Instrucțiuni pentru instalarea și utilizarea corespunzătoare a aplicației DigiSigner ONE

versiunea 1.4.1

I.Descrierea aplicației DigiSigner ONE

DigiSigner ONE este singura aplicație software din România care incorporează principalele operațiuni pentru utilizarea și gestiunea certificatelor digitale calificate.

Aplicația software DigiSigner ONE, utilizată împreună cu certificatul digital calificat sau certificatul digital pentru criptare DigiSign, aduce o securitate de necontestat documentelor și fișierelor prin funcționalitățile de semnare electronică, marcare temporală, verificare a fișierelor semnate electronic, criptare și decriptare integrate.

Sisteme de operare compatibile:
- ✓ Windows Vista
- ✓ Windows 7
- ✓ Windows 8, 8.1
- ✓ Windows 10
- ✓ Windows 11

Standarde criptografice utilizate:
- ✓ PKCS#7
- ✓ CAdES
- ✓ PAdES
- ✓ PKCS#11
- ✓ PKCS#12
- ✓ Microsoft CryptoAPI
- ✓ X.509 v3

Algoritmi de securitate integrați:
- ✓ AES
- ✓ DES
- ✓ 3DES
- ✓ SHA-1
- ✓ SHA-256
- ✓ RSA 2048 de biți

Beneficii oferite:
- ✓ Principalele operațiuni pentru utilizarea și gestiunea certificatului digital calificat DigiSign sunt integrate în cadrul unei singure aplicații software.
- ✓ Aplicația are interfață grafică modernă, intuitivă și ușor de utilizat.
- ✓ Aplicația permite vizualizarea documentelor PDF înainte ca acestea să fie semnate.
- ✓ Documentație de utilizare și funcționalități de suport tehnic sunt integrate în cadrul aplicației.
- ✓ Toate promoțiile și noutățile publicate de către DigiSign sunt afișate în cadrul meniului aplicației.

Semnarea electronică a fișierelor

Utilizând certificate digitale calificate, stocate pe dispozitive criptografice securizate compatibile cu standardul PKCS#11 sau stocate în containere de tip PKCS#12, aplicația DigiSigner-ONE permite utilizatorilor să semneze electronic orice tip de fișier într-un mod facil.
Fișierele semnate pot fi de tip .p7s/.p7m sau .PDF, în funcție de opțiunea dorită.

Aplicarea mărcilor temporale

DigiSigner ONE utilizează serverul Autorității acreditate de marcare temporală DigiSign pentru aplicarea mărcilor temporale în momentul semnării electronice a fișierelor, garantând în acest mod faptul că respectivele date au fost semnate la un moment cert de timp.

Verificarea fișierelor semnate electronic

Utilizatorii aplicației DigiSigner ONE au posibilitatea de a verifica validitatea certificatului digital semnatar prin verificarea semnăturii electronice asociate respectivului fișier și afișarea rezultatului verificării într-un mod ușor de interpretat.

Criptarea și decriptarea fișierelor

DigiSigner ONE oferă utilizatorilor posibilitatea de a cripta fișiere pentru unul sau mai mulți destinatari pentru protejarea datelor împotriva accesului neautorizat. Doar destinatarii selectați de utilizator pot decripta fișierul care a fost criptat cu ajutorul algoritmilor criptografici integrați în aplicație.

Funcționalități utile

Toți utilizatorii sunt informați de promoțiile și noutățile oferite de către DigiSign, acestea fiind afișate direct în cadrul aplicației.
În plus, departamentul de suport tehnic DigiSign, disponibil 24/7, este doar la un click distanță de dvs, fiind necesar doar să accesați opțiunea din cadrul meniului principal și să ne transmiteți un mesaj pentru ca echipa noastră să vă contacteze.

II. Instalarea aplicației DigiSigner ONE și a certificatului digital DigiSign

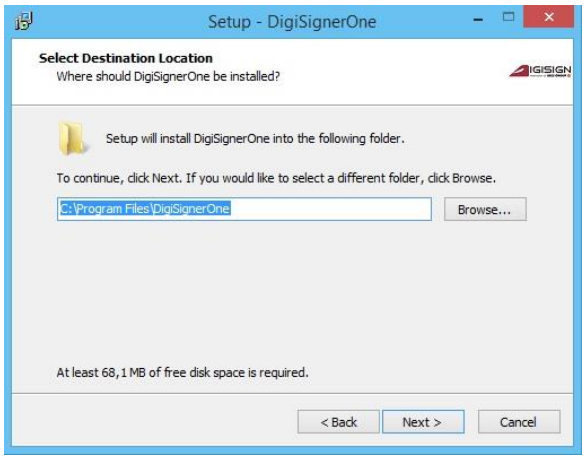
1. Descărcați în calculator kit-ul de instalare de la una din adresele de mai jos:

a) DigiSigner ONE versiunea 64 de biti dacă sistemul dvs de operare este pe 64 de biți

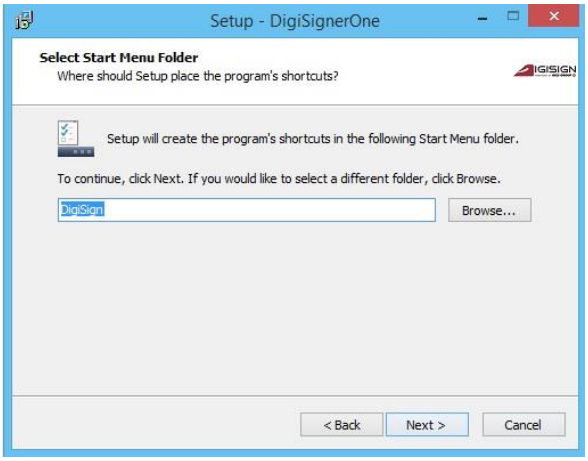
b) DigiSigner ONE versiunea 32 de biti dacă sistemul dvs de operare este pe 32 de biți

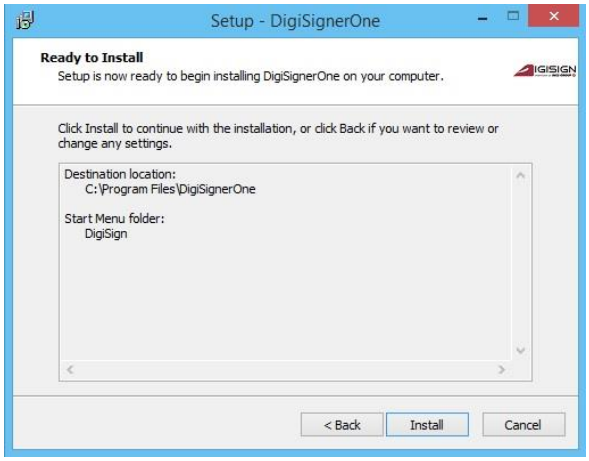
2. Deschideți fișierul descărcat în calculator, selectați limba dorită pentru instalare și apăsați butonul ***OK***

3. Apăsați butonul ***Next*** și pe urmă ***Next*** din nou



3. Apăsați butonul ***Next*** și pe urmă butonul ***Install***





4. În următorul pas va trebui să selectați componentele necesare pentru utilizarea certificatului digital calificat DigiSign, emis pe dispozitivul SafeNet eToken.

- ✓ Opțiunile **Install eToken driver** și **Install DigiSign Trust Chain** vor trebui selectate doar dacă nu ați mai utilizat dispozitivul de tip token și certificatul digital calificat DigiSign pe calculatorul dvs până în acest moment.
- ✓ Opțiunea **Install program for previewing pdf - GhostScript GPL** va instala aplicația GhostScript care va permite aplicației DigSigner ONE să afișeze documentele PDF în cadrul aplicației.
- ✓ Opțiunea **Run DigiSigner One** va deschide aplicația DigiSigner ONE după ce veți apăsa butonul ***Finish***.

III. Instalarea driver-ului dispozitivului criptografic și a lanțului de încredere DigiSign

Atenție! Aceste etape trebuie parcurse doar în cazul în care ați bifat opțiunile **Install eToken driver** și **Install DigiSign Trust Chain** specificate la pasul anterior.

Dacă nu ați bifat aceste două opțiuni, vă rugăm să treceți la pasul **IV. Utilizarea aplicației DigiSigner ONE**.

Asigurați-vă că sistemul dumneavoastră de operare este actualizat la zi și că nu aveți vreun program de tip antivirus/firewall ce ar putea bloca instalarea corespunzătoare a driver-ului dispozitivului USB eToken.

Folosiți funcția **Windows Update** sau urmați procedurile de pe site-ul Microsoft în vederea instalării ultimelor update-uri aferente sistemului dumneavoastră de operare și a browser-ului Internet Explorer.

IMPORTANT! Asigurați-vă că:

- aveți drepturi de administrator pe sistemul pe care doriți să instalați certificatul digital
- ceasul, data și fusul orar de pe calculator sunt corect setate

- dispozitivul eToken NU este conectat în extensia USB a calculatorului pe durata procesului de instalare al aplicațiilor!

