MANUAL

Using digital certificates in
Microsoft Outlook

<div align="right">

Version: 4.0

Date: 26.01.2018

103.14

</div>

KIBS AD Skopje

http://www.kibstrust.mk

Table of Contents

1. Introduction

The options for using the digital certificates in the English version of Microsoft Outlook 2010/2013/2016 are shown in this manual.

To start sending electronically signed and/or encrypted messages with the application for electronic mail Outlook, it is required to own a personal digital certificate with features for signing and encrypting of the electronic messages and must be imported in the Internet Explorer web browser.

2. Installing a certificate and security settings

In Microsoft Outlook, choose **File** from the menu and click on **Options** (Figure 1)
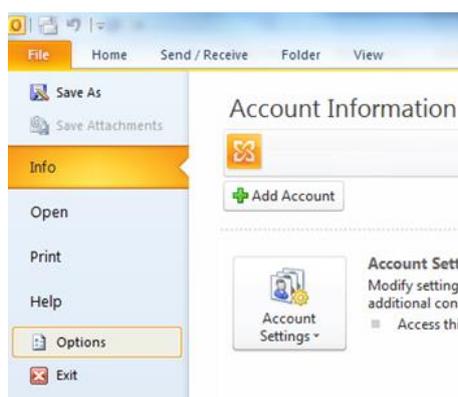

Figure 1

A new windows appears where you can change different settings for MS Outlook. In this window, select the **Trust Center** option (Figure 2). In the Microsoft Outlook Trust Center frame, click on the **Trust Center Settings**… button, which opens a new window.
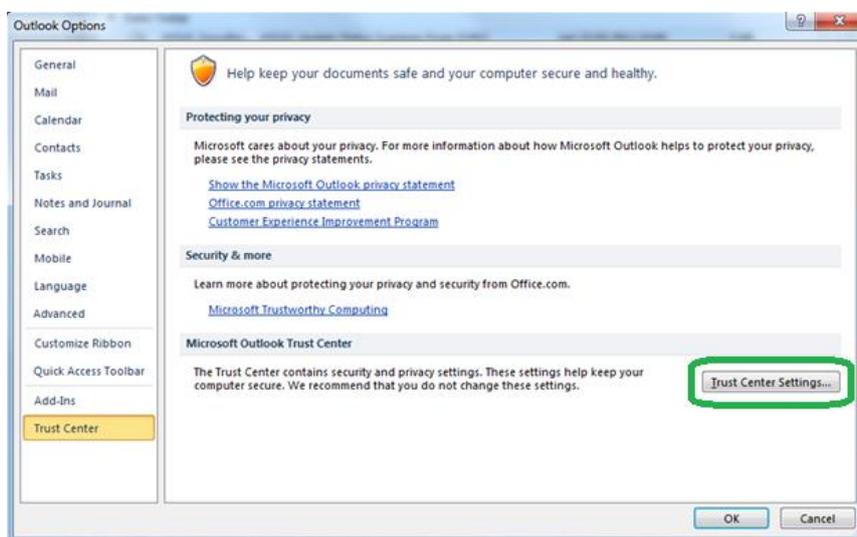

