Digisigner One user manual

version 1.3

I. Digisigner ONE application description 2
II. Installing the Digisign qualified digital certificate and the Digisigner One application 3
III. Installing the eToken usb device and the Digisign trust chain 4
IV. How to use Digisigner One application 9
1. Signing files in p7m and p7s format 10
2. Digitally signing a PDF file 13
3. Verifying a digitally signed document 18
4. Encrypting a file 20
5. Decrypting a file 22
6. Proxy settings 23
V. Errors and Warnings 24
VI. Uninstalling Digisigner One 25
VII. Updates 25

S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

I.Digisigner ONE application description

Digisigner ONE is the only software in Romania that incorporates and manages main operations using qualified digital certificates.

DigiSigner One, used with a Digisign qualified certificate or encryption certificate, brings an undeniable security to documents and files, by integrating digital signatures and timestamping; verifying digitally signed documents, encrypting and decrypting files.

Compatible operating systems:
- ✓ Windows XP Service Pack 3
- ✓ Windows Vista
- ✓ Windows 7
- ✓ Windows 8, 8.1
- ✓ Windows 10

Used Cryptographic standards :
- ✓ PKCS#7
- ✓ CAdES
- ✓ PAdES
- ✓ PKCS#11
- ✓ PKCS#12
- ✓ Microsoft CryptoAPI
- ✓ X.509 v3

Integrated security algorithms:
- ✓ AES
- ✓ DES
- ✓ 3DES
- ✓ SHA-1
- ✓ SHA-256
- ✓ RSA 2048 bit

Offered benefits:
- ✓ The main operations for managing and using a digital certificate issued by Digisign are integrated intoa single software application.
- ✓ The application has a modern and intuitive interface wich is very easy to use.
- ✓ Digisigner ONE allows you to view PDF files before signing it.
- ✓ Users manual is integrated in the Digisigner ONE application.
- ✓ News and promotions offered by Digisign are displayed directly within the application.

Digitally signing files

By using a digital certificate, stored on a secure cryptographic device, compatible with the PKCS#11 standard, or stored in a PKCS#12 archive, the Digisigner ONE allows users to digitally sign any file or document in an easy way. You can sign PDF files and also documents in p7s/p7m format.

Applying timestamp

Digisigner ONE uses the Digisign time stamping authority server, guaranteeing that the document was signed at a certain moment of time.

Verifying the digitally signed files

The Digisigner One users have the opportunity to check the certificate validity by verifying the digital signature associate to the file and displaying the verification results in a user friendly interface.

Encrypting and decrypting files

The Digisigne ONE users have the possibility to encrypt files for one or more beneficiaries in order to protect the confidentiality of the file against any unauthorized access. Only the beneficiaries selected by the user can decrypt the file that was encrypted with the help of the integrated cryptographic algorithms provided by the aplication.

Useful features

All customers are informed regarding news and promotions offered by Digisign, they are displayed directly within the application. Our technical support department is available 24/7 and it is just a click away, you have to access the "Ajutor DigiSign" button integrated in the application and send us a message, our support team will contact you shortly.

II. Installing the Digisign qualified digital certificate and the Digisigner One application

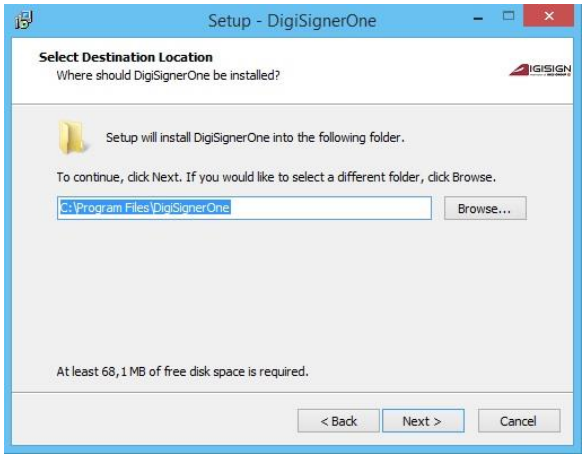
1. Download the install kit from one of the following addresses:

a) DigiSigner ONE – 64 biti

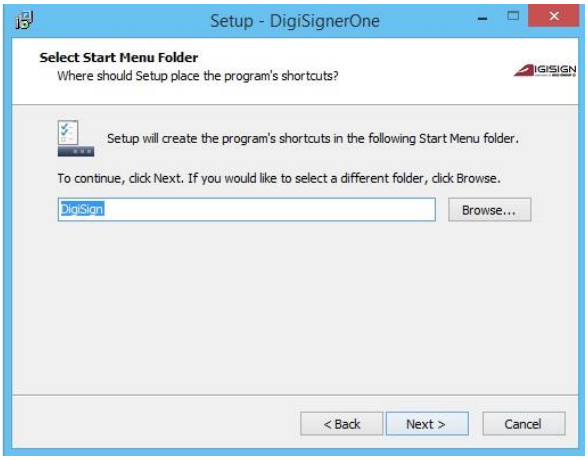
b) DigiSigner ONE – 32 biti

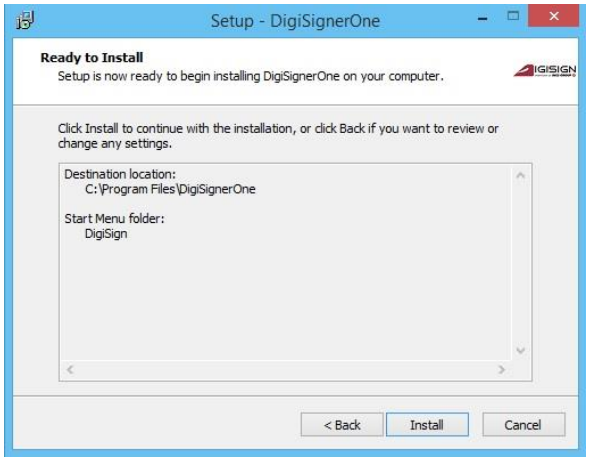
2. Open the downloaded file from your computer, select the installation language then press ***OK***

3. Press the ***Next*** button, then press ***Next*** again.



3. Press the ***Next*** button, then press ***Install.***





S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

4. In the next step you will have to select the needed component for using the DigiSign qualified digital certificate issued on your cryptographic eToken.

- ✓ Options **Install eToken driver** and **Install DigiSign Trust Chain** will be selected only if you did not use a usb eToken device and digital certificate issued by Digisign on your computer.
- ✓ Option **Install program for previewing pdf - GhostScript GPL** will install the GhostScript application wich will allow Digisigner ONE to display PDF documents within the application.
- ✓ Option **Run DigiSigner One** will open the Digisigner One application after pressing the **Finish** button.

IMPORTANT!

If your operating system is Windows XP you need to install **.NET Framework 4.0**.

III. Installing the eToken usb device and the Digisign trust chain

Warning! You need to follow this steps if you checked the options **Install eToken driver** and **Install DigiSign Trust Chain** specified in the previous step.

If you did not checked these options please proceed to the next step **IV. How to use the Digisigner ONE application.**

Make sure that your operating system is up to date, that you don't have installed an antivirus/firewall that might block the eToken driver installation.

Update your operating system using Windows Update or follow the instructions on the Microsoft website in order to install the latest updates correctly.

S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

IMPORTANT! Make sure that:

- you have administrator privileges on the operating system you wish to install the digital certificate
- time, date, and time zone on your computer are correct
- the eToken usb device isn't plugged in the computer during the installation.

