

упатство

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

РКІ токен?

Верзија: 5.0 Датум: 26.03.2025 103.18

КИБС АД Скопје ©2025 КИБС АД Скопје, сите права задржани <u>http://www.kibstrust.com/</u>

Содржина

1.	Наме	на	1
2.	Како да инсталирам посреднички софтвер за користење на РКІ токен?		
	2.1	Вовед	
	2.2	Инсталација на посреднички софтвер на Windows оперативен систем	2
3.	Пров	ерка на содржина на РКІ токен	5
4.	Пром	ена 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 РКІ токен се прикажува во Mozilla Firefox?	11
	6.1	Додавање на РКІ 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 РКІ 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 РКІ токенот со веќе инсталиран сертификат, а PINот за пристап го добиваат на својата e-mail адреса.

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

<u>Дефиниции:</u>

РК = регистрационата канцеларија

ЛРК = локална регистрационата канцеларија

Застапник = локална регистрационата канцеларија со помал обем

QSCD = квалификувано средство за електронски потпис.

РКІ 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 РКІ 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 РКІ 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 3a x64-based PC, за 64-битен оперативен систем: https://www.kibstrust.mk/Storage/Support/Software/KIBSTrust-SAC-x64-10.9-R1.msi 2aбаланииа:

<u>Забелешка:</u>

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

- 1. Постарите верзии на минидрајвери, можете да ги преземете од секцијата Софтвер и драјвери, делот "Минидрајвери за Gemalto IDPrime (.NET и MD) РКІ токени"
- 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 кликнување 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 РКІ токени за МАС и Linux оперативен систем, може да ги најдете во соодветна секција од <u>https://www.kibstrust.com/softver-drajveri.nspx</u>.

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**.





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

SafeNet Authentication Client 10.9 R1 End User Se	tup X
Interface Language Select the interface language.	THALES
Select the SafeNet Authentication Client 10.9 R1	End User interface language:
English ~	
Setup has detected existing configuration setting	IS
InstallShield	
< Back	Next > Cancel



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

HALES							
SafeNet Authentication Client							
Legal notice:							
Thales software is not sold; rather, copies of Thales software are licensed all the way through the distribution channel to the end user. UNLESS YOU HAVE ANOTHER AGREEMENT DIRECTLY WITH THALES THAT CONTROLS AND ALTERS YOUR USE OR DISTRIBUTION OF THE THALES SOFTWARE. THE							
I accept the license agreement							

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**:

🛃 SafeNet	Authentication Client 10.9 R1 End User Setup	×				
Destinati Click N install t	on Folder ext to install to this folder, or click Change to o a different folder.	THALES				
	Install SafeNet Authentication Client 10.9 R1 End User to:					
-	C:\Program Files\SafeNet\Authentication\	Change				
InstallShield -	< Back	lext > Cancel				

Слика 4

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

SafeNet Authentication Client 10.9 R1 End User Setup	×					
The wizard is ready to begin installation.	THALES					
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.						
InstallShield Sack	Install					



Почекајте додека софтверот се инсталира како на Слика 6:

💿 SafeNet	Authentication Client 10.9 R1 End User Setup - 🛛 🗙				
Installing The pro	SafeNet Authentication Client 10.9 R1 End User ogram features you selected are being installed.				
Please wait while the InstallShield Wizard installs SafeNet Authentication Client 10.9 R1 End User. This may take sever					
	Status: Validating install				
InstallShield –	< Back Next > Cancel				

Слика 6



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



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

Installer Information	×			
You must restart your system for the configuration changes made to SafeNet Authentication Client 10.9 R1 End User to take effect. Click Yes to restart now or No if you plan to restart manually later.				
Yes No				



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 РКІ токен

По инсталацијата на SAC посредничкиот софтвер, во долниот десен агол, ќе ја забележите

иконата . Кога ќе се приклучи РКІ токен на компјутерот, иконата се менува и добива посилна црвена боја: ^(S)

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

Tools About	
Certificate Information	
Exit	

Слика 9

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



Слика 10

Под тип "СС", се исчитува сертификатот на корисникот.

Под тип "СА", 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 РКІ токенот.

