MANUAL

Downloading a certificate using Internet Explorer

Version: 4.0

Date: 09.01.2018

103.10

KIBS AD Skopje

http://www.kibstrust.mk

Table of Contents

1. Prerequisites for downloading a certificate

Before you start the procedure for downloading a certificate, you need to check the security settings of your web browser. To be certain that no problems will arise while downloading the certificate, it is recommended to add the webpage https://e-shop.kibstrust.mk in the list of Trusted Sites and to enable execution of ActiveX controls in that zone.

To make the recommended settings, follow the next steps:

1. From the browser menu click on the **Tools** button and select **Internet Options** (Figure 1):

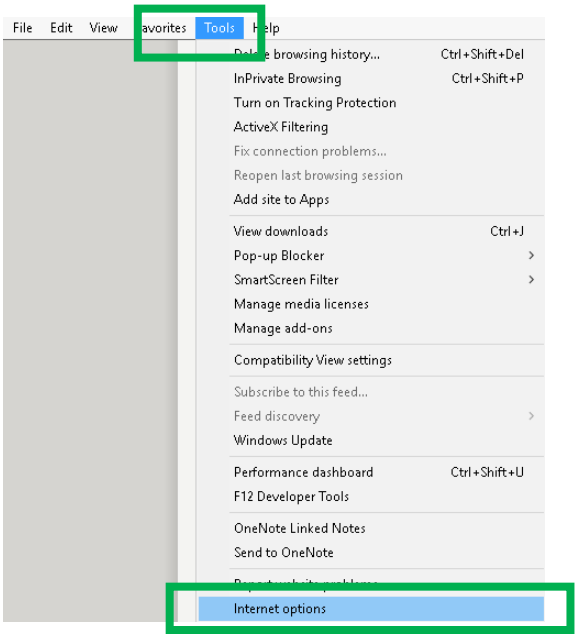

Figure 1

2. In the new window, select the **Security** tab. Click on **Trusted Sites** and then click on the **Sites** button (Figure 2):

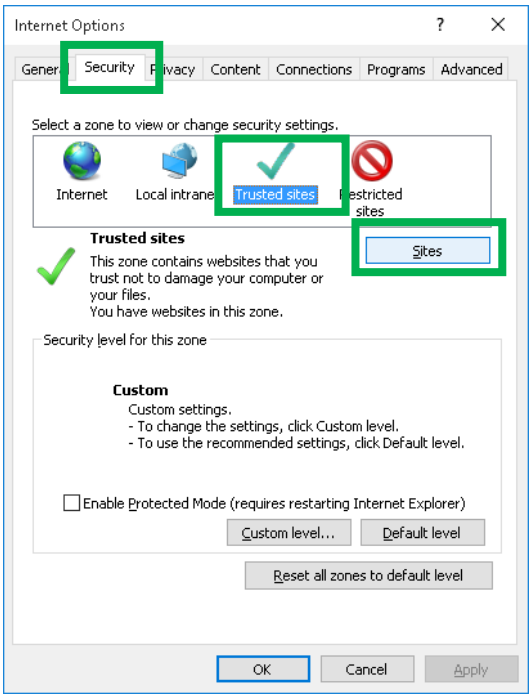

Figure 2

3. In the **Add this website to the zone** text field enter https://e-shop.kibstrust.mk and click on the **Add** button (Figure 3). By doing this, this webpage will appear in the **Websites** list as shown on Figure 4. Click Close.

