MANUAL

Downloading a certificate using Mozilla Firefox ESR

Version: 5.1

Date: 31.01.2022

103.11

KIBS AD Skopje

http://www.kibstrust.com/

Table of Contents

1. How to download the certificate?

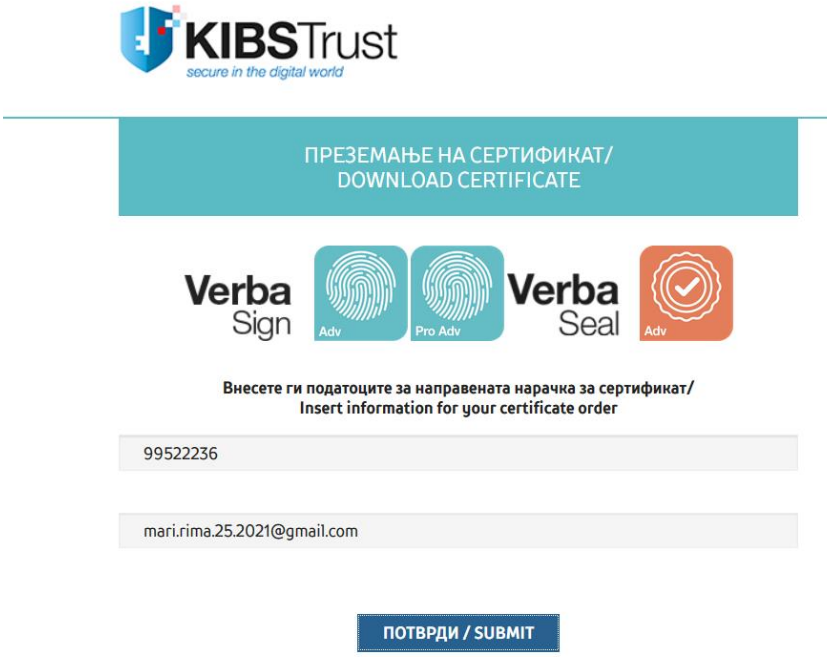
From the personal certificates that KIBS CA offers, the certificates Verba Adv, Verba Pro Adv and Verba Seal Adv are generated on the disk of your PC.

To download one of the previous mentioned certificates, please use Mozilla Firefox ESR web browser, version not higher than 68.3, which you can download from the following link: https://ftp.mozilla.org/pub/firefox/releases/68.3.0esr/ where you can choose win64/ or win32/ for 64 or 32-bit Firefox version.

Then, follow the next steps:

1. First open the web browser Mozilla Firefox ESR carefully, such as do not let the browser get upgraded automatically and open the link https://e-shop.kibstrust.com/raweb in it.
2. On the webpage (Figure 1) enter:
    - Order number: enter the number of the order which was sent to you in the same e-mail message
    - E-mail: enter the e-mail address which was entered in the request for certificate form

Click **Submit**.



ПРЕЗЕМАЊЕ НА СЕРТИФИКАТ/
DOWNLOAD CERTIFICATE

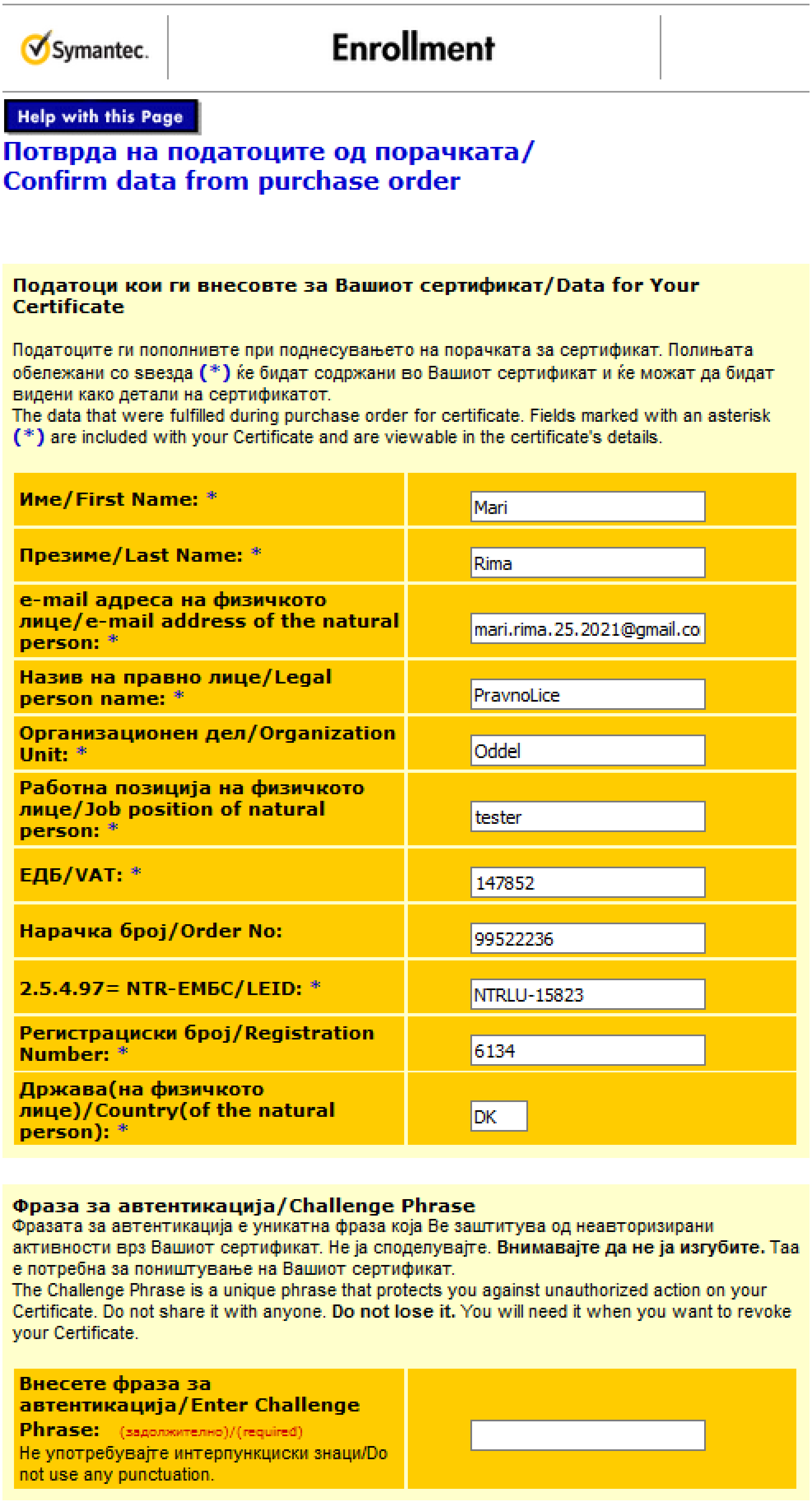
Внесете ги податоците за направената нарачка за сертификат/
Insert information for your certificate order

99522236

mari.rima.25.2021@gmail.com

Figure 1

3. A new webpage will open to confirm the registration data (on Figure 2 is shown example of Verba Sign Pro Adv certificate). Check the data, enter a **Challenge phrase** (without any punctuation). Choose **High Grade** Encryption Strength and click **Submit.**



