

Корисничко упатство за алатката DigiCert Trust Assistant

Верзија: 1.0 Датум: 13.12.2024 103.47

КИБС АД Скопје

© 2024 КИБС АД Скопје, сите права задржани

https://www.kibstrust.com/

Содржина

1.	Вовед	. 3
2.	Инсталирање на алатката	. 3
3.	Генерирање на CSR барање	. 4
4.	Инсталација на сертификат	. 6
5.	Бекап на сертификат	. 9
	5.1 Бекап преку DigiCert Trust Assistant	. 9
	5.2 Бекап преку Windows certificates store	. 9

1. Вовед

Овој документ дава преглед на активностите кои може да се извршат користејќи ја алатката DigiCert Trust Assistant.

DigiCert Trust Assistant е десктоп апликација, која се користи за управување со клучеви и сертификати на локален компјутер. Со оваа алатка може да се генерираат CSR барања за издавање на сертификати и да се прави import/export на сертификати со или без приватниот клуч.

2. Инсталирање на алатката

Алатката може да ја преземете од следните линкови:

Windows

MAC

и истата да ја инсталирате на вашиот компјутер.

Напомена: Подолу опишаните постапки поврзани со оваа алатка треба да бидат правени на еден ист компјутер!

Откако ќе се инсталира алатката, истата може да се стартува со кликнување на стрелката на taskbar-от, со десен клик на иконата на алатката и кликнување на **Dashboard** (Слика 1 и Слика 2), за Windows оперативен систем.





Слика 2

Прегледот на активирање на алатката за МАС оперативен систем е прикажан на





Потоа се отвора прозорецот од Слика 4, кој претставува почетна страна за користење на алатката DigiCert Trust Assistant:

DigiCert Trust Assistant (V1.1.4)				- 0	×
d digicert [®]	Dashboard			≡	•
Dashboard	Dashboard				^
🔑 Tokens	Where is your certificate? Select your virtual token or in:	serted hardware token to viev	v your certificates.		
	DigiCert Software KeyStore	Windows CryptoAPI	Lile Gagovska	C Refresh token	
	Memory usage in tokens An overview of the memo Lile Gagovska 62629 B Free Memory	hardware ny usage Bytes mory Used Memory			

Слика 4

Во овој дел можат да се видат виртуелните токени и приклучените хардверски токени и да се прегледаат сертификатите на нив.

3. Генерирање на CSR барање

Co DigiCert Trust Assistant алатката може да се креира CSR барање на следниот начин:

За Windows оперативен систем, во менито Tokens се избира Windows CryptoAPI, а од паѓачкото мени Quick Actions се избира Generate CSR, како на Слика 5:



За МАС оперативен систем, во менито **Tokens** се избира **MacOS Crypto**, а од паѓачкото мени **Quick Actions** се избира **Generate CSR**, како на Слика 6:

•••	DigiCert Trust Assistant	(V1.1.4)		
d digicert 🔇	Tokens			≡ 🕜
🕃 Dashboard	MacOS Crypto			
🖉 Tokens 🚺	Quick actions -			
DigiCert Software KeyStore	Subject (CN) 🗘 🍸	From Ĉ 💎	To Ĉ 💎	ES
MacOS Crypto				
2	JontralV Voltalli Mac	04 Mar 2024	14 Mar 2024	
	JontralV MacVoltaIII Mac	04 Mar 2024	06 Mar 2024	
	KIBSTrust Issuing Test CA for e-Signatures	09 May 2019	09 May 2029	

Слика 6

Се отвора прозорец, во кој се пополнуваат следните податоци: тип и големина на клучот, алгоритам за енкрипција и дали да може да се експортира приватниот клуч (Слика 7):

```
KeyType = RSA
KeySize = 2048
Signing Algorithm = sha256WithRsaEncryption
Private Key is exportable = Yes
```

Generate CS	R	×
Key type	RSA	•
Key size	2048	•
Signing algorithm	sha256WithRsaEncryption	•
Private key is export: • Yes No Generated CSR	able.	
		le
	Close	rate



Со кликнување на копчето **Generate**, се генерира CSR барањето и истото може да се ископира на копчето **Copy**, како на Слика 8. Ископираната содржина се користи за преземање на сертификат преку порталот <u>KIBSTrust Accounts</u> во Чекор 3.

Generate CS	R	×
Key type	RSA	•
Key size	2048	•
Signing algorithm	sha256WithRsaEncryption	•
Private key is export • Yes · No Generated CSR	able.	
BEGIN CERTIFICA MIICcjCCAVwCAQAwL NmM2Y2UzMzg4YTgz 4	TE REQUEST ZEtMCsGA1UEAwwkYzIzNzM5NWEtYJ MIIBIJANBgkqhkiG9w0BAQEFAAOCA(MyNC000GM2LT
	СІ	ose Copy

Слика 8

4. Инсталација на сертификат

По издавање на сертификатот преку порталот <u>KIBSTrust Accounts</u>, истиот се сочувува како датотека со име cert.pem.

