Autoritatea de înregistrare

Ghid FirmaCerta pentru Windows

Categorie	**TSP-Firma Digitale**	ID document	**NAM-User Guide**	**Namirial S.p.A.**
Autor	**Michelangelo Bonvini**	Notă privind confidențialitatea	**Document Public**	Autoritatea de înregistrare
Verificat de	**Gabriele Bocchini**	Versiunea	**1.0**	**Gabriele Bocchini**
Aprobat de	**Gabriele Bocchini**	Data emiterii	**01/02/2019**	_____

Namirial S.p.A.

Sediu social, management și administrare 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
Cod fiscal/Registrul Comerțului din Ancona nr. 02046570426 - Nr. TVA IT02046570426
Capital social 6.500.000,00 € vărsat integral
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com

UNI EN ISO 9001:2015 - Certificat nr. 223776 | **UNI EN ISO 27001:2013** - Certificat nr. IT280490

– Această pagină este lăsată necompletată în mod intenționat –

INDEX

Index **3**

Istoricul modificărilor **7**

1 Introducere **8**

1.1 Scopul documentului și domeniul de aplicare 8

1.2 Definiții și acronime utilizate în acest document 8

2 Instalarea **10**

3 Interfața grafică **12**

4 Funcții principale **12**

4.1 Semnătura: 12

4.1.1 Semnarea 13

4.1.2 Countersign (Contrasemnare) 13

1.1 Sign and time stamp (Semnare și marcare temporală) 13

1.2 Verify (Verificare) 13

1.3 Timestamp (Marcaj temporal) 14

1.4 Device Manager (Manager dispozitive) 14

4.1.3 Change Pin (Modificare PIN) 14

4.1.4 Unlock Pin (Deblocare PIN) 15

4.1.5 Change PUK (Modificare PUK) 15

4.1.6 View Certificates (Vizualizare certificate) 16

4.1.7 Device Check (Verificare dispozitiv) 17

4.1.8 Certificates Renewal (Reînnoire certificate) 17

4.2 Graphometric Signature (Semnătură grafometrică) 17

4.2.1 Sign Document (Semnare document) 18

4.2.2 Signatures Template (Șablon de semnături) 18

4.3 Utility (Utilitar) 21

4.3.1 Encrypt and Decrypt (Criptare și decriptare) 21

4.3.2 General Options (Opțiuni generale) 21

4.3.3 Proxy și conexiuni 24

4.3.4 Signature Options (Opțiuni de semnare) 25

4.3.5 Verify (Verificare) 26

4.3.6 Graphometric Signature options (Opțiuni de semnare grafometrică) 27

4.3.7 Options (Opțiuni) Timestamp (Marcaj temporal) 29

4.4 Help (Ajutor) 29

5 Anexa A: Modul de semnare și contrasemnare 31

5.1 Modul de semnare a unui document 31

5.1.1 Semnarea în CAdES - XAdES 31

5.1.2 Semnarea în PAdES 32

5.2 Modul de contrasemnare 35

6 Anexa B: Modul de marcare temporală a unui fișier 38

6.1 Configurarea parametrilor de marcare temporală 38

6.2 Modul de semnare și aplicare a marcajului temporal 39

6.3 Modul de separare a marcajului temporal 40

6.3.1 Modul de semnare a unui fișier în .p7m 40

6.3.2 Modul de marcare temporală a unui fișier .p7m semnat 42

6.3.3 Separarea marcajului temporal 44

7 Anexa C: Modul de verificare și vizualizare a unui fișier 45

7.1 Modul de setare automată a lansării verificării semnăturilor 46

7.2 Modul de vizualizare a unui fișier semnat 46

8 Anexa D: Modul de criptare și decriptare a unui fișier 47

8.1 Modul de criptare a unui fișier 47

8.2 Modul de decriptare a unui fișier 47

9 Anexa F: Linia de comandă 49

9.1 Comenzi și parametri 49

9.2 Exemple: 49

10 Anexa G: Caracteristici avansate 50

10.1 Semnarea mai multor documente 50

10.2 Marcarea temporală a mai multor documente 50

10.3 Semnarea și marcarea temporală a mai multor documente 51

11 Anexa H: Reînnoirea certificatului 52

11.1 Configurarea serverului proxy 52

11.2 Metode de reînnoire: Smartcard și token 53

11.3 Metode de reînnoire: Certificate automate și la distanță 55

12 Anexa I: Configurarea semnăturii la distanță 57

12.1 Introducere în aplicația Namirial OTP 57

12.1.1 Modul de deschidere a aplicației 57

12.1.2 Configurarea OTP Namirial 57

12.1.3 Android 58

12.1.4 iOS 58

12.2 Activarea serviciului Namirial SignEngine 59

12.3 Modul de semnare a unui document 60

12.3.1 Username (Nume de utilizator) 61

12.3.2 Selectarea Remote Device (Dispozitiv la distanță) 62

12.3.3 Semnarea în format PAdES 63

12.4 Procedura OTP SMS 64

12.5 Procedură OTP pentru mobil: OTP Namirial 65

12.6 Procedura Hardware OTP 66

12.6.1 Activare OTP 66

13 Autentificare web 68

14 Anexa J: Bit4id – Linux 68

14.1 Change PIN (Modificare PIN) 69

14.2 Unlock PIN (Deblocare PIN) 70

14.3 Change PUK (Modificare PUK) 70

15 Anexa K: Bit4id – MacOS 71

15.1 Change PIN (Modificare PIN) 72

15.2 Unlock PIN (Deblocare PIN) 72

15.3 Change PUK (Modificare PUK) 73

Referințe 73

Index tabele 74

Index figuri 74

ISTORICUL MODIFICĂRILOR

VERSIUNEA	**<version>**
Data	01/02/2019
Motive	Prima ediție a documentului cu funcționalitate nouă
Modificări	---

1 INTRODUCERE

În sistemul de drept italian, termenul SEMNATURĂ DIGITALĂ se referă la un tip de semnătură electronică calificată, căreia îi este atribuită o valoare probatorie completă comparabilă, în mod substanțial, cu o semnătură originală. La fel ca semnarea unui document pe hârtie, semnătura digitală poate fi plasată într-un document electronic.