Tools About)	
Certific	te Informatio	n
Exit		



SafeNet Authentication Client Tools		- 0 X	
KIBS Trust		THALES SafeNet Authentication Client	
Isidora Martinovska	/	Rename Token	
**	***	Change Token PIN	
1		Unlock Token	
(×	Delete Token Content	
	Ø	View Token Info	

Слика 12

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





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

×		
THALES SafeNet Authentication Client		
Isidora Martinovska		
Current Language: EN		
OK Cancel		



Потоа внесето го новото име на РКІ токенот и кликнете ОК (Слика 15):



Слика 15

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



Слика 16

4. Промена на кориснички PIN

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

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

5. Дали сертификатот од мојот РКІ 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):

0	Settings	Q. Search settings		
G ®	You and Google Autofill and passwords		Your browser is managed by your organization Check	
0	Privacy and security Performance	0	Chrome regularly checks to make sure your browser has the safest settings. We'll let you know if anything needs your review.	to Safety Check
Ø	Appearance	Privacy	and security	
۹	Search engine	Ū	Delete browsing data	,
	Default browser		Delete history, cookies, cache, and more	
U	On startup	٢	Third-party cookies Third-party cookies are blocked in Incognito mode	,
Ŕ	Languages	R	Ad privacy Customize the infolused by sites to show you ads	,
$\overline{\mathbf{T}}$	Downloads	-		
Ť	Accessibility	₿	Security Safe Browsing (protection from dangerous sites) and other security settings	,
S,	System	0-	Site settings	
ð	Reset settings		Controls what information sites can use and show (location, camera, pop-ups, and more	2)

Слика 18

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

Secure connections	
Always use secure connections For sites that don't support secure connections, get warned before visiting the site	۲
Advanced	
Use secure DNS This setting is disabled on managed browsers	۲
Manage V8 security Turn on additional protection in Chrome's JavaScript and WebAssembly engine	•
Manage phones Control which phones you use as security keys	•
Manage certificates Manage HTTPS/SSL certificates and settings	ß
Google Advanced Protection Program Provides Google's strongest account security for people at risk of targeted attacks	Ľ

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 токенот (Слика 21):

0	Certificate Manager		
	Local certificates	Your certificates	
E	Your certificates	Client certificates are certificates that identify you to other servers.	
0	Chrome Root Store	Windows	
		View imported certificates from Windows	•
		Manage imported certificates from Windows	Ø

Слика 20

← Client certificates from platform	
a7819f2c-3c2c-47af-8b1c-2d295a966173	6a0533838f1c7886a668a0fc36967ec28 📋 💿
Isidora Martinovska Prime	3e91f1d2913520ffc34e91b5048e82de9 📋 💿
KIBS KIBSAdapterTest	1a02ef85394ed35d523c805f51244038 📋 💿
Isidora Martinovska	1955d3e1db56847942a0ac458c109e25 🛅 📀
Company	80cf31c73f49a0be0f0769758625d7dc9 🛅 📀
lsiXXVII TestAdvXII	4f03c9486ac561e127bf64e32226f0367f 🛅 💿
lsitest Martinovska	0dc1e845008e0c2790a237dc4ec543d2 📋 💿
ImeAdv PrezimeAdv	9dc48b980d15948a721461ac0ab7a957 🚺 💿

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: <u>https://www.kibstrust.com/mk-MK/Home/Support/</u>.

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

<u>Појаснување</u>: 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).

0	Certificate Manager		
	Local certificates	Your certificates	
	Your certificates	Client certificates are certificates that identify you to other servers.	
0	Chrome Root Store	Windows	
		View imported certificates from Windows	>
		Manage imported certificates from Windows	ß

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.

Included To	Terrined Du	Evening the	Colonally, Name	
Issued to	Issued by	Expiratio	Friendly Name	
COMODO RSA Cod	COMODO RSA Certific	09.05.2028	<none></none>	
DigiCert Global G2	DigiCert Global Root G2	30.03.2031	<none></none>	
DigiCert SHA2 Assu	DigiCert Assured ID R	22.10.2028	<none></none>	
DigiCert SHA2 Secu	Digicert Global Root CA	23.09.2030	<inone></inone>	
WEUS-INI C-KEYID-72	MICROSOTE IPM ROOT C	25.10.2028	<ivone></ivone>	
	KIDS EXC	22.02.2007		
	KIBS Poot Certificatio	22.02.2020		
KIBS TEST CA G3	KIBS Root TEST CA	24.04.2022	<none></none>	
mport Export	Remove			Advance

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.