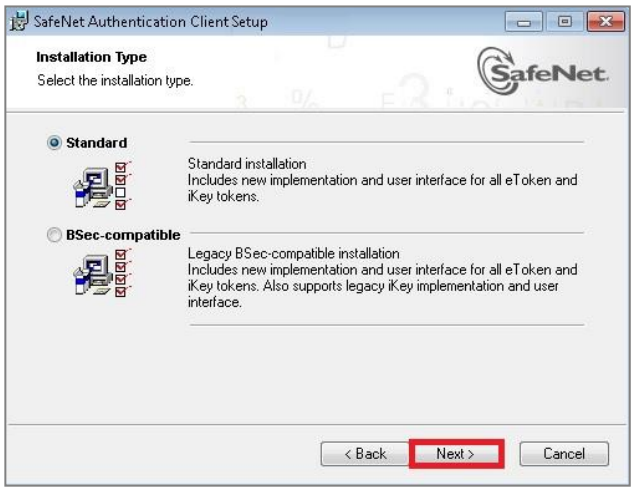
1. Instalarea driver-ului DigiSign eToken PKI Client

Compatibilitate:
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11;
- Windows Server 2003, Windows Server 2008, Windows Server 2012.

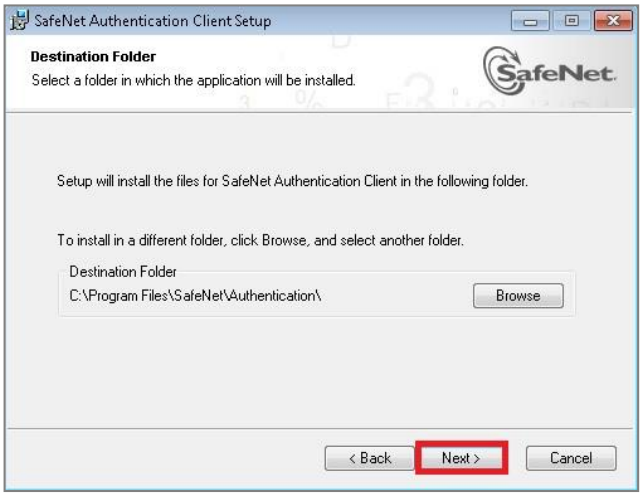
Dacă opțiunea *Install eToken driver* a rămas bifată, va porni instalarea driverului și va trebui să apăsați butonul *Run* pentru a începe procesul de instalare.

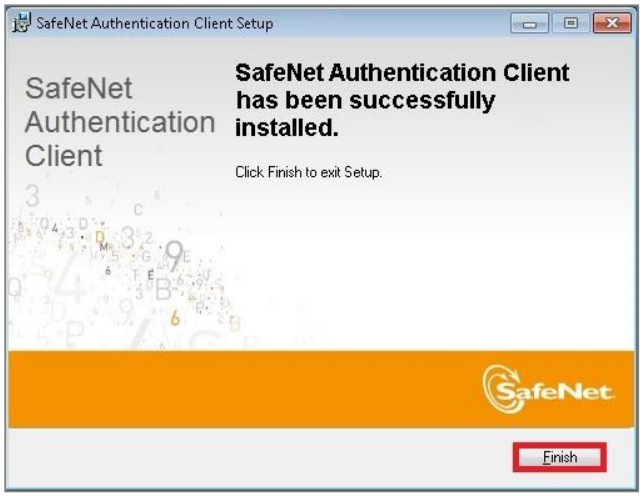
În fereastra nou deschisă, apăsați butonul *Next* pentru a începe instalarea, selectați limba dorită și apăsați butonul *Next.*

Bifați câmpul ***I accept the license agreement***, apăsați butonul *Next*, iar în următoarea fereastră lăsați bifat tipul ***Standard*** și continuați alegând butonul *Next.*



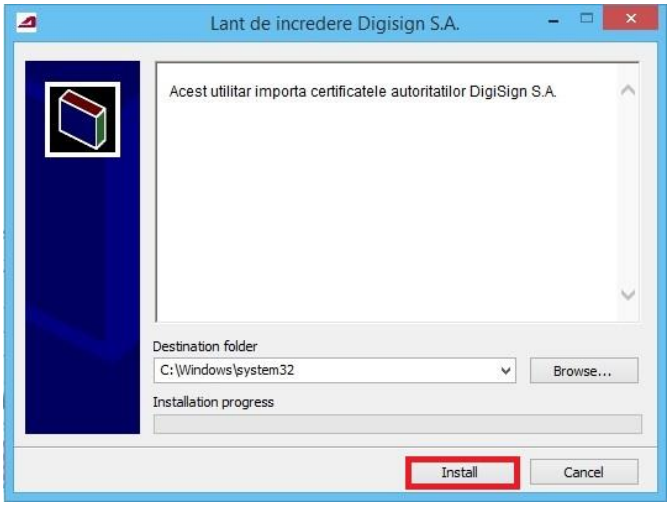
Apăsați butonul *Next* și *Finish* pentru a finaliza instalare driver-ului.





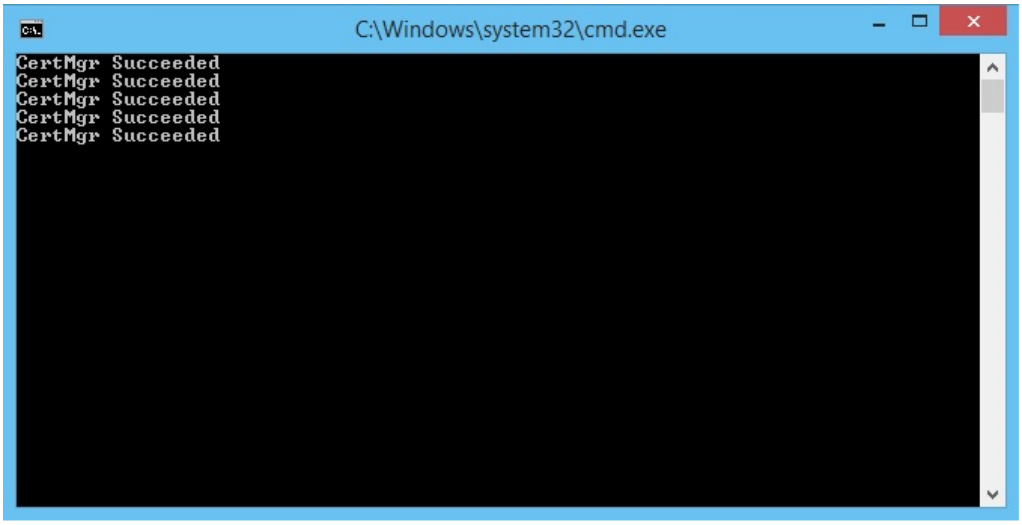
2. Instalarea lanțului de încredere DigiSign

Dacă opțiunea *Install DigiSign Trust Chain* a rămas bifată, va porni instalarea lanțului de încredere DigiSign și va trebui să apăsați butonul *Install* pentru a începe procesul.



IMPORTANT! Asigurați-vă că lanțul de încredere se instalează corect.

Într-o fereastră asemănătoare cu cea prezentată în imaginea de mai jos, va fi afișat mesajul „**CertMgr Succeeded**” atunci când lanțul de încredere a fost instalat de succes.

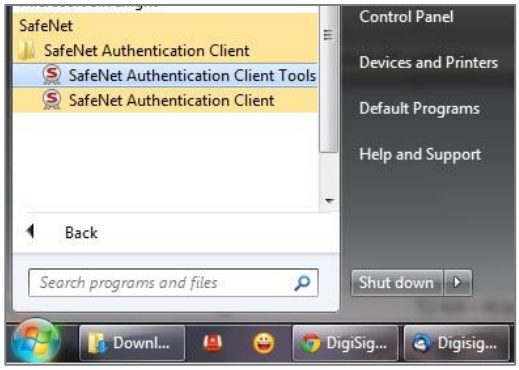


Dacă primiți mesajul *CertMgr Failed*, va trebui să descărcați în mod manual lanțul de încredere de la adresa http://digisign.ro/uploads/cert.zip , să dați *click-dreapta* pe fișierul ***cert.exe*** și să selectați opțiunea *„**Run as Administrator**”*.

În acest moment va trebui să conectați dispozitivul criptografic securizat USB SafeNet eToken la calculator.

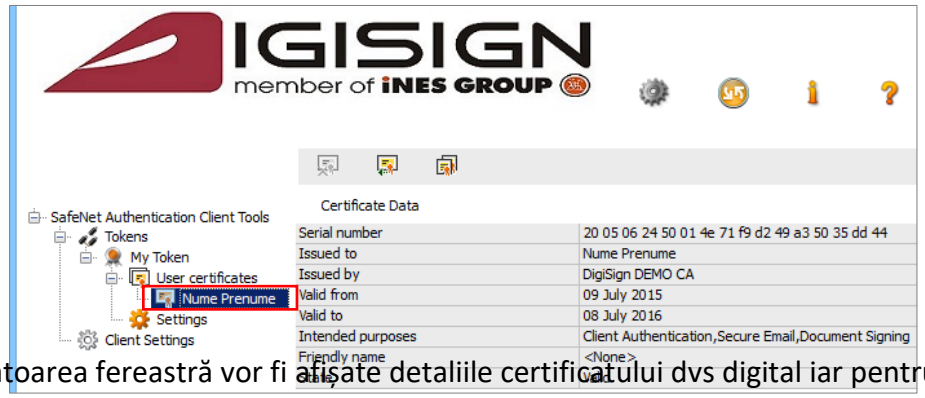
3. Verificarea instalării corespunzătoare a lanțului de încredere DigiSign și a driverului SafeNet

a) Din meniul **Start**, alegeți **All Programs** → **SafeNet** → **SafeNet Authentication Client** → **SafeNet Authentication Tools**.