Tehnologia din spatele semnăturii digitale asigură, în plus, că documentul semnat nu poate fi modificat fără invalidarea aceleiași semnături și oferă posibilitatea de a atribui documentului o anumită dată și oră, prin mecanismul de marcare temporală.

FirmaCerta este instrumentul ideal pentru a semna în același timp volume mari de documente digitale, cum ar fi facturi, polițe de asigurare, chitanțe, plăți, transferuri și orice alt document digital;
Facilități:

- Semnarea documentelor păstrând formatul original (.PDF sau .XML după semnare, prin menținerea aceluiași format);
- Posibilitatea de a selecta dispozitivul hardware pe care doriți să îl utilizați pentru a pune semnătura (Smart Card – Token – semnătură la distanță);
- Posibilitatea de a plasa/asocia un marcaj temporal unui document sau unei semnături (grafometrice);
- Permite glisarea și fixarea (drag and drop) unuia sau mai multor fișiere în aceeași casetă pentru semnătură;
- Permite semnarea documentelor PDF protejate prin parolă.

1.1 SCOPUL DOCUMENTULUI ȘI DOMENIUL DE APLICARE

Acest document, identificat prin codul prezentat în titlu, descrie pașii de urmat pentru a instala Clientul FirmaCerta și driverele bit4id pentru recunoașterea certificatelor; descrie, de asemenea, funcțiile Clientului FirmaCerta, care este un software pentru gestionarea semnăturilor digitale și a marcajelor temporale personale.
Un document semnat nu poate fi modificat de software-ul folosit pentru a-l crea. În orice caz, dacă ar fi posibil, pentru principiile criptografiei asimetrice nu mai poate exista corespondență între conținutul documentului și semnăturile sale asociate, FirmaCerta va eșua în timpul operațiunii de verificare a documentului.

1.2 DEFINIȚII ȘI ACRONIME UTILIZATE ÎN ACEST DOCUMENT

TERMEN	SEMNIFICAȚIE
Semnătură digitală	Este un tip special de semnătură electronică calificată și reprezintă setul de date în formă electronică, atașate sau conectate prin asociere logică cu alte date electronice, utilizate ca metodă de identificare electronică.
Marcaj temporal (marcă de timp)	Este o secvență de caractere care reprezintă o dată și/sau o oră pentru a asigura apariția reală a unui anumit eveniment. Data este de obicei prezentată într-un format compatibil, deci va fi ușor de comparat cu alta pentru a determina ordinea cronologică. Aplicația practică se numește marcare temporală. O extensie de fișier marcat conține marcajul temporal .m7m
Semnătură grafometrică	Este o semnătură electronică realizată conform unui proces care este capabil să compileze într-un document electronic un set de date obținute prin prelevarea unei semnături comune
PDF: (Portable Document Format)	Format de fișier grafic dezvoltat de Adobe Systems. Acest standard este utilizat în mod normal pentru a pune la dispoziție documente reprezentative, pagini tipărite de cărți, reviste, broșuri, cataloage, liste de prețuri etc. și pentru toate acele documente pentru care este important să se păstreze aspectul grafic. Paginile vizibile pe ecran pot fi de obicei tipărite (dar nu întotdeauna), dar nu modificate folosind Acrobat Reader, care este o aplicație gratuită utilizată pentru citirea documentelor PDF.

XML: (Extensible Markup Language)	Este un metalimbaj pentru definirea limbajelor de marcare bazat pe un mecanism sintactic pentru a defini și controla semnificația elementelor incluse într-un document sau într-un text.
Smart Card	Este un dispozitiv hardware similar cu un card de credit care are potențial pentru procesarea și stocarea datelor de înaltă securitate.
Token USB	Este o cheie USB care include un cip similar cu cel al unui smart card și este introdusă direct într-un port USB: astfel are aceleași funcții ale smart cardului cu același cip, drivere și software inclus, dar nu necesită un cititor cu conexiune directă la computerul dvs. prin port USB.
Drag and Drop	Glisare și fixare (Drag and Drop). Tehnică ce permite transferul fișierelor dintr-un punct în altul în interiorul unui program printr-o simplă glisare, ținând apăsat butonul din stânga al mouse-ului (drag: glisare - drop: fixare).
PIN	(Personal Identification Number) cod unic pentru identificarea unui utilizator.
Semnătură electronică	În sensul legii privind semnătura electronică, se înțelege un set de date în formă electronică, atașate sau conectate prin asociere logică cu alte date electronice, utilizate ca metodă de identificare computerizată.
Instrument	Unealtă, instrument.
Șablon	Formă. Este un șablon predefinit, care permite compunerea unei scrisori, crearea unui fișier mic etc., mult mai rapid și mai ușor.
Adobe	Este o aplicație dezvoltată de Adobe Systems pentru a crea și edita fișiere PDF. Adobe Acrobat, produs de aceeași companie care a dezvoltat PDF-ul, a fost primul program care poate procesa acest format.
captură de ecran	Acest termen se referă la o imagine sau o porțiune a unei imagini, „capturată" de pe ecran (ecran).
Etichetă	Etichetă, marcaj
.bmp	Fișier bitmap. Este formatul grafic oficial pentru Windows (a se vedea Bitmap)
Bitmap	Literalmente: „bitmap". format grafic (rastru), printre cele mai populare, acceptat de toate aplicațiile. Permite stocarea unei imagini fără pierderi de informații. Unele extensii tipice de fișiere bitmap sunt .BMP, .GIF, .JPG, .PNG, .TIFF.
Base64	Este un sistem de numerotare pozițională care folosește 64 de simboluri. Este folosit mai ales pentru codificarea datelor binare în e-mailuri, pentru a converti datele în format ASCII. Codificarea Base64 determină o creștere generală de 33 % a volumului de date care trebuie decodate.
PDF/A	Standard internațional (ISO19005), subset al standardului PDF, conceput special pentru arhivarea pe termen lung a documentelor electronice care trebuie afișate întotdeauna în același mod, chiar și după mult timp și cu diferite programe software.
Proxy	Sistem de protecție a rețelei locale împotriva accesului altor utilizatori de internet. Serverul proxy acționează ca o barieră de securitate între rețeaua internă și internet, împiedicând accesul altor utilizatori la informații confidențiale ale rețelei interne. De asemenea, serverul reduce considerabil traficul prin stocarea în memoria cache, la nivel local, a documentelor utilizate frecvent.
Program de completare	Supliment. În mediul hardware poate reprezenta orice „dispozitiv" extern (modem, scaner, mouse, monitor etc.) care trebuie adăugat la computer, în mediul software, cu toate acestea, se referă la un modul care adaugă sau extinde capacitățile unei anumite funcționalități a programului de bază.

