MoldSign Desktop

Ghidul utilizatorului

Instituția Publică

”Serviciul Tehnologia Informației

și Securitate Cibernetică”

Conținut

1 Introducere

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

- Legea nr. 124/2023 *privind identificarea electronică și serviciile de încredere*,
- *Cerințe tehnice în domeniul serviciilor de încredere calificate*,
- 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 AlgoritmsSpecification,

IETF RFC 3029 Data Validation and Certification Server Protocols (DVCS).

2 Cerințe tehnice

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

- sistem de operare Windows 8/8.1/10/11, Windows Server 2016/2019/2022/23H2, MacOS sau Linux;
- minim 200MB spațiu disponibil pe disc;
- conexiune Internet,
- PDF versiunea 1.7.

NOTĂ: MoldSign Desktop nu funcționează pe sistemele de operare vechi.

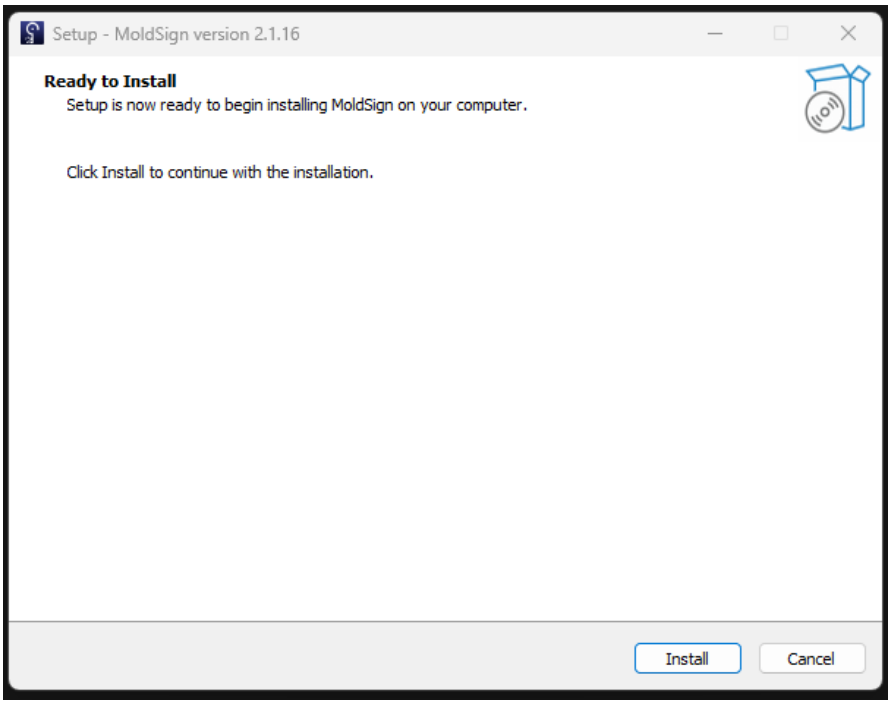
3 MoldSign Desktop pentru SO Windows

3.1 Instalare, setare

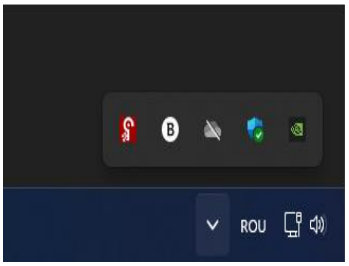
Goliți memoria cache a stației de lucru, restartați computerul.

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

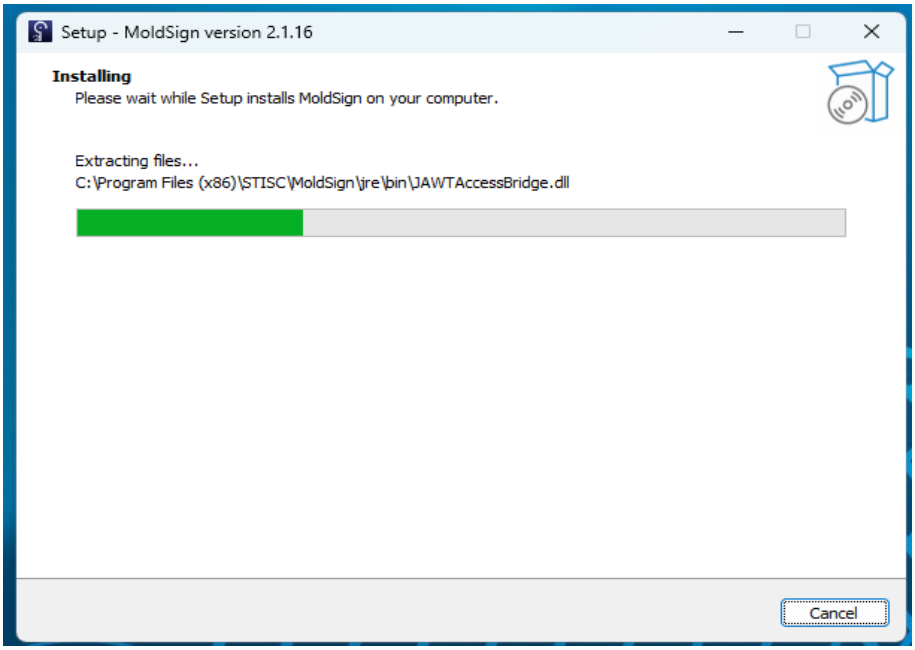
Demarează procesul de instalare efectivă a programului. Faceți click pe butonul **Install**.



NOTĂ: Dacă aplicația MoldSign Server nu a fost dezactivată anterior procesului de actualizare a programului MoldSign Desktop, adică în bara de lucru zona „tray" este prezentă Faceți click dreapta pe și selectați **Exit** (**Ieșire**), apoi apăsați **Retry** (**Reîncearcă**).

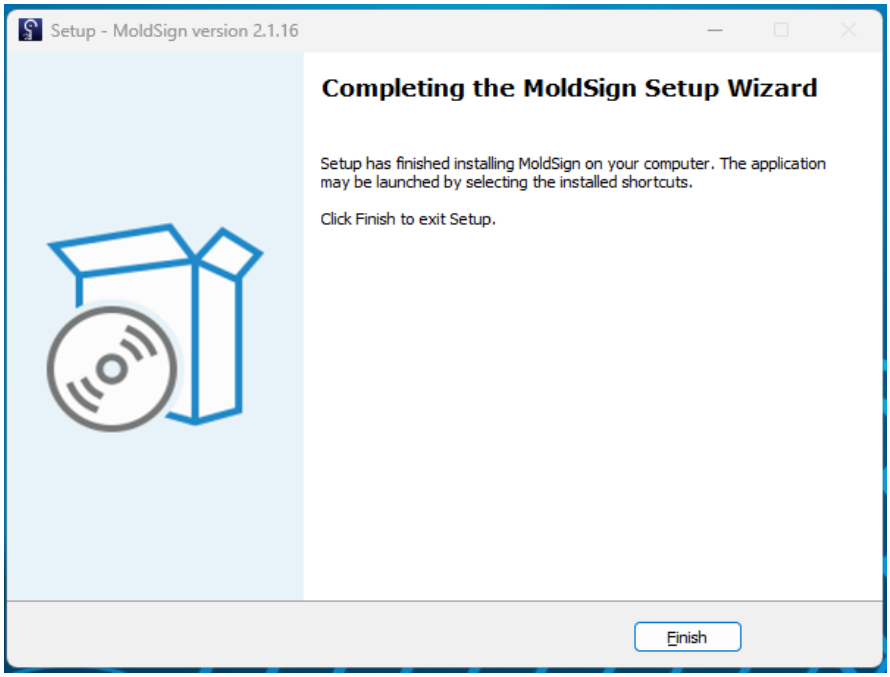


Procesul de instalare continuă prin copierea programului din fișierul de instalare pe calculator. Vă rugam să așteptați finalizarea acestei operațiuni.



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

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.

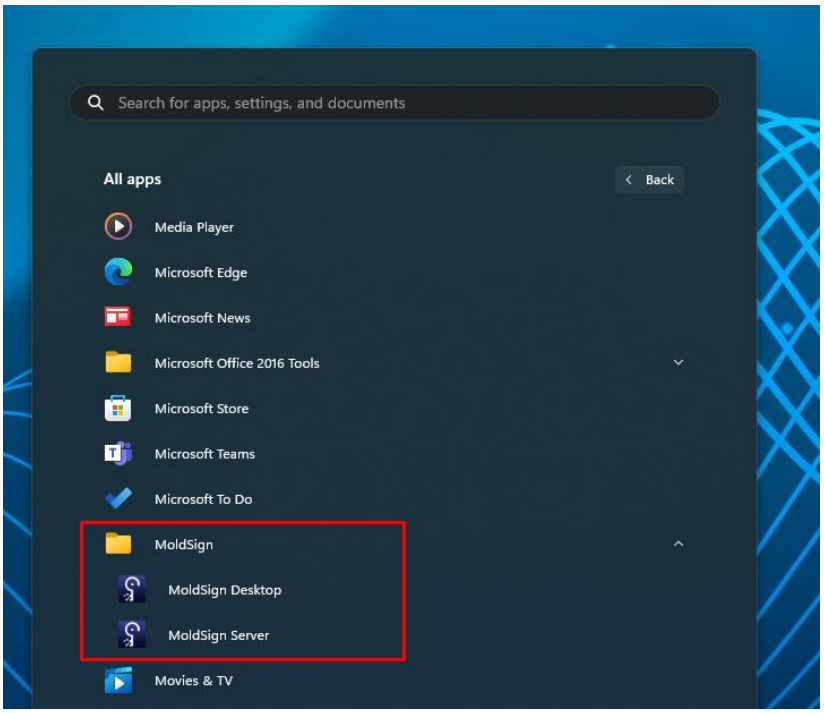


La lansarea aplicatiei MoldSign Server, vedeți iconița pe bara de lucru în zona „tray” (colțul din dreapta jos lângă ceas).