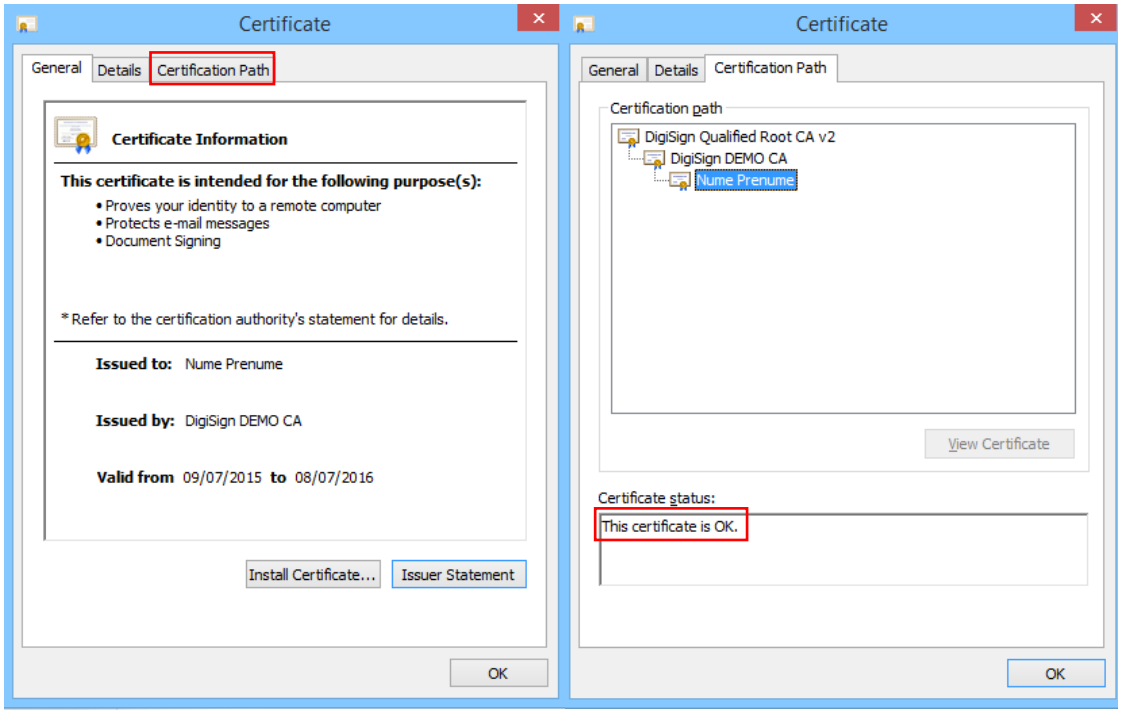


b) În fereastra care s-a deschis, apăsați butonul *Advanced View* (pictograma )

c) În meniul din partea stângă a aplicației, va trebui să dați dublu-click pe câmpul *User Certificates* și pe urmă din nou dublu click numele certificatului dvs digital.



d) În următoarea fereastră vor fi afișate detaliile certificatului dvs digital iar pentru a verifica faptul că acesta a fost instalat corespunzător va trebui să selectați panoul *Certificate Path* din partea superioară a ferestrei.



IMPORTANT! Daca vă apare mesajul *The issuer of this certificate could not be found* în câmpul *Certificate status* atunci **va trebui să parcurgeți din nou pașii pentru instalarea lanțului de încredere DigiSign** (pasul nr. 2 de la pag. 7 a prezentului document).

IV. Utilizarea aplicației DigiSigner ONE

Conectați în calculator dispozitivul criptografic USB eToken care conține certificatul digital calificat obținut de la DigiSign și porniți aplicația DigiSigner ONE fie prin deschiderea pictogramei DigiSigner ONE de pe desktop, fie prin deschiderea meniului **Start** ⇨ **All Programs** ⇨ **DigiSign** ⇨ **DigiSigner ONE**

Pictograma DigiSigner ONE

La deschiderea aplicației DigiSigner ONE, se va afișa pe ecran meniul principal care conține toate categoriile de funcționalități oferite.

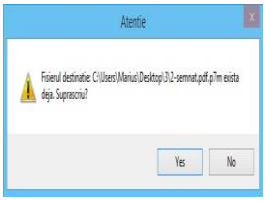
Meniul principal al aplicației DigiSigner ONE

1. Semnarea de fișiere P7M și P7S

a. Semnarea electronică a unui fișier se efectuează folosind opțiunile:

- **Fișier sursă:** Selectați fișierul pe care doriți să îl semnați;
- **Fișier semnat:** Selectați locul în care doriți să salvați fișierul semnat, precum și denumirea acestuia;
- **Certificat cu care se semnează:** Selectați certificatul digital cu care doriți să semnați;
- **Format fișier:** Selectați formatul fișierului semnat, respectiv:
  - **P7S**: **a.** Semnătură atașată – se va salva atât semnătura aplicată, cât și fișierul;
    b. Semnătură detașată – se va salva doar semnătura aplicată;
  - **P7M**: Se va salva atât semnătura aplicatâ, cât și fișierul original.
- **Standard:** *PKCS#7* sau *CADES*;
  Semnăturilor electronice extinse/avansate, create utilizând standardul CAdES, le este recunoscută valabilitatea și după ce perioada de valabilitate a certificatului a expirat.
- **Semnătură:** Selectați tipul semnăturii pe care doriți să o aplicați - semnătură, *co*-semnătură sau *contra*-semnătură;
- **Algoritm:** Selectați algoritmul criptografic pe care doriți să îl utilizați, respectiv *SHA-1* sau *SHA-256;*
- **Aplică marcă temporală:** Bifați această opțiune dacă doriți să includeți pe lângă semnătura electronică, și o marcă temporală care să ateste data și ora la care s-a semnat fișierul;
- **Extrage conținut:** Butonul devine activ dacă documentul selectat conține deja o semnătură;
- **Semnează fișier**: Apăsați acest buton în momentul în care doriți să semnați fișierul ales.

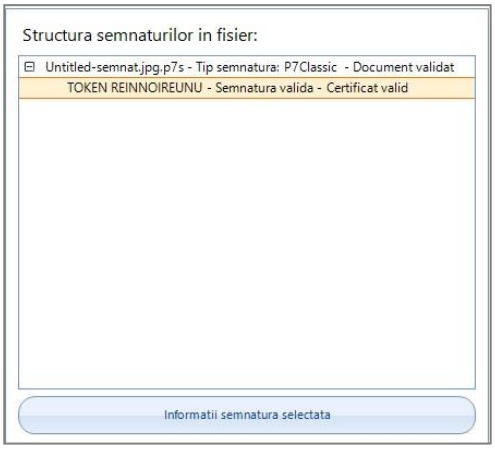
După selectarea butonului *Semnează fișier*, va fi afișat mesajul *Fisierul a fost semnat.*



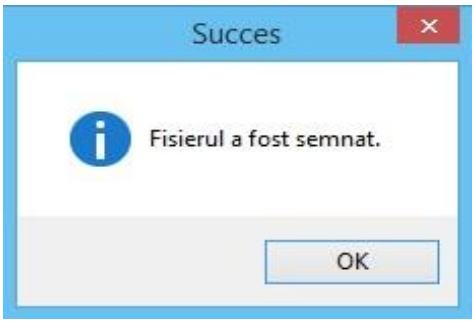
Dacă fișierul care urmează a fi semnat există deja în directorul respectiv, programul va afișa o atenționare în acest sens în care vă întreabă dacă doriți suprascrierea lui.

b. Structura semnăturilor din fișier

Dacă fișierul selectat pentru semnare conține deja o semnătura, ea va fi afișată în partea dreaptă, precum în exemplul de mai jos:

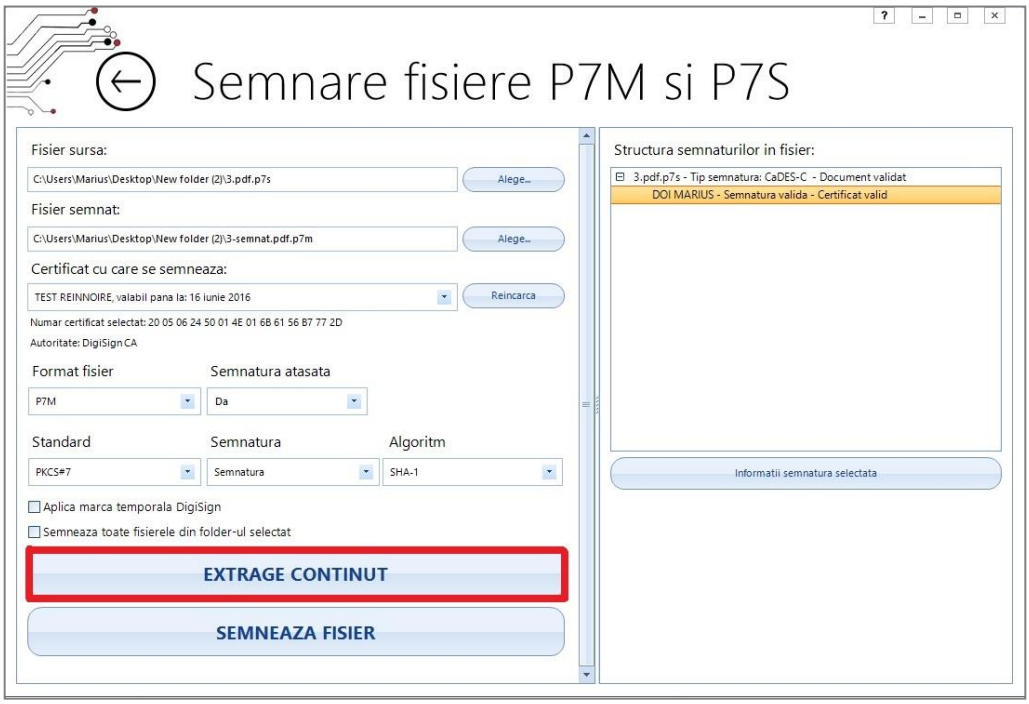


Pentru a vizualiza informațiile semnăturii, trebuie în primul rând să selectați o semnătură apoi să apăsați butonul *Informații semnatură selectată* și toate detaliile semnăturii vor apărea într-o fereastră nouă, precum starea semnăturii, dar și momentul aplicării ei.



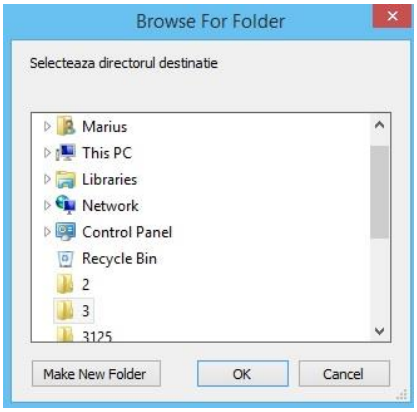
c. Extrage conținut

În cazul în care doriți să aplicați o co-semnătură sau contra-semnătură pe un fișier deja semnat, aveți posibilitatea de a-l verifica înainte prin selectarea butonului *Extrage conținut*, care va salva local fișierul original.

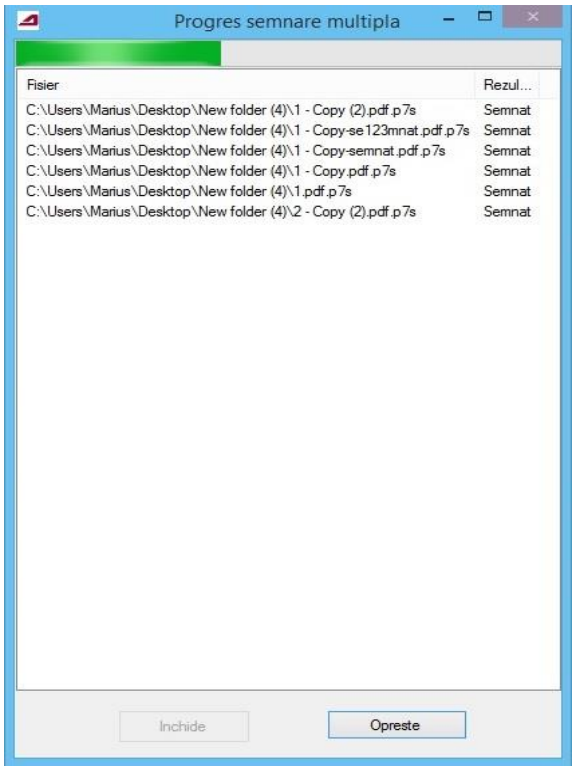


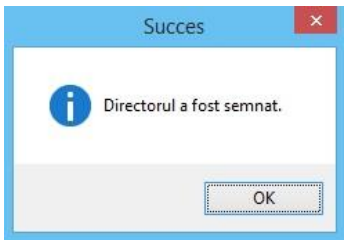
- **Semnează toate fișierele din folder-ul selectat:** Această opțiune vă permite semnarea tuturor documentelor dintr-un folder și necesită licențierea certificatului.
  Pentru achiziționarea licenței ne puteți contacta la adresa sales@digisign.ro și la numărul de telefon 031.620.12.88.

Dacă ați achiziționat deja o licența pentru semnarea unui folder de fișiere în format *p7m* și *p7s*, la selectarea opțiunii *Semnează toate fișierele din folder-ul selectat* va trebui să selectați folderul destinație, acesta fiind locul în care vor fi salvate fișierele semnate.



După selectarea folderului destinație, apăsați butonul *Semnează fisier* pentru a începe procesul de semnare. La finalul acestui proces veți primi mesajul *Directorul a fost semnat.*

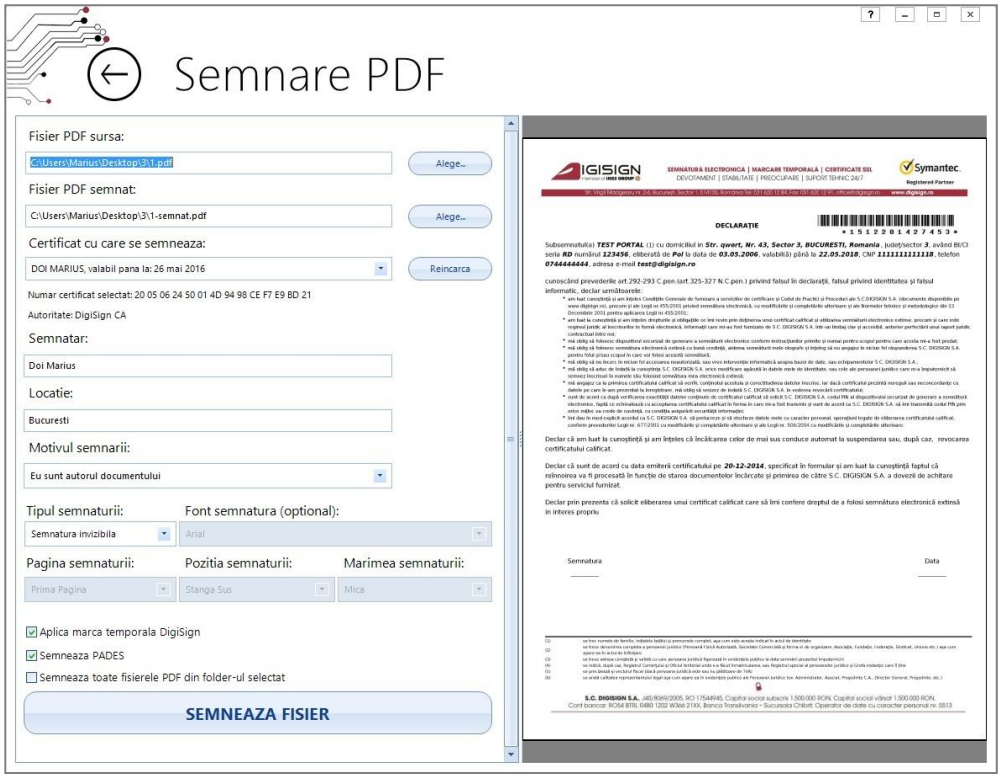




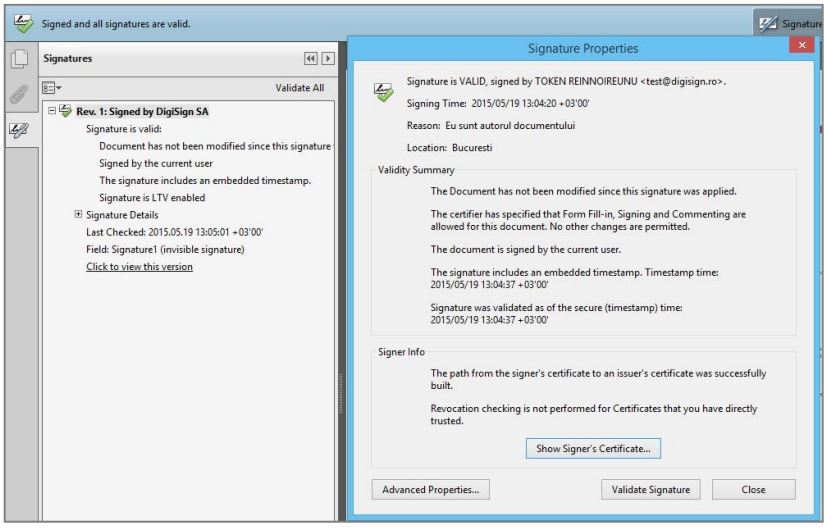
2. Semnarea electronică a unui fișier PDF