Tabelul 1 - Definiții și acronime

Tabelul 1: Definiții și acronime

2 INSTALAREA

Descărcați software-ul de pe site-ul www.firmacerta.it secțiunea Download > Software Firmacerta > Desktop Version for Windows (Descărcare > Software Firmacerta > Versiune desktop pentru Windows) (LINK).

Și accesați expertul.

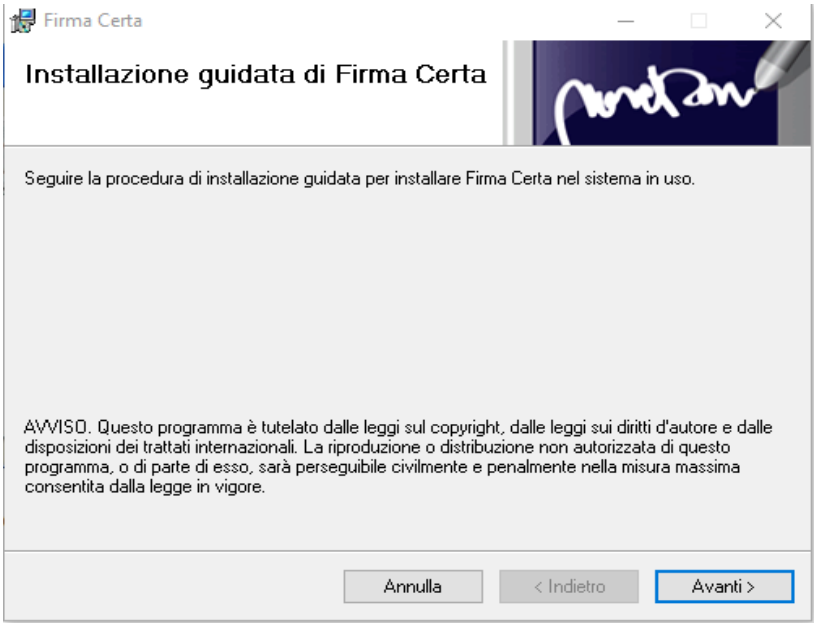


Figura 1 - Expertul firmacerta

După confirmarea respectării legilor privind drepturile de autor ale software-ului, instalarea va propune folderul de utilizator implicit.

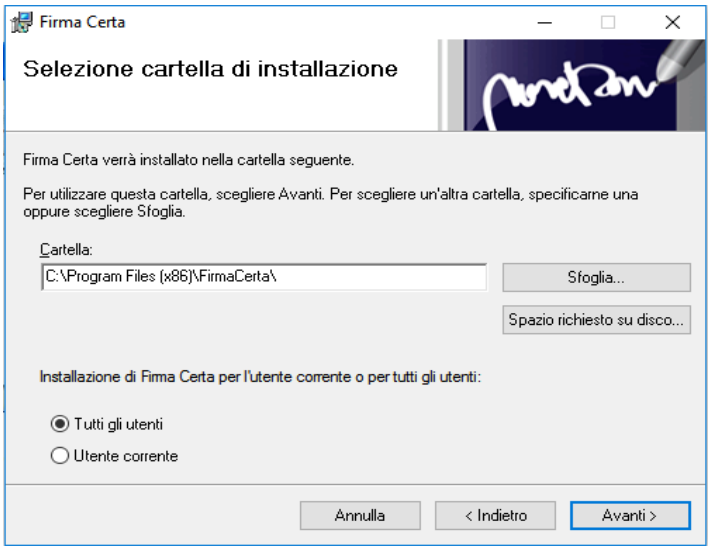


Figura 2 - Selectați folderul de destinație

ATENȚIE: *pentru a modifica folderul de destinație, asigurați-vă că aveți permisiunea necesară sau solicitați asistența administratorului de sistem.*

Apăsați Forward (Înainte) pentru a începe instalarea.

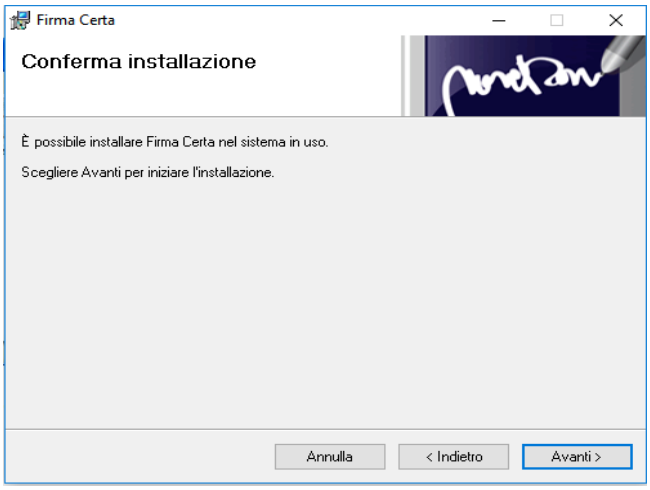


Figura 3 - Confirmarea instalării

Așteptați până la finalizarea instalării.