Issu	ed By	Expiratio	Friendly	Name
e Ser AAA	Certificate Servi	tes 01.01.20	29 Sectigo	(AAA)
rnal Add	Trust External CA	30.05.20	20 Sectigo	(AddTrust)
erTru Balti	more CyberTrust	13.05.20	25 DigiCert	Baltimor
erTru Balti	more CyberTrust	13.05.20	25 <none:< td=""><td>•</td></none:<>	•
Cert	tum CA	11.06.20	27 Certum	
d Ne Cert	um Trusted Netw	31.12.20	29 Certum	Trusted
d Ne Cert	um Trusted Netw	06.10.20	46 Certum	Trusted
rima Clas	s 3 Public Primary	02.08.20	28 VeriSign	Class 3
Cert COM	IODO RSA Certini	19.01.20	38 Sectigo	(tormeri
	-			
xport	Remove			Advance
purposes				
	Issu e Ser AAA rnal Add erTru Balti Cert d Ne Cert d Ne Cert d Ne Clas Cert CON	Issued By E Ser AAA Certificate Servir mal AAA Certificate Servir mal AddTust External CA "Tru Baltimore CyberTrust Certum CA d Ne Certum Trusted Netw hma Class 3 Public Primary Cert COMODO RSA Certifi purpose	Issued By Expiratio E Ser AAA Certificate Services 01.01.20 rmal AAA Certificate Services 01.01.20 rmal AddTust External CA 30.05.20 rTru Baltimore CyberTrust 13.05.20 rTru Baltimore CyberTrust 13.05.20 certum CA 11.06.20 d Ne Certum Trusted Netw 06.10.20 rma Class 3 Public Primary 02.08.20 Cert COMODO RSA Certific 19.01.20 xport Remove	Issued By Expiratio Friendly E Ser AAA Certificate Services 01.01.2029 Sectigo rmal AddTrust External CA 30.05.2020 Sectigo Tru Baltimore CyberTrust 13.05.2025 DigiCert stru Baltimore CyberTrust 13.05.2025 Certum d Ne Certum Trusted Netw 01.10.6.2029 Certum d Ne Certum Trusted Netw 01.10.6.2029 Certum d Ne Certum Trusted Netw 01.06.2029 Certum d Ne Certum Trusted Netw 02.08.2029 Certum d Ne Certum Trusted Netw 02.08.2028 VerSign Cert COMODO RSA Certific 19.01.2038 Sectigo xport Remove



6. Дали сертификатот од мојот РКІ токен се прикажува во Mozilla Firefox?

6.1 Додавање на РКІ токен како сигурносен уред

Во Mozilla Firefox, за да може да пристапите до сертификатот издаден на PKI токен, 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:

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





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

G Google ×	A Options X +
← → ♂ ŵ	€) Firefox about:preferences#privacy
	${f O}$ Your browser is being managed by your organization. ${\cal P}$ Find in Options
🔅 General	Allow Firefox to install and run studies view Firefox studies Allow Firefox to make personalized extension recommendations Learn more
Home Home	Allow Firefox to send backlogged crash reports on your behalf
Q Search	
Privacy & Security	Security
🛱 Sync	Deceptive Content and Dangerous Software Protection
	Block dangerous and deceptive content Learn more
	✓ Block dangerous downloads
	✓ Warn you about unwanted and un <u>c</u> ommon 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 View Certificates
Extensions & Themes	certificates Security <u>D</u> evices
Tirefox Support	

Слика 26

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

	Device M	anager	×
Security Modules and Devices	Details	Value	Log I <u>n</u>
 NSS Internal PKCS #11 Module 			Log Out
Generic Crypto Services			
Software Security Device			Change Password
✓ Builtin Roots Module			Load
NSS Builtin Objects			<u>U</u> nload
			Enable <u>F</u> IPS
			ОК



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

Enter the information for the	module you war	nt to add.
Module Name eToken		
Module <u>f</u> ilename		Browse

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).

$\leftrightarrow \rightarrow \checkmark \uparrow$	≪ Gemalto → IDGo 800 PKCS#11	~ C	Search IDGo 800 PKCS#11				
Organize • New folde	er		≣ •				
🚞 Sigurnost i zasti	Name	Date modified	Type Size				
	IDPrimePKCS11.dll	10.10.2024 20:31	Application extens	29 KB			
KIBS AD Skopje	IDPrimePKCS1164.dll	10.10.2024 20:25	Application extens	31 KB			
This PC							
> \$ 05(C)							
DAIA (D.)							
	IDD-im-DKCC11C1-dll		All Files (# #)				

Слика 29



Слика 30

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

→ C ⁴ ⁽²⁾	Sirefox abou	t:preferences#privacy		습	
Setting Started 🚯 Adacom	Control Center 🗎 Adaco	от Жолти страни			
		Device Ma	inager		
Security Modules and I	Devices	Details	Value		Log In
 NSS Internal PKCS #1 	1 Module	1			Log Out
Generic Crypto Services					Change Password
 Builtin Roots Module 	Device				Load
NSS Builtin Objects					Unland
∽ eToken					Qhioad
Gemalto USB Smar	tCard Reader 0				Enable EIPS

Слика 31

6.2 Проверка дали сертификатот се прикажува во Mozilla Firefox

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

	ē	G Google		×	+									\sim		-		×
←	\rightarrow	C D	08	https	://www.g	google.c	.co.uk						ź	2	\bigtriangledown	٢	Ŷ	
													Sync	and save date	•		Sign	In
													New t	ab			Ct	rl+T
													News	window			Cti	rl+N
													Newp	private windo	w	0	trl+Shi	ft+P
													Book	marks				>
													Histor	У				>
													Down	loads			C	trl+J
													Passw	ords				
								5				2	Add-o	ons and them	es	C	trl+Shit	ft+A
											9"		Print.				Ct	rl+P
													Save	page as			Ct	rl+S
				Q									 Find i	n page			Ct	trl+F
													Transl	ate page				
						П	lpeðap	руван	ье на Goog	lle	Ме след	и среќа	Zoom		-	100%	+	2
													Settin	gs				
								0	Google пону	ди во:	English		More	tools				>
													Repor	t broken site				>
													Help					>
													Exit			Ct	rl+Shif	ft+Q
													 -					



