Корисничко упатство за алатката DigiCert Trust Assistant

Верзија: 1.0

Датум: 13.12.2024

103.47

КИБС АД Скопје

https://www.kibstrust.com/

Содржина

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

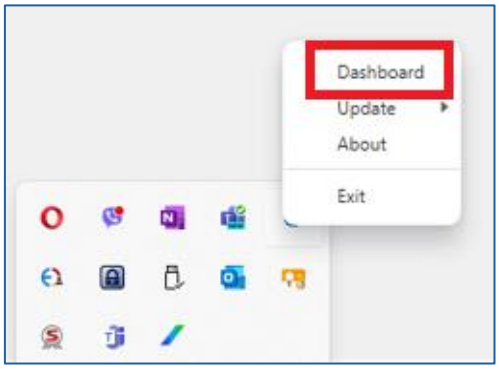
MAC

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 1

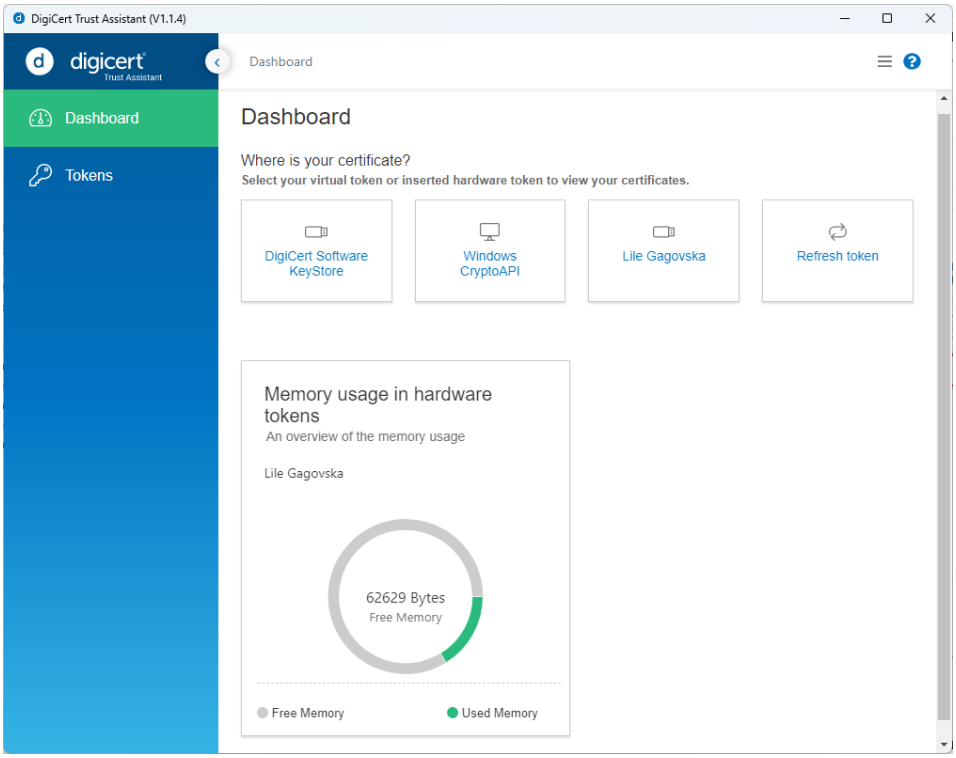


Слика 2

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

Слика 3

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



