Centrul de Calcul S.A. Târgu Jiu, str. Tudor Vladimirescu, nr. 17 Tel 0253.214.767, fax 0253.213.409, Suport: 031.94.66

Web: www.certdigital.ro mail: office@certdigital.ro

Versiune: 1.1

Data: 01/02/2023

Manual de instalare, configurare și utilizare a dispozitivelor criptografice:

Longmai mToken Crypto ID

Feitian ePass2003

Cuprins

1.Informații generale 3
1.1. Accesibilitate 3
1.2. Cerințe minime 3
1.3. Cerințe recomandate 3
2. Descărcarea și instalarea driverelor dispozitivelor criptografice: 3
2.1 Dispozitivul Longmai mToken CryptoID 3
2.1.1 Sistemul de operare Windows 4
2.1.2 Sistemul de operare macOS 8
2.1.3 Schimbare cod PIN(Change user PIN) – mToken CryptoID 10
2.2 Dispozitivul Feitian ePass2003 11
2.2.1 Sistemul de operare Windows: 11
2.2.2 Sistemul de operare macOS: 12
2.2.3 Schimbare cod PIN(Change user PIN) – Feitian ePass 2003 14
3. **Configurarea dispozitivelor criptografice în Adobe Reader DC - macOS** 15
Notă finală sistem macOS 17

1. Informații generale

1.1. Accesibilitate

- ✓ Dispozitivele criptografice Longmai mToken Crypto ID/Feitian epass2003 reprezintă dispozitive securizate(de tip token) care pot stoca doar certificatul digital și cheile de securitate ale acestuia.
- ✓ Din punct de vedere tehnic nu au funcționalitatea unui stick de memorie.
- ✓ Este protejat de un cod PIN, pin pe care îl regăsiți în documentația primită în plic.
- ✓ Introducerea eronată a pinului de 10 ori consecutiv duce la blocarea dispozitivului.
- ✓ Pentru a-l debloca va trebui sa contactați autoritatea emitentă și să urmați pașii indicați de furnizor.
- ✓ Nu ștergeti fișierele stocate pe dispozitiv. În cazul ștergerii certificatului digital sau a cheilor de pe acesta este necesară achiziționarea unui nou certificat digital.

1.2. Cerințe minime

- Sistem de operare: Windows 7, Windows 8, Windows 10, Windows 11, macOS, Linux
- Memorie RAM: 1 GB
- Spațiu liber Hard Disk: 100 MB

1.3. Cerințe recomandate

- Sistem de operare: Windows 10, Windows 11, macOS, Linux
- Memorie RAM: 2 GB
- Spațiu liber Hard Disk: 100 MB

2. Descărcarea și instalarea driverelor dispozitivelor criptografice:

2.1 Dispozitivul Longmai mToken CryptoID

- Accesați următoarele linkuri sau www.certdigital.ro secțiunea Suport tehnic-Descarcă-Drivere token:

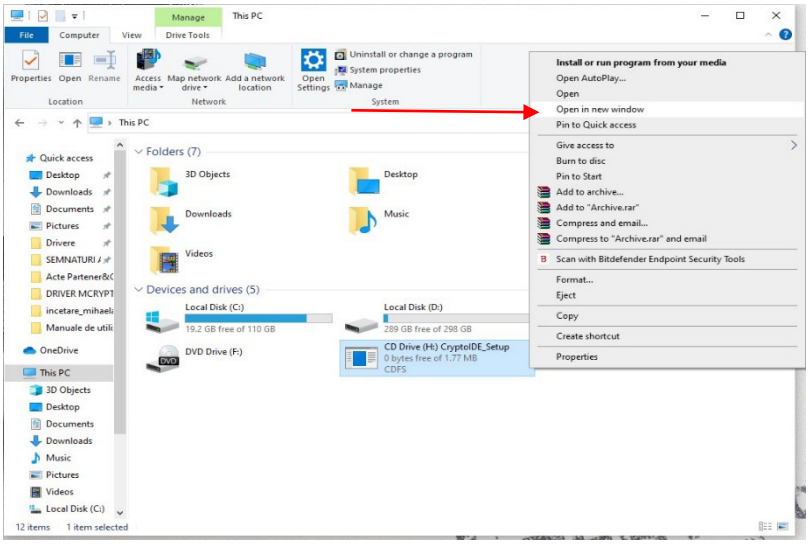
a) https://certdigital.ro/wp-content/uploads/2021/04/CertDigitalCrypto.zip (Windows)

b) https://certdigital.ro/wp-content/uploads/2021/04/mac.zip (macOS)

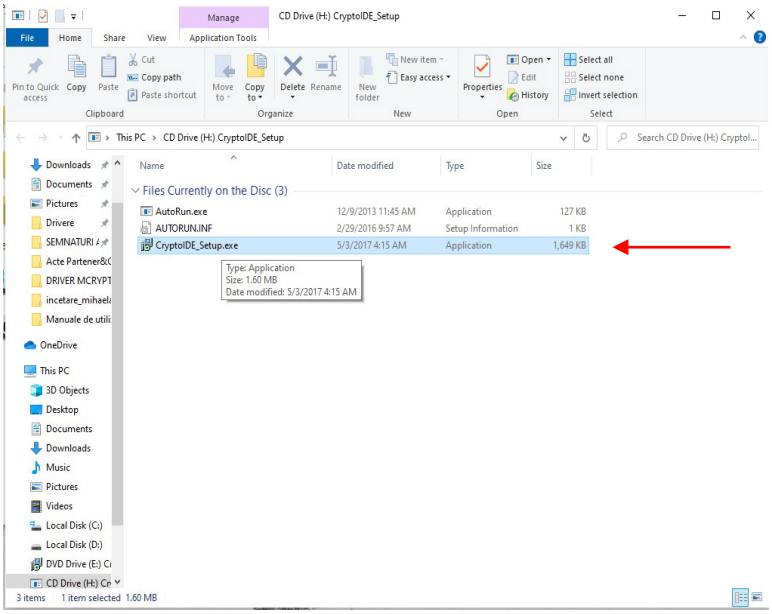
c) https://certdigital.ro/wp-content/uploads/2021/04/linux.zip (Linux)