Потврда на податоците од порачката/
Confirm data from purchase order

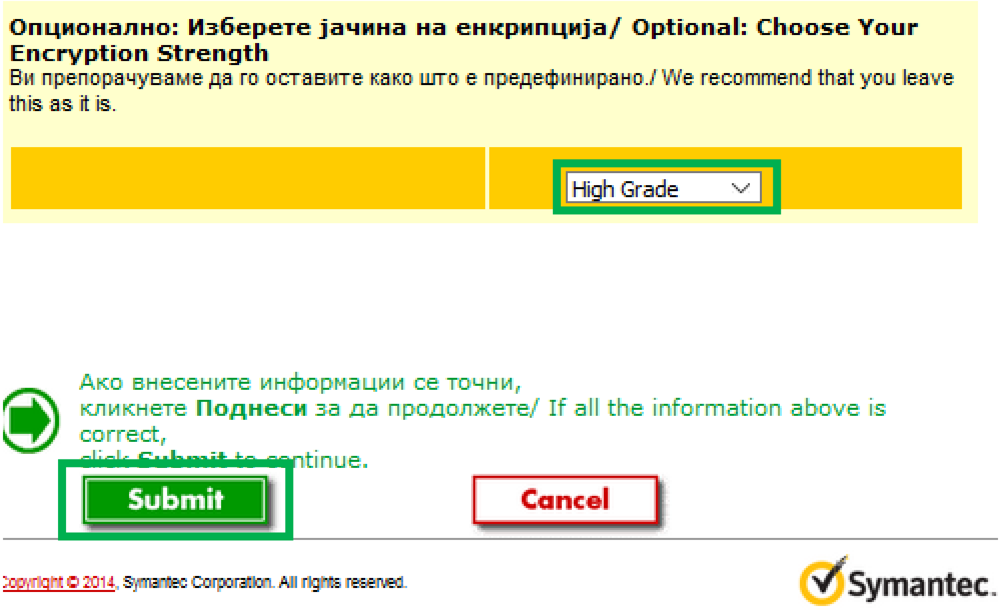
Податоци кои ги внесовте за Вашиот сертификат/Data for Your Certificate

Податоците ги пополнивте при поднесувањето на порачката за сертификат. Полињата обележани со звезда (*) ќе бидат содржани во Вашиот сертификат и ќе можат да бидат видени како детали на сертификатот.
The data that were fulfilled during purchase order for certificate. Fields marked with an asterisk (*) are included with your Certificate and are viewable in the certificate's details.

Име/First Name: *	Mari
Презиме/Last Name: *	Rima
e-mail адреса на физичкото лице/e-mail address of the natural person: *	mari.rima.25.2021@gmail.co
Назив на правно лице/Legal person name: *	PravnoLice
Организационен дел/Organization Unit: *	Oddel
Работна позиција на физичкото лице/Job position of natural person: *	tester
ЕДБ/VAT: *	147852
Нарачка број/Order No:	99522236
2.5.4.97= NTR-ЕМБС/LEID: *	NTRLU-15823
Регистрациски број/Registration Number: *	6134
Држава(на физичкото лице)/Country(of the natural person): *	DK

Фраза за автентикација/Challenge Phrase
Фразата за автентикација е уникатна фраза која Ве заштитува од неавторизирани активности врз Вашиот сертификат. Не ја споделувајте. **Внимавајте да не ја изгубите.** Таа е потребна за поништување на Вашиот сертификат.
The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Certificate. Do not share it with anyone. **Do not lose it.** You will need it when you want to revoke your Certificate.

Внесете фраза за автентикација/Enter Challenge Phrase: (задолжително)/(required) Не употребувајте интерпункциски знаци/Do not use any punctuation.	



Опционално: Изберете јачина на енкрипција/ Optional: Choose Your Encryption Strength

Ви препорачуваме да го оставите како што е предефинирано./ We recommend that you leave this as it is.

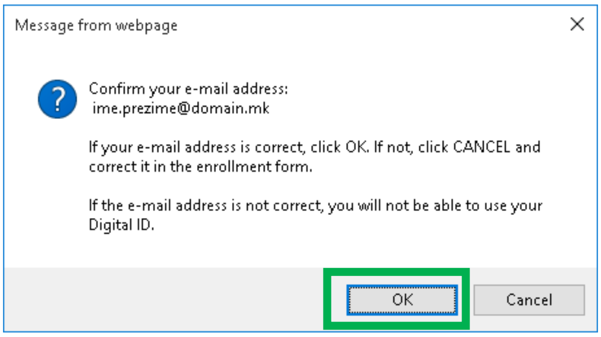
High Grade

Ако внесените информации се точни, кликнете **Поднеси** за да продолжете/ If all the information above is correct, click **Submit** to continue.

Copyright © 2014, Symantec Corporation. All rights reserved.

Figure 2

4. After clicking on **Submit**, a message will appear, as shown on Figure 3. Once again, check the e-mail address and click **OK** if everything is in order.



Message from webpage

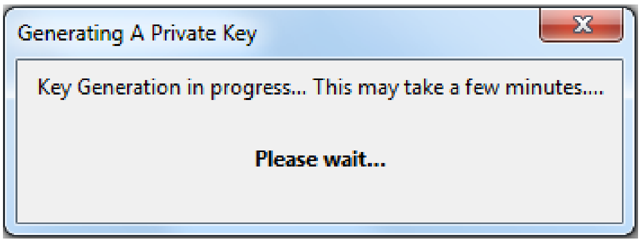
Confirm your e-mail address:
ime.prezime@domain.mk

If your e-mail address is correct, click OK. If not, click CANCEL and correct it in the enrollment form.

If the e-mail address is not correct, you will not be able to use your Digital ID.

Figure 3

5. After choosing **OK**, a window will appear, as shown on Figure 4, which will inform you that the key pair generation for your certificate is in progress. **Please wait**.



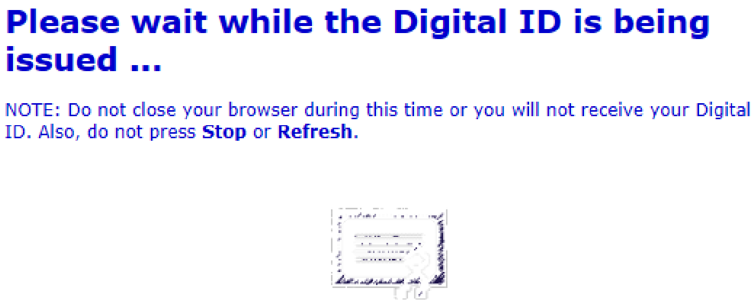
Generating A Private Key

Key Generation in progress... This may take a few minutes....

Please wait...

Figure 4

6. After this, the process for generating your certificate starts. Please wait while this process is in progress (Figure 5).

