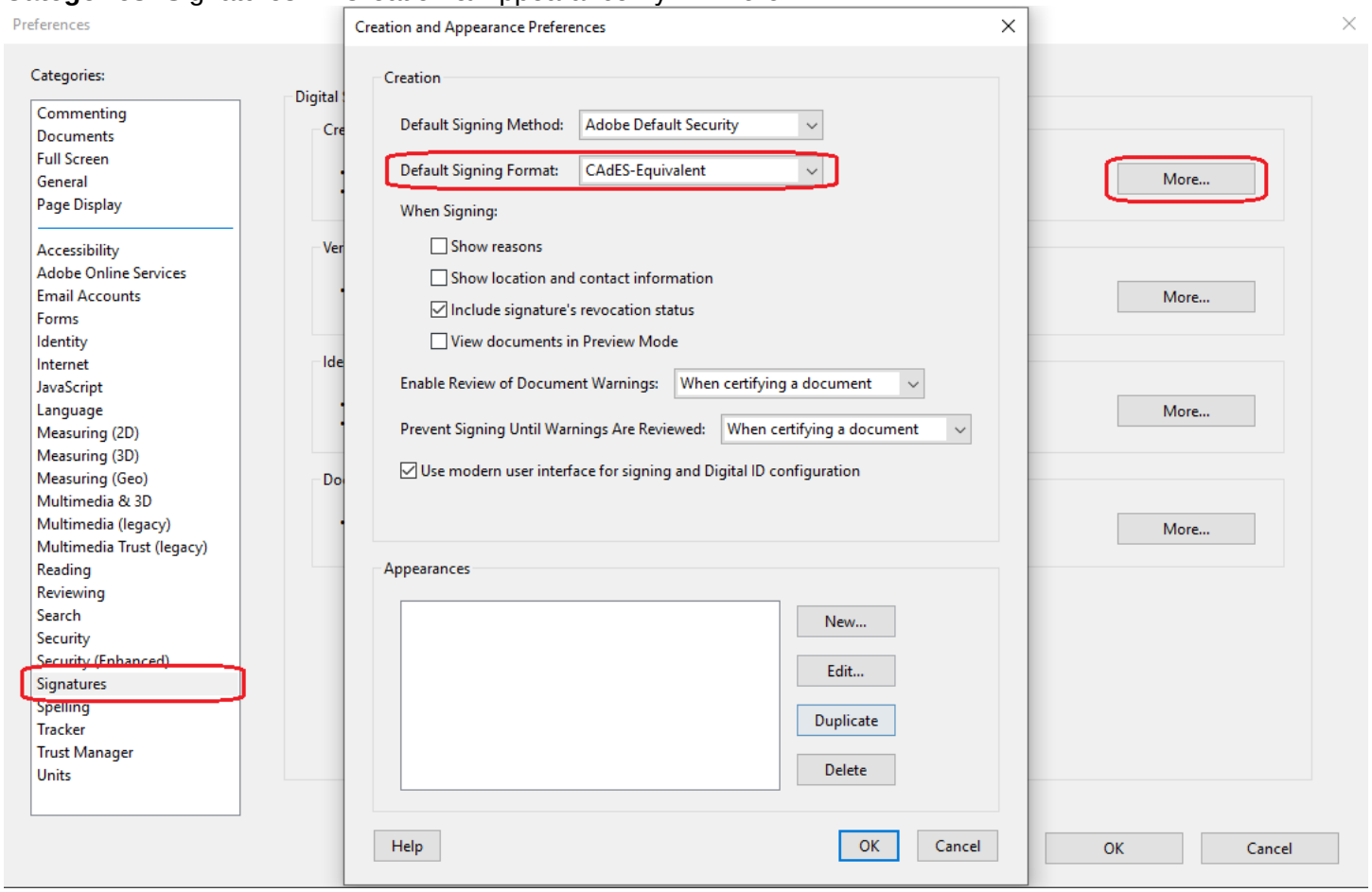
ИНСТРУКЦИИ ЗА НАСТРОЙКИ И ПОДПИСВАНЕ
с Adobe Acrobat DC
за Windows операционни системи

Ако нямате инсталиран Adobe Acrobat DC може да го изтеглите от тук.