La lansarea MoldSign Desktop apare fereastra de mai jos:

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

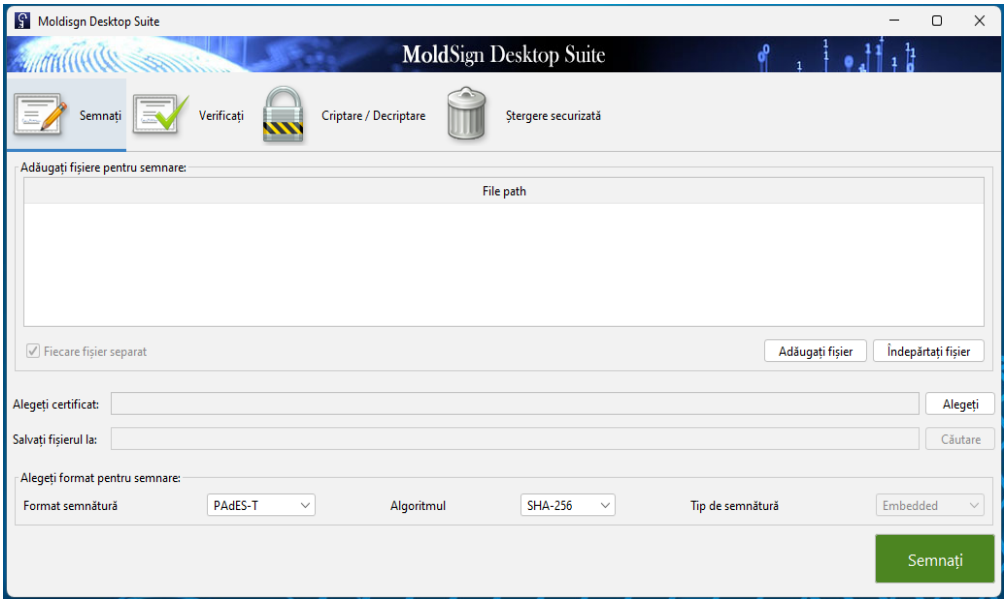
Lansați aplicația MoldSign Desktop urmînd calea ***Start->All Programs->MoldSign ->MoldSign Desktop***



3.2 Semnarea fișierelor

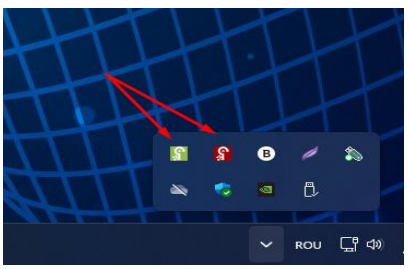
Semnarea fișierelor prin tabul **Semnați** din meniul principal al aplicației se realizează prin executarea procesului de semnare descris mai jos:

1. Adăugați fișierele ce trebuie semnate în lista de fișiere. Acest lucru poate fi realizat prin apăsarea pe butonul **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.



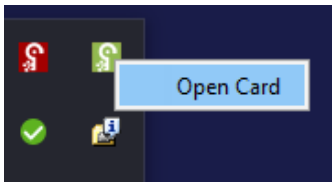
Pentru eliminarea unui fișier din listă acesta trebuie selectat, apoi apăsați pe butonul **Îndepărtați fișier.**

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

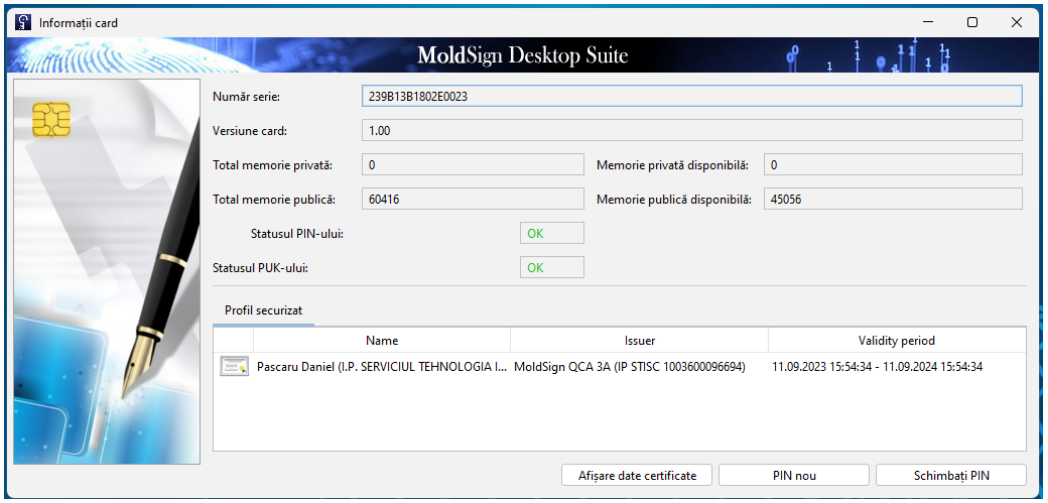


IMPORTANT! Dacă dispozitivul nu a fost identificat de aplicația MoldSign Server, adică iconița nu este prezentă, verificați dacă ați instalat driverul pentru dispozitivul utilizat (acesta poate fi descărcat de pe https://semnatura.md).

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



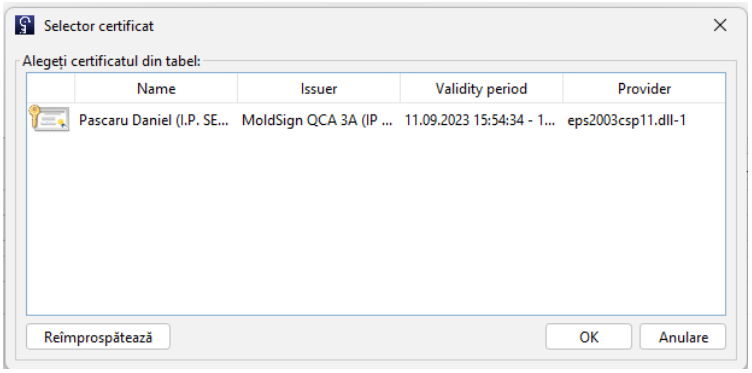
Se va deschide **Informații card** (**Card Information)**



în care puteți vizualiza conținutul certificatului cheii publice selectat (**Display Certificate Data**), atribui un **PIN nou** numeric (**New PIN**) sau **Schimbați 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**).

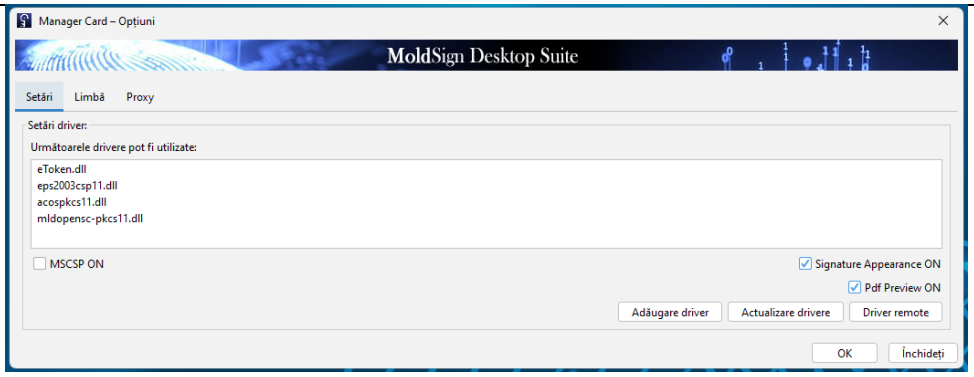
Pentru formatul **XAdES** sunt disponibile ambele tipuri, însă, pentru limitarea consumului de resurse, formatul **Embedded** (**Încorporată**) este disponibil numai pentru fișiere mai mici de 100KB.

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 **Opțiuni** (**Options**). Se va deschide fereastra

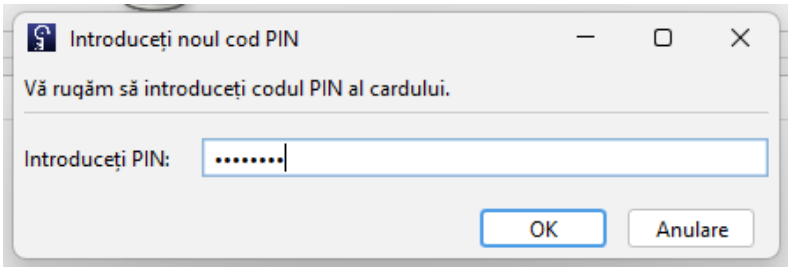


în care puteți bifa/debifa opțiunile **Signature Apperance ON** (**Apariția semnăturii**) și **Pdf Preview ON** (**Previzualizarea semnăturii**).

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 **OK**; 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 și faceți click pe **OK**. 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.

Fișierele semnate vor fi stocate în mapa cu documentele inițiale, pe care a fost aplicată semnătura.

3.3 Verificarea semnăturilor XAdES

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

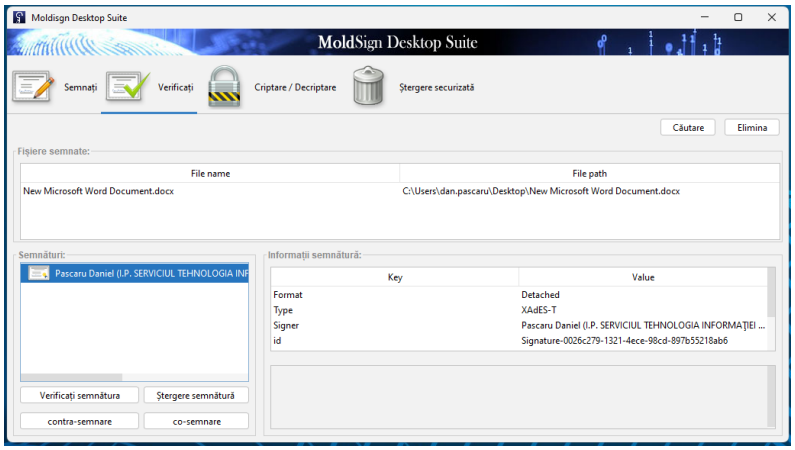
fi completate cu date:

- **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**).

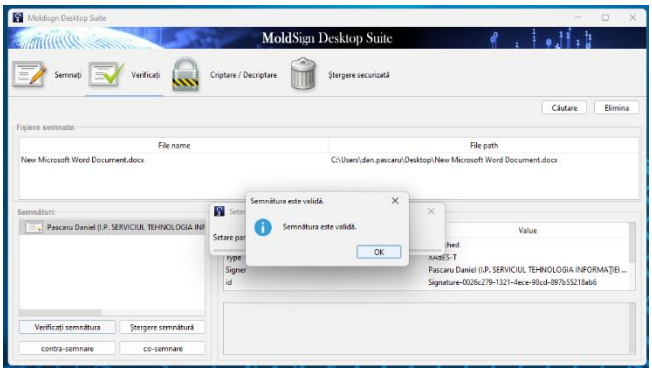
NOTĂ: acest cîmp se completează doar în cazul semnăturii format XAdES tip Detașată!

