

Instructiuni pentru instalarea si utilizarea aplicatiei DigiSigner

Versiunea documentului: 1.4

Instructiuni pentru instalarea si utilizarea aplicatiei DigiSigner	1
1. Descriere Generala	2
2. Instalarea aplicatiei.....	2
3. Utilizarea produsului DigiSigner.....	4
4. Semnarea electronica a unui fisier	5
5. Verificarea unui fisier semnat	10
a) Deschiderea fisierului semnat.....	10
b) Extragerea fisierului original.....	12
c) Exportarea certificatului semnatar.....	13
d) Verificarea certificatului semnatar	14
e) Adaugare semnatura pentru un fisier semnat	15
6. Criptarea unui fisier.....	16
a) Adaugarea certificatului destinatar.....	17
b) Stergerea certificatului destinatar	18
c) Criptarea unui fisier.....	19
7. Decriptarea unui fisier criptat.....	20
8. Verificarea marcii temporale.....	23
9. Pagina de setari.....	24
10. Dezinstalarea aplicatiei.....	25
11. Actualizari	27



1. Descriere Generala

Aplicatia DigiSigner se instaleaza ca o extensie shell a sistemului de operare.

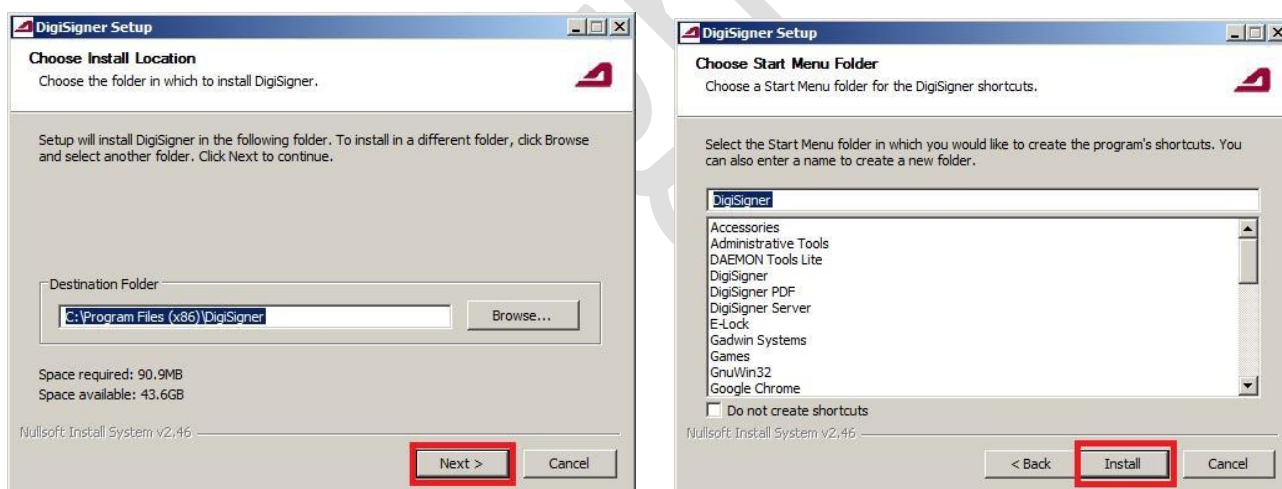
Cerinte de instalare si functionare:

- Windows XP Service Pack 3, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003/R2, Windows Server 2008/R2
- Certificat calificat eliberat de catre autoritatea DigiSign S.A. instalat pe un dispozitiv criptografic in conformitate cu cerintele legislatiei romanesti.
- Dispozitiv eToken introdus in calculatorul dumneavoastra unde este lansata aplicatia.

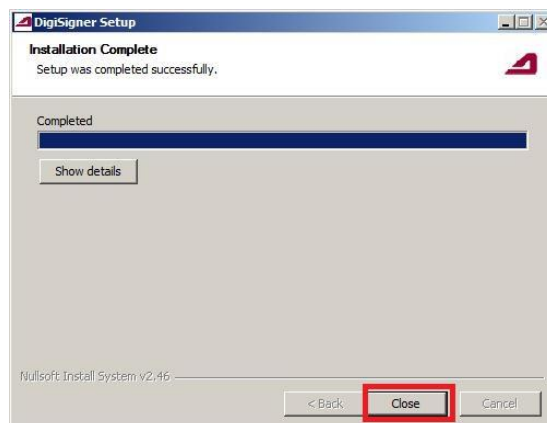
2. Instalarea aplicatiei

Instalarea aplicatiei se face prin deschiderea fișierului *DigiSigner.exe*.

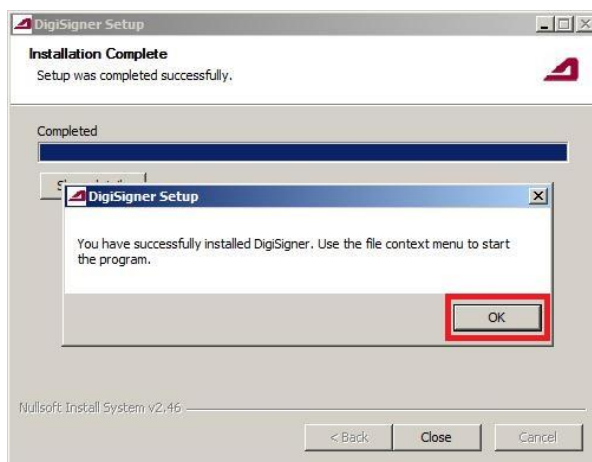
Apasati pe butonul **Next** ⇒ **Install**




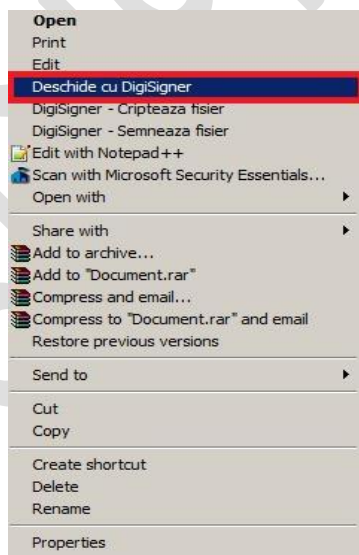
Atunci cand apare mesajul „Completed”, dati click pe butonul **Close**.



Pentru finalizarea procesului de instalare, apăsați pe butonul **OK**.



După instalare, în meniul-context al sistemului de operare apare un nou meniu sub denumirea: **Deschide cu DigiSigner**. Aceasta intrare poate fi verificată prin click dreapta pe orice fișier. Fișierele semnate au asociată o pictogramă de forma  și pot avea extensia p7s, p7m respectiv p7e.



