MoldSign Desktop Suite

Ghidul utilizatorului

Instituția Publică

”Serviciul Tehnologia Informației

și Securitate Cibernetică”

Conținut

1 Introducere

Produsul asociat semnăturii electronice MoldSign Desktop Suite este un mijloc de program (*program*) ce permite aplicarea semnăturii electronice avansată calificată pe informația în format electronic (*.pdf, *.doc, *.png, *jpg, *.txt, etc) utilizînd dispozitivul securizat de creare a semnăturii electronice (*dispozitiv*), verificarea autenticității semnăturii electronice avansată calificată, criptarea/decriptarea cu parolă a fișierului și ștergerea securizată (ireversibilă) a fișierului de pe calculator. Acest program corespunde prevederilor cadrului normativ în domeniul semnăturii electronice, și anume:

- Legea nr. 91/2014 *privind semnătura electronică și documentul electronic*,
- *Normele tehnice în domeniul semnăturii electronice avansate calificate*, aprobate prin Ordinul directorului Serviciului de Informaţii şi Securitate nr. 69/2016,
- SMV CWA 14170:2008 *Cerințe de securitate pentru aplicațiile de creare a semnăturii*,
- SMV CWA 14171:2008 *Ghid general pentru verificarea semnăturii electronice*.
- IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 5816 ESSCertIDv2 Update for RFC 3161,
- IETF RFC 5905: Network Time Protokol Version 4: Protocol and Algoritms Specification,
- IETF RFC 3029 Data Validation and Certification Server Protocols (DVCS).

2 Cerințe tehnice

Programul MoldSign Desktop Suite poate fi utilizat de către calculatoarele ce satisfac următoarele cerințe:

- sistem de operare Windows Vista/7/8/8.1/10, Windows Server 2008/2012/2016, MacOS sau Linux;
- minim 200MB spațiu disponibil pe disc;
- conexiune Internet.

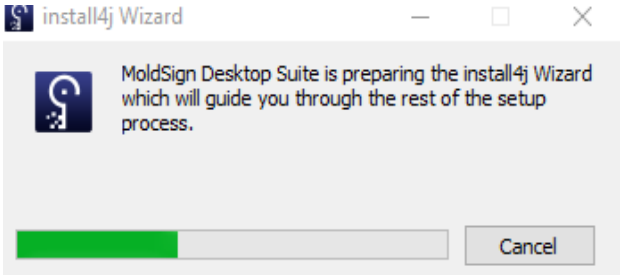
NOTĂ: Din motive de securitate, sistemele de operare vechi (e.g., Windows XP) categoric nu sunt recomandate, însă, MoldSign Desktop Suite funcționează pe acestea.

3 MoldSign Desktop Suite pentru SO Windows

3.1 Instalare, setare

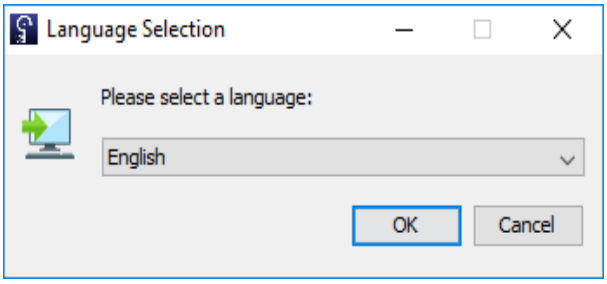
Accesați https://semnatura.md/ și descărcați programul MoldSign Desktop Suite. Instalarea este demarată prin lansarea fișierului de instalare MoldSign_Last.exe.

După aceea, începe instalarea programului.

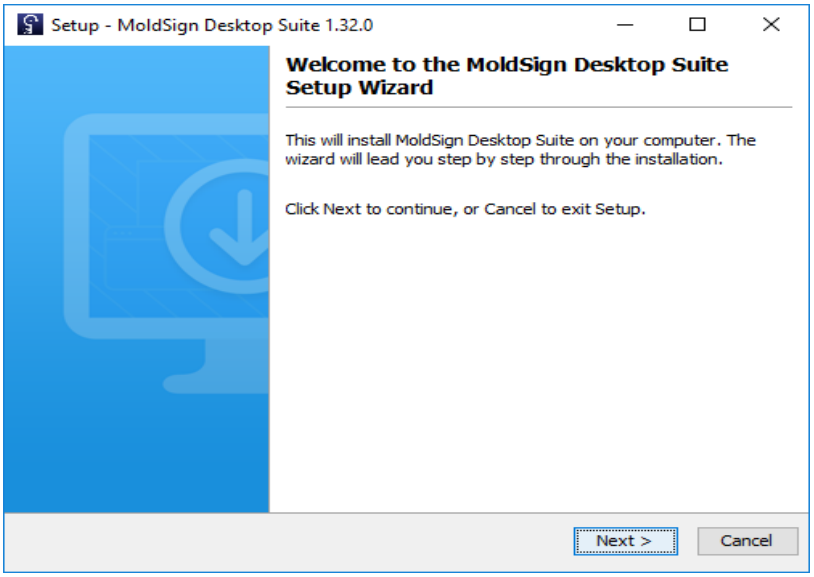


Fișierul de instalare pregătește toți pașii necesari pentru instalarea programului.

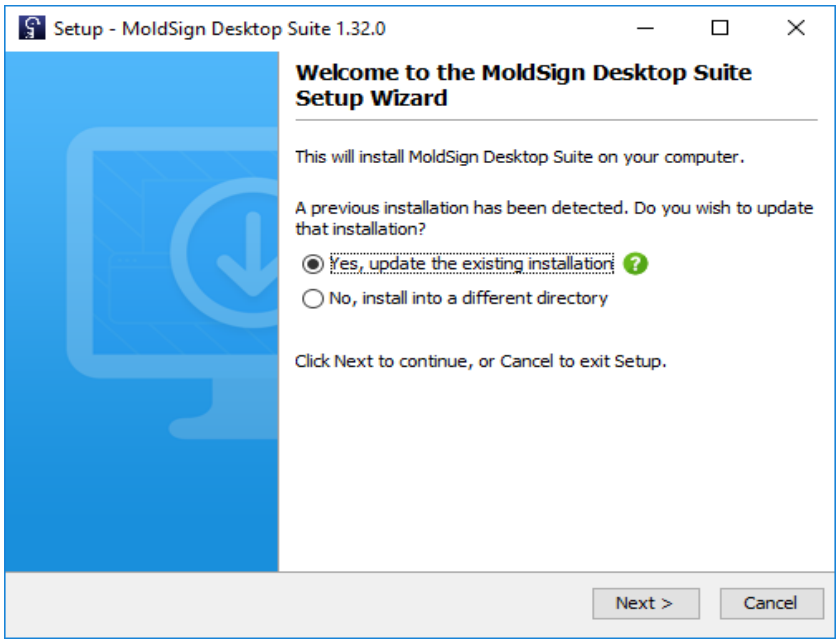
Selectați limba în care doriți să instalați programul, apoi apăsați **OK**.



Demarează procesul de instalare efectivă a programului. Apăsați pe butonul **Next** (**Următorul**).

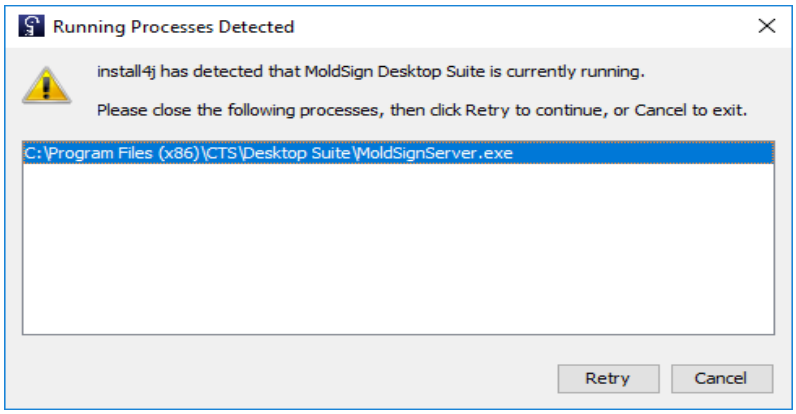


NOTĂ: în cazul actualizării programului MoldSign Desktop Suite (fără a dezinstala versiunea deja existentă pe calculator) va apărea fereastra



în care bifați **Yes, update the existing installation**, apoi apăsați butonul **Next** (**Următorul**). Dacă aplicația MoldSign Server nu a fost dezactivată anterior procesului de actualizare a programului MoldSign Desktop Suite, adică în bara de lucru zona „tray” este prezentă

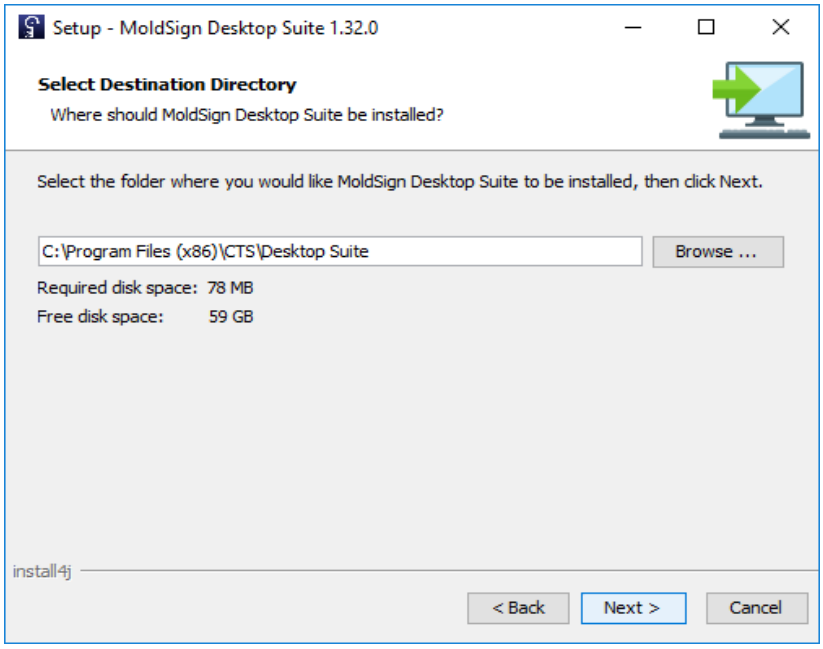
veți primi mesajul



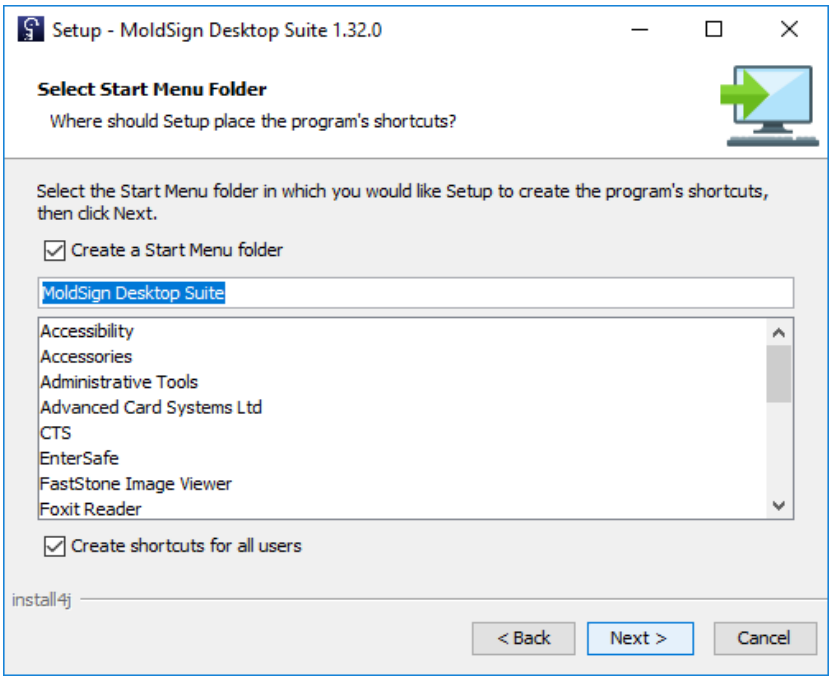
Faceți click dreapta pe și selectați **Exit** (**Ieșire**), apoi apăsați **Retry** (**Reîncearcă**).