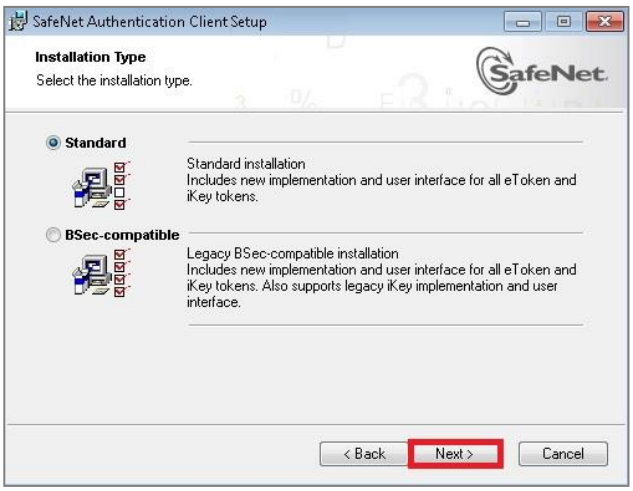
1. Installing DigiSign eToken PKI Client driver

Compatibility: - Windows XP Service Pack 3, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10;
- Windows Server 2003, Windows Server 2008, Windows Server 2012.

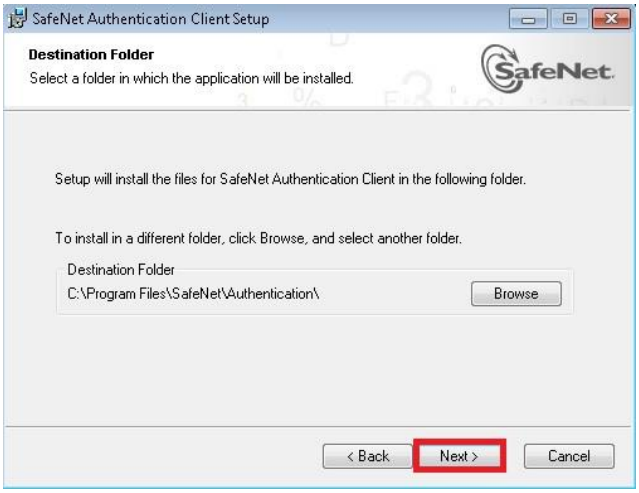
If the *Install eToken driver* was checked, the installation will start and you will have to press the *Run* button.

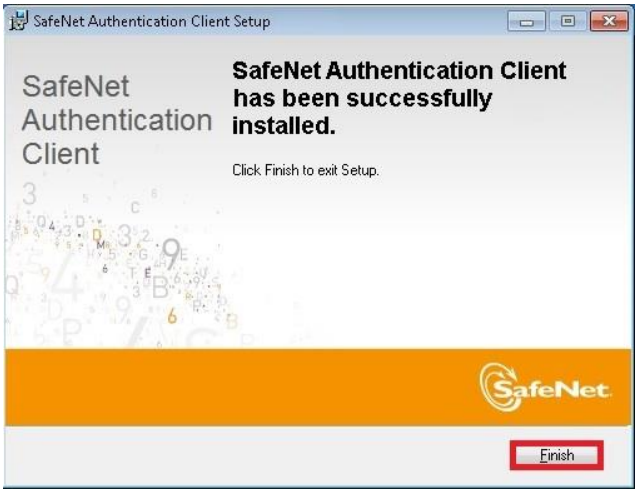
In the new open window, in order to start the installation press the *Next* button then select, the desired language and press *Next* again.

Check the field **I accept the license agreement**, press *Next* and in the following window make sure to check **Standard** and proceed by clicking the *Next* button.



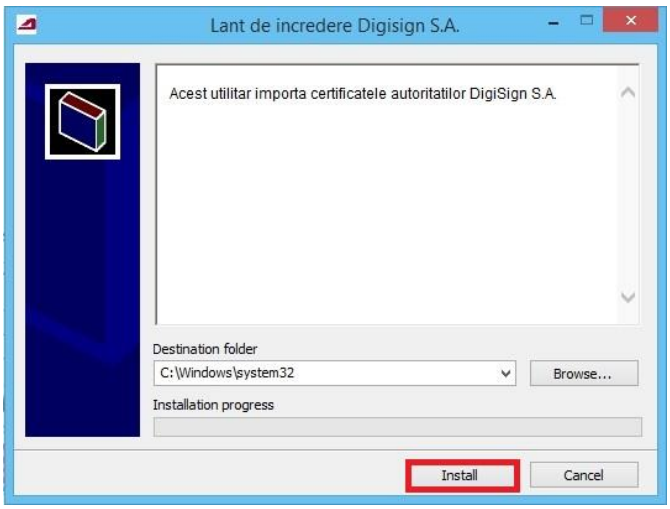
Press **Next,** then **Finish** in order to complete the driver installation process.





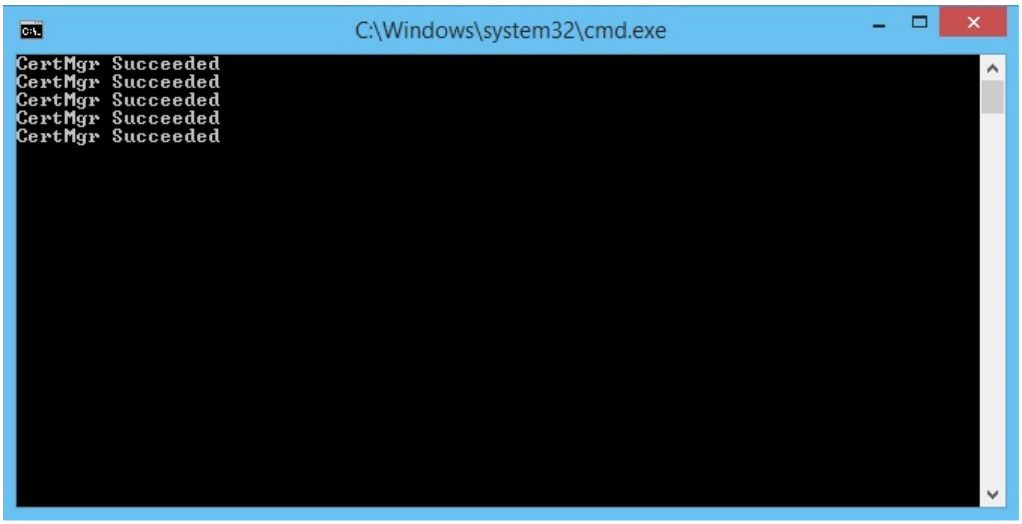
2. Installing the Digisign Trust Chain.

If the option *Install DigiSign Trust Chain* was checked, the installation of the Digising trust chain will start, you need to press the *Install* button to proceed further in the installation process.



IMPORTANT! Make sure that the Digisign Trust Chain is installing correctly.

In the next window the message **„CertMgr Succeeded"** will appear when the Trust Chain is successfully installed.



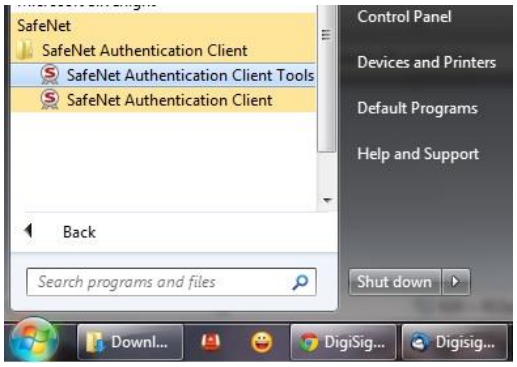
If you recieve the message *CertMgr Failed* , you have to manually download the Trust Chain from the following address https://digisign.ro/uploads/cert.zip , right click on **cert.exe** file and select **"Run As Administrator"**.

Plug into your computer the cryptographic USB SafeNet eToken device.

