Report Number: C4-017R-01

Guide to Using DoD PKI Certificates in Outlook 2000

Security Evaluation Group

Author:
Margaret Salter

Updated: April 6, 2001
Version 1.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2Kguides@nsa.gov

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 16-04-2001	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE
Guide to Using DoD PKI Certificates in Outlook 2000
Unclassified

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Salter, Margaret ;

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
National Security Agency
9800 Savage Road, Suite 6704
Ft. Meade, MD20755-6704

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
National Security Agency
9800 Savage Road, Suite 6704
Ft. Meade, MD20755-6704

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The purpose of this guide is to provide detailed information on the configuration of Office 2000 in order to permit the use of DoD PKI Certificates and the checking of Certificate Revocation Lists (CRLs).

15. SUBJECT TERMS
IATAC Collection; information security; configuration management

16. SECURITY CLASSIFICATION OF:

a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 17	19. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil

19b. TELEPHONE NUMBER
International Area Code
Area Code Telephone Number
703767-9007
DSN
427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 4/16/2001	**3. REPORT TYPE AND DATES COVERED** Report 4/16/2001

4. TITLE AND SUBTITLE
Guide to Using DoD PKI Certificates in Outlook 2000 (Report Number: C4-017R-01)

5. FUNDING NUMBERS

6. AUTHOR(S)
Salter, Margaret

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Seucrity Agency
9800 Savage Road, Suite 6704
Ft. Meade, MD 20755-6704

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Security Agency
9800 Savage Road, Suite 6704, Ft. Meade, MD
20755-6704

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The purpose of this guide is to provide detailed information on the configuration of Office 2000 in order to permit the use of DoD PKI Certificates and the checking of Certificate Revocation Lists (CRLs).

14. SUBJECT TERMS
IATAC Collection, information security, configuration management

15. NUMBER OF PAGES
15

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** UNLIMITED

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
4/16/2001

3. REPORT TYPE AND DATES COVERED
Report 4/16/2001

4. TITLE AND SUBTITLE
Guide to Using DoD PKI Certificates in Outlook 2000 (Report Number: C4-017R-01)

5. FUNDING NUMBERS

6. AUTHOR(S)
Salter, Margaret

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Seucrity Agency
9800 Savage Road, Suite 6704
Ft. Meade, MD 20755-6704

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Security Agency
9800 Savage Road, Suite 6704, Ft. Meade, MD
20755-6704

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The purpose of this guide is to provide detailed information on the configuration of Office 2000 in order to permit the use of DoD PKI Certificates and the checking of Certificate Revocation Lists (CRLs).

14. SUBJECT TERMS
IATAC Collection, information security, configuration management

15. NUMBER OF PAGES
15

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UNLIMITED

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of April 6, 2001. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Trademark Information

This Page Intentionally Left Blank

Table of Contents

Table of Figures

Introduction

The purpose of this guide is to provide detailed information on the configuration of Office 2000 in order to permit the use of DoD PKI Certificates and the checking of Certificate Revocation Lists (CRLs).

Getting the Most from this Guide

The following list contains suggestions to successfully use the *Guide to Using DoD PKI Certificates in Outlook 2000*:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide.
  - Ensure that the latest Windows 2000 service pack and hotfixes have been installed. For further information on critical Windows 2000 updates, see the Windows Update for Windows 2000 web page.
- Follow the security settings that are appropriate for your environment.

About the Guide to Using DoD PKI Certificates in Outlook 2000

This document consists of the following chapters:

Chapter 1, "Outlook 2000 Certificate Configuration," contains information on configuring DoD PKI certificates, suppressing name checking, enabling service release features, and checking Certificate Revocation Lists (CRLs).

Appendix A, "References," contains a list of resources cited.

This Page Intentionally Left Blank

Chapter

1

Outlook 2000 Certificate Configuration

Previous versions of Outlook are compatible with S/MIME version 2. In S/MIME version 2, certificates for email are required to have the correct email address in the certificate. In S/MIME version 3, the email address is not required to be in the certificate. Microsoft Outlook 2000 can be configured to conform to S/MIME version 3 and use any valid certificate for email. In addition, Outlook 2000 can be configured to check Certificate Revocation Lists (CRLs) for the entire certificate chain of an email certificate. This paper shows the changes that need to be made to the configuration of Office 2000 to permit the use of DoD PKI Certificates and the checking of CRLs.