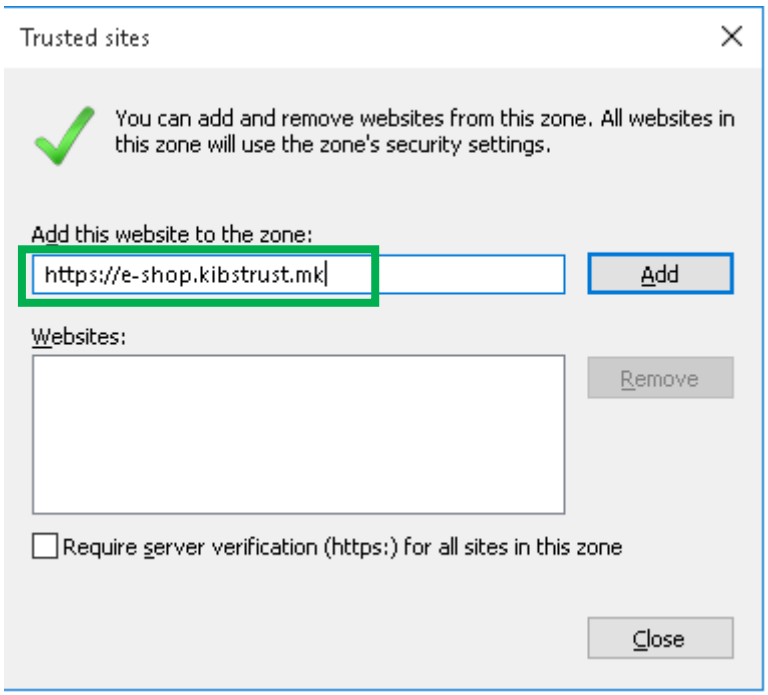

Figure 3

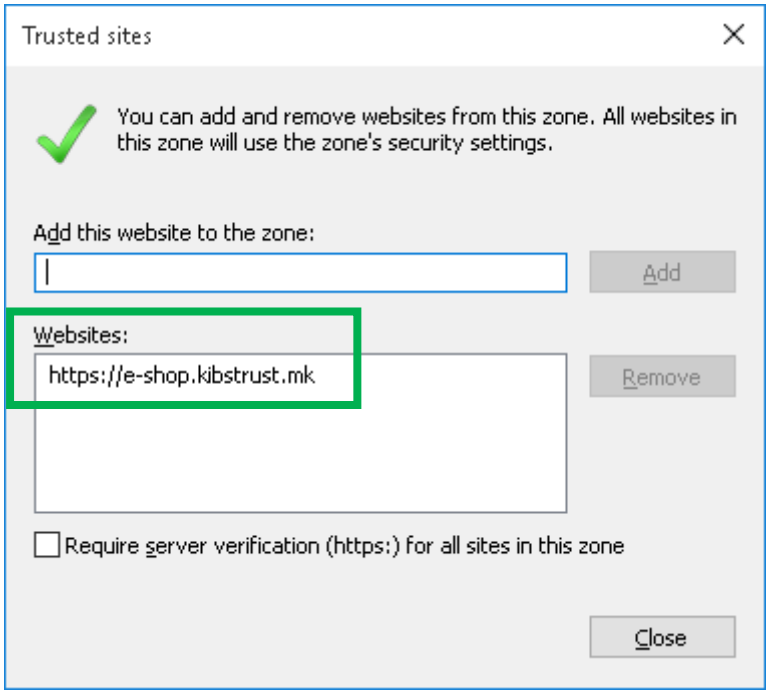

Figure 4

4. In the **Security** tab, choose **Trusted Sites** and click on the **Custom Level**… button (Figure 5):

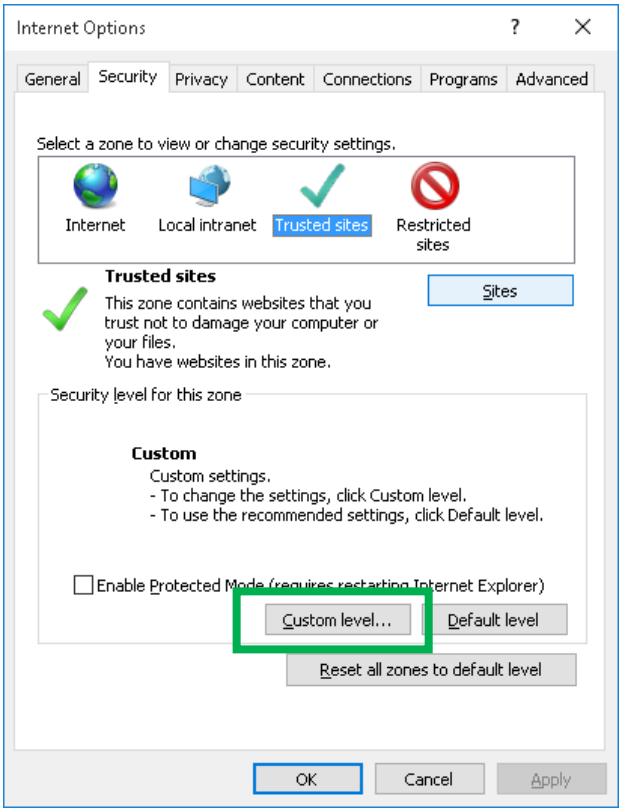

Figure 5

5. In **Reset Custom Settings**, from the **Reset to**: list choose **Medium**, as shown on Figure 6. This enables execution of ActiveX controls on the websites you trust. Click **OK** two times.

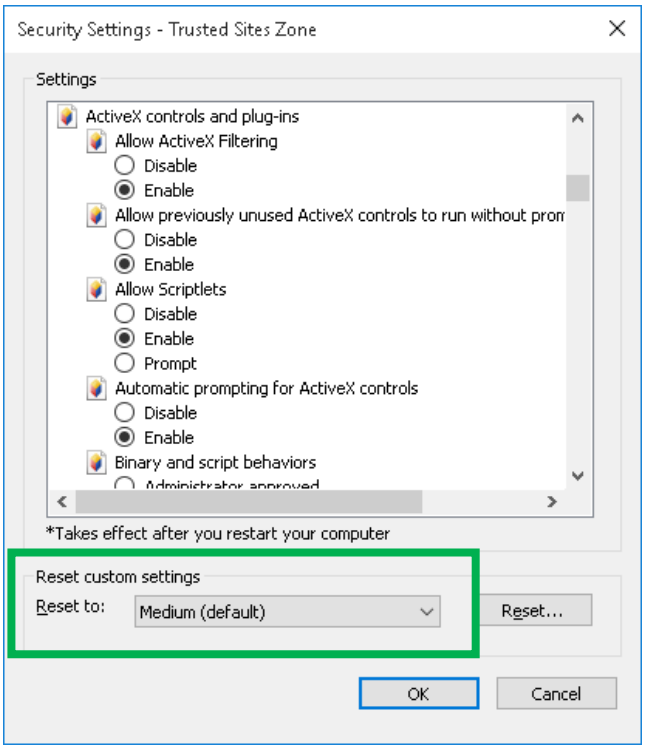

Figure 6

6. In Internet Explorer 11, it is necessary to add the domain kibstrust.mk in the Compatibility View. To do that, from the browser menu select Tools->Compatibility View settings (Figure 7):

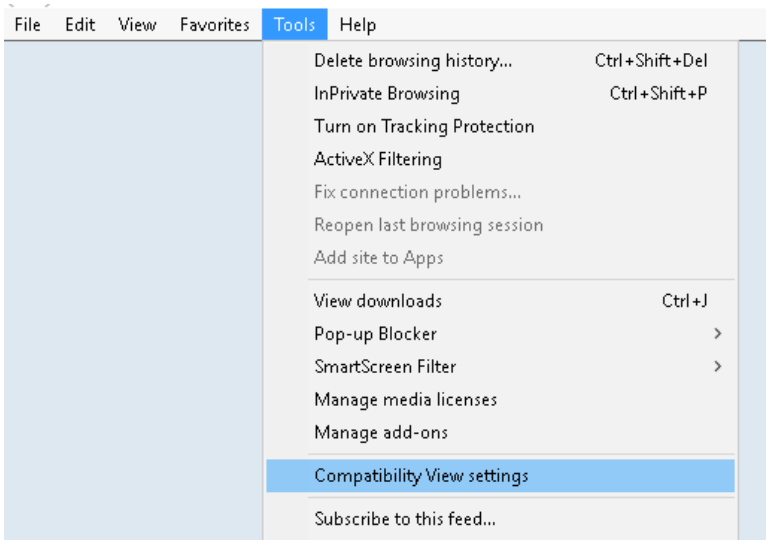

Figure 7

In the new window check whether “kibstrust.mk” is entered in the Add this website field and then click Add (Figure 8):

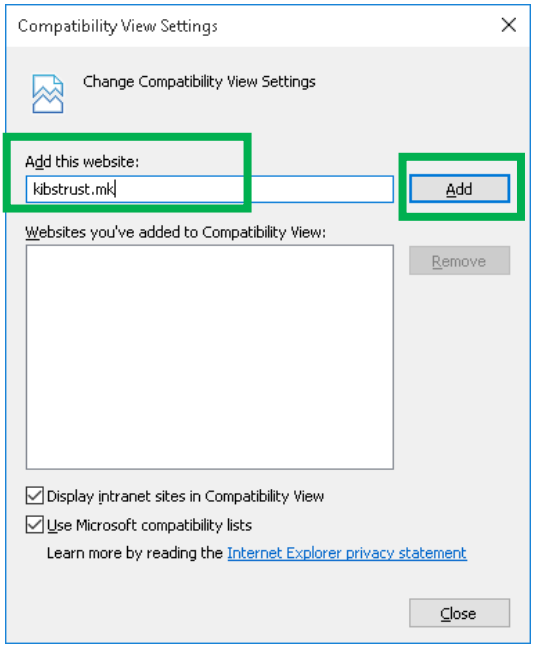

Figure 8

To finish the procedure click Close (Figure 9):

