

УПАТСТВО

Како да започнам со користење на сертификат издаден на Gemalto Java PKI токен?

Version: 4.0 Date: 18.01.2018 103.17

КИБС АД Скопје

© 2018 КИБС АД Скопје, сите права задржани

http://www.kibstrust.mk



Содржина

1.	Намена1
2.	Како да инсталирам софтвер за работа со Gemalto Java токенот?
3.	Како да проверам дали имам сертификат во Gemalto Java PKI токенот?4
4.	Како да инсталирам коренски сертификати?7
5.	Како да го променам корисничкиот ПИН за пристап до Gemalto Java PKI токенот? .10
6.	Како да го деблокирам корисничкиот ПИН?12
7.	Како да овозможам прелистувачот Firefox да го препознае Gemalto Java PKI токенот? 13

1. Намена

Ова упатство е наменето исклучиво за корисниците на Verba Sign K2, Verba Sign K2 и Verba Seal S2 сертификати, кои имаат подигнато сертификат со генериран пар на клучеви на Gemalto Java PKI токен во некоја од локалните регистрациони канцеларии (ЛРК) на Издавачот на сертификати КИБС (КИБС ИС).

Сертификатот е инсталиран на Gemalto Java 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 Gemalto Java PKI токенот кој се предава на корисникот.

Корисникот треба да ги следи чекорите од 2 до 5 дадени во продолжение.

Во случај корисникот да го блокира корисничкиот ПИН се применува постапката од точката 6.

Доколку корисникот сака да го користи сертификатот во интернет прелистувачот Mozilla Firefox потребно е да се направи и постапката од точка 7.

2. Како да инсталирам софтвер за работа со Gemalto Java токенот?

Софтверот за работа со Gemalto Java PKI токен е објавен на веб страница на КИБС ИС, во делот Софтвер и драјвери од: <u>https://www.kibstrust.mk/mk-MK/Home/Support</u>, а е наменет за следните оперативни системи: Microsoft Windows 7 / 8 / 8.1 / 10¹.

Во зависност од типот на оперативниот систем (32 или 64-битен оперативен систем), потребно е да се инсталира соодветниот софтверски пакет. Проверката на типот на оперативен систем се прави на начин опишан во следната постапка:

Кликнете Start->Programs->Accessories->System Tools->System Information. Во делот System Type ја има една од следните информации:

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

За инсталација на софтверот, од локацијата <u>https://www.kibstrust.mk/mk-MK/Home/Support</u>, секција "**Софтвер за работа со Gemalto Java PKI токен**", потребно е да се отвори датотека соодветна за оперативниот систем:

- Windows 32-битни, за 32-битен оперативен систем
- <u>Windows 64-битен</u>, за 64-битен оперативен систем

и на прозорецот што ќе се појави се избира Run (Слика 1).

¹За други оперативни системи контактирајте нѐ преку <u>helpdesk@kibstrust.mk</u>.



Слика 1

(Напомена: Во ова упатство како пример е употребен софтвер Classic Client v.6.1 за 64-битен Windows 7 оперативен систем)

ВАЖНО: За корисниците на Windows 8/8.1 оперативниот систем како предуслов за инсталирање на Gemalto софтверот за Java PKI токен е инсталација на .NET Framework 3.5 кој може да се преземе и_инсталира од локацијата_<u>http://www.microsoft.com/en-us/download/details.aspx?id=22</u>.

Инсталацијата на софтверот за Java PKI Токен, Gemalto Classic Client, започнува со прозорец како на Слика 2, со избирање на копчето **Next**.



Слика 2

Изберете "I accept the terms in the license agreement", а потоа Next (Слика 3):



Слика 3

На следниот прозорец (Слика 4) е наведена локацијата каде што ќе биде инсталиран софтверот.

Се остава пред дефинираната патека, освен ако имате 64-битен оперативен систем и пристапувате до веб страната на УЈП.