Figure 2

In the new windows, from the options on the left hand side, select the **E-mail Security** option (Figure 3).
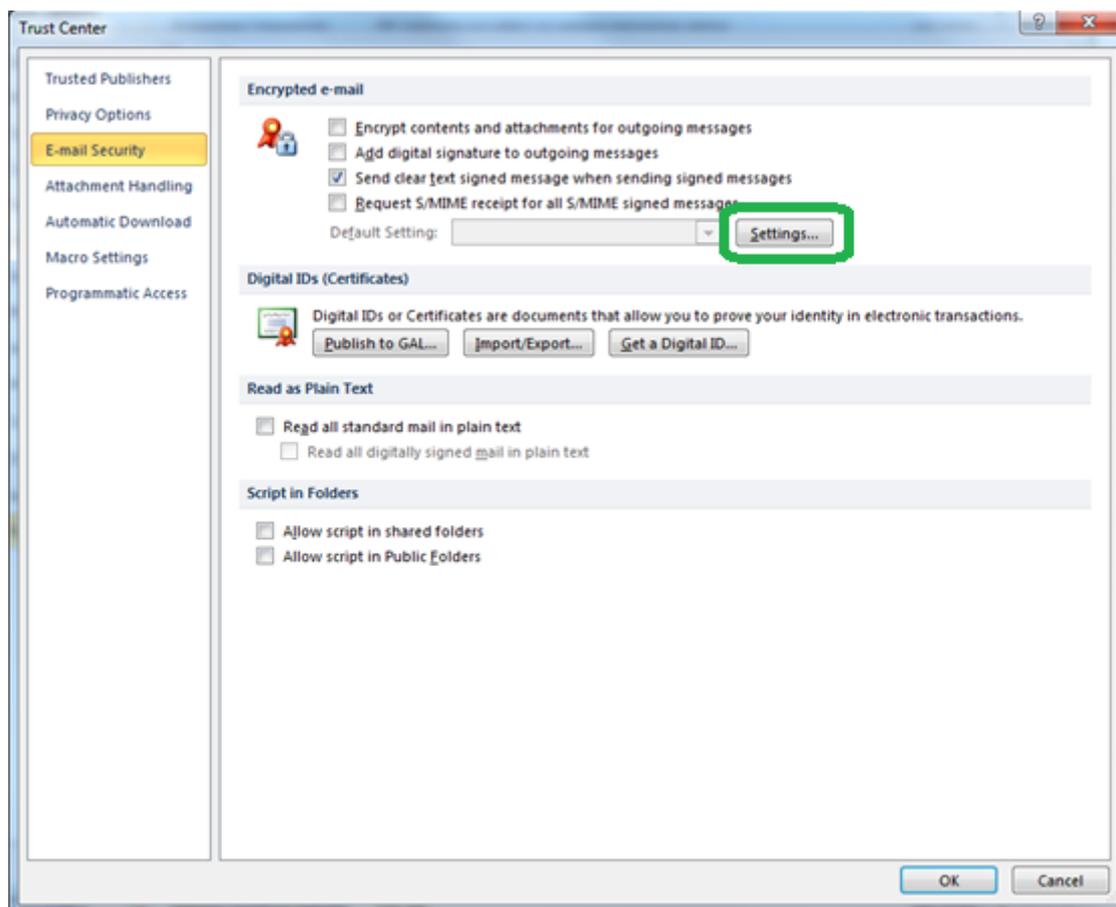
Figure 3

In **Encrypted e-mail**, by choosing the "Encyrpt contents and attachments for outgoing messages" option, every sent message will always be electronically encrypted. If you choose the "Add digital signature to outgoing messages" option, every sent message will be electronically signed.

Recommendation: Do not choose the option for encrypting all of your messages, instead encrypt only those messages that you want to protect. Do not choose the option for signing every message, instead sign only those messages that you wish to sign.

To define which certificate you will use when sending signed messages with encrypted or clear text, it is necessary to click on the **Settings…** button, which will open the next window for changing the security settings (Figure 4).