3. Utilizarea produsului DigiSigner

Pentru afisarea panoului de utilizator al aplicatiei *DigiSigner* selectati un fisier oarecare, dati click dreapta si alegeti optiunea *Deschide cu DigiSigner*:



In cazul selectarii unui fisier semnat anterior (fisier cu extensie p7m sau p7s) , optiunea de deschidere este cea prezentata mai sus.

Aplicatia DigiSigner poate aplica o semnatura electronica de tip co-semnatura si contra-semnatura fisierului selectat, sa verifice un fisier semnat digital, sa cripeze un fisier si sa decripteze un fisier criptat.



4. Semnarea electronică a unui fișier

Se lansează aplicația folosind meniul context al sistemului de operare prezentat la pasul anterior.



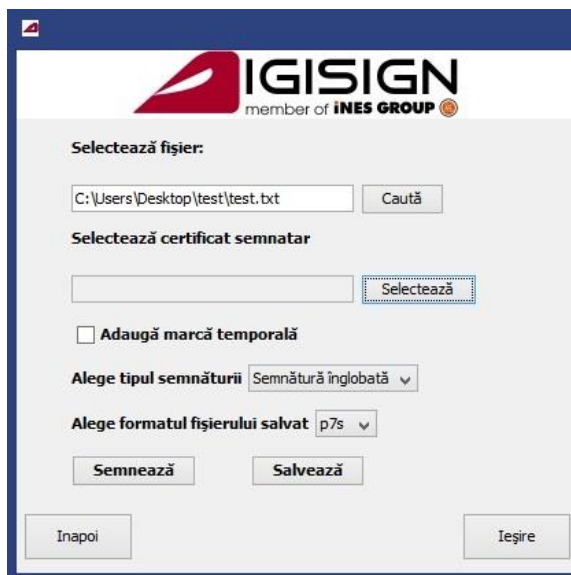
Alegeti butonul **Semnează un fișier**. Se va deschide fereastra de semnare în care aveți posibilitatea să alegeți un fișier care va fi semnat, certificatul folosit pentru semnarea fișierului. De asemenea aveți posibilitatea de a alege opțiunea de marcarea temporală și să definiți formatul fișierului semnat.

ATENȚIE:

- Funcția de marcarea temporală este o funcționalitate opțională și reprezintă un serviciu furnizat de autoritatea DigiSign.
- Aveți opțiunea de a utiliza aplicația **DigiSigner** pentru a obține un fișier cu semnatura **inglobată** (de tip **.p7s** sau **.p7m**) sau un fișier cu semnatura **detasată** (de tip **.p7s**). Dacă doriți obținerea unui fișier care să conțină atât documentul semnat cât și detalii despre certificatul digital semnat, selectați opțiunea **semnatura inglobată**.
- În cazul în care opțiunea dvs este pentru o semnatura cu formatul p7s va atragem atenția să nu modificați sau salvați fișierul original ulterior semnării, deoarece acesta poate duce la invalidarea semnăturii. Prezentarea semnăturii sub formatul p7s unei părți terțe presupune prezentarea fișierului semnat alături de fișierul p7s obținut.



Pentru a aplica o semnatura unui fisier alegeti **certificatul semnatar**, **tipul semnaturii** si **formatul fisierului dorit** si apasati butonul **Semneaza**. Pentru a aplica o semnatura cu marca temporală inclusa bifati optiunea **Adauga Marca Temporală**.



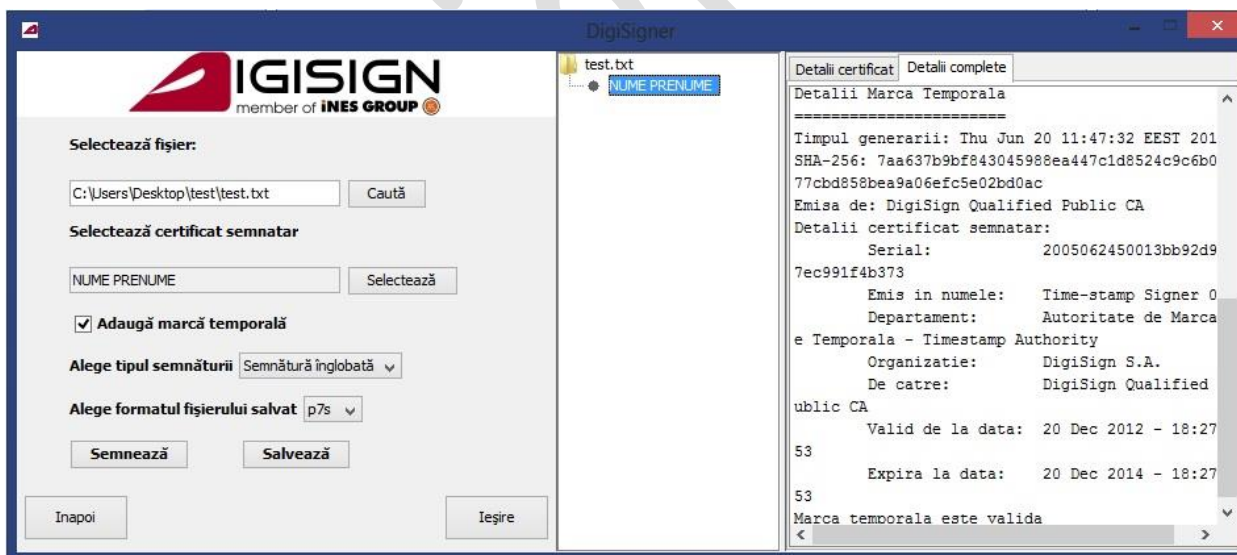
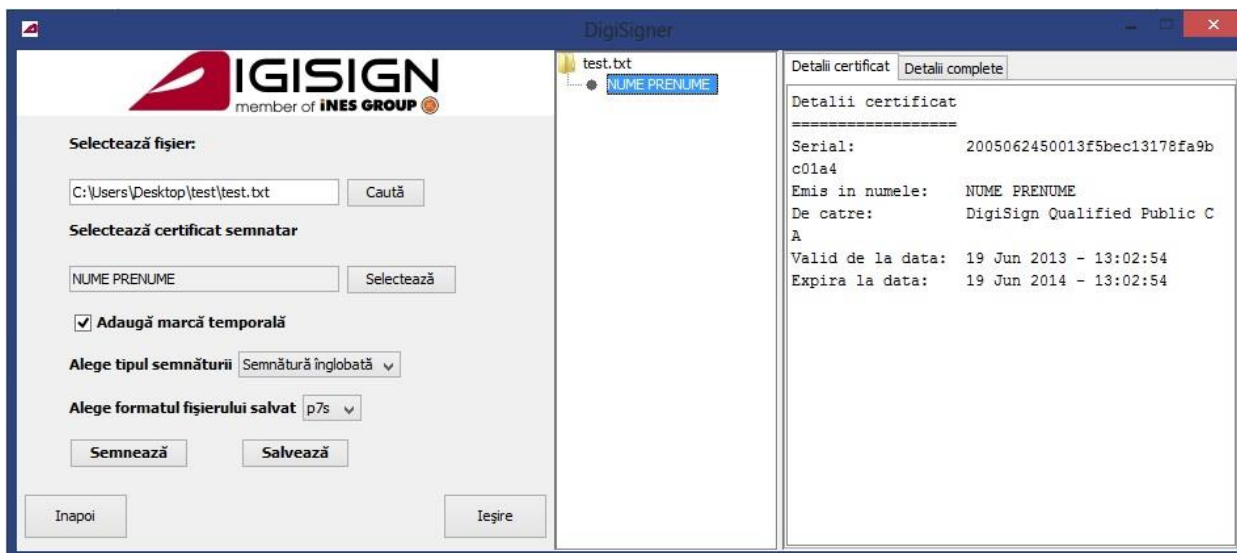
În momentul selectării certificatului apare fereastra de întrebare pentru PIN-ul dispozitivului criptografic. Introduceți parola dispozitivului e-Token și apăsați butonul **OK**.