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



Sunt disponibile următoarele operațiuni pentru fiecare dintre semnături:

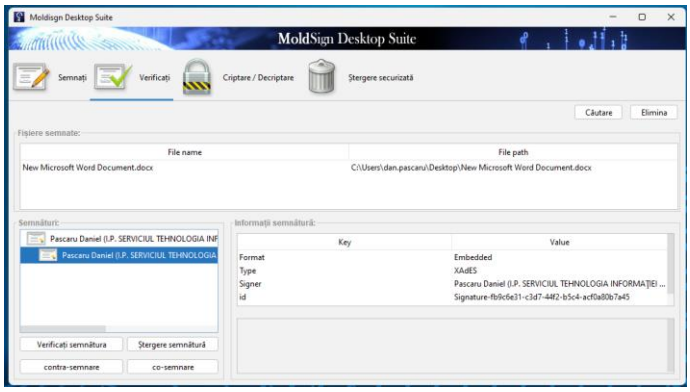
Verificați semnătura. Aceasta operațiune verifică dacă semnătura electronică calificată este validă prin examinarea documentelor electronice semnate și a tuturor celorlalte atribute ce sunt semnate. Dacă semnătura electronică calificată este validă, atunci apare un mesaj de tip pop-up "Semnătura este validă".



Ștergere semnătură. Această operațiune vă permite să ștergeți o semnătură electronică calificată dacă ați făcut o greșeală. Operațiunea permite ștergerea numai dacă această semnătură electronică calificată nu a fost ulterior contrasemnată. De asemenea, dacă există doar o semnătură electronică calificată în arbore, aceasta nu poate fi ștearsă. Înainte de ștergerea unei semnături electroncie calificate se va solicita confirmarea suplimentară de a o șterge.

Co-semnare/Contra-semnare. Aceste operațiuni adaogă o semnătură electronică calificată suplimentar la cele deja aplicate. Acestea sunt utilizate ca și confirmare a semnăturii.

În cazul co-semnării, noua semnătură electronică calificată este adăugată la același nivel ca și certificatul selectat.



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

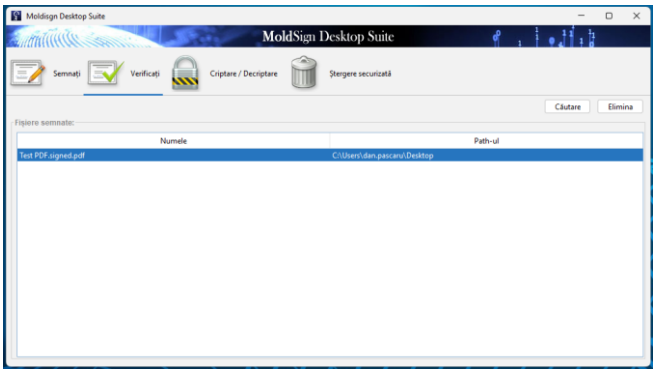
Astfel, co-semnătura semnează aceleași date ca și semnătura electronică calificată originală. Contra- semnătura semnează semnătura originală, făcând-o „rezistentă" la modificare.

3.4 Verificarea semnăturilor PAdES

Semnăturile pot fi verificate prin tabul **Verificați**. Pentru aceasta selectați fișierul ce trebuie verificat. Atunci când alegeți un fișier valid PAdES(.pdf), câmpurile din fereastră vor fi completate cu date:

- **Fișiere semnate -** *Prima coloană* afișează numele fișierelor ce au fost semnate, în timp ce a *doua coloană* prezintă calea completă a acestui fișier pe calculatorul dvs.

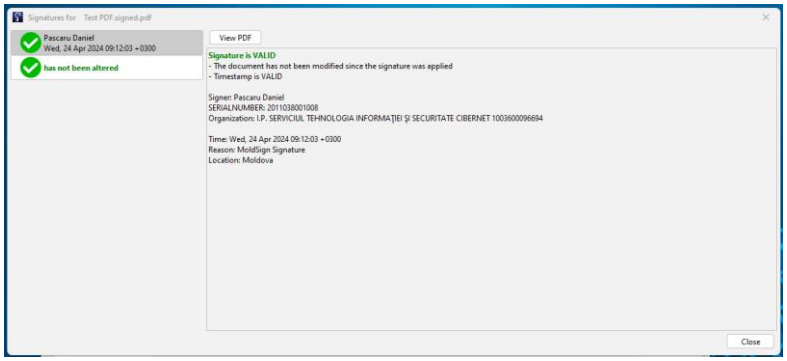
NOTĂ: Similar etapei de semnare, la cea de verificare, pentru selectarea documentului electronic, se va deschide o nouă fereastră pentru căutarea fișierelor în sistemul de fișiere. Există și posibilitatea introducerii în listă a fișierelor prin Drag & Drop direct din aplicația File Explorer.



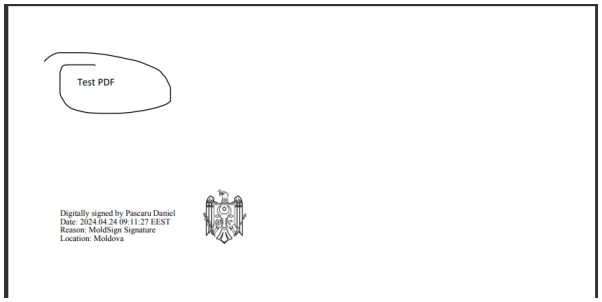
Dacă semnătura electronică calificată este validă, apare mesaj de tip pop-up, care prezintă următoarele detalii:

Semnatar, data/ora semnării, și IMPORTANT - verificarea conținutului documentului și confirmarea faptului că conținutul supus verificării nu a suportat modificări/alterări din momentul aplicării semnăturii electronice calificate.

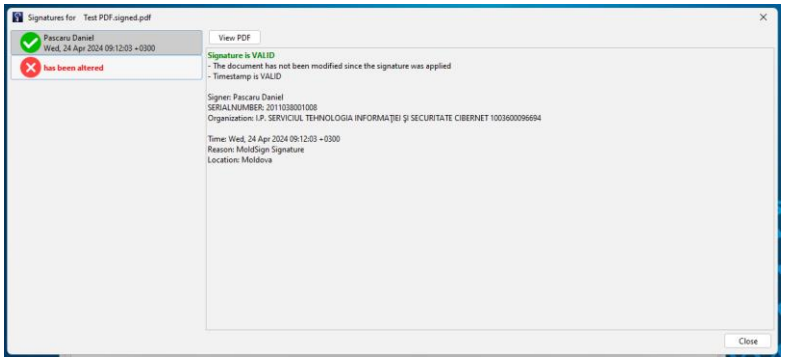
"The document has not been modified since the signature was applied".



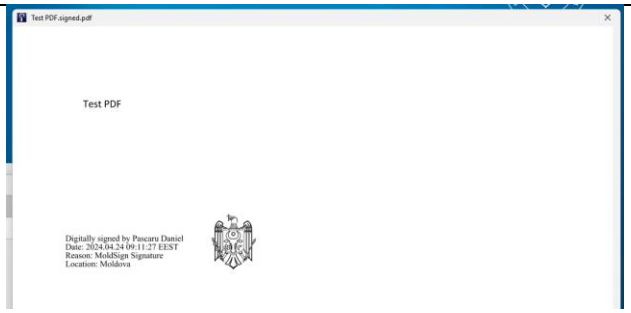
Dacă conținutul documentului electronic a suportat modificări/alterări după aplicarea semnăturii electroncie calificate (exemplu doc alterat mai jos):



La verificarea acestui document apare mențiunea ***"has been altered"***, fapt care se referă la **modificări aduse în conținutul documentului electronic** și **nu semnăturii electronice calificate aplicată**:



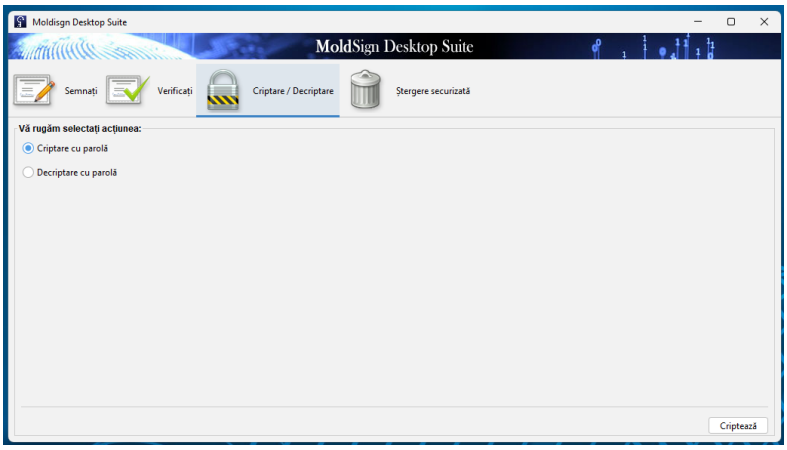
În fereastra **„View PDF"**, după notificare că documentul electronic a suportat modificări, la tentativa de a descărca acest document pentru a identifica modificările/alterările aduse, se va deschide documentul electronic inițial, care nu conține intervențiile ulterioare (după cum se poate vedea în imagine).



NOTĂ: Verificarea autenticității semnăturii electronice calificate este obligatorie pentru orice document electronic primit, deoarece este posibil ca conținutul acestuia să fie modificat și să fie semnat din nou de către o altă persoană.

3.5 Criptarea/ decriptarea fișierelor

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



3.5.1 Criptare cu parolă

Pentru criptarea cu parolă a unui fișier selectați opțiunea **Criptare cu parolă** (**Encrypt with password**) din tabul **Criptare/Decriptare (Encrypt/ Decrypt)**. 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

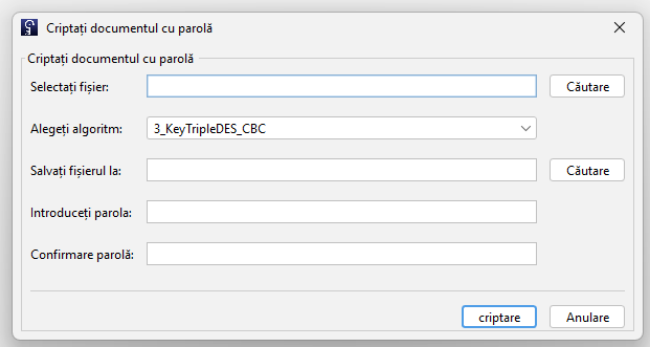
- 128bit_AES
- 192bit_AES
- 256bit_AES

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

Calea de salvare a fișierului criptat este completată automat de aplicație. La necesitate, se va putea selecta stocarea fișierului într-un alt folder sau sub un nume diferit.

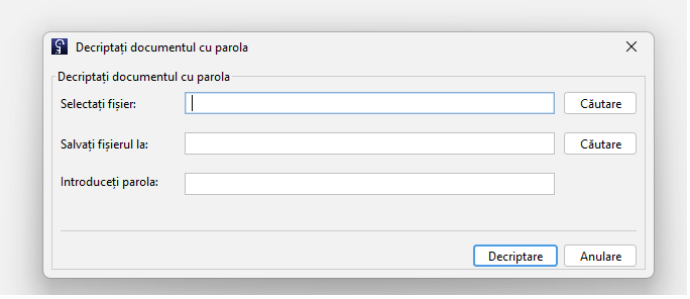
În final trebuie să introduceți parola pentru criptare. Pentru a evita erorile la scrierea parolei, aceasta trebuie confirmată.