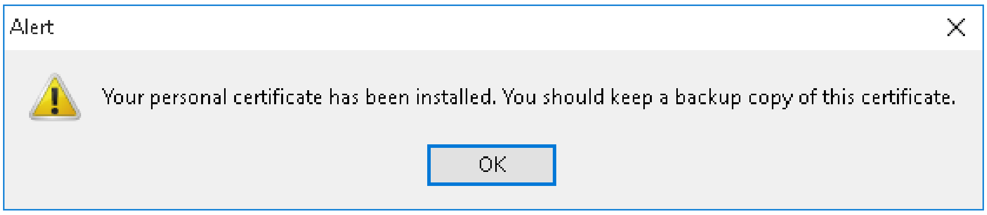


Please wait while the Digital ID is being issued ...

NOTE: Do not close your browser during this time or you will not receive your Digital ID. Also, do not press **Stop** or **Refresh**.

Figure 5

7. A message will appear that your certificate has been installed (Figure 6). Click **OK**.

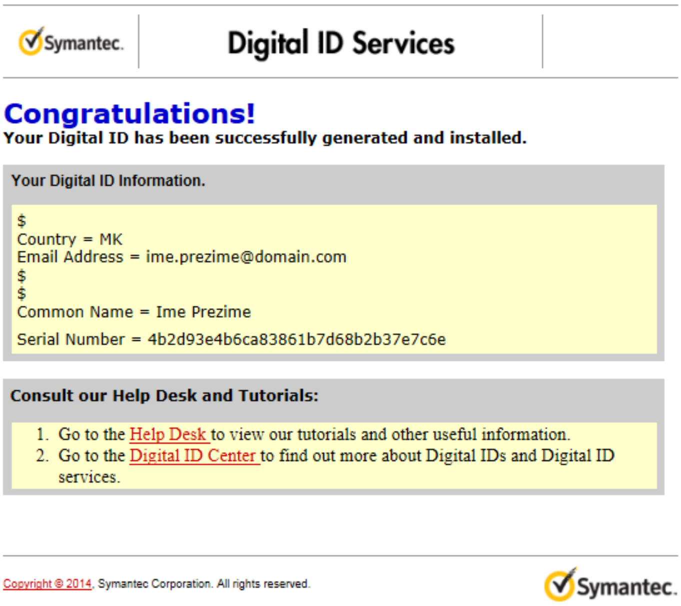


Alert

Your personal certificate has been installed. You should keep a backup copy of this certificate.

Figure 6

8. On wen site, you can see: Congratulations, your certificate has been successfully generated and installed (Figure 7)!



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.

Figure 7

2. 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 right upper button and select **Options** (Figure 8):

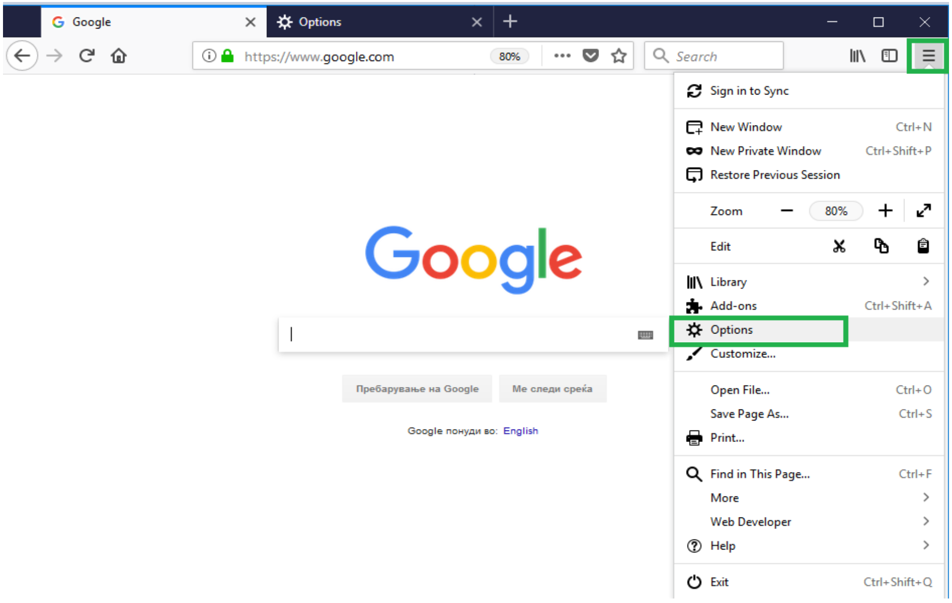
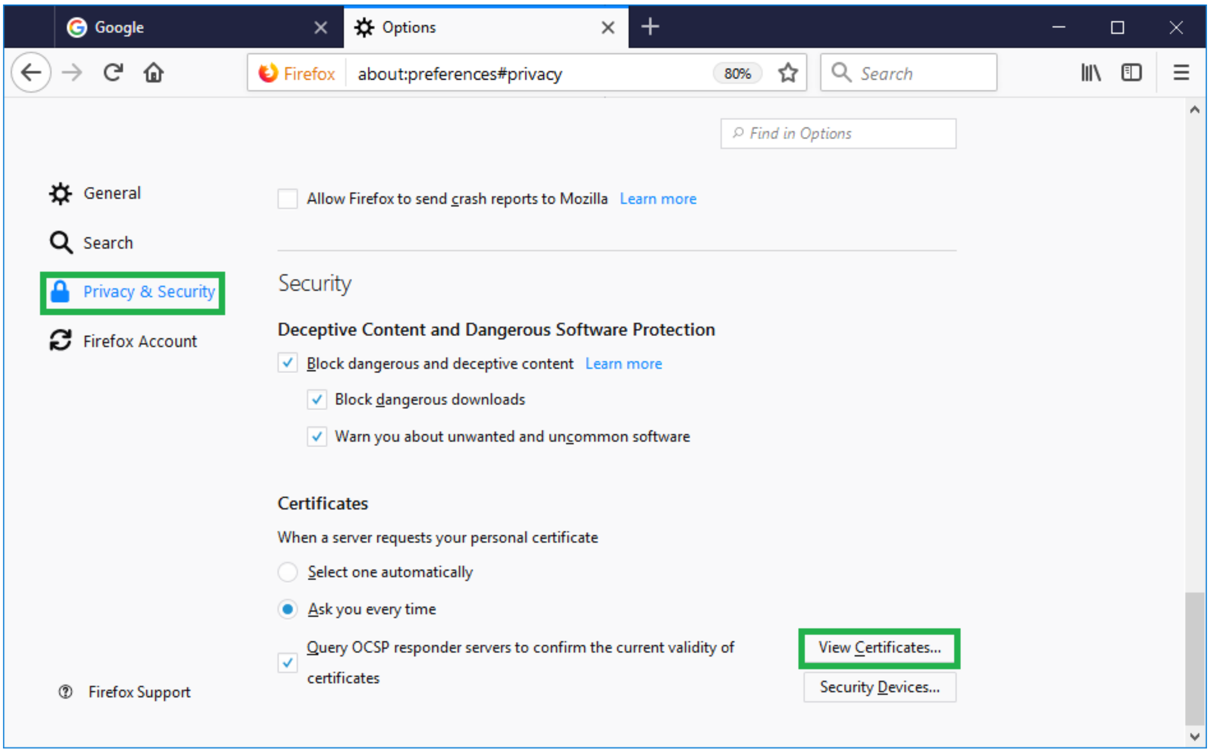