ВАЖНО: За корисниците на услугата <u>E-Даноци</u> кои имаат 64-битен оперативниот систем, препорачана локација за инсталација е C:\Gemalto. Пред инсталација информирајте се во УЈП или погледнете ја стр. 15 од упатството на следната локација: <u>https://etax-fl.ujp.gov.mk/includes/setUpBrowser/Upatstvo_za_Okolina.pdf</u>.



Слика 4

На следниот прозорец (Слика 5), се оди на Install:



Слика 5

Кога ќе заврши инсталацијата, се кликнува на Finish (Слика 6)

B Classic Client 6.1 for 64 bits	s - InstallShield Wizard
gemalto	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed Classic Client 6.1 for 64 bits. Click Finish to exit the wizard.
	< Back Einish Cancel

Слика 6

На прашањето "Дали сакате да се рестартира вашиот компјутер?" (Слика 7), се избира Yes.



Слика 7

Откако компјутерот ќе се рестартира, постапката за инсталација на софтверот Gemalto Classic Client Toolbox за Gemalto Java PKI токен е завршена.

ВАЖНО: Постапка за инсталација на софтвер опишана во точка 2 треба да се повтори на секој компјутер на којшто сакате да го користите Gemalto Java PKI токен.

3. Како да проверам дали имам сертификат во Gemalto Java PKI токенот?

За проверка на содржината на Gemalto Java PKI токен, се вметнува токенот во компјутерот на кој е инсталиран софтвер согласно точка 2 од ова упатство. Кликнете Start -> All Programs ->Gemalto, и активирајте ја апликацијата Classic Client Toolbox.



Слика 8

Во делот Card Contents, се избира Certificates, и се клика на Gemplus USB Key Smart Card Reader. Во делот PIN Code се внесува ПИН– от добиен во електронската порака (e-mail) која КИБС ИС ја праќа откако ќе го одобри издавањето сертификат. Кликнете Login, по што се добива приказ како на Слика 9, на која се прикажани парот од приватен и јавен клуч, како и сертификатот издаден за нив.

Дополнително, на токенот се сместени и коренските сертификати на издавачот КИБС ИС, со следните имиња:

- "KIBS Qualified Certificate Services CA KIBS AD Skopje" и "KIBS Verba CA VeriSign, Inc." доколку Вашиот сертификат е издаден пред 23.02.2016 година.
- "KibsTrust Qualified Certificate Services KibsTrust Certification Authority" и "KibsTrust Certification Authority's VeriSign Class 2 Public Primary Certification Authority – G3" доколку Вашиот сертификат е издаден по 23.02.2016 година.

100100X		0
	Certificates	
Card Contents	1/10	PIN Code: Logout
Certificates		
		FujitsuTechnologySolutions GmbH SmartCase KB SCR eS
a		Ime 14 Prezime 14's KIBS AD Skopje ID'S Ime 14 Prezime
Card Properties		PSA Public Key 2048 bits
oura i ropentea		
		RSA Private Key 2048 bits Status Certification Authority'S VeriSign Class 2 Pi
cura nopelitea		SRA Private Key 2048 bits KibsTrust Certification Authority'S VeriSign Class 2 Pi KibsTrust Qualified Certificate Services'S KibsTrust C
		KibsTrust Qualified Certificate Services'S KibsTrust C
Curd i roponica		RSA Private Key 2048 bits RSA Private Key 2048 bits RKibsTrust Certification Authority'S VeriSign Class 2 Pr KibsTrust Qualified Certificate Services'S KibsTrust C
cura ropentes		KibsTrust Qualified Certificate Services'S KibsTrust C KibsTrust Qualified Certificate Services'S KibsTrust C
cuis ropoties		KibsTrust Certification Authority'S VeriSign Class 2 Pr KibsTrust Qualified Certificate Services'S KibsTrust C
		Sch Private Key 2048 bits Sch Private Key 2048 bits KibsTrust Certification Authority'S VeriSign Class 2 P KibsTrust Qualified Certificate Services'S KibsTrust C Show details Erase Set as default
Card Administration		Show details Erase Set as default Export Erase All Register All

Слика 9

Кликнете во делот **Ime Prezime' S,** а потоа кликнете на Show details. Треба да го добиете приказот од Слика 10, каде се дадени информации за сертификатот.

Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
Proves your identity to a remote computer Protects e-mail messages
• 2.16.840.1.113733.1.7.23.2
Smart Card Logon
* Refer to the certification authority's statement for details.
Issued to: Ime14Prezime14
Issued by: KibsTrust Qualified Certificate Services
Valid from 27. 11. 2015 to 27. 11. 2016
Install Certificate Issuer Statement Learn more about <u>certificates</u>
ОК

Слика 10

Кликнете на делот Certification Path. Можни се 2 (два) прикази:

1. Ако е приказот како на Слика 11, тогаш се продолжува со чекор 5.

Certificate	×
General Details Certification Path Certification path VeriSign Class 2 Public Primary Certification KibsTrust Certification Authority KibsTrust Qualified Certificate Se	ion Authority - G3 ervices
Certificate <u>s</u> tatus: This certificate is OK	View Certificate
Learn more about <u>certification paths</u>	ОК

Слика 11

2. Ако е приказот како на Слика 12 (прикажано е само име и презиме) тогаш **се продолжува** на чекор 4.

Certificate	—
General Details Certification Path	
Certification path	
Ime14 Prezime14	
	View Certificate
Certificate <u>s</u> tatus:	
The issuer of this certificate could not be found.	
Learn more about certification paths	
	ОК

Слика 12

4. Како да инсталирам коренски сертификати?

За функционирање на дигиталниот сертификат, потребно е да се инсталираат коренските сертификати на Издавачот КИБС. За таа цел потребно е да се извршат следните чекори:

- 1. Се активира софтверот Start->Programs->Gemalto->Classic Client-> Classic Client Toolbox
- 2. Од менито на левата страна се избира Certificates
- 3. Од десната страна се избира коренски сертификат и се избира Show details... (Слика 13)

Classic Client				gemalto
1001002	Certificates			
Card Contents		e PIN	Code:	Login
Certificates		FujitsuTechnology Gemplus USB Key	/Solutions GmbH Smart(Smart Card Reader 0 e14's KIBS AD Skopje II	Case KB SCR eSIG 0 D'S Ime 14 Prezime 14's I
Cald Hopeties		- 💦 KibsTrust Cer	lified Certificate Service	riSign Class 2 Public Pri es'S KibsTrust Certifica
		•	m	4
		Show details	Erase	Set as default
Card Administration		Export	Erase All	Register All
Diagnostic/Help				

Слика 13

4. Во новиот отворен прозорец се клика на Install certificate... (Слика 14)

Certificate	x
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	
• 2.16.840.1.113733.1.7.23.2 • All application policies	
	_
Issued to: KibsTrust Certification Authority	
Issued by: VeriSign Class 2 Public Primary Certification Authority - G3	
Valid from 13. 10. 2015 to 13. 10. 2025	
Install Certificate	nent
Learn more about certificates	
	ОК

Слика 14

5. Се започнува постапката за инсталација на сертификатот. Во наредните два прозорци се оставаат пред-дефинираните поставувања и се кликнува на **Next.** (Слика 15 и Слика 16)



Слика 15

Certificate stores are system a	reas where certificates are kept.
Windows can automatically sele the certificate.	ect a certificate store, or you can specify a location for
Automatically select the opening of the opening	certificate store based on the type of certificate
Place all certificates in the	e following store
Certificate store:	
	Browse
earn more about <u>certificate stores</u>	

Слика 16

6. Во последниот прозорец се оди на **Finish** за завршување на постапката (Слика 17). По неколку секунди се појавува информативен прозорец за успешна инсталација на сертификатот (Слика 18).

Certificate Import Wizard	×
	Completing the Certificate Import Wizard
	The certificate will be imported after you click Finish.
	You have specified the following settings: Certificate Store Selected Automatically determined by t Certificate
	< Þ
	< Back Finish Cancel
	Слика 17
Certificate In	nport Wizard
	The import was successful.
	ОК
	Слика 18

7. За инсталација на вториот коренски сертификат, потребно е да се повторат чекорите од 3 до 6.