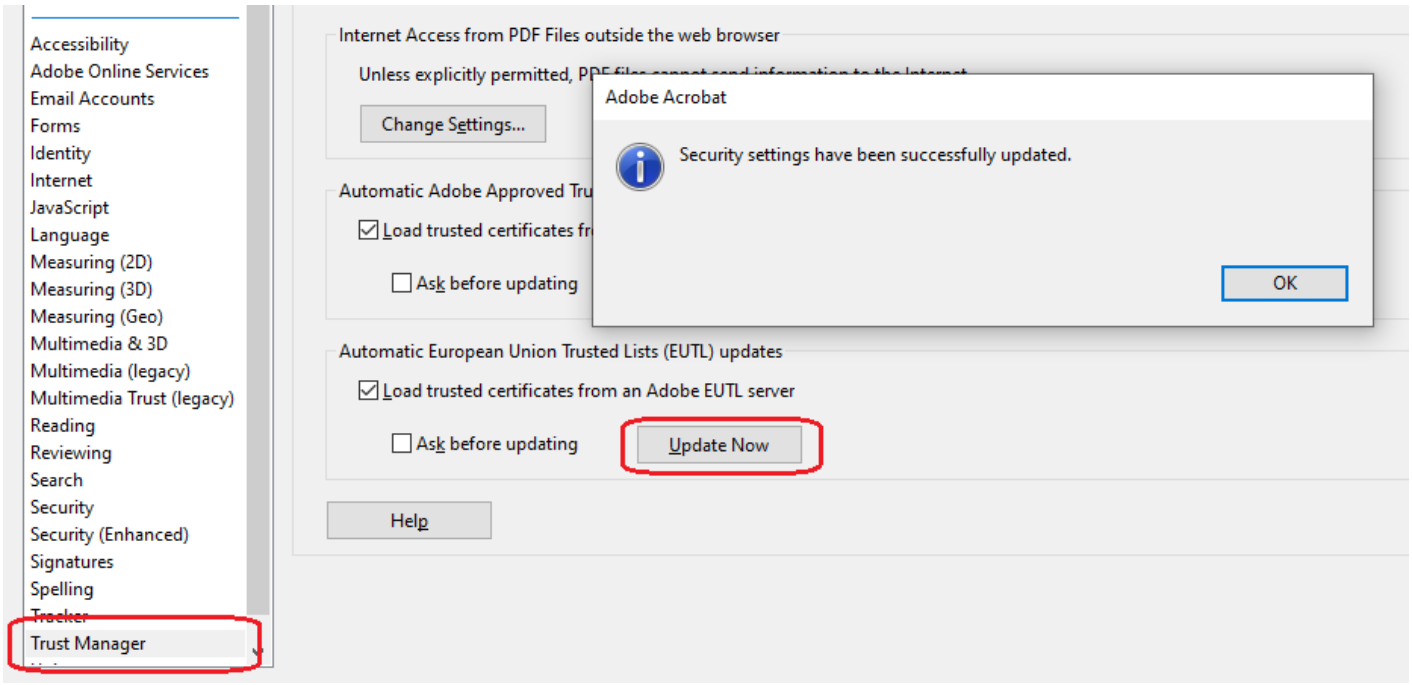
Инсталирайте всички удостоверителни вериги на B-Trust от тук.