Fișierul de instalare ne înștiințează în legătură cu locația în care va instala programul. Recomandăm să nu schimbați directorul **Destination Directory** (**Director Destinație**), ci să mergeți mai departe apăsând butonul **Next** (**Următorul**).

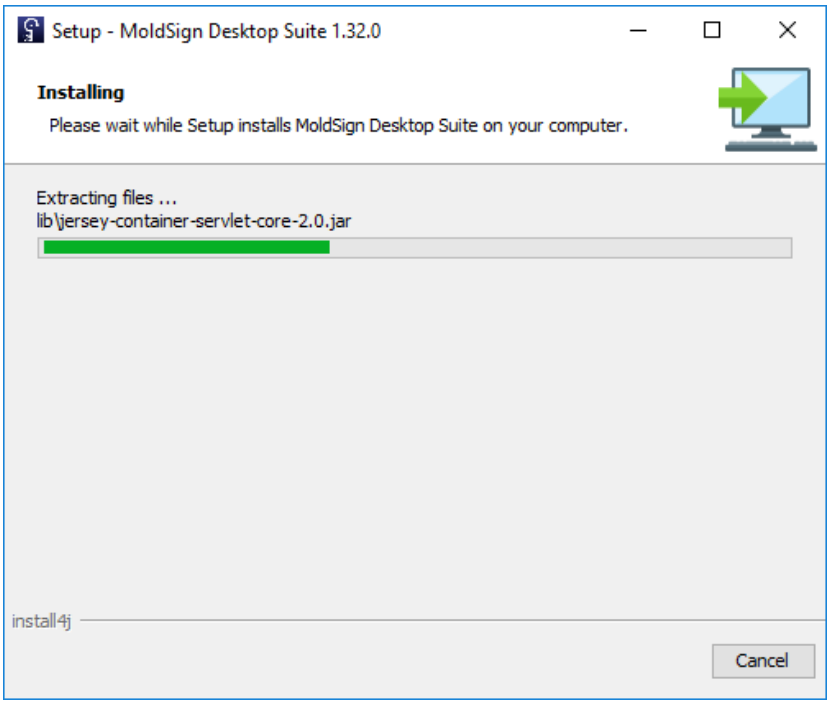
NOTĂ: Destination Directory (Director Destinație) poate fi schimbat doar dacă nu aveți suficient spațiu liber disponibil pe hard diskuri.



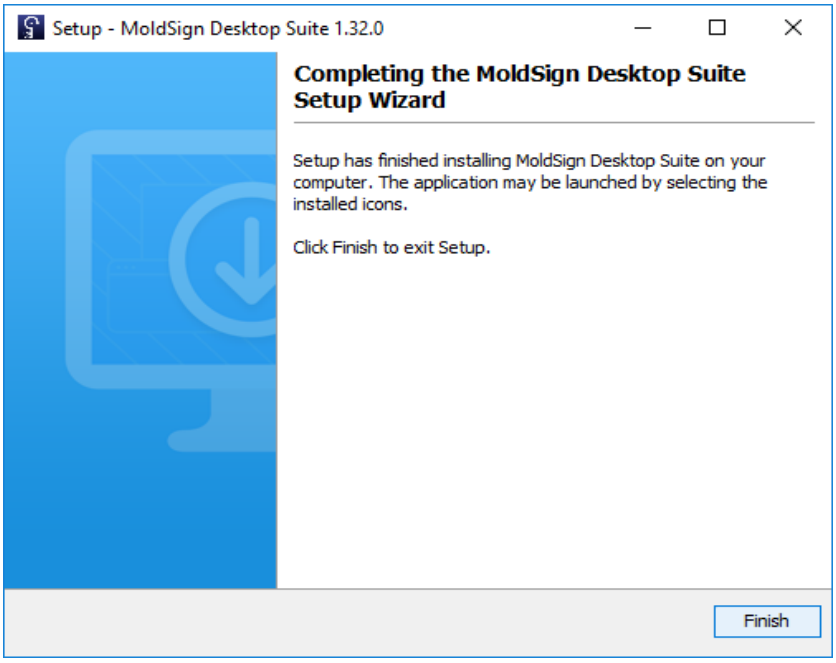
Sunteți întrebat unde doriți să fie plasate scurtăturile (shortcuts) programului. Recomandăm să nu schimbați nimic din setări, iar apoi să apăsați pe butonul **Next** (**Următorul**).



Procesul de instalare continuă prin copierea programului din fișierul de instalare pe calculator. Vă rugam să așteptați finalizarea acestei operațiuni.

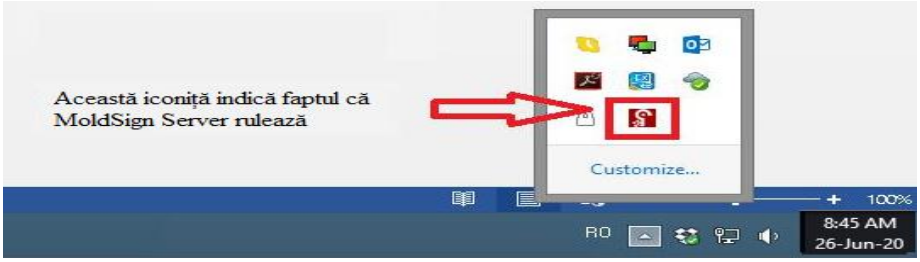


Fereastra de mai jos arată că procesul de instalare s-a finalizat cu succes și, după apăsarea butonului **Finish** (**Finalizare**), puteți utiliza programul MoldSign Desktop Suite.



După finalizarea cu succes a procesului de instalare vi se cere să reporniți calculatorul. Reporniți-l.

La pornirea calculatorului, în mod automat se va lansa și aplicația MoldSign Server. Acest lucru poate fi observat prin apariția iconiței pe bara de lucru în zona „tray” (colțul din dreapta jos lângă ceas).



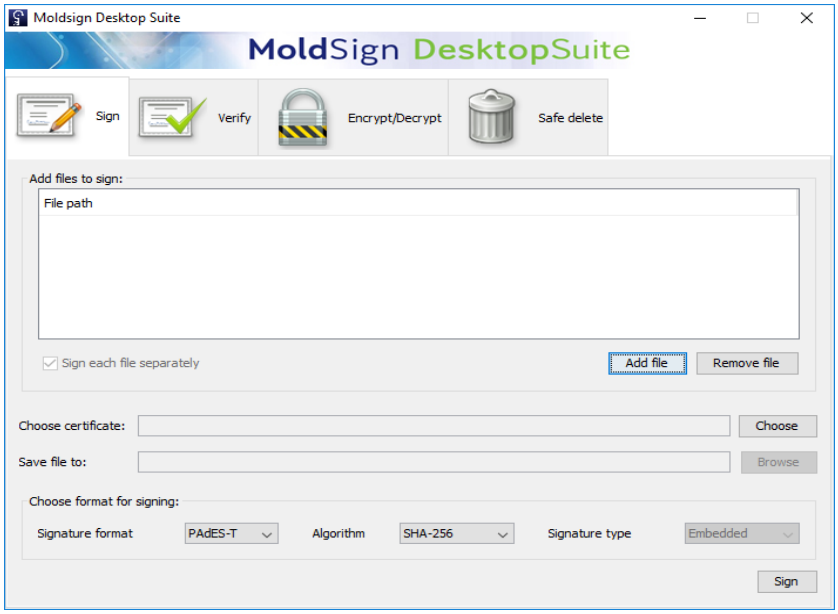
Dacă aplicația dată nu a fost lansată automat sau a fost oprită din careva motive, o puteți lansa manual accesând ***Start->All Programs->MoldSign Desktop Suite->MoldSign Server***.

Lansați aplicația MoldSign Desktop Suite urmînd calea ***Start->All Programs->MoldSign Desktop Suite->MoldSign Desktop Suite***

3.2 Semnarea fișierelor

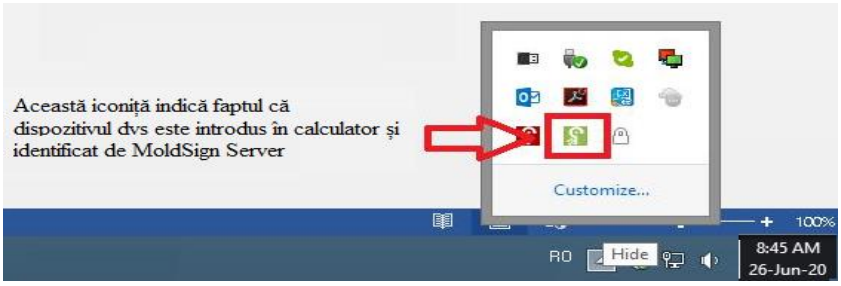
Semnarea fișierelor prin tabul **Sign (Semnați)** din meniul principal al aplicației se realizează prin executarea procesului de semnare descris mai jos:

1. adăugați fișierele ce trebuie semnate în lista de fișiere. Acest lucru poate fi realizat prin apăsarea pe butonul **Add file (Adăugați fișier),** ce va deschide o nouă fereastră pentru căutarea fișierelor în sistemul de fișiere. Există și posibilitatea introducerii în listă a fișierelor prin Drag & Drop direct din aplicația File Explorer.



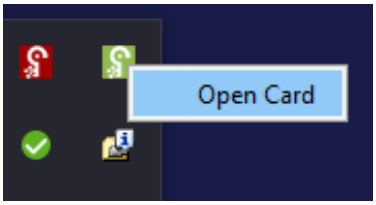
Pentru eliminarea unui fișier din listă acesta trebuie selectat, apoi apăsați pe butonul **Remove file** (**Îndepărtați fișier**).

2. introduceți în calculator dispozitivul cu care doriți să semnați și așteptați câteva secunde. La depistarea dispozitivului introdus va apărea, lângă iconița , și iconița .