- **Fișier sursă*:*** Selectați fișierul pe care doriți să îl semnați;
- **Fișier semnat:** Selectați locul în care doriți să salvați fișierul semnat, precum și denumirea acestuia;
- **Certificat cu care se semnează:** Selectați certificatul digital cu care doriți să semnați;
- **Semnatar:** Aici este afișat numele din certificat si poate fi modificat (modificarea acestui câmp este vizibilă pe document dacă tipul semnăturii este *Semnătură vizibilă*);
- **Locație:** Completați acest câmp dacă doriți să apară locația în structura semnăturii sau pe document dacă tipul semnăturii este *Semnătură vizibilă*;
- **Motivul semnăturii:** Puteți selecta din listă un motiv pentru care doriți să semnați documentul sau puteți scrie unul nou. Acest câmp este vizibil în structura semnăturii sau pe document dacă tipul semnăturii este *Semnătură vizibilă;*
- **Tipul semnăturii:** Selectați tipul semnăturii, respectiv:

  ➢ **Semnătură invizibilă** - Semnătura nu este vizibilă pe document, dar apare în cadrul structurii documentului PDF;



Structura semnăturii electronice în cadrul documentului PDF va fi afișată în următorul mod:



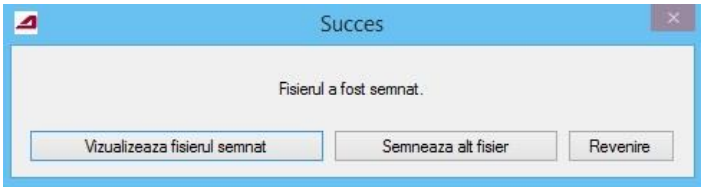
➢ **Semnătură vizibilă** - Semnătura va fi vizibilă pe document și poate fi configurată prin următoarele opțiuni:

- ✓ Font semnătură (opțional) – selectați font-ul dorit pentru semnatură;
- ✓ Pagina semnăturii – selectați pagina unde doriți să apară semnătura *Prima pagină, Ultima pagină* sau ***Toate paginile (necesită licențierea certificatului, pentru achiziționarea licenței ne puteți contacta la adresa sales@digisign.ro și la numărul de telefon 031.620.12.88)***
- ✓ Poziția semnăturii – *Stânga sus, Dreapta sus, Stânga jos* sau *Dreapta jos*;
- ✓ Mărimea semnăturii – *Mică, Medie* sau *Mare*.

Spre deosebire de opțiunea *Semnătură invizibilă,* opțiunea *Semnătura vizibilă* vă oferă posibilitatea de a muta semnătura oriunde pe document cu un simplu click pe chenar și poziționarea acestuia în locul dorit.

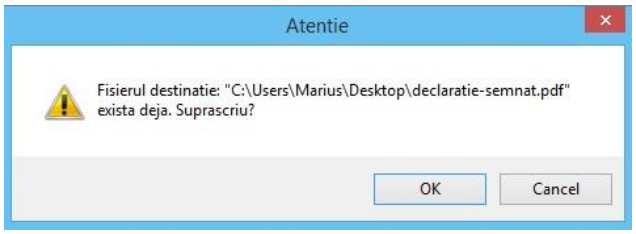
- **Aplică marcă temporală:** Bifați această opțiune dacă doriți să includeți pe lângă semnătura electronică, și o marcă temporală care să ateste data și ora la care s-a semnat fișierul;
- **Semnează PADES:** Bifați această opțiune dacă doriți ca standardul semnăturii să include PADES;
  Semnăturilor electronice extinse/avansate, create utilizând standardul PAdES, le este recunoscută valabilitatea și după ce perioada de valabilitate a certificatului a expirat.
- **Semnează fișier**: Apăsați acest buton în momentul în care doriți să semnați fișierul ales.

După selectarea butonului *Semnează fișier* apare mesajul *Fisierul a fost semnat* și puteți selecta una din opțiunile: *Vizualizează fișier semnat, Semnează alt fișier* și *Revenire.*

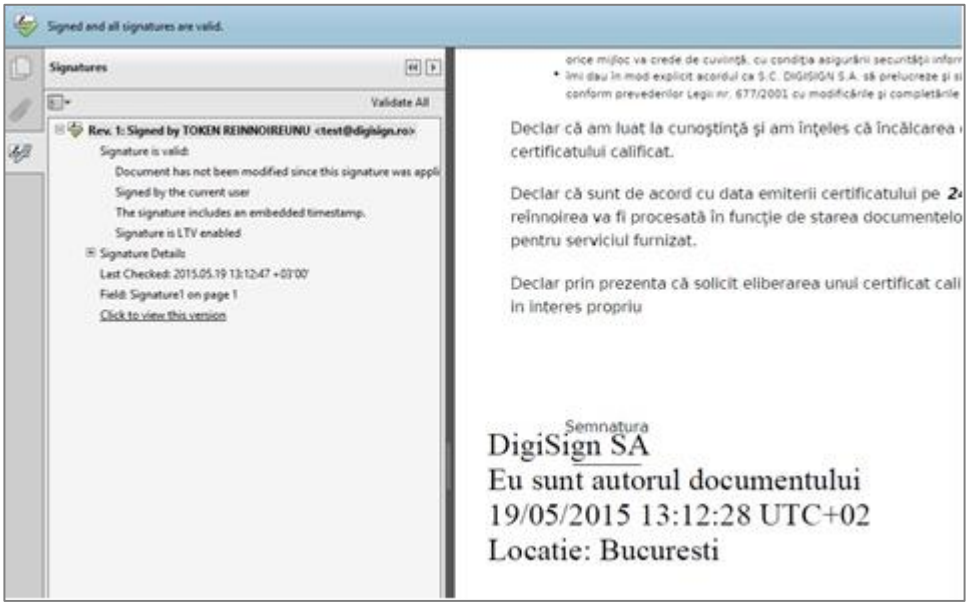


- **Vizualizează fișierul semnat –** selectând acest buton se deschide documentul PDF semnat;
- **Semnează alt fișier –** selectând acest buton puteți semna un alt document păstrând opțiunile anterioare;
- **Revenire –** selectând acest buton va reseta opțiunile anterioare.

Dacă fișierul care urmează a fi semnat există deja în directorul respectiv, programul va afișa o atenționare în acest sens în care veți fi întreabat dacă doriți suprascrierea lui.

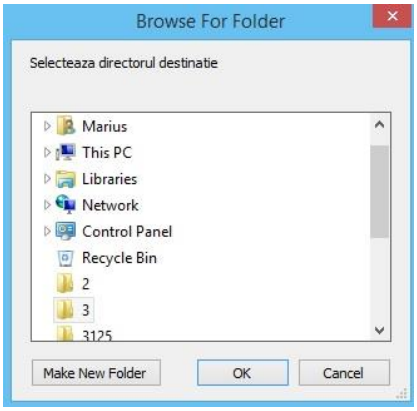


Structura semnăturii electronice în cadrul documentului PDF va fi afișată în următorul mod:

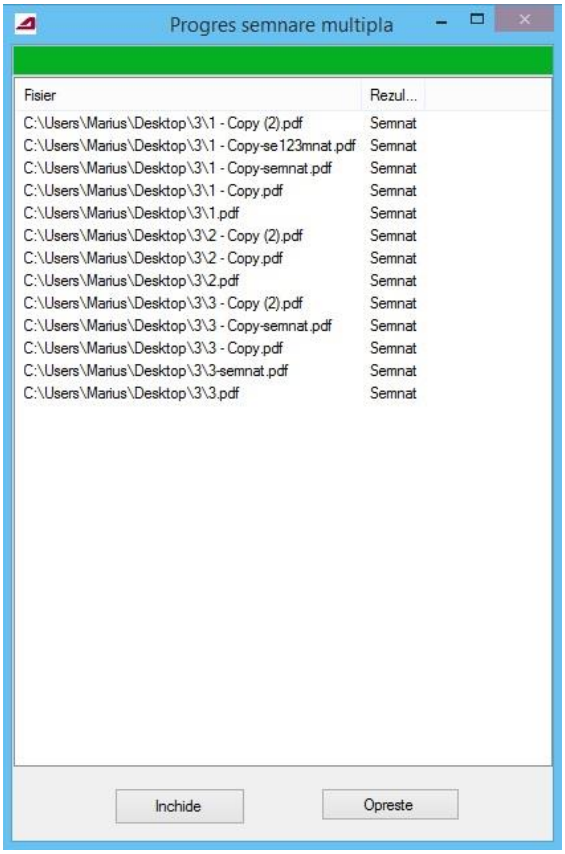


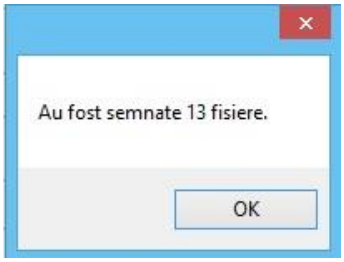
- **Semnează toate fișierele din folder-ul selectat:** Această opțiune necesită licențierea certificatului;

Dacă ați achiziționat deja o licența pentru semnarea unui folder PDF , la selectarea opțiunii *Semnează toate fișierele din folder-ul selectat* veți putea să selectați folder-ul destinație, acolo unde se vor salva fișierele semnate.