2.1.1 Sistemul de operare Windows:

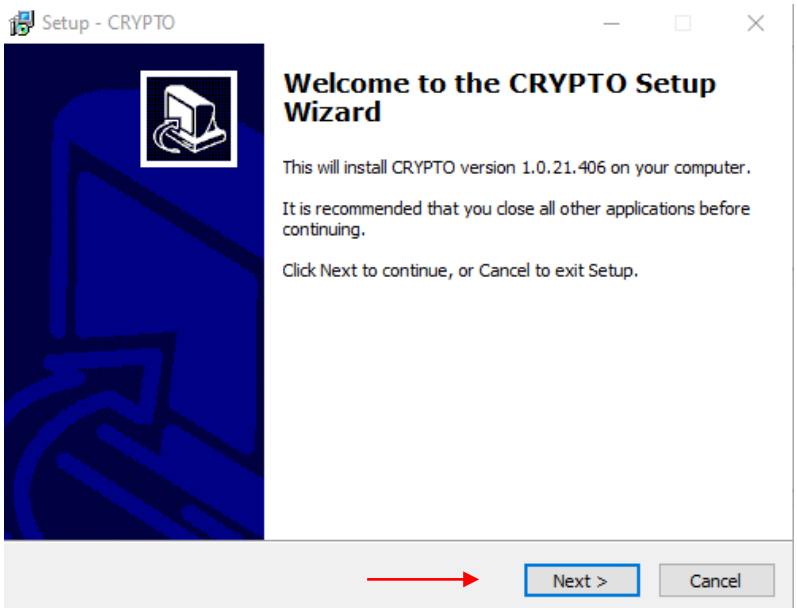
- Accesați My Computer(Computerul Meu)-Click Dreapta pe CD Drive CryptoIDE Setup-Open in New Window(Deschidere într-o fereastră nouă) sau accesați fișierul .exe din arhiva descarcată:



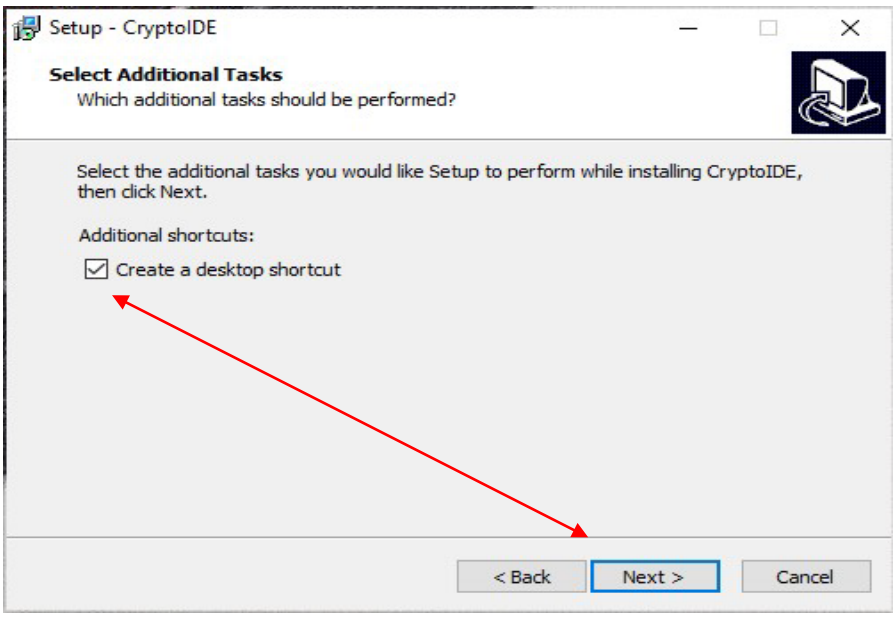
- Dublu Click pe **CryptoIDE_setup.exe/CertDigitalCrypto.exe**



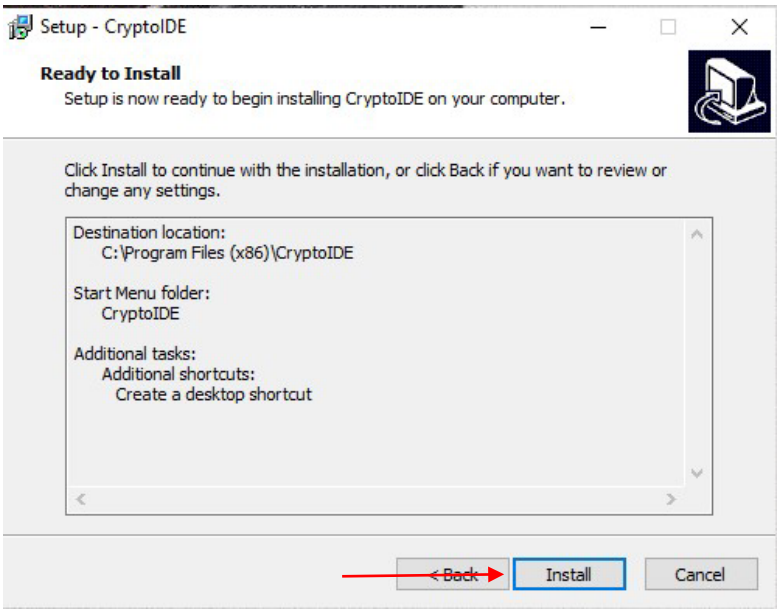
- **Next** până va apărea butonul **Install**:



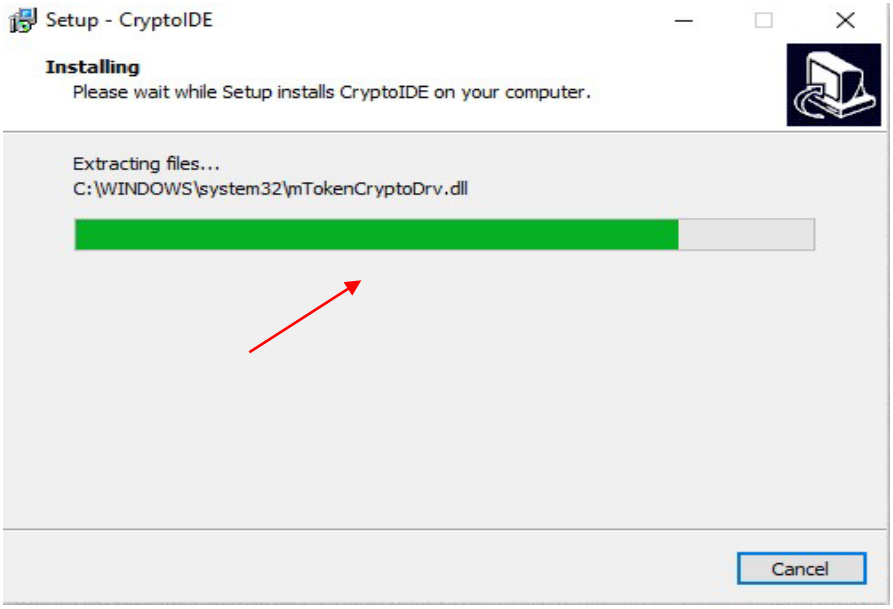
- Aveți posibilitatea de a selecta dacă va crea scurtătura a utilitarului pe Desktop.