Enter your name and surename in the **Security Settings Name** field. Choose the options **Default Security Setting for this cryptographics message format** and **Default Security Settings for all cryptographic messages**.
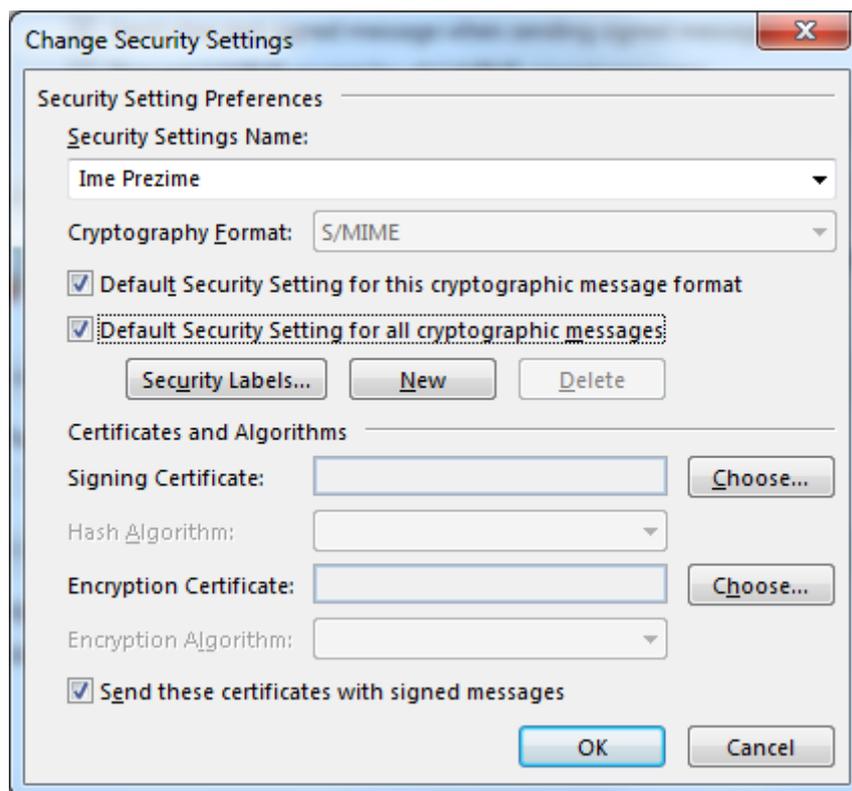
Figure 4

The **Certificates and Algorithms** part enables you to choose the certificate which will be used for signing or encrypting your electronic messages and the algorithms for signing and encrypting. For setting a certificate for the digital signature, click on the **Choose…** button and choose a certificate (Figure 5).
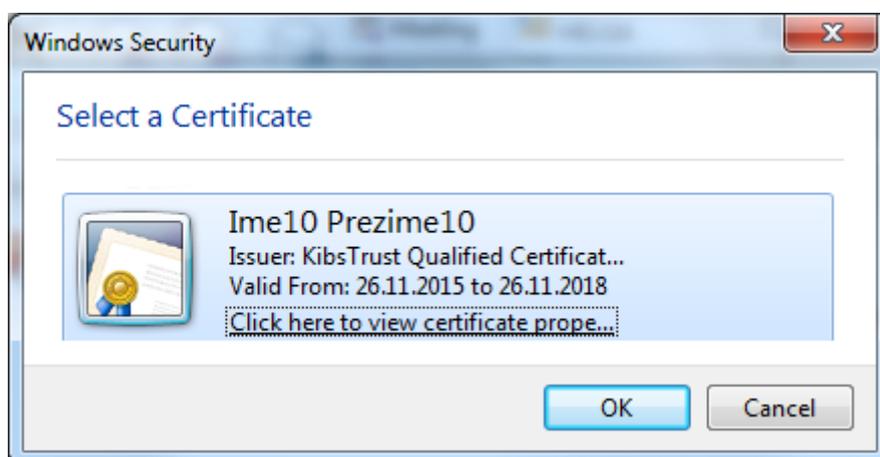

Figure 5

Repeat the procedure for a certificate for encrypting an electronic message.