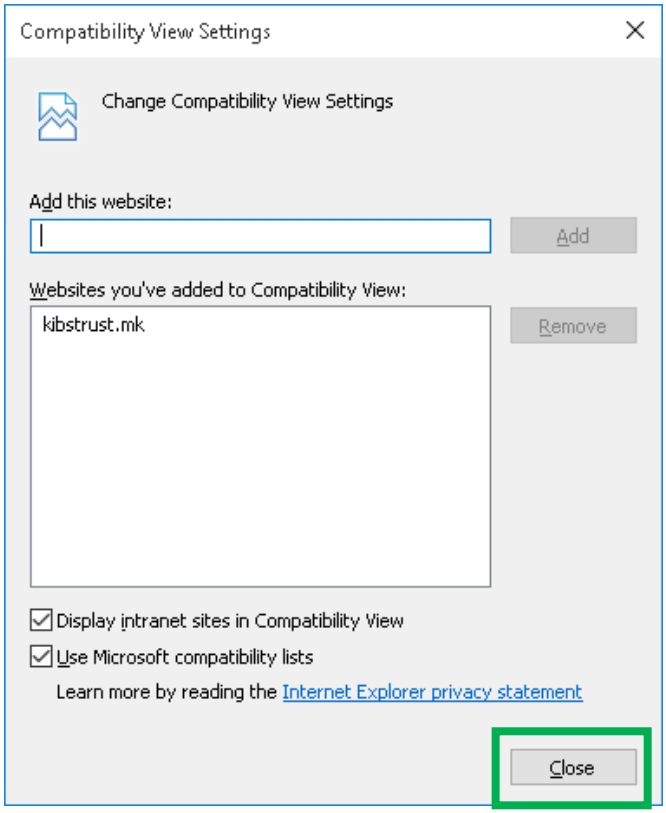

Figure 9

In order for the changes to take place, please close the web browser and then open it again. Now you are ready to download your certificate.

2. How to download the certificate?

From the certificates that KIBS CA offers, the certificates Verba Sign K1, Verba Sign Pro1 and Verba Seal S1 are generated on the disk of your PC.

To download one of the previous mentioned certificates, by using Internet Explorer, follow the next steps:

1. Follow the link which is listed in the e-mail message that you received with a notification that your purchase order for a certificate is approved (https://e-shop.kibstrust.mk/raweb/verbaen.aspx). If you use Internet Explorer 11 continue with step 2, otherwise go to step 3.

   On the web page (Figure 10) enter:

   - Order: enter the number of the order which was sent in the same e-mail message
   - E-mail: enter the e-mail address which was entered in the request for certificate form

   Click **Submit**.

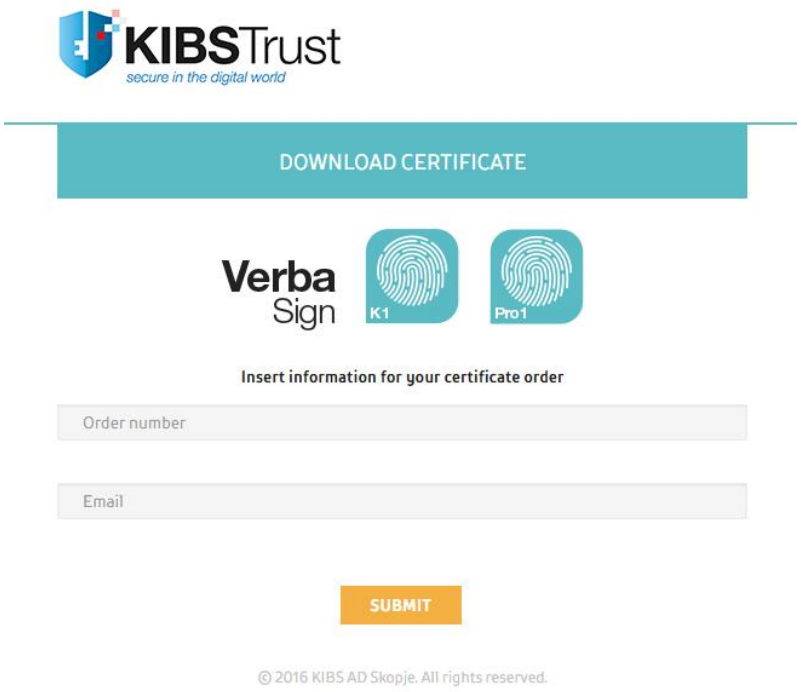

Figure 10

2. A new webpage will open to confirm the registration data (Figure 11). Check the data, enter an **Authentication phrase** and click **Submit.**
3. After clicking on **Submit**, a message will appear, as shown on Figure 12. Once again, check the e-mail address and click **OK** if everything is in order.

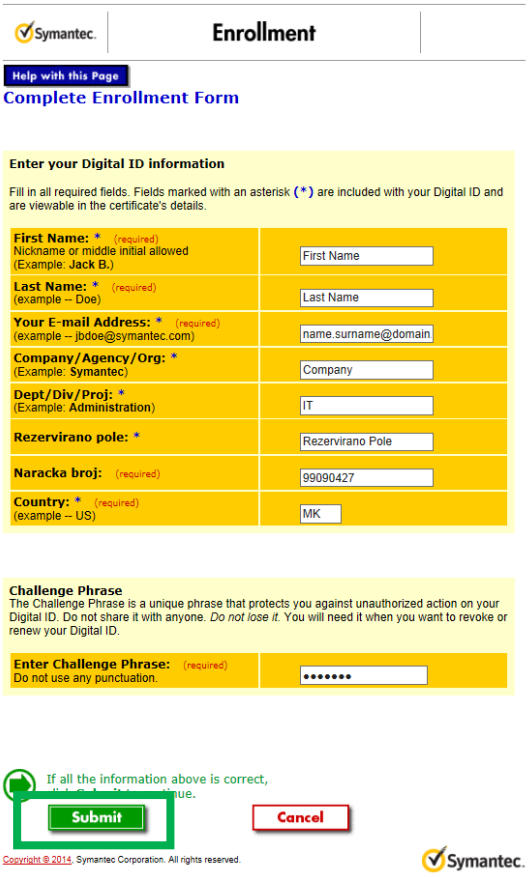

Figure 11

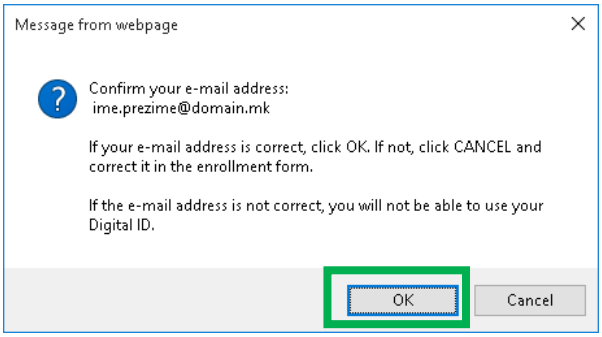

Figure 12

4. A windows appears, as shown on Figure 13, which asks for a confirmation that you allow the execution of the operation regarding the digital certificates. This window appears two times and both times you need to click **Yes**.