1. *Основни настройки:*

Categories: Signatures → Creation & Appearance бутон *More*…



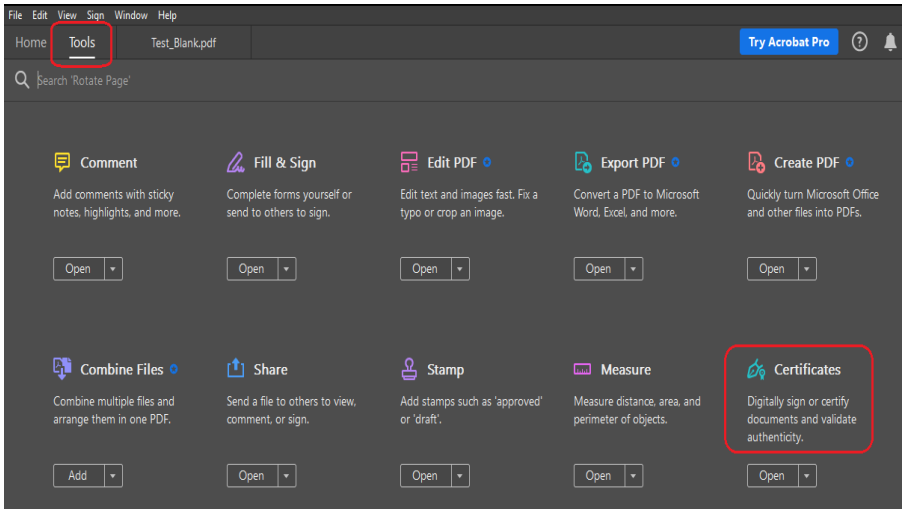
Categories: Trust Manager → Automatic European Union Trusted List (EUTL) update → „Update Now“



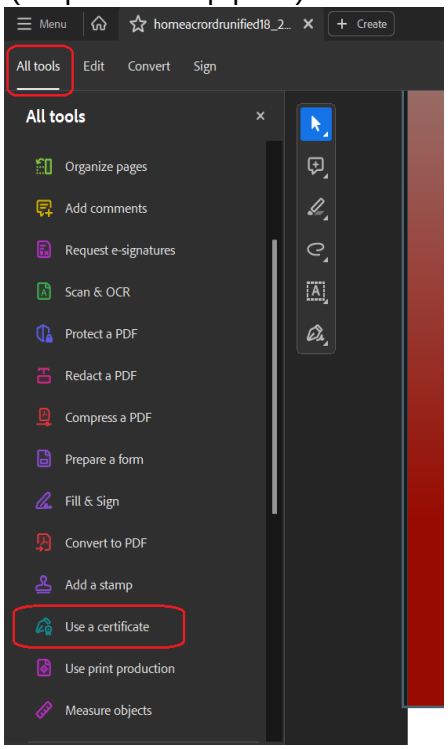
Изчаква се да излезе съобщението „Security settings have been successfully updated“.

2. *Подписване на документ с вградената функция на Acrobat Reader DC.*

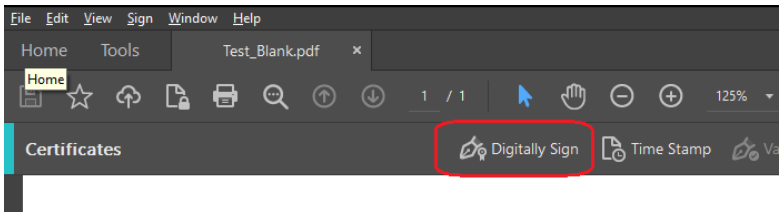
   a. Отваряте документа, който искате да подпишете и следвате следните стъпки - от меню ***Tools / All tools*** избирате ***Certificates / Use a certificate*** (стар/нов интерфейс):



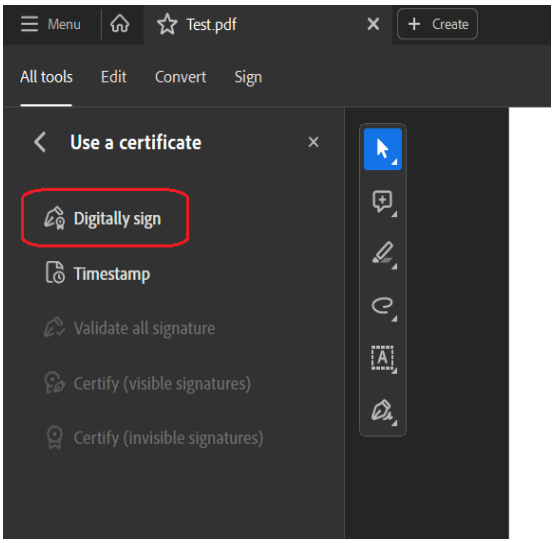
или



b. Избирате опция ***Digitally Sign***:



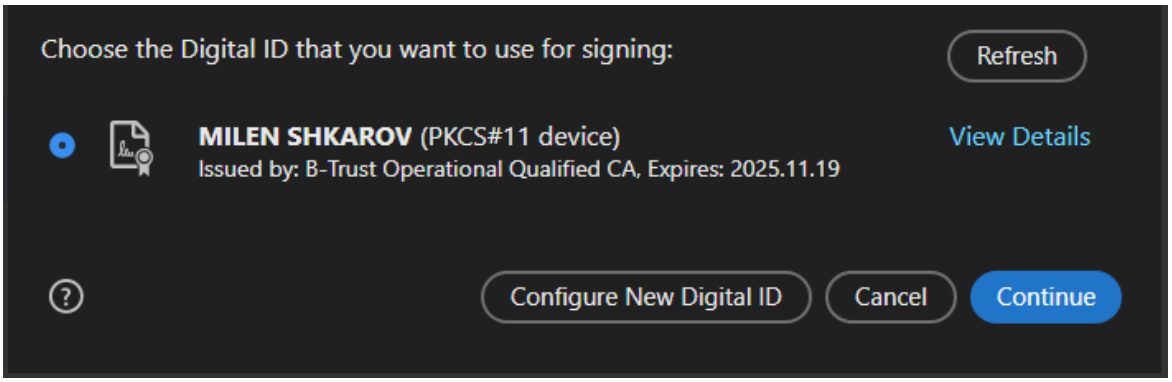
или



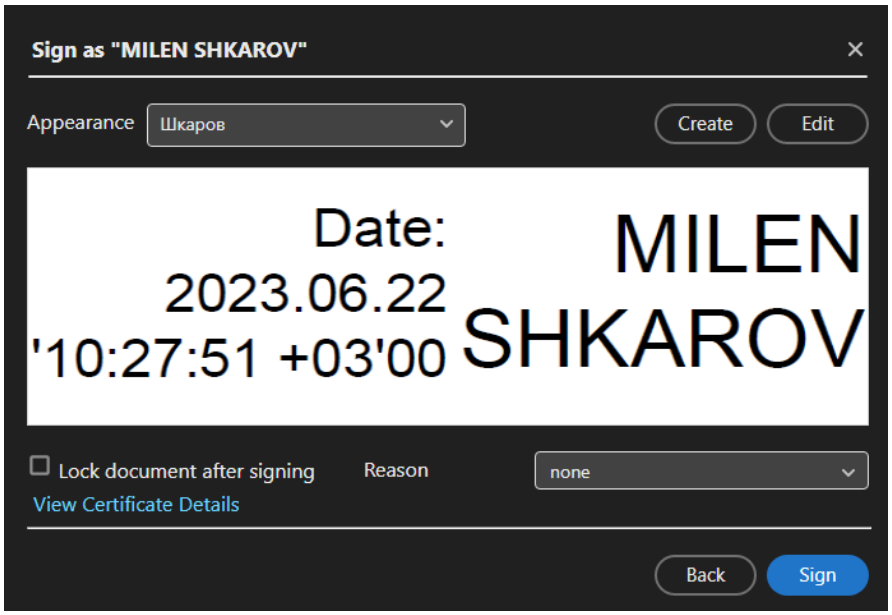
c. С левия бутон на мишката очертавате мястото, на което желаете да разположите подписа:

или

d. Посочвате сертификата, с който трябва да подпишете и натискате бутон **Continue**:



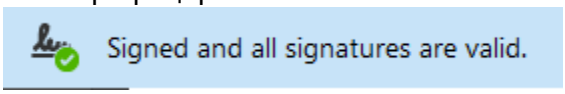
e. Визуализират се данните за избрания сертификат и подписването се извършва, чрез бутона **Sign**.



f. Избирате къде да бъде записан подписваният файл и с какво име и въвеждате PIN, когато компютъра го изиска;

g. В подписаният документ се визуализират имената на подписващия и дата/час на подписване.

h. Горе в ляво на подписания документ трябва да излиза както е показано, че документа е успешно подписан и верифициран:



3. Проверка / валидация на електронно подписан документ може да направите на B-TRUST | Квалифицирана услуга за валидация (Qualified Signature Validation Service)

