УПАТСТВО

Преземање сертификат користејќи Mozilla Firefox ESR

Верзија: 5.1

Датум: 31.01.2022

103.11

КИБС АД Скопје

©2022 КИБС АД Скопје, сите права задржани

http://www.kibstrust.com/

Содржина

1. Како да го преземам сертификатот? 2
2. Како да проверам дека сертификатот е добро инсталиран? 5
3. Како да направам безбедносна копија од сертификатот? 9
4. Како да го импортирам сертификатот во Internet Explorer? 11
5. Проверка на коренски сертификати во Internet Explorer 14

1. Како да го преземам сертификатот?

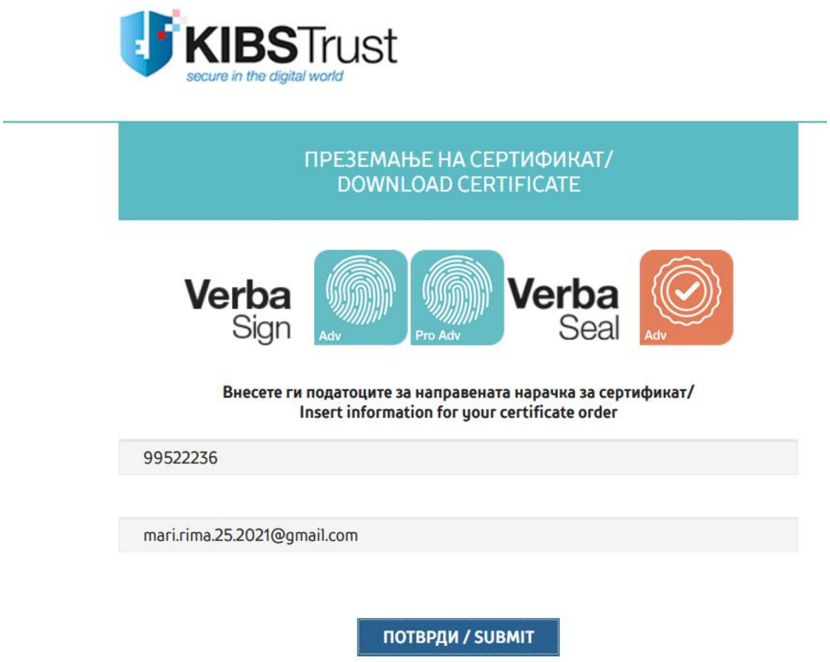
Од сертификати кои ги нуди КИБС ИС, сертификатите Verba Sign Adv, Verba Sign Pro Adv и Verba Seal Adv се генерираат на дискот на вашиот компјутер.

За да преземете еден од горенаведените сертификати, Ве молиме да го користете го веб прелистувачот Mozilla Firefox ESR, верзија која не е повисока од 68.3, која можете да ја преземете од веб локцијата: https://ftp.mozilla.org/pub/firefox/releases/68.3.0esr/, каде бирате подфолдер win64/ за 64 или win32/ за 32-битна верзија на Firefox.

Потоа, следете ги следните чекори:

1. Првин, отворете го веб прелистувачот Mozilla Firefox ESR, при што внимавајте да не направи Upgrade, па отворете го линкот https://e-shop.kibstrust.com/raweb во него.
2. На веб страната (Слика 1) внесете:
    - Нарачка: внесете го бројот на нарачка кој ви е испратен во истата електронска порака
    - E-mail: внесете ја e-mail адресата која ја наведовте во формуларот за барање за сертификат

   и кликнете **Потврди.**



Слика 1

3. Ќе ви се отвори страната за потврда на податоците од регистрација (на Слика 2 е прикажан пример за Verba Sign Pro Adv сертификат). Проверете ги податоците и внесете **Фраза за автентикација**, без интерпункциски знаци. Изберете **High Grade** кај Јачина на енкрипција. Кликнете **Submit (Потврди).**

Symantec. **Enrollment**

Help with this Page

Потврда на податоците од порачката/ Confirm data from purchase order

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

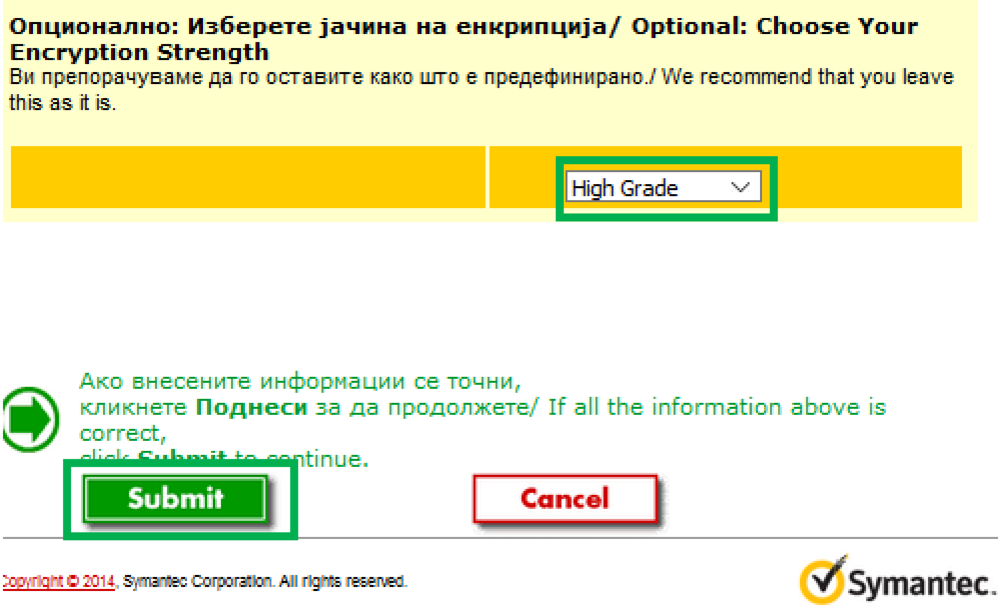
Податоците ги пополнивте при поднесувањето на порачката за сертификат. Полињата обележани со ѕвезда (*) ќе бидат содржани во Вашиот сертификат и ќе можат да бидат видени како детали на сертификатот.
The data that were fulfilled during purchase order for certificate. Fields marked with an asterisk (*) 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