Забелешка: Коренските сертификати може да се преземат и од веб страната https://www.kibstrust.mk/mk-MK/Home/Support во делот Коренски сертификати.

5. Како да го променам корисничкиот ПИН за пристап до Gemalto Java PKI токенот?

Токенот се добива со поставен кориснички ПИН. ПИН-от се доставува со електронска порака испратена од КИБС ИС, или со отпечатено Писмо со ПИН, и е познат само од страна на сопственикот на Gemalto Java PKI токенот. Заради ваша заштита, се препорачува овој ПИН да го промените и **запаметите**. Промената се прави на следниот начин:

- 1. Се активира Start->Programs->Gemalto->Classic Client-> Classic Client Toolbox.
- 2. Од менито на левата страна се избира Card Administration, односно PIN Management (Слика 19).

Classic Client				gemalto [×]
100100	Certificates			
Card Contents Card Administration	1	e Pin	I Code:	Login
PIN Management		FujitsuTechnolog Gemplus USB Key Ime 14 Prezim SRA Publ RSA Publ KibsTrust Cer	ySolutions GmbH Smart(Smart Card Reader 0 e 14's KIBS AD Skopje II c Key 2048 bits tification Authority'S Ve alified Certificate Service	Case KB SCR eSIG 0 D'S Ime 14 Prezime 14's I riSign Class 2 Public Pri es'S KibsTrust Certifica
		Show details	III Eraca	Set ac default
		Export	Erase All	Register All
Diagnostic/Help				



3. Се избира Gemplus USB Key Smart Card Reader, а потоа Change PIN и се кликнува на **Next** (Слика 20)

gemalte
ement
Select an installed smart card reader
FUJITSU SCR USB 2A 0
Gemplus USB Key Smart Card Rea
- Select a task you want to perform on
G KIBS CA
Change PIN
C Unblock PIN
Next>>



4. Во полето **Current PIN**, се внесува важечкиот ПИН (ПИН-от добиен од КИБС ИС или ПИНот кој со истава постапка сами сте го дефинирале), а во полињата **New PIN** и **Confirm New PIN** се внесува новиот ПИН (Слика 21).

ВАЖНО: Новиот ПИН треба да има минимум 6, а максимум 8 цифри.

Classic Client		ge	malto
1001000	PIN Management		
Card Contents Card Administration	Gemplus USB Key Smart Card Reader 0 PIN User	PIN Policy	
	Current PIN: xecococ New PIN: xecococ Confirm New PIN: xecococ Force user to change PIN Change PIN	Must be at least 6 characters long Must be less than or equal to 8 characters long Must contain only numeric characters	> > >
Diagnostic/Help		<< F	revious

Слика 21

5. Се кликнува на копчето **Change PIN**, по што се јавува порака дека PIN-от е променет (Слика 22)



Слика 22

6. Како да го деблокирам корисничкиот ПИН?

Доколку **3 пати** последователно се внесе погрешен ПИН, Вашиот Gemalto Java PKI TOKEH (токен) ќе се блокира (locked).

За проверка дали е блокиран ПИН-от на Gemalto Java PKI токенот, отворете го Gemalto Classic Client софтверот, внесете го ПИН-от и кликнете Login. Доколку може да се логирате, тогаш сè е во ред, ПИН-от не е блокиран. Но, доколку се појави порака "PIN is Locked", тогаш ПИН-от е блокиран.

За деблокада на ПИН-от, носителот на сертификатот треба **ЛИЧНО** да го донесе токенот во Регистрационата канцеларија на Издавачот на сертификати КИБС за да биде направена деблокада. За оваа услуга се наплатува надомест согласно објавениот ценовник.

