

УПАТСТВО

Како да започнам со користење на G3 сертификат издаден од КИБС на

PKI токен?

Верзија: 5.0

Датум: 26.03.2025

103.18

КИБС АД Скопје

©2025 КИБС АД Скопје, сите права задржани

<http://www.kibstrust.com/>

Содржина

1. Намена.....	1
2. Како да инсталирам посреднички софтвер за користење на PKI токен?.....	1
2.1 Вовед.....	1
2.2 Инсталација на посреднички софтвер на Windows оперативен систем	2
3. Проверка на содржина на PKI токен.....	5
4. Промена на кориснички PIN	8
5. Дали сертификатот од мојот PKI токен се прикажува во Google Chrome?.....	8
5.1 Проверка дали сертификатот се прикажува во Google Chrome.....	8
5.2 Како да инсталирам коренски сертификати во Google Chrome?	10
6. Дали сертификатот од мојот PKI токен се прикажува во Mozilla Firefox?.....	11
6.1 Додавање на PKI токен како сигурносен уред.....	11
6.2 Проверка дали сертификатот се прикажува во Mozilla Firefox	14
6.3 Како да инсталирам коренски сертификати во Mozilla Firefox?	16

1. Намена

Ова упатство е наменето за корисниците на квалификувани сертификати од генерација 3 (G3) за креирање на квалификуван електронски потпис: **Verba Sign PKI token** и **Verba Sign Pro PKI token**, како и за квалификуван електронски печат **Verba Seal PKI token**.

Во некоја од локалните регистрациони канцеларии (ЛРК), во регистрационата канцеларија (РК), или кај Застапник на Издавачот на сертификати КИБС (КИБС ИС), сертификатот од генерација **G3** е инсталиран на PKI токен, во присуство на корисникот, со помош на софтвер за безбедно управување со сертификати.

Овој софтвер гарантира дека приватниот клуч е сместен единствено на PKI токенот кој се предава на корисникот.

Корисниците во ЛРК/РК/Застапник го добиваат PKI токенот со веќе инсталиран сертификат, а PIN-от за пристап го добиваат на својата e-mail адреса.

Корисникот само треба да инсталира посреднички софтвер на компјутерот каде ќе го користи PKI токенот.

Дефиниции:

РК = регистрационата канцеларија

ЛРК = локална регистрационата канцеларија

Застапник = локална регистрационата канцеларија со помал обем

QSCD = квалификувано средство за електронски потпис.

PKI токен е заедничко име за токен на кој е издаден сертификатот:

- Gemalto IDPrime MD 840 PKI токен (QSCD);
- Gemalto IDPrime MD 940 PKI токен (QSCD);
- SafeNet 5110 (QSCD).

Листата на модели на PKI токен не е конечна, таа ќе се менува согласно условите на пазарот.

За сите овие типови на токени се користи ист софтвер за поддршка.

2. Како да инсталирам посреднички софтвер за користење на PKI токен?

2.1 Вовед

За да започнете со користење на сертификатот издаден на PKI токен, потребно е да го инсталирате специјално креираниот посреднички софтвер **SafeNet Authentication client (SAC Client)**.

Пред да започнете со инсталација на посредничкиот софтвер, потребно е да ги преземете следните чекори:

1. Отстранете ги сите токени од USB портите на вашиот компјутер;
2. Деинсталирајте го IDGo800 Minidriver и PKCS11 библиотеката, доколку веќе биле инсталирани (или постари верзии на драјвери);
3. Деинсталирајте го SafeNet Authentication Client (SAC Client), доколку имате инсталирано;

4. Рестартирајте го компјутерот;
5. Инсталирајте го SafeNet Authentication Client (SAC Client), според постапката опишана во продолжение;
6. Рестартирајте го компјутерот.

Посредничкиот софтвер (**SafeNet Authentication Client**) можете да го преземете од линковите:

За x86-based PC, за 32-битен оперативен систем:

<https://www.kibstrust.mk/Storage/Support/Software/KIBSTrust-SAC-x32-10.9-R1.msi>

За x64-based PC, за 64-битен оперативен систем:

<https://www.kibstrust.mk/Storage/Support/Software/KIBSTrust-SAC-x64-10.9-R1.msi>

Забелешка:

Овој пакет ја заменува потребата да се инсталираат посебно минидрајвер и PKCS11 библиотека. Заради поддршка на некои кориснички апликации (како на пример некои апликации од УЈП), овие постари посреднички софтвери сеуште може да се најдат на нашиот веб портал: <https://www.kibstrust.com/softver-drajveri.nspix> :

1. Постарите верзии на минидрајвери, можете да ги преземете од секцијата **Софтвер и драјвери**, делот “Минидрајвери за Gemalto IDPrime (.NET и MD) PKI токени”
2. Постарите верзии на PKCS11 библиотеката, можете да ја преземете од секцијата **Софтвер и драјвери**, делот “PKCS#11 Библиотеки за Gemalto ID Prime (.NET и MD) PKI токени” .

За да изберете соодветна верзија на посреднички софтвер, проверете ја верзијата на вашиот оперативниот систем (32 или 64-битен), со кликување на Start->Programs->Accessories->System Tools->System Information.

Во делот **OS name**, може да се исчита верзијата на оперативниот систем.

Во делот System Type се наоѓа една од следните информации:

- x86-based PC, за 32-битен оперативен систем
- x64-based PC, за 64-битен оперативен систем

Забелешка: Посреднички софтвер за PKI токени за MAC и Linux оперативен систем, може да ги најдете во соодветна секција од <https://www.kibstrust.com/softver-drajveri.nspix>.

Доколку имате дополнителни прашања, испратете меил порака до helpdesk@kibstrust.com.

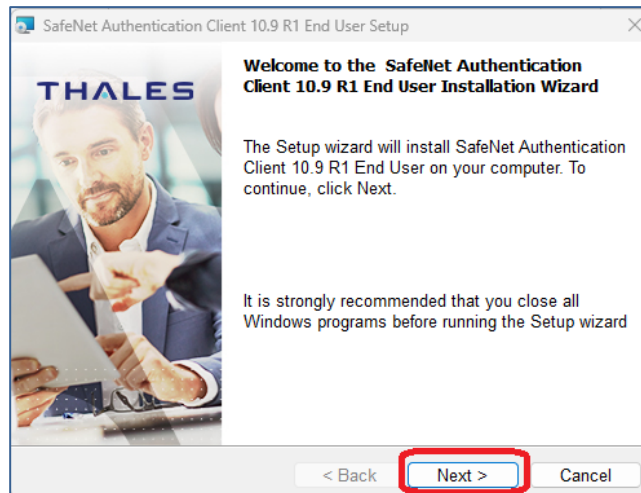
2.2 Инсталација на посреднички софтвер на Windows оперативен систем

Поддржани Windows оперативни системи за **SafeNet Authentication client** верзија 10.9 R1 се:

- Windows 11 (64-bit), Windows 10 (32-bit, 64-bit);
- Windows Server 2022 (64 bit), Windows Server 2019 (64 bit), Windows Server 2016 (64 bit), Windows Server 2012 и 2012 R2 (64-bit).