You can view the certificate by clicking the **Click here to view certificate prope…** link. Then you will see a window which gives a detailed summary of the certificate, similar to the one shown on Figure 6:
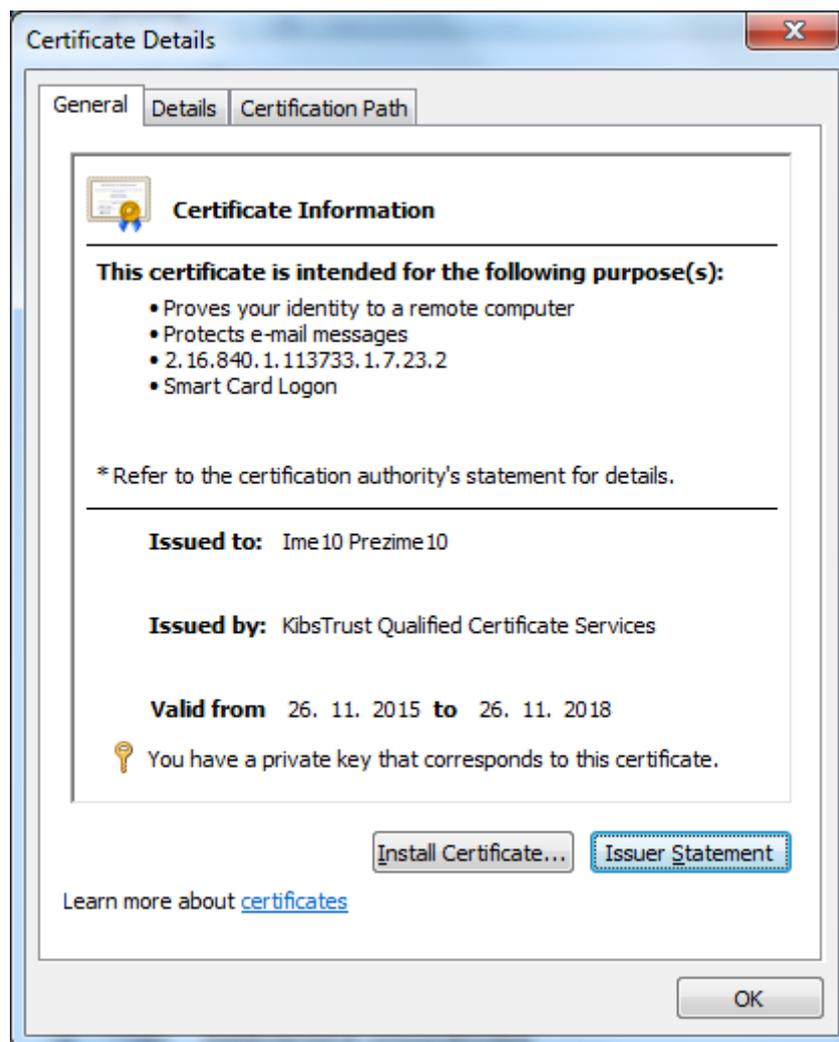
Figure 6

In Outlook the algorithm SHA-1 is used for creating your signature and the 3DES algorithm is used for encrypting your messages. For changing the predefined algorithms click on the drop-down menus.

3. Digital signing of messages in Microsoft Outlook

Your digital signature provides verification to the recipient that you truthfully have sent the message and that the message has not been changed while being transported.

The signing of the message does not affect the message's content and cannot be protected from interception and reading from a third party, for whom it is not intended. To be certain that only the intended recipient will read the message, you must encrypt it.

If you would like to digitally sign a new message, you must click on the Sign button, from the **Options** menu in the new message. By doing this, the message you will write and send will be digitally signed (Figure 7).

Figure 7

If the intended recipient of the message uses a S/MIME e-mail client, he will be able to read the message. In that case, your digital signature appears as an attachment, whose contents can be seen by the recipient by clicking on the ![signed icon] (signed) icon in the received signed message.

4. Message encryption in Microsoft Outlook

Electronic messages can be relatively easy intercepted or read by third parties, which are not intended recipients. This can be avoided with encrypting the message, which in turn enables only the intended recipient to read the message.

Encrypting in Outlook 2007 is simply done, as is the signing of the message and is done by clicking the ![Encrypt] button.

You must create a contact in your **Address Book,** for the person who you wish to send encrypted electronic messages. To encrypt the message, you need a copy of public key of the intended recipient's digital certificate. The public key of the intended recipient's digital certificate can be obtained from a signed e-mail message by him or can be downloaded from the online directory of the Certificate Authority KIBS.