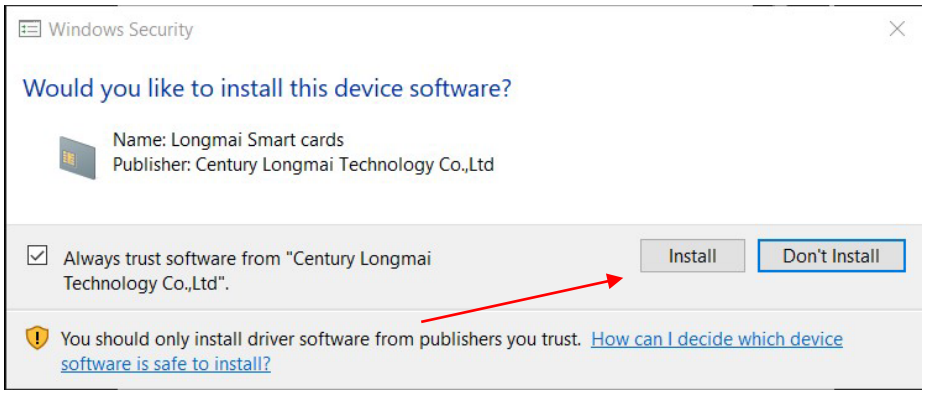
- Click **Install**:



- Vi se va afișa progresul instalării:



- Veți primi o solicitare de Securitate Windows pentru actualizarea serviciului Smartcard(Card Inteligent) și veți permite acest lucru bifând “Always trust software from….” și **Install**:

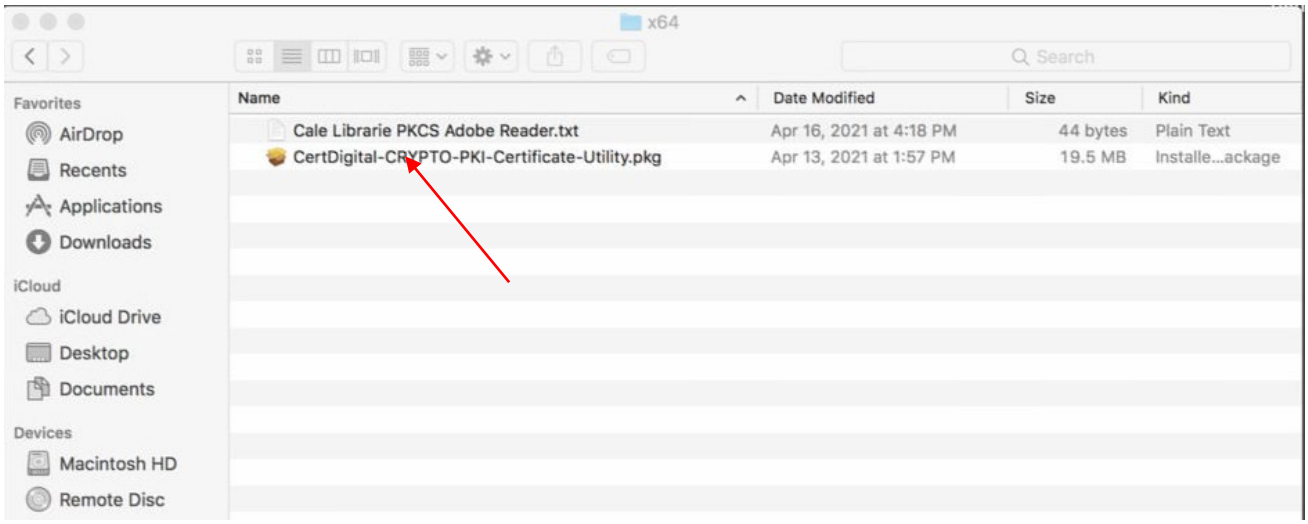


- Click **Finish/Finalizare**:

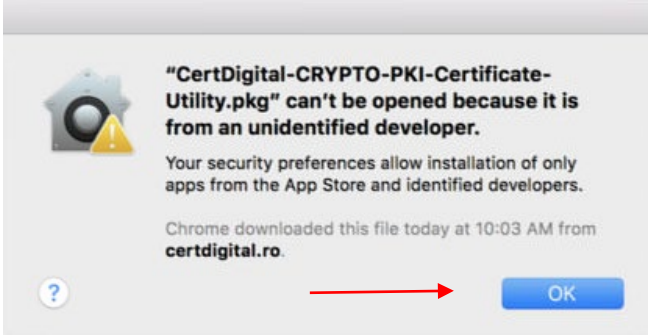
***Este recomandat ca după instalarea Dispozitivului Criptografic să reporniți stația de lucru PC/Laptop astfel încât să se asigure o funcționare corectă de la prima utilizare.

2.1.2 Sistemul de operare macOS

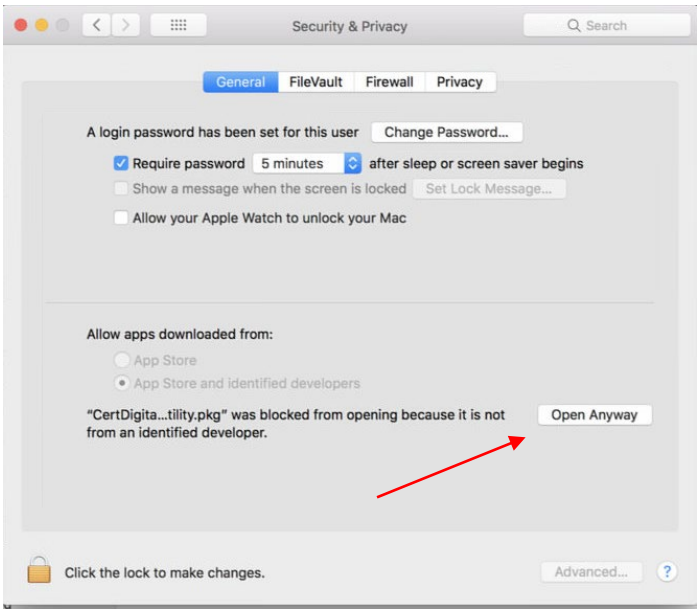
- Accesați fișierul descărcat și dezarhivat din dosarul x64 ”CertDigital-CRYPTO-PKI-Certificate-Utility.pkg”



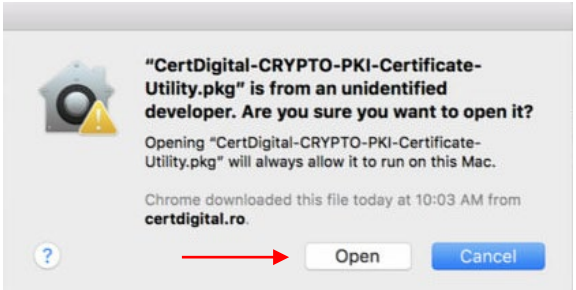
- Veți primi notificare că fișierul nu poate fi deschis pentru că este furnizat de către un dezvoltator necunoscut. Click OK.