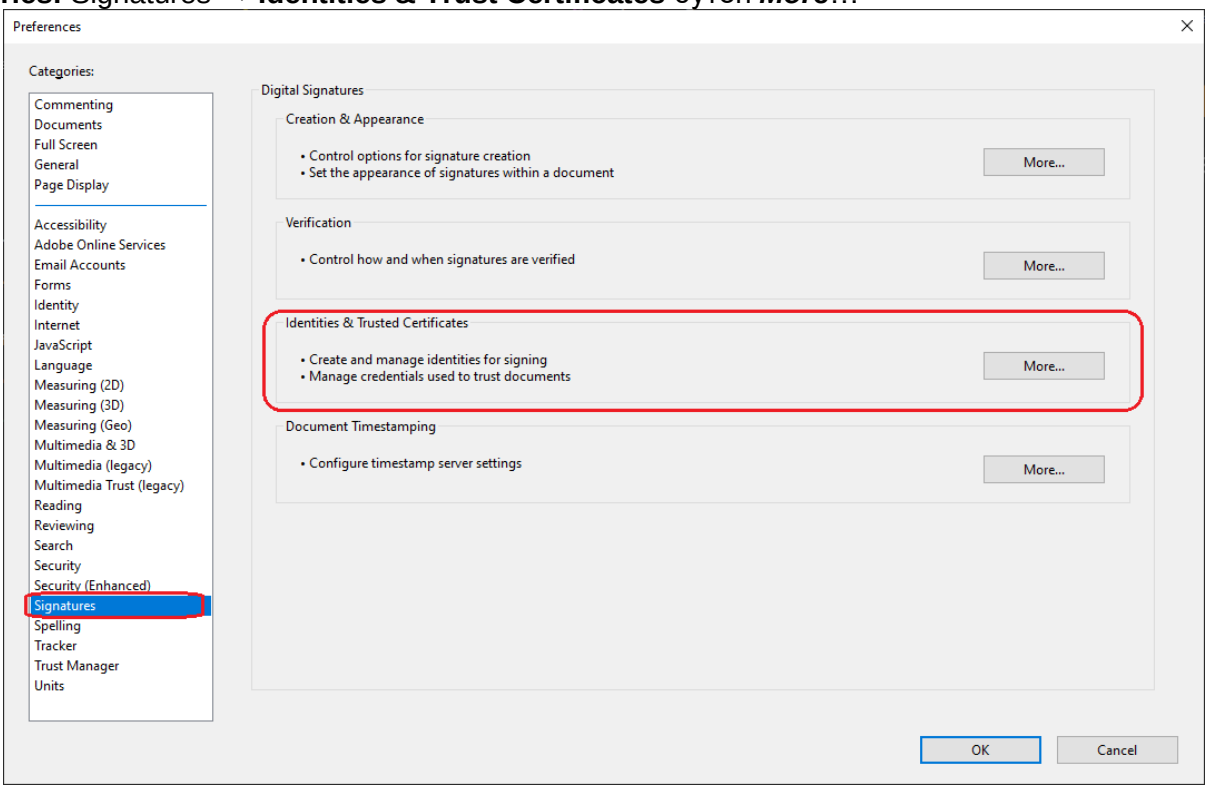
За контакти:
T: 0700 199 10
M: *9910
e-mail: support@borica.bg

Важно!