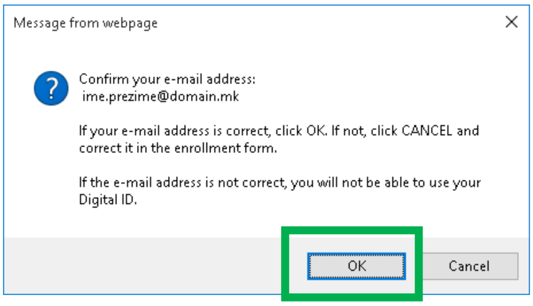
Фразата за автентикација е уникатна фраза која Ве заштитува од неавторизирани активности врз Вашиот сертификат. Не ја споделувајте. **Внимавајте да не ја изгубите.** Таа е потребна за поништување на Вашиот сертификат.
The Challenge Phrase is a unique phrase that protects you against unauthorized action 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.	



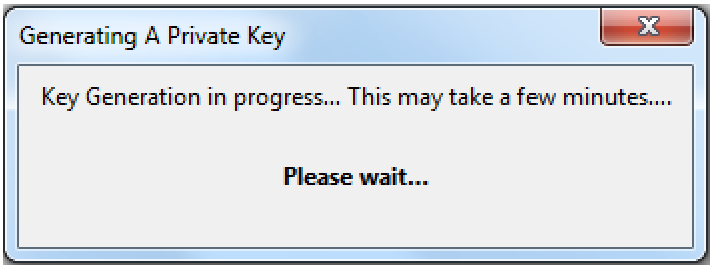
Слика 2

4. По кликнување на копчето **Submit (Потврди)**, ќе ви се јави порака како на Слика 3. Уште еднаш проверете ја e-mail адресата и кликнете **OK** ако сè е во ред.



Слика 3

5. По кликнување на **OK** ќе се појави прозорче како на Слика 4, кое Ве информира дека во тек е генерирањето на парот клучеви за вашиот сертификат**. Ве молиме почекајте**.

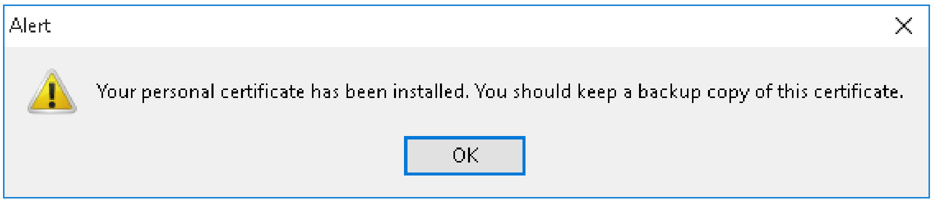


Слика 4

6. Потоа започнува процесот на генерирање на Вашиот сертификат. Ве молиме почекајте додека трае овој процес (Слика 5).

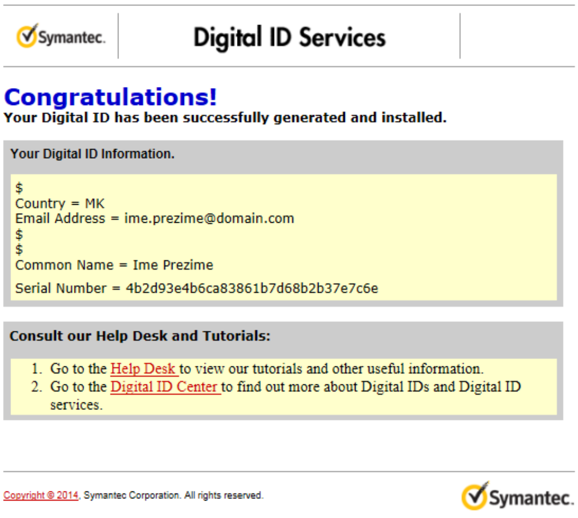
Слика 5

7. Ќе ви се јави порака дека Вашиот сертификат е инсталиран (Слика 6). Кликнете **OK**.



Слика 6

8. Потоа, на веб страната ќе се прикаже дека сертификатот е генериран и инсталиран (Слика 7)!

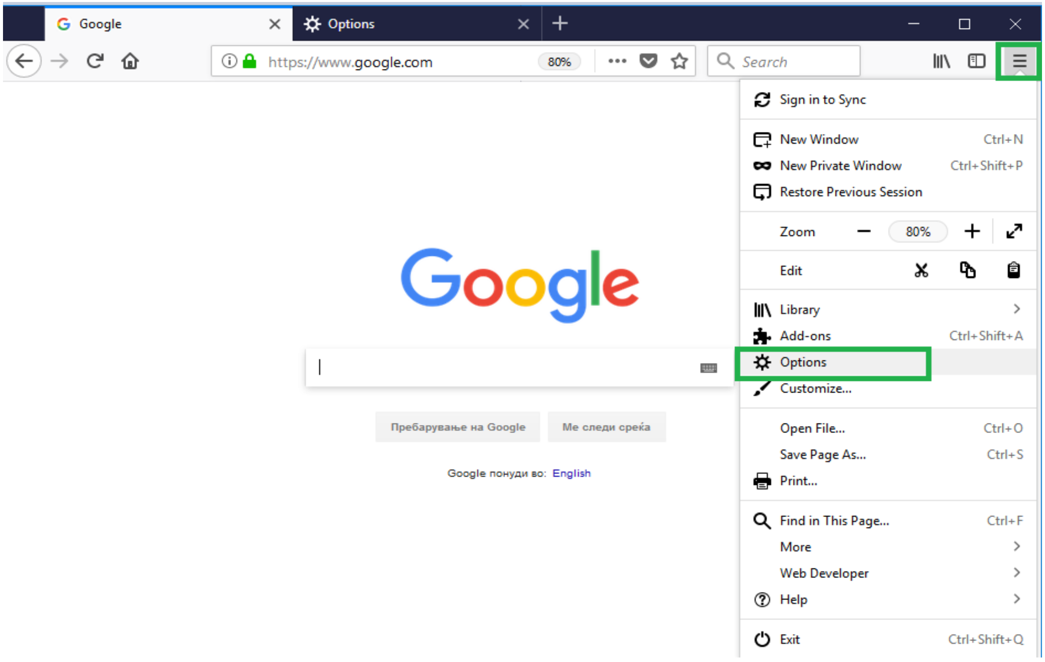


Слика 7

2. Како да проверам дека сертификатот е добро инсталиран?