За користење на порталот <u>KIBSTrust Accounts</u>, можете да го прегледате корисничкото упатство на следниот <u>линк</u>.

Постапката за инсталација на сертификат е следна:

Во менито **Tokens** се избира **Windows CryptoAPI**, а од паѓачкото мени **Quick Actions** се избира **Import Certificate** (Слика 9).



Се отвора прозорец, во кој со кликнување на **Choose File** се прикачува сертфикатот (Слика 10):

 DigiCert Trust Assistant (V1.1.4) 		- 🗆 X
d digicert [®]	Tokens	≡ 0
🚯 Dashboard	Windows CryptoAPI	
🔑 Tokens	Quick actions 👻	
DigiCert Software KeyStore		
> Windows CryptoAPI	Import certificate	
Isidora Martinovska	May 09, 2029	
Advanced	Supported file formats: [X.509 (.pem), PKCS#7 (.p7b), PKCS#12 (.pfx .p12) or GLCK (.glck)]	
	Choose File No file chosen Jun 19, 2024	
	Cancel Import	

Слика 10

Сертификатот се прикачува во .pem формат и се кликнува на Import (Слика 11):

Import cer	tificate >	<
Supported file for (.pfx .p12) or GLC	mats: [X.509 (.pem), PKCS#7 (.p7b), PKCS#12 K (.glck)]	
Choose File	Adv certificate.pem	
CommonName : .	Adv certificate	
	Cancel Import	

Слика 11

Сертификатот може да се види во листата на сертификати во DigiCert Trust Assistant алатката, во менито **Tokens**, каде се избира **Windows CryptoAPI** (Слика 12):

DigiCert Trust Assistant (V1.1.4)				-		\times
d digicert°	Tokens				≡	3
🚯 Dashboard	KIBSTrust Issuing Test CA for e-Signatures	May 09, 2019	May 09, 2029			- ^
🔑 Tokens	Isi Martin	Mar 29, 2024	Mar 29, 2025			
DigiCert Software KeyStore	Ime prezime	Jun 28, 2024	Jun 28, 2025			ł
Isidora Martinovska	Isidora Mar	Jul 04, 2024	Jul 14, 2024			
∰\ Advanced	Adv certificate	Jul 10, 2024	Aug 09, 2024			

Кога ќе се додаде сертификат со алатка DigiCert Trust Assistant, истиот може да се види во Manage user certificates во делот Certificates - Current user -> Personal -> Certificates за Windows оперативен систем (Слика 13), односно во Keychain Access -> Certificates за MAC оперативен систем (Слика 14).

🔚 certmgr - [Certificates - Current	User\Personal\Certificates]			-		×
File Action View Help						
🗢 🔿 🙍 📊 🗎 🙆 🔒 🗌	? 🖬					
🙀 Certificates - Current User	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	ame _
✓ Personal	196b753a9-52f2-4ee1-a1a7-29db	MS-Organization-Access	06.09.2033	Client Authentication	<none></none>	
Certificates	🛱 Adv certificate	KIBSTrust Issuing Qsig CA G3	09.08.2024	Secure Email, Client	<none></none>	
Fnterprise Trust	Sellme prezime	KIBSTrust Issuing Qsig CA G3	28.06.2025	Secure Email, Client	<none></none>	

Слика 13



Слика 14

По успешно завршена постапка, опишана во горенаведените чекори, можете да почнете со користење на вашиот сертификат.

5. Бекап на сертификат

5.1 Бекап преку DigiCert Trust Assistant

Со користење на Digicert Trust Assistant алатката може да се направи бекап на сертификатот на следниот начин:

Во менито **Tokens** се избира **Windows Crypto API**. Се кликнува на трите точки кај сертификатот кој сакаме да го експортираме, и се кликнува на Download (Слика 15):

OigiCert Trust Assistant (V1.1.4)				-		>	×
d digicert 🔹	Tokens				≡	0	
Dashboard	KIBSTrust Issuing Test CA for e-Signatures	May 09, 2019	May 09, 2029				*
🖉 Tokens	Isi Martin	Mar 29, 2024	Mar 29, 2025				
DigiCert Software KeyStore Windows CryptoAPI	Ime prezime	Jun 28, 2024	Jun 28, 2025				i
Isidora Martinovska	Isidora Mar	Jul 04, 2024	Jul 14, 2024				I
Advanced	Adv certificate	Details	Aug 09, 2024				l
	Isido Martinnn	Download Delete	Apr 05, 2025				
	lardanka Bashkava	Generate signature	Apr 00, 2025				

Слика 15

Во наредниот чекор се појавува прозорец во кој треба да се избере во кој формат сакаме да го симнеме сертификатот (Слика 16):

Се избира **.pfx** формат, каде ќе се појави поле во кое треба да се внесе лозинка, со која ќе го заштитите приватниот клуч на сертификатот и се кликнува на **Download**. Се одбира име и локација каде да се зачува сертификатот.