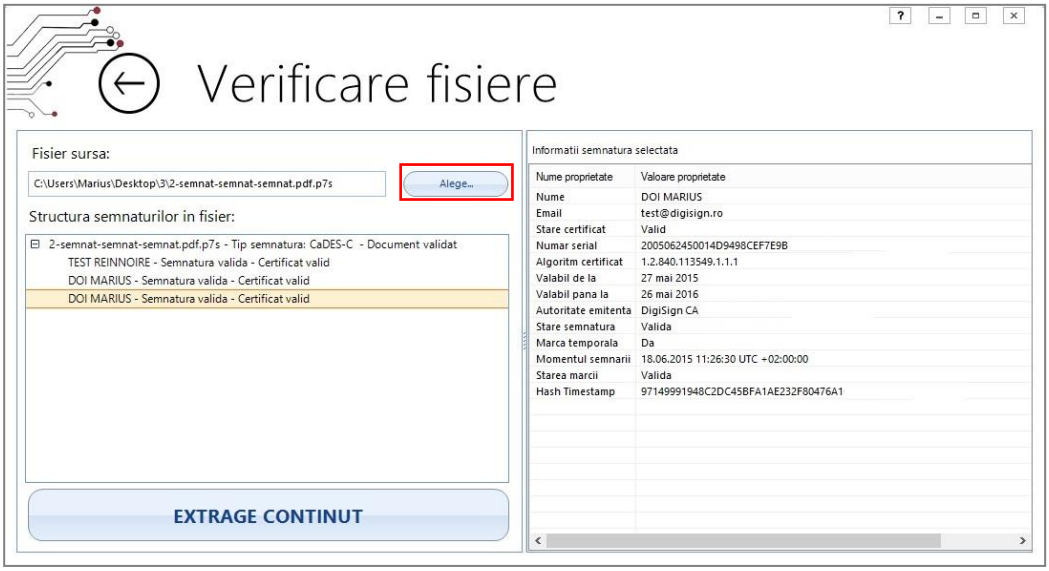
După selectarea folderului destinație, apăsați butonul *Semnează fisier* pentru a începe procesul de semnare. La finalul acestui proces veți primi mesajul *Au fost semnate 13 fișiere.*



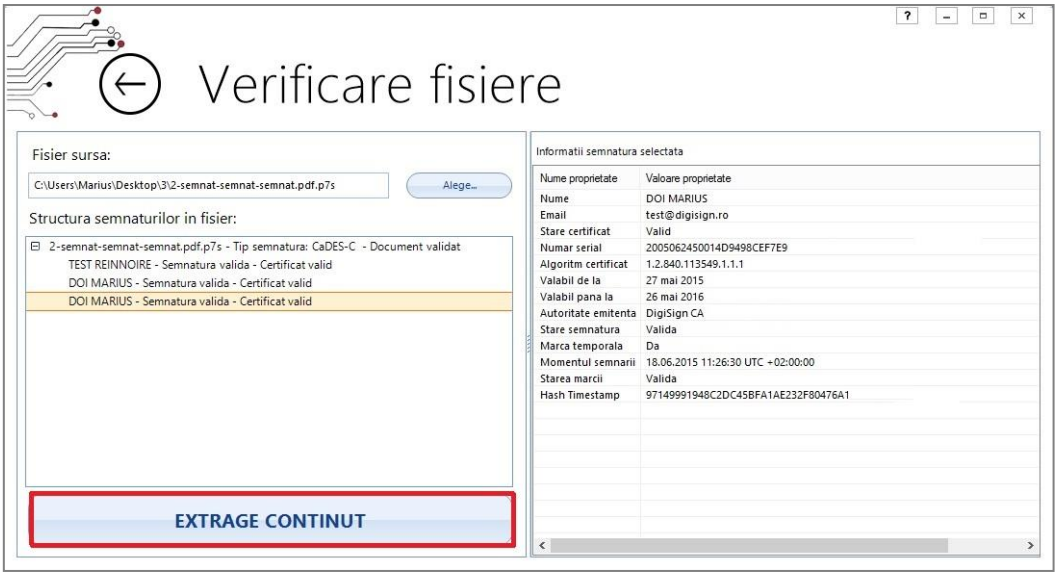


3. Verificarea unui fișier semnat electronic

Pentru a verifica un fișier semnat electronic (fișier cu extensia p7s, respectiv p7m) trebuie să accesați funcționalitatea *Verificare fișiere* din meniul și să selectați opțiunea *Alege...*

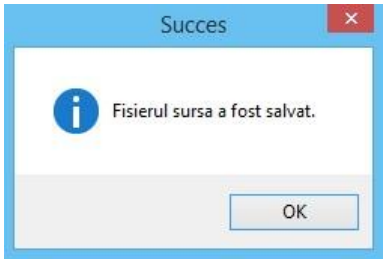


După selectarea fișierului semnat, în partea stângă vor fi afișate semnăturile aplicate documentului, iar în partea dreaptă sunt afișate detaliile semnăturii electronice selectată.

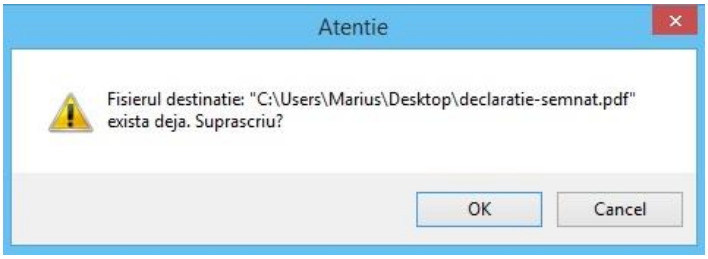


Pentru a extrage fișierul original va trebui să apăsați butonul *Extrage conținut* și să selectați locația unde doriți salvarea fișierului.

După selectarea butonului *Extrage conținut* va fi afișat mesajul *Fisierul sursă a fost salvat.*

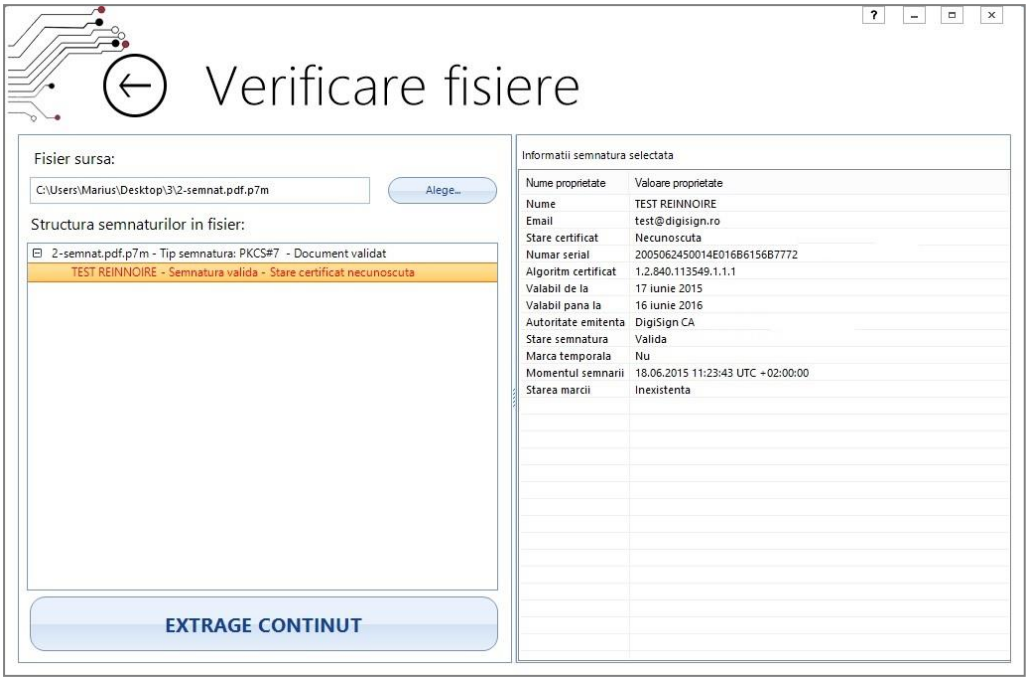


Dacă fișierul care urmează a fi extras există deja în directorul respectiv, programul va afișa o atenționare în acest sens prin care vă întreabă dacă doriți suprascrierea lui.