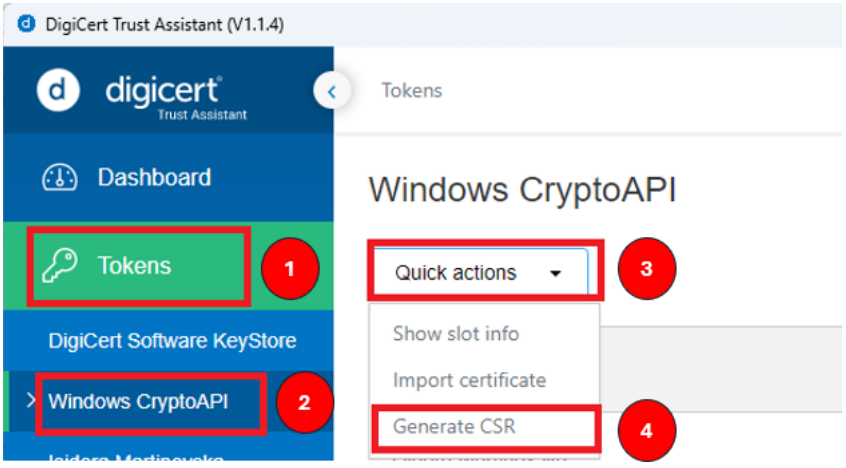
Слика 4

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

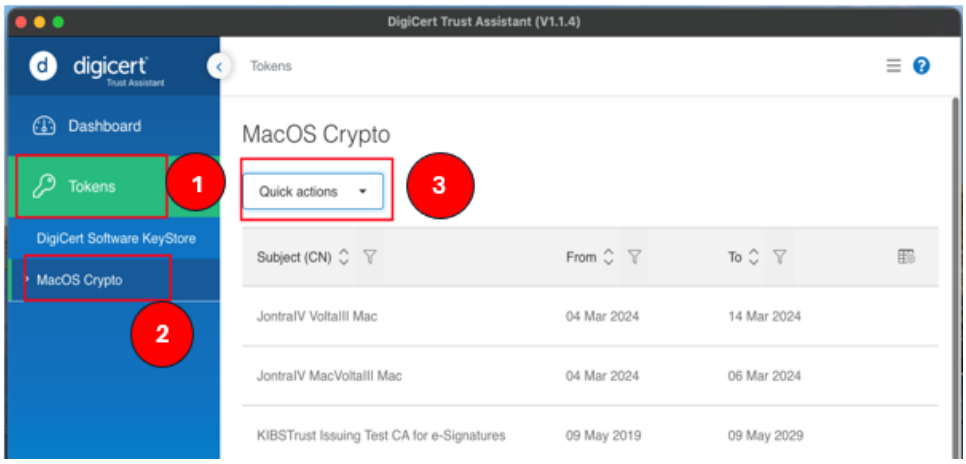
Со DigiCert Trust Assistant алатката може да се креира CSR барање на следниот начин:

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:



Слика 5

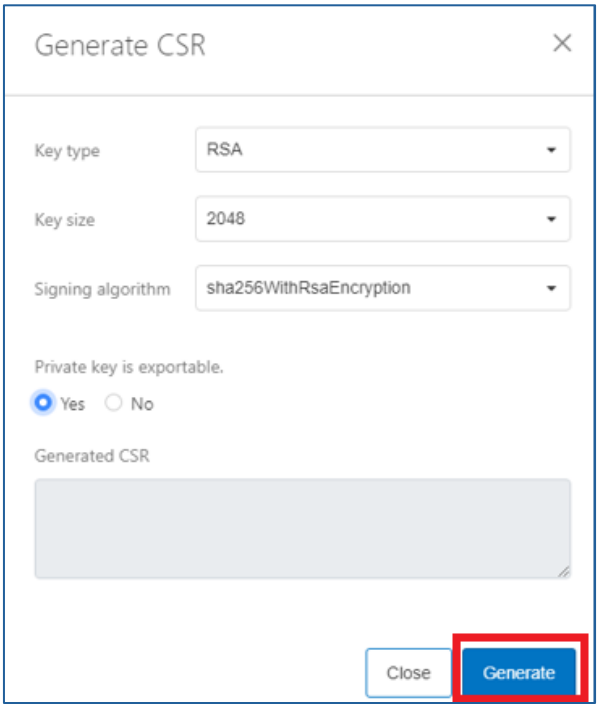
За MAC оперативен систем, во менито **Tokens** се избира **MacOS Crypto**, а од паѓачкото мени **Quick Actions** се избира **Generate CSR**, како на Слика 6:



Слика 6

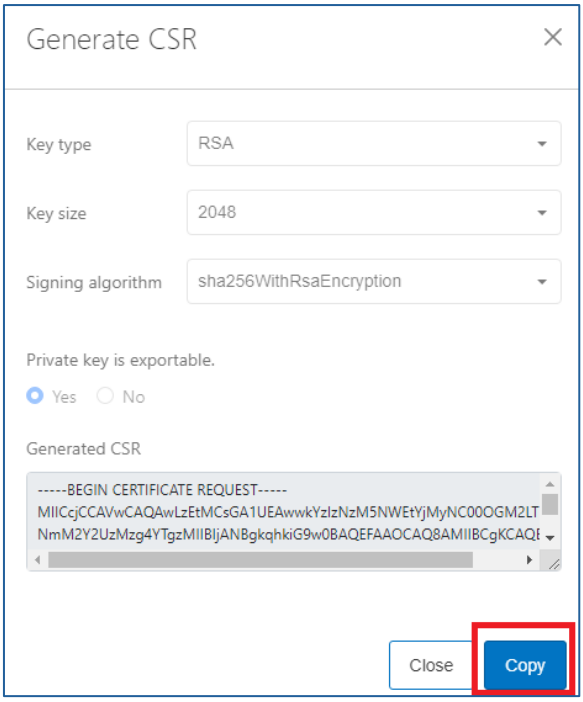
Се отвора прозорец, во кој се пополнуваат следните податоци: тип и големина на клучот, алгоритам за енкрипција и дали да може да се експортира приватниот клуч (Слика 7):

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



Слика 7

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 KIBSTrust Accounts во Чекор 3.