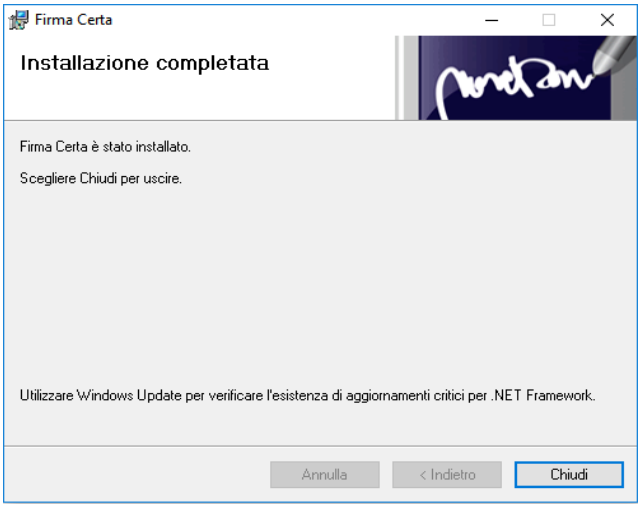


Figura 4 - Mesaj pentru instalare reușită

3 INTERFAȚA GRAFICĂ

Interfața grafică FirmaCerta este simplă și intuitivă.
Meniul este alcătuit din principalele funcții ale software-ului:

- Semnați digital orice tip de fișiere;
- Aplicați marcajul temporal;
- Utilizați semnătura grafometrică;
- Vizualizați și verificați fișierele semnate digital;

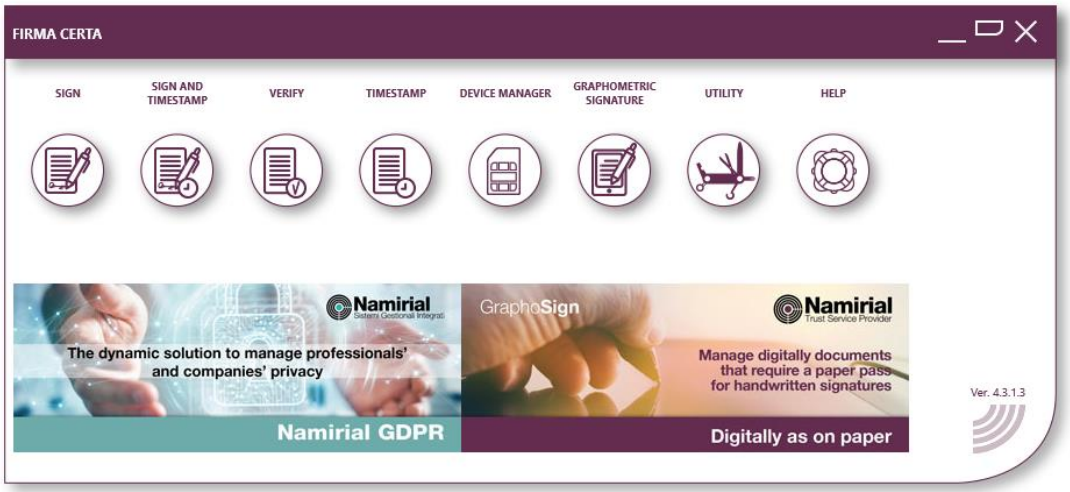


Figura 5 - Interfața grafică FirmaCerta

4 FUNCȚII PRINCIPALE

4.1 SEMNĂTURA:

Dacă dați clic pe pictograma Sign (Semnare) veți alege dacă semnați sau contrasemnați fișierul

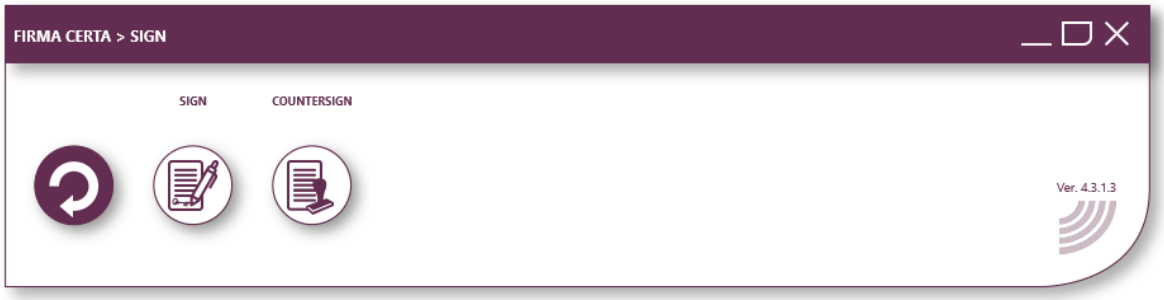


Figura 6 - Submeniu pentru semnătură

4.1.1 SEMNAREA

Cu FirmaCerta puteți semna orice document în una dintre următoarele modalități:

	Glisare și fixare (Drag & Drop): Trageți (drag & drop) simultan unul sau mai multe fișiere în fereastra FirmaCerta Software (Software FirmaCerta) și dați clic pe pictograma „Sign" (Semnare).
	Din fișier: Dați clic direct pe pictograma fișierului/fișierelor pentru a semna cu butonul din dreapta al mouse-ului, apoi selectați elementul „Sign" (Semnare) din meniul vertical.
	Din software: Dați clic pe pictograma Sign (Semnare); astfel puteți căuta, în folderele computerului dvs., fișierul pe care doriți să îl semnați.