Figure 8

2. In the new tab (Figure 9) select the **Privacy & Security** option from the menu on the left side, go down and click on the **View Certificates** button:



□ Allow Firefox to send crash reports to Mozilla

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

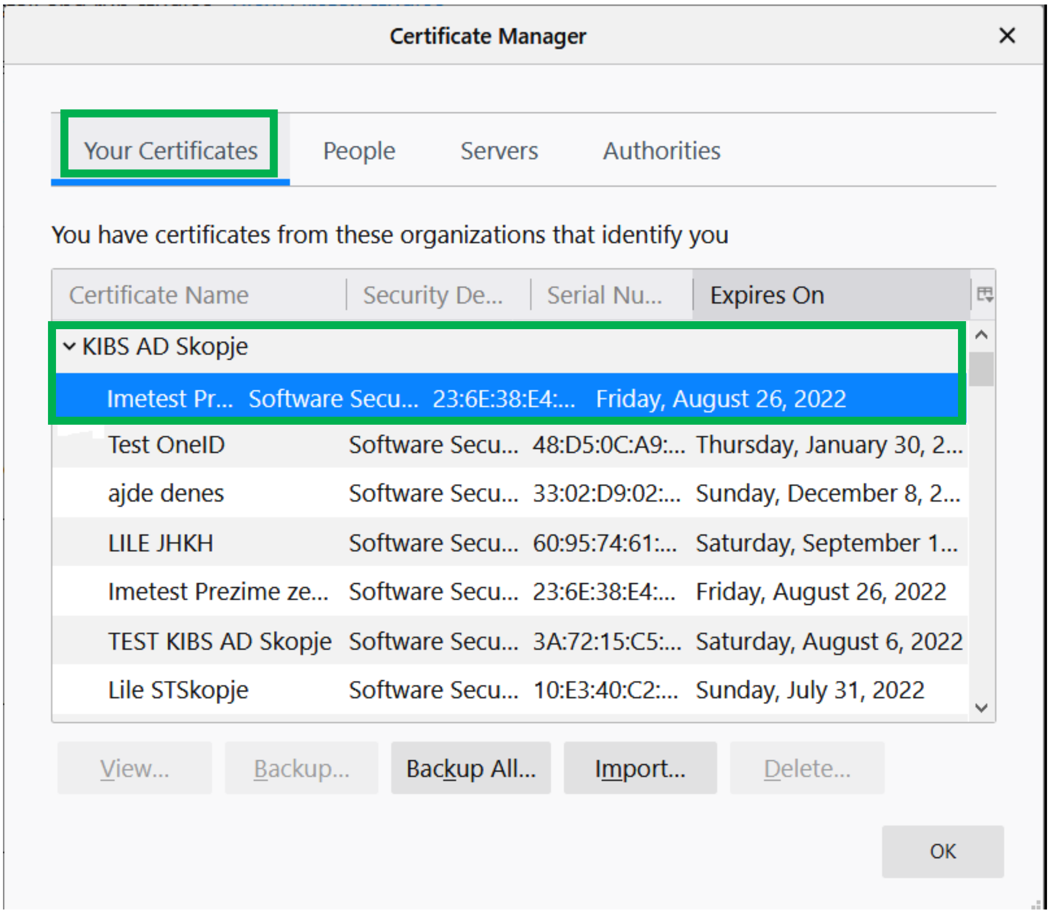
○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Figure 9

3. If your certificate is successfully installed, it will appear in the certificate list in the **Your Certificates** tab (Figure 10):



You have certificates from these organizations that identify you

Certificate Name	Security De...	Serial Nu...	Expires On
KIBS AD Skopje			
Imetest Pr...	Software Secu...	23:6E:38:E4:...	Friday, August 26, 2022
Test OneID	Software Secu...	48:D5:0C:A9:...	Thursday, January 30, 2...
ajde denes	Software Secu...	33:02:D9:02:...	Sunday, December 8, 2...
LILE JHKH	Software Secu...	60:95:74:61:...	Saturday, September 1...
Imetest Prezime ze...	Software Secu...	23:6E:38:E4:...	Friday, August 26, 2022
TEST KIBS AD Skopje	Software Secu...	3A:72:15:C5:...	Saturday, August 6, 2022
Lile STSkopje	Software Secu...	10:E3:40:C2:...	Sunday, July 31, 2022

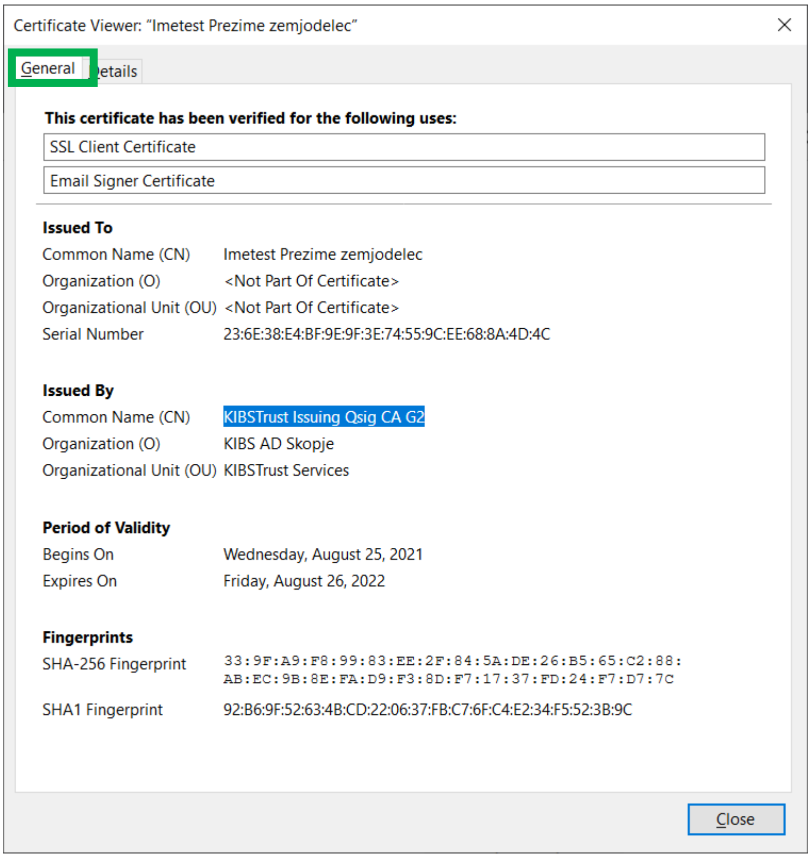
Figure 10

Click **View** and a new window will open which shows a detailed review of information regarding the certificate. In the **General** tab (Figure 11), the common information regarding the certificate are given:

Issued to: The name of the Subject to which the certificate is issued and its serial number

Issued by: The name of the Certificate Authority (**KIBSTrust Issuing Qsig CA G2 или KIBSTrust Issuing Qseal CA G2**)

Validity: Date of issue and expiry date.