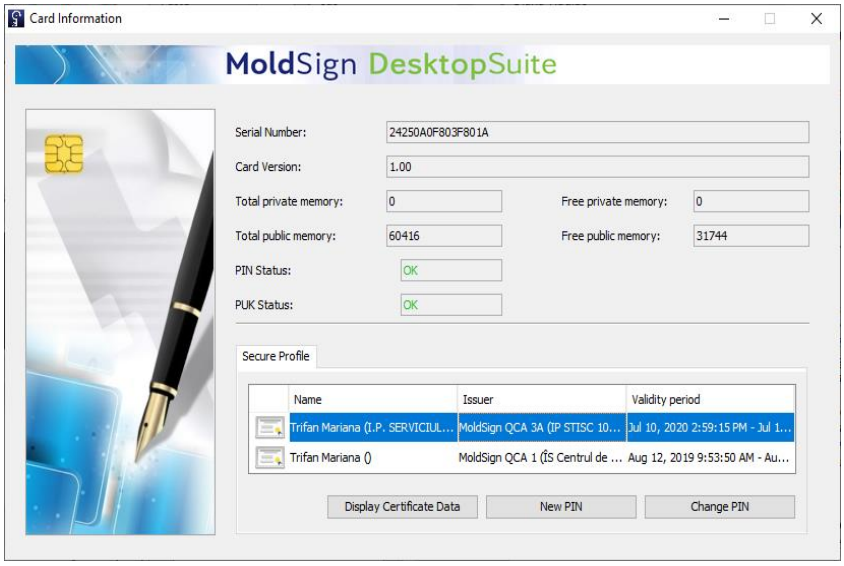


IMPORTANT! Dacă dispozitivul nu a fost identificat de aplicația MoldSign Server, adică iconița nu este prezentă, verificați dacă ați instalat driverul pentru dispozitivul utilizat (acesta poate fi descărcat de pe https://semnatura.md).

NOTĂ: pentru a vizualiza informația ce se conține pe dispozitiv faceți click dreapta pe , apoi clik pe **Open Card**



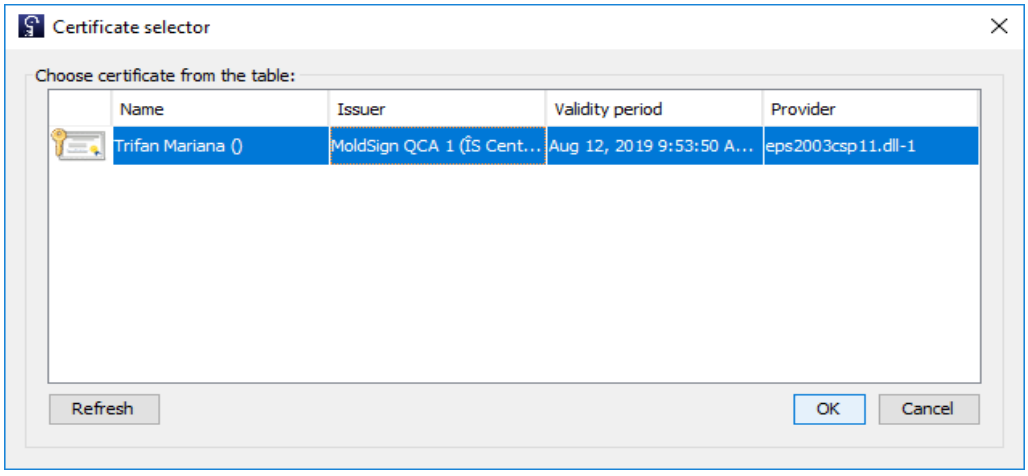
Se va deschide **Card Information**



în care puteți vizualiza conținutul certificatului cheii publice selectat (**Display Certificate Data**), atribui un PIN nou numeric (**New PIN**) sau schimba PIN-ul vechi (**Change PIN**) al dispozitivului.

Atenție! Nu introduceți mai multe dispozitive concomitent în același calculator. Dacă aveți nevoie să semnați cu mai multe dispozitive introduceți și semnați pe rând cu câte un singur dispozitiv.

3. selectați certificatul calificat al cheii publice (ce conține o cheie privată) de pe dispozitiv. Acest lucru poate fi realizat prin apăsarea butonului **Choose** (**Alegeți**), ce va deschide o nouă fereastră din care poate fi selectat certificatul (sunt afișate doar certificatele cheilor publice valide). Această acțiune este finalizată prin apăsarea pe butonul **OK.**



4. selectați formatul și tipul de semnătură. Sunt disponibile următoarele formate:

PAdES - semnătura fișierelor pdf;

PAdES-T - semnătura fișierelor pdf ce include și un marcaj temporal din partea unui server autorizat pentru marcare temporală;

XAdES-BES – semnătură de bază în format XML;

XAdES-T – semnătură de bază cu marcaj temporal adițional din partea unui server autorizat pentru marcare temporală;

XAdES-C – XAdES-T cu statut adițional al certificatului cheii publice.

Tipul de semnătură poate fi **Detached** (**Detașată**) sau **Embedded** (**Încorporată**). Semnătura **Detached** (**Detașată**) presupune existența unui fișier separat ce conține semnătura pentru unul sau mai multe fișiere; în timp ce, semnătura **Embedded** (**Încorporată**) presupune că atât fișierul semnat, cât și semnătura sunt localizate în cadrul aceluiași fișier.

În cazul semnăturilor fișierelor pdf (**PAdES**, **PAdES-T**) este aplicabil doar tipul **Embedded** (**Încorporată**).

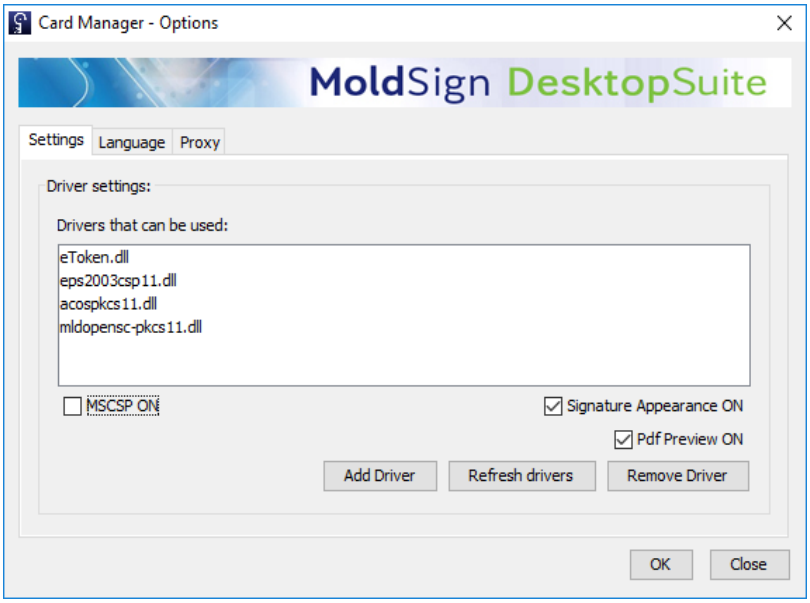
Pentru formatul **XAdES** sunt disponibile ambele tipuri, însă, pentru limitarea consumului de resurse, formatul **Embedded** (**Încorporată**) este disponibil numai pentru fișiere mai mici de 100KB.

În anumite cazuri (când semnătura este în formatul **XAdES** și de tip **Detached** (**Detașată**) pot fi semnate mai multe fișiere cu un singur fișier de semnătură. Această semnătură este realizată dacă debifați opțiunea **Sign each file separately** (**Fiecare fișier separat**). În acest caz, selectați numele și locația fișierului de semnătură.

Altfel, fișierele sunt salvate prin adăugarea automată a extensiei **.xades** la sfârșitul numelui fișierului (pentru formatele de semnătură **XAdES**), sau prin adăugarea **.signed** în fața extensiei **.pdf** (pentru formate de semnătură **PAdES**).

5. După finalizarea pașilor descriși mai sus, apăsați pe butonul **Sign** (**Semnați)** pentru a realiza procesul de aplicare a semnăturii.

NOTĂ: în cazul fișierelor pdf aveți posibilitatea de a alege poziționarea semnăturii în raport cu paginile documentului ce urmează a fi semnat și localizarea acesteia pe pagina selectată. Pentru aceasta, după lansarea aplicației MoldSign Server, faceți click dreapta pe  și selectați **Options** (**Opțiuni**). Se va deschide fereastra

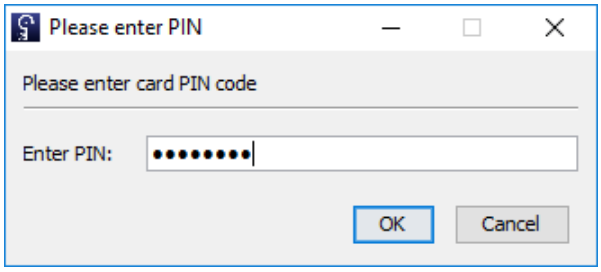


în care puteți bifa/debifa opțiunile **Signature Apperance ON** (**Apariția semnăturii pe**) și **Pdf Preview ON** (**Previzualizarea semnăturii pe**).

Pdf Preview ON se activează doar în cazul bifării opțiunii **Signature Apperance ON.**

Dacă bifați **Pdf Preview ON** veți previzualiza poziționarea semnăturii în document, apoi veți apăsa butonul **Accept**; în caz contrar nu veți previzualiza poziționarea semnăturii în document și semnătura va fi poziționată în coltul din stînga jos pe prima pagină a documentului.

Introduceți codul PIN al dispozitivului. Dacă codul PIN este corect, fișierele vor fi semnate.



După ce operațiunea este finalizată, toate fișierele care au fost semnate cu succes vor fi eliminate din lista fișierelor ce trebuie semnate.

3.3 Verificarea semnăturilor XAdES

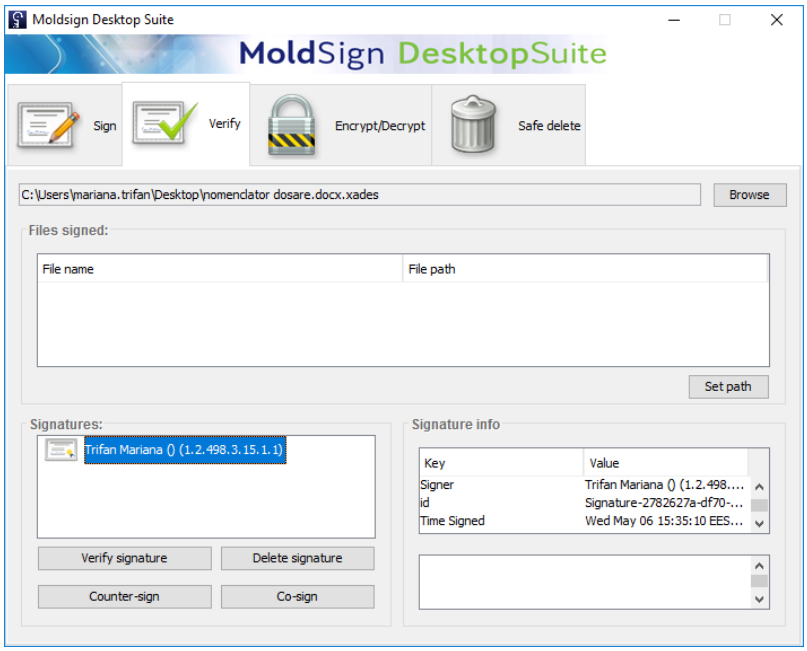
Semnăturile pot fi verificate prin tabul **Verify** (**Verifică**). Pentru aceasta selectați fișierul ce trebuie verificat. Atunci când alegeți un fișier valid XAdES restul câmpurilor din fereastră vor fi completate cu date:

- **Files signed** (**Fișiere semnate**) – fișierele care au fost semnate cu fișierul de

semnătură selectat. Prima coloană afișează numele fișierelor ce au fost semnate, în timp ce a doua coloană prezintă calea completă a acestui fișier pe calculatorul dvs. Dacă fișierele semnate sunt în același director (folder) ca și fișierul de semnătură, atunci a doua coloană este completată automat. Altfel trebuie să furnizați căile pentru fișiere prin selectarea unui fișier și apăsarea butonului **Set path** (**Setează cale**).