When you receive an encrypted message, the ![lock icon] icon shows that the message is encrypted. This icon appears in the lower right corner of the address frame (Figure 8).

Figure 8

5. Correspondents' certificate management

In order to send an encrypted message, you need a copy of the public key of recipient's digital certificate in your address book. A of the public key of recipient's digital certificate can be obtained from signed message by him or or can be downloaded from the online directory of users from KIBS CA.

5.1 Saving a certificate from a signed message

When you receive a signed message, you can save the public key of the sender's digital certificate in your **Address Book**. Open the signed message and right-click on the name of the sender. A menu opens from which you need to choose **Add to Outlook Contacts** (Figure 9).
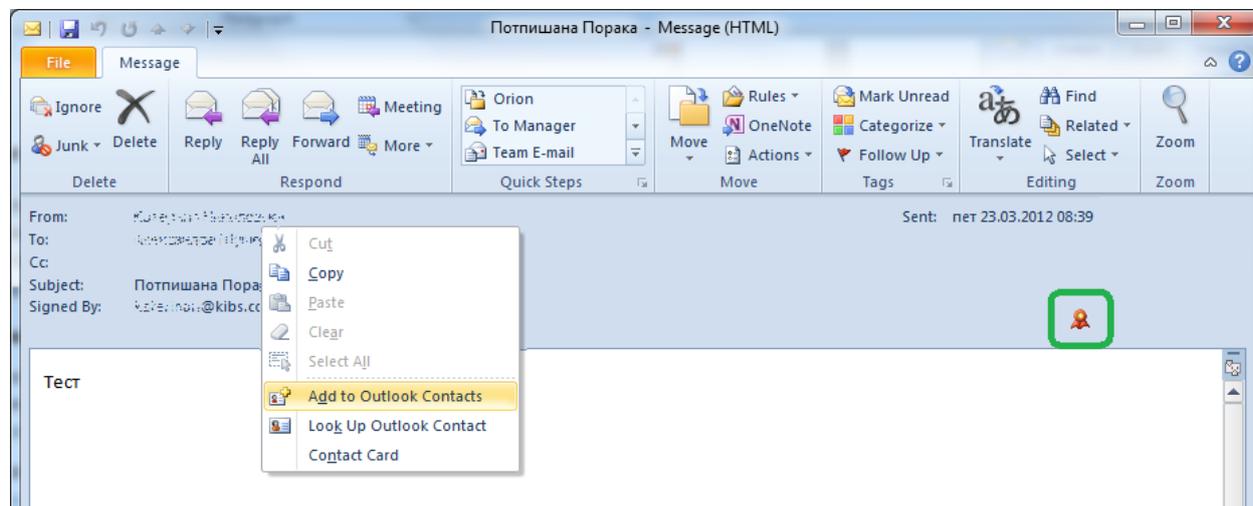

Figure 9

A window will open for creating a new contact. To check whether the certificate is coupled with the contact, click on the ![Certificates] button. The certificate should be displayed as shown on Figure 10:

Click on the **Save & Close** option to save the contact.

Figure 10

5.2 Inserting a downloaded digital certificate

The public key of recipient's digital certificate can be downloaded from the online directory of users from KIBS CA and added to your Address Book. The downloaded certificate is usually saved as a file with a **.cer** extension.