S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

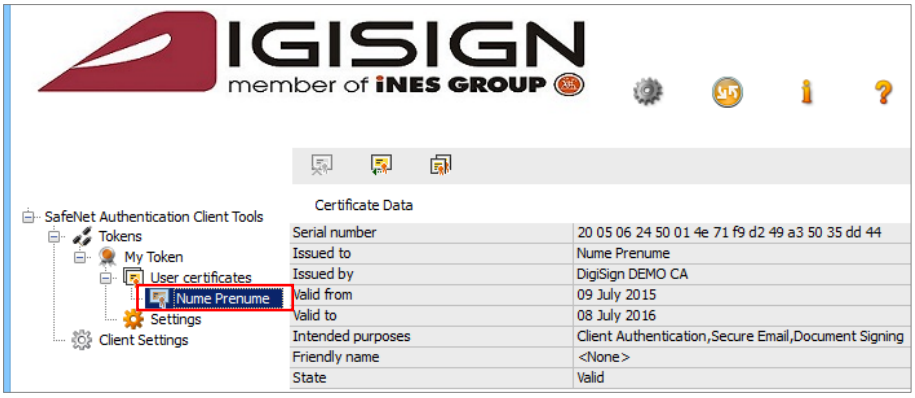
3. Verifying the Digisign Trust Chain and the SafeNet Driver installation.

a) From the **Start** menu choose **All Programs**-> **SafeNet-> SafeNet Authentication Client**-> **SafeNet Authentication Tools**.

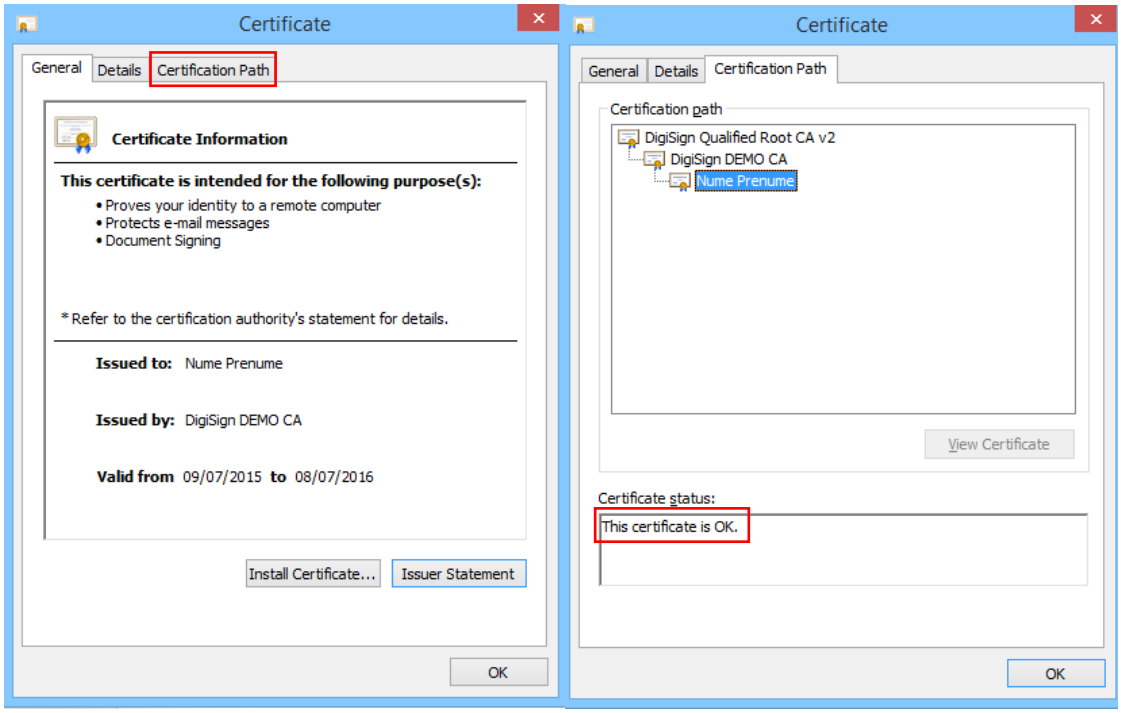


b) In the next window press the *Advanced View* button (picture)

c) On the left side menu double click on the *User Certificates* field, then double click on your certificates name.



d) The next window will display details about your digital certificate, in order to verify if the certificate is correctly installed select the *Certificate Path* tab.



IMPORTANT! If the displayed message in the ***Certificate status*** field is ***The issuer of this certificate could not be found***, please proceed by installing Digisign's **Trust Chain**(page 7, step 2 of the present document)

IV. How to use Digisigner One application

Connect the cryptographic eToken device which contains the digital certificate issued by Digisign and start the Digisigner One software from the desktop shortcut or by opening **Start ⇨ All Programs ⇨ DigiSign ⇨ DigiSigner ONE**

DigiSigner ONE picture

S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

When you open *Digisigner One* the category menu will appear.

Home screen of DigiSigner ONE application

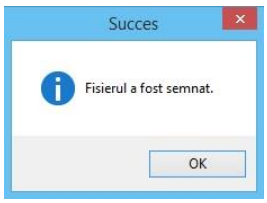
1. **Signing files in p7m and p7s format**

a. To digitally sign a document you need to use the following options:

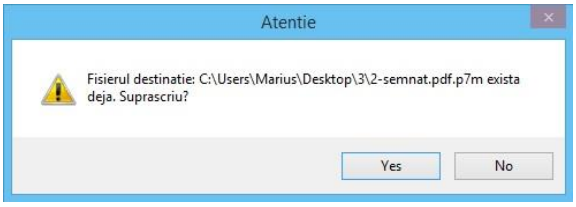
- ***Main file:*** *Select the file you want to sign*
- **Signed file:** Select the file's name and the location of the file
- **Signing certificate:** Select the digital certificate issued by Digisign;
- **File extension:** Select the signed file extension**:**
  - ➢ **P7S**: **a.** Attached signature – it will save the signed file and also the applied signature;
    b. Detached signature – it will save only the applied signature;
  - ➢ **P7M**: it will save the applied signature and also the original file.
- **Standard:** *PKCS#7* or *CADES*;
  The extended/advanced digital signature created using the CADES standard allows the signature validity to be available even when the digital certificate has expired.
- **Signature:** Select the type of signature you wish to apply on the document - signature, co-signing or counter-signature;
- **Algoritm:** Select the SHA-1 or SHA-256 cryptographic algorithm you want to use*;*
- **Aplică marcă temporală:** By choosing this option beside the digital signature you wish to include, there will also be a time stamp wich certifies that the document has been signed at a certain time and date;
- **Extrage conținut:** If the selected document contains a digital signature then the *Extrage Continut* button becomes activ;

- **Semnează fișier**: Press this button when you want to sign a file that you previously selected

After selecting the *Semneaza fisier* button you will recieve the following message *Fisierul a fost semnat.*

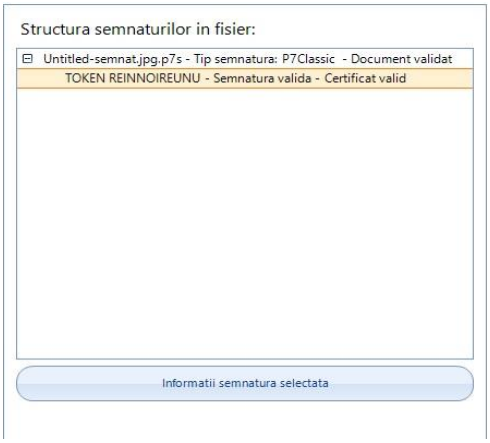


If the file you want to sign already exists in the folder, the program will ask if you want to overwrite the existing document.