NOTĂ: acest cîmp se completează doar în cazul semnăturii format XAdES tip Detașată!

- **Signatures** (**Semnături**) – vizualizarea ierarhică a semnăturilor aplicate.
- **Signature info** (**Informații semnătură**) – detaliile despre semnătura ce este selectată din secțiunea **Signatures** (**Semnături**).



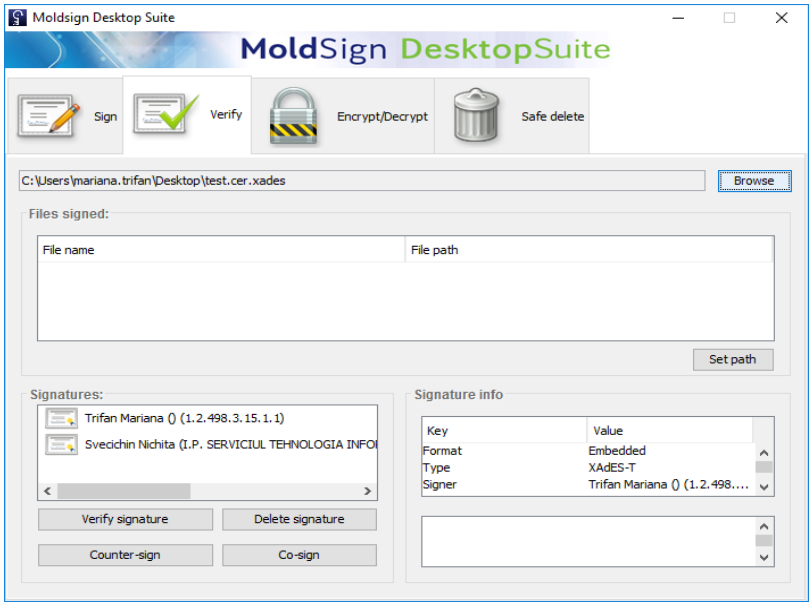
Sunt disponibile următoarele operațiuni pentru fiecare dintre semnături:

Verify signature (**Verificați semnătura**). Aceasta operațiune verifică dacă semnătura este validă prin examinarea fișierelor semnate și a tuturor celorlalte atribute ce sunt semnate. Dacă semnătura este validă, atunci apare un mesaj de tip pop-up.

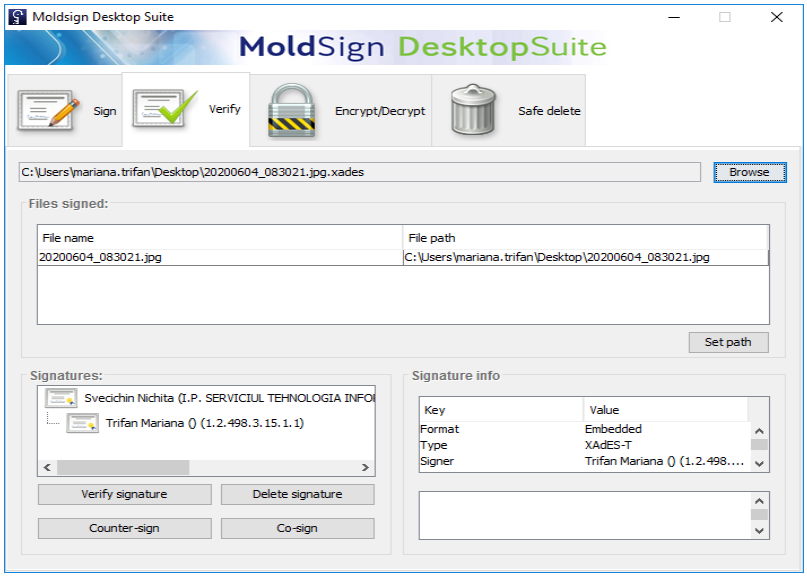
Delete signature (**Ștergere semnătură**). Această operațiune vă permite să ștergeți o semnătură dacă ați făcut o greșeală. Operațiunea permite ștergerea unei semnături numai dacă această semnătură nu este contrasemnată. De asemenea, dacă există doar o semnătură în

arbore, aceasta nu poate fi ștearsă. Înainte de ștergerea unei semnături vi se solicită confirmarea de a o șterge.

Co-sign/Counter-sign (Co-semnare/ Contra-semnare). Aceste operațiuni adaugă o semnătură suplimentară semnăturilor existente. Acestea sunt utilizate ca și confirmare a semnăturii. În cazul co-semnării, noua semnătură este adăugată la același nivel ca și certificatul selectat.



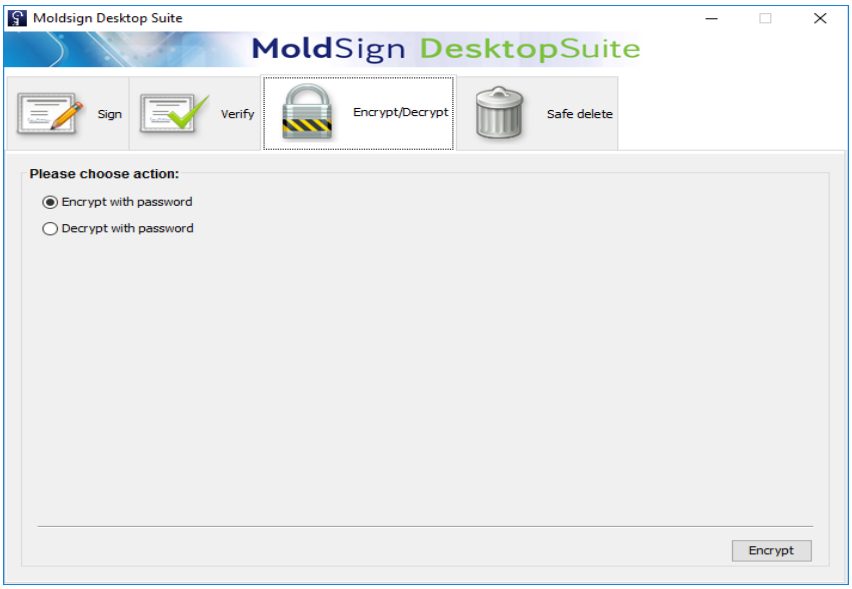
În cazul contra-semnării, semnătura este adăugată ca și confirmare a semnăturii existente și, prin urmare, la un nivel nou.



Cu alte cuvinte, co-semnătura semnează aceleași date ca și semnătura originală. Contra-semnătura semnează semnătura originală, făcând-o „rezistentă” la modificare.

3.4 Criptarea/ decriptarea fișierelor

Aplicația permite criptarea/decriptarea fișierelor prin utilizarea unei parole. Fișierele pot fi criptate sau decriptate din tabul **Encrypt/ Decrypt** (**Criptare/ Decriptare**). În acest tab există două opțiuni spre alegere.



3.4.1 Criptare cu parolă

Pentru criptarea cu parolă a unui fișier selectați opțiunea **Encrypt with password** (**Criptare cu parolă**) din tabul **Encrypt/ Decrypt** (**Criptare/ Decriptare**). Dacă ați selectat această opțiune și ați apăsat butonul **Encrypt** (**Criptează**), va apărea o nouă fereastră. Aici selectați întâi fișierul (prin căutare în sistemul de fișiere) ce va fi criptat, apoi selectați algoritmul de criptare din lista algoritmilor de criptare disponibili:

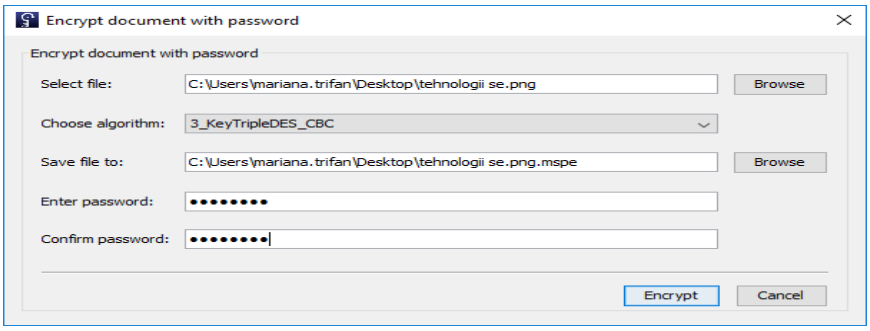
- 3 KeyTripleDES CBC
- 2 KeyTripleDES CBC
- DES CBC
- RC2 CBC
- RC4
- 128bit_AES
- 192bit_AES
- 256bit_AES

Algoritmii variază de la cei mai complecși la cei mai puțin complecși.

Calea de salvare a fișierului criptat este completată automat de aplicație. Dacă doriți, puteți decide asupra stocării fișierului într-un alt folder sau sub un nume diferit.

În final trebuie să introduceți parola pentru criptare. Pentru a evita erorile la scrierea parolei, aceasta trebuie confirmată.

Criptarea este realizată după apăsarea butonului **Encrypt** (**Criptează**).

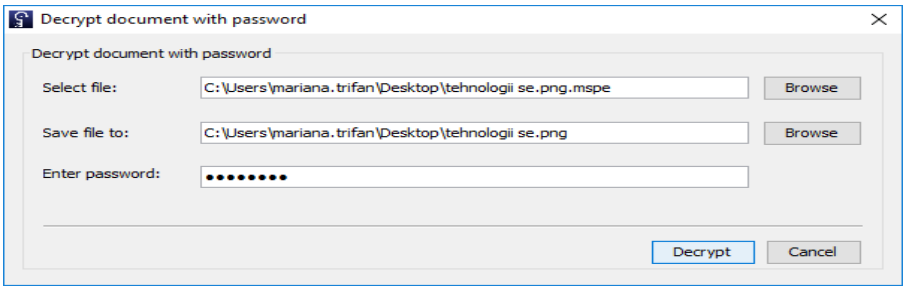


3.4.2 Decriptare cu parolă

Decriptarea unui fișier criptat anterior cu o parolă are loc prin selectarea opțiunii **Decrypt with password** (**Decriptare cu parolă**) din tabul **Encrypt/ Decrypt** (**Criptare/ Decriptare**). Dacă ați selectat această opțiune și ați apăsat butonul **Decrypt** (**Decriptează**), apare o nouă fereastră. Aici selectați fișierul (prin căutare în sistemul de fișiere) ce va fi decriptat.