Figura 7 - Accesarea funcției de semnare

După ce apăsați pe „Sign" (Semnare), software-ul vă va cere să selectați directorul în care doriți să salvați fișierul/fișierele semnat/e, apoi PIN-ul dispozitivului dvs. de semnare (Smart Card/cartelă SIM token).

- pentru a vizualiza întreaga procedură de semnare a unui document Anexa A: Modul de semnare a unui document
- pentru a vizualiza procedura pentru posesorii de semnătură la distanță Anexa I: Semnătura la distanță

4.1.2 COUNTERSIGN (CONTRASEMNARE)

Cu această funcție este posibilă contrasemnarea unei semnături deja prezente în document, oferind un fel de validare ierarhică.

După ce dați clic pe Countersign (Contrasemnare), software-ul va solicita folderul de destinație pentru a salva fișierul contrasemnat, apoi o confirmare cu privire la documentul selectat care urmează să fie semnat și, în cele din urmă, introducerea codului PIN al dispozitivului de semnare conectat la computer.

Consultați întreaga procedură pentru contrasemnarea unui document Anexa A: Modul de contrasemnare

Figura 8 - Accesarea funcției de contrasemnare

1.1 SIGN AND TIME STAMP (SEMNARE ȘI MARCARE TEMPORALĂ)

Prin această funcție este posibilă semnarea și marcarea temporală, într-o singură operațiune, a unuia sau mai multor documente digitale. Clientul Signature (Semnătură) vă solicită să selectați folderul de destinație al fișierului semnat. După ce apăsați pe „Sign and Timestamp" (Semnare și marcare temporală) și introduceți codul PIN, software-ul vă va solicita să introduceți acreditările „User" (Utilizator) și „Password" (Parolă) pentru a utiliza marcajele temporale.

Consultați întreaga procedură pentru semnarea și marcarea temporală a unui document: Anexa B: Modul de semnare și aplicare a marcajului temporal pe un document

Figura 9 - Accesarea funcției de semnare și marcare

1.2 VERIFY (VERIFICARE)

Această funcție permite verificarea și afișarea stării semnăturii/semnăturilor de pe document. Fereastra Result (Rezultat) va confirma integritatea, fiabilitatea, validitatea legală a certificatului și verificarea CRL și OCSP, adică faptul că certificatul este activ. În plus, datorită acestei funcții, puteți să deschideți fereastra cu detaliile care vor afișa principalele caracteristici ale certificatului (Type (Tip), Issuer Entity (Entitate emitentă), Owner (Proprietar), Certificate validity (Valabilitate certificat))

Consultați întreaga procedură pentru verificarea unui document: Anexa C: Modul de verificare și vizualizare a unui fișier

Figura 10 - Accesarea funcției de verificare

1.3 TIMESTAMP (MARCAJ TEMPORAL)

După selectarea unui fișier, cu această caracteristică puteți marca temporal fișierul respectiv, aplicând o anumită dată și oră documentului, opozabile pentru terți.
De asemenea, pentru această operațiune vi se va solicita să selectați un folder de destinație și să introduceți codul PIN al dispozitivului de semnare.

Consultați întreaga procedură pentru marcarea unui document: Anexa B: Modul de marcare a unui fișier

Figura 11 - Accesarea funcției de marcare

1.4 DEVICE MANAGER (MANAGER DISPOZITIVE)

Această funcție îi permite utilizatorului să acceseze setările dispozitivului de semnare.

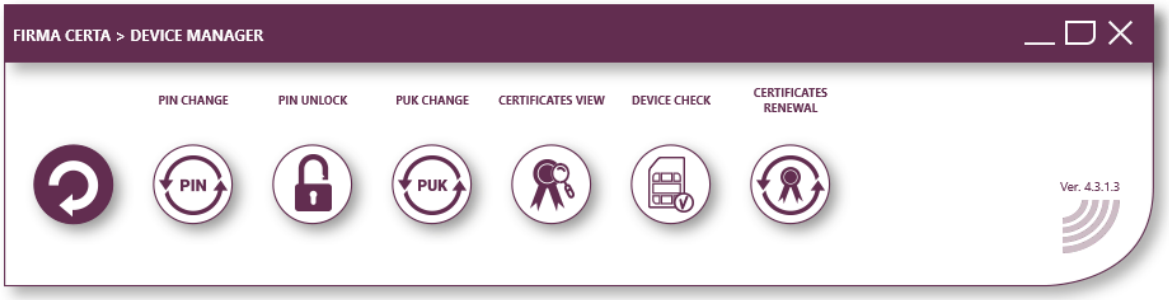


Figura 12 - Panoul de administrare a dispozitivelor

4.1.3 CHANGE PIN (MODIFICARE PIN)

Permite editarea codului PIN curent prin introducerea unui nou PIN (introducere și verificare).
NB: Posesorii de semnătură la distanță nu pot modifica codul PIN cu FirmaCerta.

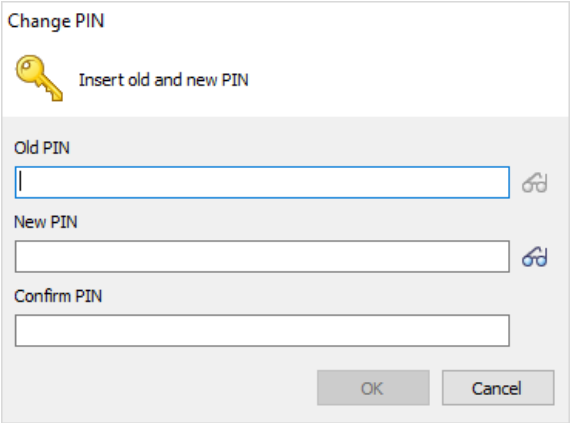


Figura 13 - Funcția de modificare a codului

4.1.4 UNLOCK PIN (DEBLOCARE PIN)

Funcție utilă pentru deblocarea codului PIN, dacă este blocat. Introduceți codul PUK (codul numeric format din 8 cifre) pe care îl găsiți în plicul neinscripționat.