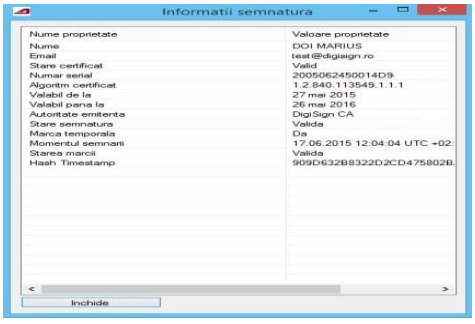


b. The structure of a digital signature in a document

If the document already contains a digital signature it will be displayed as in the example below:

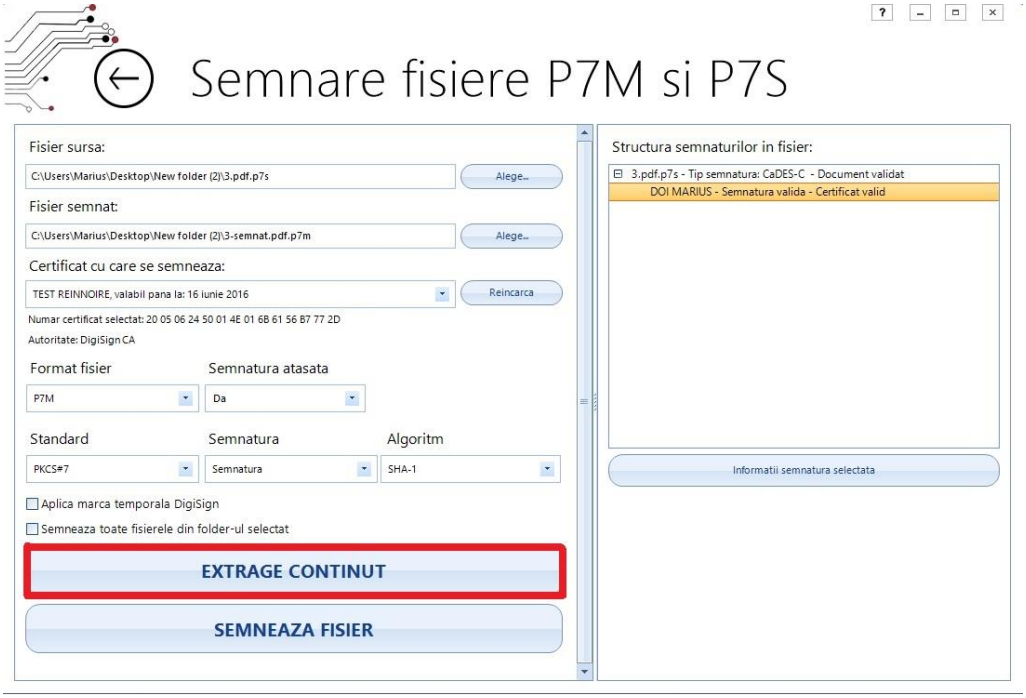


In order to view the signatures information you need to select a signature then press the ***Informații semnatură selectată*** button, you will see the signatures status and also on what time and date has the document been signed.



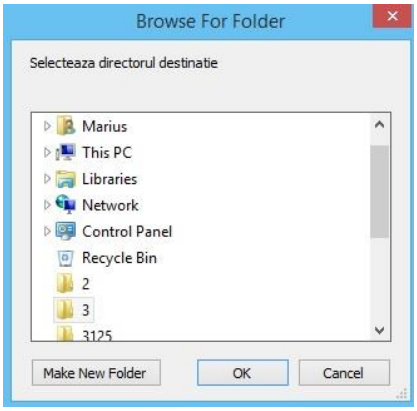
c. Extract content

If you want to apply a co-signature or counter sign a signed document, you have the possibility to verify that document by pressing the ***Extrage conținut*** button which will save the document on your computer.

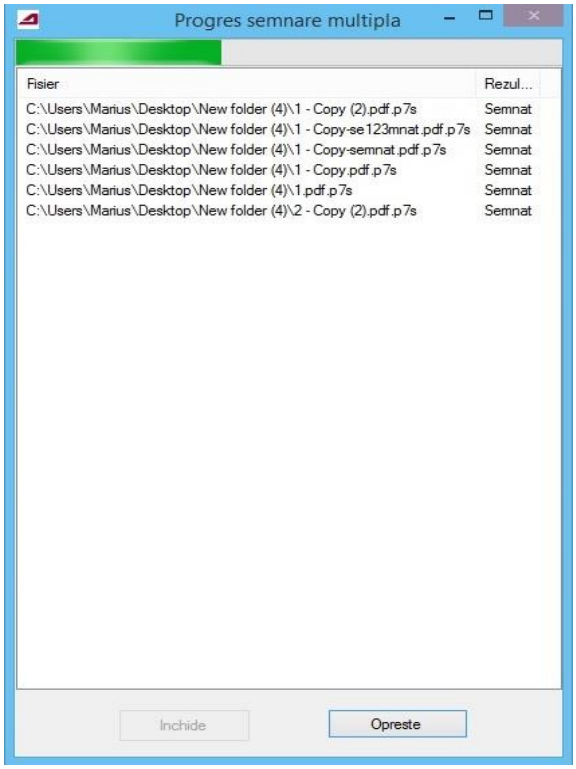


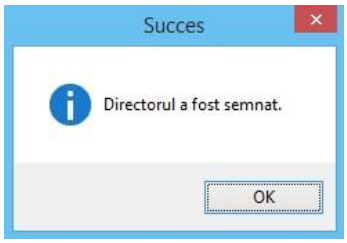
- **Semnează toate fișierele din folder-ul selectat:** This option allows you to sign all documents from a folder , but in order to do that you need to have a certificate license. If you wish to purchase a license please contact us at helpdesk@digisign.ro or at the telephone number 031.620.12.88

If you already purchased a certificate license, in order to sign every document in a folder in a p7m and p7s format please select the *Semnează toate fișierele din folder-ul selectat* option then it's necessary to select a destination folder if you want to save the signed files.



After selecting the destination folder press *Semnează fisier* to start the signing process. When the signing process is completed the following message will be displayed : *"Directorul a fost semnat".*