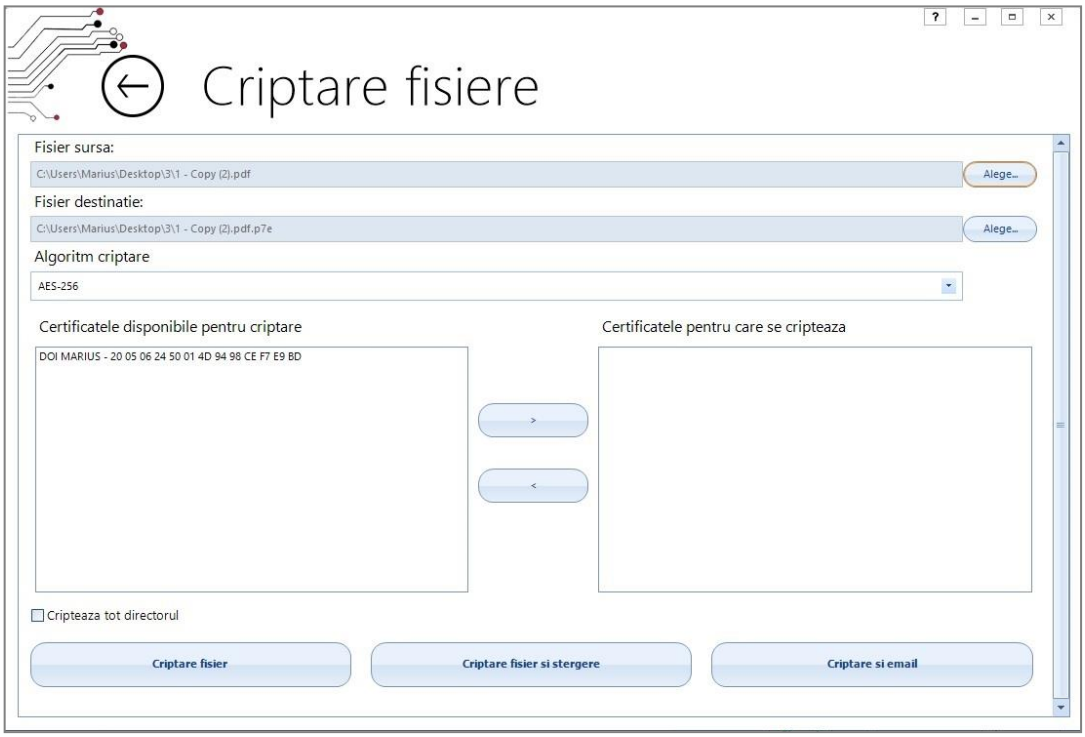


Note:

- Mesajul ***Stare certificat necunoscută*** apare atunci când nu aveți instalat lanțul de încredere al autorității de certificare, care a emis certificatul semnatar, pe calculator.
- Mesajul ***Certificat invalid*** apare în situația în care certificatul digital semnatar este expirat, revocat sau suspendat.

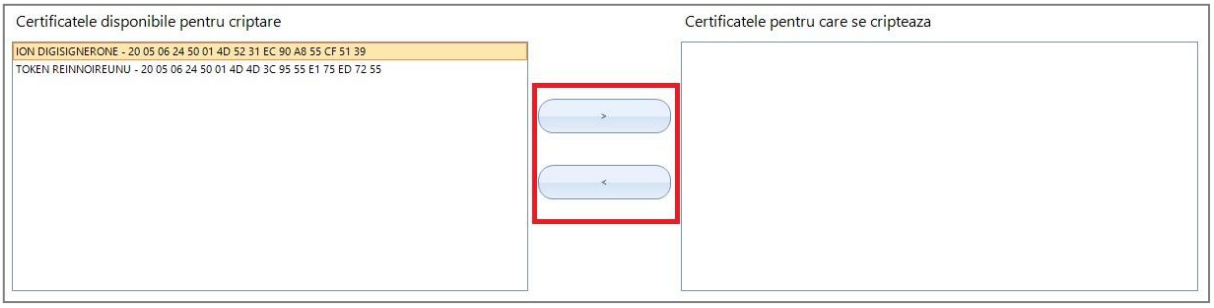


4. Criptarea unui fișier



- **Fișier sursă*:*** Selectați fișierul pe care doriți să îl criptați;
- **Fișier semnat:** Selectați locul în care doriți să salvați fișierul criptat, precum și denumirea acestuia;
- **Algoritm criptare:** Selectați algoritmul de criptare;

- **Certificatele disponibile pentru criptare:** Aici sunt afișate certificatele din *Personale store*;
- **Certificatele pentru care se criptează:** Se selectează certificatul sau certificatele dorite din *Certificatele disponibile pentru criptare* și se apasă pe săgeată;

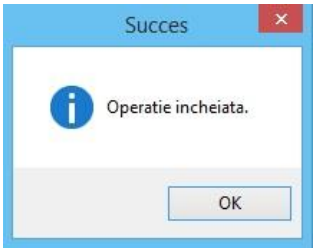


- **Criptează tot directorul:** Această opțiune vă permite criptarea tuturor fișierelor dintr-un folder și necesită licențierea certificatului.

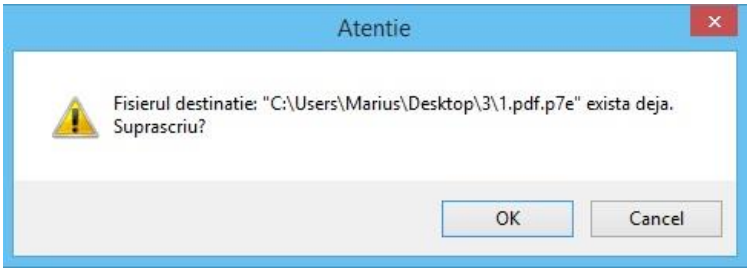
Pentru achiziționarea licenței ne puteți contacta la adresa sales@digisign.ro și la numărul de telefon 031.620.12.88.

- **Criptare fișier:** După ce ați selectat documentul, algoritmul și certificatul apăsați acest buton pentru a cripta fișierul;
- **Criptare fișier și ștergere:** După ce ați selectat documentul, algoritmul și certificatul apăsați butonul pentru a cripta fișierul, iar fișierul original va fi șters;
- **Criptare și email**: După ce ați selectat documentul, algoritmul și certificatul apăsați butonul pentru a cripta fișierul și a-l atașa unui email.

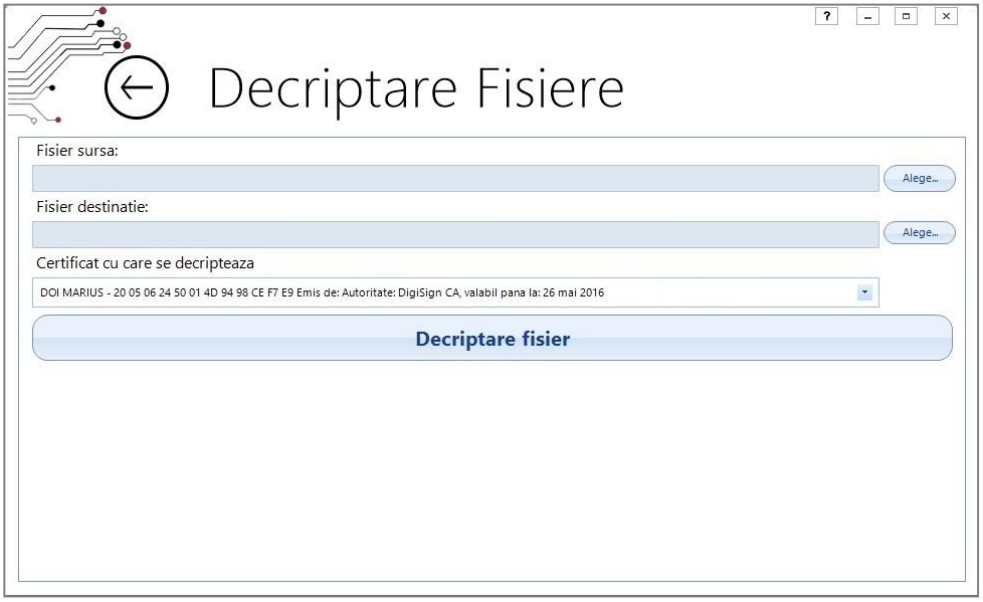
După selectarea butoanelor *Criptare fișier, Criptare fișier și ștergere* și *Criptare și email* apare mesajul *Operație încheiată.*



Dacă fișierul care urmează a fi criptat există deja în directorul respectiv, programul va afișa o atenționare în acest sens în care vă întreabă dacă doriți suprascrierea lui.

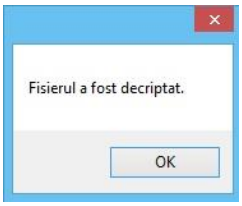


5. Decriptarea unui fișier

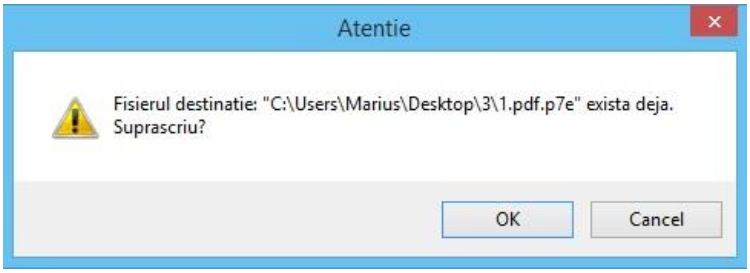


- **Fișier sursă:** Selectați fișierul pe care doriți să îl decriptați;
- **Fișier semnat:** Selectați locul în care doriți să salvați fișierul decriptat, precum și denumirea acestuia;
- **Certificat cu care se decriptează:** Selectați certificatul pentru care a fost criptat fișierul;
- **Decriptare fișier:** Selectați *Decriptare fișier* pentru a fi decriptat fișierul.