ATENȚIE: Pentru a finaliza procedura, este obligatoriu ca plicul neinscripționat să vă fie pus la dispoziție după emitere.

După 3 încercări greșite de scriere a codului PUK, dispozitivul va fi blocat definitiv și va fi necesar să solicitați un nou dispozitiv de semnare.

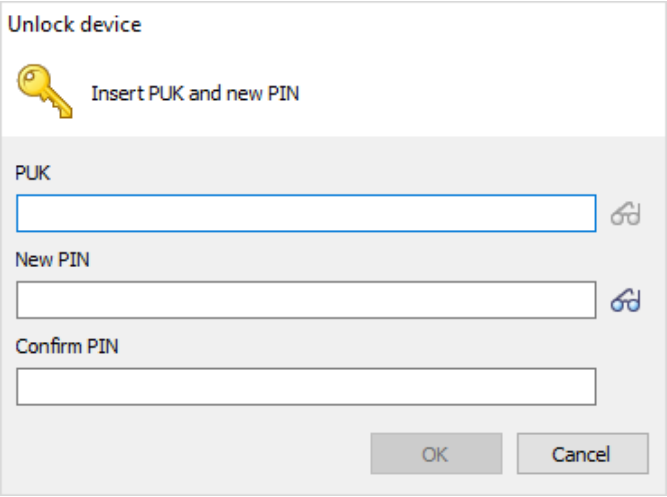


Figura 14 - Funcția de deblocare a codului PIN

4.1.5 CHANGE PUK (MODIFICARE PUK)

Permite modificarea codului PUK curent prin introducerea unui nou cod PUK (introducere și verificare).
ATENȚIE: *pentru semnătura la distanță, modificarea codului PUK nu este posibilă.*

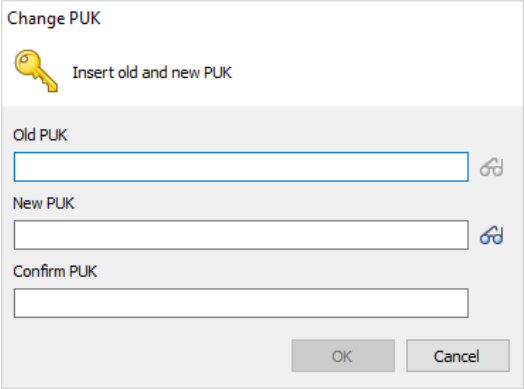
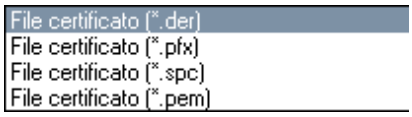


Figura 15 - Funcția de modificare a codului PUK

4.1.6 VIEW CERTIFICATES (VIZUALIZARE CERTIFICATE)

Cu această funcție este posibil exportul certificatelor dispozitivului în următoarele formate:



DER: Aceasta nu este decât o versiune binară a formatului PEM. Extensia este .der, dar uneori .cer; în acest caz, singura modalitate de a distinge formatul este să deschideți fișierul cu un editor pentru a vedea dacă este în format ASCII sau binar. Acestea sunt utilizate de obicei în platforma Java

PFX: PKCS # 12 sau PFX este un format binar care permite salvarea în formă criptată atât a certificatului serverului, cât și a certificatelor intermediare și a cheii private.
Extensia este de obicei .pfx sau .p12. Fișierele PFX sunt utilizate de obicei pe mașinile Windows pentru a face backup și pentru migrarea de la un certificat de server la altul, cu cheile private respective ale acestora.

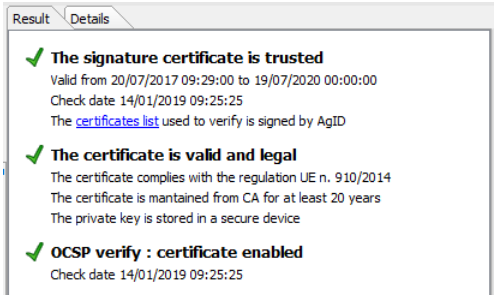
SPC: Cel mai frecvent format utilizat de autoritățile de certificare pentru testare

PEM: Cel mai frecvent format utilizat de autoritățile de certificare pentru a emite certificate, folosind în mod normal extensii convenționale .pem, .crt și cer. Acestea sunt fișiere ASCII cu codificare Base64 și conțin "----- BEGIN CERTIFICATE -----" la început și "----- END CERTIFICATE -----" la sfârșit. Pot fi în format PEM pentru certificate de server, chei private și certificate intermediare.

Prin apăsarea acestui buton veți anula pur și simplu listele de certificate înregistrate în dispozitiv din fereastra activă (fără eliminarea acestora de pe dispozitivul conectat).

Pentru accesarea opțiunilor de verificare, accesibile și din meniul Firmacerta> Utility (Utilitar).

Prin apăsarea acestei taste se efectuează verificarea certificatelor dispozitivului. Dacă dați clic pe eticheta Result (Rezultat) și/sau Details (Detalii), puteți vedea rezultatul verificării și particularitățile certificatului selectat.