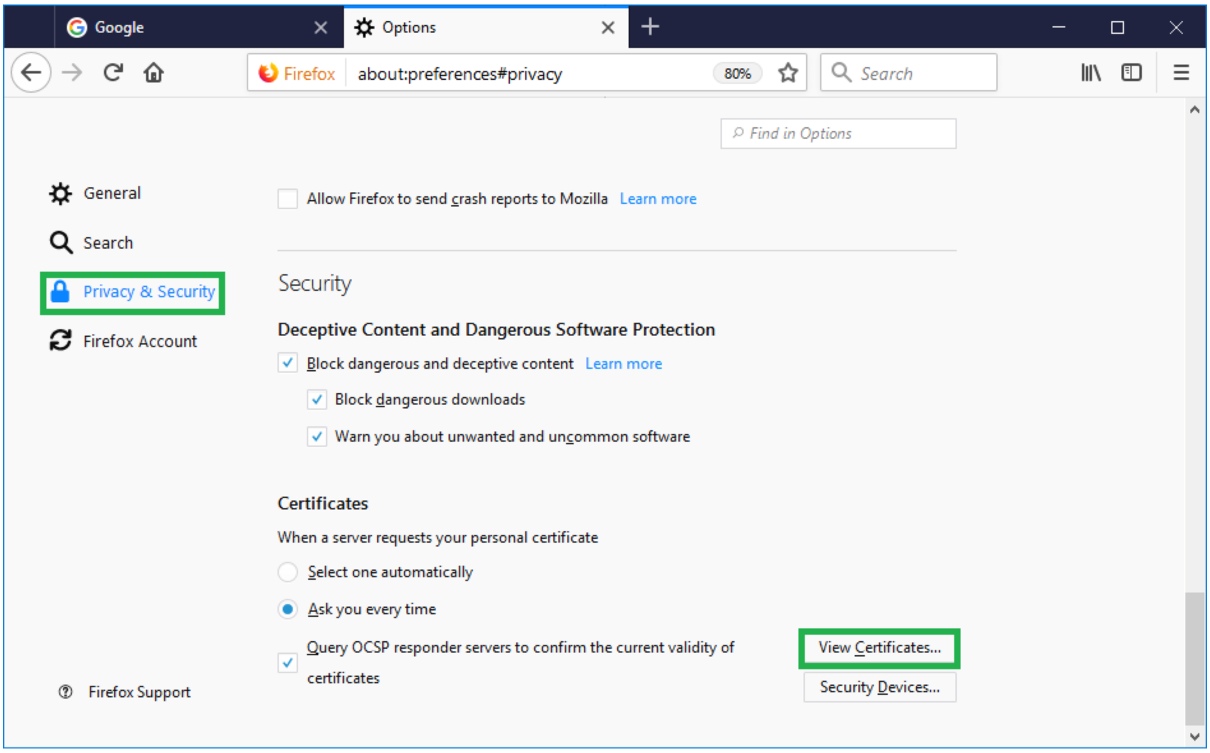
По добивање на пораката дека Вашиот сертификат е успешно инсталиран, потребно е да проверите дали истиот е додаден во листата на персонални сертификати во веб прелистувачот. За да ја направите оваа проверка, извршете ги следните чекори:

1. Од менито на прелистувачот во горен десен агол селектирајте **Options** (Слика 8):



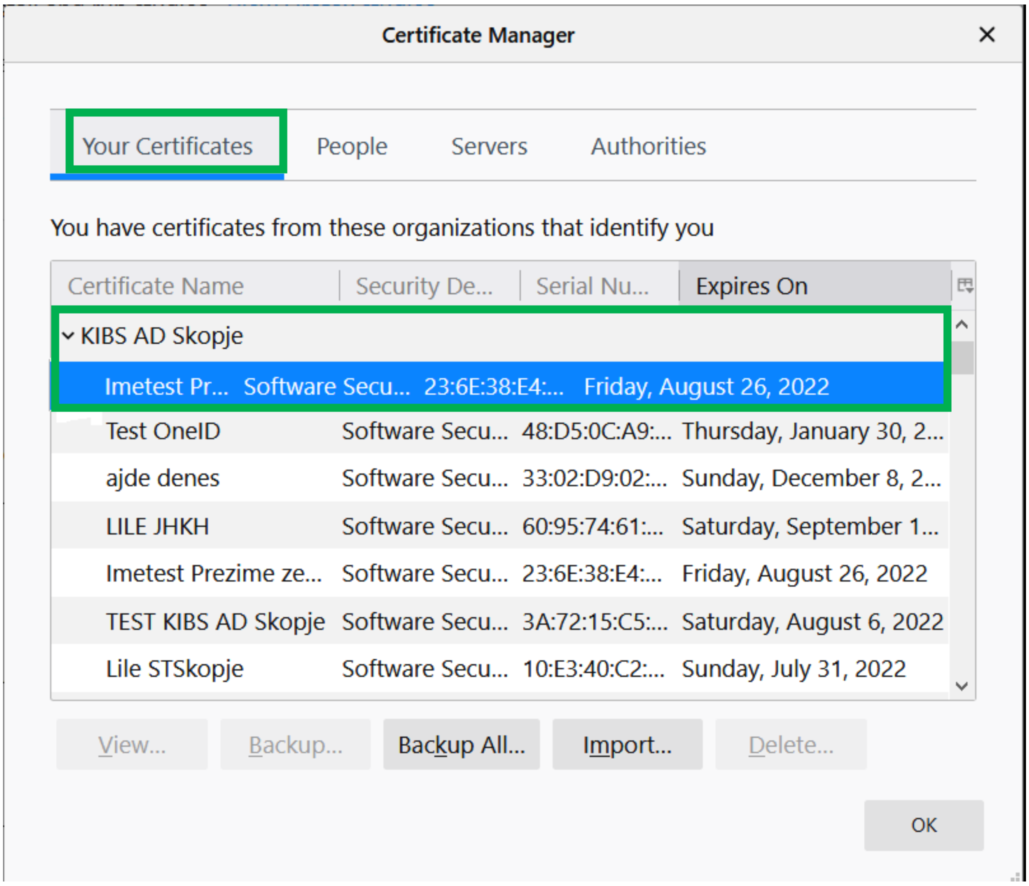
Слика 8

2. Во новиот прозорец (Слика 9) од менито на левата страна изберете ја опцијата **Privacy & Security,** отидете најдолу, притиснете на копчето **View Certificates**:



Слика 9

3. Ако Вашиот сертификат е успешно инсталиран, тој ќе се наоѓа во листата на сертификати во картичката **Your Certificates** (Слика 10):



Слика 10

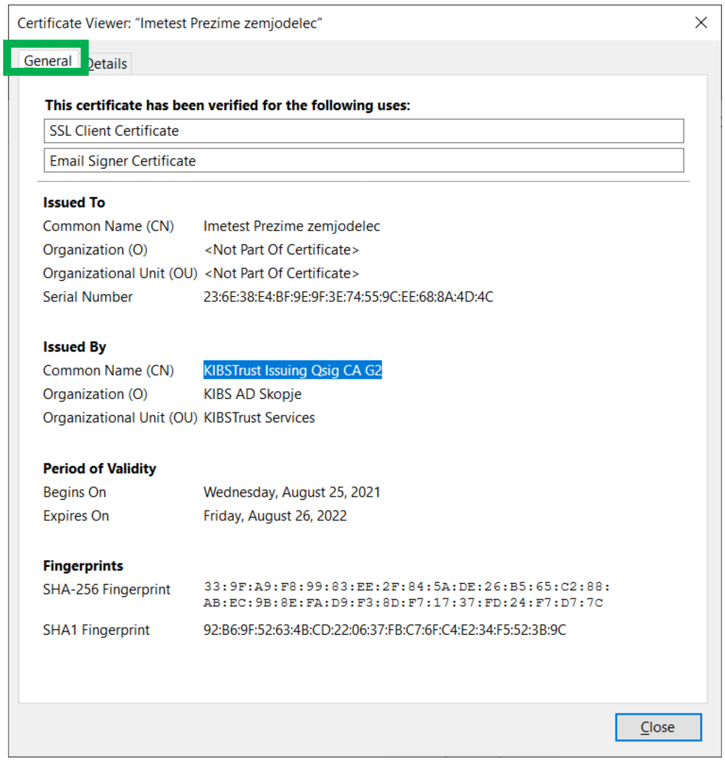
Кликнете на View и ќе ви се прикаже нов прозорец во кој е даден преглед на подетални информации за истиот. Во картичката General (

Слика 11) дадени се општите информации за сертификатот:

Issued to: Податоци за субјектот за кој е издаден сертификатот и серискиот број на сертификатот

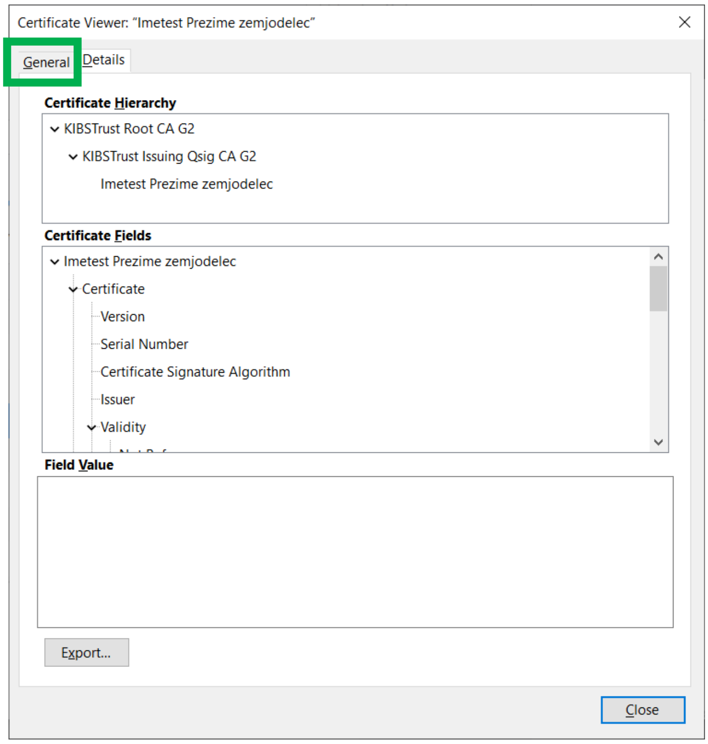
Issued by: Податоци за Издавачот на сертификати (**KIBSTrust Issuing Qsig CA G2** или **KIBSTrust Issuing Qseal CA G2**)

Validity: Датум на издавање и датум на истекување на периодот на важење.



Слика 11

Во картичката **Details** (Слика 12) се прикажуваат коренските сертификати (Certificate Hierarchy) со кои е потпишан Вашиот сертификат. Проверете дали се прикажуваат 2 коренски сертификати: **KIBSTrust Root CA G2** (Root сертификат) и **KIBSTrust Issuing Qsig CA G2** или **KIBSTrust Issuing QSealCA G2** како издавачки сертификати.