This certificate has been verified for the following uses:

SSL Client Certificate

Email Signer Certificate

Issued To

Common Name (CN)	Imetest Prezime zemjodelec
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	23:6E:38:E4:BF:9E:9F:3E:74:55:9C:EE:68:8A:4D:4C

Issued By

Common Name (CN)	KIBSTrust Issuing Qsig CA G2
Organization (O)	KIBS AD Skopje
Organizational Unit (OU)	KIBSTrust Services

Period of Validity

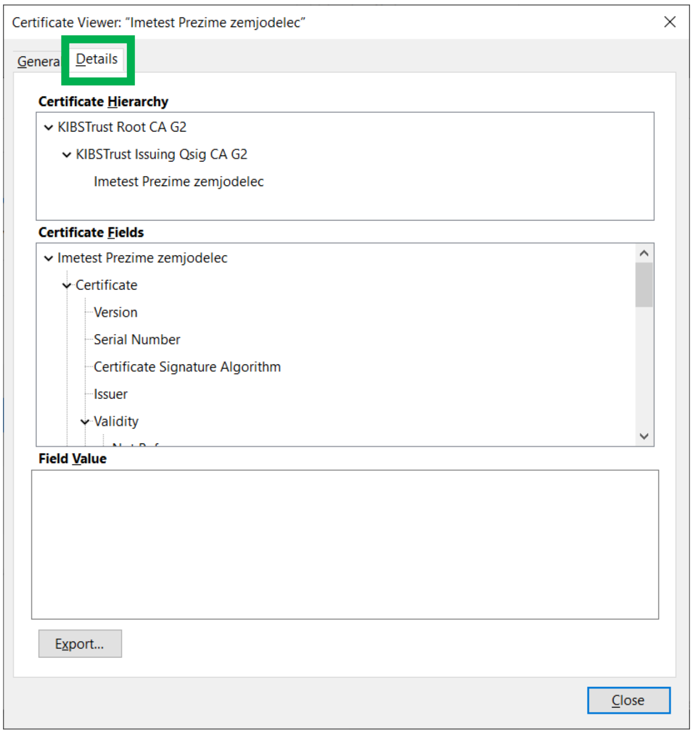
Begins On	Wednesday, August 25, 2021
Expires On	Friday, August 26, 2022

Fingerprints

SHA-256 Fingerprint	33:9F:A9:F8:99:83:EE:2F:84:5A:DE:26:B5:65:C2:88: AB:EC:9B:8E:FA:D9:F3:8D:F7:17:37:FD:24:F7:D7:7C
SHA1 Fingerprint	92:B6:9F:52:63:4B:CD:22:06:37:FB:C7:6F:C4:E2:34:F5:52:3B:9C

Figure 11

The root certificates, with which your certificate is signed, are shown in the **Details** tab (Figure 12). Check whether the two root certificates are shown: **KIBSTrust Root CA G2** (Root certificate) and issuing **KIBSTrust Issuing Qsig CA G2** or **KIBSTrust Issuing QsealCA G2 certificate**.



Certificate Hierarchy

- KIBSTrust Root CA G2
  - KIBSTrust Issuing Qsig CA G2
    - Imetest Prezime zemjodelec

Certificate Fields

- Imetest Prezime zemjodelec
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity

Figure 12

3. 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 .p12 file.**

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

1. From the browser menu, click right upper button and select **Options** (Figure 13):

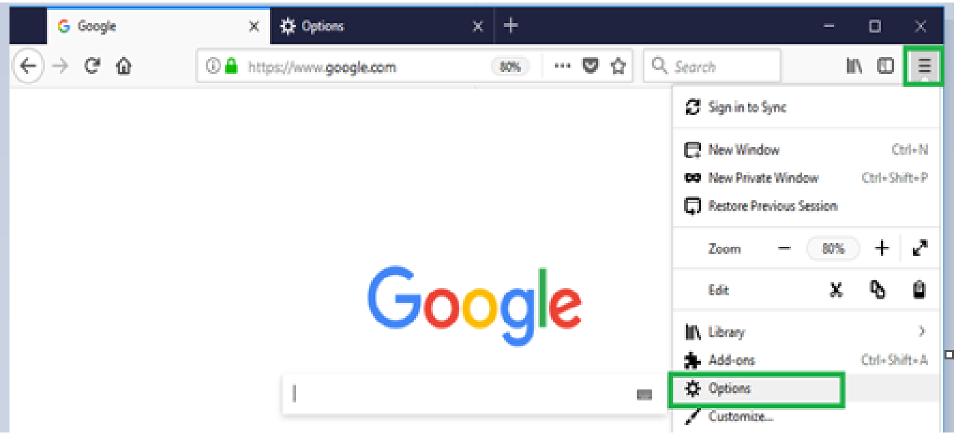
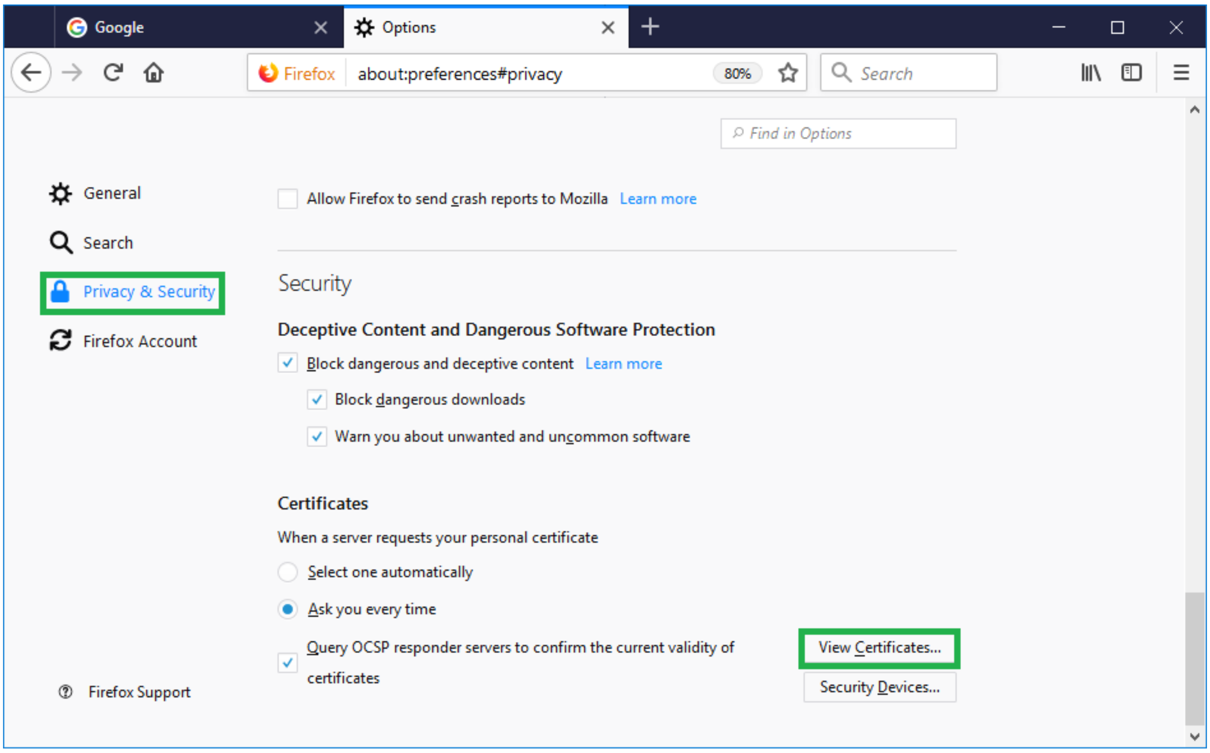