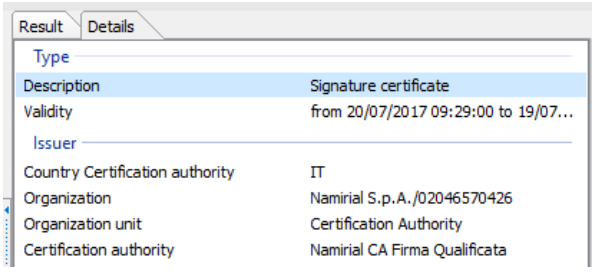
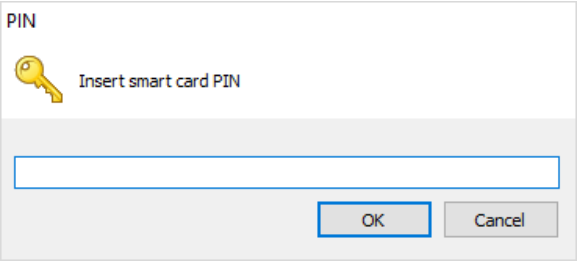


Figura 16 - Funcția de afișare a certificatelor

4.1.7 DEVICE CHECK (VERIFICARE DISPOZITIV)

Cu această funcție puteți efectua un test pentru cititorul de smart card; introducând codul PIN al dispozitivului, utilizatorul va primi informațiile despre starea echipamentului hardware (presupunând că dispozitivul a fost activat corect).



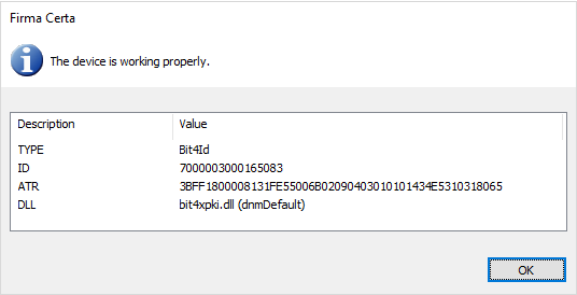


Figura 17 - Funcția de verificare a dispozitivului

4.1.8 CERTIFICATES RENEWAL (REÎNNOIRE CERTIFICATE)

Funcție necesară pentru reînnoirea certificatelor de semnătură digitală pentru încă trei ani.
Consultați **ghidul** cu informațiile esențiale pentru reînnoire (consultați Anexa H).

ATENȚIE:

1. Dacă nu apare în meniu, descărcați software-ul FirmaCerta Device Manager (Manager dispozitive FirmaCerta);
2. Dacă utilizatorul nu a fost deblocat de RAO, reînnoirea nu poate fi finalizată;
3. Certificatele nu pot fi reînnoite a doua oară.

Figura 18 - Accesarea funcției de reînnoire a certificatelor

4.2 GRAPHOMETRIC SIGNATURE (SEMNĂTURĂ GRAFOMETRICĂ)

Semnătura grafometrică este o semnătură electronică realizată conform unui proces capabil să asocieze într-un document electronic un set de date obținute prin prelevarea unei semnături comune.

Aceste date sunt obținute folosind un dispozitiv care detectează și digitalizează imaginea grafică a unei semnături la care se adaugă, în general, în funcție de caracteristicile dispozitivului utilizat, alți parametri biometrici, cum ar fi gradul de apăsare și viteza particularității grafice. Dispozitivul constă dintr-o tabletă capabilă să afișeze pentru abonat documentul semnat, recreând o experiență foarte asemănătoare cu cea a semnării unui document pe hârtie.

4.2.1 SIGN DOCUMENT (SEMNARE DOCUMENT)

Cu această funcție puteți încărca fișierul .PDF pe care doriți să îl semnați cu semnătura grafometrică.

4.2.2 SIGNATURES TEMPLATE (ȘABLON DE SEMNĂTURI)

Acest instrument permite crearea de modele diferite pentru a fi utilizate cu combinația de documente PDF, în timpul fazei aplicării semnăturii grafometrice propriu-zise. Șabloanele permit, prin selectarea unui anumit document, detectarea imediată a câmpurilor de semnătură, evidențierea acestora pe tabletă, fără ca fișierul PDF să fie răsfoit de utilizator. Pentru a înțelege cum funcționează, vom folosi ca exemplu un document generic pentru o cerere de concediu (figura de mai jos).

Dați clic pe "Signature Template" (Șablon de semnături), apoi FILE (FIȘIER) -> open (Deschidere) -> selectați fișierul .pdf pe care doriți să îl păstrați ca parametru. Lângă cursor va apărea un chenar galben, corespunzător zonei de semnătură; suprafața acestuia poate fi mărită sau micșorată prin apăsarea butoanelor corespunzătoare din bara de instrumente (figura de mai jos).

Dați clic cu butonul din stânga (sau dreapta) al mouse-ului pentru a salva primul câmp al șablonului

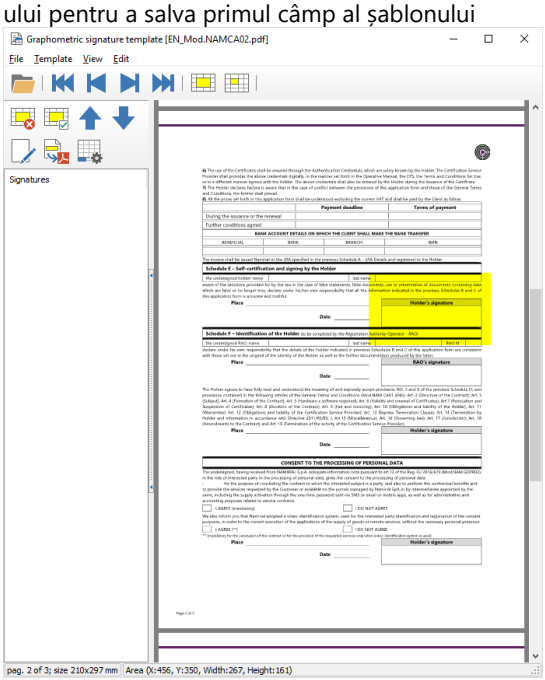
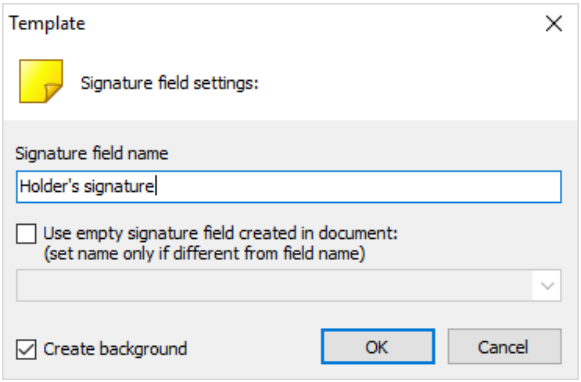


Figura 19 - Marcator în șablon

După ce câmpul a fost selectat, va apărea următoarea fereastră.