ATENȚIE!: Folosirea aplicației DigiSigner necesită instalarea în prealabil a driverului eToken și al lanțului de încredere al autorității DigiSign S.A. (vezi manual de instalare certificat digital la adresa <http://www.digisign.ro/uploads/MCIP.pdf>) altfel se întoarce un mesaj care indică faptul că certificatul nu poate fi validat și trebuie verificat/instalat lanțul autorității.



Rezultatul întors după aplicarea cu succes a semnăturii arată ca în imaginile de mai jos, conținând detalii despre certificatul care a fost folosit pentru semnatura. De asemenea vor fi afișate detalii despre semnatura și despre marca temporală, în cazul în care opțiunea a fost utilizată.



Salvarea fișierului semnat se face prin apăsarea butonului **Salveaza**. Rezultatul operațiunii este întocmirea unui fișierului cu extensia specificată la câmpul **Alegeți formatul fișierului salvat** în directorul de unde a fost deschisă aplicația. (ex. test.txt.p7s).



Observatii:

În cazul în care calculatorul dumneavoastră nu este conectat la internet nu aveți posibilitatea obținerii unei marci temporale pentru documentul semnat !

În cazul în care calculatorul dumneavoastră nu este conectat la internet trebuie să prezentați CRL-ul emis de DigiSign pentru ziua respectivă în scopul validării certificatului !

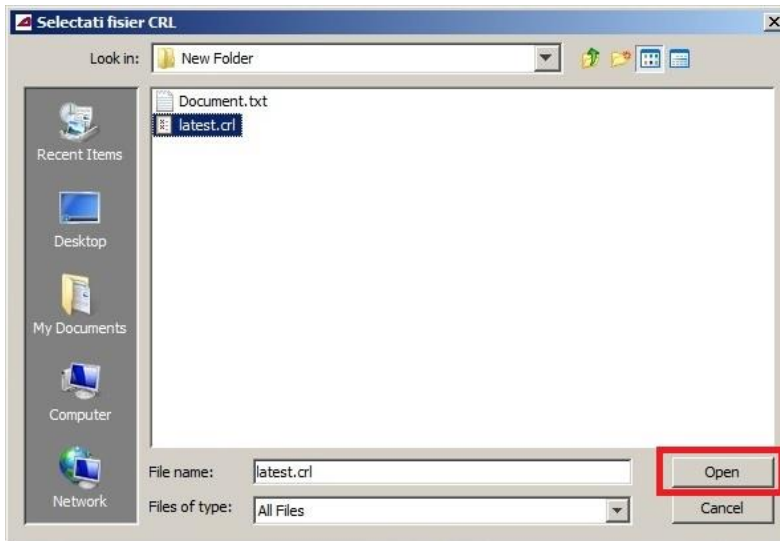
Această operațiune se face în felul următor:

Selectați fișierul *latest.crl*, pe care ați descărcat în prealabil de la adresa:

SHA1: <http://crl.digisign.ro/qualifiedpublicca/latest.crl>

SHA2: <http://crl.digisign.ro/repository/qualifiedpubliccav3.crl>





Alegeti butonul **Open**

In caz de succes numele titularului certificatului va fi afisat in sectiunea *Selecteaza certificat semnatar*.



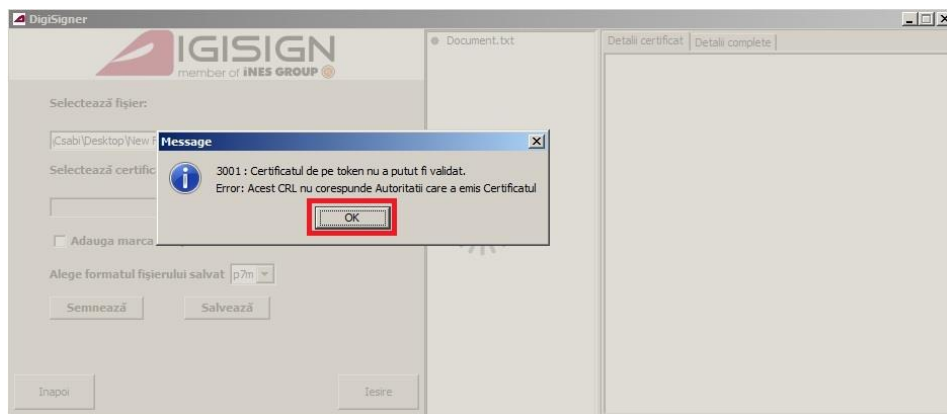
In cazul in care la fereastra de Selectati fisier CRL ati apasat pe **Cancel** urmatorul mesaj va fi afisat pe monitor:



Apasati pe butonul **OK** pentru a inchide aplicatia.



In cazul in care introduceti un CRL invalid sau apartinand unei alte autoritati mesajul de mai jos va fi afisat pe monitor:



Apasati pe butonul **OK** pentru a inchide aplicatia.

5. Verificarea unui fisier semnat

a) Deschiderea fisierului semnat

Pentru a deschide un fisier semnat (extensia p7s, respectiv p7m) lansati aplicatia din meniul context al sistemului de operare prin click dreapta pe fisierul selectat si alegeti optiunea **Deschide cu DigiSigner**.



Apasati pe butonul **Verifica un fisier semnat**.