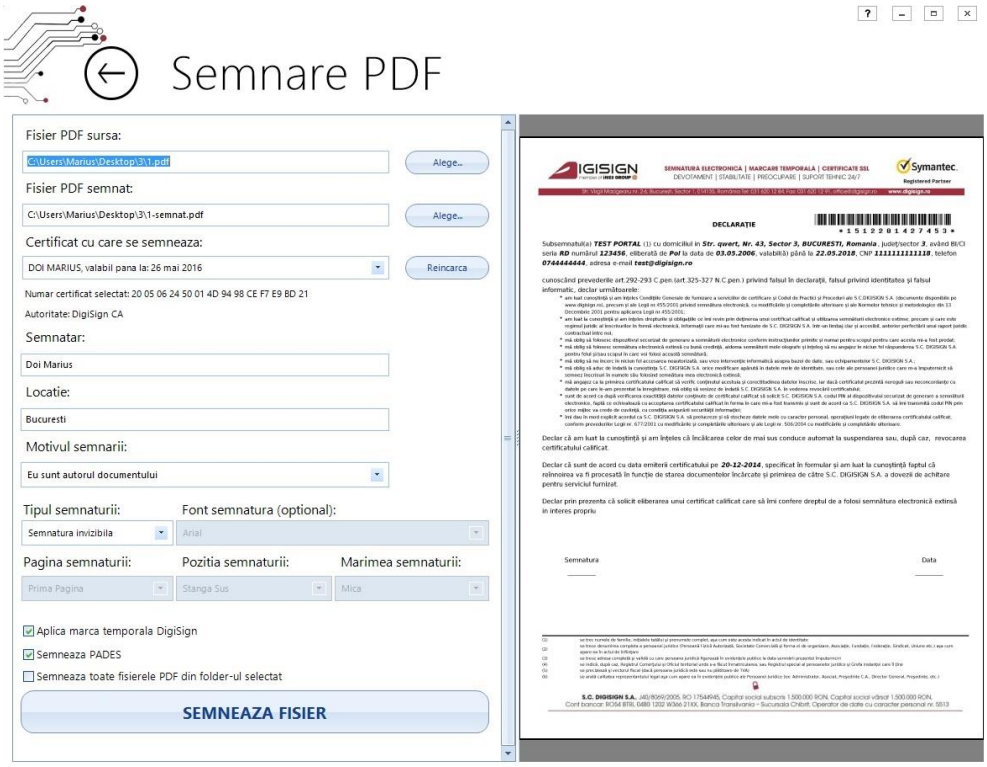




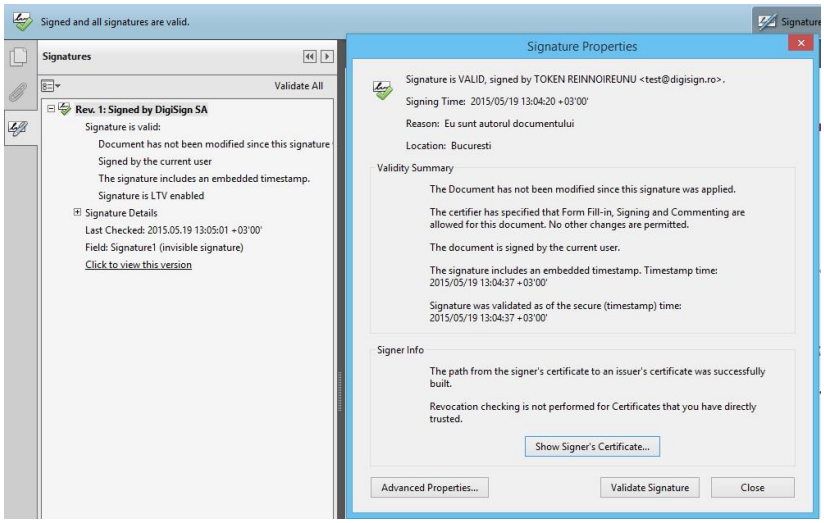
2. **Digitally signing a PDF file**
   - **Fișier sursă***:* Select the file you want to sign;
   - **Fișier semnat:** Select the name and destination folder before saving the file ;
   - **Certificat cu care se semnează:** Select the digital signature you want to apply on the document;
   - **Semnatar:** It will display the certificate name, also the displayed name can be changed (to modify this field you have to select *Semnătură vizibilă*);
   - **Locație:** For your location to appear in the digital certificates structure please select *Semnătură vizibilă*;
   - **Motivul semnăturii:** You can write or select a "signing reason" (Motivul Semnarii). This field/option can be found in the PDF's signature structure only if the signature type is visible (Semnatura Vizibila)*;*
   - **Tipul semnăturii:** Select the digital signature tipe:

     ➢ **Semnătură invizibilă** - The signature is not visible but it appears in the PDF structure;

S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit



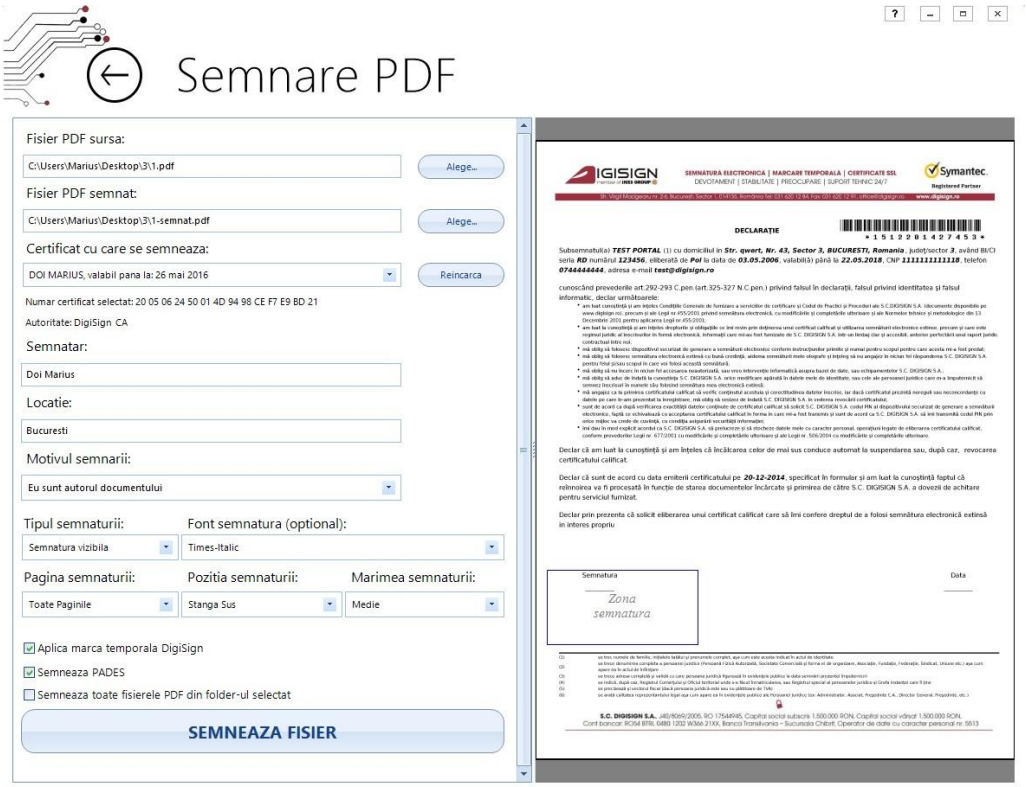
The digital signature will be displayed in the PDF structure in the following way:



➢ **Semnătură vizibilă** - The signature is visible on the document and can be configured by using the following options:

- ✓ Font semnătură (opțional) – Select the font for the digital signature;
- ✓ Pagina semnăturii – *Select the page wich will contain the signature, you can choose to display it on the first page(Prima Pagina), the last page(Ultima Pagina) or all pages(Toate paginile).* ***In order to digitally sign every page(Toate paginile) you need to purchase a certificate license, please contact us at helpdesk@digisign.ro or at our telephone number 031.620.12.88)***

- ✓ Poziția semnăturii – *Stânga sus(upper left corner), Dreapta sus(upper right corner), Stânga jos(down left corner)* sau *Dreapta jos(down right corner)*;
- ✓ Mărimea semnăturii – *Mică(small), Medie(medium)* sau *Mare(wide)*.

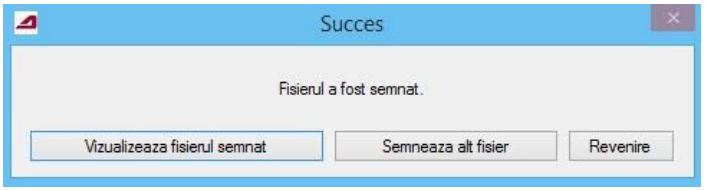


Unlike the Semnătură invizibilă option, the Semnătura vizibilă option offers you the possibility to place the signature in any location you desire just drag the signature anywhere on the document.

- **Aplică marcă temporală:** Check this option if you wish to include a time stamp attesting that the document was signed at a certain time and date.
- **Semnează PADES:** Check this option if you wish to include the PADES standard to the signature;
  The extended/advanced digital signature created using the PADES standard allows the signature validity to be available even when the digital certificate has expired.
- **Semnează fișier**: Press this button in order to sign the chosen document.

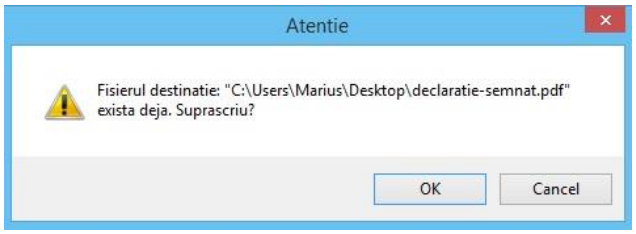
S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

After selecting the *Semneaza fisier* button the message *Fisierul a fost semnat* will appear , you must choose one of the following options: *Vizualizează fișier semnat* (view signed document), *Semnează alt fișier* (sign another file) and *Revenire* (return).