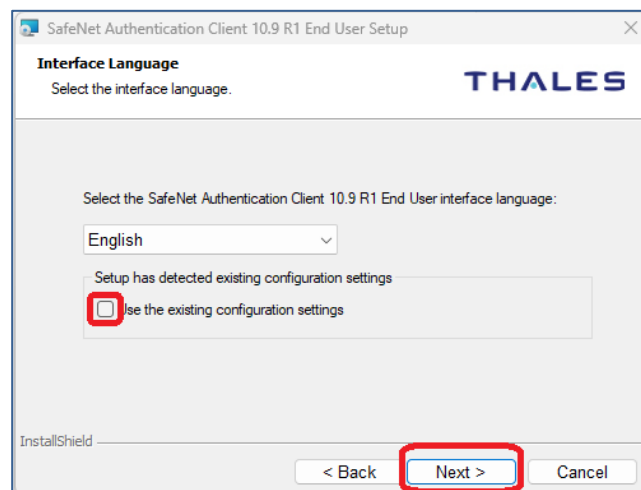
Инсталацијата на софтверот е едноставна, само со следење на екраните и прифаќање на предефинирани вредности. Инсталацијата започнува со двоен клик на соодветниот инсталациски фајл, од локација каде го имате зачувано, при што се отвара прозорец како на Слика 1. Одберете го копчето **Next**.

103.18 Како да започнам со користење на G3 сертификат издаден од КИБС на PKI токен? в.5.0



Слика 1

На следниот прозорец го оставате пред дефинираниот јазик – English, не го селектирајте “Use the existing configuration settings”, а потоа одберете **Next** (Слика 2):



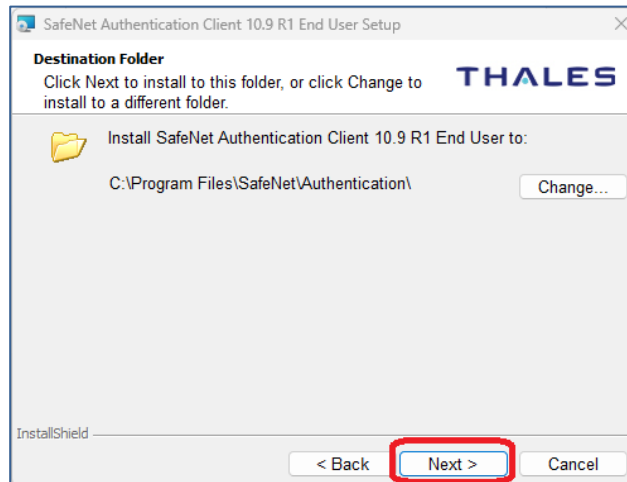
Слика 2

Во следниот чекор, изберете “I accept the terms in the license agreement” (Слика 3) и одберете **Next**:



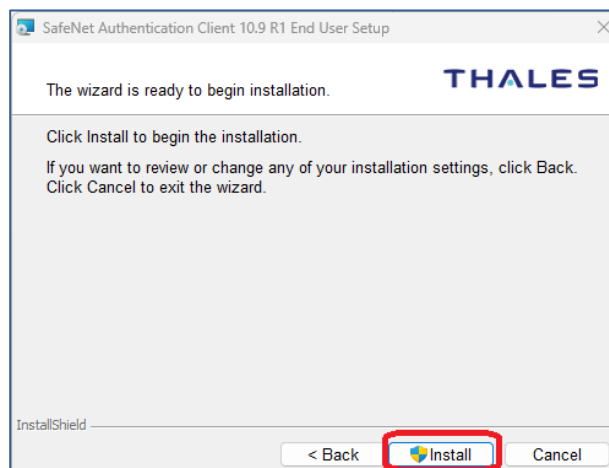
Слика 3

Се појавува прозорец како на Слика 4, во кој треба да ја наведете локацијата каде што ќе биде инсталиран софтверот. Се препорачува да се остави пред дефинираната патека. Потоа, изберете **Next**:



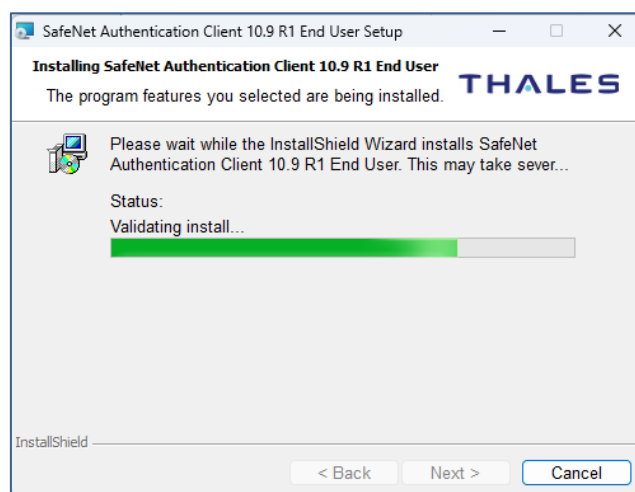
Слика 4

На следниот прозорец, Слика 5, кликнете на копчето **Install**:



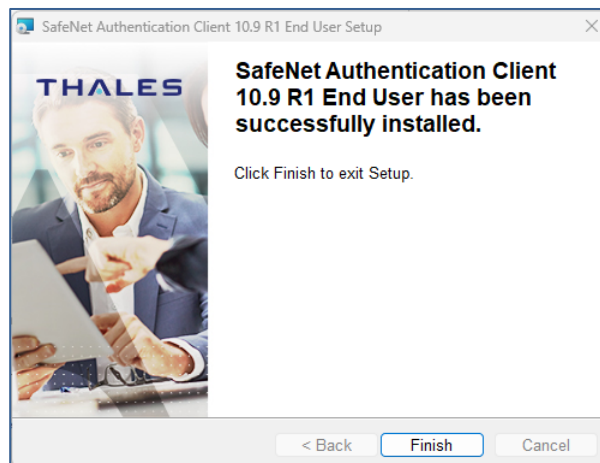
Слика 5

Почекајте додека софтверот се инсталира како на Слика 6:



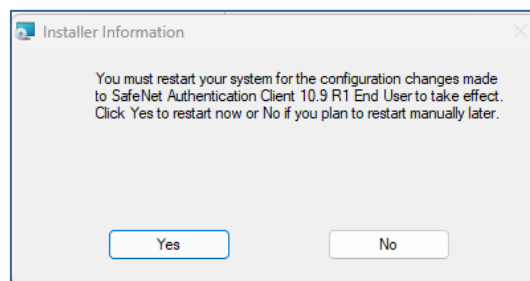
Слика 6

Кога ќе заврши инсталацијата, изберете **Finish** (Слика 7).