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



3.5.2 Decriptare cu parolă

Decriptarea unui fișier criptat anterior cu o parolă are loc prin selectarea opțiunii **Decriptați documentul cu parolă** (**Decrypt with password**) din tabul **Encrypt/Decrypt** (**Criptare/ Decriptare**). Dacă ați selectat această opțiune și ați apăsat butonul **Decriptare** (**Decrypt**), 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 modificarea acesteia.
La etapa finală trebuie să introduceți parola pentru decriptare, iar apoi să apăsați pe butonul **Decriptare** (**Decrypt**).



3.6 Ștergerea securizată (distrugerea) fișierelor

Scopul acestei acțiuni este ștergerea fișierelor astfel încât acestea să nu poată fi recuperate

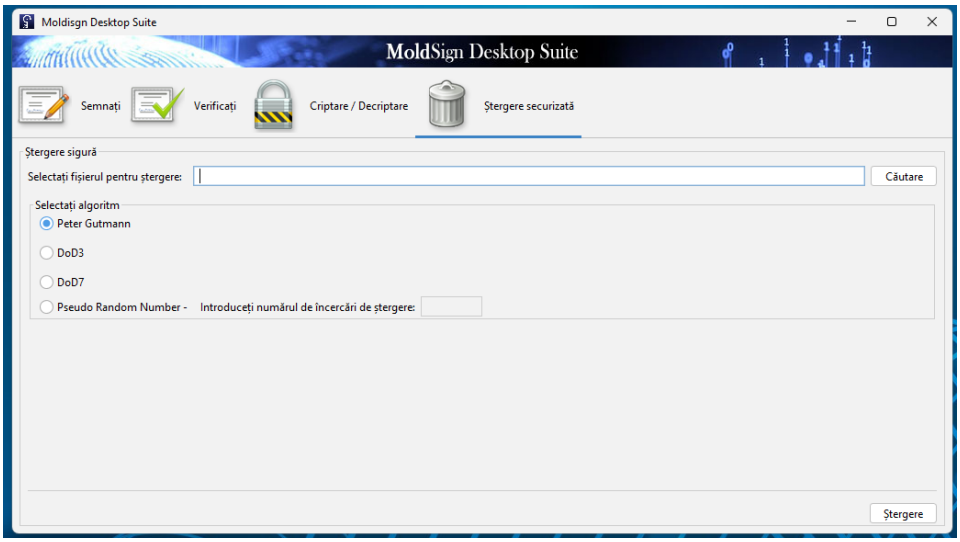
prin intermediul oricărui mijloc de program. Toți algoritmii minimalizează posibilitatea recuperării prin supra-scrierea acelui fișier de mai multe ori (în anumite cazuri, de până la 35 de ori) pentru a elimina toate câmpurile magnetice reziduale de pe discurile unde este (sunt) stocat/e fișierul (fișierele).

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 **Ștergere (Delete)**.



4 MoldSign Desktop pentru SO MAC

4.1 Instalare, setare

Goliți memoria cache a stației de lucru, restartați computerul.

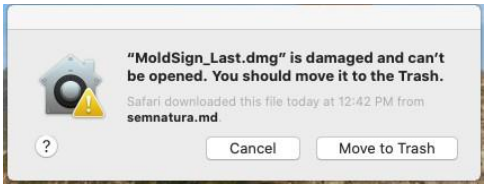
Accesați https://semnatura.md/ și descărcați programul MoldSign Desktop. Instalareaeste demarată prin lansarea fișierului de instalare MoldSign_ Last.dmg.

Instalarea la Mac a fost simplificata prin adaugare versiunii portabile ale aplicatiei, doar se lanseaza MoldSign_ Last.dmg

Lansați aplicația MoldSign Server, urmînd calea **Applications –> STISC ->MoldSign Server**

Lansați aplicația MoldSign Desktop, urmînd calea **Applications –> STISC ->MoldSign Desktop**

NOTĂ: dacă întîmpinați 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

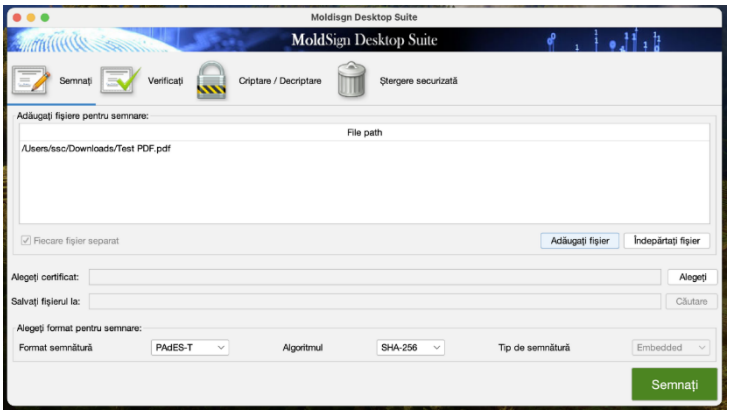
și pe Desktop apare iconița MoldSign  împreună cu fereastra

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

4.2 Semnarea fișierelor

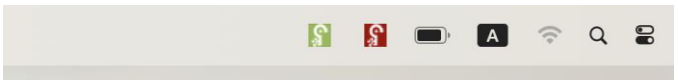
Semnarea fișierelor prin tabul **Semnați (Sign)** din meniul principal al aplicației se realizează prin executarea procesului de semnare descris mai jos:

1. adăugați fișierele ce trebuie semnate în lista de fișiere. Acest lucru poate fi realizat prin apăsarea pe butonul **Adăugați fișier (Add file),** 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 **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

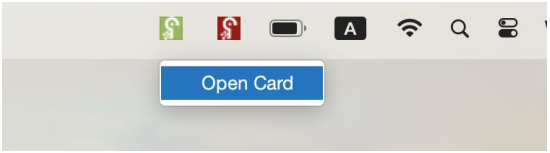
```
sh-3.2# xattr -cr /Users/nick/Downloads/ePass2003-Castle-mac-20170718_Release.dmg
```

(pentru ePass2003) sau

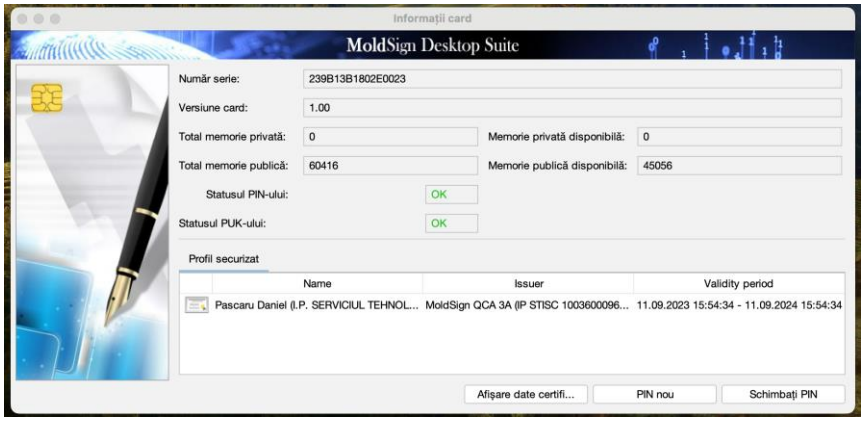
```
sh-3.2# xattr -cr /Users/nick/Downloads/acsccid_installer-1.1.4.dmg
```

pentru cryptomate 64.

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



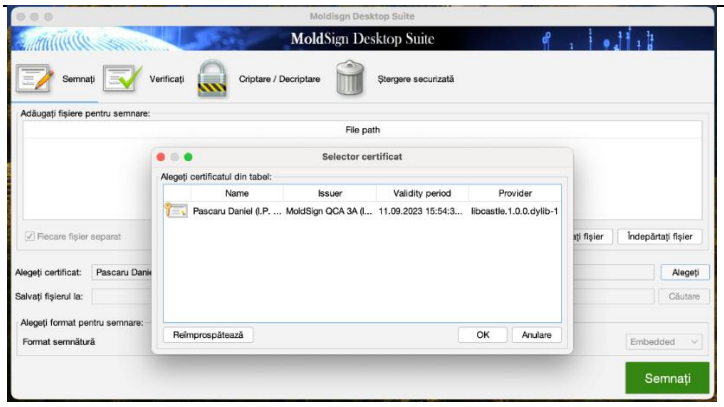
și fereastra **Card Information**



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 **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 pentrufișiere 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.

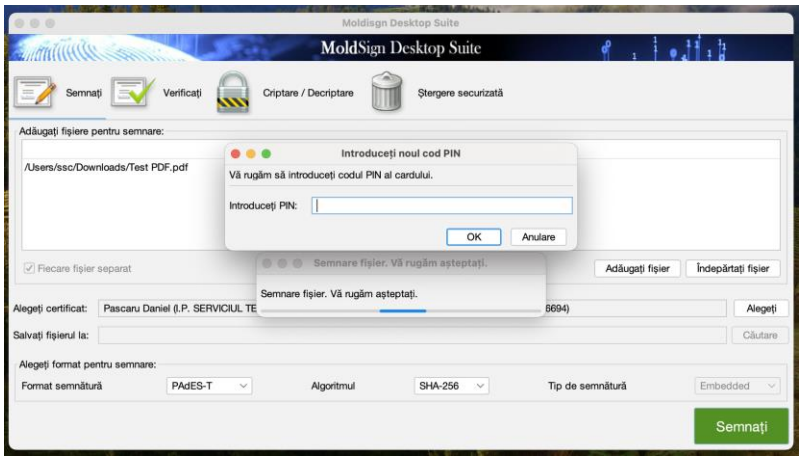
Altfel, fișierele sunt salvate prin adăugarea automată a extensiei **.xades** la sfârșitul numelui fișierului (pentru formatele de semnătură **XAdES**), sau prin adăugarea **.signed** în fața extensiei **.pdf** (pentru formate de semnătură **PAdES**).

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**) și **Pdf Preview ON** (**Previzualizarea semnătuii**).
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.



La finalizarea operațiunii, toate fișierele care au fost semnate cu succes vor fi eliminate din lista fișierelor ce trebuie semnate.