Calea de salvare a fișierului decriptat (original) va fi setată automat, însă dvs puteți alege schimbarea acesteia.

În cele din urmă trebuie să introduceți parola pentru decriptare, iar apoi să apăsați pe butonul **Decrypt** (**Decriptează**).



3.5 Ștergerea securizată (distrugerea) fișierelor

Scopul acestei acțiuni este ștergerea fișierelor astfel încât acestea să nu poată fi recuperate prin intermediul oricărui mijloc de program. Toți algoritmii minimalizează posibilitatea recuperării prin supra-scrierea acelui fișier de mai multe ori (în anumite cazuri, de până la 35

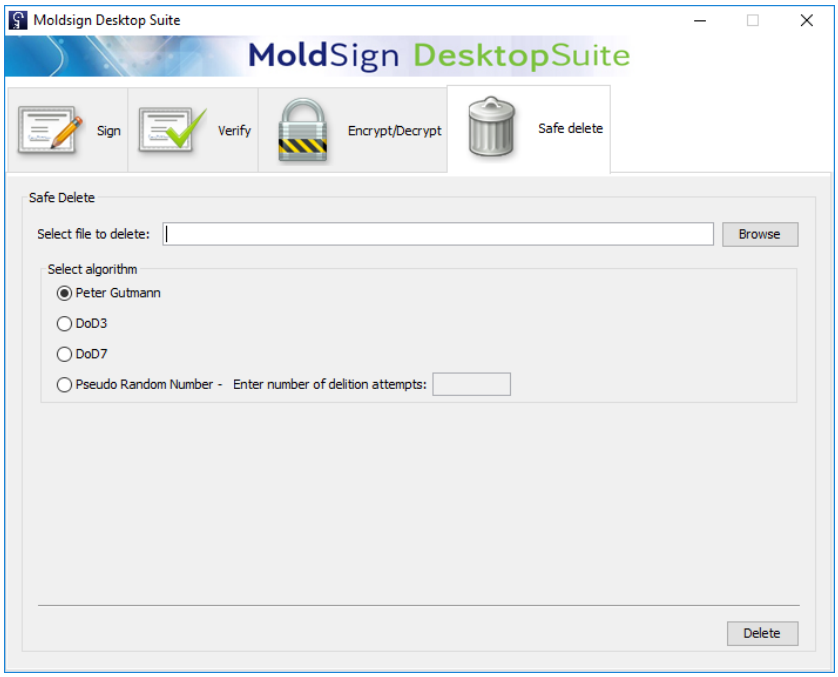
de ori) pentru a elimina toate câmpurile magnetice reziduale de pe discurile unde este (sunt) stocat/e fișierul (fișierele).

Pentru a șterge securizat un fișier acesta trebuie găsit în sistemul de fișiere.

Următorul pas este selectarea unui algoritm pentru ștergerea securizată a acestui fișier. Sunt furnizați următorii algoritmi:

- Peter Gutmann – șterge fișierul după ce îl supra-scrie de 35 de ori cu o schemă de biți strict definită, pentru minimalizarea urmelor magnetice reziduale,
- DoD3 – algoritmul Ministerului Apărării (SUA) cu 3 treceri,
- DoD7 – algoritmul Ministerului Apărării (SUA) cu 7 treceri,
- Pseudo Random Number – umple fișierul cu numere la întâmplare pentru un număr de treceri definit de dvs.

Această operațiune este realizată după apăsarea butonului **Delete** (**Ștergere**).



4 MoldSign Desktop Suite pentru SO MAC

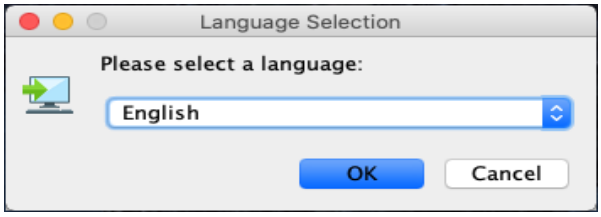
4.1 Instalare, setare

Accesați https://semnatura.md/ și descărcați programul MoldSign Desktop Suite. Instalarea este demarată prin lansarea fișierului de instalare MoldSign_ Last.dmg.

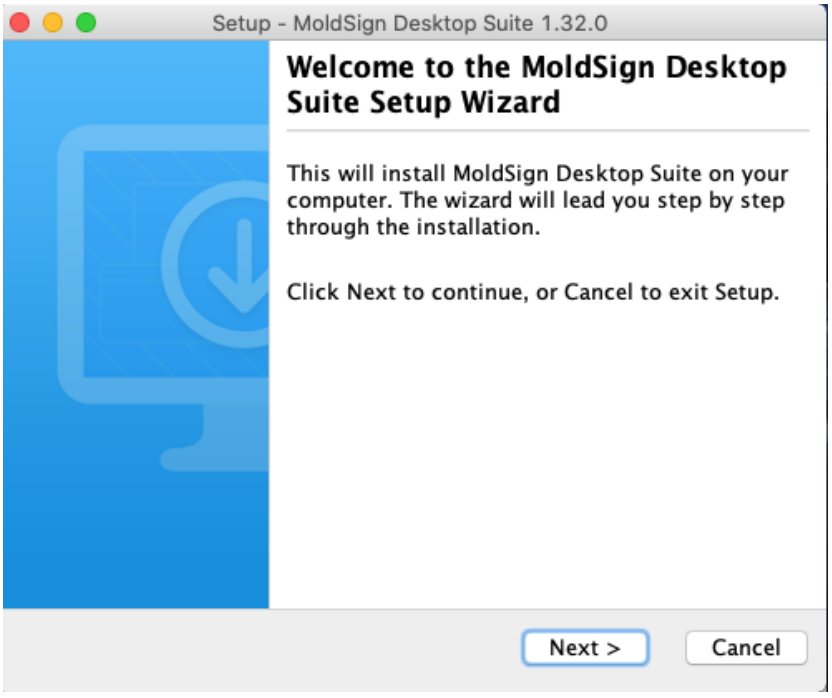
După aceea, începe instalarea programului MoldSign Desktop Suite.

Fișierul de instalare pregătește toți pașii necesari pentru instalarea programului.

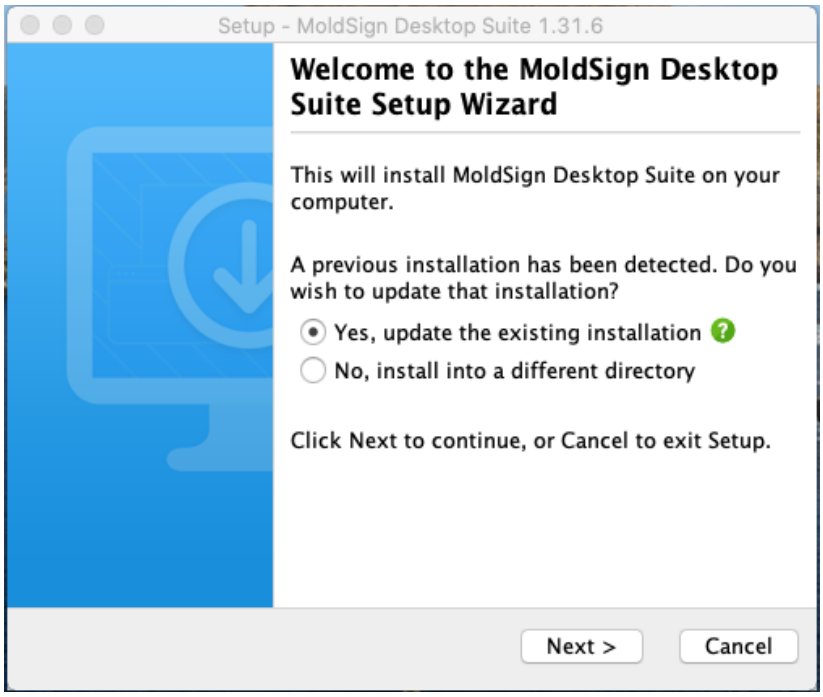
Selectați limba în care doriți să instalați programul, apoi apăsați **OK**.



Demarează procesul de instalare efectivă a programului. Apăsați pe butonul **Next** (**Următorul**).

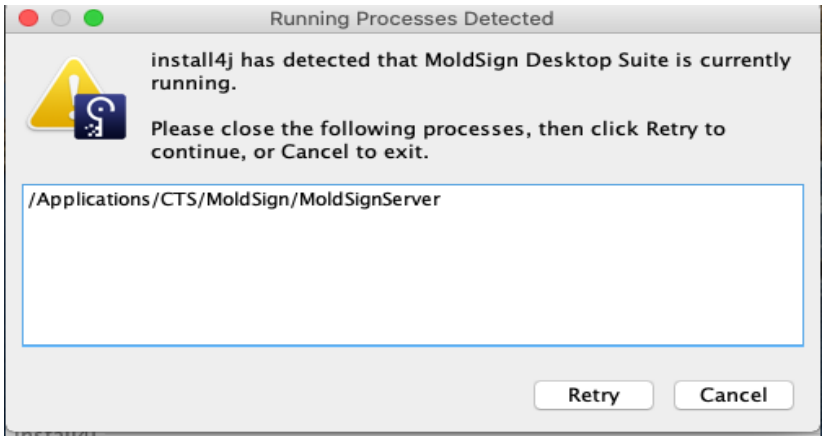


NOTĂ: în cazul actualizării programului MoldSign Desktop Suite (fără a dezinstala versiunea deja existentă pe calculator) va apărea fereastra



în care bifați **Yes, update the existing installation**, apoi apăsați butonul **Next** (**Următorul**). Dacă aplicația MoldSign Server nu a fost dezactivată anterior procesului de actualizare a programului MoldSign Desktop Suite, adică în bara de sus este prezentă iconița