Слика 7



Доколку се појави порака како на Слика 8, рестартирајте го компјутерот!



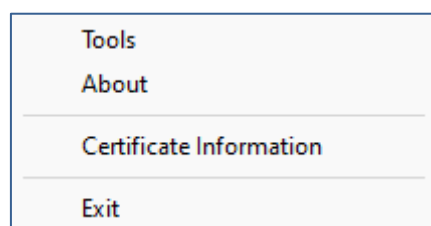
Слика 8

ВАЖНО: Постапка за инсталација на посреднички софтвер опишана во точка 2.2 треба да се повтори соодветно на секој компјутер на којшто сакате да го користите сертификатот на PKI токен.

3. Проверка на содржина на PKI токен

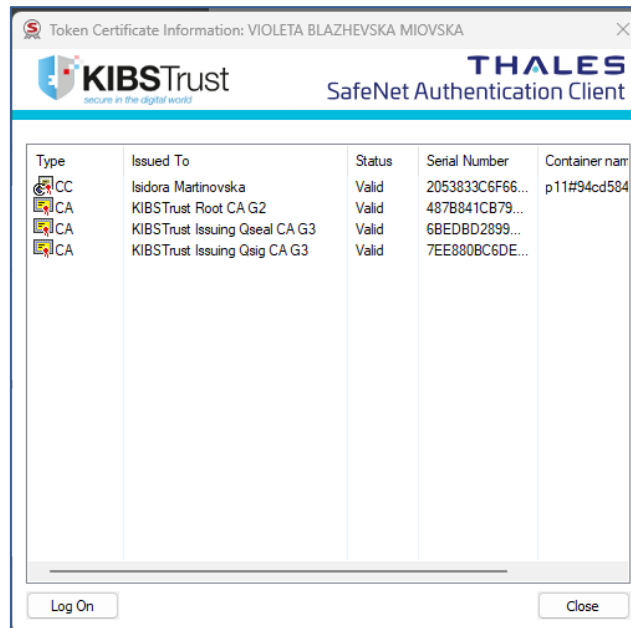
По инсталацијата на SAC посредничкиот софтвер, во долниот десен агол, ќе ја забележите иконата . Кога ќе се приклучи PKI токен на компјутерот, иконата се менува и добива посилна црвена боја: 

Со десен клик на оваа икона, како на Слика 9, може да се видат следните информации за PKI токено:



Слика 9

Доколку изберете „Certificate Information“, ќе добиете приказ како на Слика 10.



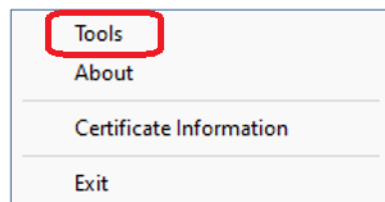
Слика 10

Под тип „CC“, се исчитува сертификатот на корисникот.

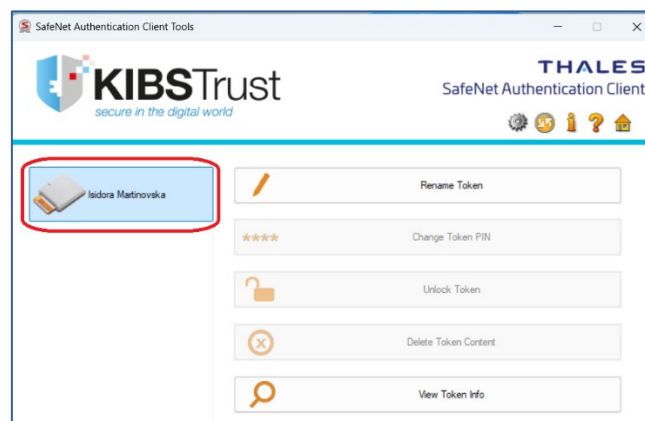
Под тип „CA“, се исчитуваат коренските сертификати на издавачот.

Со двоен клик, може да ги исчитате сертификатите и да ги проверите нивните карактеристики.

Од Слика 9, доколку ја изберете опцијата **Tools** (Слика 11), ќе се отвори прозорец како на Слика 12, на кој од левата страната може да го видите името на PKI токенот.



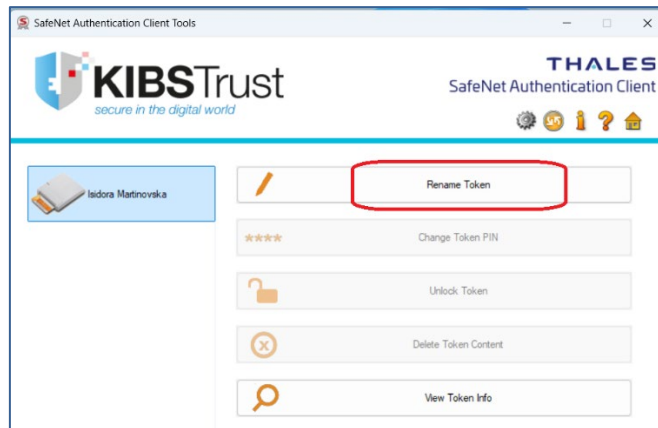
Слика 11



Слика 12

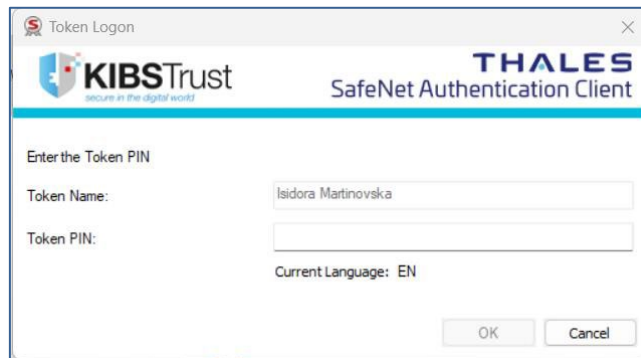
Доколку сакате да го промените името на PKI токенот, изберете **Rename Token** (Слика 13):