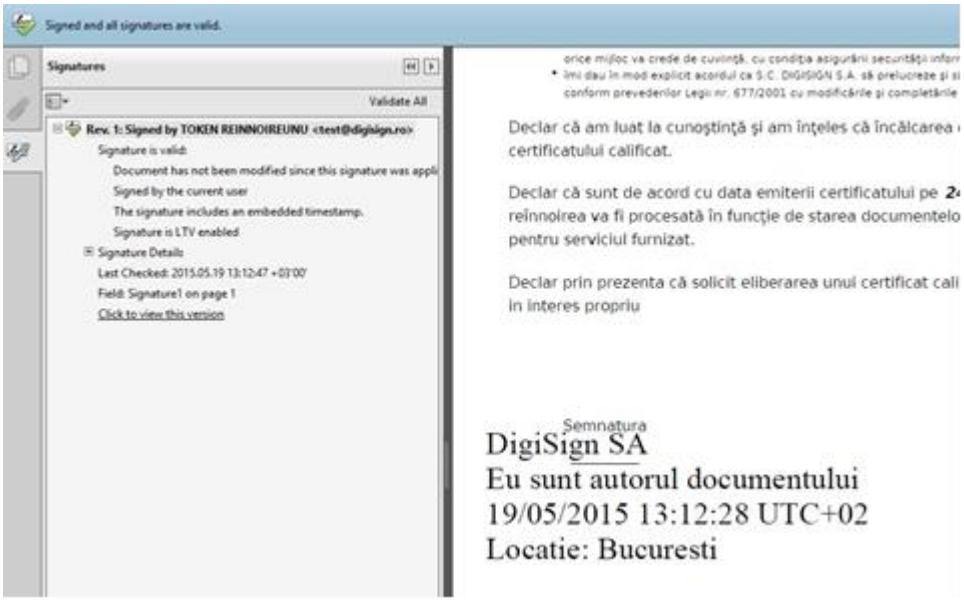


- **Vizualizează fișierul semnat –** By selecting this button the signed PDF will open;
- **Semnează alt fișier –** By selecting this button you can sign a different document using the configuration you already selected;
- **Revenire –** By selecting this button the previous configuration will reset..

If the file you want to sign already exists in the folder, the program will ask if you want to overwrite the existing document.

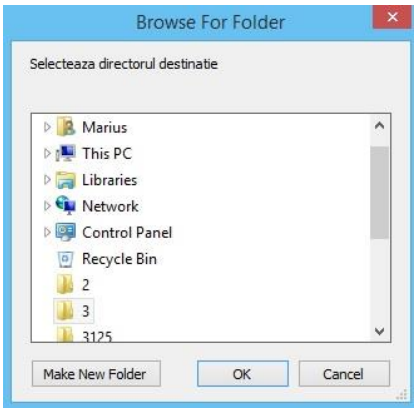


Inside the PDF the digital signature will be displayed in the following manner:

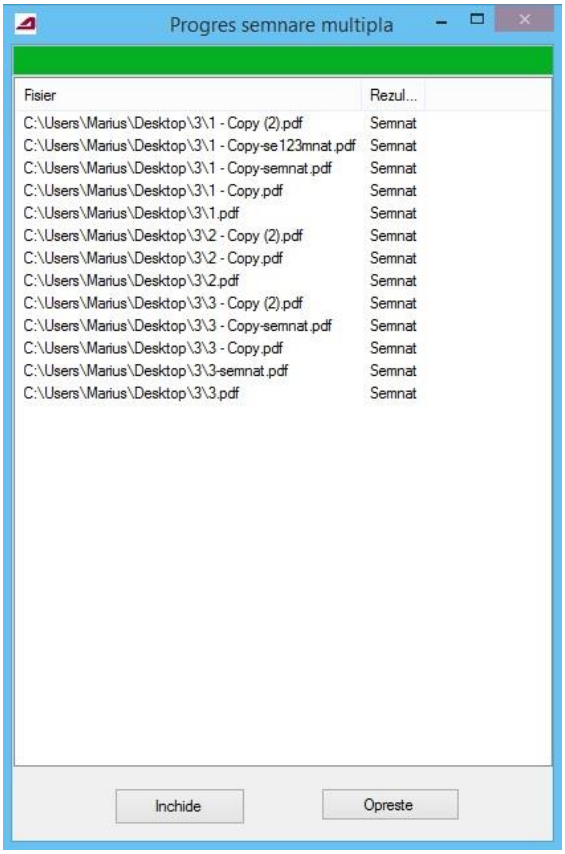


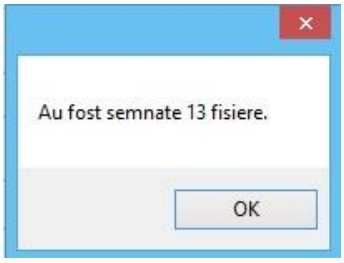
- **Semnează toate fișierele din folder-ul selectat:** You need a certificate license.

If you already purchased a certificate license, in order to sign every PDF document in a folder please select the *Semnează toate fișierele din folder-ul selectat* option then it's necessary to select a destination folder for saving the signed files.



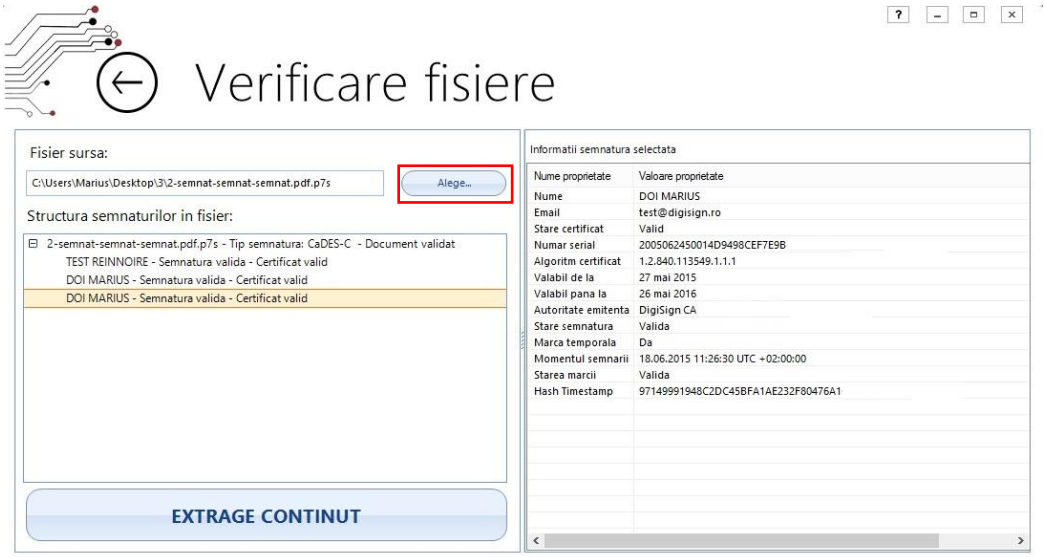
After selecting the destination folder press *Semnează fisier* to begin the signing process. When the signing process is completed the following message will appear *Au fost semnate 13 fișiere* (13 is the example in the following picture).