Pentru a selecta un fisier semnat apasati pe butonul **Cauta**.

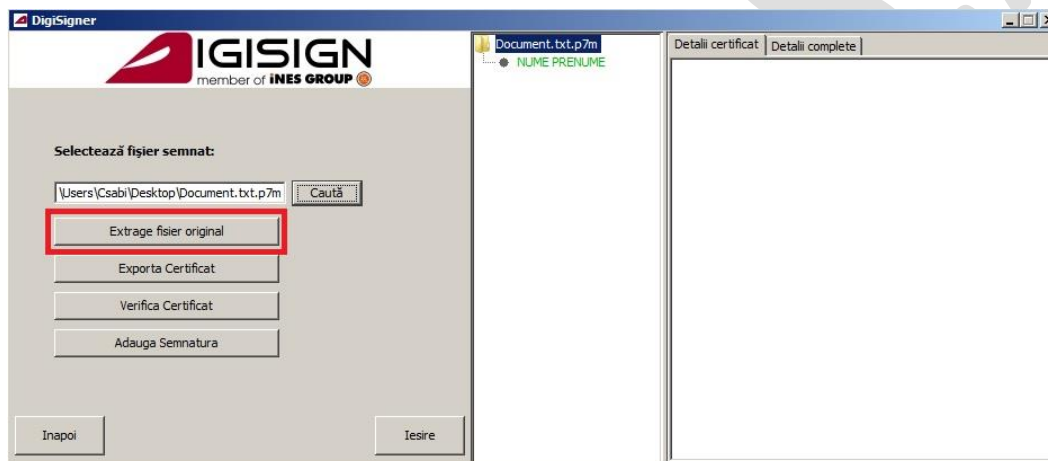


Detalii legat de semnatar, semnatura si marca temporală sunt afisate pe panoul din partea dreapta a aplicatiei DigiSigner.

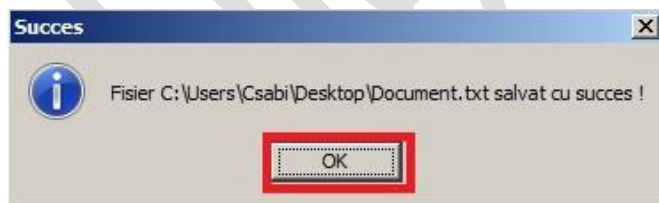


Butoanele *Extrage fișier original*, *Exporta Certificat* și *Verifica Certificat* devin active în acest moment.

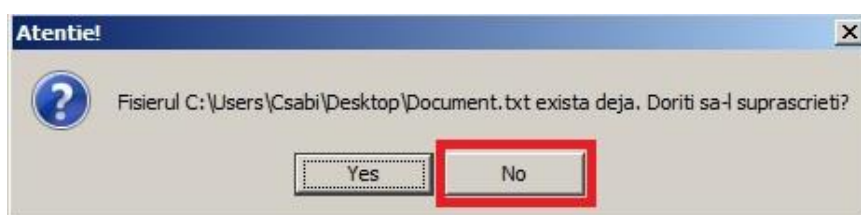
b) Extragerea fișierului original



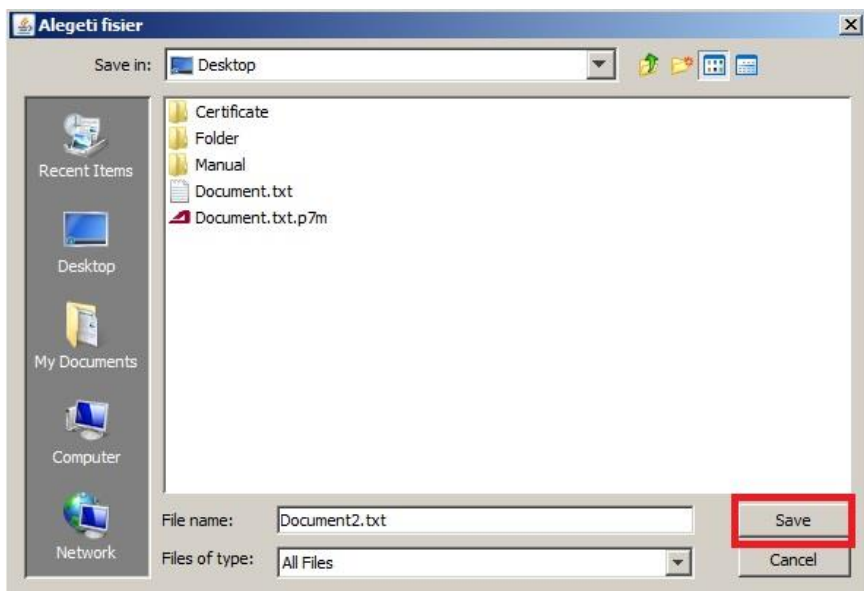
Pentru a deschide fișierul original din interiorul unui fișier semnat, având extensia p7m, trebuie utilizat butonul *Extrage fișier original* din aplicația deschisă.



În cazul în care documentul original nu a fost încă salvat în directorul curent va apărea fereastra de Succes. Apasați pe butonul **OK**.



Daca fisierul a mai fost extras in directorul curent atunci apare fereastra **Atentie!**. Pentru a evita suprascrierea fisierului deja extras, apasati pe butonul **No**.



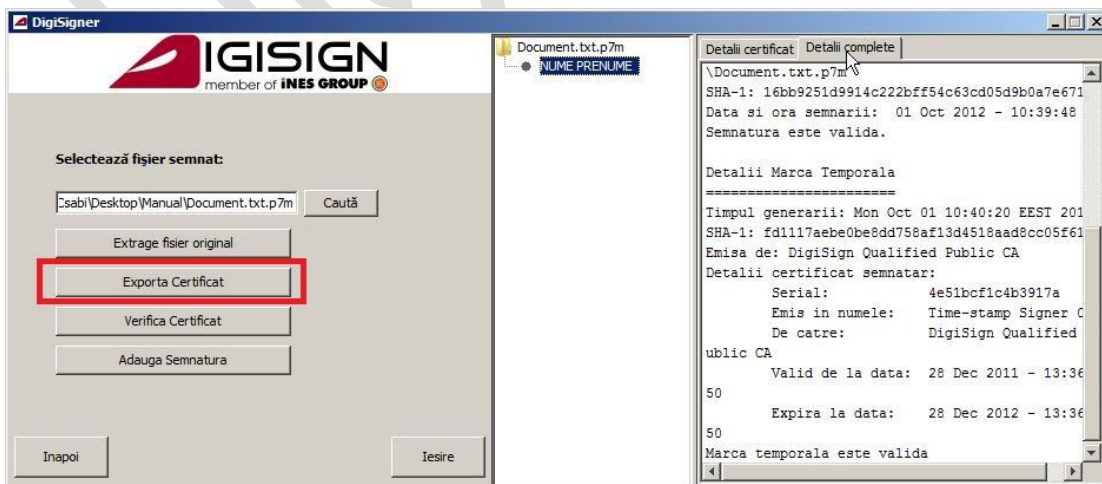
Adaugati o alta denumire fisierului si apasati pe butonul **Save**.