Слика 8

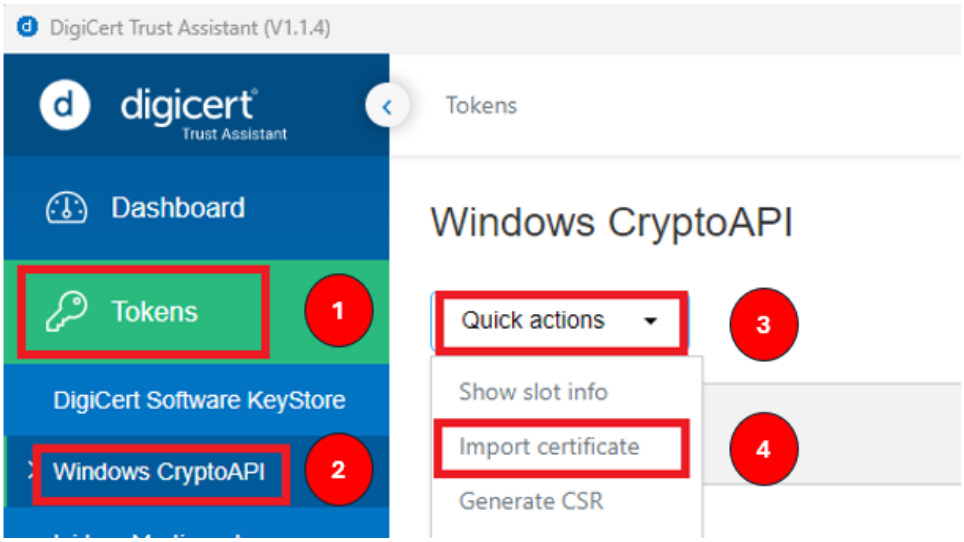
4. Инсталација на сертификат

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

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

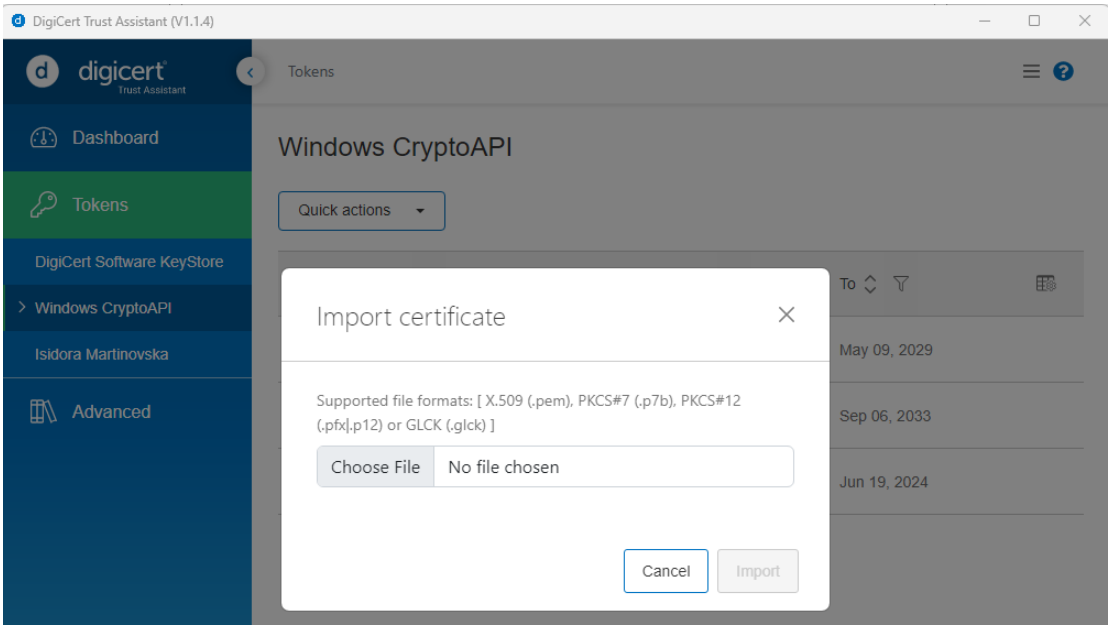
Постапката за инсталација на сертификат е следна:

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



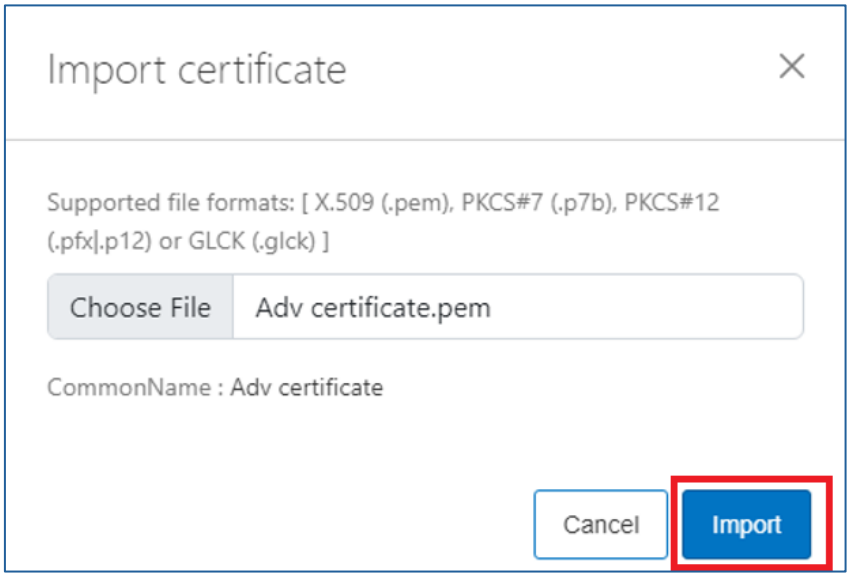
Слика 9

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



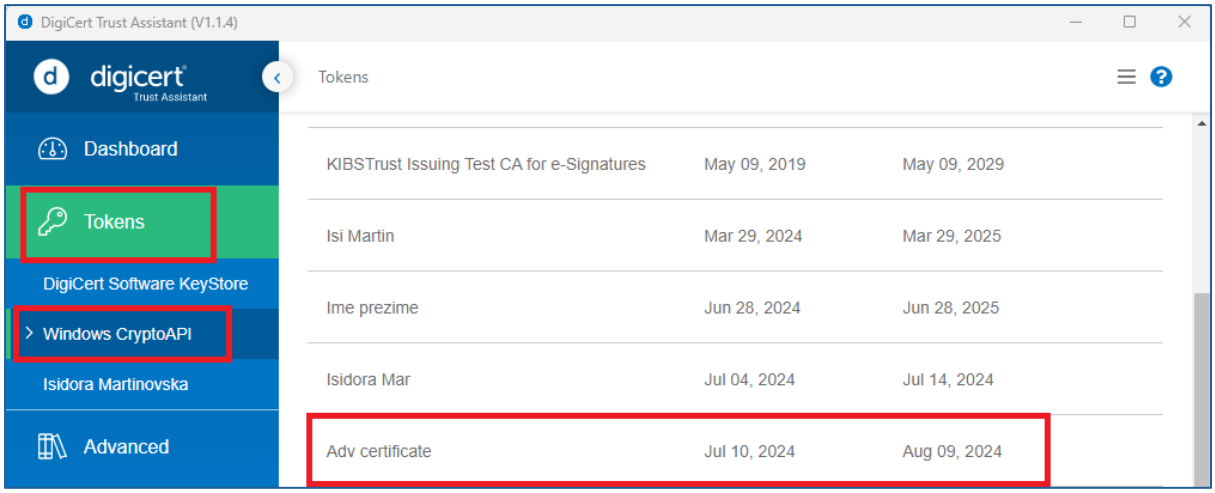
Слика 10

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



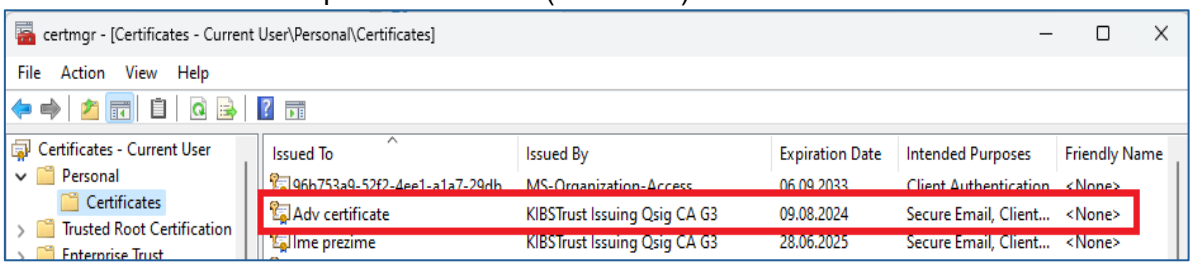
Слика 11

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

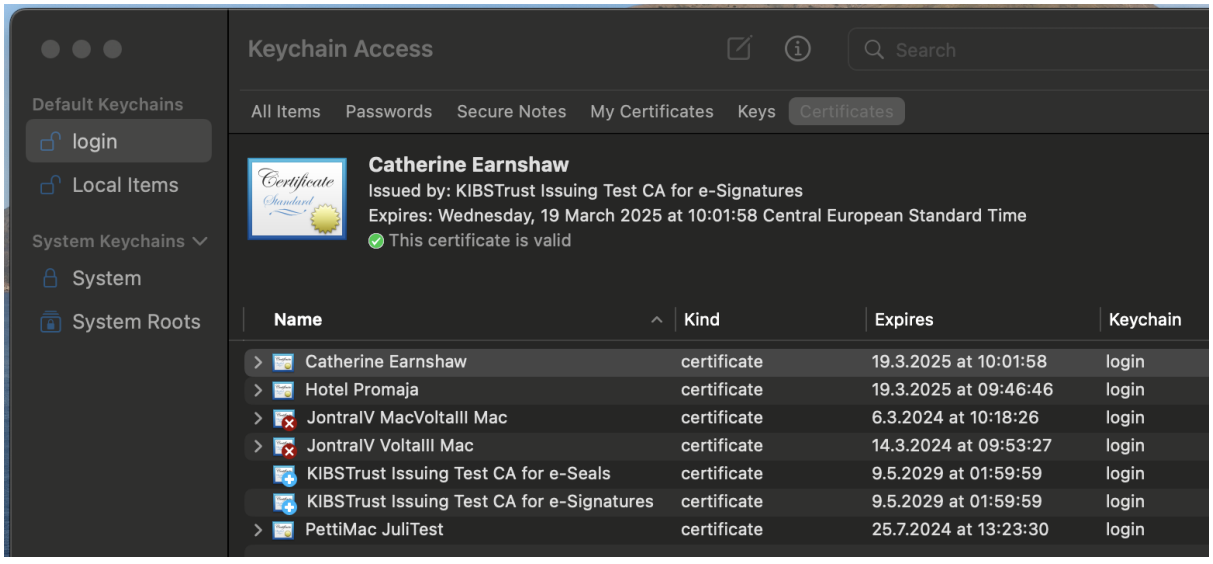


Слика 12

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).