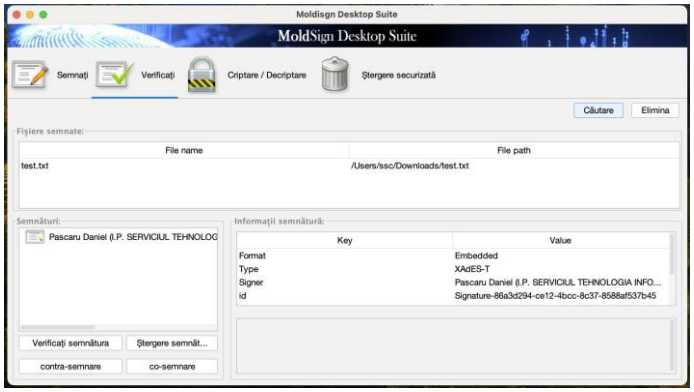
4.3 Verificarea semnăturilor XAdES

Semnăturile pot fi verificate prin tabul **Verifică**. Pentru aceasta selectați documentul electronic ce trebuie verificat. Atunci când alegeți un fișier valid XAdES restul câmpurilor din fereastră vorfi completate cu date:

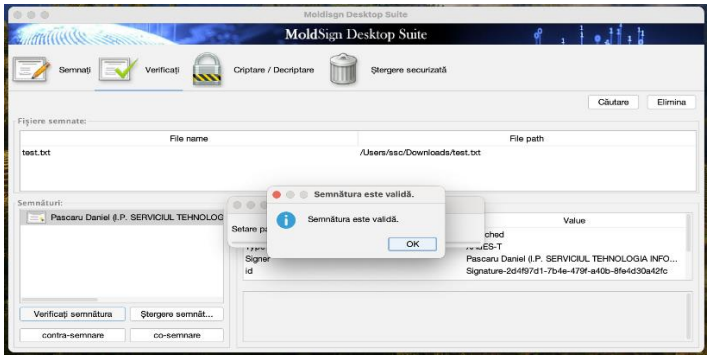
- **Files signed** (**Fișiere semnate**) – fișierele care au fost semnate cu fișierul de semnătură selectat. Prima coloană afișează numele fișierelor ce au fost semnate, în timp ce a doua coloană prezintă calea completă a acestui fișier pe calculatorul dvs. Dacă fișierele semnate sunt în același director (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 electronică calificată ce este selectatădin secțiunea **Signatures** (**Semnături**).

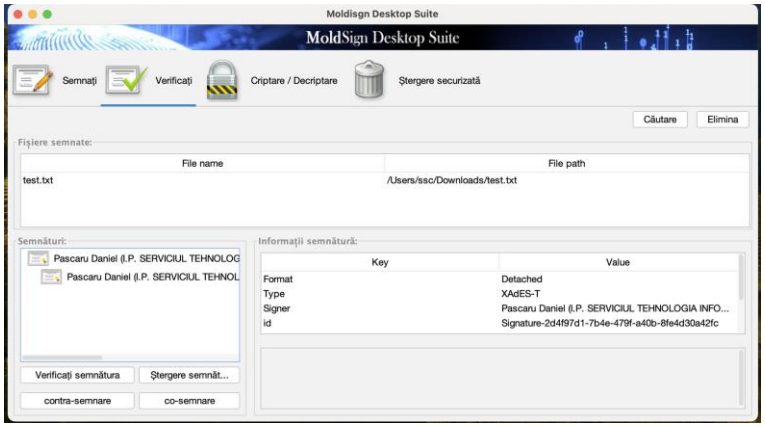


Sunt disponibile următoarele operațiuni pentru fiecare dintre semnăturile electronice calificate: **Verificați semnătura**. Aceasta operațiune verifică dacă semnătura electronică calificată este validă prin examinarea fișierelor semnate și a altor atribute ce sunt semnate. Dacă semnătura electronică calificată este validă, atunci apare un mesaj de tip pop-up.



Ștergere semnătură. Această operațiune vă permite să ștergeți o semnătură electronică calificată dacă ați făcut o greșeală. Operațiunea permite ștergerea acesteia numai dacă această semnătură a fost ulterior contrasemnată. De asemenea, dacă există doar o semnătură electronică calificată în arbore, aceasta nu poate fi ștearsă. Înainte de ștergerea unei semnături electronice calificate se va solicita o confirmare suăplimentară pentru ștergere.

Co-semnare/Contra-semnare. Aceste operațiuni adaugă o semnătură electronică calificată suplimentară semnăturilor existente. Acestea sunt utilizate ca și confirmare a semnăturii. În cazul co-semnării, noua semnătură electronică calificată 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.

Astfel, co-semnătura semnează aceleași date ca și semnătura electronică calificată originală. Contra- semnătura semnează semnătura electronică calificată originală, făcând-o „rezistentă" la modificare.

4.4 Verificarea semnăturilor PAdES

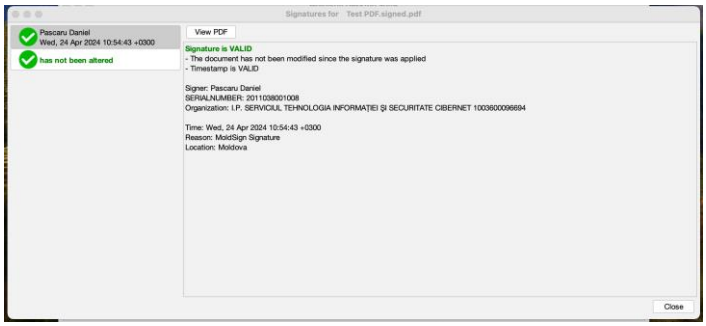
Semnăturile pot fi verificate prin tabul **Verifică**. Pentru aceasta selectați fișierul ce trebuie verificat. Atunci când alegeți un fișier valid PAdES(.pdf), câmpurile din fereastră vor fi completate cu date:

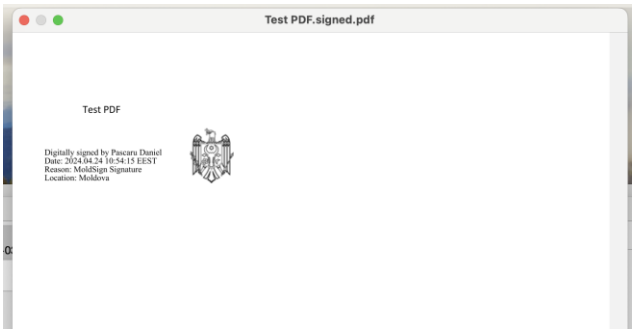
- **Fișiere semnate -** *Prima coloană* afișează numele fișierelor ce au fost semnate, în timp ce a *doua coloană* prezintă calea completă a acestui fișier pe calculatorul dvs.

NOTĂ: Similar cu etapa de semnare a documentului electronic, la verificare, pentru selectarea documentului, 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.

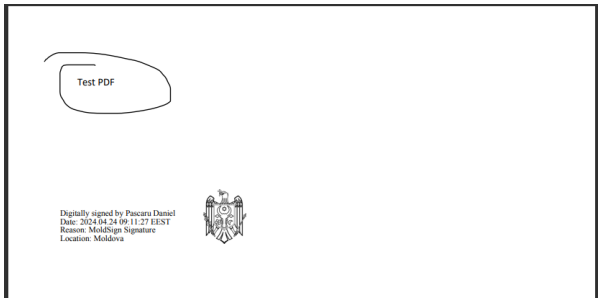
Semnatar, data/ora semnării, și IMPORTANT - verificarea conținutului documentului și confirmarea faptului că conținutul supus verificării nu a suportat modificări/alterări din momentul aplicării semnăturii electronice calificate.

"The document has not been modified since the signature was applied".



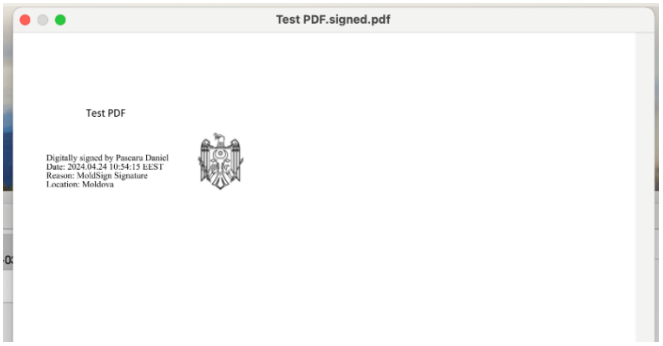


Dacă conținutul documentului electronic a suportat modificări/alterări după aplicarea semnăturii electroncie calificate (exemplu doc alterat mai jos):



La verificarea acestui document apare mențiunea ***"has been altered"***, care se referă la **modificări aduse în conținutul documentului electronic** și **nu semnăturii electronice calificate aplicată**:

În fereastra **„View PDF"**, după notificare că documentul electronic a suportat modificări, la tentativa de a descărca acest document pentru a identifica modificările/alterările aduse, se va deschide documentul electronic inițial, care nu conține intervențiile ulterioare (după cum se poate vedea în imagine).



NOTĂ: Verificarea autenticității semnăturii electronice calificate este obligatorie pentru orice document electronic primit, deoarece este posibil ca conținutul acestuia să fie modificat și să fie semnat din nou de către o altă persoană.

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

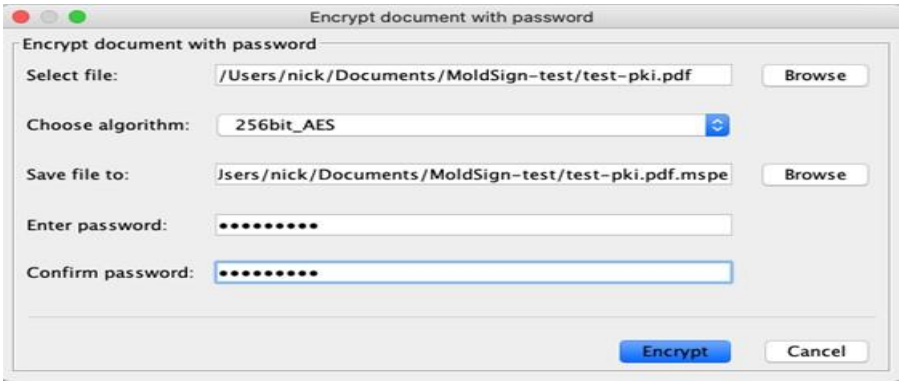
- 128bit_AES
- 192bit_AES
- 256bit_AES

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**).