  După selectarea butoanelor *Decriptare fișier* apare mesajul *Fișierul a fost decriptat.*



Dacă fișierul care urmează a fi decriptat există deja în directorul respectiv, programul va afișa o atenționare în acest sens în care vă întreabă dacă doriți suprascrierea lui.



6. Setări

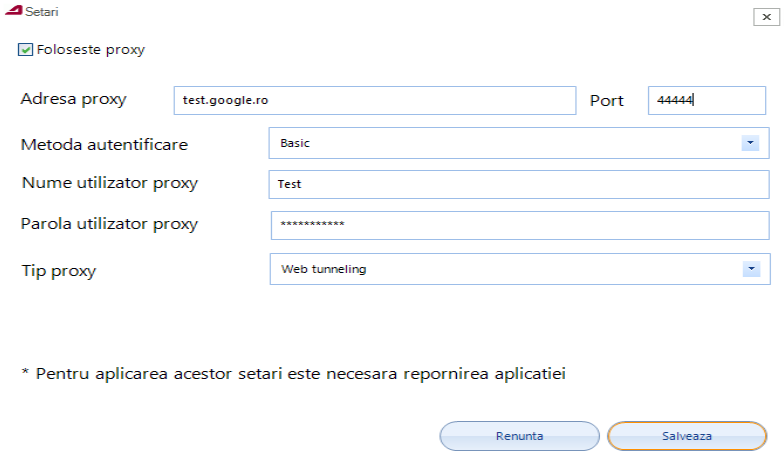
a) Proxy

Setările de proxy pot fi configurate accesând butonul de setări al aplicației.

Setările de proxy oferă 3 modalități de autentificare și anume:

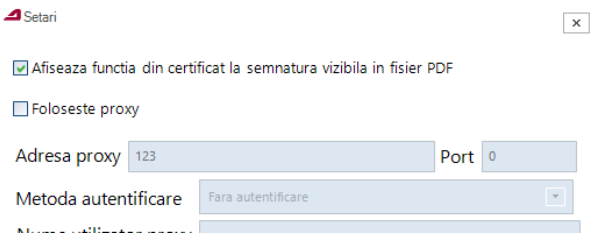
- Fără autentificare
- Basic - prin nume utilizator și parolă
- Digest - prin nume utilizator și parolă

De asemenea, există opțiunea de selectare a tipului de proxy din Web Tunneling sau SOCKS.



b) Afișare funcție la semnare PDF

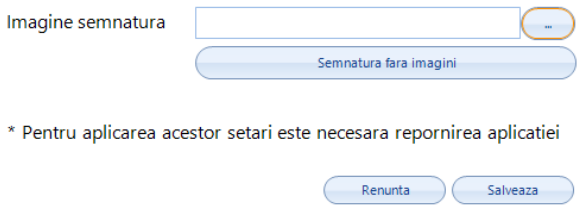
Pentru a afișa funcția din certificat in documentele PDF semnate cu semnătura vizibilă, trebuie selectat din **Setări** - *Afișează funcția din certificat la semnătura vizibilă în fișier PDF*.



c) Imagine în semnătura PDF

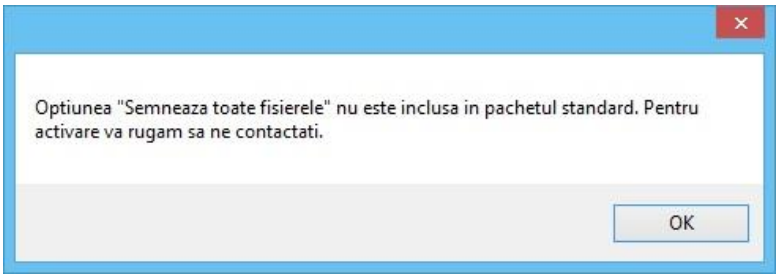
La semnarea documentelor PDF cu semnătura vizibilă există posibilitatea de a afișa o imagine pe langă datele din semnătură.

Acest lucru se poate faci prin selectarea unei poze din meniul de **Setări**.



V. Erori și atenționări

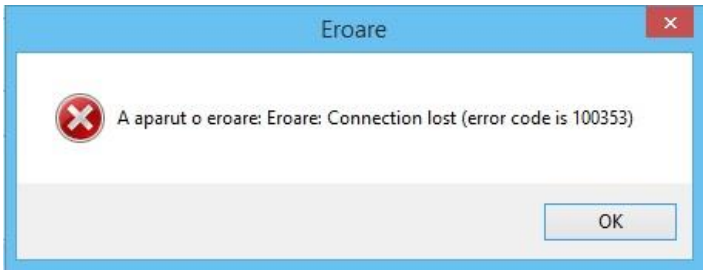
a) Opțiunea „Semnează toate fișierele”



Soluție:

- ✓ Trebuie sa achiziționați o licența pentru certificatul dumneavoastră.
- ✓ Dacă aveți deja o licența și totuși primiți acest mesaj, trebuie sa intrați în C:\Users\NumeUser\AppData\Roaming\Digisigner și să ștergeți toate fișierele.

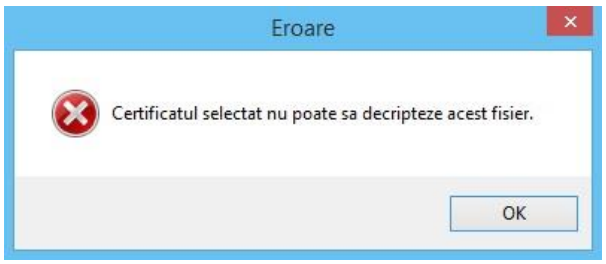
b) A apărut o eroare: Error code is 100353



Soluție:

- ✓ Verificați dacă data, ora și time zone-ul de la calculator dvs sunt corecte.

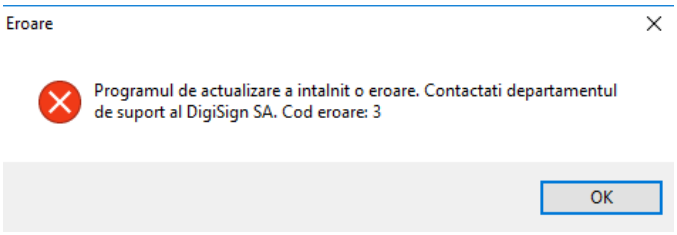
c) Eroare decriptare fișier



Soluție:

- ✓ Certificatul selectat pentru decriptarea fișierului nu corespunde cu certificatul pentru care s-a criptat.

d) Programul de actualizare a intalnit o eroare.

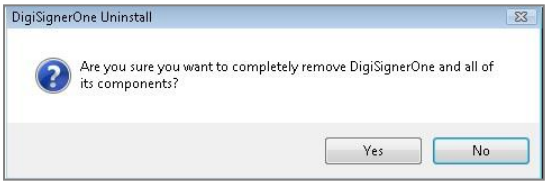


Soluție:

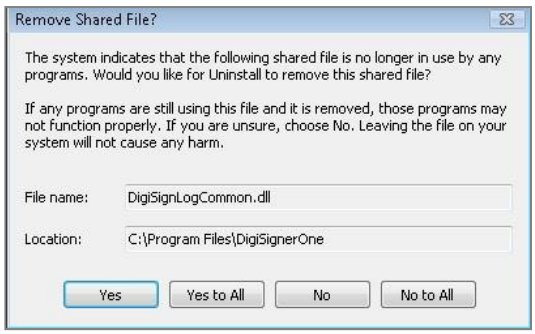
- ✓ Aplicația nu a putut descărca actualizările. Verificați dacă aveți conexiunea la internet.

VI. Dezinstalarea aplicației

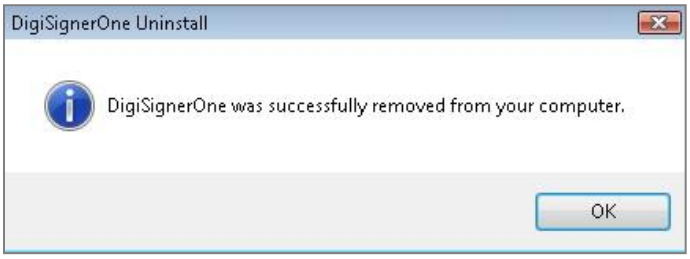
Dacă doriți să dezinstalați aplicația DigiSigner One, va trebui să intrați în meniul *Control Panel – Programs and Features,* să selectați aplicația *DigiSignerOne*, să apăsați butoanele *Uninstall* și pe urmă să selectați opțiunea *Yes*



Selectați opțiunea *Yes to All*



La sfârșitul procesului de dezinstalare, apăsați butonul *OK*.



VII. Actualizări

Nr. Crt.	Versiune	Data
1	1.0	09.07.2015
2	1.1	22.02.2016
3	1.2	13.10.2016
4	1.3	15.05.2018
5	1.4	15.10.2024
6	1.4.1	22.12.2024