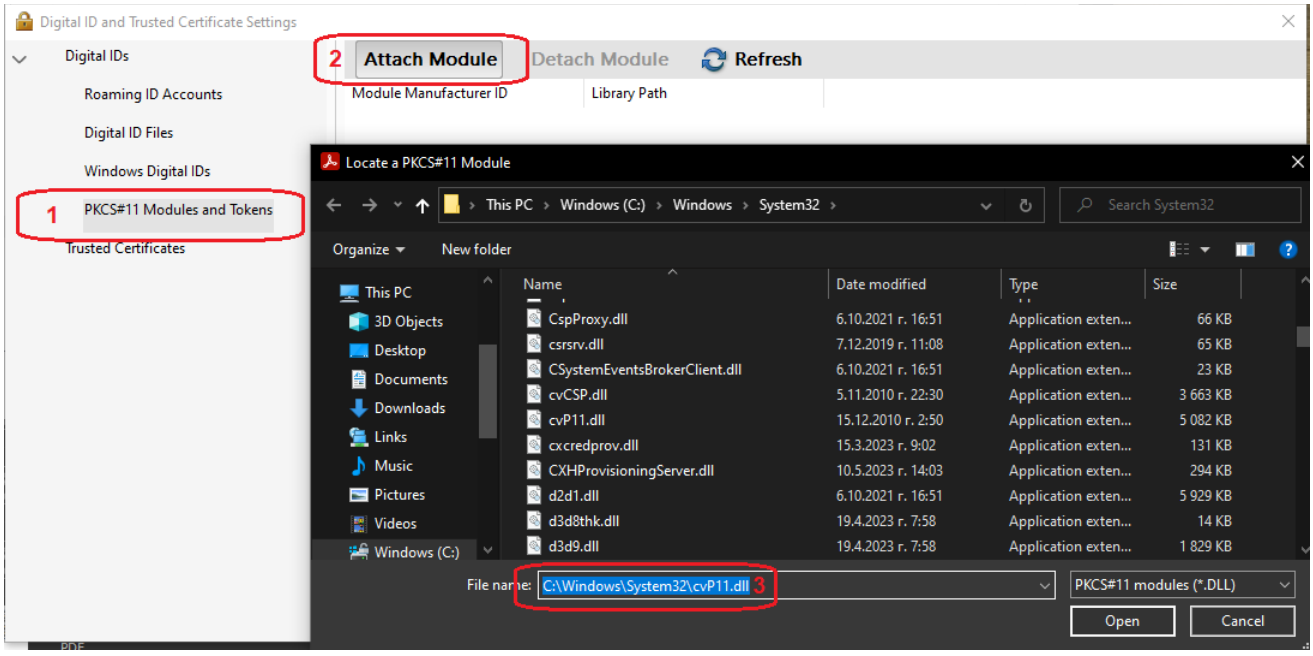
За клиенти, които използват по-стари тип карти Siemens и CryptoVision, Acrobat Reader трябва да се настрои да подписва документи, чрез PKCS#11 механизъм.

Следващите настройки са допълнение към тези от първа точка.

Categories: Signatures → **Identities & Trust Certificates** бутон ***More***…

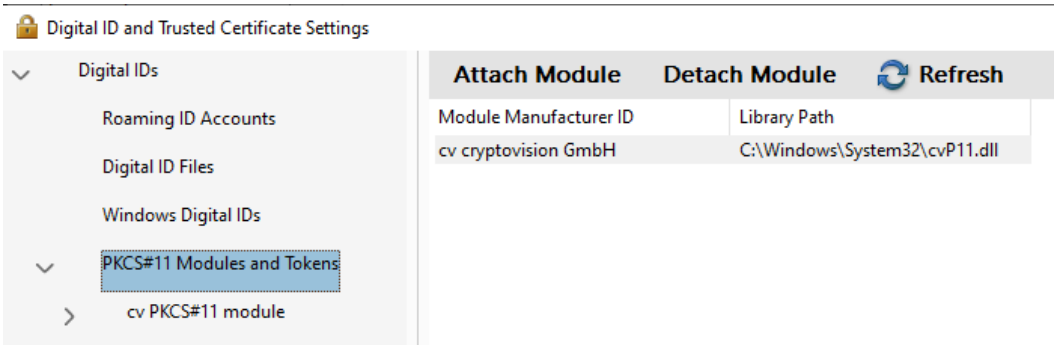


Избирате ***PKCS#11 Modules and Tokens*** (1), ***Attach Module*** (2):