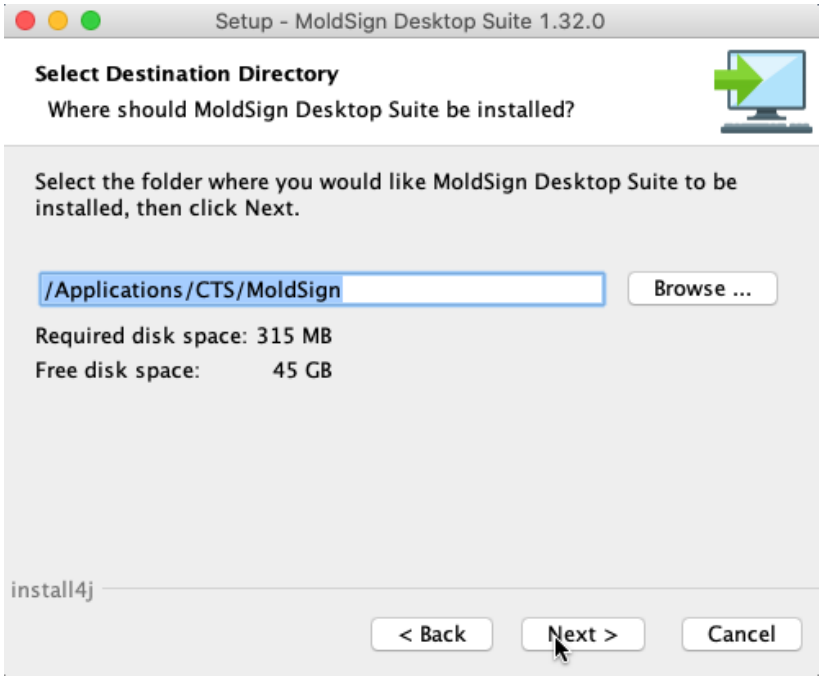
veți primi mesajul



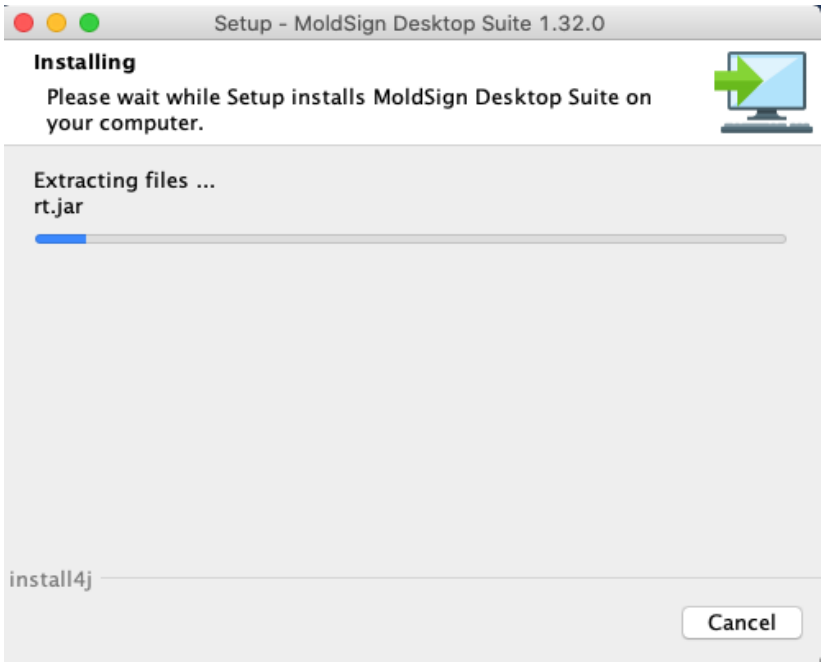
Faceți click dreapta pe și selectați **Exit** (**Ieșire**), apoi apăsați **Retry** (**Reîncearcă**).

Fișierul de instalare ne înștiințează în legătură cu locația în care va instala programul. Recomandăm să nu schimbați directorul **Destination Directory** (**Director Destinație**), ci să mergeți mai departe apăsând butonul **Next** (**Următorul**).

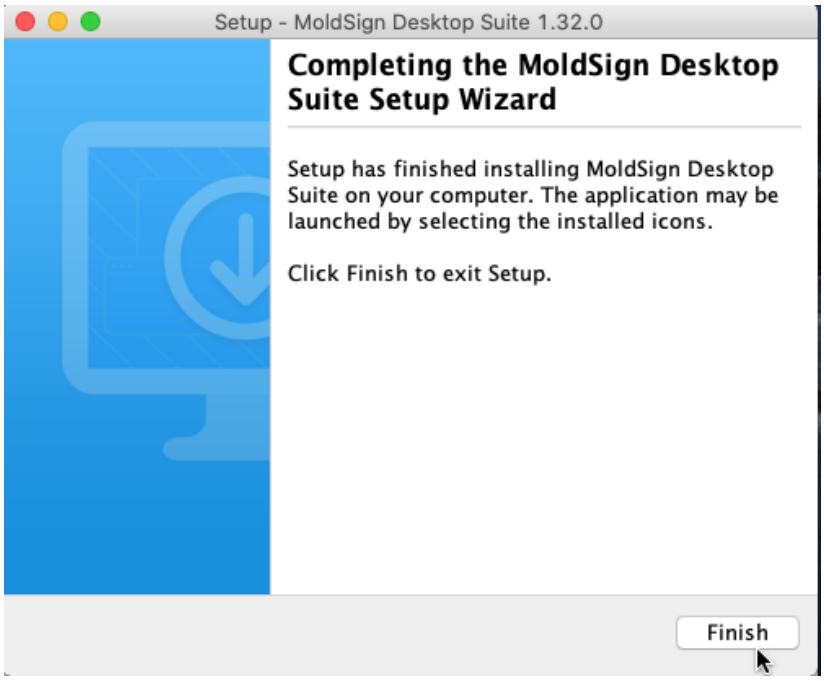
NOTĂ: Destination Directory (Director Destinație) poate fi schimbat doar dacă nu aveți suficient spațiu liber disponibil pe hard diskuri.



Procesul de instalare continuă prin copierea programului din fișierul de instalare pe calculator. Vă rugam să așteptați finalizarea acestei operațiuni.



Fereastra de mai jos arată că procesul de instalare s-a finalizat cu succes și, după apăsarea butonului **Finish (Finalizare),** puteți utiliza programul MoldSign Desktop Suite.

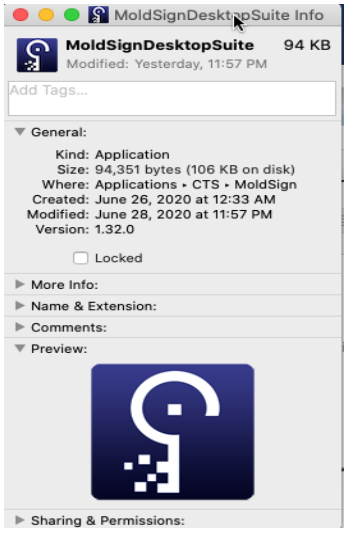


După finalizarea cu succes a procesului de instalare vi se cere să reporniți calculatorul. Reporniți-l.

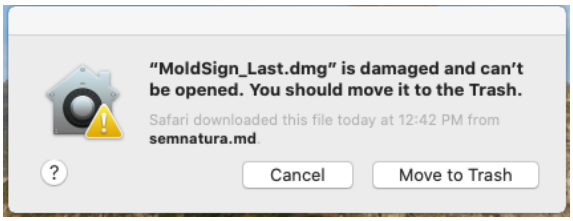
La pornirea calculatorului, în mod automat se va lansa și aplicația MoldSign Server. Acest lucru poate fi observat prin apariția iconiței din bara de sus.

Dacă aplicația dată nu a fost lansată automat sau a fost oprită din careva motive, o puteți lansa manual prin click pe iconița MoldSign

Lansați aplicația MoldSign Desktop Suite urmînd calea **Applications –> CTS -> MoldSign**



NOTĂ: dacă ați întîmpinat dificultăți în procesul de instalare a programului



copiați fișierul MoldSign_Last.dmg din Downloads în directoriul utilizatorului (Home). Deschideți *Terminal* și scrieți comanda `sh-3.2# xattr -cr /Users/nick/MoldSign_Last.dmg`

Apăsați dublu click pe fișierul descărcat

și pe Desktop apare iconița MoldSign 

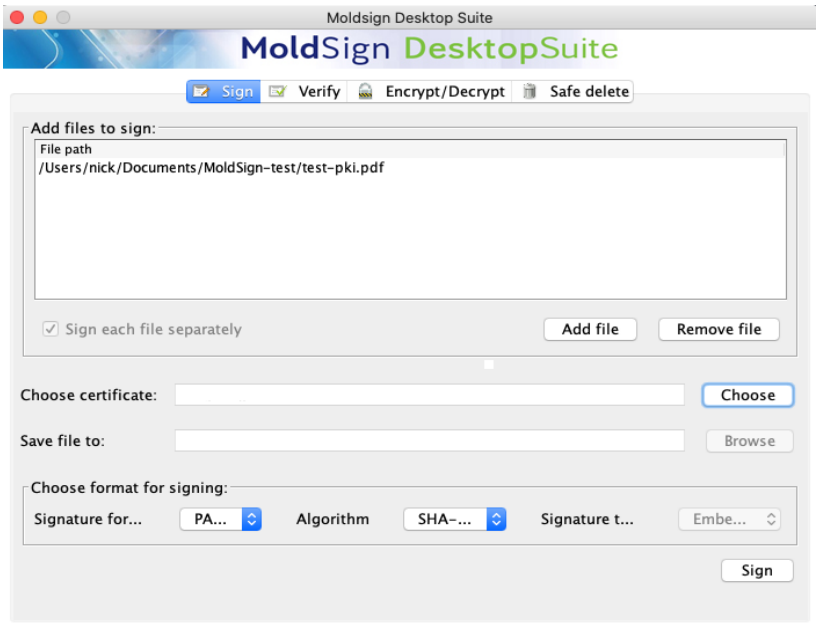
împreună cu fereastra

Apăsați dublu click pe iconița  . Apare fereastra de instalare a programului.

4.2 Semnarea fișierelor

Semnarea fișierelor prin tabul **Sign (Semnați)** din meniul principal al aplicației se realizează prin executarea procesului de semnare descris mai jos:

1. adăugați fișierele ce trebuie semnate în lista de fișiere. Acest lucru poate fi realizat prin apăsarea pe butonul **Add file (Adăugați fișier),** ce va deschide o nouă fereastră pentru căutarea fișierelor în sistemul de fișiere. Există și posibilitatea introducerii în listă a fișierelor prin Drag & Drop direct din aplicația File Explorer.



Pentru eliminarea unui fișier din listă acesta trebuie selectat, apoi apăsați pe butonul **Remove file (Îndepărtați fișier)**.

2. introduceți în calculator dispozitivul cu care doriți să semnați și așteptați câteva secunde. La depistarea dispozitivului introdus va apărea, lângă iconița , și iconița .

IMPORTANT! Dacă dispozitivul nu a fost identificat de aplicația MoldSign Server, adică iconița nu este prezentă, verificați dacă ați instalat driverul pentru dispozitivul utilizat (acesta poate fi descărcat de pe https://semnatura.md).