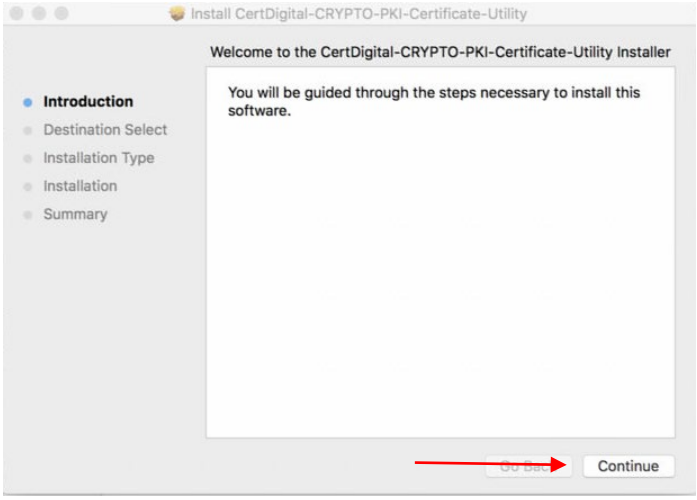
- Accesați System Preferences(Preferințe Sistem)-Security&Privacy(Securitate și Intimitate), click Open Anyway(Deschide Oricum).

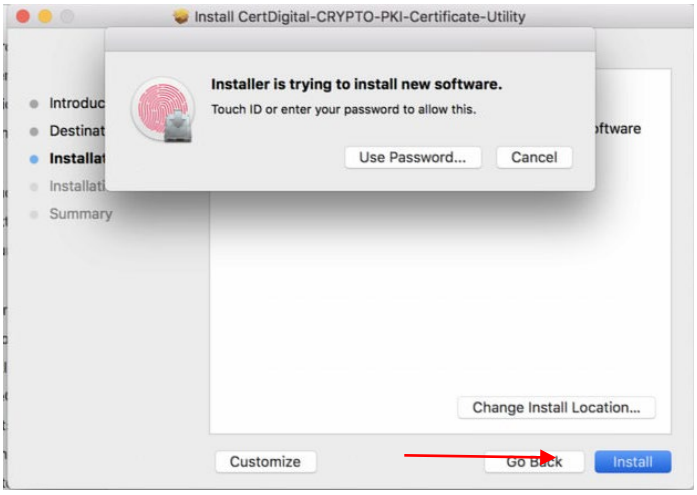


- Veți primi notificare că fișierul nu poate fi deschis pentru că este furnizat de către un dezvoltator necunoscut - Ești sigur că vrei să îl deschizi? Click Open(Deschide).



- Continuați cu instalarea driverului click Continue(continuă), introduceți parola dispozitivului dvs. și click Install(Instalează).





2.1.3 Schimbare cod PIN(Change user PIN) – mToken CryptoID

Dispozitivul cryptografic are atașată fișa cu datele de securitate(cod PIN de utilizator, cod de deblocare SO PIN) sub această formă:

CERTDIGITAL semnează sigur

Centrul de Calcul S.A. Târgu Jiu, str. Tudor Vladimirescu, nr. 17 Tel 031.94.66, fax 0253.213.409
Web: www.certdigital.ro, mail:office@certdigital.ro

Stimate client,

Vă mulțumim că ați achiziționat certficatul digital calificat CertDigital!

Codul PIN de utilizator aferent token-ului (Dispozitiv securizat pentru crearea semnăturii) dumneavoastră este: **rdmTXTBp**

Codul de deblocare (SO PIN) aferent token-ului dumneavoastră este: **unlKtcEN**

Număr Serial dispozitiv : 940359443868BP527

Introducerea eronată a codului PIN pentru dispozitivul mToken Crypto ID de mai mult de 10 ori consecutiv duce la blocarea codului PIN. Deblocarea se poate realiza dacă se introduce codul SO PIN.

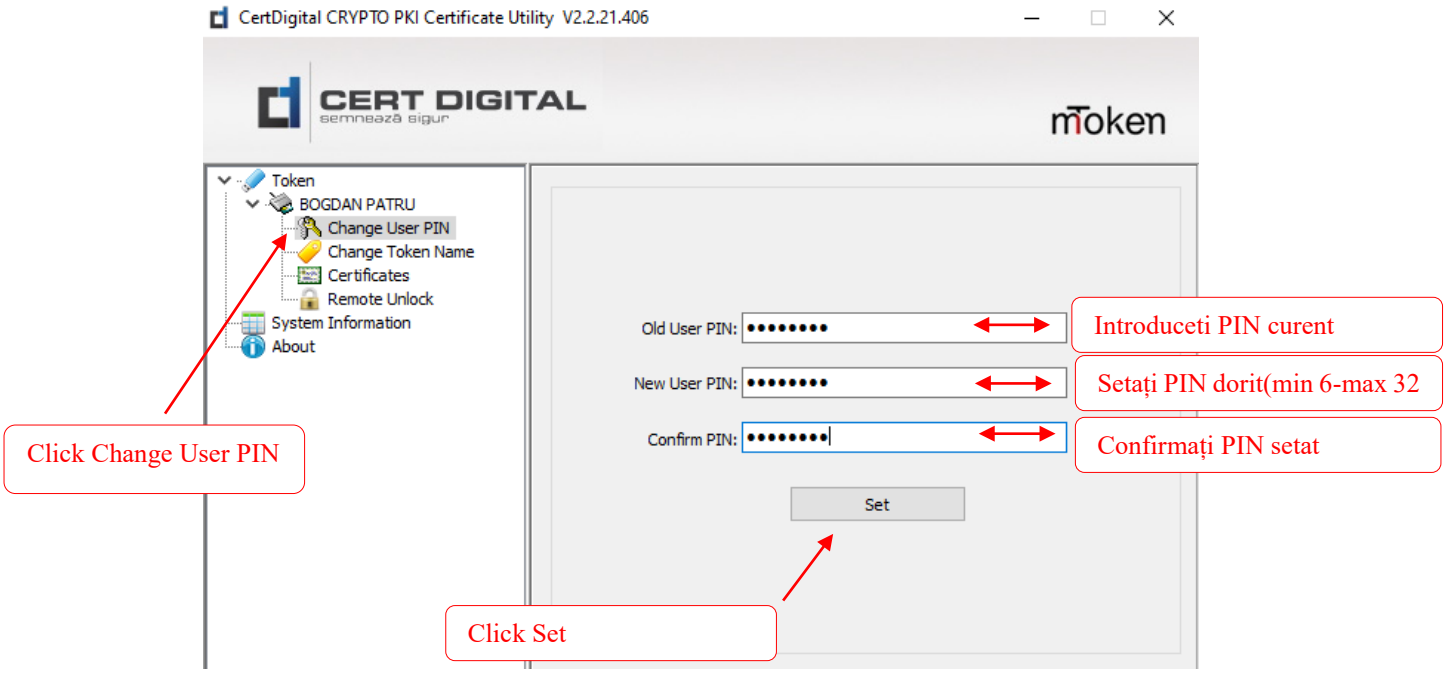
Introducerea eronată a codului PUK pentru dispozitivul mToken Crypto ID de mai mult de 10 ori consecutiv duce la blocarea token-ului și implicit a certificatului calificat. În cazul blocării dispozitivului este necesară achiziționarea unui nou certificat calificat și a unui nou dispozitiv.