•••••	•		R
Password			
 X.509 (.pem) GLCK (.glck) 	O PKCS#7 (.p7b)	O PKCS#12 (.pfx))
Select format			
Certificate name Adv certificate			

Слика 16

5.2 Бекап преку Windows certificates store

Во Certificates - Current user -> Personal -> Certificates (Windows Certificate Store) за Windows оперативен систем, се селектира сертификатот на кој треба да се направи

backup. Се кликнува десен клик на сертификатот, и во **All Tasks** се избира **Export** (Слика 17):

le Action View Help	1 📑 🛛 🖬					
Certificates - Current User	Issued To		Issued By MS-Organization-Access	Expiration Date 06.09.2033	Intended Purposes Client Authentication	Friendly No <none></none>
Certificates	Contraction Adv certification and a certification of the second s	Open	STrust Issuing Qsig CA G3 STrust Issuing Qsig CA G3	09.08.2024 28.06.2025	Secure Email, Client Secure Email, Client	<none> <none></none></none>
Intermediate Certification Active Directory User Obje	🗐 lsi Mar 🗐 lsi Martir	All Tasks	> Open		Client Authenticati Client Authenticati	lsi Mar's Kl Isi Martin's
Trusted Publishers	Sido Mai	Cut Copy	Request Certificate with Ne	iew Key w Key	Client Authenticati Client Authenticati	Isido Marti Isido Marti
Third-Party Root Certificat	SISIDORA -	Delete	Advanced Operations	>	Client Authenticati	ISIDORA M
Client Authentication issu Client Authentication issu Cher People Preview Build Roots	Sidora N	Help	STrust Issuing Osig CA G2	16.04.2025	Client Authenticati Client Authenticati	Isidora Ma <none></none>

Во следниот прозорец се избира дали да експортира приватниот клуч на сертификатот (Слика 18):

÷	🐉 Certificate Export Wizard	×
	Export Private Key You can choose to export the private key with the certificate.	
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
	Do you want to export the private key with the certificate?	
	• Yes, export the private key	
	\bigcirc No, do not export the private key	
	Next Cance	1

Слика 18

Доколку се избере експортирање на приватниот клуч на сертификатот, се избира .pfx формат (Слика 19):

Ex	port File Format
	Ceruncates can be exported in a variety of nie formats.
	Select the format you want to use:
	OER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	 Microsoft Serialized Certificate Store (.SST)

Слика 19

На следниот прозорец се кликнува на Password и во полињата треба да се внесе и потврди лозинката со која ќе се заштити приватниот клуч на сертификатот (Слика 20):

← 🛿 ← Frificate Export Wizard	×
Security To maintain security, you must protect the private ke using a password.	y to a security principal or by
Group or user names (recommended)	
	Add
	<u>R</u> emove
Password:	
<u>C</u> ontrm password:	
Encryption: AES256-SHA256	
	Next Cancel

Слика 20

Се избира име и локација каде да се зачува сертификатот и постапката завршува со кликнување на Finish (Слика 21):

You have successfully completed the Certificate Export wizard. You have specified the following settings: File Name C:\Users\isidoram\Downloads\certttt. Export Keys Yes Include all certificates in the certification path Yes File Format Personal Information Exchange (*.pf:	Completing the Certificate Export Wizard						
You have specified the following settings: File Name C:\Users\isidoram\Downloads\certttt. Export Keys Yes Include all certificates in the certification path Yes File Format Personal Information Exchange (*.pf.	You have successfully completed the Certificate Export wizard.						
File Name C:\Users\isidoram\Downloads\certttt Export Keys Yes Include all certificates in the certification path Yes File Format Personal Information Exchange (*.pf	You have specified the following settings:						
Export Keys Yes Include all certificates in the certification path Yes File Format Personal Information Exchange (*.pf	File Name	C: \Users \isidoram \Downloads \certttt					
Include all certificates in the certification path Yes File Format Personal Information Exchange (*.pl	Export Keys	Yes					
File Format Personal Information Exchange (*.pl	Include all certificates in the certification path	Yes					
	File Format	Personal Information Exchange (*.pf					

Слика 21