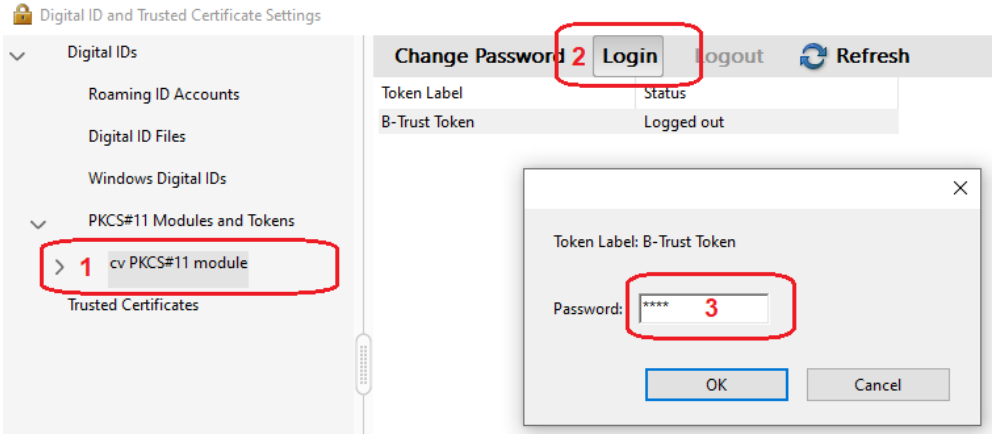


и избирате и зареждате следната библиотека: ***C:\Windows\System32\cvP11.dll*** (3)

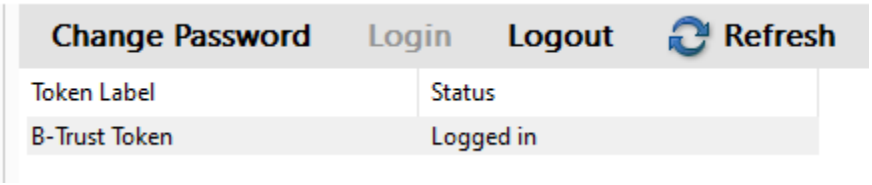
Заредената библиотека трябва да изглежда така:



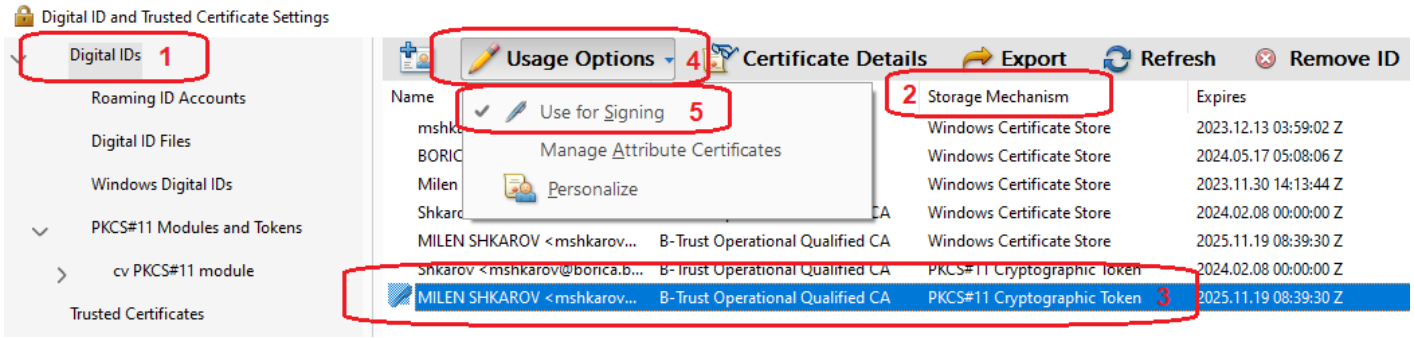
Избирате ***cv PKCS#11 modul*** (1), натискане бутона ***Login*** (2) и въвеждате ***PIN*** (3) на картата:



Статуса на token трябва да бъде ***Logged in***:



Избирате ***Digital IDs*** (1), където в списъка със сертификати трябва да имате по два еднакви сертификата, но ще се различават по място, от където се зареждат. Това се вижда в колона ***Storage Mechanism*** (2):



Избирате сертификата, с който желаете да подпишете и е от ***PKCS#11 Cryptographic Token*** – пример (3) и отваряте падащото меню ***Usage Options*** (4) и се избира ***Use for Signing*** (5). Когато е избран пред ***Use for Signing*** (5) трябва да има чек  , а в списъка преди името  .

Ако на компютърът на който работите използвате повече от един подпис с карти от тип: Siemens и CryptoVision, когато сменяте устройствата трябва избирате в ***Digital IDs*** или да се уверите, че сертификата, с който ще подписвате е отметнат  .

Затваряте ***Digital ID and Trusted Certificate Setting*** и ***Preferences*** и може преминете към подписване на нужните файлове (точка 2).