Pentru informații suplimentare privind utilizarea certificatului digital calificat accesați site-ul www.certdigital.ro.

Codul PIN pentru utilizarea dispozitivului.

Codul SO PIN pentru deblocarea dispozitivului – Procedură efectuată doar de Autoritatea de certificare.

Deschideți aplicația **mToken CryptoID**:



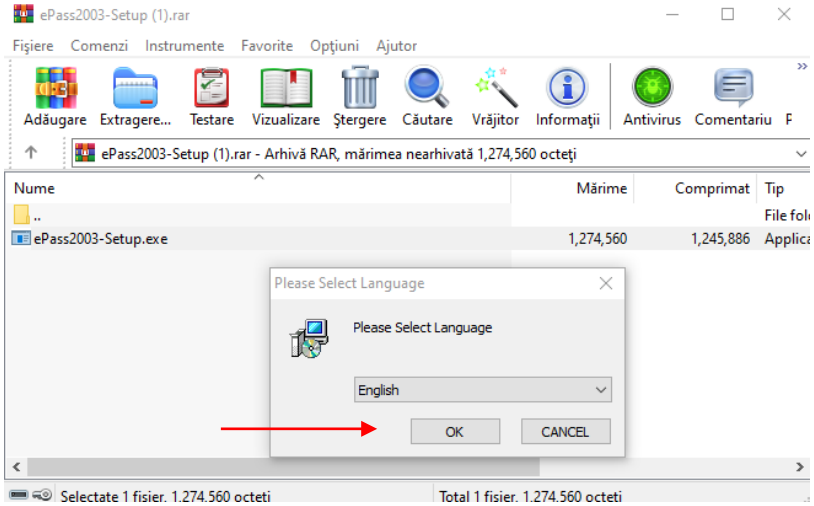
2.2 Dispozitivul Feitian ePass2003 – Accesați următoarele linkuri sau www.certdigital.ro secțiunea Suport tehnic - Descarcă-Drivere token:

a) https://certdigital.ro/wp-content/uploads/2021/05/ePass2003-Setup.rar (Windows)

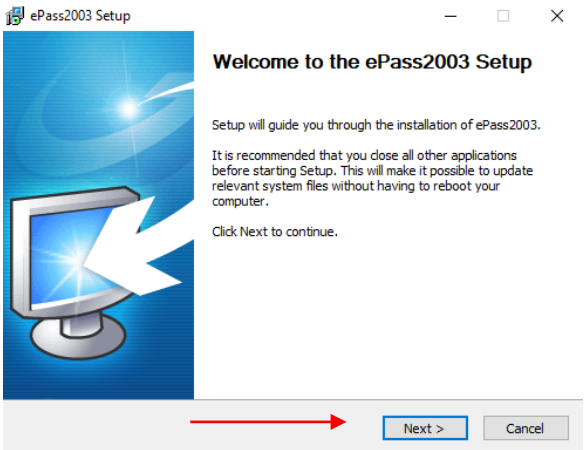
b) https://certdigital.ro/wp-content/uploads/2022/01/ePass2003-Castle-mac-20211111.rar (macOS)

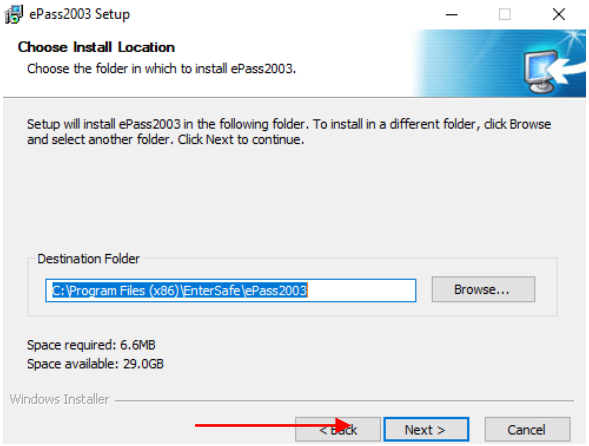
2.2.1 Sistemul de operare Windows:

- Deschideți arhiva descărcată și rulati fișierul ePass2003-Setup.exe.
- Click OK.

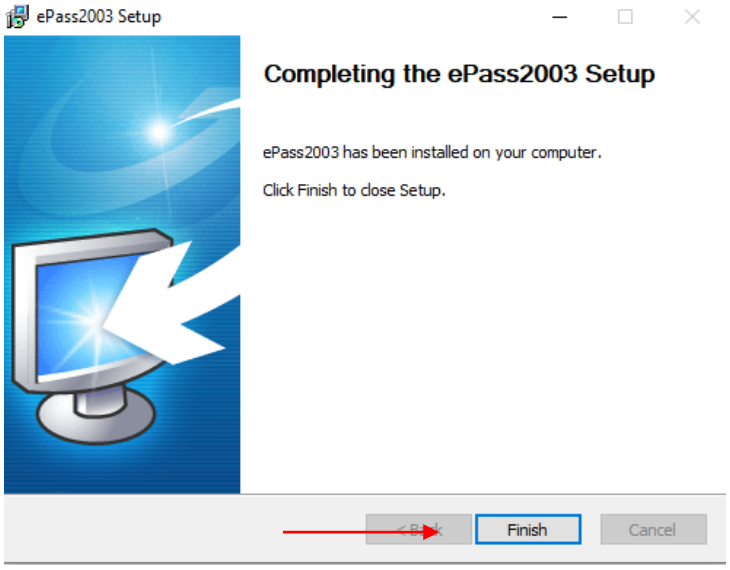


- Click Next(Următorul) pentru instalare.