Слика 13



Слика 14

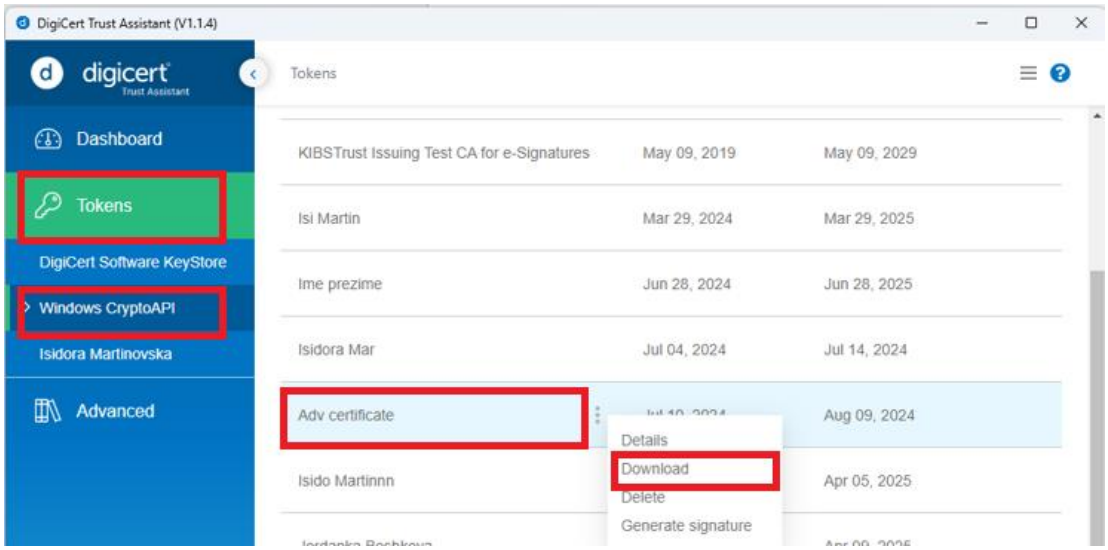
По успешно завршена постапка, опишана во горенаведените чекори, можете да почнете со користење на вашиот сертификат.

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:

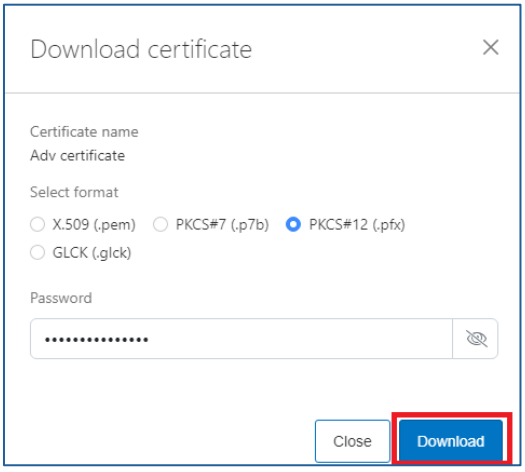
Во менито **Tokens** се избира **Windows Crypto API**. Се кликнува на трите точки кај сертификатот кој сакаме да го експортираме, и се кликнува на Download (Слика 15):



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.