Fisierul va fi semnat cu alta denumire. Apasati pe butonul **OK**.

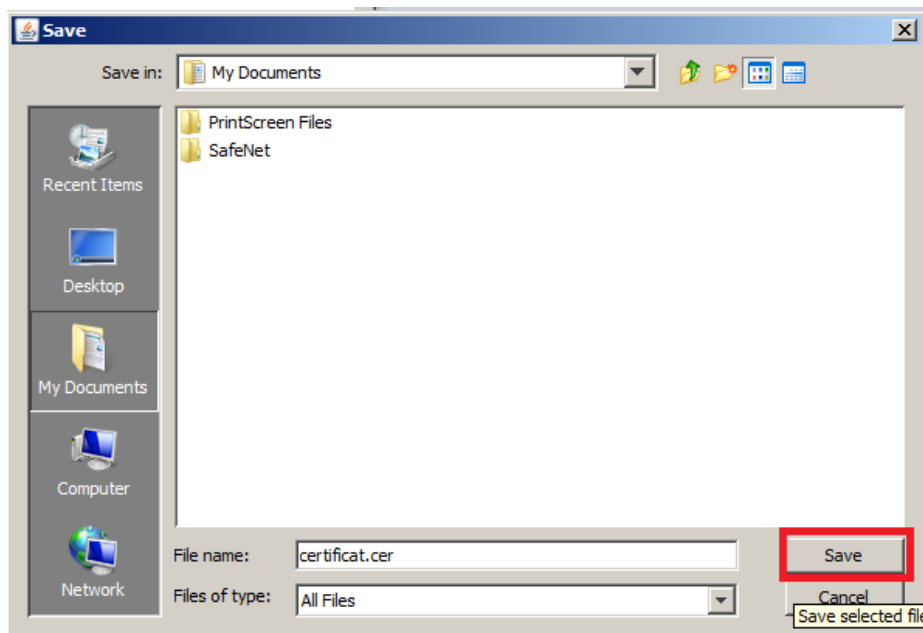
Dupa acest pas fisierul extras poate fi prelucrat si utilizat pentru modificari ulterioare.

c) Exportarea certificatului semnatar

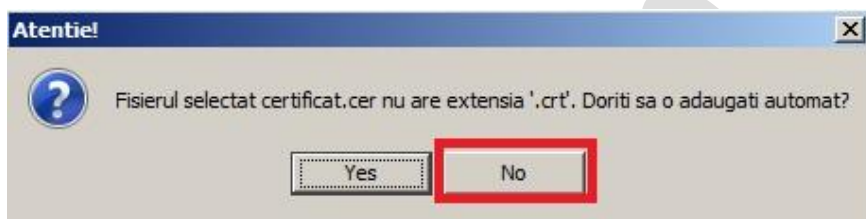


Prin butonul de **Exporta Certificat** puteti extrage certificatul semnatarului din fisierul semnat.





Tastati numele ales pentru certificat, adaugati extensia **.cer** si apasati pe butonul **Save**.



Pentru a nu adauga extensia **.cer**, dati click pe butonul **No**.

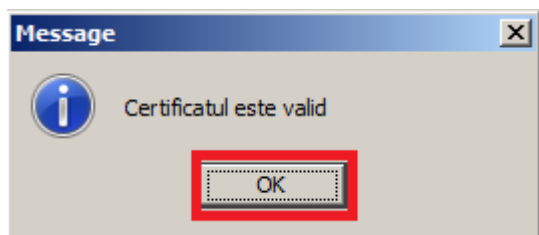
Verificati existenta fisierului salvat in directorul specificat la salvare.

d) Verificarea certificatului semnat

Folosind butonul *Verifica Certificat* se poate verifica validitatea certificatului. Pentru a se putea realiza acest pas trebuie instalat in prealabil lantul de incredere al autoritatii emitente.



Pentru a verifica validitatea certificatului, apăsați pe butonul **Verifica Certificat**.

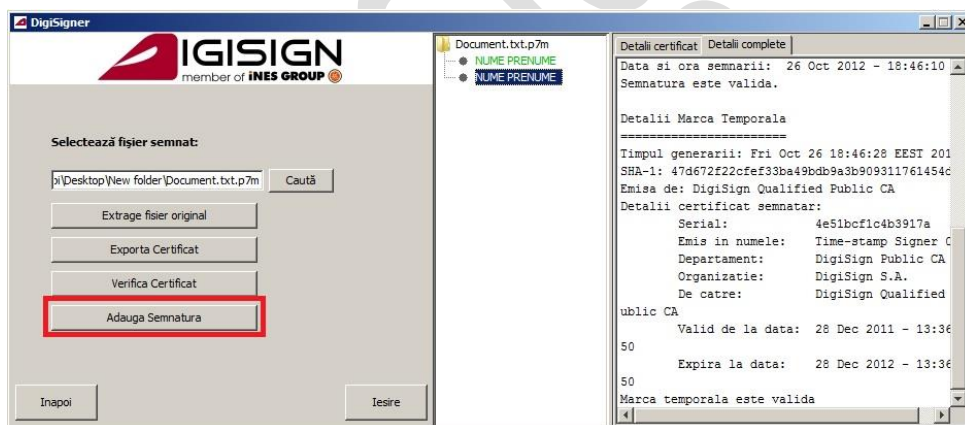


Dacă lanțul a fost instalat corect mesajul întors este *Certificatul este valid* și se apasă pe **OK** pentru a închide fereastra.



Dacă lanțul de încredere al autorității nu a fost instalat mesajul întors este cel din imaginea de mai sus. Apăsați **OK** pentru a închide fereastra.

e) Adăugare semnatura pentru un fișier semnat



Pentru contrasemnarea unui fișier semnat anterior, alegeți butonul **Adauga Semnatura**.

Pentru continuarea procesului de semnare reluați pașii de la *punctul 4* în vederea alegerii certificatului semnatar și semnarea propriu-zisă a fișierului.

6. Criptarea unui fisier

Pentru criptarea unui fisier se lanseaza aplicatia din meniul context al sistemului de operare dati click dreapta pe fisierul selectat si alegeti optiunea **Deschide cu DigiSigner**.