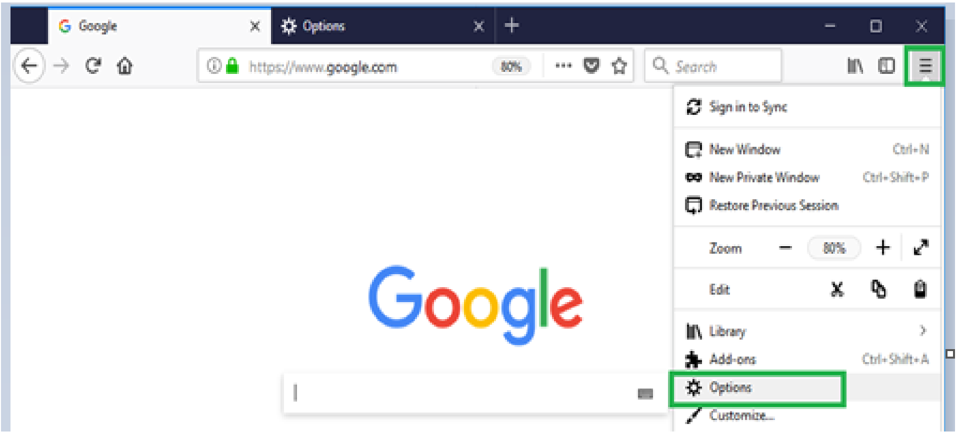
Слика 12

3. Како да направам безбедносна копија од сертификатот?

Вашиот сертификат е инсталиран на дискот на Вашиот компјутер и истиот може да биде избришан при појава на грешки во оперативниот систем или откажување на хардверот на Вашиот компјутер. За да го заштитите Вашиот сертификат во вакви ситуации, **потребно е да направите безбедносна копија од сертификатот односно да го експортирате во .p12 датотека**.

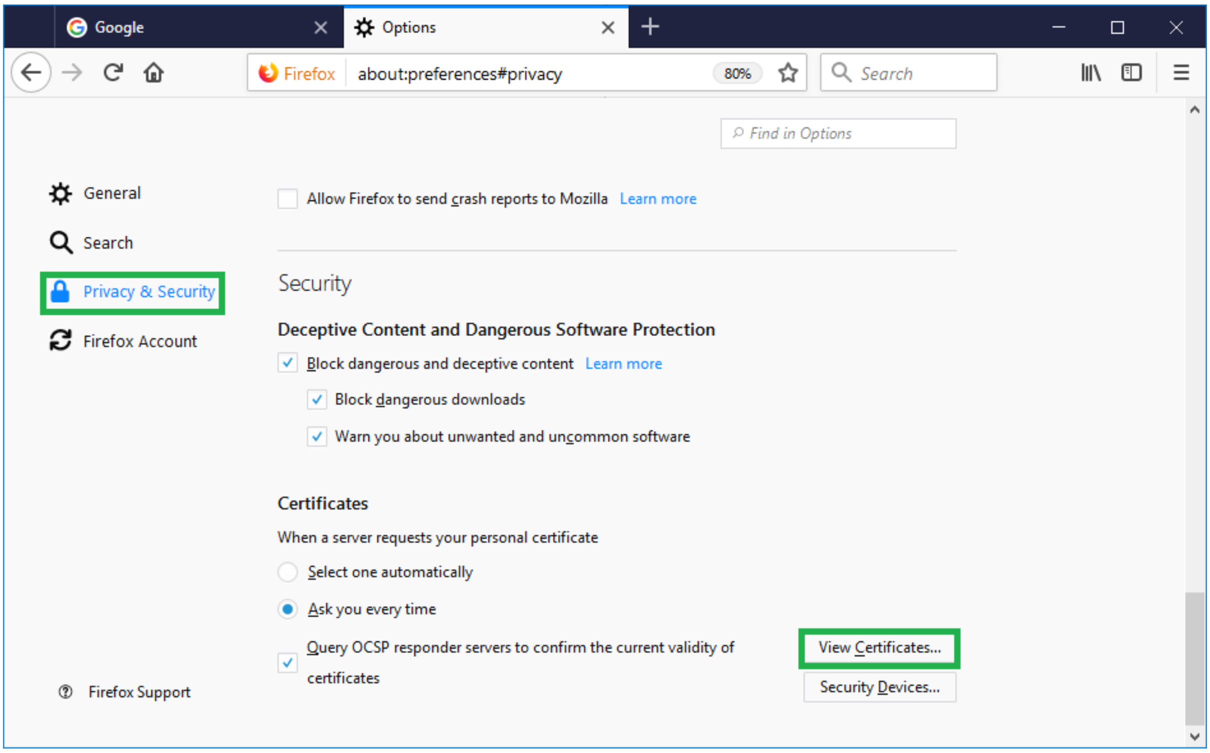
За да направите безбедносна копија од Вашиот сертификат треба да ги извршите следните чекори:

1. Од менито на прелистувачот во горен десен агол селектирајте **Options** (Слика 13):



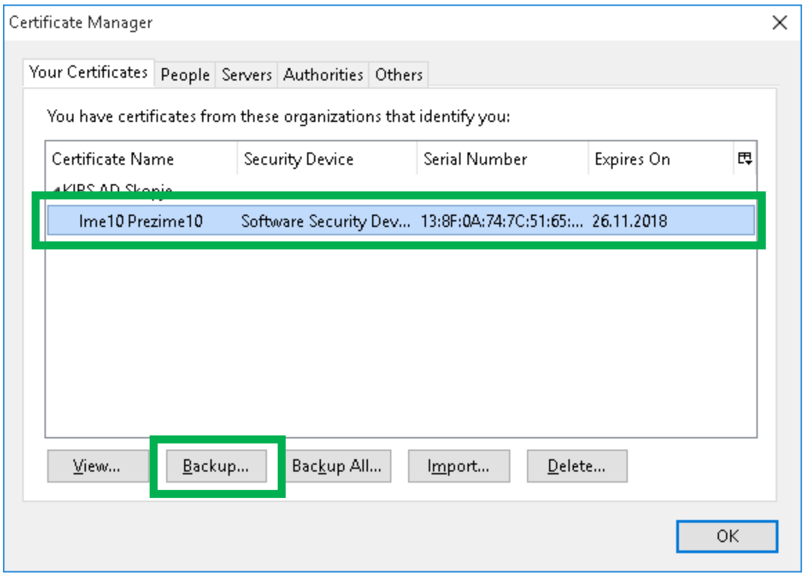
Слика 13

2. Во новиот прозорец (Слика 14) од менито на левата страна изберете ја опцијата **Privacy & Security,** отидете најдолу, притиснете на копчето **View Certificates**:



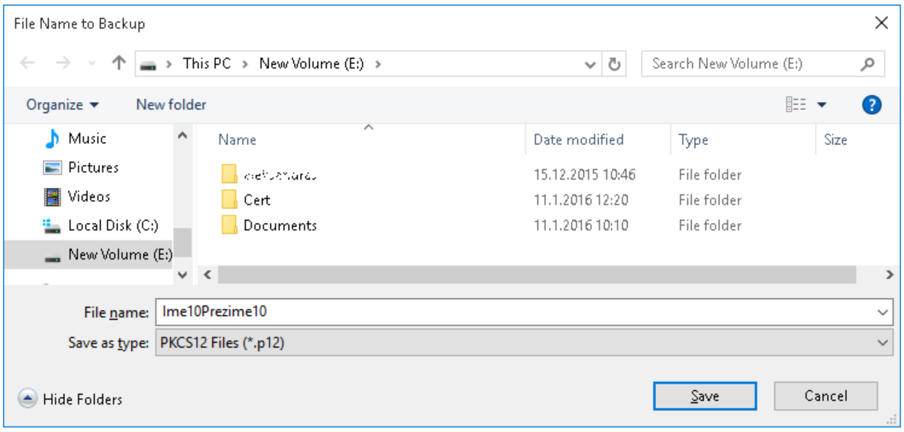
Слика 14

3. Од картичката **Your Certificates** (Слика 15) изберете го Вашиот сертификат и кликнете на копчето **Backup...**:



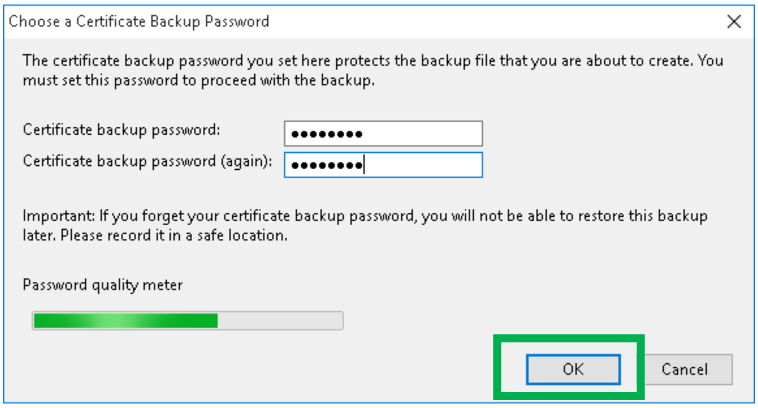
Слика 15

4. Изберете локација каде што ќе се зачува датотеката и внесете име на датотеката (Слика 16). Кликнете **Save** за да продолжите:



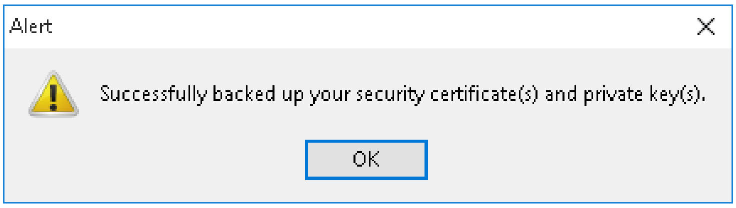
Слика 16

5. Внесете лозинка со која ќе го заштитите приватниот клуч (Слика 17). **Поставената лозинка ја знаете само Вие, Ве молиме да ја запаметите или да ја запишете на безбедно место!** Кликнете **OK** за да продолжите:



Слика 17

6. Ќе добиете порака дека успешно го експортиравте Вашиот сертификат (Слика 18):

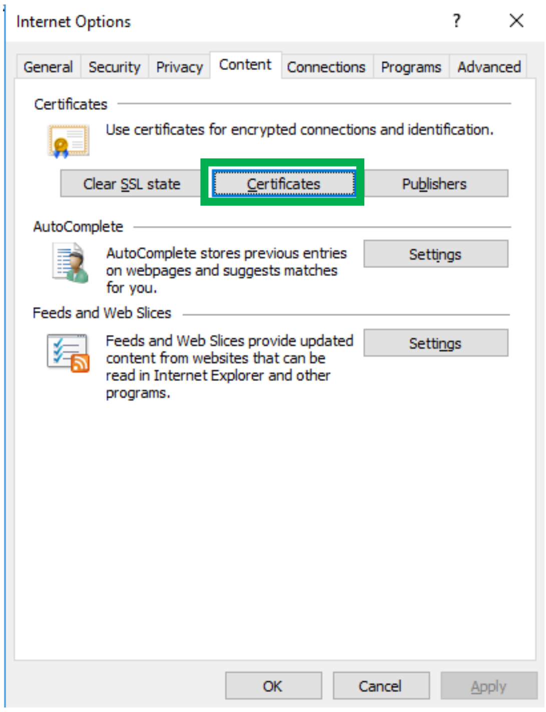


Слика 18

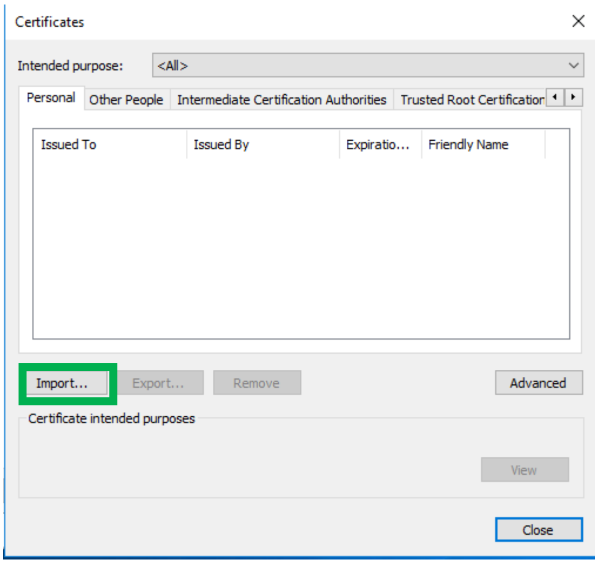
ВАЖНО: **.P12 датотеката во која е експортиран Вашиот сертификат и лозинката за истата зачувајте ги на безбеден надворешен медиум (надворешен хард диск, USB flash меморија, CD/DVD…)!**

4. Како да го импортирам сертификатот во Internet Explorer?