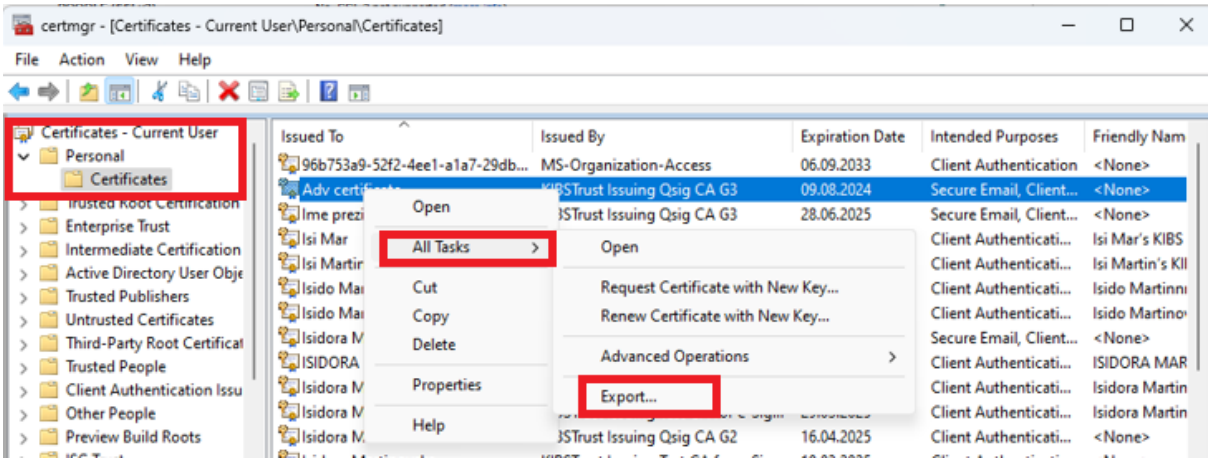


Слика 16

5.2 Бекап преку Windows certificates store

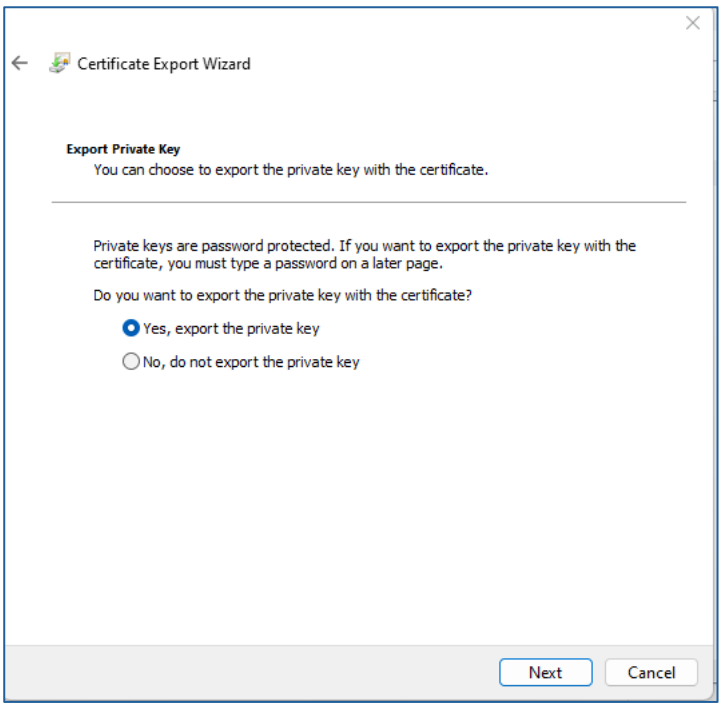
Во **Certificates - Current user -> Personal -> Certificates (Windows Certificate Store)** за **Windows** оперативен систем, се селектира сертификатот на кој треба да се направи