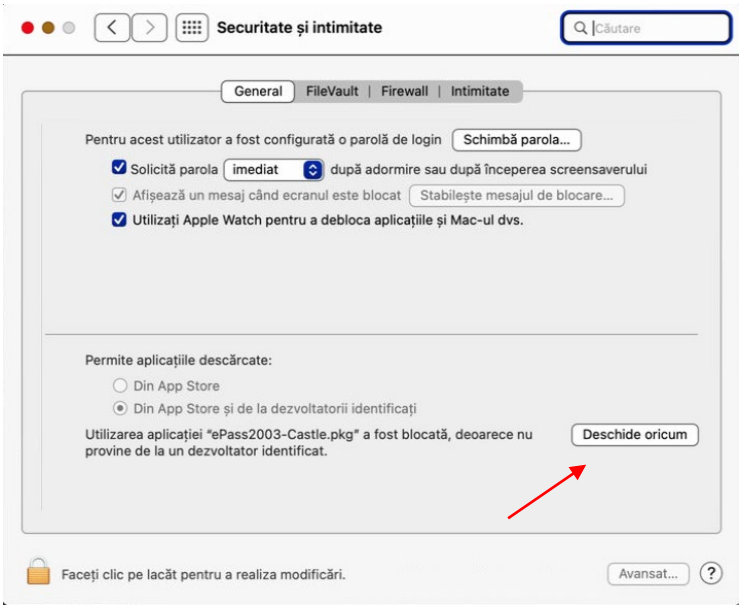
- Click Finish(Finalizare) pentru a încheia instalarea.



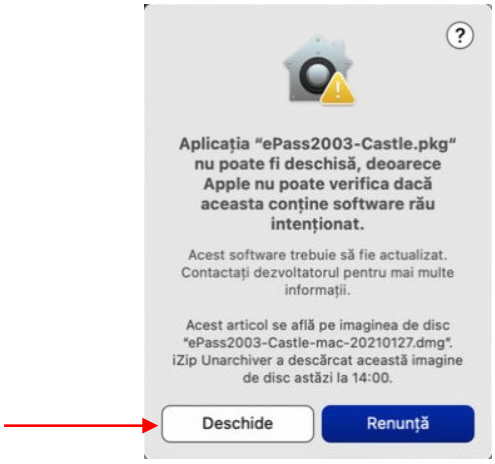
2.2.2 Sistemul de operare macOS:

- Deschideți fișierul ePass2003-Castle.pkg din arhiva descărcată:

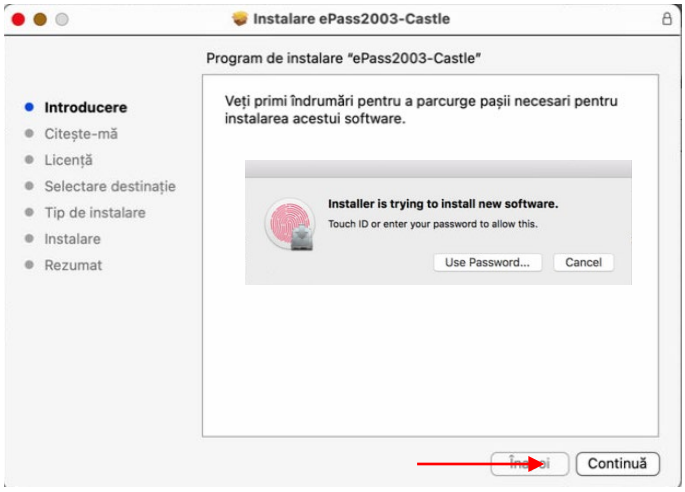
- Veți primi notificare că fișierul nu poate fi deschis pentru că este furnizat de către un dezvoltator necunoscut - Click OK.
- Accesați System Preferences(Preferințe Sistem) Security&Privacy(Securitate și Intimitate), click Open Anyway(Deschide Oricum).

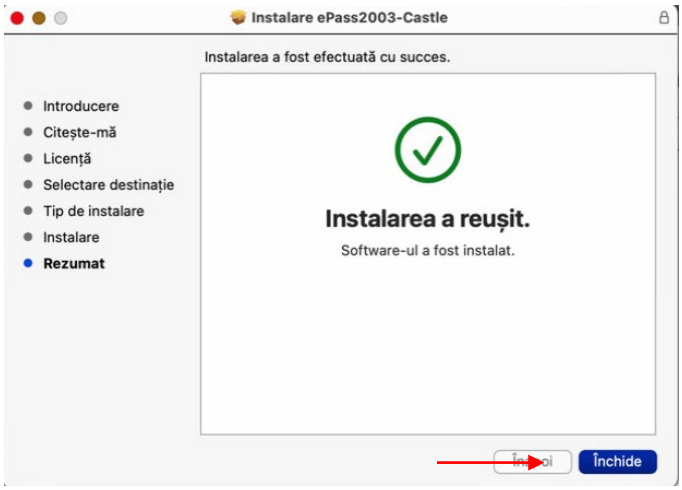


- Veți primi notificare că fișierul nu poate fi deschis pentru că este furnizat de către un dezvoltator necunoscut.
- Click Open(Deschide).



- Continuați cu instalarea driverului click Continue(continuă), introduceți parola dispozitivului dvs. și click Install(Instalează) și Close(Închide).





2.2.3 Schimbare cod PIN(Change user PIN) – Feitian ePass 2003

Dispozitivul cryptografic are atașată fișa cu datele de securitate(cod PIN de utilizator, cod de deblocare SO PIN) sub această formă:

CERTDIGITAL semnează sigur

Centrul de Calcul S.A. Târgu Jiu, str. Tudor Vladimirescu, nr. 17 Tel 031.94.66, fax 0253.213.409
Web: www.certdigital.ro, mail:office@certdigital.ro

Stimate client,

Vă mulțumim că ați achiziționat certficatul digital calificat CertDigital!

Codul PIN de utilizator aferent token-ului (Dispozitiv securizat pentru crearea semnăturii) dumneavoastră este: **rDmTxTbp**

Codul PIN pentru utilizarea dispozitivului.