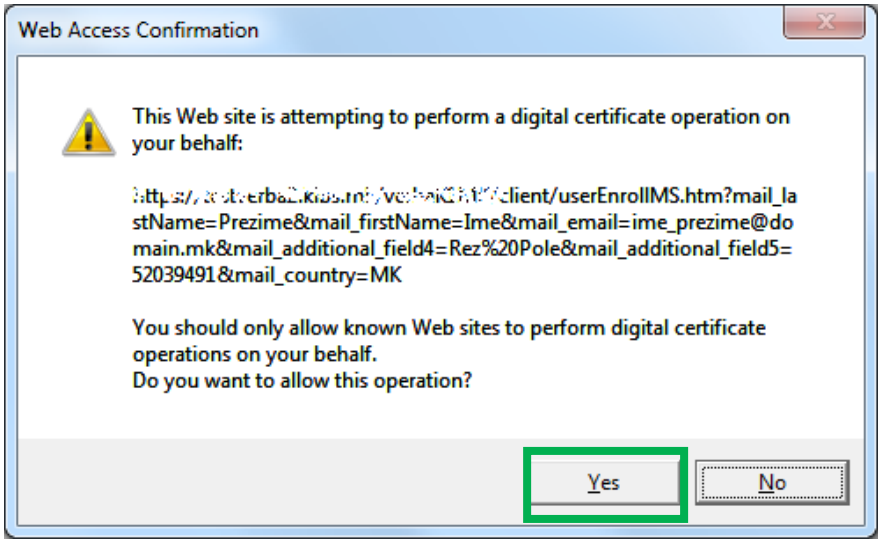

Figure 13

5. The certificate generation process start. **Please wait while the process executes** (Figure 14).

Figure 14

6. On the windows with messages on Figure 15 click **Yes**.

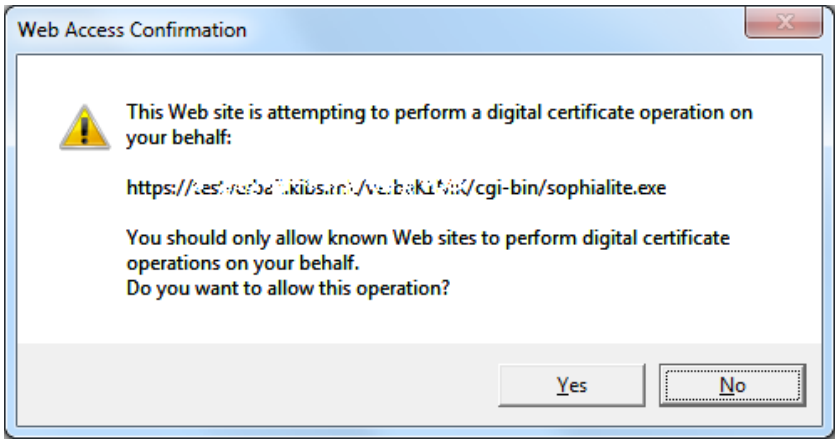

Figure 15

7. Congratulations, your certificate has been successfully generated and installed (Figure 16)!

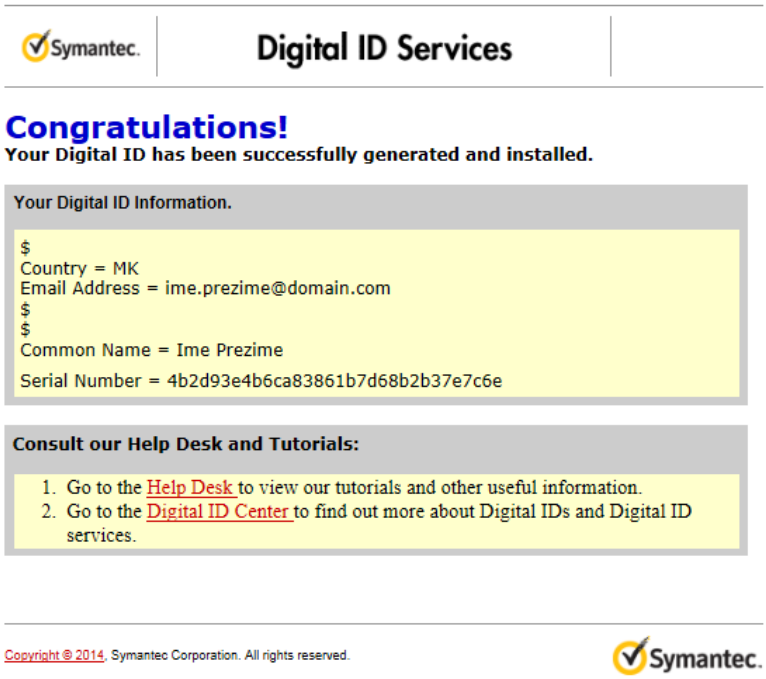
Symantec.
Digital ID Services
Congratulations!
Your Digital ID has been successfully generated and installed.
Your Digital ID Information.
$
Country = MK
Email Address = ime.prezime@domain.com
$
$
Common Name = Ime Prezime
Serial Number = 4b2d93e4b6ca83861b7d68b2b37e7c6e
Consult our Help Desk and Tutorials:
1. Go to the Help Desk to view our tutorials and other useful information.
2. Go to the Digital ID Center to find out more about Digital IDs and Digital ID services.
Copyright © 2014, Symantec Corporation. All rights reserved.
Symantec.