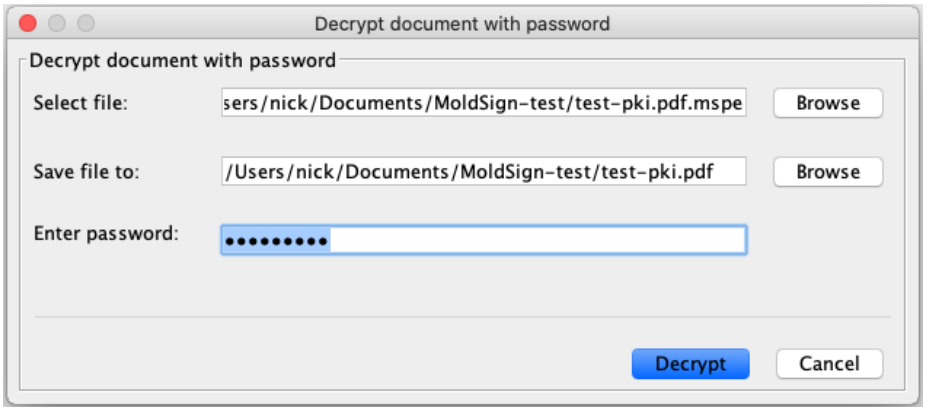


4.4.2 Decriptare cu parolă

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

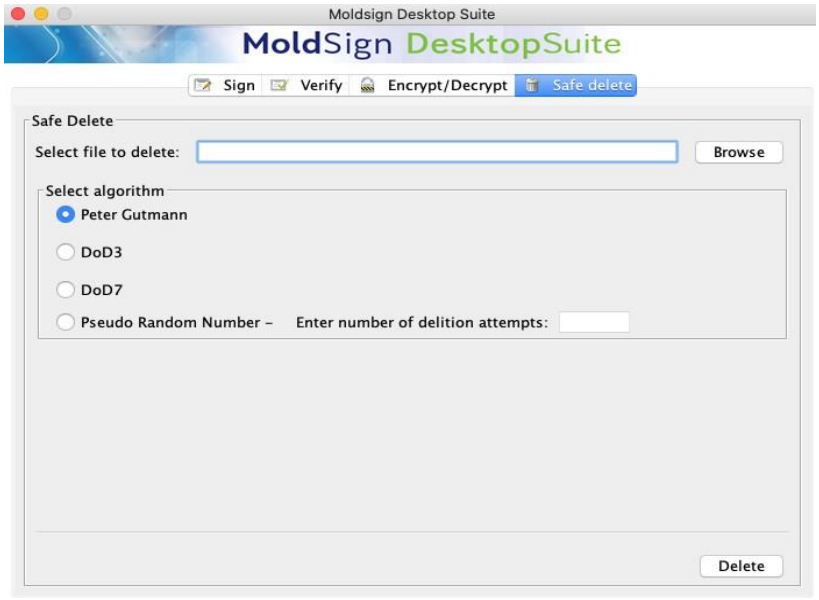
Scopul acestei acțiuni este ștergerea fișierelor astfel încât acestea să nu poată fi recuperate prin intermediul oricărui mijloc de program. Toți algoritmii minimalizează posibilitatea recuperării prin supra-scrierea acelui fișier de mai multe ori (în anumite cazuri, de până la 35 de ori) pentru a elimina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



5 MoldSign Desktop pentru SO Linux

5.1 Instalare, setare

Goliți memoria cache a stației de lucru, restartați computerul.

Accesați https://semnatura.md/ și descărcați fișierul MoldSign_2.2.0.tar.xz care contine MoldSign Desktop. Extragem din arhiva fisierele.

1. Deschide Terminalul: Începe prin a deschide un terminal pe sistemul tău.

2. Navighează la directorul fișierului: Folosește comanda cd pentru a te muta în directorul unde se află fișierul .tar.gz pe care vrei să-l extragi. De exemplu:

cd ~/Downloads

3. Extrage fișierul: Folosește comanda tar pentru a extrage fișierul. Comanda completă este:

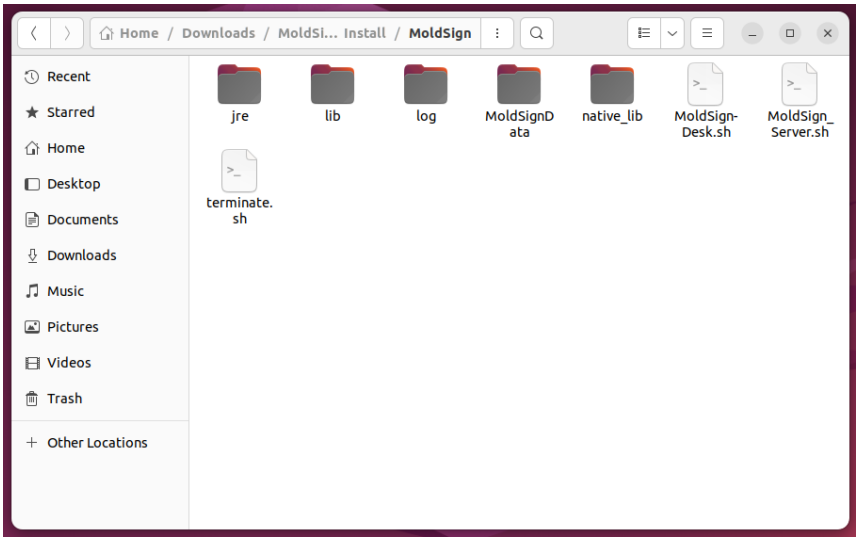
tar -xzvf MoldSign_2.2.0.tar.xz

Instalarea la Linux a fost simplificata prin adaugare versiunii portabile ale aplicatiei, doar se lanseaza MoldSign_Server.sh apoi MoldSign_Desk.sh

Lansați aplicația MoldSign Server, urmînd calea **Downloads –> MoldSign_Install -> MoldSign -> MoldSign_Server.sh**

Lansați aplicația MoldSign Desktop, urmînd calea **Downloads –> MoldSign_Install ->**

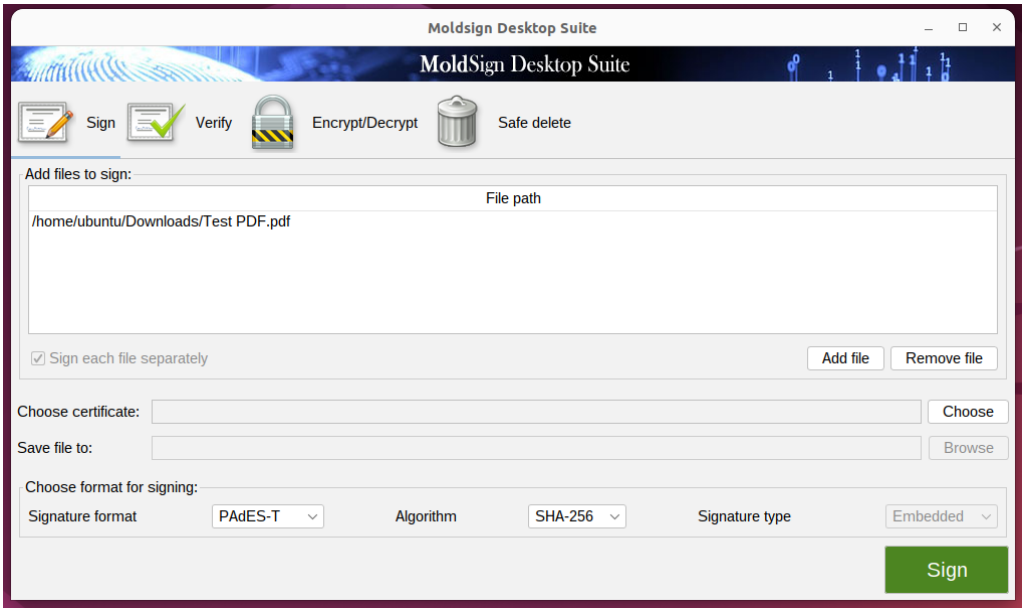
MoldSign -> MoldSign_Desk.sh



5.2 Semnarea fișierelor

Semnarea fișierelor prin tabul **Semnați (Sign)** 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 **Adăugați fișier (Add file),** 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

Îndepărtați fișier.

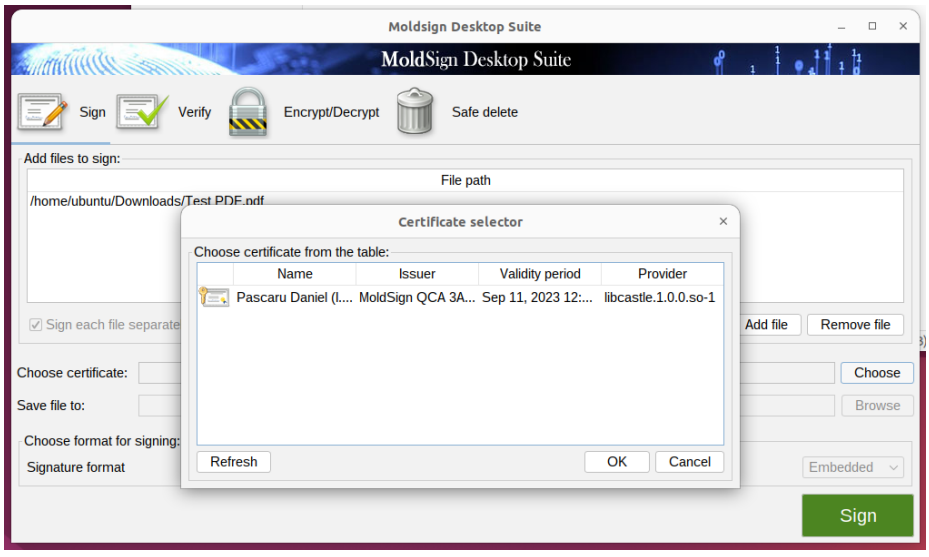
2. Introduceți în calculator dispozitivul cu care doriți să semnați și așteptați câteva secunde.

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

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 **Alegeți(Choose)**, 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**).

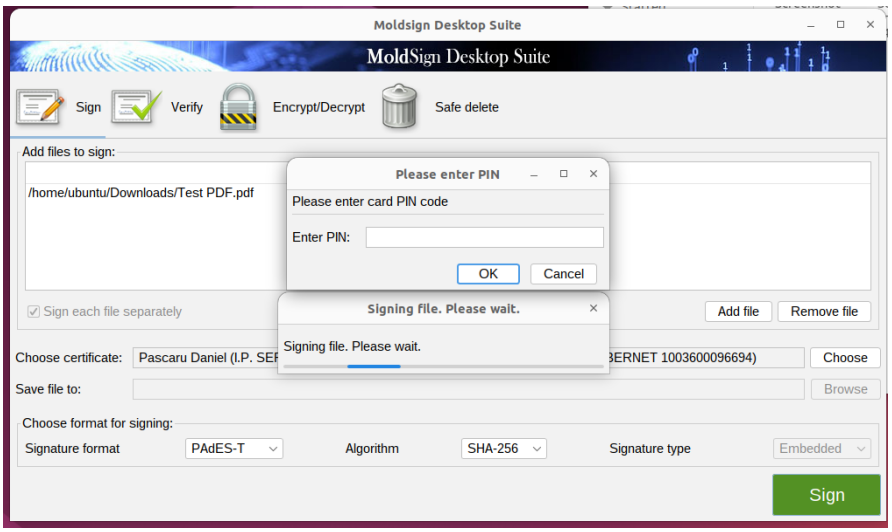
Pentru formatul **XAdES** sunt disponibile ambele tipuri, însă, pentru limitarea consumului de resurse, formatul **Embedded** (**Încorporată**) este disponibil numai pentrufișiere mai mici de 100KB.

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.