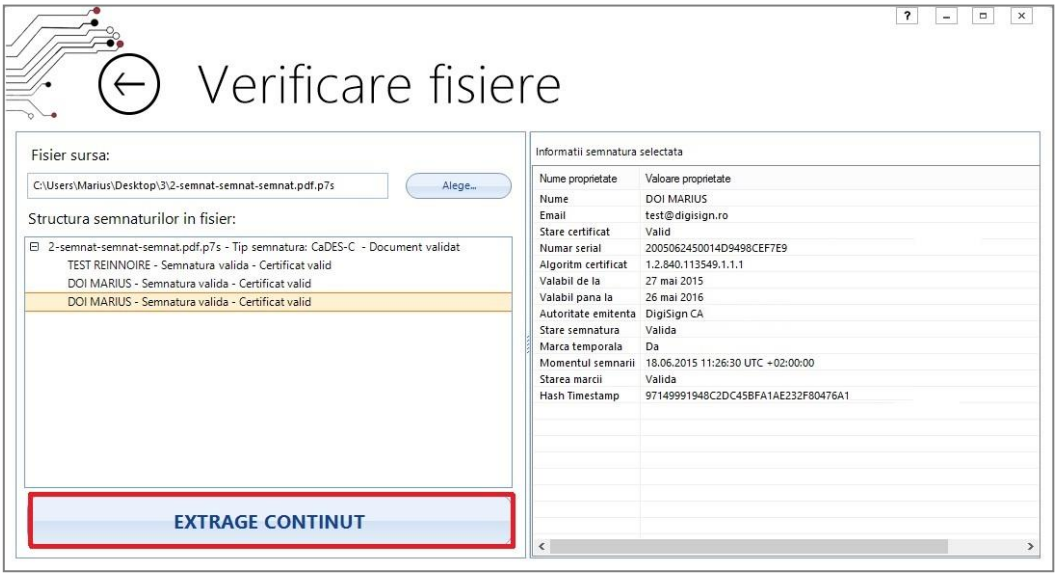


3. **Verifying a digitally signed document**

To verify a signed document (a signed file in p7m/p7s format) you need to access *Verificare fisiere* from the main menu and press *Alege* button.

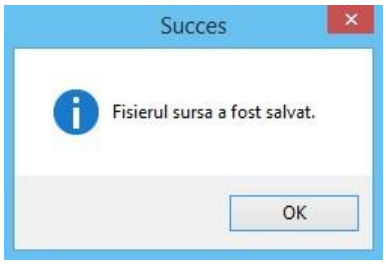


After selecting the signed document , the digital signatures applied to the document will be displayed on the left side and on the right side if you select a signature it will show the signature details.

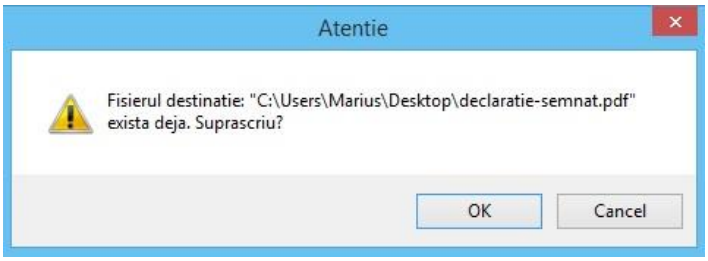


If you want to extract the original file press the *Extrage conținut* button and select the destination folder.

After selecting the *Extrage continut* button the following message will appear: *Fisierul sursă a fost salvat.*

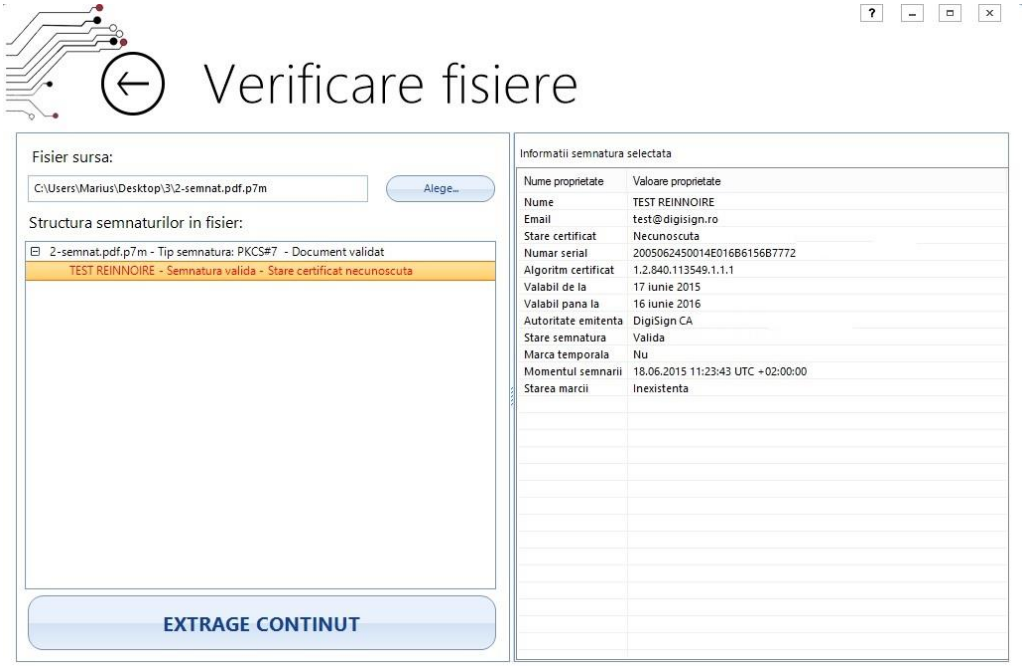


If the file you want to extract already exists in the destination folder the program will ask if you want to overwrite that document.



Note:

- If the message ***Stare certificat necunoscuta*** is shown it means that you don't have the certification authority chain of trust installed
- If the message ***Certificat invalid*** is shown it means that the signing certificate is expired, revoked or suspended.



4. Encrypting a file

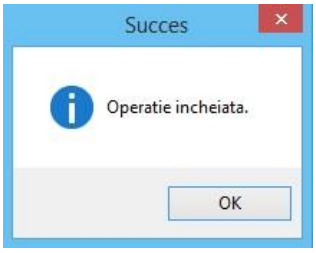
- **Fișier sursă:** Select the file you want to encrypt;
- **Fișier semnat:** Select where you want to save the encrypted file and its name;
- **Algoritm criptare:** Select the encryption algorithm;

- **Certificatele disponibile pentru criptare:** It will display the certificate available in the Personal certificate store;
- **Certificatele pentru care se criptează:** Select the desired certificate/certificates then pres the arrow;

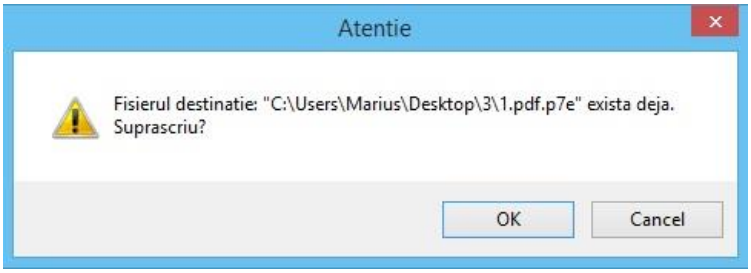
S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

- **Criptează tot directorul:** This option will allow you to encrypt all the documents in a folder, you need a certificate license. In order to encrypt all the documents in a folder you need to purchase a certificate license, please contact us at helpdesk@digisign.ro or at our telephone number 031.620.12.88
- **Criptare fișier:** After you selected the document, the algorithm and the certificate press this button in order tot encrypt the file ;
- **Criptare fișier și ștergere:** Select the document, algorithm and certificate then press this button in order to encrypt the document. After presing this button your original document will be deleted.;
- **Criptare și email**: After selecting the document, algorithm and certificate press this button to encrypt the document and send it via email.

After selecting the *Criptare fișier, Criptare fișier și ștergere and Criptare și email* buttons the following message will appear *Operație încheiată*.



If the file you want to encrypt already exists in the destination folder the program will ask if you want to overwrite that document.