Pentru continuarea procesului de criptare a unui fisier apasati butonul **Cripteaza un fisier**.



Specificati fisierul care va fi criptat. Apasati pe butonul **Cauta**.

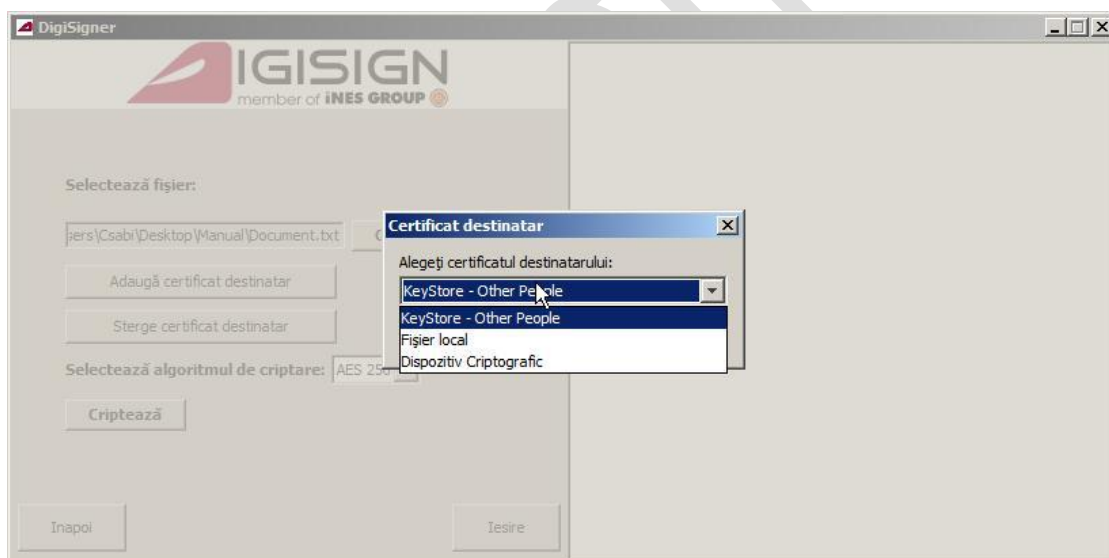


Butoanele *Adauga certificat destinatar* si *Sterge certificat destinatar* devin active atunci cand aveti un fisier selectat.

a) Adaugarea certificatului destinatar



Pentru a adauga destinatar apasati butonul **Adauga certificat destinatar**.



Alegeti certificatul destinatar intr-unul din urmatoarele locatii:

- KeyStore – Other People = certificat care este stocat in sectiunea de Other People din store-ul de Microsoft
- Fișier local = certificatul salvat anterior pe calculatorul dumneavoastra
- Dispozitiv Criptografic = certificat aflat pe dispozitivul dumneavoastra criptografic

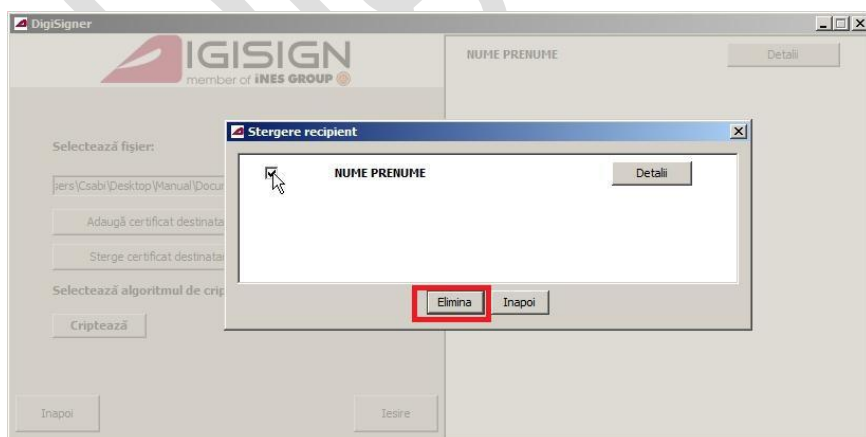


În partea dreapta a aplicației se listează certificatele adăugate pentru criptare. Prin butonul detalii puteți obține mai multe informații despre certificatul adăugat.

b) Stergerea certificatului destinatar

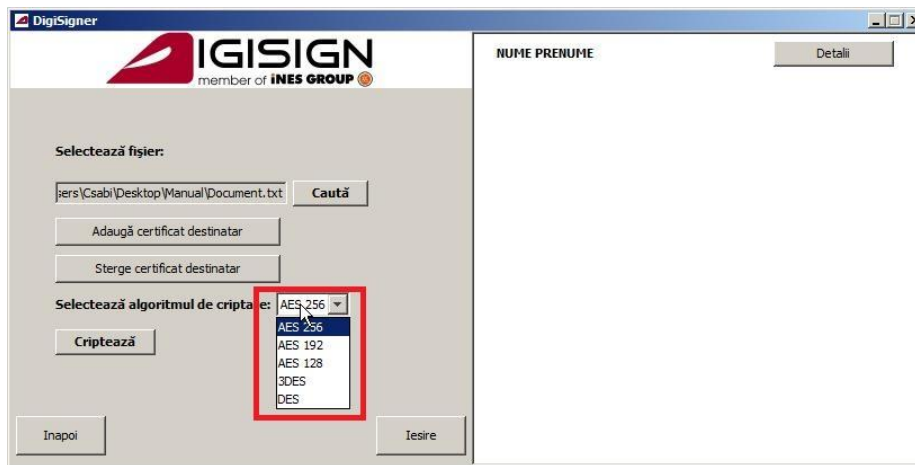


Pentru a șterge destinatar apăsați butonul Adăuga certificat destinatar.



Bifați certificatul care se dorește a fi șters din lista și apăsați pe butonul de **Elimina**.

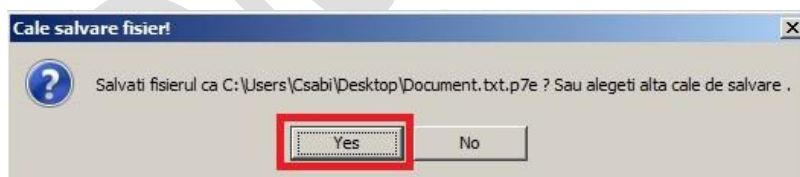
c) Criptarea unui fisier



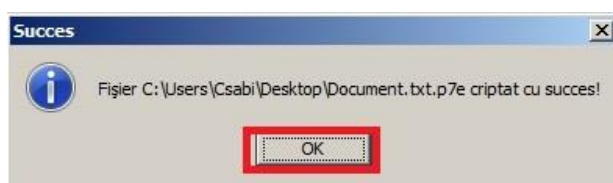
Alegeti algoritmul de criptare la optiunea **Selecteaza algoritmul de criptare**.