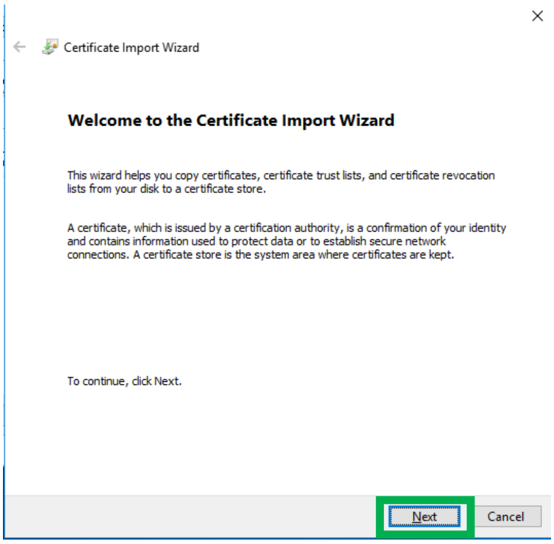
За да импортирате сертификат во Internet Explorer (IE), прво треба да имате датотека од вашиот сертификат со екстензија .pfx или .p12, а потоа да ги извршите следните чекори:
Во Internet Explorer бирате Tools/Internet Options/Content/Certificates (или пак директно од **Manage User Certificates** конзолата) изберете **Certificates** (Слика 19), а потоа **Import** (Слика 20), Next (Слика 21), Browse (Слика 22).



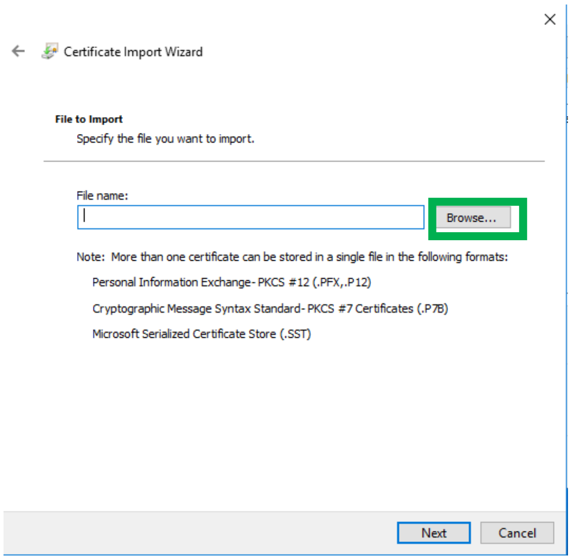
Слика 19



Слика 20

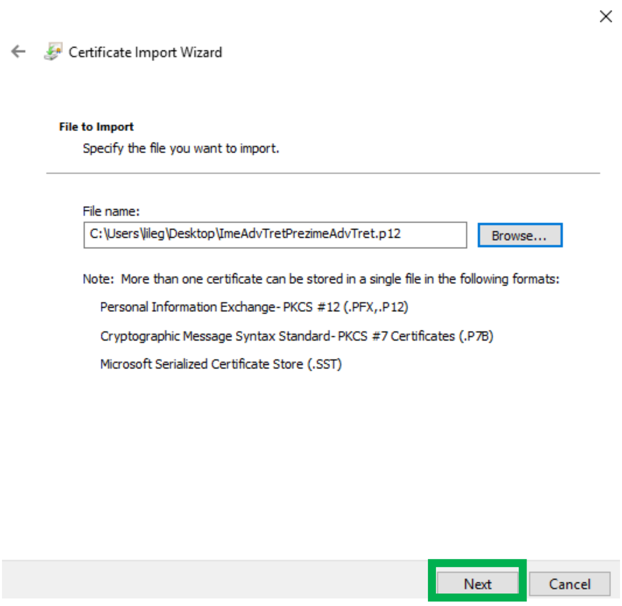


Слика 21



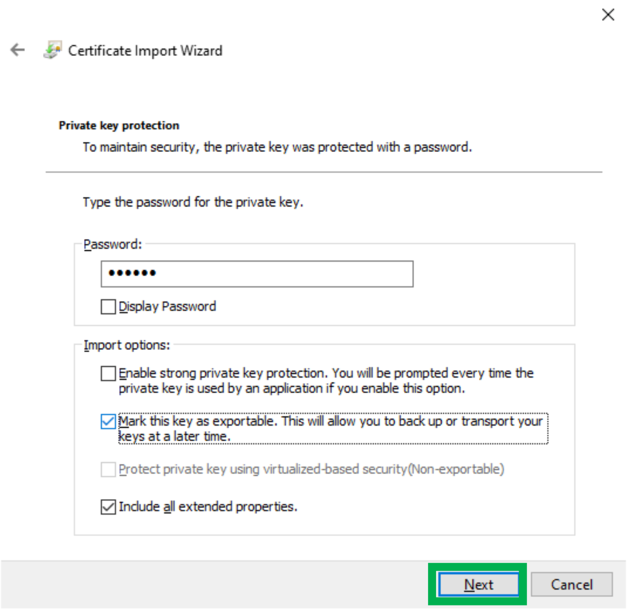
Слика 22

Потоа потврдете го направениот избор со кликање на **Next** (Слика 23).



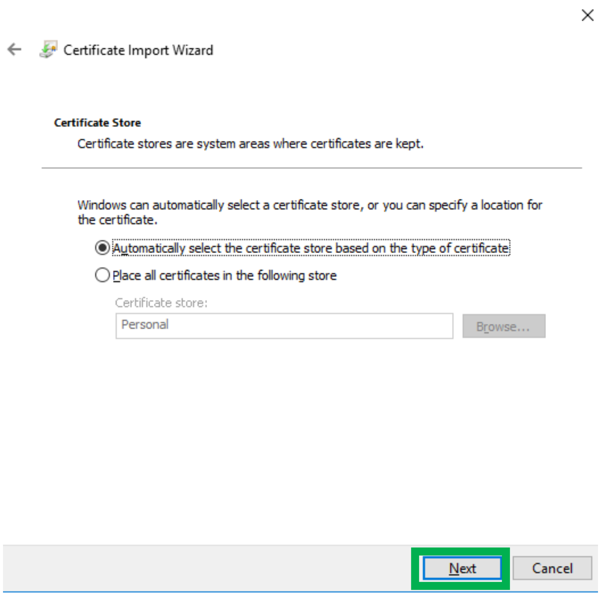
Слика 23

Ставете ја лозинката од бекап фајлот изберете ја опцијата "Mark the private key as exportable" и изберете **Next** (Слика 24).