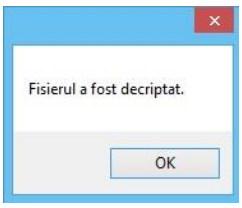


S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

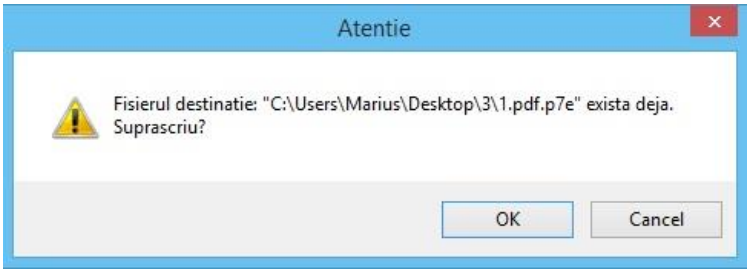
5. **Decrypting a file**

- **Fișier sursă***: Select the file you want to decrypt*;
- **Fișier semnat:** Select where you want to save the decrypted file and its name;
- **Certificat cu care se decriptează:** Select the certificate that was used to decrypt files
- **Decriptare fișier:** Select *Decriptare fișier* in order to decrypt the file.

After selecting the *Decriptare fisier* button the following message will appear *Fișierul a fost decriptat.*



If the file you want to decrypt already exists in the destination folder the program will ask if you want to overwrite that document.



S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

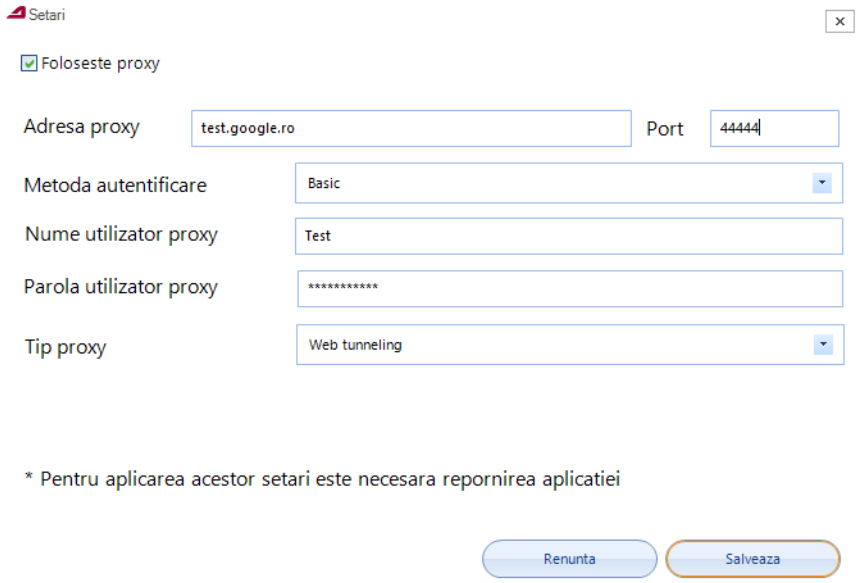
6. Proxy settings

The proxy settings can be configured by pressing the settings button.

Proxy settings offers you three ways of authentication:

- Fără autentificare – it does not require authentication
- Basic - By user and password
- Digest - By user and password

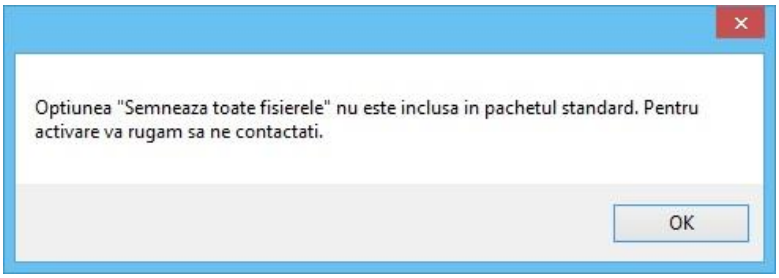
Also you can select the proxy tipe: by Web Tunneling or SOCKS.



S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

V. Errors and Warnings

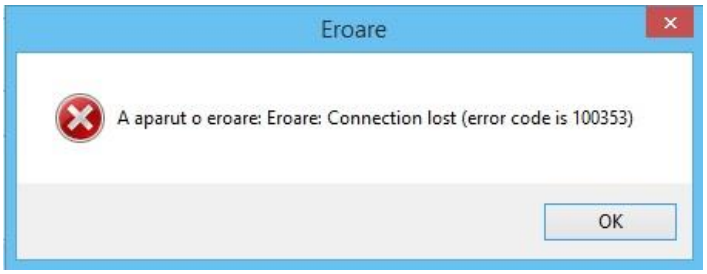
a) The „Semnează toate fișierele" option



Solution:

- ✓ You need to purchase a certificate license.
- ✓ If you already have a license and the message still appears please delete all the files from C:\Users\NumeUser\AppData\Roaming\Digisigner

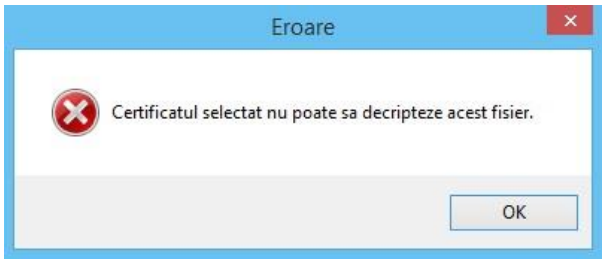
b) A apărut o eroare: Error code is 100353



Solution:

- ✓ *Check if the time, date and time zone are properly set up.*

c) Error decrypting a file



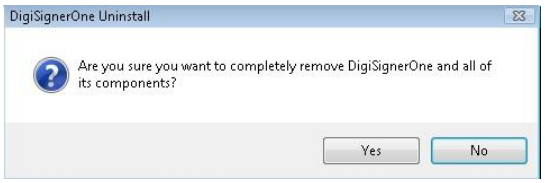
Solution:

- ✓ The selected certificate for decrypting a file does not correspond with the certificate for wich was encrypted.

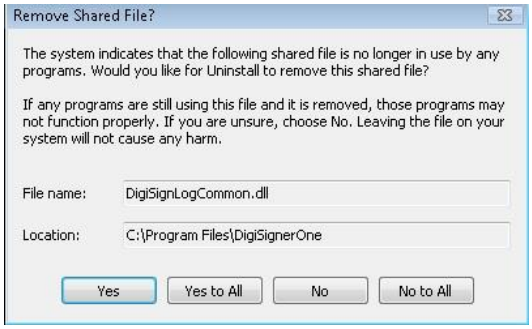
S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit

VI. Uninstalling Digisigner One

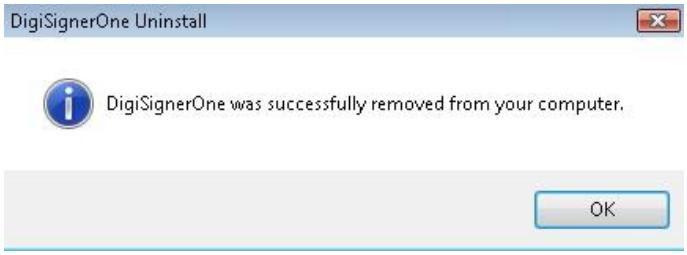
If you want to uninstall the Digisigner ONE application go to *Control Panel-> Programs and Features*, select *Digisigner One*, choose *Uninstall* then press *Yes*



Select *Yes to All*



In order to complete the uninstall process press the *OK* button.



VII. Updates

Nr. Crt.	Version	Date
1	1.0	09.07.2015
2	1.1	22.02.2016
3	1.2	13.10.2016
4	1.3	15.05.2018

S.C. DIGISIGN S.A., J40/8069/2005, RO 17544945, Capital social subscris 1.500.000 RON, Capital social vărsat 1.500.000 RON,
Cont bancar: RO54 BTRL 0480 1202 W366 21XX, Banca Transilvania – Sucursala Chibrit