Figure 13

2. In the new tab (Figure 14) select the **Privacy & Security** option from the menu on the left side, then click on the **View Certificates** button:



□ Allow Firefox to send crash reports to Mozilla Learn more

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

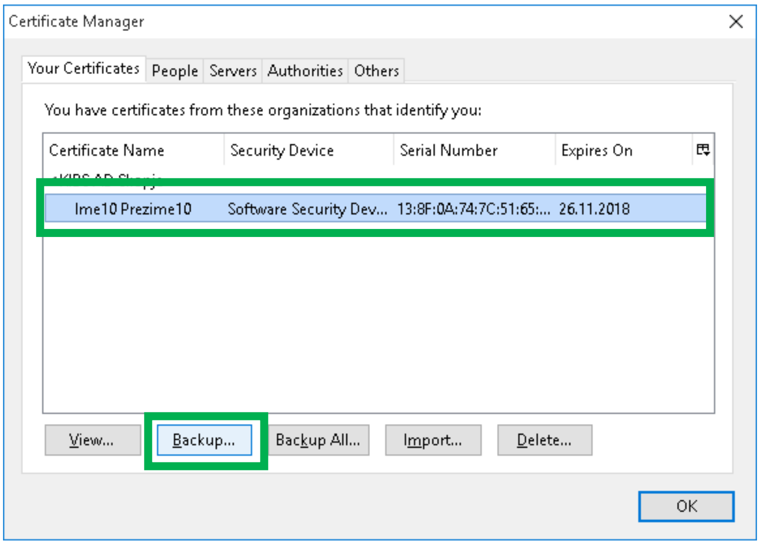
○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Figure 14

3. From the **Your Certificates** tab (Figure 15), select the certificate which you would like to export and click on the **Backup**… button:



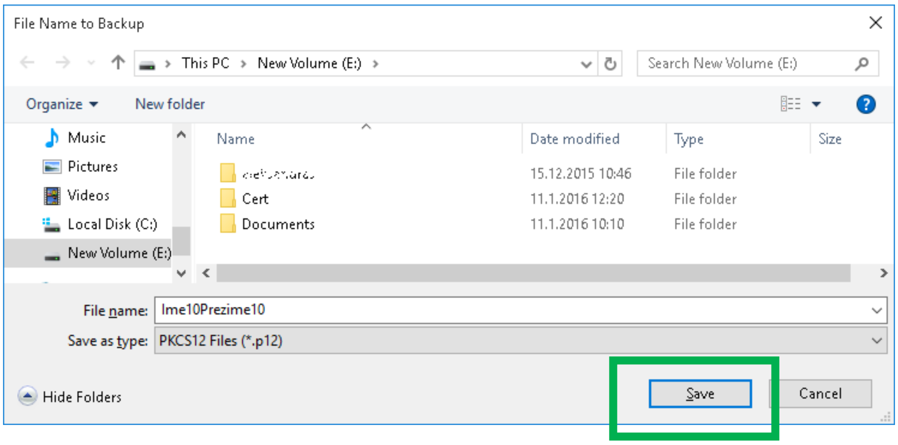
Certificate Manager

You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
Ime10 Prezime10	Software Security Dev...	13:8F:0A:74:7C:51:65:...	26.11.2018

Figure 15

4. Enter a file name and location (Figure 16). Choose the format of the file in which you will export the certificate. Click on **Save** to continue:



File Name to Backup

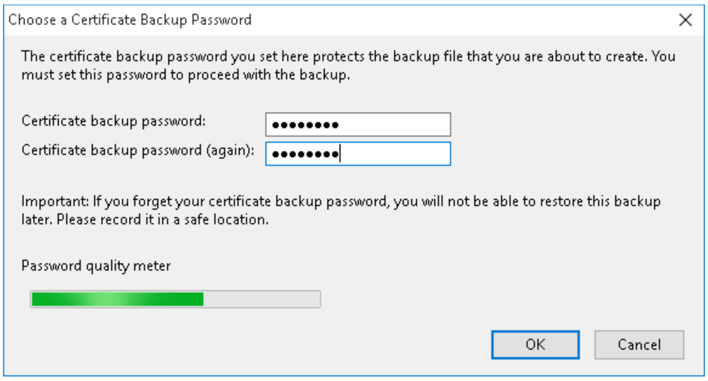
Name	Date modified	Type	Size
[illegible]	15.12.2015 10:46	File folder	
Cert	11.1.2016 12:20	File folder	
Documents	11.1.2016 10:10	File folder	

File name: Ime10Prezime10

Save as type: PKCS12 Files (*.p12)

Figure 16

5. Enter a password to protect the private key (Figure 17). **You are the only one that knows the password, please remember it or keep it written down in a safe place!** Click **OK** to continue:



Choose a Certificate Backup Password

The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Certificate backup password: ●●●●●●●●●

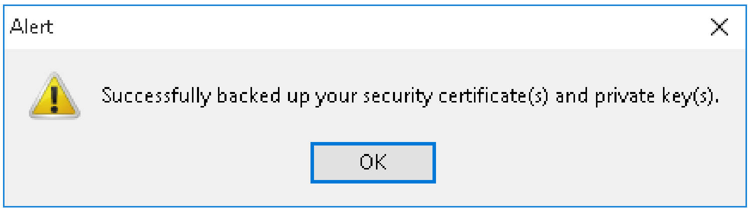
Certificate backup password (again): ●●●●●●●●●

Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location.

Password quality meter

Figure 17

6. You will receive a message that you successfully exported your certificate (Figure 18):



Alert

Successfully backed up your security certificate(s) and private key(s).

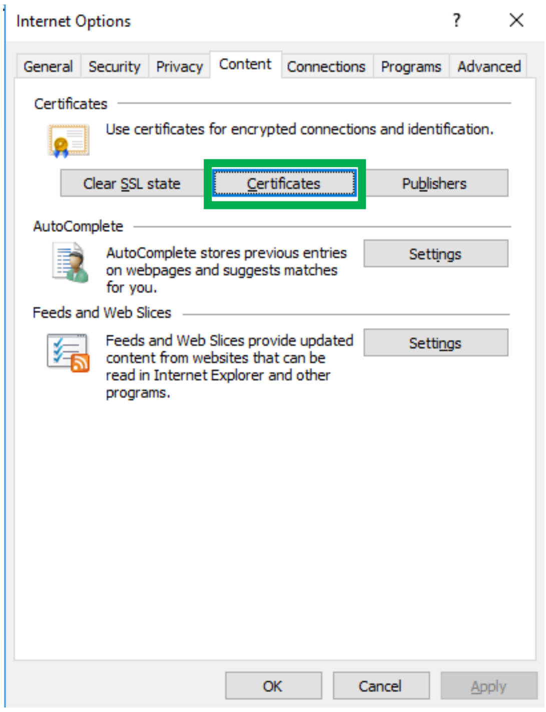
Figure 18

IMPORTANT: Store the .P12 file to which your certificate is exported and the password for it on a safe external media (external hard drive, usb flash, CD/DVD…)!