103.18 Како да започнам со користење на G3 сертификат издаден од КИБС на PKI токен? в.5.0



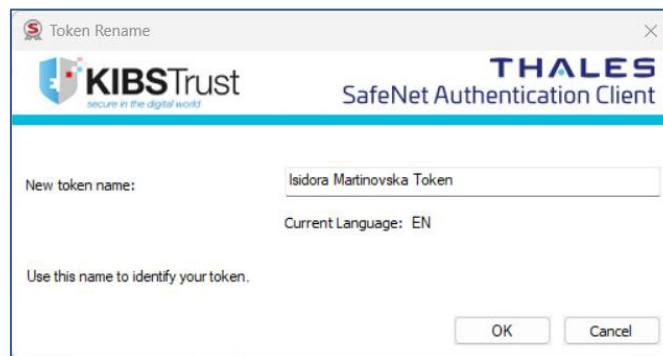
Слика 13

Во наредниот прозорец, внесете го корисничкиот PIN, кој е испратен на вашата e-mail адреса (Слика 14):



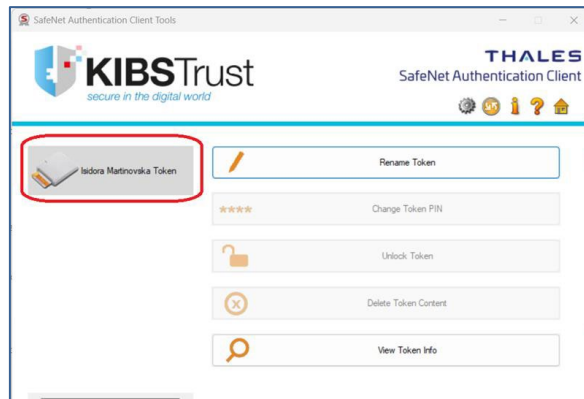
Слика 14

Потоа внесете го новото име на PKI токенот и кликнете ОК (Слика 15):



Слика 15

По направената промена, ќе го забележите новото име на PKI токенот (Слика 16):



Слика 16

4. Промена на кориснички PIN

Корисниците го добиваат PIN-от за пристап на својата е-mail адреса.

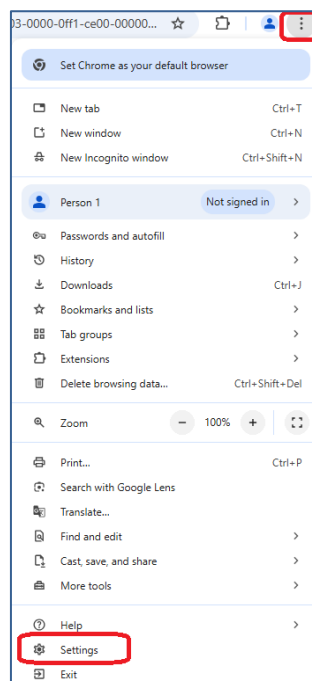
Доколку сакате да го промените корисничкиот PIN на вашиот PKI токен, ве молиме обратете се во РК/ЛРК/Застапник на Издавачот на сертификати КИБС или пишете е-mail порака на адресата: helpdesk@kibstrust.com.

5. Дали сертификатот од мојот PKI токен се прикажува во Google Chrome?

5.1 Проверка дали сертификатот се прикажува во Google Chrome

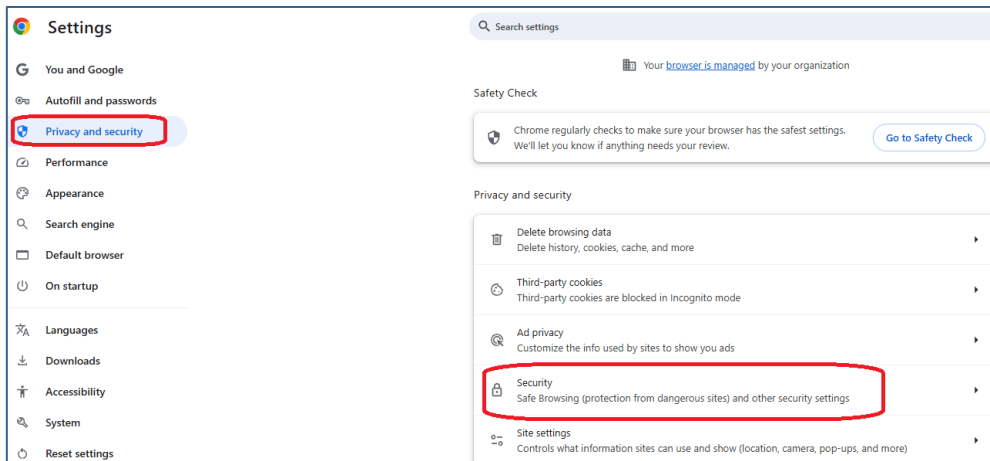
PKI токенот треба да биде приклучен во компјутерот каде што е инсталиран посредничкиот софтвер, согласно точка 2.2 од ова упатство.

Отворете го прелистувачот Google Chrome и одберете **Settings** (Слика 17):



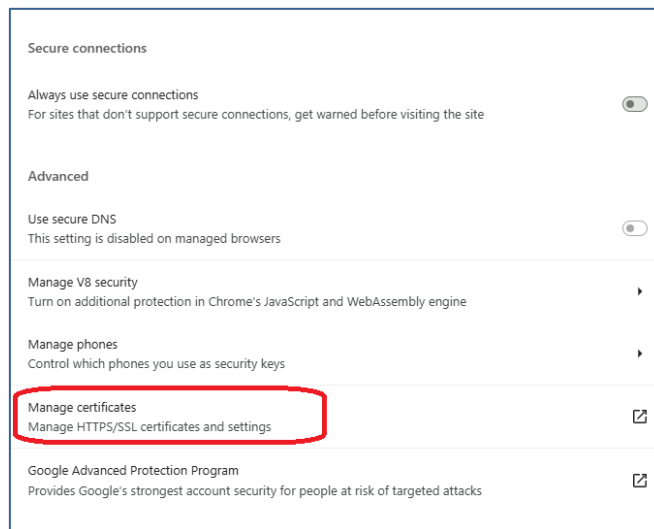
Слика 17

Од менито **Privacy and Security**, одберете **Security** (Слика 18):



