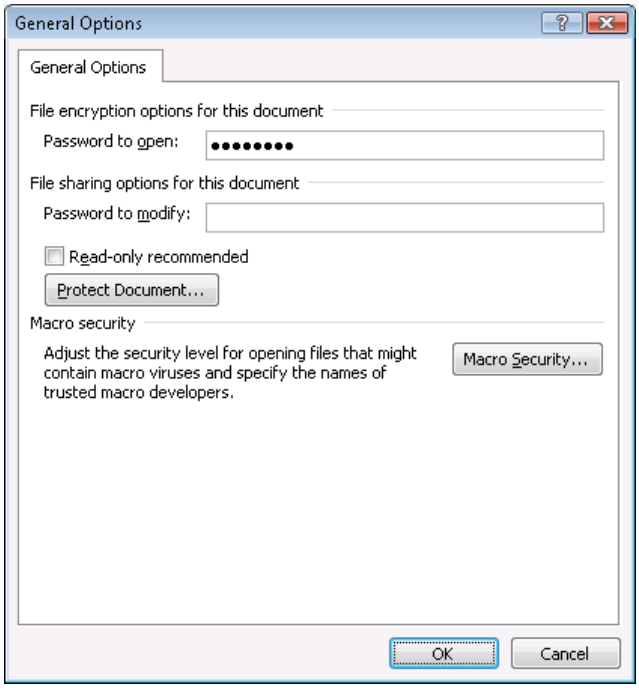

Figure 7: Entering an encryption password in the Generation Options dialog box

4. In the **Confirm Password** dialog box, reenter the password in the **Reenter password to open** text box and then click **OK**.

Figure 8: Reentering the encryption password

5. Click **Save** in the **Save As** dialog box to save the document.

Document Encryption for the Network Administrator

There are two ways that network administrators can control how documents are encrypted in Microsoft 2007 Office system. These include the Office Customization Tool and Active Directory Group Policy.

Configure Document Protection Settings by using the Office Customization Tool

Use the following procedure to configure encryption settings for Office Open XML Formats files. Before you perform this procedure, you must know the cryptographic service provide (CSP), the cryptographic algorithm, and the key length that you want to use for encryption settings. The following registry key contains a list of the CSPs that are installed on a computer:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Defaults/Provider
```

Configure encryption settings for Office Open XML Formats files

1. In the left pane of the OCT, under **Features**, click **Modify user settings**.
2. In the tree view of the OCT, open **Microsoft Office 2007 system**, and click **Security Settings**.
3. In the details pane, double-click **Encryption type for password protected Office Open XML files**.
4. Click **Enabled**, and in **Encryption type** enter the following information, separated by commas:

   CSP

   Cryptographic algorithm

   Key length

5. Verify that your entry looks like the following example (no spaces are allowed on either side of the commas):

For Windows Server 2003 and Windows Vista:

```
Microsoft Enhanced RSA and AES Cryptographic Provider,AES 128,128
```

For Windows XP:

```
Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype),AES
128,128
```

6. Click **OK** to save your settings.

Use the following procedure to configure encryption settings for Office 97-2003 format files. Note that AES cannot be used to protect binary formatted documents (e.g., .doc, .xls and .ppt). Before you perform this procedure, you must know the CSP, the cryptographic algorithm, and the key length that you want to use for encryption settings. The following registry key contains a list of the CSPs that are installed on a computer:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Defaults/Provider
```

Configure encryption settings for Office 97-2003 format files

1. In the left pane of the OCT, under **Features**, click **Modify user settings**.
2. In the tree view of the OCT, open **Microsoft Office 2007 system**, and click **Security Settings**.
3. In the details pane, double-click **Encryption type for password protected Office 97-2003 files**.
4. Click **Enabled**, and in **Encryption type** type the following information, separated by commas:

   CSP

   Cryptographic algorithm

   Key length

5. Verify that your entry looks like the following example (no spaces are allowed on either side of the commas):

   ```
   Microsoft Enhanced Cryptographic Provider v1.0, RC4, 128
   ```

6. Click **OK** to save your settings.

You can deploy document protection settings by using the Setup program or by using the Windows Installer program. For more information, see Run Setup for the 2007 Office system on users' computers and Change users' configurations after installing the 2007 Office system

Configure Document Protection Settings using Group Policy

Use the following procedure to configure encryption settings for Office Open XML Formats files. Before you perform this procedure, you must know the CSP, the cryptographic algorithm, and the key length that you want to use for encryption settings. The following registry key contains a list of the CSPs that are installed on a computer:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Defaults/Provider
```

Configure encryption settings for Office Open XML Formats files

1. In the Group Policy Object Editor tree, navigate to the following:
   User Configuration/Administrative Templates/Microsoft Office 2007 system/Security Settings
2. In the details pane, double-click **Encryption type for password protected Office Open XML files**.
3. Click **Enabled**, and in **Encryption type** type the following information, separated by commas:

   CSP

   Cryptographic algorithm

   Key length
4. Verify that your entry looks like the following example (no spaces are allowed on either side of the commas):

   For Windows Server 2003 and Windows Vista:

   ```
   Microsoft Enhanced RSA and AES Cryptographic Provider,AES 128,128
   ```

   For Windows XP:

   ```
   Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype), AES 128,128
   ```

5. Click **OK** to save your settings.

Use the following procedure to configure encryption settings for Office 97-2003 format files. Before you perform this procedure, you must know the CSP, the cryptographic algorithm, and the key length that you want to use for encryption settings. The following registry key contains a list of the CSPs that are installed on a computer:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Defaults/Provider
```

Configure encryption settings for Office 97-2003 format files

1. In the Group Policy Object Editor tree, navigate to the following:

   User Configuration/Administrative Templates/Microsoft Office System 2007/Security Settings

2. In the details pane, double-click **Encryption type for password protected Office 97-2003 files**.
3. Click **Enabled**, and in **Encryption type** type the following information, separated by commas:

   CSP

   Cryptographic algorithm

   Key length

4. Verify that your entry looks like the following example (no spaces are allowed on either side of the commas):

   ```
   Microsoft Enhanced Cryptographic Provider v1.0, RC4, 128
   ```

5. Click **OK** to save your settings.

Summary

The Microsoft 2007 Office system introduces a number of new security improvements aimed at protecting your private data. One of the most effective ways to protect data is by using Microsoft 2007 Office system document encryption. Microsoft 2007 Office system document encryption is greatly improved over encryption methods used for previous versions of Microsoft Office and introduces industry-standard AES encryption support. Using Microsoft 2007 Office system document encryption, you can prevent users without the encryption password from opening Microsoft Office Word 2007 documents, Excel 2007 workbooks and PowerPoint 2007 presentations. Microsoft 2007 Office system document encryption should be used as part of a secure defense in depth strategy for protecting private information stored in Office documents.