Codul de deblocare (SO PIN) aferent token-ului dumneavoastră este: **unLKtcEn**

Număr Serial dispozitiv : 2C2513900070029

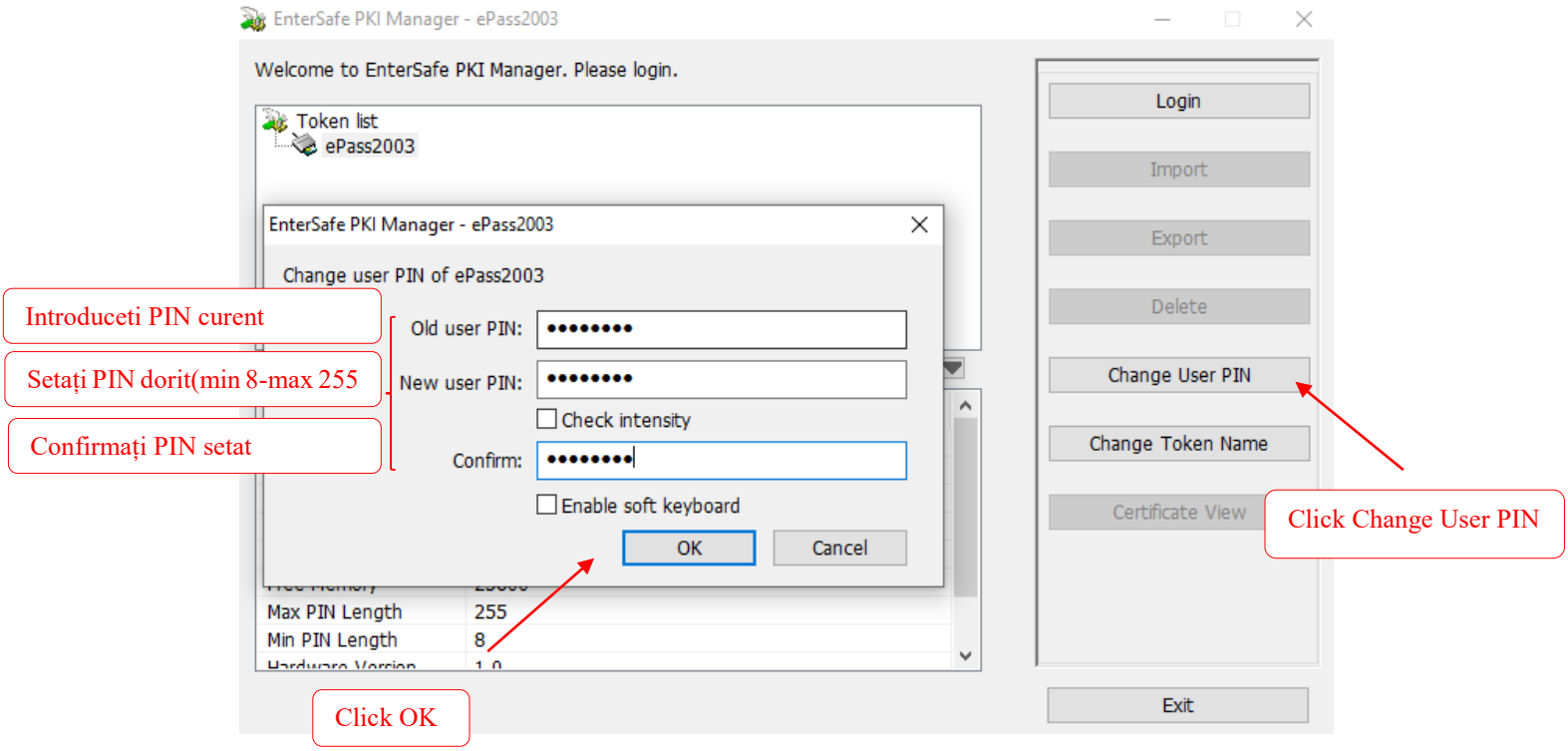
Introducerea eronată a codului PIN pentru dispozitivul mToken Crypto ID de mai mult de 10 ori consecutiv duce la blocarea codului PIN. Deblocarea se poate realiza dacă se introduce codul SO PIN.

Introducerea eronată a codului PUK pentru dispozitivul mToken Crypto ID de mai mult de 10 ori consecutiv duce la blocarea token-ului și implicit a certificatului calificat. În cazul blocării dispozitivului este necesară achiziționarea unui nou certificat calificat și a unui nou dispozitiv.

Codul SO PIN pentru deblocarea dispozitivului – Procedură efectuată doar de Autoritatea de certificare.

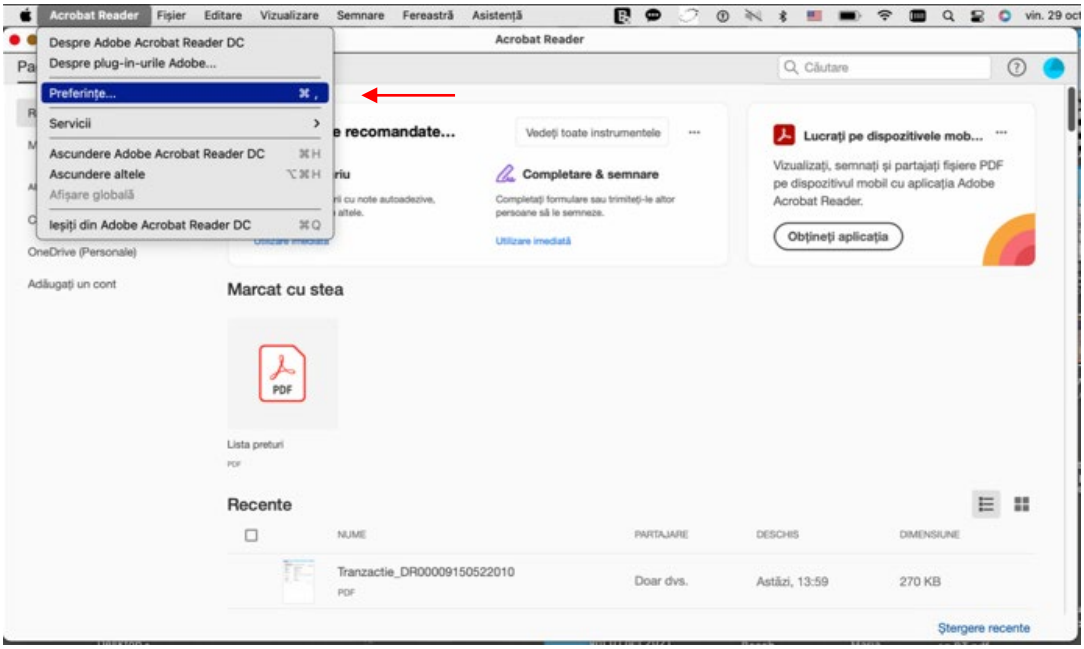
Pentru informații suplimentare privind utilizarea certificatului digital calificat accesați site-ul www.certdigital.ro.

Deschideți aplicația **ePass2003 Token Manager**:

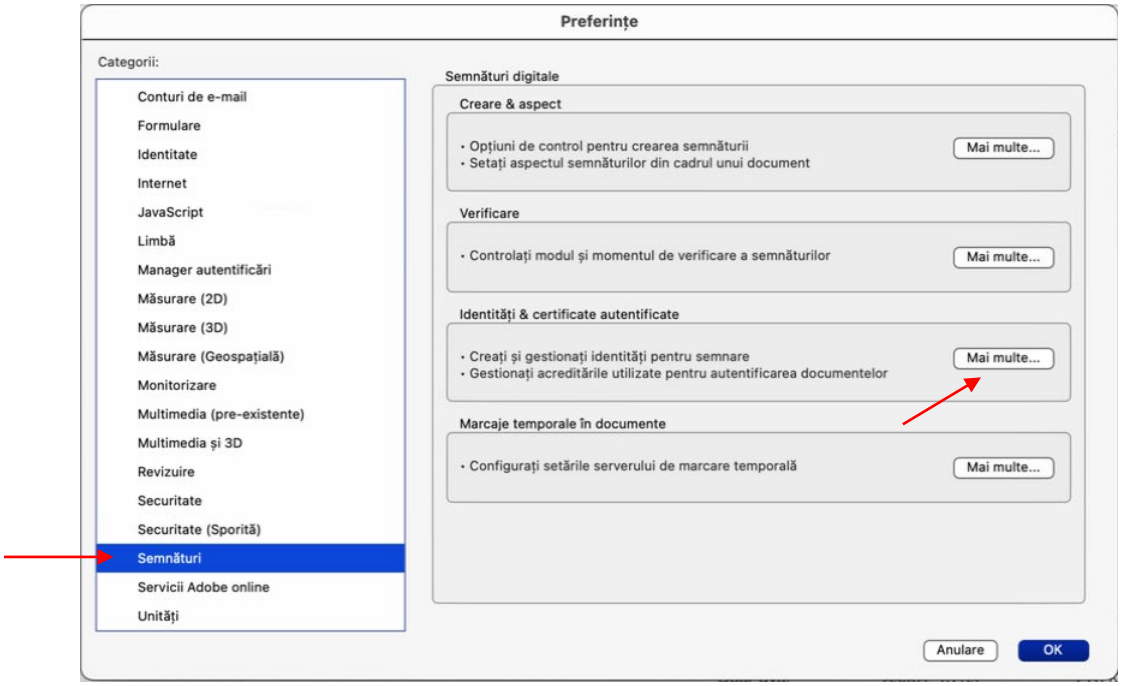


3. Configurarea dispozitivelor criptografice în Adobe Reader DC - macOS

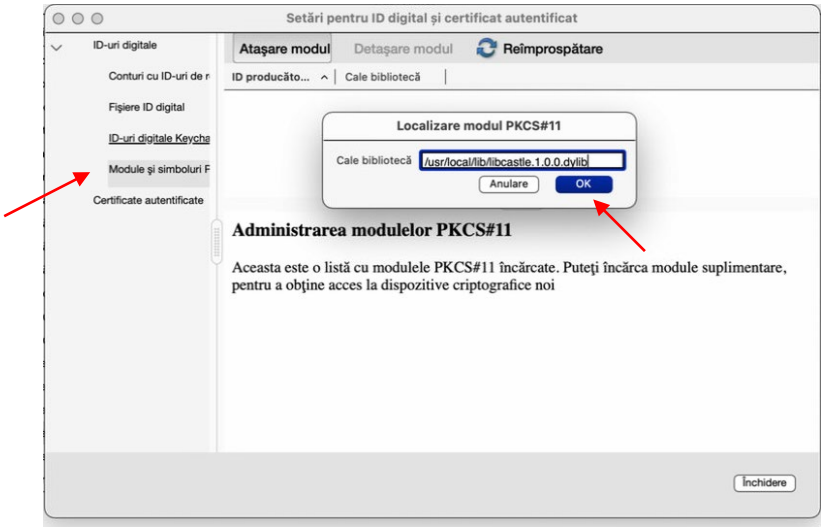
- Deschideți aplicația Adobe Acrobat Reader-Preferences(Preferințe).



- Click Signatures(Semnături)-Identities&Trusted certificates-More(Mai multe).



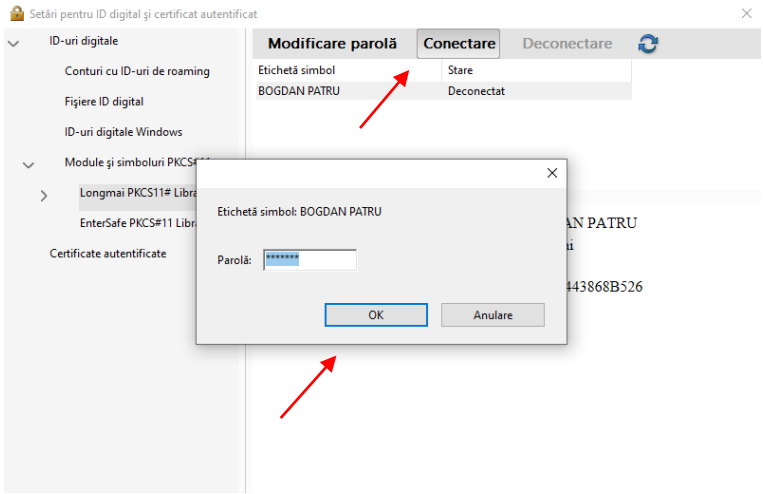
- Click Modules and symbols PKCS#11(Module și simboluri PCKS#11)-Attach module(Atașare modul) și copiați calea pentru a obține acces la dispozitivul criptografic – Click OK.

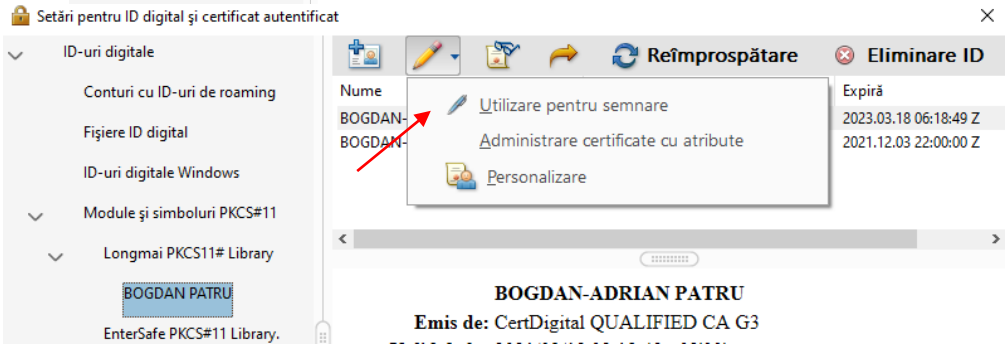


➢ Pentru Longmai mToken CryptoID calea pentru localizarea modulului este: /opt/CryptoIDE/lib/libcryptoide_pkcs11.dylib

➢ Pentru Feitian ePass2003 calea pentru localizarea modulului este: /usr/local/lib/libcastle.1.0.0.dylib

- Click Connect(Conectare), introduceți PIN numeric - click OK - selectați certificatul valid-Click Use for signing(Utilizare pentru semnare).





Notă finală sistem macOS

- ✓ Sistemul de operare **Mac** gestionează diferit de **Windows** dispozitivul criptografic:
- ✓ Introduce tokenul în stand-by dacă nu este utilizat o perioadă de timp.
- ✓ La reluarea activității trebuie să închideți toate aplicațiile care folosesc dispozitivul(Acrobat Reader, browser, CDP Client), scoateți, reintroduceți tokenul și reluați procedura de semnare dorită.
- ✓ La semnarea în Acrobat Reader cu ajutorul librăriei criptografice este recomandat când terminați procedura de semnare să închideți Acrobat Reader din bara de lansare rapidă(Quick Launch) – click dreapta- Quit și abia apoi să scoateți tokenul din portul usb.