4. How to import a certificate in Internet Explorer?

To import a certificate in Internet Explorer (IE), you have to have backup file (.pfx or .p12) and folow the steps:
From IE, chose Tools/Internet Options/Content/Certificates or you can open console **Manage User Certificates**. (Figure 19)

Then in **Personal** tab, click **Import** (Figure 20), and the wizard will guide you through the procedure of importing a certificate (Figure 21). Choose **Browse** (Figure 22).



Internet Options

Certificates

Use certificates for encrypted connections and identification.

AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Figure 19

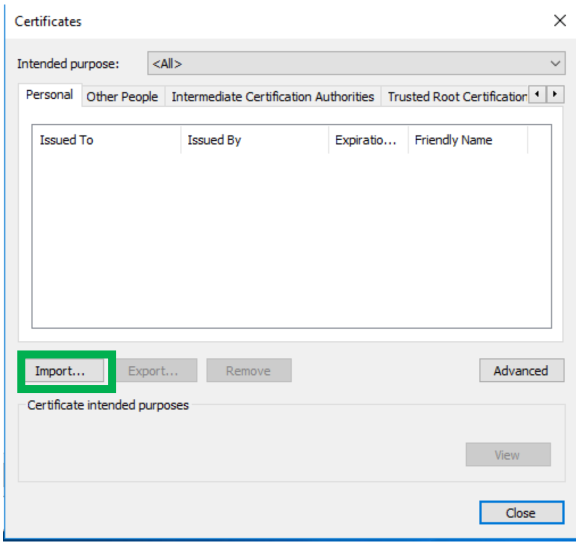
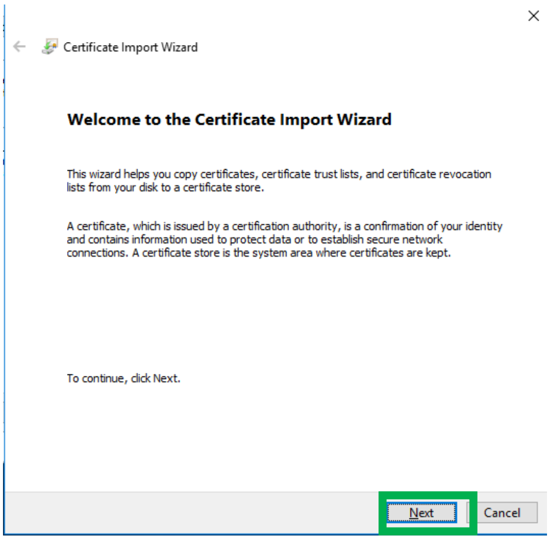


Figure 20



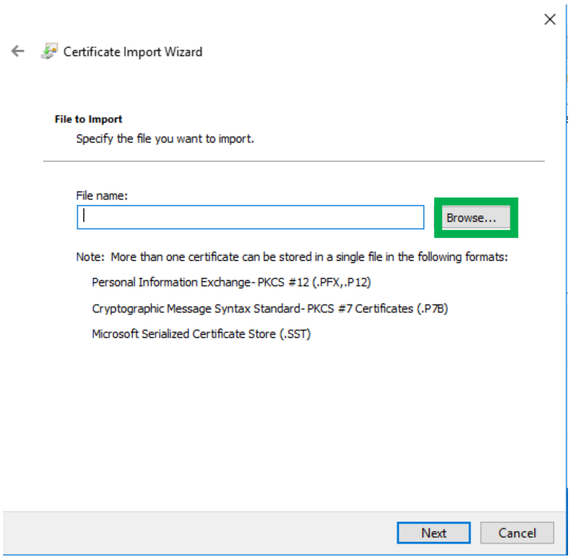
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 21



File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

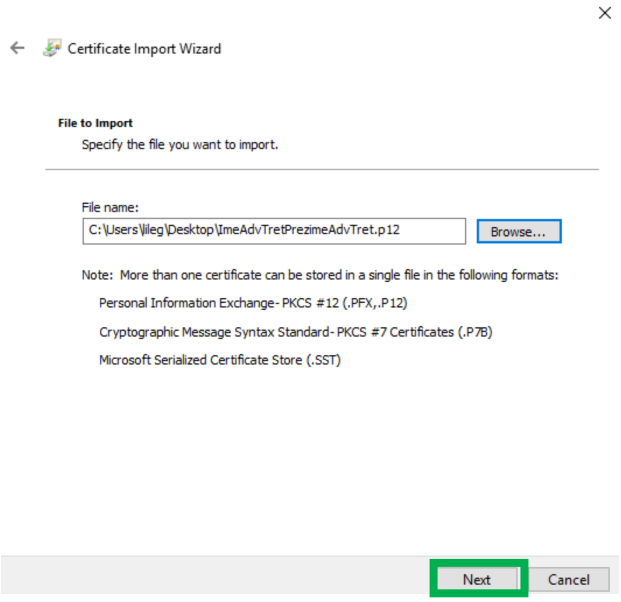
Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

Figure 22

Then you can select the file with your certificate (Figure 23).



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\ileg\Desktop\ImeAdvTretPrezimeAdvTret.p12

Note: More than one certificate can be stored in a single file in the following formats:

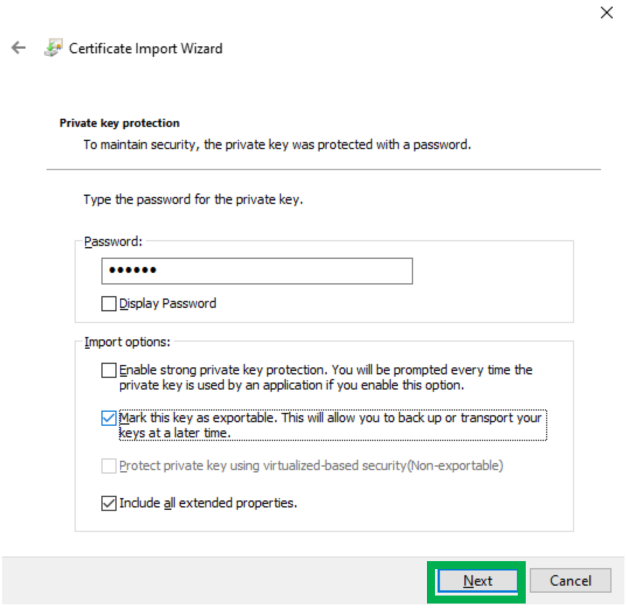
Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

Enter the password which you have set during the backup procedure for the certificate, check “Mark the private key as exportable” and click **Next** to continue (Figure 24).

Figure 23



Certificate Import Wizard

Private key protection

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

Type the password for the private key.