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



La finalizarea operațiunii, toate fișierele care au fost semnate cu succes vor fi eliminate din lista fișierelor ce trebuie semnate.

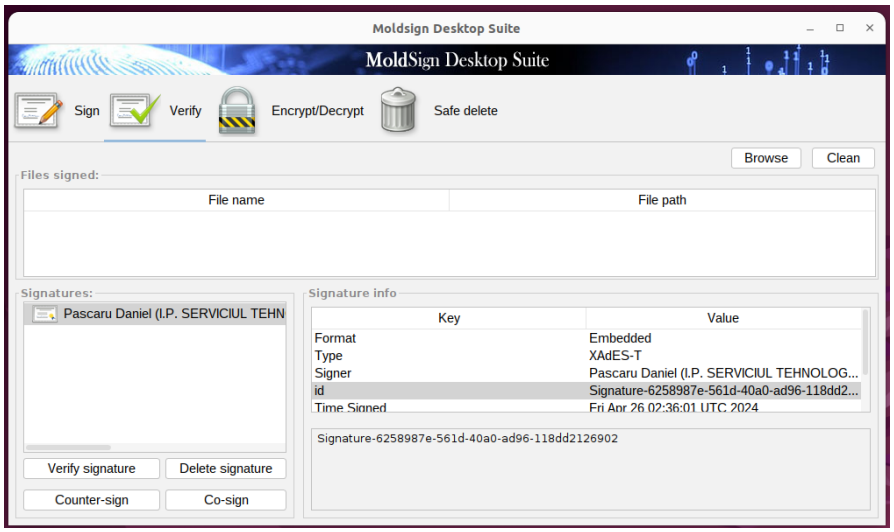
5.3 Verificarea semnăturilor XAdES

Semnăturile pot fi verificate prin tabul **Verifică**. Pentru aceasta selectați documentul electronic ce trebuie verificat. Atunci când alegeți un fișier valid XAdES restul câmpurilor din fereastră vorfi completate cu date:

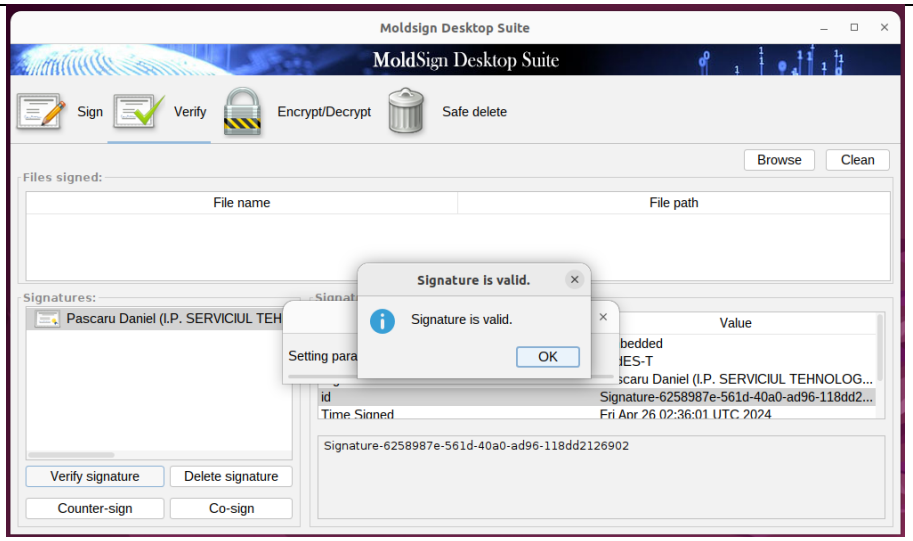
- **Files signed (Fișiere semnate)** – fișierele care au fost semnate cu fișierul de semnătură selectat. Prima coloană afișează numele fișierelor ce au fost semnate, în timp ce a doua coloană prezintă calea completă a acestui fișier pe calculatorul dvs. Dacă fișierele semnate sunt în același director (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 electronică calificată ce este selectatădin secțiunea **Signatures (Semnături)**.

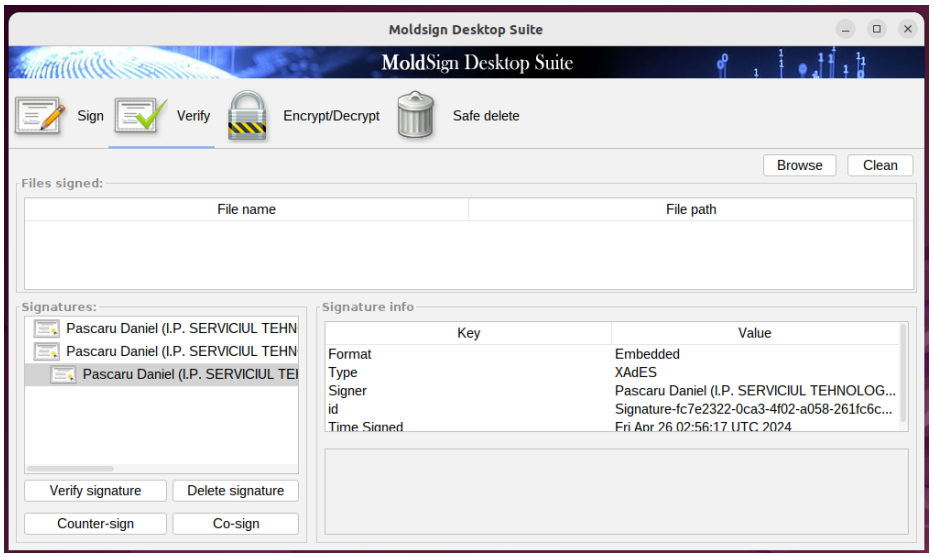


Sunt disponibile următoarele operațiuni pentru fiecare dintre semnăturile electronice calificate: **Verificați semnătura**. Aceasta operațiune verifică dacă semnătura electronică calificată este validă prin examinarea fișierelor semnate și a altor atribute ce sunt semnate. Dacă semnătura electronică calificată este validă, atunci apare un mesaj de tip pop-up.



Ștergere semnătură. Această operațiune vă permite să ștergeți o semnătură electronică calificată dacă ați făcut o greșeală. Operațiunea permite ștergerea acesteia numai dacă această semnătură a fost ulterior contrasemnată. De asemenea, dacă există doar o semnătură electronică calificată în arbore, aceasta nu poate fi ștearsă. Înainte de ștergerea unei semnături electronice calificate se va solicita o confirmare suăplimentară pentru ștergere.

Co-semnare/Contra-semnare. Aceste operațiuni adaugă o semnătură electronică calificată suplimentară semnăturilor existente. Acestea sunt utilizate ca și confirmare a semnăturii. În cazul co-semnării, noua semnătură electronică calificată 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.

Astfel, co-semnătura semnează aceleași date ca și semnătura electronică calificată originală. Contra- semnătura semnează semnătura electronică calificată originală, făcând-o „rezistentă”

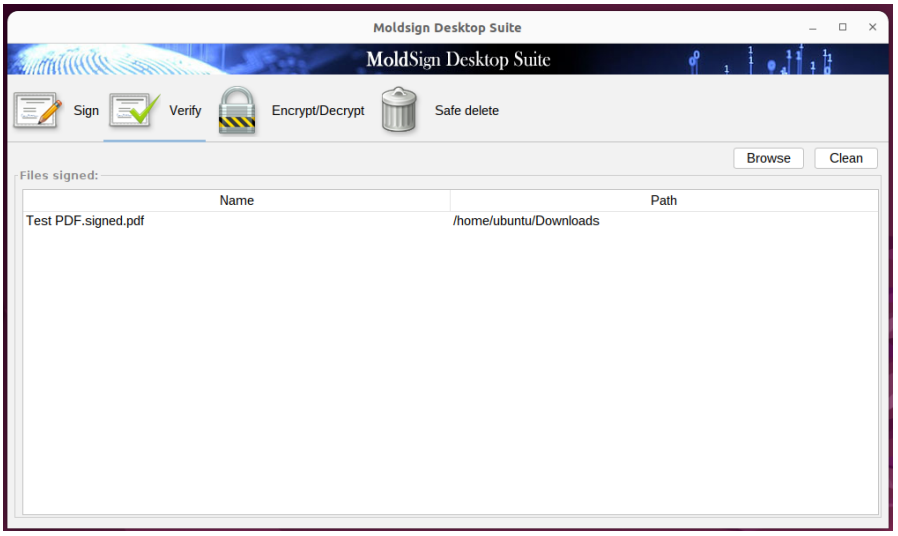
la modificare.

5.4 Verificarea semnăturilor PAdES

Semnăturile pot fi verificate prin tabul **Verifică**. Pentru aceasta selectați fișierul ce trebuie verificat. Atunci când alegeți un fișier valid PAdES(.pdf), câmpurile din fereastră vor fi completate cu date:

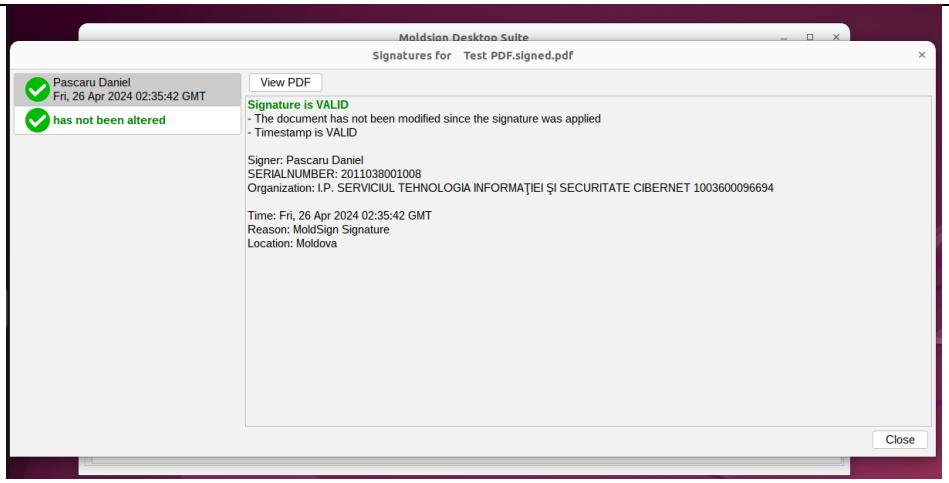
- **Fișiere semnate -** *Prima coloană* afișează numele fișierelor ce au fost semnate, în timp ce a *doua coloană* prezintă calea completă a acestui fișier pe calculatorul dvs.