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



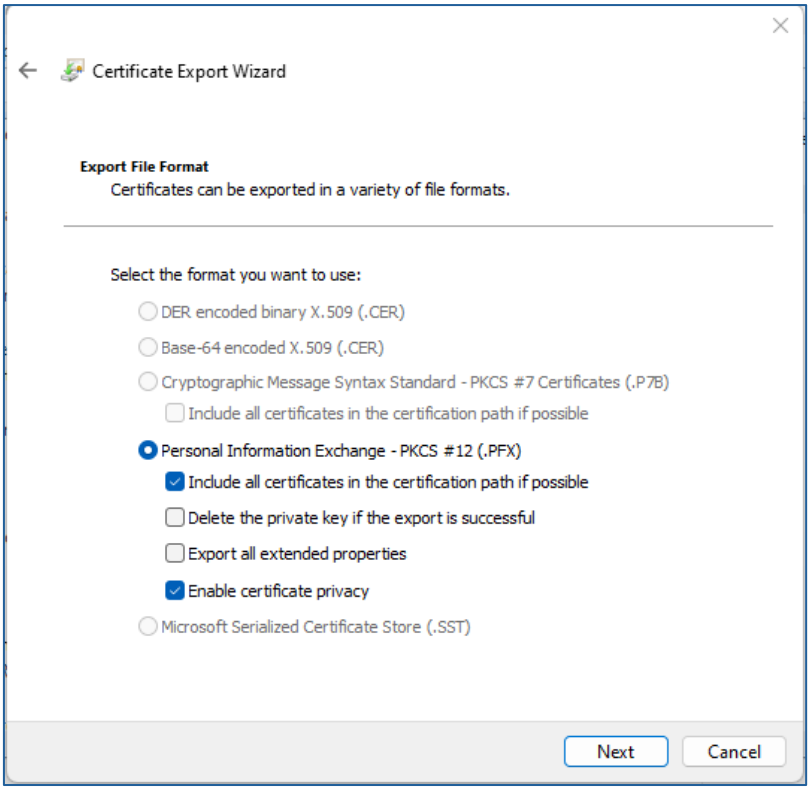
Слика 17

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



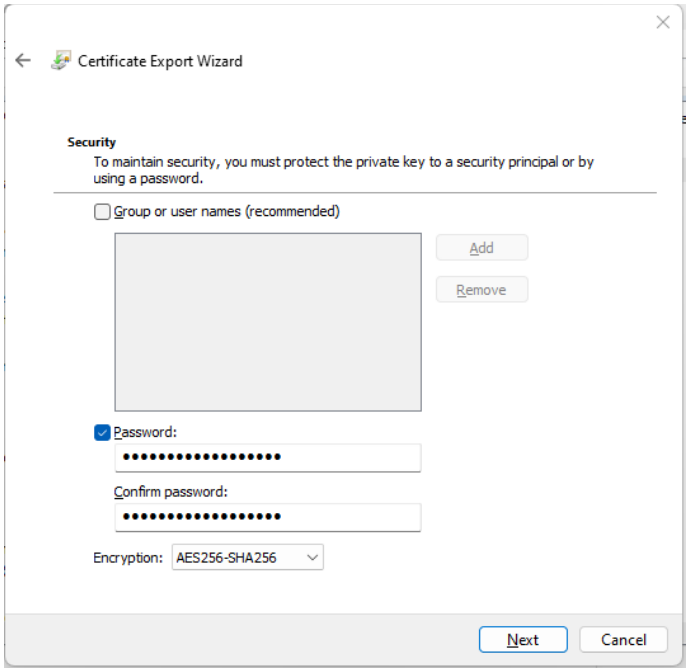
Слика 18

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



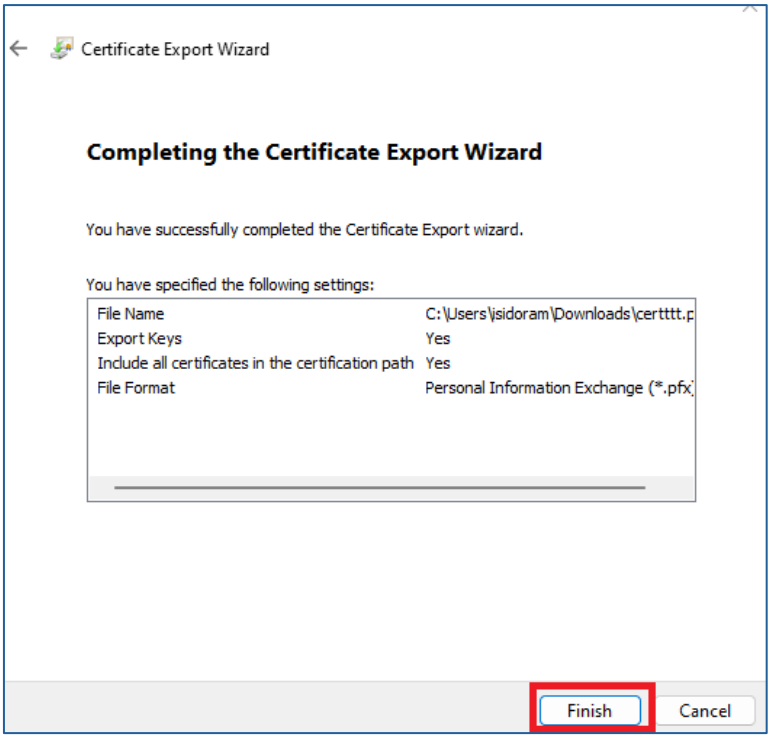
Слика 19

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):



Слика 20

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


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

Слика 21