Доколку носителот на сертификатот не е во можност лично да дојде, тогаш може:

- Да даде полномошно (<u>https://www.kibstrust.mk/Storage/Dokumenti/4-103.01-65 Полномошно.pdf</u>) со своерачен потпис, на друго лице кое ќе го донесе PKI токенот за деблокада, заедно со потврдата за уплата во КИБС ИС, или
- 2. Да го испрати токенот и потврдата за уплата по пошта до Регистрационата канцеларија на КИБС ИС на адреса објавена на <u>https://www.kibstrust.mk/mk-MK/Home/contact</u> или

3. Да го остави токенот заедно со уплатата кај некој од застапниците на КИБС ИС (<u>https://www.kibstrust.mk/mk-MK/Home/contact</u>).

7. Како да овозможам прелистувачот Firefox да го препознае Gemalto Java PKI токенот?

Оваа точка е наменета за корисниците на дигитални сертификати кои користат прелистувач Mozilla Firefox.

<u>Важно:</u> Gemalto Java PKI токенот е поддржан само во 32-битна верзија на прелистувачот Mozilla Firefox! најнова 32-битна верзија може да се преземе од <u>https://www.mozilla.org/en-</u> US/firefox/all/.

За Gemalto Java PKI токенот со дигитален сертификат, кој го поседувате, да стане препознатлив и да може да се користи од страна на интернет прелистувачот Mozilla Firefox, извршете ги следните чекори:

1. Од менито на прелистувачот во горен десен агол изберете Options (Слика 23).



Слика 23

2. Од менито на левата страна изберете ја опцијата **Privacy & Security**, отидете најдолу, притиснете на копчето **Security Devices** (Слика 24)



Слика 24

3. Ќе се појави прозорче како Слика 25. Кликнете Load

	Dev	ce Manager	×
Security Modules and Devices	Details	Value	Log I <u>n</u>
✓NSS Internal PKCS #11 Module Generic Crypto Services			Log <u>O</u> ut
Software Security Device			Change Password
✓Builtin Roots Module Builtin Object Token			Load
			Unload
			Enable EIPS
			ОК

Слика 25

- 4. Во новиот прозорец кликнете Browse (
- 5. Слика 26) за да ја најдете потребната датотека gclib.dll. Датотеката се наоѓа на патека C:\Program Files\Gemalto\Classic Client\BIN или на патека C:\gemalto\Classic Client\BIN, доколку при инсталација на Mozilla Firefox сте ја одбрале патеката c:\gemalto.

Селектирајте ја датотеката gclib.dll. Кликнете **Open** (Слика 27), во **Module Name** внесете **Gemalto Java PKI token**, а потоа кликнете **OK** (Слика 28).

🕌 Load PKCS#11 Device Driver 🛛 —	
Enter the information for the module you w	ant to add.
Module Name New PKCS#11 Module	
Module <u>f</u> ilename	<u>B</u> rowse
ОК	Cancel

Слика 26

)	Local Disk (C:) 🕨 gemalto	 Classic Client BIN 		▼ ⁴ y Search BIN	V		
Organize 🔻 New folder						(?	
🛠 Favorites	Name	Date modified	Туре	Size			
Deskton	👒 RegTool	08.11.2012 11:25	Application	1.212 KB			
Downloads	🚳 PluginPINMngt.dll	14.09.2012 15:31	Application extens	1.864 KB			
OneDrive	🚳 PluginInformationCard.	dll 08.08.2012 13:31	Application extens	1.764 KB			
Recent Places	🚳 PluginDocumentation.d	II 08.08.2012 13:52	Application extens	974 KB			
Mecenic Places	🚳 PluginCertificates.dll	16.11.2012 17:06	Application extens	1.825 KB			
I thursday	pkcs11_Uninstall	27.11.2012 13:48	HTML Document	5 KB			
Dennes	pkcs11_install	27.11.2012 13:47	HTML Document	8 KB			
Documents	🚳 pk2p15.dll	07.11.2012 18:58	Application extens	2.495 KB			
J Music	🚳 pk2GemID.dll	07.11.2012 18:39	Application extens	1.568 KB			
Pictures	🚳 MSIAction.dll	30.07.2012 16:50	Application extens	623 KB			
Videos Videos	🚳 kharon.dll	22.11.2012 21:50	Application extens	475 KB			
	🚳 GUICore.dll	30.07.2012 22:22	Application extens	656 KB			
Computer	🔲 GslShmSrvc	27.07.2012 15:39	Application	84 KB			
🏭 Local Disk (C:)	🚳 GSafeCsp.dll	06.11.2012 10:33	Application extens	1.036 KB			
🕎 DirIIT (\\Iris\OrgDelovi)	🗟 GemPPM.dll	07.08.2012 19:06	Application extens	813 KB			
	🔤 Gemplus	07.12.2006 17:49	JPEG image	47 KB			
📮 Network	🔂 GCSMregistration	12.01.2015 09:12	Shortcut	2 KB			
	S gclib.dll	27.07.2012 18:54	Application extens	1.096 KB			
	🗟 gck2015x.dll 🛛	File description: PKCS#11 v2.01 - Multip	lexer for Cryptoki API	1.437 KB			
File <u>n</u> ame	: gclib.dll	Company: Gemalto File version: 8.0.2.0 Date created: 27.07.2012 18:54 Size: 1.07 MB		All Files Open	Cance	•	