Figure 16

3. How to check whether the certificate is successfully installed?

After receiving a message that your certificate is successfully installed, it is necessary to check whether it is added in the list of personal certificates in the web browser. To make this check, please follow the next steps:

1. From the browser menu click on the **Tools** button and select **Internet Options** (Figure 17):

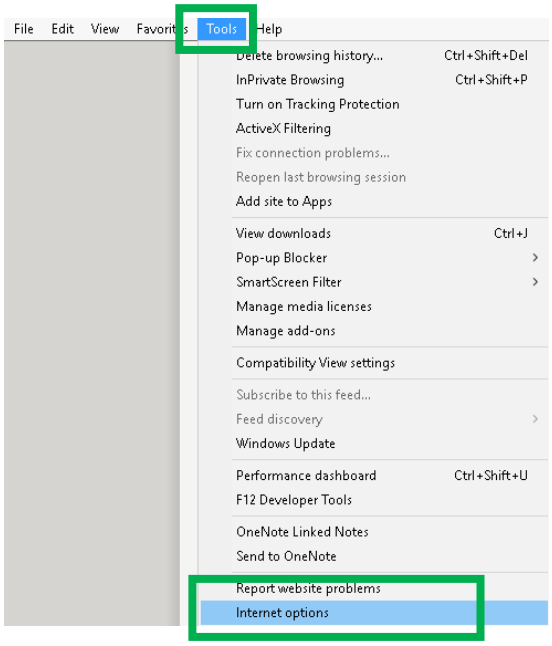

Figure 17

2. In the new window select the **Content** tab. In the **Certificates** frame, click on the **Certificates** button (Figure 18):

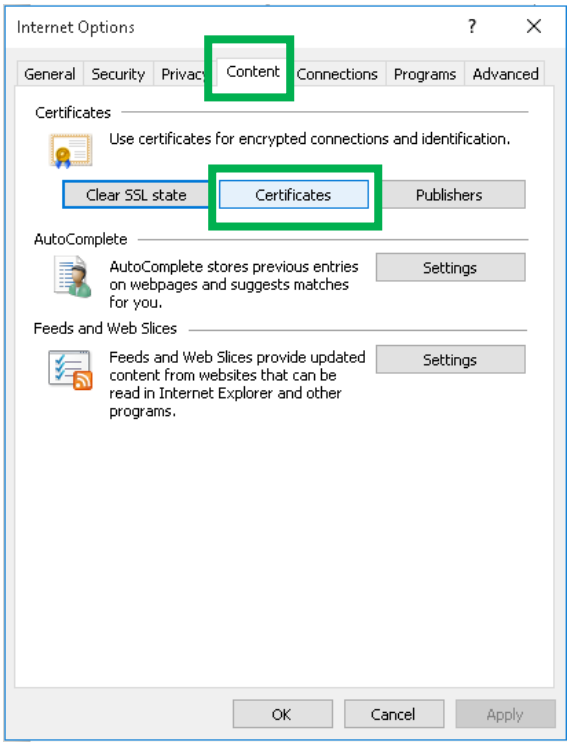

Figure 18

3. If your certificate is successfully installed, it will be in the certificate list in the **Personal** tab (Figure 19):

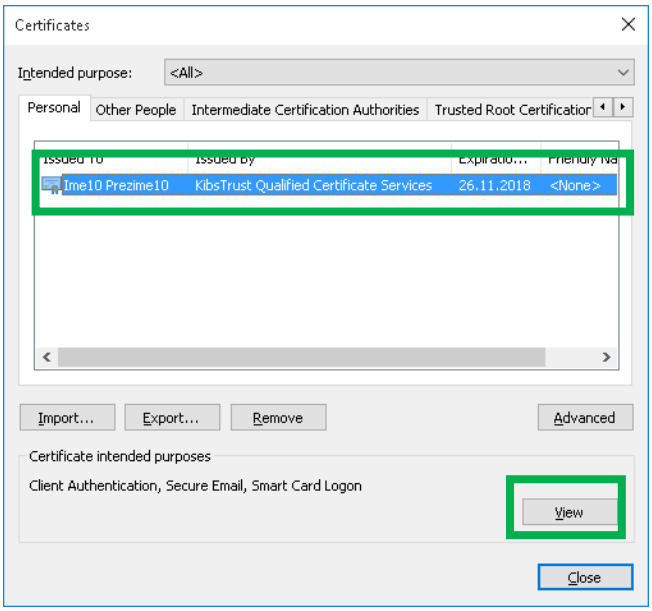

Figure 19

Click **View** and a new window will open which shows a detailed review of information regarding the certificate. In the **General** tab (Figure 20), the common information regarding the certificate are given:

Issued to: The name of the person to which the certificate is issued

Issued by: The name of the Certificate Authority (KibsTrust Qualified Certificate Services)

Valid from: Issue date **to:** Expiration date

At the bottom there is information that you own the private key which corresponds to the certificate: „**You have a private key that corresponds to this certificate.** “

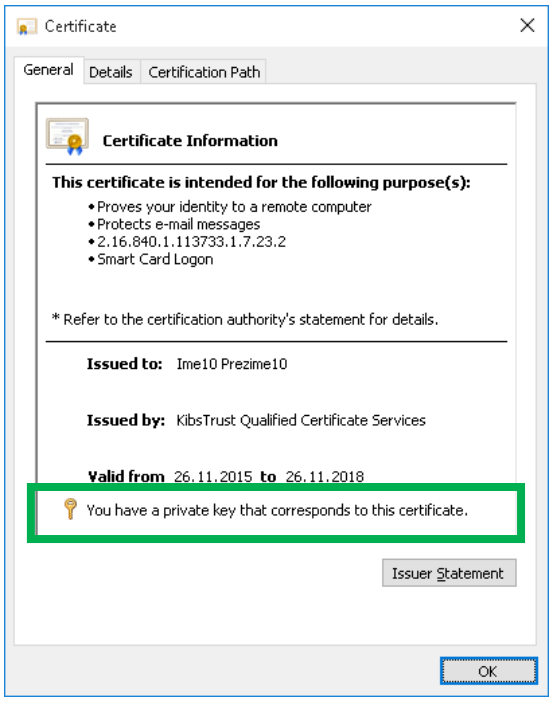

Figure 20

The root certificates, with which your certificate is signed, are shown in the **Certification Path** tab (Figure 21). Check whether the three root certificates are shown: **VeriSign Class 2 Public Primary Certification Authority – G3, KibsTrust Certification Authority and KibsTrust Qualified Certificate Services**. In the bottom of the **Certification Path** tab is the information about the status of the certificate. If your certificate is OK, then this message will be shown: „This certificate is OK. “