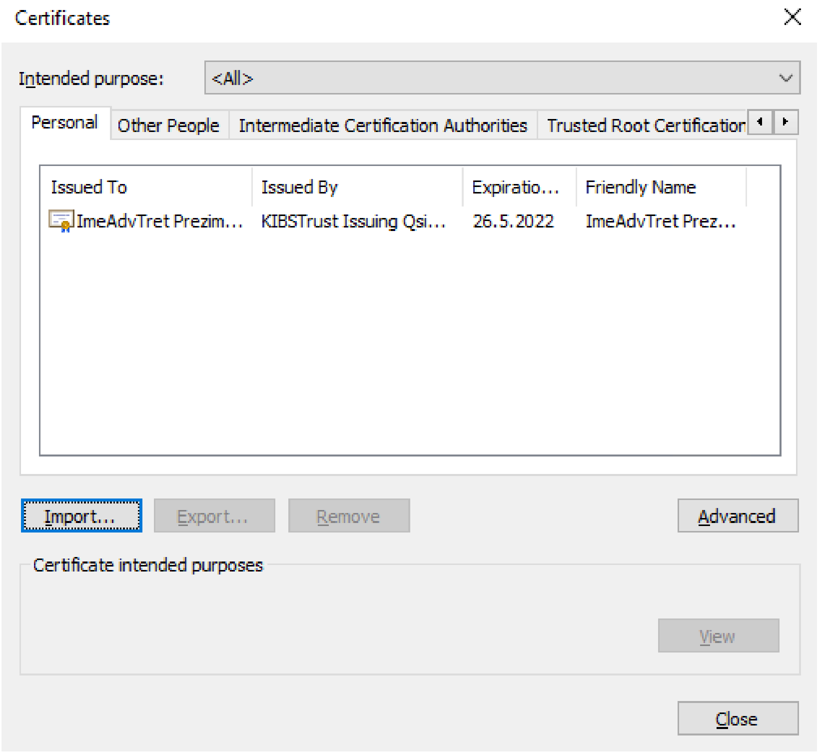
Слика 24

Изберете Изберете ја опцијата „Automatically select the certificate store based on the type of certificate“, потоа избирајте **Next** како на Слика 25 и на крај **Finish**.



Слика 25

Сертификатот сега треба да се појави во Вашата листа на лични сертификати (Слика 26):



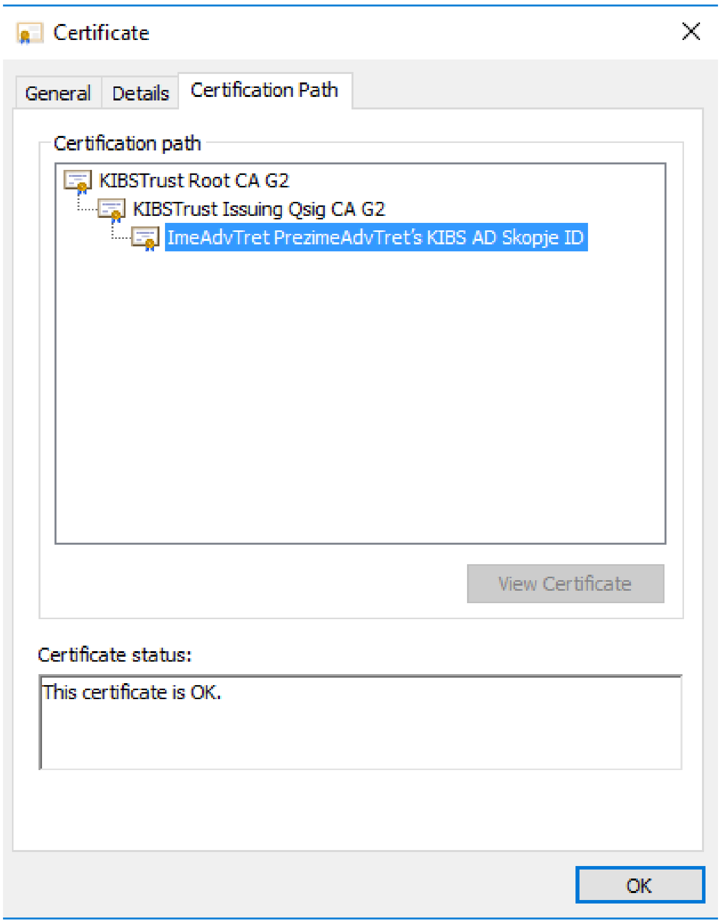
Слика 26

Вака импортиран сертификатот е достапен и преку прелистувачот Google Chrome.

5. Проверка на коренски сертификати во Internet Explorer

Со двоен клик на сертификатот (Слика 26) отворете го и проверете дали во табот **Certification Path** приказот е како на Слика 27, односно дали се прикажува ланец од вашиот сертификат и:

- коренски сертификат **KIBSTrust Root CA G2** и
- издавачки **KIBSTrust Issuing Qsig CA G2** или **KIBSTrust Issuing Qseal CA G2**



Слика 27

Доколку во приказот над вашиот сертификат недостасува некој од коренските сертификати на издавачот KIBSTrust, Ве молиме да ги преземете од секцијата **Коренски сертификати** од https://www.kibstrust.com/mk-MK/Home/Support/ и да ги инсталирате:

KIBSTrust Root CA G2 (Инсталирајте ги во Trusted Root Certficate Authorities)

KIBSTrust Issuing Qsig CA G2 (Инсталирајте ги во Intermediate Certificate Authorities)

KIBSTrust Issuing Qseal CA G2 (Инсталирајте ги во Intermediate Certificate Authorities)

* * *