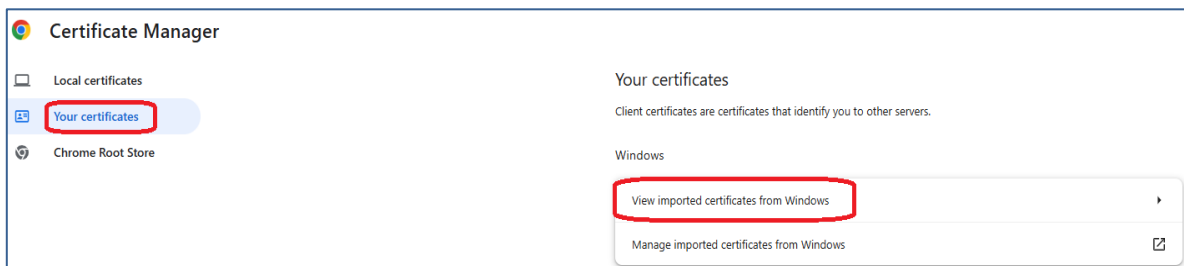
Слика 18

Во следниот прозорец, одберете **Manage certificates** (Слика 19):

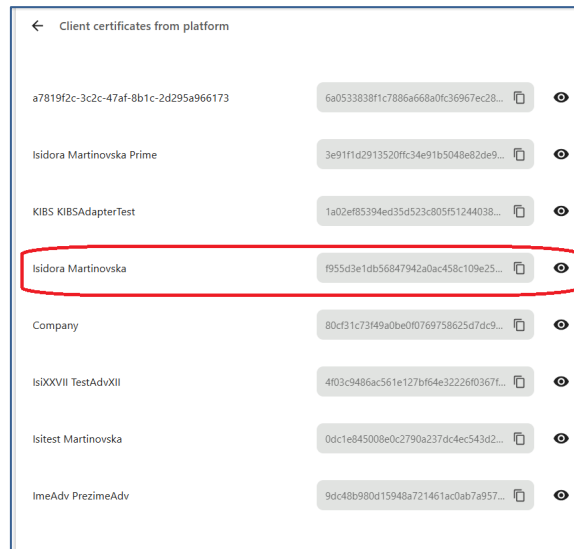


Слика 19

Од **Your certificates** ако одберете **View Imported Certificates from Windows** (Слика 20) може да ја видите листата на сертификати од Windows Certificate Store на вашиот компјутер, а во листата се гледа сертификатот од РКІ токентот (Слика 21):



Слика 20



Слика 21

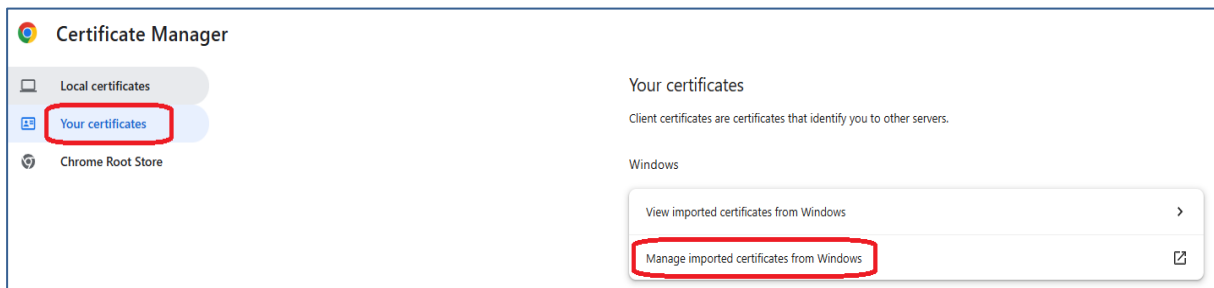
5.2 Како да инсталирам коренски сертификати во Google Chrome?

Коренските сертификати на издавачот KIBSTrust можете да ги преземете од секцијата **Коренски сертификати** од следниот линк: <https://www.kibstrust.com/mk-MK/Home/Support/>.

- Доколку вашиот сертификат е издаден од генерација G2, преземете ги коренскиот (Root) сертификат KIBSTrust Root CA G2 и издавачките (Issuing) сертификати: KIBSTrust Issuing Qsig CA G2 и KIBSTrust Issuing Qseal CA G2. Датотеките rootg2.crt, CA-qSig-G2.crt и CA-qSeal-G2.crt зачувајте ги локално на вашиот компјутер.
- Доколку вашиот сертификат е издаден од генерација G3, преземете ги коренскиот (Root) сертификат KIBSTrust Root CA G2 и издавачките (Issuing) сертификати: KIBSTrust Issuing Qsig CA G3 и KIBSTrust Issuing Qseal CA G3. Датотеките rootg2.crt, KIBSTrustIssuingQsigCAG3.crt и KIBSTrustIssuingQsealCAG3.crt зачувајте ги локално на вашиот компјутер.

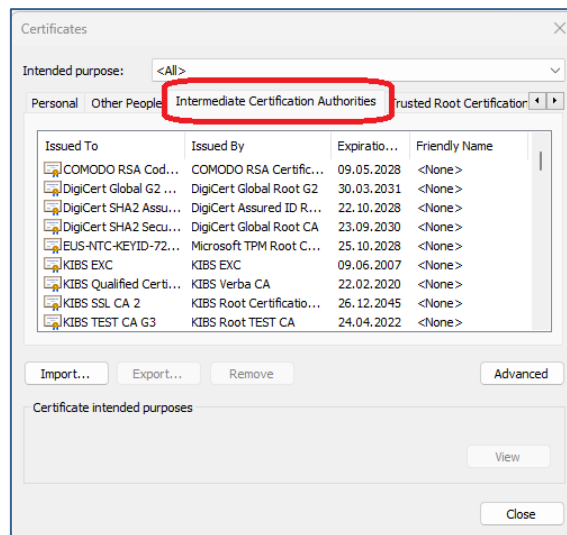
Појаснување: Издавачот на сертификати КИБС од февруари 2025 започна со издавање на сертификати од генерација 3 – G3. Препорака е да ги инсталирате коренските сертификати и од генерација G2 и од генерација G3.

Од менито Your Certificates (Слика 20), изберете ја опцијата **Manage imported certificates from Windows** (Слика 22).



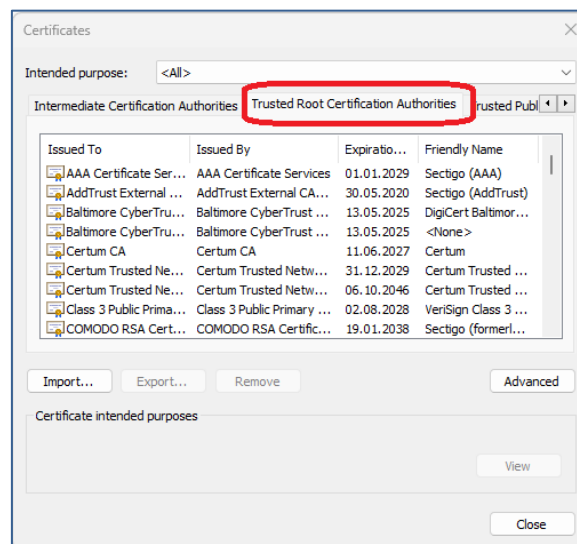
Слика 22

Во прозорецот кој ќе ви се отвори, изберете го табот **Intermediate Certification Authorities** и ќе добиете преглед на додадените издавачки сертификати (Слика 23). Со одбирање на Import, може да додавате нови издавачки сертификати во листата.