Create a new contact in Outlook or open an existing one from the address book. A new windows appears, as shown on Figure 11.
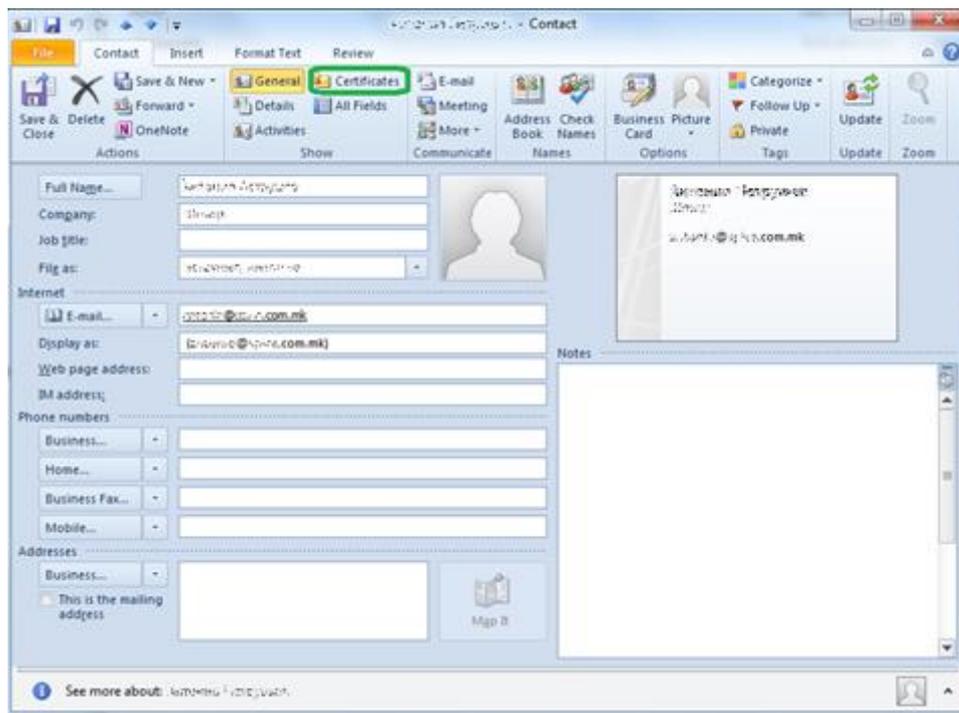

Figure 11

By clicking the **Certificates** button, a window opens for managing the certificates of the contact. Click on the **Import…** button (Figure 12). Choose the downloaded file with the digital certificate (*.cer) and click **Open**.
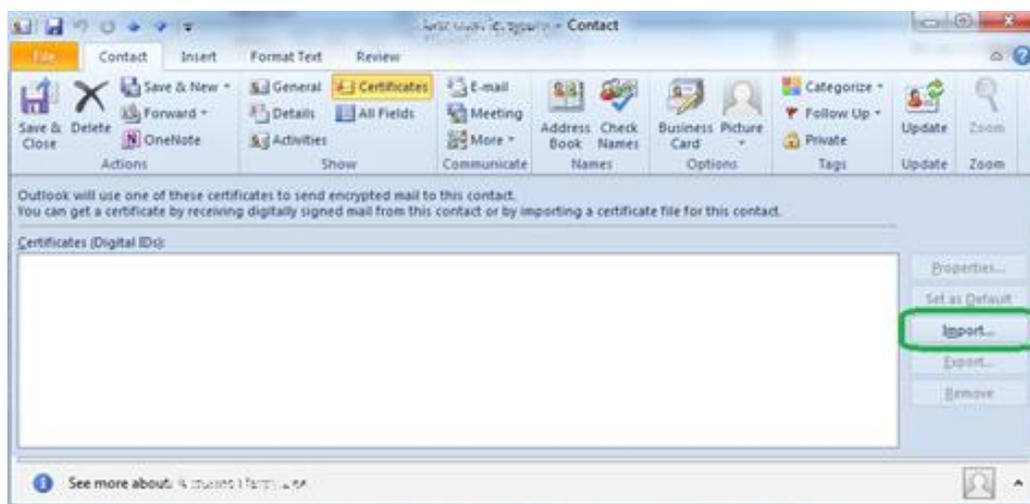

Figure 12

5.3   Removing a certificate from your Address Book

Open the entry in the address book for the person whose certificate you want to delete. Click on the Certificates button and a window will open for managing the certificates of the contact. From the list of certificates, select the certificate you wish to delete and click Remove (Figure 13Figure 13).

Once you delete someone's digital certificate, you will no longer be able to send encrypted messages to that person.

Figure 13

* * *