Слика 27



Слика 28

6. По додавање на вашиот Gemalto Java PKI токен, тој се појавува во листата од левата страна (Слика 29). На ова прозорче кликнете OK.

	Device Manager		×
Security Modules and Devices eNSS Internal PKCS #11 Module Generic Crypto Services Software Security Device a:Builtin Roots Module Builtin Roots Module Builtin Object Token Germalto Java PI2 token	Details Module Path	Value Gemalto Java PKI token CAgemalto\Classic Client\BINgclib.dll	Log Jn Log Qut Change Password Load Unload Enable EIPS
			ОК

Слика 29

 Доколку при додавање на модулот се појави грешка како на Слика 30, тогаш најверојатно имате инсталирано 64-битна верзија на Mozilla Firefox, која не поддржува додавање на 32-битен модул.

Alert		×
	Unable to add module	
	OK	

Слика 30

 За да го прегледате Вашиот сертификат, од менито на левата страна изберете ја опцијата Privacy & Security, отидете најдолу, притиснете на копчето View Certificates (Слика 31).



Слика 31

9. Во прозорчето за внесување лозинка (Слика 32) **НЕ ВНЕСУВАЈТЕ НИШТО**, само кликнете ОК или Cancel.

Passwor	d Required
?	Please enter the master password for the Ime prezime
	OK Cancel

Слика 32

10. Вашиот сертификат се наоѓа во делот Your Certificates (Слика 33).

You have certif	ficates fro	m these	organizatio	ns that i	dentify you:		
Certificate Nat #KIBS AD Skop	me pje	Secu	rity Device	1	Serial Number	Expires On	Ľ\$
Ime10 Pres	zime10	Softw	vare Security	Dev 1	13:8F:0A:74:7C:51:6	5: 26.11.2018	

Слика 33

ВАЖНО ПРЕДУПРЕДУВАЊЕ:



При прегледување на Вашиот сертификат во Mozilla Firefox (Слика 33), **ВО НИКОЈ СЛУЧАЈ НЕ СМЕЕТЕ да го изберете**

копчето DELETE. Со избирање на ова копче, се иницира бришење на Вашиот сертификат директно од Вашиот РКІ ТОКЕН!

Ако сепак кликнете Delete, ќе добиете предупредување како на Слика 34. Во ова прозорче задолжително изберете CANCEL!

Бришењето на Вашиот сертификат преку Mozilla Firefox е целосно Ваша одговорност!

Во ваков случај НЕ постои начин да се поврати сертификатот, поради што Вие ќе треба да ја започнете постапката за добивање нов сертификат и да ги покриете трошоците за негово издавање!

Delete your Certificates
Are you sure you want to delete these certificates?
Ime10 Prezime10
If you delete one of your own certificates, you can no longer use it to identify yourself.
OK Cancel

Слика 34

* * *