Слика 23

Од листата на сертификати во Google Chrome, ако го изберете табот **Trusted Root Certification Authorities**, ќе добиете преглед на додадените коренски сертификати (Слика 24). Со одбирање на Import, може да додавате нови коренски сертификати во листата.



Слика 24

6. Дали сертификатот од мојот PKI token се прикажува во Mozilla Firefox?

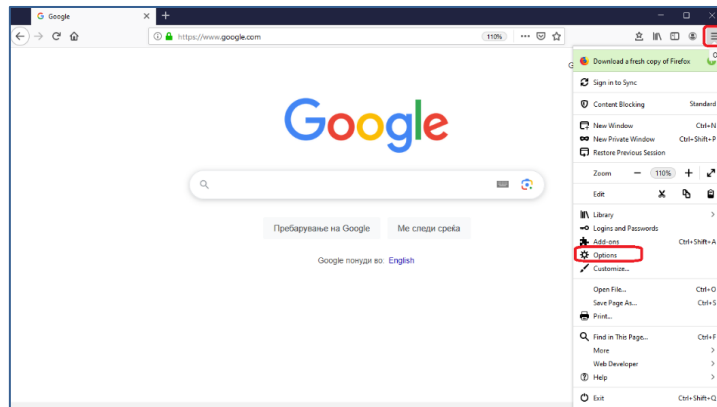
6.1 Додавање на PKI token како сигурносен уред

Во Mozilla Firefox, за да може да пристапите до сертификатот издаден на PKI token, покрај инсталација на посреднички софтвер опишана во Чекор 2.2 од ова упатство, потребно е да се провери дали постои сигурносен уред (зависно од верзијата на Mozilla Firefox).

Во поновите верзии на Mozilla Firefox, со инсталација на посредничкиот софтвер, автоматски се додава сигурносен уред, но доколку користите постара верзија на пребарувачот (пример Mozilla Firefox 68.3.0 esr), потребно е сигурносниот уред да се додаде, според постапката во продолжение:

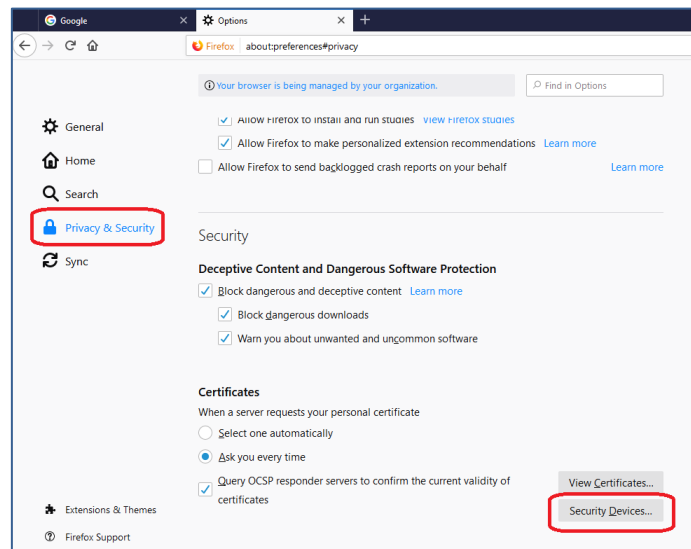
103.18 Како да започнам со користење на G3 сертификат издаден од КИБС на PKI token? в.5.0

Од менито на прелистувачот Mozilla Firefox, во горен десен агол изберете **Options** (Слика 25):



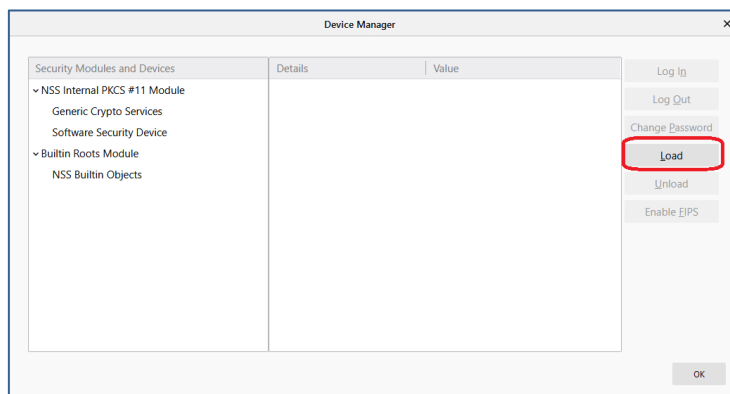
Слика 25

Од менито на левата страна изберете ја опцијата **Privacy & Security**, а потоа изберете **Security Devices** (Слика 26):



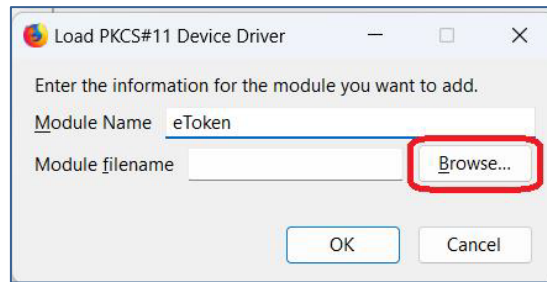
Слика 26

Во следниот прозорец, кликнете на **Load** (Слика 27):



Слика 27

Во новиот прозорец во полето **Module Name** внесете „eToken“ и кликнете **Browse** (Слика 28) за да ја најдете потребната датотека.