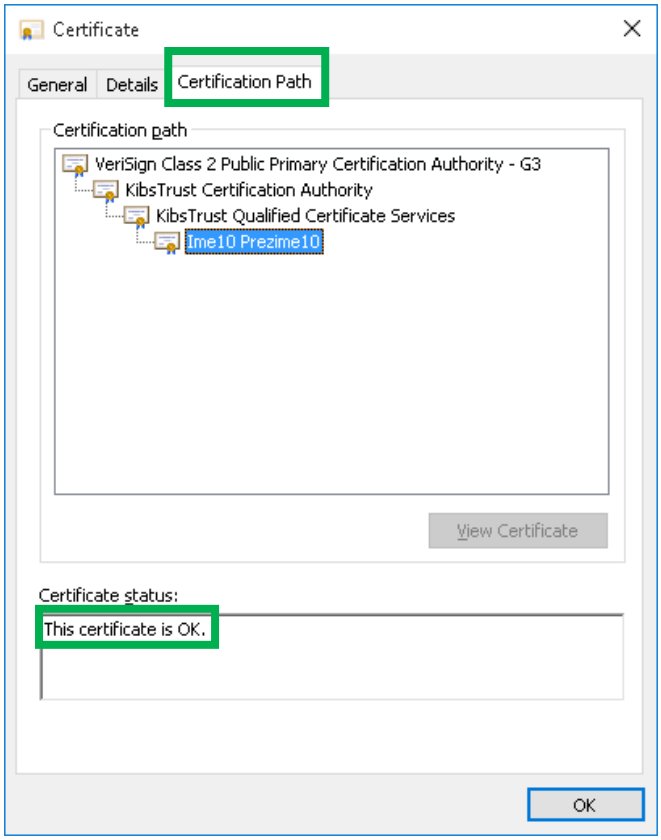

Figure 21

4. How to back up the certificate?

Your certificate is installed on the disk of your PC and can be erased by a bug in operating system or hardware failure. To protect your certificate in these kind of situations, **it is necessary to make a backup of the certificate i.e. export it in a .PFX file.**

To make a backup of your certificate you need to follow these steps:

1. From the browser menu click on the **Tools** button and select **Internet Options** (Figure 22):

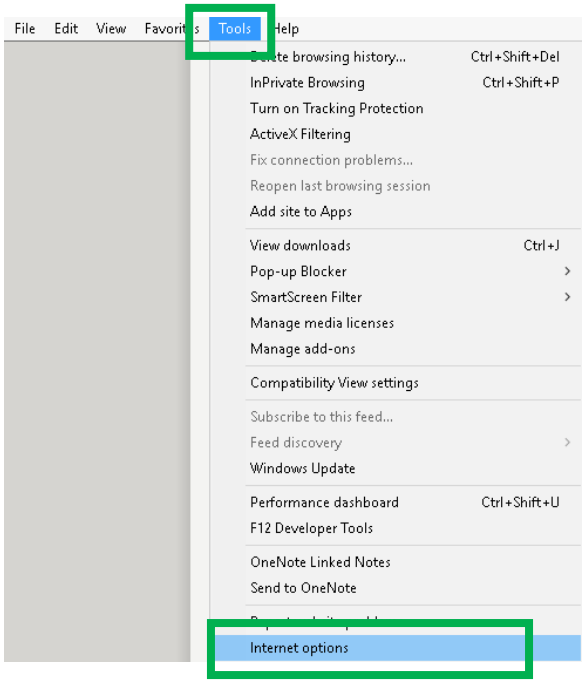

Figure 22

2. In the new window select the **Content** tab. In the **Certificates** frame, click on the **Certificates** button (Figure 23):

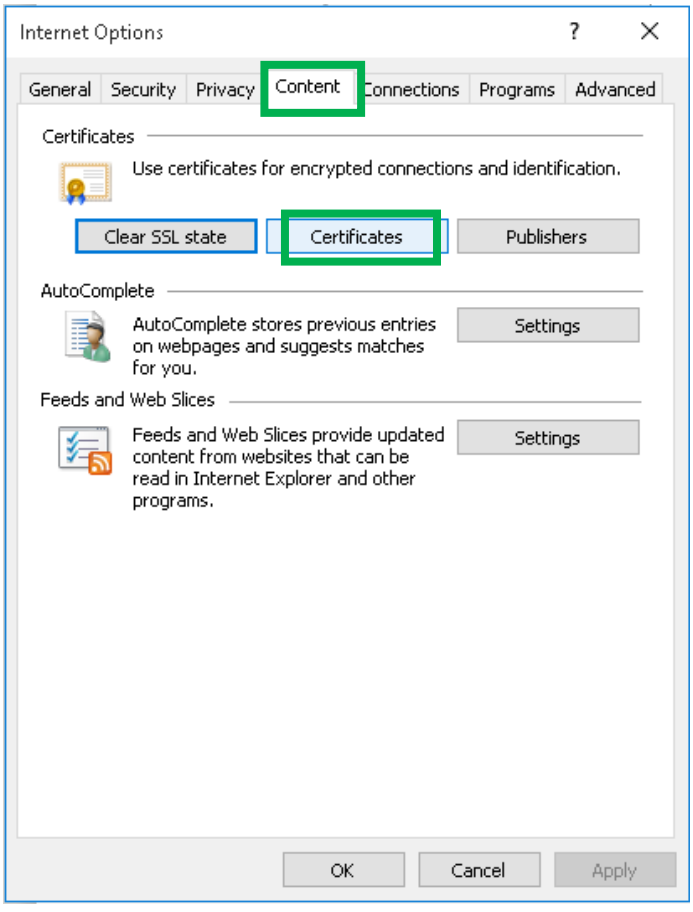

Figure 23

3. In the **Personal** tab, choose your certificate and click on the **Export** button (Figure 24):

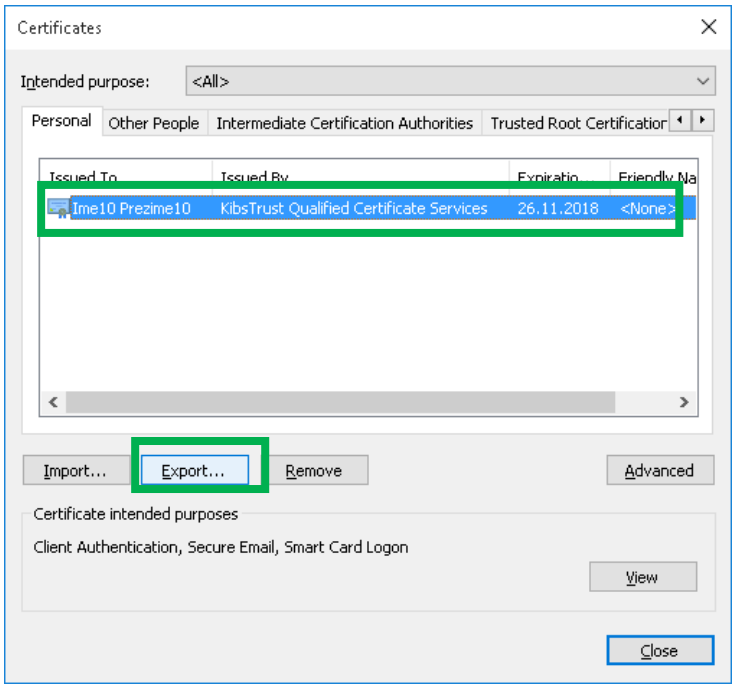

Figure 24

4. By clicking the **Export** button, a wizard opens which will guide you through the procedure of exporting a certificate (Figure 25). To continue click **Next**:

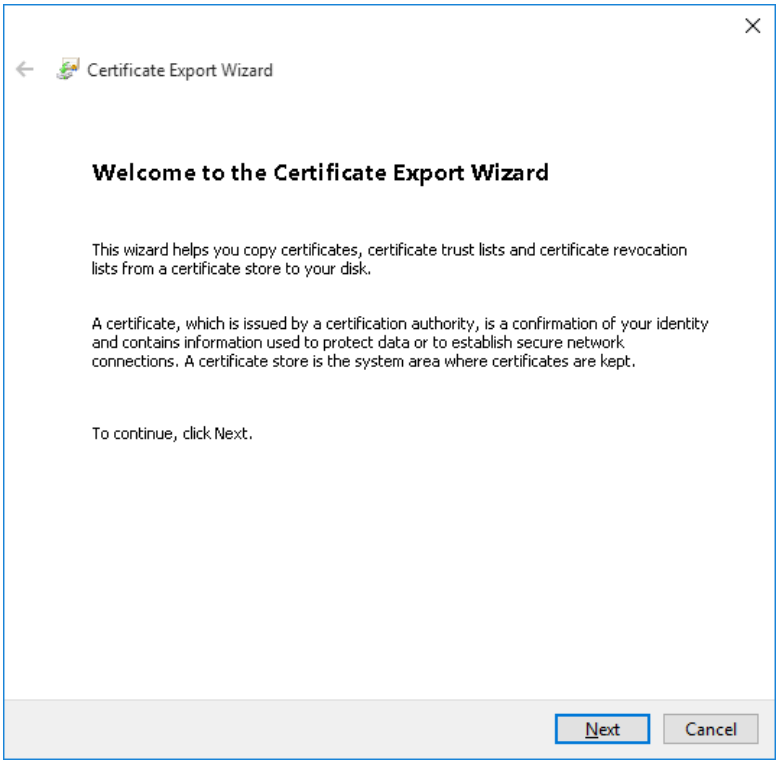

Figure 25

5. Choose the „**Yes, export the private key**“ option (Figure 26). To continue click **Next**:

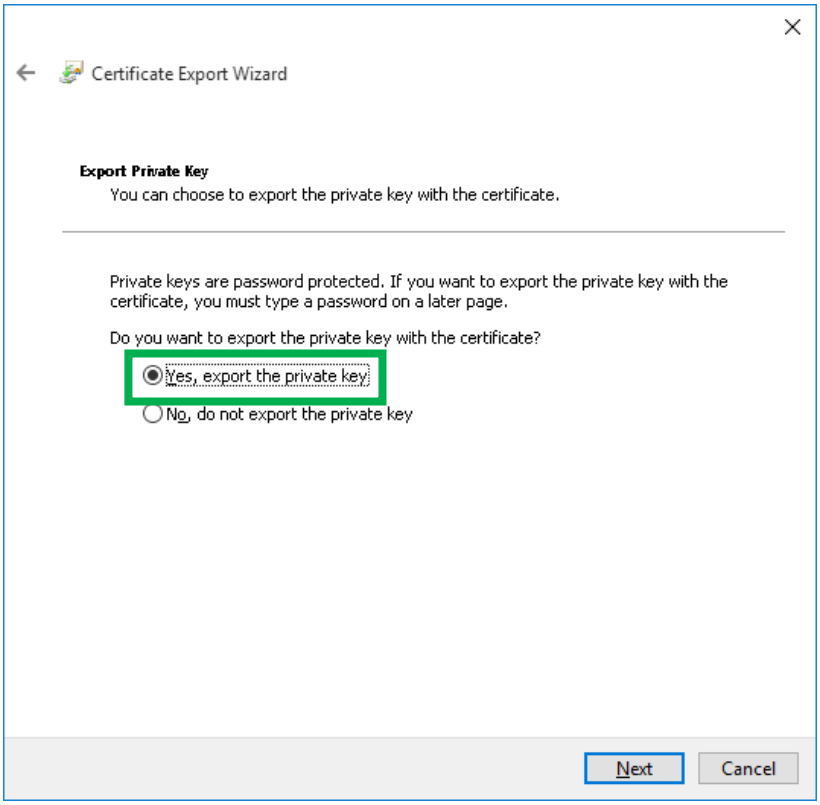

Figure 26

6. Choose a .PFX file format in which you the certificate will export and choose to export the root certificates (Figure 27). To continue click **Next**:

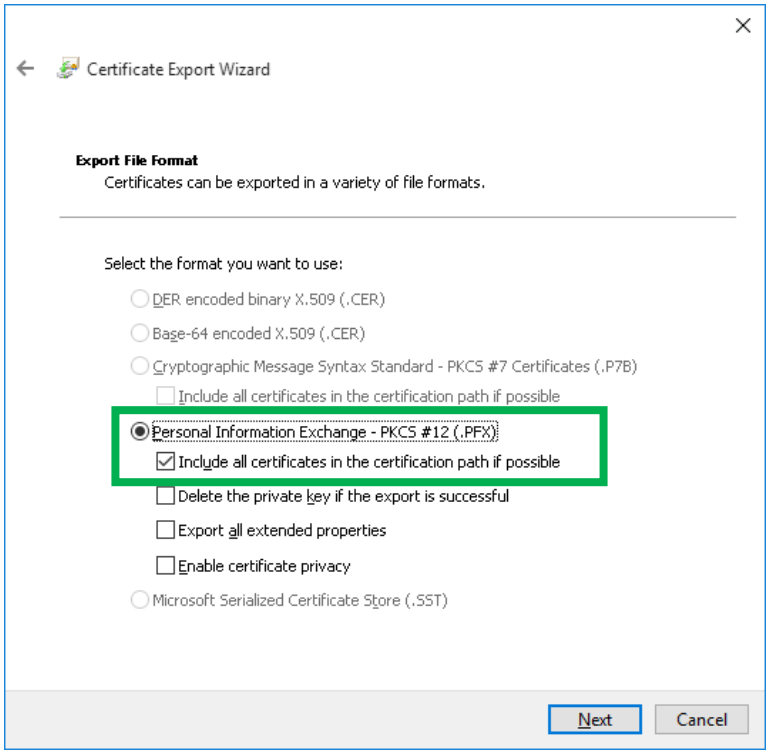

Figure 27

7. Enter a password to protect the private key (Figure 28). **You are the only one that knows the password, please remember it or keep it written down in a safe place!** Click **Next** to continue:

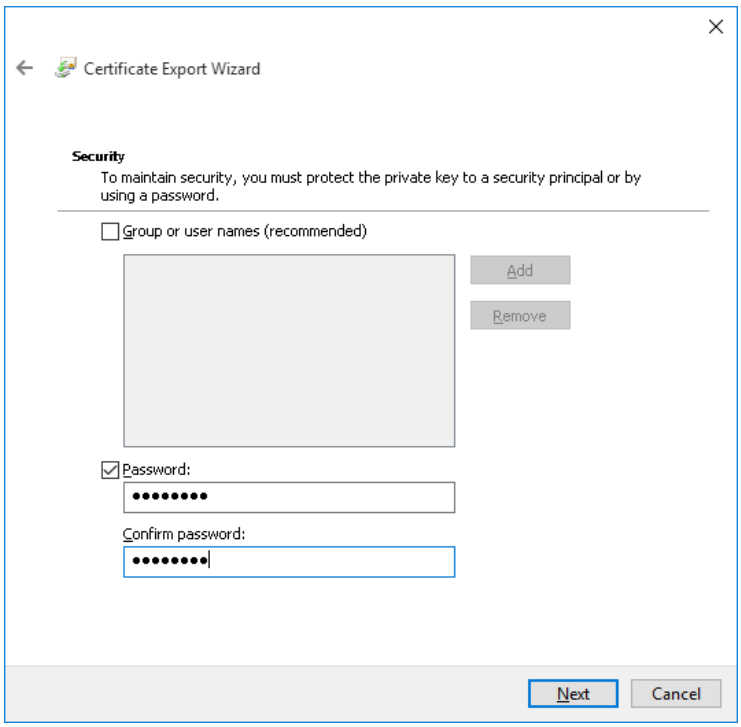

Figure 28

8. Enter a file name and location to which you will export the certificate (Figure 29). Click **Next** to continue:

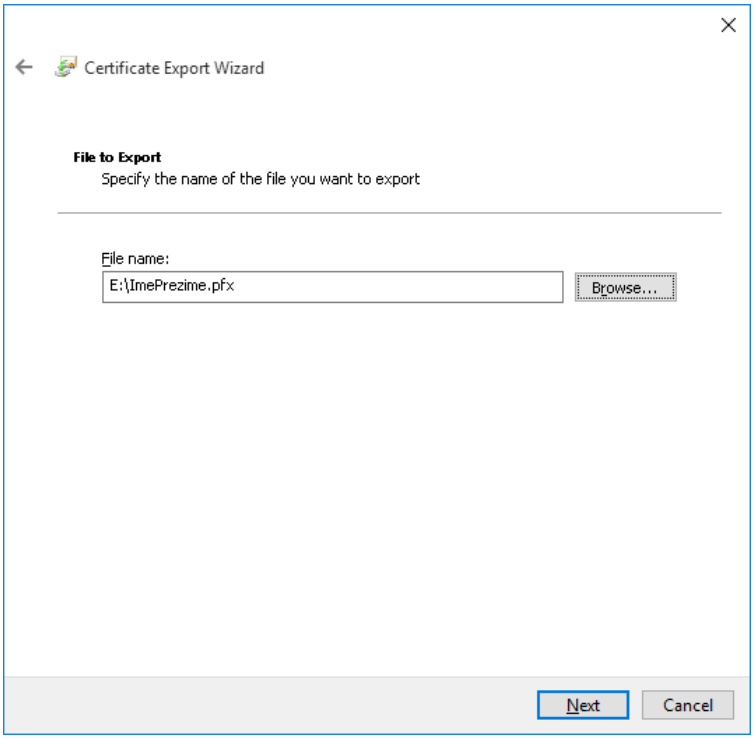

Figure 29

9. In the next window (Figure 30) you get a short preview of the settings you made. Click on the **Finish** button to finish the procedure of exporting a certificate:

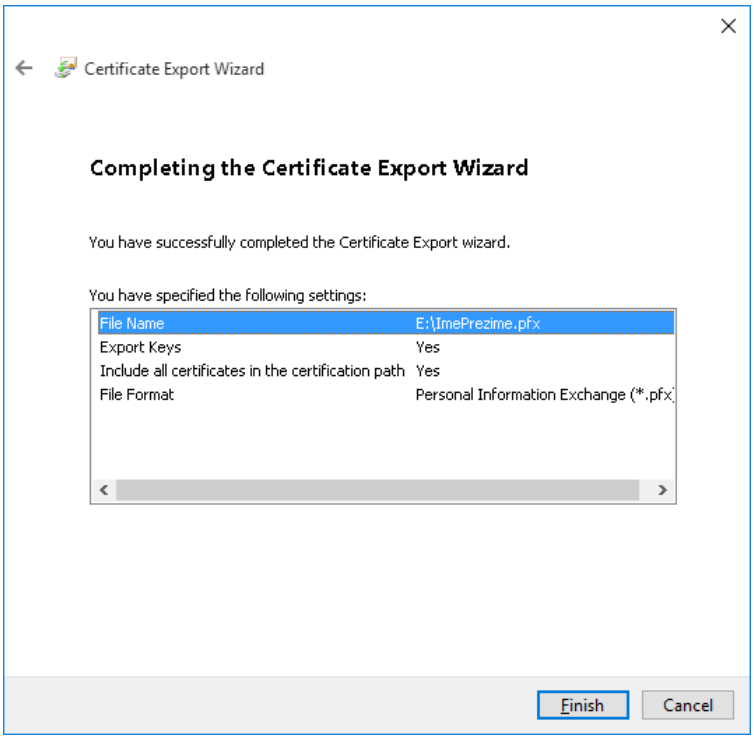

Figure 30

10. You will receive a message that you successfully exported your certificate (Figure 31):

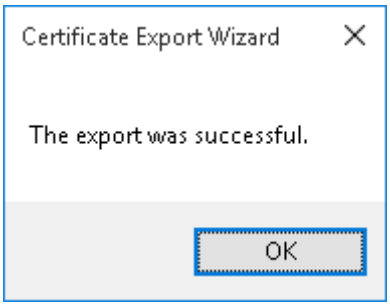

Figure 31

IMPORTANT: Store the .PFX file to which your certificate is exported and the password for it on a safe external media (external hard drive, USB flash, CD/DVD…)!

* * *