NOTĂ: dacă ați întîmpinat dificultăți în procesul de instalare a driverului pentru dispozitiv copiați fișierul corespunzător din Downloads în directoriul utilizatorului (Home). Deschideți *Terminal* și scrieți comanda

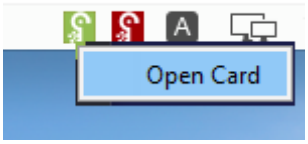
```
sh-3.2# xattr -cr /Users/nick/Downloads/ePass2003-Castle-mac-20170718_Release.dmg
```

(pentru ePass2003) sau

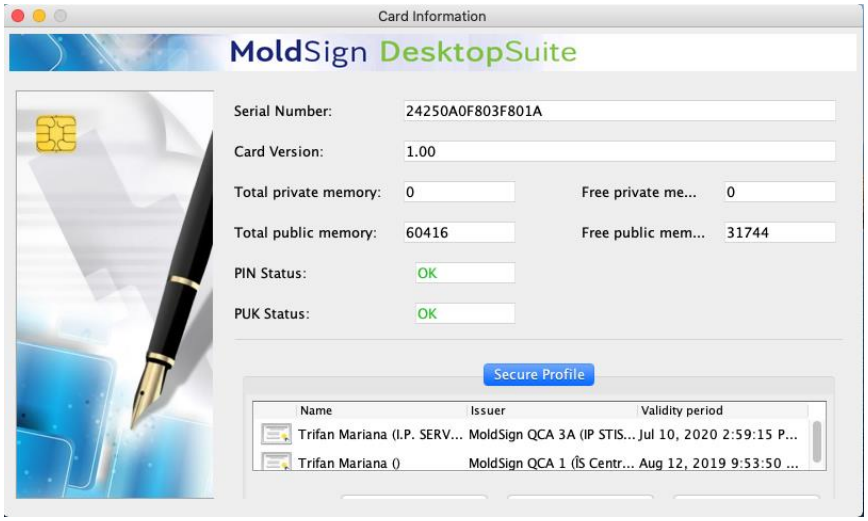
```
sh-3.2# xattr -cr /Users/nick/Downloads/acsccid_installer-1.1.4.dmg
```

pentru cryptomate 64.

NOTĂ: pentru a vizualiza informația ce se conține pe dispozitiv faceți click pe . Automat apare **Open Card**



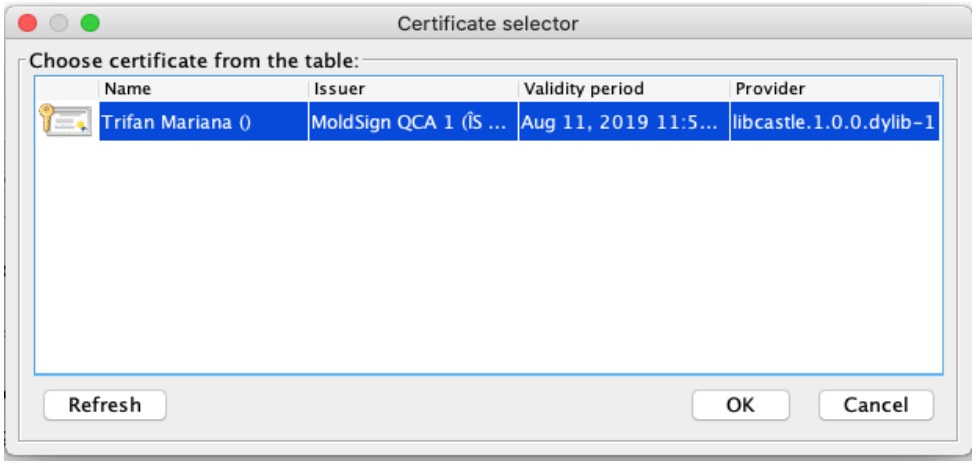
și fereastra **Card Information**



în care puteți vizualiza conținutul certificatului cheii publice selectat (**Display Certificate Data**), atribui un PIN nou (**New PIN**) sau schimba PIN-ul vechi (**Change PIN**) al dispozitivului.

Atenție! Nu introduceți mai multe dispozitive concomitent în același calculator. Dacă aveți nevoie să semnați cu mai multe dispozitive introduceți și semnați pe rând cu câte un singur dispozitiv.

3. selectați certificatul calificat al cheii publice (ce conține o cheie privată) de pe dispozitiv. Acest lucru poate fi realizat prin apăsarea butonului **Choose** (**Alegeți**), ce va deschide o nouă fereastră din care poate fi selectat certificatul (sunt afișate doar certificatele cheilor publice valide). Această acțiune este finalizată prin apăsarea pe butonul **OK.**



4. selectați formatul și tipul de semnătură. Sunt disponibile următoarele formate:

PAdES - semnătura fișierelor pdf;

PAdES-T - semnătura fișierelor pdf ce include și un marcaj temporal din partea unui server autorizat pentru marcare temporală;

XAdES-BES – semnătură de bază în format XML;

XAdES-T – semnătură de bază cu marcaj temporal adițional din partea unui server autorizat pentru marcare temporală;

XAdES-C – XAdES-T cu statut adițional al certificatului cheii publice.

Tipul de semnătură poate fi **Detached** (**Detașată**) sau **Embedded** (**Încorporată**). Semnătura **Detached** (**Detașată**) presupune existența unui fișier separat ce conține semnătura pentru unul sau mai multe fișiere; în timp ce, semnătura **Embedded** (**Încorporată**) presupune că atât fișierul semnat, cât și semnătura sunt localizate în cadrul aceluiași fișier.

În cazul semnăturilor fișierelor pdf (**PAdES**, **PAdES-T**) este aplicabil doar tipul **Embedded** (**Încorporată**).

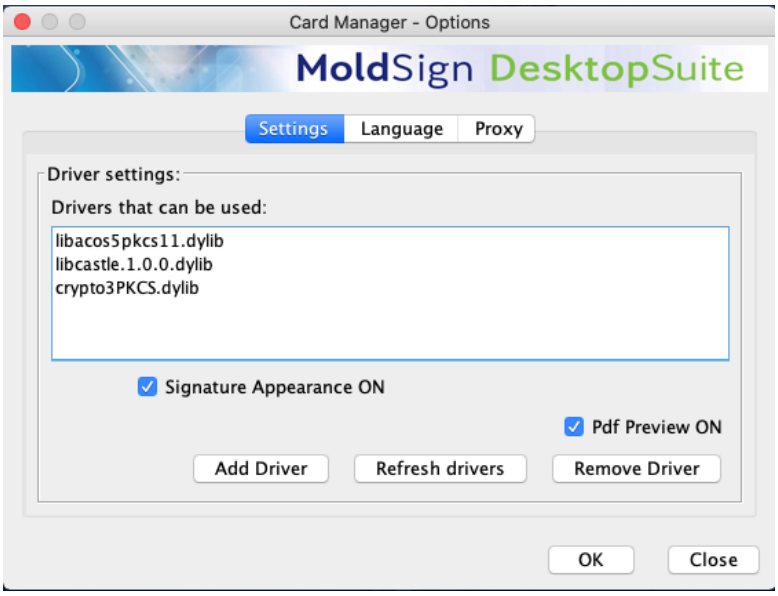
Pentru formatul **XAdES** sunt disponibile ambele tipuri, însă, pentru limitarea consumului de resurse, formatul **Embedded** (**Încorporată**) este disponibil numai pentru fișiere mai mici de 100KB.

În anumite cazuri (când semnătura este în formatul **XAdES** și de tip **Detached** (**Detașată**) pot fi semnate mai multe fișiere cu un singur fișier de semnătură. Această semnătură este realizată dacă debifați opțiunea **Sign each file separately** (**Fiecare fișier separat**). În acest caz, selectați numele și locația fișierului de semnătură.

Altfel, fișierele sunt salvate prin adăugarea automată a extensiei **.xades** la sfârșitul numelui fișierului (pentru formatele de semnătură **XAdES**), sau prin adăugarea **.signed** în fața extensiei **.pdf** (pentru formate de semnătură **PAdES**).

5. După finalizarea pașilor descriși mai sus, apăsați pe butonul **Sign** (**Semnați)** pentru a realiza procesul de aplicare a semnăturii.

NOTĂ: în cazul fișierelor pdf aveți posibilitatea de a alege poziționarea semnăturii în raport cu paginile documentului ce urmează a fi semnat și localizarea acesteia pe pagina selectată. Pentru aceasta, după lansarea aplicației MoldSign Server, faceți click dreapta pe și selectați **Options** (**Opțiuni**). Se va deschide fereastra



în care puteți bifa/debifa opțiunile **Signature Apperance ON** (**Apariția semnăturii pe**) și **Pdf Preview ON** (**Previzualizarea semnătuii pe**).
Pdf Preview ON se activează doar în cazul bifării opțiunii **Signature Apperance ON.**

Dacă bifați **Pdf Preview ON** veți previzualiza poziționarea semnăturii în document, apoi veți apăsa butonul **Accept**; în caz contrar nu veți previzualiza poziționarea semnăturii în document și semnătura va fi poziționată în coltul din stînga jos pe prima pagină a documentului.
Introduceți codul PIN al dispozitivului. Dacă codul PIN este corect, fișierele vor fi semnate.

După ce operațiunea este finalizată, toate fișierele care au fost semnate cu succes vor fi eliminate din lista fișierelor ce trebuie semnate.

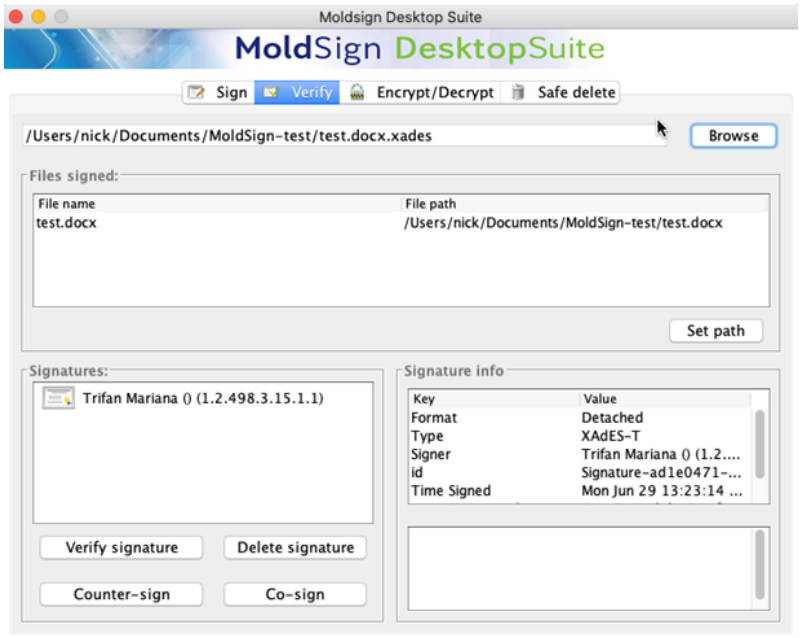
4.3 Verificarea semnăturilor XAdES

Semnăturile pot fi verificate prin tabul **Verify (Verifică)**. Pentru aceasta selectați fișierul ce trebuie verificat. Atunci când alegeți un fișier valid XAdES restul câmpurilor din fereastră vor fi completate cu date:

- **Files signed (Fișiere semnate)** – fișierele care au fost semnate cu fișierul de semnătură selectat. Prima coloană afișează numele fișierelor ce au fost semnate, în timp ce a doua coloană prezintă calea completă a acestui fișier pe calculatorul dvs. Dacă fișierele semnate sunt în același director (folder) ca și fișierul de semnătură, atunci a doua coloană este completată automat. Altfel trebuie să furnizați căile pentru fișiere prin selectarea unui fișier și apăsarea butonului **Set path (Setează cale)**.

NOTĂ: acest cîmp se completează doar în cazul semnăturii format XAdES tip Detașată!