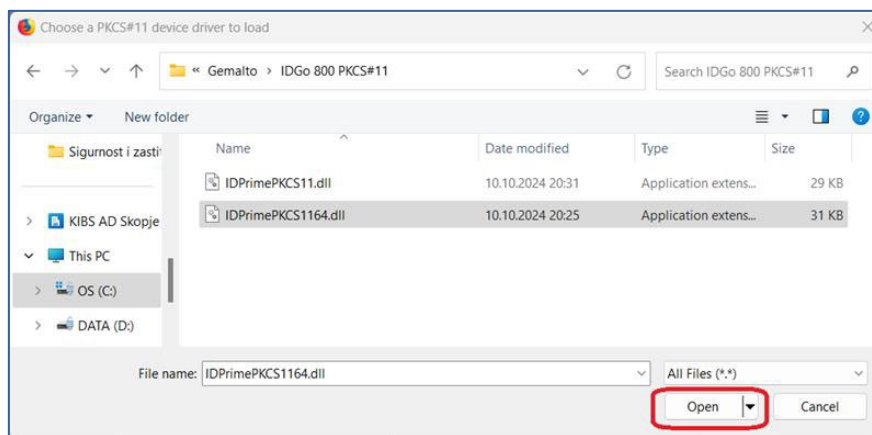


Слика 28

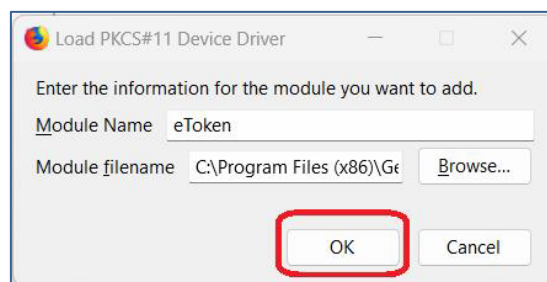
Датотеката се наоѓа на патека:

- C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11 (за 64-битни оперативни системи), или на
- C:\Program Files\Gemalto\IDGo 800 PKCS#11 (за 32-битни оперативни системи).

Селектирајте ја датотеката **IDPrimePKCS11.dll** за 32-битна верзија на Mozilla Firefox (или IDPrimePKCS1164.dll за 64-битна верзија на Mozilla Firefox) и кликнете **Open** (Слика 29), а потоа кликнете **OK** (Слика 30).

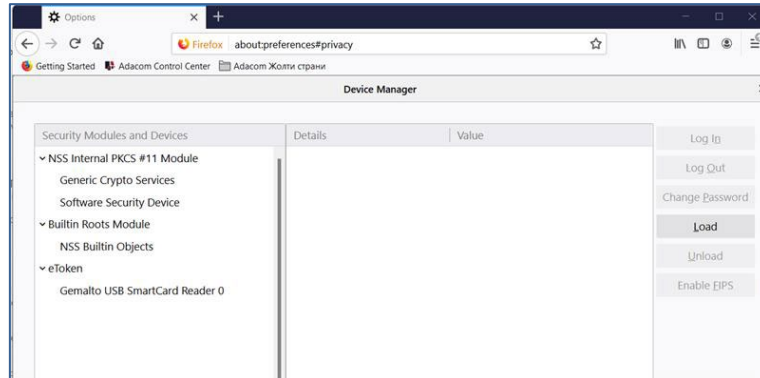


Слика 29



Слика 30

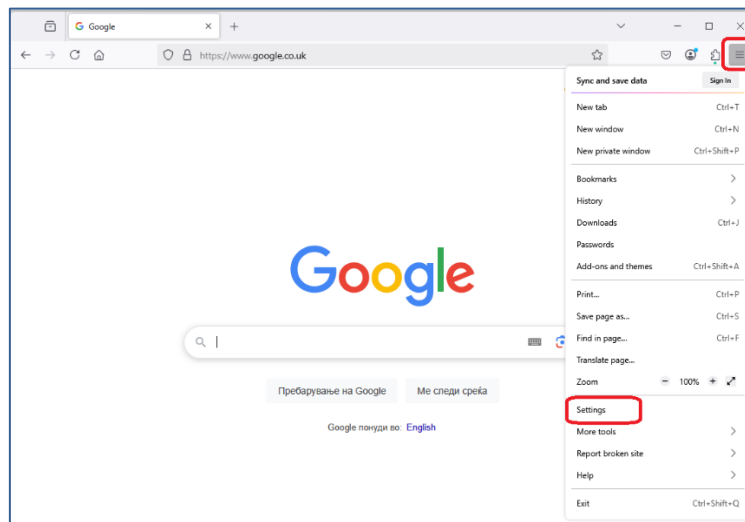
Вашиот PKI токен сега е додаден како сигурносен уред и се појавува во листата од левата страна на прозорецот (Слика 31):



Слика 31

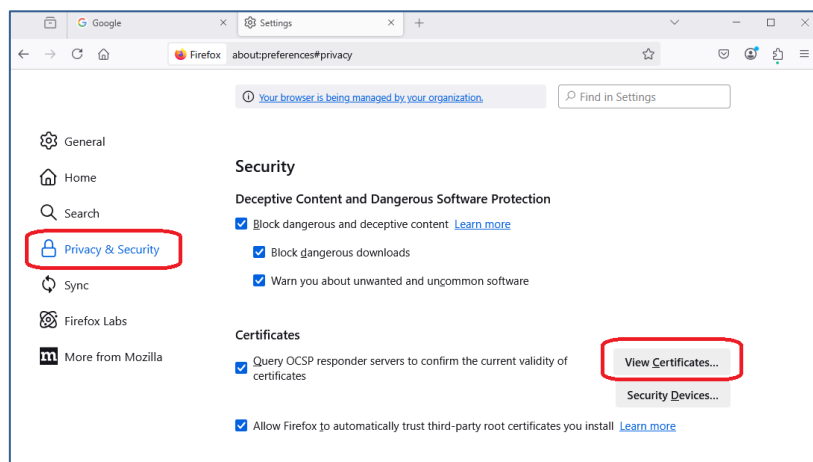
6.2 Проверка дали сертификатот се прикажува во Mozilla Firefox

Приклучете го PKI tokenот во компјутерот и отворете го интернет пребарувачот Mozilla Firefox. Од менито во горниот десен агол изберете **Settings**, како на Слика 32:



Слика 32

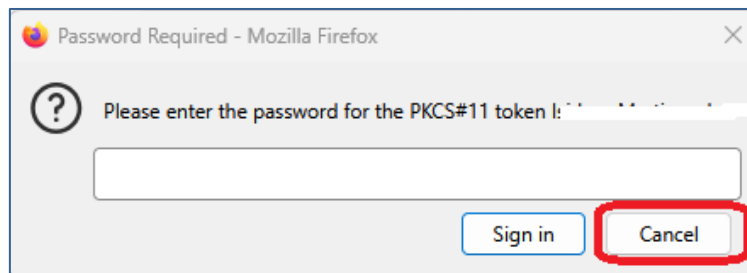
Од менито на левата страна изберете ја опцијата **Privacy & Security**, а потоа копчето **View certificates**, како на Слика 33:



Слика 33

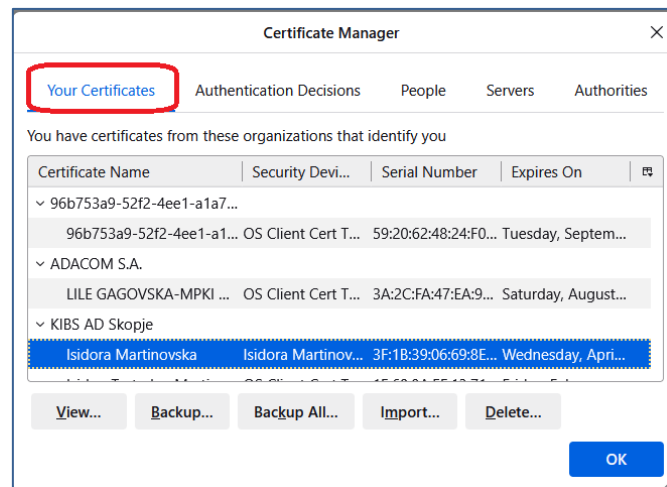
103.18 Како да започнам со користење на G3 сертификат издаден од КИБС на PKI token? в.5.0

Во прозорецот за внесување лозинка (Слика 34) **не внесувајте ништо**, само кликнете на Cancel:



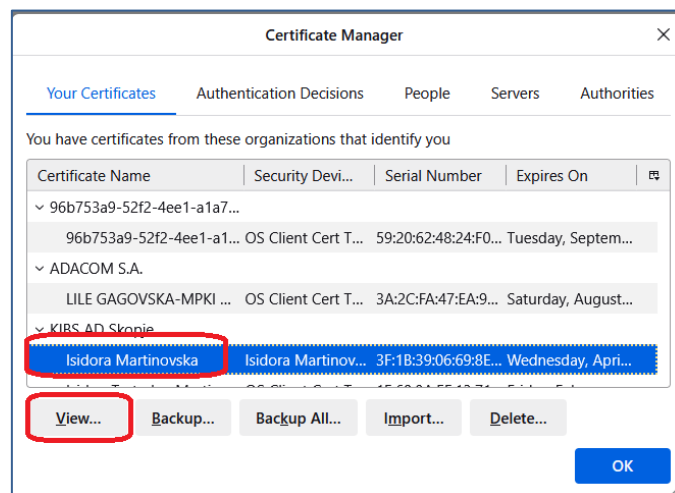
Слика 34

Ќе добиете прозорец како на Слика 35, каде во табот **Your certificates** се прикажува листата на инсталирани сертификати.



Слика 35

Доколку одберете сертификат од листата и го изберете копчето **View** (Слика 36), ќе ги видите карактеристиките за избраниот сертификат (Слика 37).



Слика 36

Certificate	
Isidora Martinovska	KIBSTrust Issuing Qsig CA G2
KIBSTrust Root CA G2	
Subject Name	
Country	MK
Serial Number	226152
	Martinovska
	Isidora
Common Name	Isidora Martinovska
Issuer Name	
Country	MK
Organization	KIBS AD Skopje
Organizational Unit	KIBSTrust Services
	NTRMK-5529581
Common Name	KIBSTrust Issuing Qsig CA G2
Validity	
Not Before	Tue, 16 Apr 2024 10:38:07 GMT
Not After	Wed, 16 Apr 2025 10:38:06 GMT
Subject Alt Names	
Email Address	isidora.martinovska@kibs.mk
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	D5:8B:AC:46:87:A8:3C:C4:0E:6C:BA:79:CC:CA:6F:55:8C:67:67:C3:86:28:8B:D7:69...

Слика 37

6.3 Како да инсталирам коренски сертификати во Mozilla Firefox?

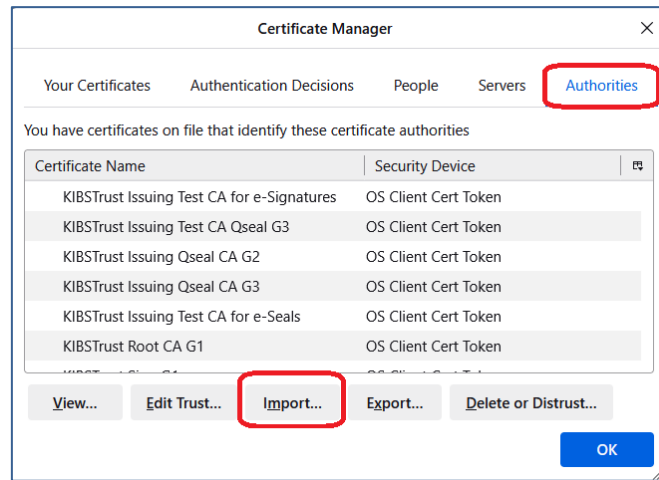
Коренските сертификати на издавачот KIBSTrust можете да ги преземете од секцијата **Коренски сертификати** од следниот линк: <https://www.kibstrust.com/mk-MK/Home/Support/>.

- Доколку вашиот сертификат е издаден од генерација G2, преземете ги коренскиот (Root) сертификат [KIBSTrust Root CA G2](#) и издавачките (Issuing) сертификати: [KIBSTrust Issuing Qsig CA G2](#) и [KIBSTrust Issuing Qseal CA G2](#). Датотеките rootg2.crt, CA-qSig-G2.crt и CA-qSeal-G2.crt зачувајте ги локално на вашиот компјутер.
- Доколку вашиот сертификат е издаден од генерација G3, преземете ги коренскиот (Root) сертификат [KIBSTrust Root CA G2](#) и издавачките (Issuing) сертификати: [KIBSTrust Issuing Qsig CA G3](#) и [KIBSTrust Issuing Qseal CA G3](#). Датотеките rootg2.crt, KIBSTrustIssuingQsigCAG3.crt и KIBSTrustIssuingQsealCAG3.crt зачувајте ги локално на вашиот компјутер.

Појаснување: Издавачот на сертификати КИБС од февруари 2025 започна со издавање на сертификати од генерација 3 – G3. Препорака е да ги инсталирате коренските сертификати и од генерација G2 и од генерација G3.

Во пребарувачот Mozilla Firefox, во **Certificate Manager**, во табот **Authorities**, со кликување на копчето **Import** може да ги додадете коренските сертификати, преземени од горенаведените линкови (Слика 38):

103.18 Како да започнам со користење на G3 сертификат издаден од КИБС на PKI токен? в.5.0



Слика 38

Постапката за инсталација на коренски сертификати подетално е опишана во следното упатство: [Како да инсталирам коренски сертификати?](#)

* * *