Apasati pe butonul **Cripeaza**.



Salvati fisierul in directorul specificat in fereastra prin butonul **Yes** sau adaugati o noua destinatie alegand butonul **No**.



Apasati pe butonul **OK** pentru a inchide fereastra.



7. Decriptarea unui fișier criptat

Pentru a decripta un fișier, se lansează aplicația din meniul context al sistemului de operare aplicând click dreapta pe fișierul selectat.



Pentru a continua procesul de decriptare alegeți opțiunea de **Decriptează un fișier**.



Apasați pe butonul **Caută** pentru a specifica un fișier criptat.

Fișierul selectat trebuie să aibă extensia **.p7e**.

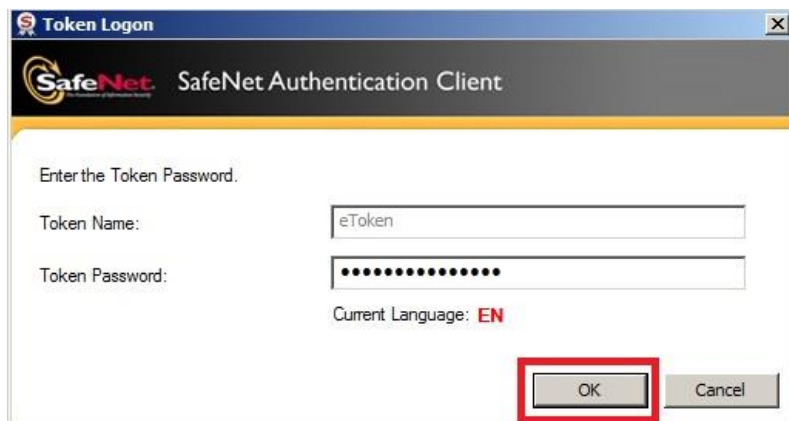




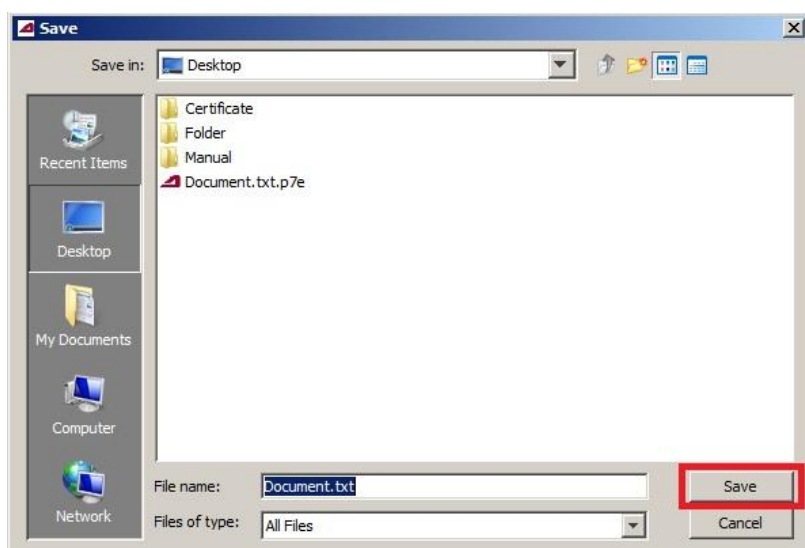
Introduceti dispozitivul criptografic intr-unul din porturile USB ale calculatorului si apasati pe butonul **Selecteaza**.



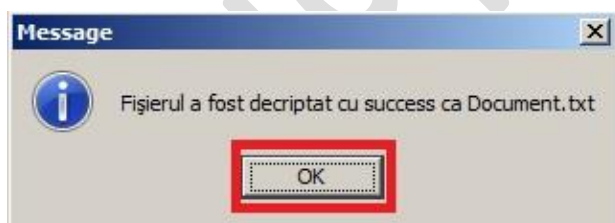
Dupa ce ati selectat un fisier criptat si ati specificat certificatul pentru decriptare, apasati pe butonul **Decripteaza**.



Introduceți pinul dispozitivului criptografic și apăsați pe butonul **OK**.



Specificați un nume de fișier și apăsați butonul de **Save**.



Pentru a termina procesul de decriptare și a închide fereastra, apăsați pe butonul **OK**.

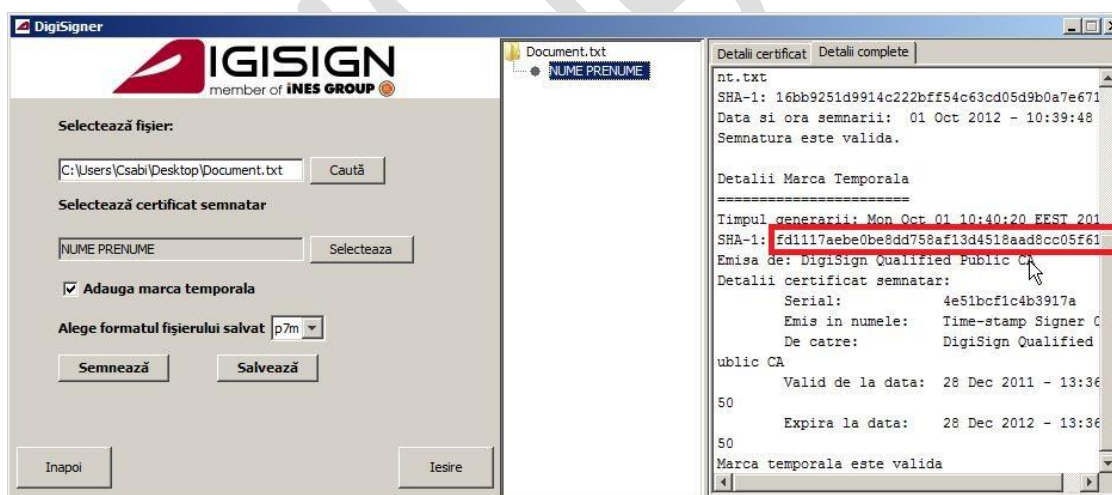
8. Verificarea marcii temporale

DigiSign S.A. pune la dispozitia clientilor un registru electronic operativ de evidenta a marcilor temporale la adresa: https://secure.digisign.ro/register_timestamp.php pentru verificarea, respectiv validarea amprenteii.

Se poate cauta dupa timpul semnarii, respectiv dupa amprenta semnaturii folosind informatiile din aplicatie.