Password:

••••••

□ Display Password

Import options:

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

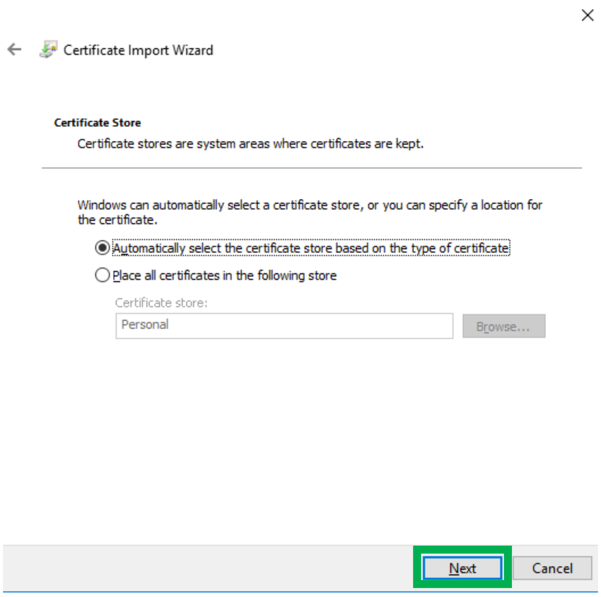
☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

Figure 24

Select the “Automatically select the certificate store-based on the type of certificate” opinion, then **Next** and **Finish** (Figure 25).



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.

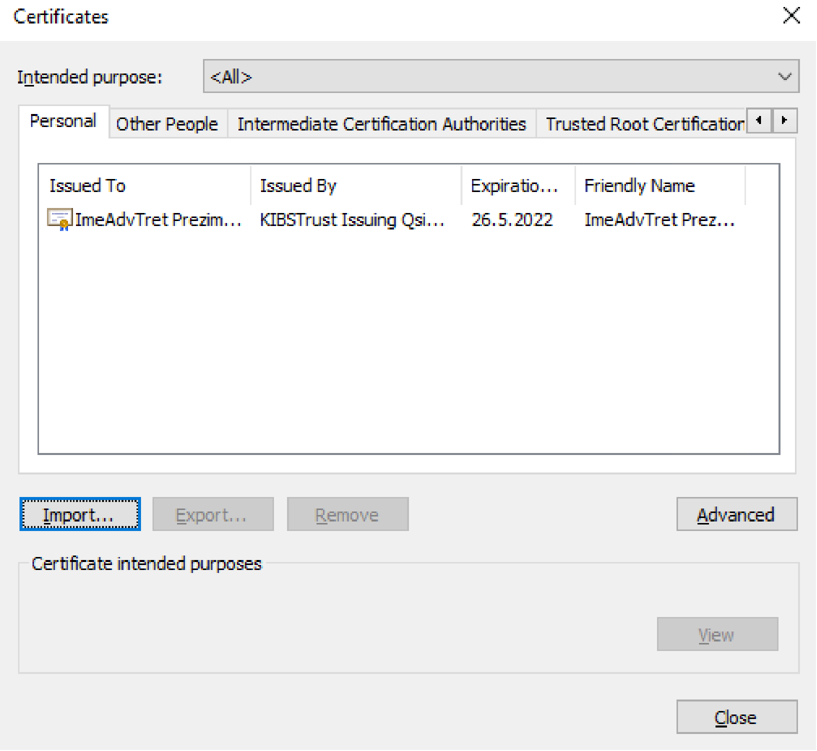
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store: Personal

Figure 25

You will receive a message that your certificate was successfully imported. The certificate should now appear in your list of personal certificates (Figure 26).



Certificates

Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
ImeAdvTret Prezim...	KIBSTrust Issuing Qsi...	26.5.2022	ImeAdvTret Prez...

Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

Figure 26

Now, the certificate is also available in Google Chrome web browser.

5. How to check Root certificates in Internet Explorer

Open your certificate (Figure 26) with double click, then in tab **Certification Path** check whether you can see certificate chain made by your certificate and:

- **KIBSTrust Root CA G2** root CA certificate and
- **KIBSTrust Issuing Qsig CA G2** or **KIBSTrust Issuing Qseal CA G2** issuing CA certificate

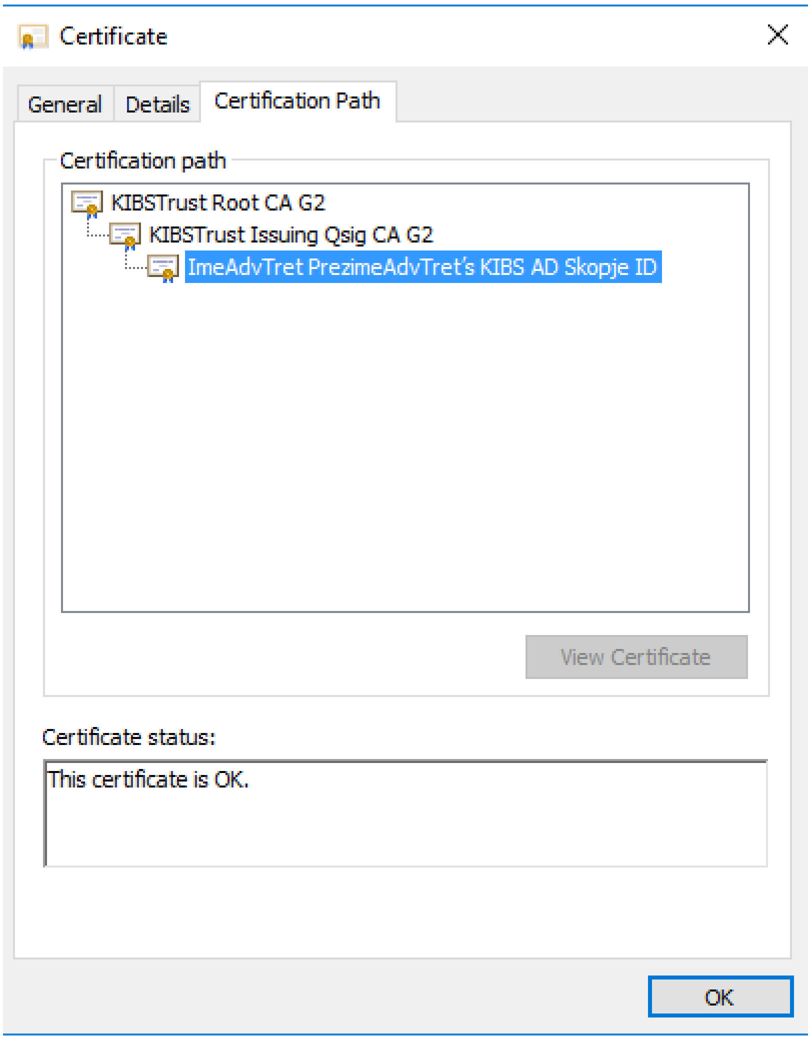


Figure 27

If some of KIBSTrust root certificates is missing in the certificate chain, you download from section **Root certificates** from https://www.kibstrust.com/en-GB/Home/Support/ and please install them:

[KIBSTrust Issuing Qsig CA G2](#) (install in Intermediate Certificate Authorities)

[KIBSTrust Issuing Qseal CA G2](#) (install in Intermediate Certificate Authorities)

[KIBSTrust Root CA G2](#) (install in Trusted Root Certficate Authorities)

* * *