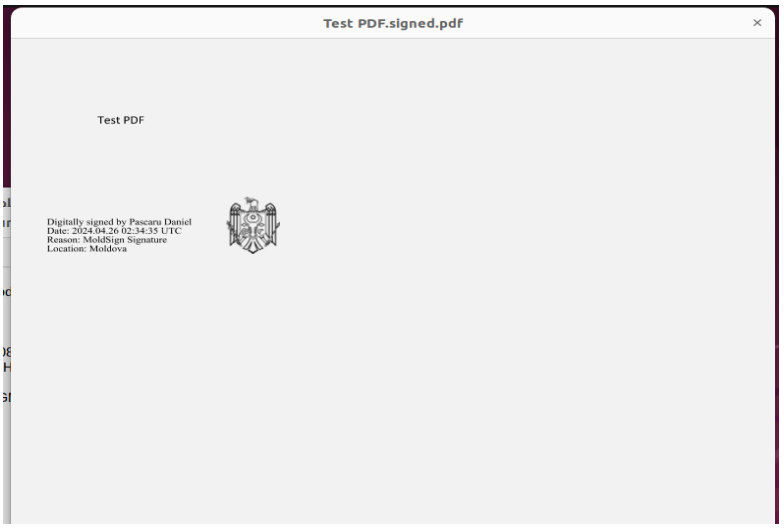
NOTĂ: Similar cu etapa de semnare a documentului electronic, la verificare, pentru selectarea documentului, ce va deschide o nouă fereastră pentru căutarea fișierelor în sistemul de fișiere. Există și posibilitatea introducerii în listă a fișierelor prin Drag & Drop direct din aplicația File Explorer.



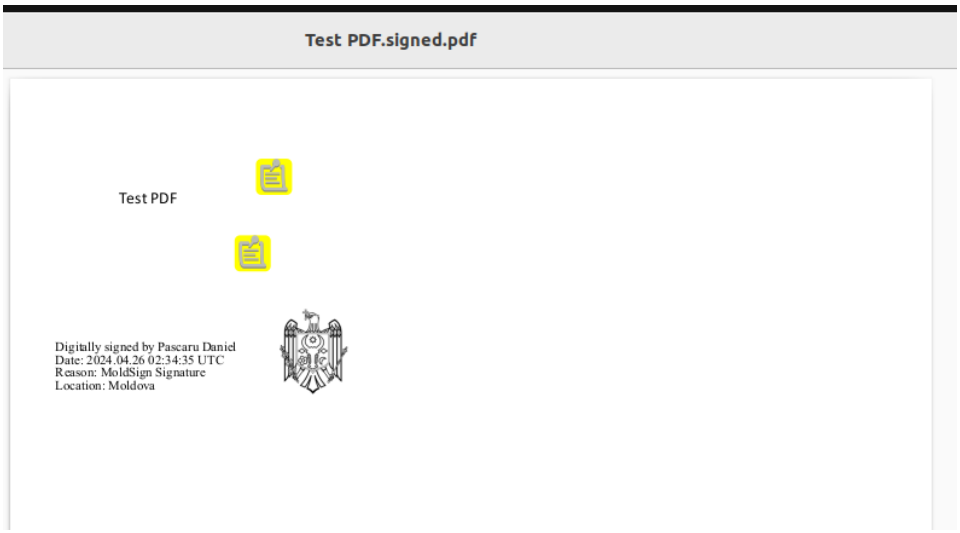
Semnatar, data/ora semnării, și IMPORTANT - verificarea conținutului documentului și confirmarea faptului că conținutul supus verificării nu a suportat modificări/alterări din momentul aplicării semnăturii electronice calificate.

"The document has not been modified since the signature was applied".

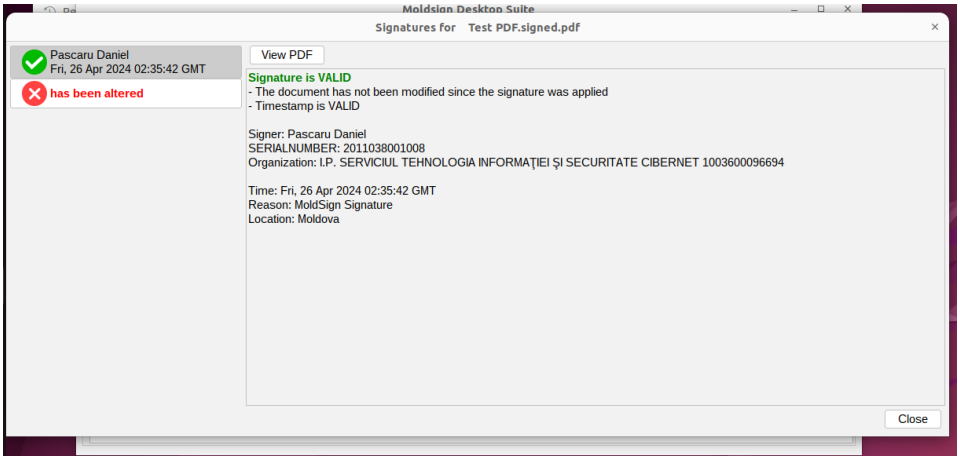




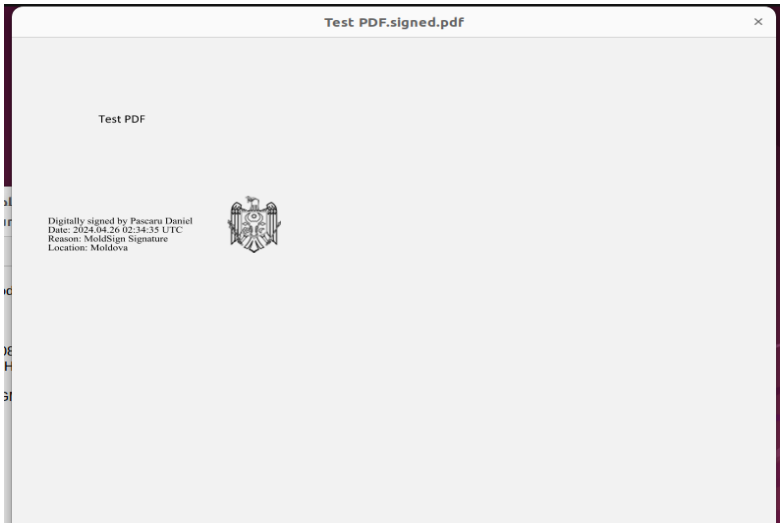
Dacă conținutul documentului electronic a suportat modificări/alterări după aplicarea semnăturii electroncie calificate (exemplu doc alterat mai jos):



La verificarea acestui document apare mențiunea ***"has been altered"***, care se referă la **modificări aduse în conținutul documentului electronic** și **nu semnăturii electronice calificate aplicată**:



În fereastra **„View PDF”**, după notificare că documentul electronic a suportat modificări, la tentativa de a descărca acest document pentru a identifica modificările/alterările aduse, se va deschide documentul electronic inițial, care nu conține intervențiile ulterioare (după cum se poate vedea în imagine).



NOTĂ: Verificarea autenticității semnăturii electronice calificate este obligatorie pentru orice document electronic primit, deoarece este posibil ca conținutul acestuia să fie modificat

și să fie semnat din nou de către o altă persoană.

5.4.1 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:

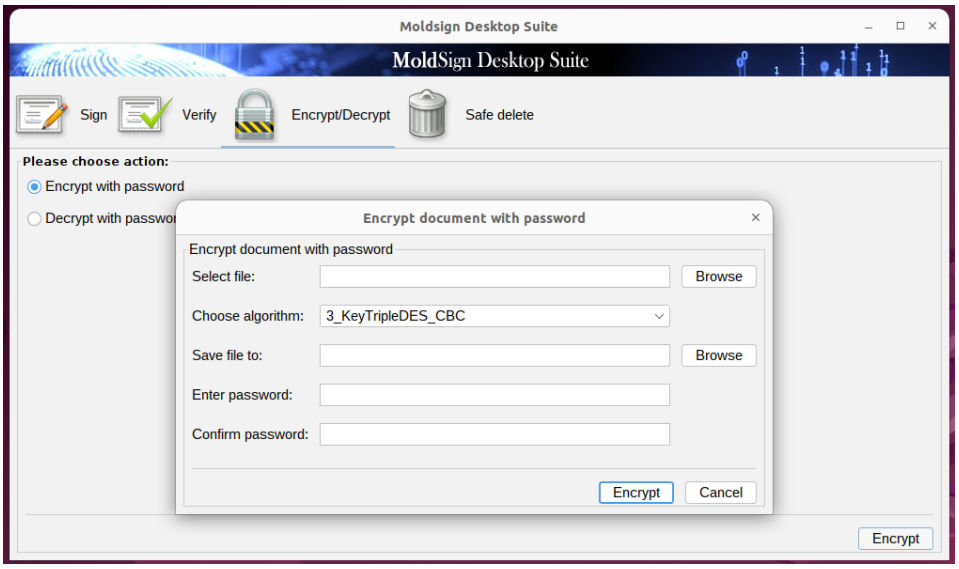
- 3 KeyTripleDES CBC
- 2 KeyTripleDES CBC
- DES CBC
- RC2 CBC
- RC4
- 128bit_AES
- 192bit_AES
- 256bit_AES

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.

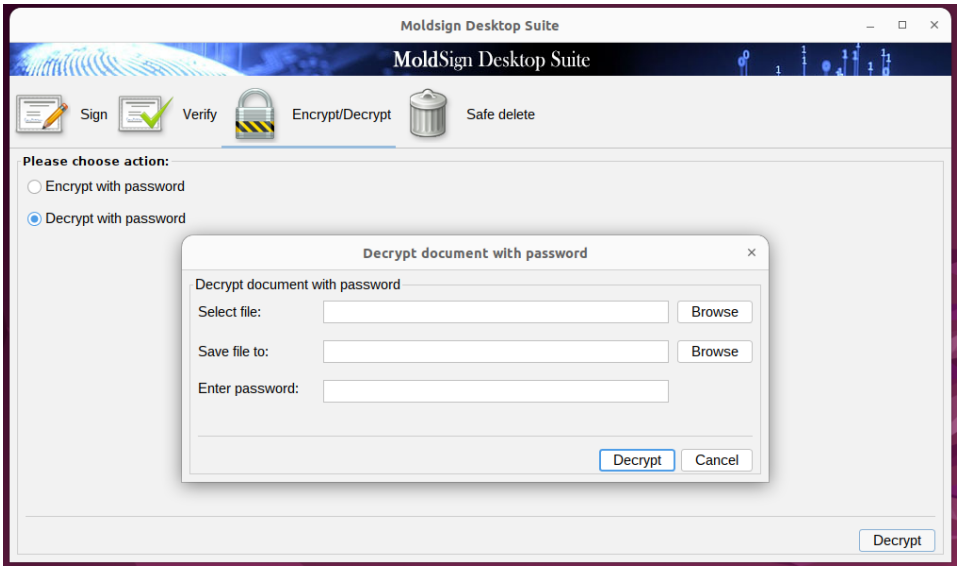
Criptarea este realizată după apăsarea butonului **Encrypt** (**Criptează**).



5.4.2 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**).



5.5 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**).