DoD PKI Certificates

The DoD PKI intends to issue two certificates to all users - one certificate to be used for encryption and one to be used for signing. These certificates will not contain any user information that changes frequently. The email address of the user, for instance, will not be in the certificate. Both of these certificates are used for email, one to sign outgoing messages and one to decrypt incoming encrypted email. The certificates will contain an extension called the Certificate Revocation List Distribution Point (CDP). This extension should contain a URL that is used to obtain the latest CRLs from the DoD.

Suppress Name Checking

To use a certificate without an email address in Outlook 2000, you need to have your system administrator add the following registry key:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Office/9.0/Outlook/Security
```

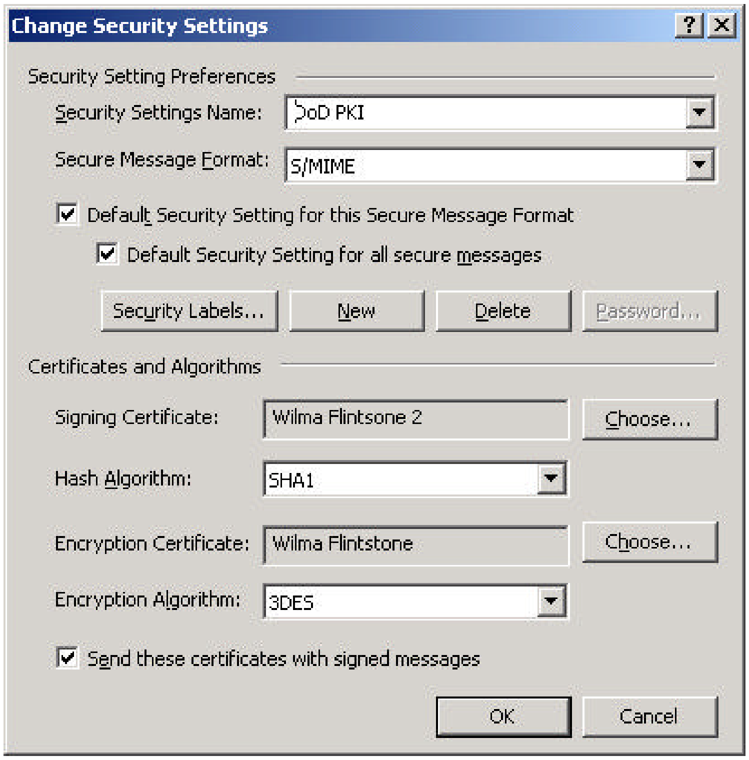
Then add a new DWORD value called `SupressNameChecks` and set it to `0x1`. The conscientious spellers out there will want to note the misspelling of the word `Supress` in this key. Make sure that it is spelled exactly as above (with only one p in `Supress`). This will allow the use of certificates without the email address check being applied.

Choose the DoD PKI Certificates

To use your DoD PKI Certificates to sign and receive encrypted email (See **Figure 1**):

- ❑ Open Outlook 2000
- ❑ Click on the **Tools** menu and select **Options**.

- ❑ Select the **Security** tab
- ❑ Click on the **Settings** button.
- ❑ Click on the **New** button to create a new set of security settings. Give the setting a name. If you wish to use this setting as default for all email messages, check the default buttons.
- ❑ Use the **Choose** button to select the certificates to be used for signing and encryption. In this window you should also choose SHA1 as the hash and 3DES for encryption. These certificates will now be used to sign and encrypt your email.



Change Security Settings

Security Setting Preferences

Security Settings Name: DoD PKI

Secure Message Format: S/MIME

☑ Default Security Setting for this Secure Message Format

☑ Default Security Setting for all secure messages

Certificates and Algorithms

Signing Certificate: Wilma Flintsone 2

Hash Algorithm: SHA1

Encryption Certificate: Wilma Flintstone

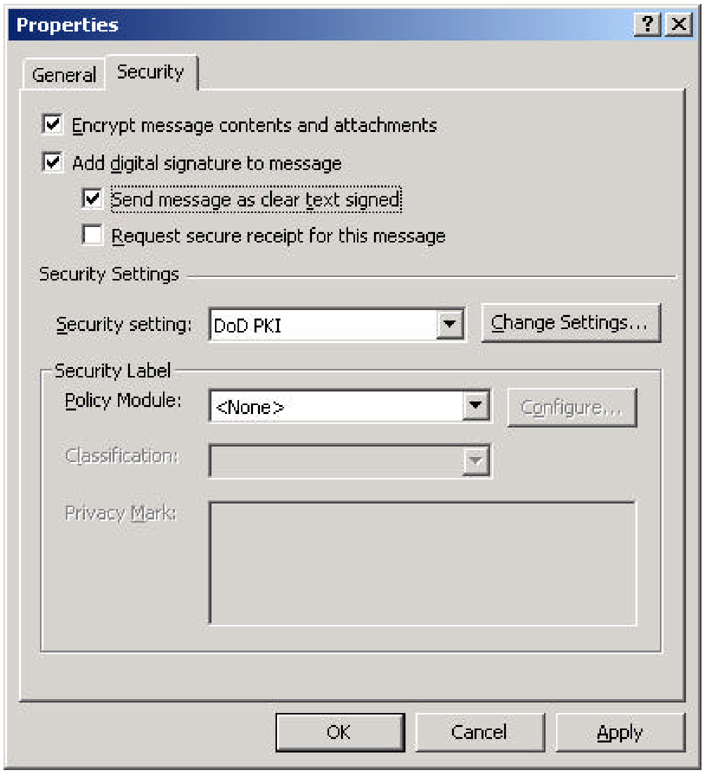
Encryption Algorithm: 3DES

☑ Send these certificates with signed messages

Figure 1 – Changing the Security Settings Dialog Box