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

		-	G	Google	×	🔞 Settings	×	+		\sim		-		×
¢	-	\rightarrow	C		😫 Firefox	about:preferences#privacy				☆	\bigtriangledown	٢	సి	=
						① Your browser is being many	i <u>ged by</u>	your organization.		ings				
	;	ŝ	Gen	eral										
	1	ጔ	Hon	ne		Security								
	,	0	Saar	ch		Deceptive Content and	Dange	erous Software Protection						
L	_	~	Jeal	u	-	Block dangerous and de	ceptive	e content Learn more						
	Ŀ	8	Priva	acy & Security	J	Block dangerous dov	vnload	s						
		Φ	Syno	:		🗹 Warn you about unw	anted	and uncommon software						
	8	<u></u>	Fire	ox Labs		Certificates			_		_			
	More from Mozilla					Query OCSP responder servers to confirm the current validity of certificates Security <u>Devices</u>								
	Allow Firefox to automatically trust third-party root certificates you install Learn more													

Слика 33

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.

Certificate Manager								
Your Certifica	ates Auther	ntication Decisions	People	Servers	Authorities			
You have certifi	cates from these	organizations that	identify you					
Certificate Na	me	Security Devi	Serial Number	Expires	On 🛛 🛤			
~ 96b753a9-5	2f2-4ee1-a1a7							
96b753a9-52f2-4ee1-a1 OS Client Cert T 59:20:62:48:24:F0 Tuesday, Se								
~ ADACOM S.	A.							
LILE GAG	ovska-mpki	OS Client Cert T	3A:2C:FA:47:EA:9	9 Saturday,	August			
~ KIBS AD Sko	pje							
lsidora M	artinovska	lsidora Martinov	3F:1B:39:06:69:8	E Wednesd	lay, Apri			
<u>V</u> iew	<u>B</u> ackup	Bac <u>k</u> up All	I <u>m</u> port	Delete				
					ОК			



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

		Certificate Mar	ager		>
Your Certifica	ates Authe	ntication Decisions	People	Servers	Authorities
You have certific	ates from these	e organizations that	identify you		
Certificate Nar	ne	Security Devi	Serial Number	Expires	On I¤
~ 96b753a9-52	2f2-4ee1-a1a7				
96b753a9	-52f2-4ee1-a1	. OS Client Cert T	59:20:62:48:24:F0) Tuesday,	Septem
~ ADACOM S.A	Α.				
LILE GAGO	ovska-mpki	OS Client Cert T	3A:2C:FA:47:EA:9	Saturday,	August
✓ KIRS AD Sko	nie				
Isidora Ma	artinovska	Isidora Martinov	3F:1B:39:06:69:8I	E Wednesd	ay, Apri
<u>V</u> iew	<u>B</u> ackup	Backup All	I <u>m</u> port	Delete	
					ОК

Слика 36

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	МК	
Organization	KIBS AD Skopje	
Organizational Unit	KIBSTrust Services	
	NTRMK-5529581	
Common Name	KIBSTrust Issuing Osig 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	D5:88:AC:46:87:A8:3C:C4:0E:6C:BA:79:CC:CA:66	: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: <u>https://www.kibstrust.com/mk-MK/Home/Support/</u>.

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

<u>Појаснување</u>: 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 кликнување 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 РКІ токен? в.5.0

Certificate Manager								
Your Certifica	ates Authent	ication Decisions	People	Servers	Authorities			
You have certifie	cates on file that i	dentify these certi	ficate authorit	ties				
Certificate Na	me		Security De	vice	D			
KIBSTrust	Issuing Test CA fo	r e-Signatures	OS Client Ce	rt Token				
KIBSTrust	Issuing Test CA Q	seal G3	OS Client Cert Token					
KIBSTrust	Issuing Qseal CA	G2	OS Client Cert Token					
KIBSTrust	Issuing Qseal CA	G3	OS Client Cert Token					
KIBSTrust	Issuing Test CA fo	r e-Seals	OS Client Cert Token					
KIBSTrust	Root CA G1		OS Client Cert Token					
<u>V</u> iew	Edit Trust	l <u>m</u> port	E <u>x</u> port	Delete or Di	istrust			
					ОК			

Слика 38

Постапката за инсталација на коренски сертификати подетално е опишана во следното упатство: Како да инсталирам коренски сертификати?

* * *