Pentru a cauta dupa timpul semnarii copiati informatia din campul de *Timpul generării*



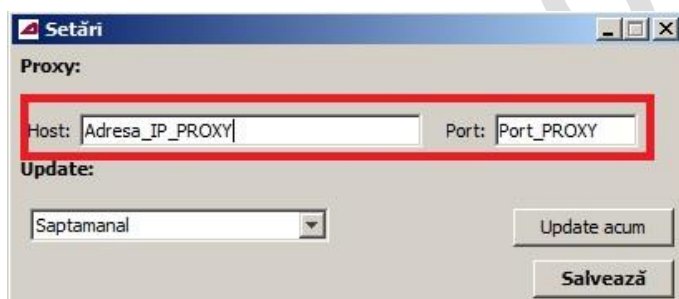
Pentru a cauta dupa amprenta semnaturii trebuie copiati informatia din campul de *SHA-1* la Detalii Marca Temporală

9. Pagina de setari

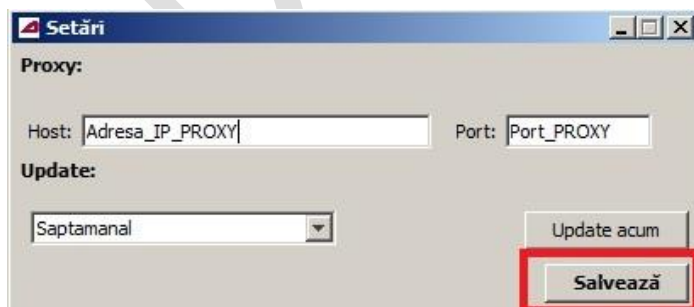
Pentru specificarea adresei IP si a portului de proxy si pentru a defini intervalul de actualizare pentru aplicatia DigiSigner, se lanseaza aplicatia din meniul context al sistemului de operare aplicand click dreapta pe orice fisier selectat si se alege optiunea de **Deschide cu DigiSigner**.



Pentru a intra in fereastra de setari apasati pe butonul **Setari** aflata in partea de stanga jos a ferestrei.



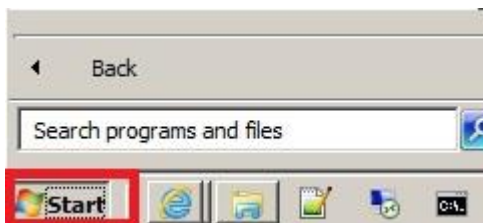
Se specifica adresa IP si portul serverului proxy. (In cazul in care nu cunoasteti aceste informatii, luati legatura cu administratorul dumneavoastra de retea)



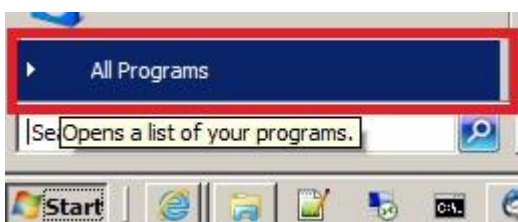
Apasati pe butonul **Salveaza** pentru a salva modificarile introduse.

10. Dezinstalarea aplicatiei

Aplicatia se dezinstaleaza folosind butonul de **Uninstall** din Start Menu sau folosind Control Panel.



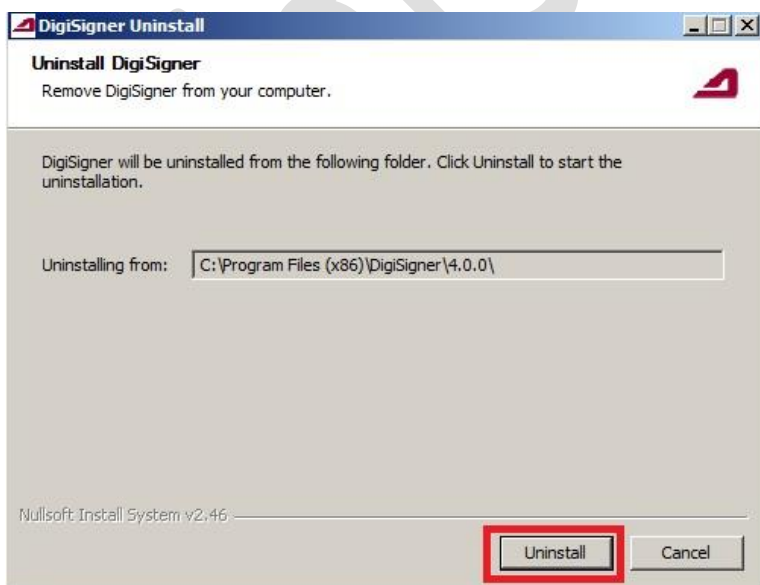
Apasati pe butonul **Start**.



Selectati optiunea **All Programs**.

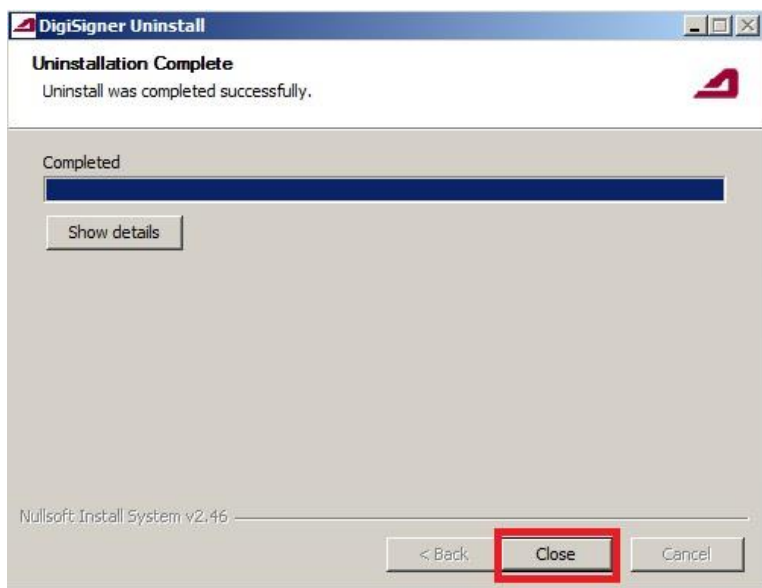


Dati click stanga pe intrarea **Uninstall**.



Pentru continuarea procesului de dezinstalare apasati pe butonul **Uninstall**.





Apasati pe butonul **Close**.



Pentru a finaliza procesul de dezinștalare și a închide fereaștra, apasati pe butonul **OK**.

11. Actualizari

Nr. Crt.	Versiune	Data
1	1.0	25.10.2011
2	1.1	31.10.2012
3	1.2	15.10.2012
4	1.3	20.06.2013
5	1.4	16.10.2014