- **Signatures (Semnături)** – vizualizarea ierarhică a semnăturilor aplicate.
- **Signature info (Informații semnătură)** – detaliile despre semnătura ce este selectată din secțiunea **Signatures (Semnături)**.

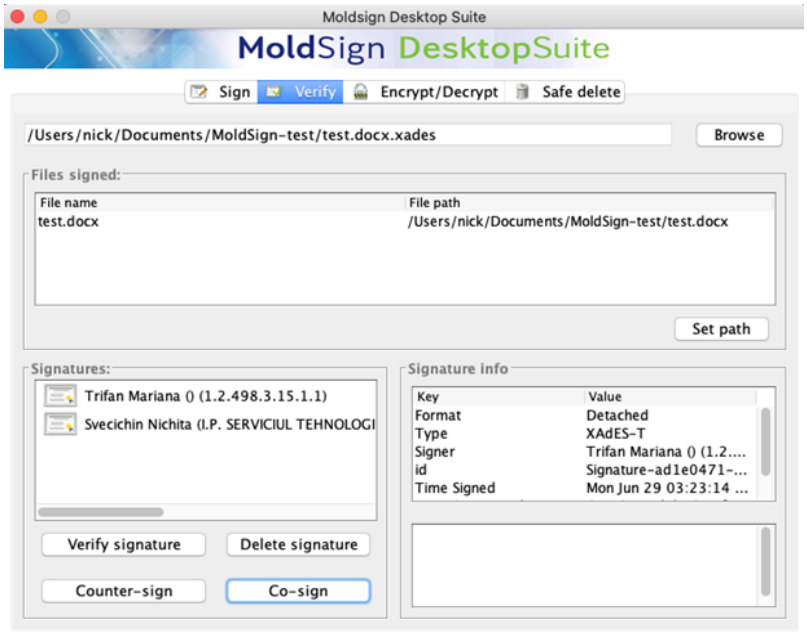


Sunt disponibile următoarele operațiuni pentru fiecare dintre semnături:

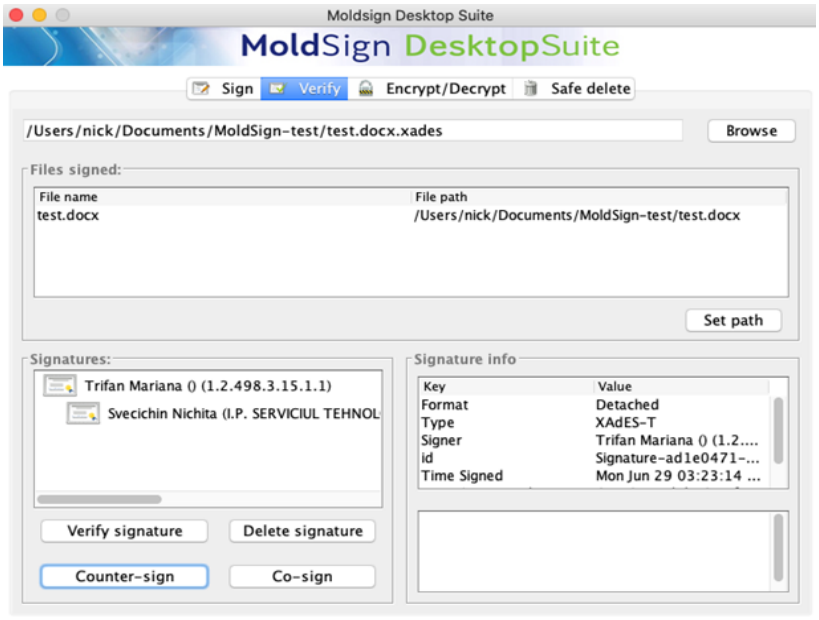
Verify signature (**Verificați semnătura**). Aceasta operațiune verifică dacă semnătura este validă prin examinarea fișierelor semnate și a tuturor celorlalte atribute ce sunt semnate. Dacă semnătura este validă, atunci apare un mesaj de tip pop-up.

Delete signature (**Ștergere semnătură**). Această operațiune vă permite să ștergeți o semnătură dacă ați făcut o greșeală. Operațiunea permite ștergerea unei semnături numai dacă această semnătură nu este contrasemnată. De asemenea, dacă există doar o semnătură în arbore, aceasta nu poate fi ștearsă. Înainte de ștergerea unei semnături vi se solicită confirmarea de a o șterge.

Co-sign/Counter-sign (**Co-semnare/ Contra-semnare**). Aceste operațiuni adaugă o semnătură suplimentară semnăturilor existente. Acestea sunt utilizate ca și confirmare a semnăturii. În cazul co-semnării, noua semnătură este adăugată la același nivel ca și certificatul calificat al cheii publice selectat.



În cazul contra-semnării, semnătura este adăugată ca și confirmare a semnăturii existente și, prin urmare, la un nivel nou.



Cu alte cuvinte, co-semnătura semnează aceleași date ca și semnătura originală. Contra-semnătura semnează semnătura originală, făcând-o „rezistentă" la modificare.

4.4 Criptarea/ decriptarea fișierelor

Aplicația permite criptarea/decriptarea fișierelor prin utilizarea unei parole. Fișierele pot fi criptate sau decriptate din tabul **Encrypt/ Decrypt** (**Criptare/ Decriptare**). În acest tab există două opțiuni spre alegere.

4.4.1 Criptare cu parolă

Pentru criptarea cu parolă a unui fișier selectați opțiunea **Encrypt with password** (**Criptare cu parolă**) din tabul **Encrypt/ Decrypt** (**Criptare/ Decriptare**). Dacă ați selectat această opțiune și ați apăsat butonul **Encrypt** (**Criptează**), va apărea o nouă fereastră. Aici selectați întâi fișierul (prin căutare în sistemul de fișiere) ce va fi criptat, apoi selectați algoritmul de criptare din lista algoritmilor de criptare disponibili:

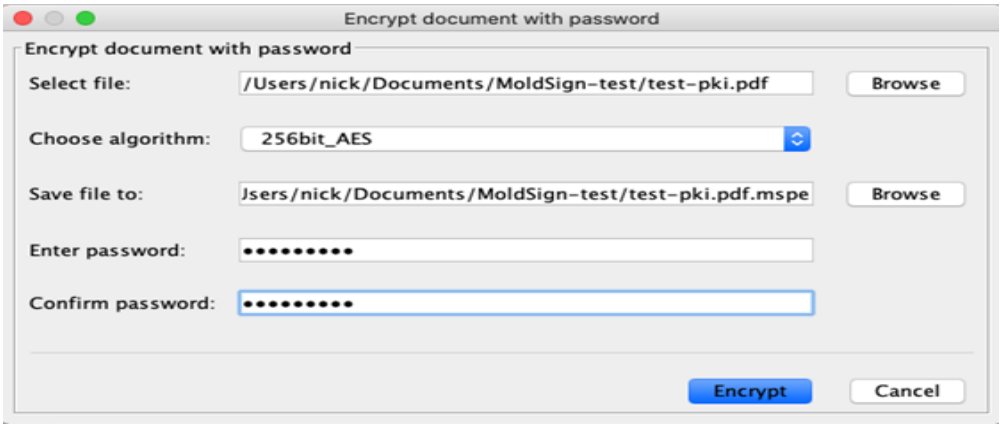
- 3 KeyTripleDES CBC
- 2 KeyTripleDES CBC
- DES CBC
- RC2 CBC
- RC4
- 128bit_AES
- 192bit_AES
- 256bit_AES

Algoritmii variază de la cei mai complecși la cei mai puțin complecși.

Calea de salvare a fișierului criptat este completată automat de aplicație. Dacă doriți, puteți decide asupra stocării fișierului într-un alt folder sau sub un nume diferit.

În final trebuie să introduceți parola pentru criptare. Pentru a evita erorile la scrierea parolei, aceasta trebuie confirmată.

Criptarea este realizată după apăsarea butonului **Encrypt** (**Criptează**).

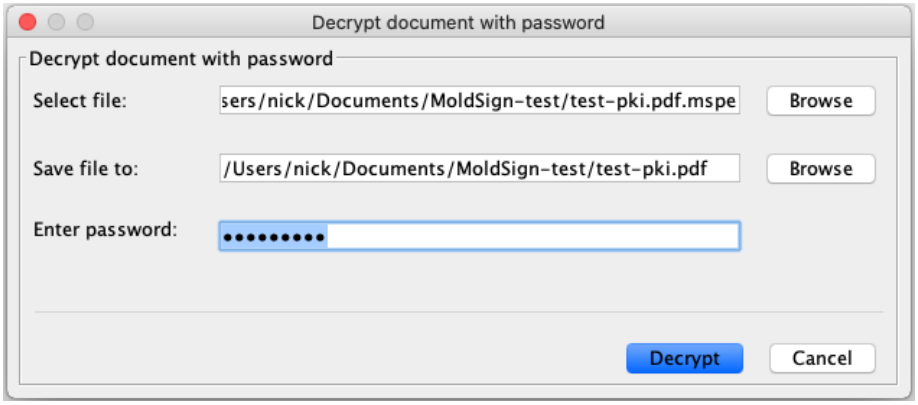


4.4.2 Decriptare cu parolă

Decriptarea unui fișier criptat anterior cu o parolă are loc prin selectarea opțiunii **Decrypt with password** (**Decriptare cu parolă**) din tabul **Encrypt/ Decrypt** (**Criptare/ Decriptare**). Dacă ați selectat această opțiune și ați apăsat butonul **Decrypt** (**Decriptează**), apare o nouă fereastră. Aici selectați fișierul (prin căutare în sistemul de fișiere) ce va fi decriptat.

Calea de salvare a fișierului decriptat (original) va fi setată automat, însă dvs puteți alege schimbarea acesteia.

În cele din urmă trebuie să introduceți parola pentru decriptare, iar apoi să apăsați pe butonul **Decrypt** (**Decriptează**).



4.5 Ștergerea securizată (distrugerea) fișierelor

Scopul acestei acțiuni este ștergerea fișierelor astfel încât acestea să nu poată fi recuperate prin intermediul oricărui mijloc de program. Toți algoritmii minimalizează posibilitatea recuperării prin supra-scrierea acelui fișier de mai multe ori (în anumite cazuri, de până la 35

de ori) pentru a elimina toate câmpurile magnetice reziduale de pe discurile unde este (sunt) stocat/e fișierul (fișierele).

Pentru a șterge securizat un fișier acesta trebuie găsit în sistemul de fișiere.

Următorul pas este selectarea unui algoritm pentru ștergerea securizată a acestui fișier. Sunt furnizați următorii algoritmi:

- Peter Gutmann – șterge fișierul după ce îl supra-scrie de 35 de ori cu o schemă de biți strict definită, pentru minimalizarea urmelor magnetice reziduale,
- DoD3 – algoritmul Ministerului Apărării (SUA) cu 3 treceri,
- DoD7 – Algoritmul Ministerului Apărării (SUA) cu 7 treceri,
- Pseudo Random Number – Umple fișierul cu numere la întâmplare pentru un număr de treceri definit de dvs.

Această operațiune este realizată după apăsarea butonului **Delete** (**Ștergere**).