For any given message that you are sending, you can check that these settings are the ones being applied to the message (See **Figure 2**):

- ❑ In the message composition window under the **File** menu, choose **Properties**.
- ❑ Select the **Security** tab. Choose the **Security Setting** that you created using the window above. Make sure that you have chosen to encrypt and/or sign the message.



☑ Encrypt message contents and attachments

☑ Add digital signature to message

☑ Send message as clear text signed

□ Request secure receipt for this message

Security Settings

Security setting: DoD PKI

Security Label

Policy Module: <None>

Classification:

Privacy Mark:

Figure 2 – Checking Security Setting Dialog Box

Enable Service Release Features

Outlook can be configured to display more information about the certificates being used in the email tool. Specifically, the status of the CRLs for the certificates can be displayed. To enable these extra security displays, you need to have your system administrator edit the following registry key:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Office/9.0/Outlook/Security
```

Then add a new DWORD value called `EnableSRFeatures`, and set it to `0x1`. Once this setting is added, you will see that the displays of information are different when you click on either the certificate icon or the lock icon on any signed or encrypted email.

Get and Check the CRL

Outlook does not currently download the CRL without some modification to the registry. The system administrator needs to add the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\{7801ebd0-
cf4b-11d0-851f-0060979387ea}
```

Then add a new DWORD value called `PolicyFlags` and set it to `0x00010000`. This causes Outlook to actually download the CRL. Verify that the CRL was downloaded by opening Internet Explorer and performing the following steps:

- In the Internet Explorer menu, select **Tools** → **Options**
- Click the **General** tab
- Click **Settings**. This will present you with another dialog box.
- Select **View Files** and you should see the CRLs in the Temporary Internet Files.

Unfortunately, the Outlook 2000 display still indicates that the CRL's were not checked. To get the results of the CRL checking displayed by the Outlook software, you must also apply a hotfix. The number of the hotfix is `Q269784`, but you must obtain it by directly contacting Microsoft.

Appendix

A

References

Microsoft's Web Page, http://www.microsoft.com/

Windows Update for Windows 2000 Web Page,
http://www.microsoft.com/windows2000/downloads/default.asp