Use the empty signature field that is already present into the pdf (Se utilizează câmpul de semnătură necompletat care este deja prezent în fișierul PDF)
Acesta detectează câmpurile de semnătură create anterior în document utilizând Adobe Acrobat.

Create Background Image (Creare imagine de fundal)
Datorită acestei caracteristici, este posibil să faceți o captură de ecran a zonei de semnătură selectată, care poate fi personalizată și utilizată cu orice fel de modificări făcute în timpul aplicării semnăturii olografe; în acest fel, utilizatorul care urmează să semneze cu tableta grafică va vedea pe afișaj nu numai secțiunea corespunzătoare zonei selectate, ci și indicațiile introduse manual de operator.

Figura 20 - Fundal pentru semnătură

Pentru a modifica fundalul, trebuie să accesați proprietatea câmpului de semnătură salvată, dând clic pe pictograma corespunzătoare (imaginea din stânga), apoi să vă deplasați la eticheta Background (Fundal).

Apăsați butonul Save (Salvare) pentru a salva imaginea în format .bmp. În acest moment va fi posibil să editați fișierul cu un editor grafic sau să utilizați unul deja prezent în sistemul de operare, cum ar fi Paint. Odată ce modificările au fost finalizate, pur și simplu recuperați imaginea din interiorul câmpului de semnătură folosind butonul Open (Deschidere) (imaginea din partea stângă) și, în cele din urmă, apăsați OK pentru a confirma operațiunea.

Se recomandă cu fermitate salvarea fișierului bitmap al unui șablon în același folder, deoarece, după modificare, acesta poate fi actualizat în șablon cu funcția Update signature backgrounds (Actualizare fundaluri semnătură).

Don't use background for the signature (Nu se utilizează fundal pentru semnătură)
Fundalul salvat nu va fi afișat pe ecranul tabletei în timpul aplicării semnăturii originale

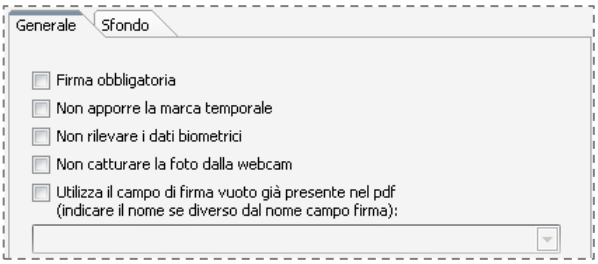


Figura 21 - General (Generalități) Signature Properties (Proprietăți semnătură)

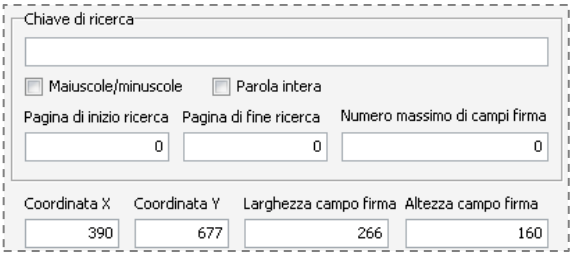
În secțiunea General (Generalități) din Signature Properties (Proprietăți semnătură) sunt incluse următoarele opțiuni:

Obligatory Signature (Semnătură obligatorie)
Obligă utilizatorul să deseneze o semnătură originală pe tabletă în câmpul selectat, fără a permite posibilitatea de a trece la câmpul următor sau de a salva documentul.

Don't put the timestamp (Nu se aplică marcajul temporal)
Prin intermediul software-ului FirmaCerta este, de asemenea, posibil să aplicați marcajul temporal pe întregul document sau pentru semnăturile individuale incluse în acesta; prin bifarea casetei de selectare specifice va fi posibil să nu aplicați niciun marcaj temporal pe câmpul de semnătură selectat.

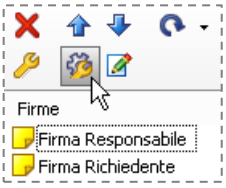
Don’t detect biometric data (Nu se detectează date biometrice)
Această caracteristică împiedică detectarea din semnătură a datelor semnatarului, prin achiziționarea doar a semnăturii grafice.

Don’t capture pictures from webcam (Nu se capturează imagini de la camera web)
Această funcție poate fi setată în cazul în care computerul nu este echipat cu o cameră web sau nu este necesară capturarea imaginii solicitantului în cauză (în cazurile în care aceasta ar fi criptată în interiorul documentului)



Search key (Cuvânt cheie de căutare)
Prin introducerea unui cuvânt prezent în documentul pe care doriți să îl semnați sau prin specificarea coordonatelor exacte puteți crea câmpuri de semnătură fără alți parametri, care se vor afișa pentru semnatar în timpul procedurii de semnare. De exemplu, această funcție ar fi extrem de utilă la aplicarea unei etichete cu un titlu pe un model .PDF folosit ca șablon pentru altul

Figura 22 - Cuvinte cheie de căutare



Această caracteristică vă permite să extindeți două preferințe importante (descrise mai sus) în toate câmpurile de semnătură salvate în șablon:

- Don’t use background for the signature (Nu se utilizează fundal pentru semnătură)
- Don’t capture pictures from webcam (Nu se capturează imagini de la camera web)

4.3 UTILITY (UTILITAR)

Această caracteristică îi permite utilizatorului să acceseze setările principale ale software-ului Firmacerta.

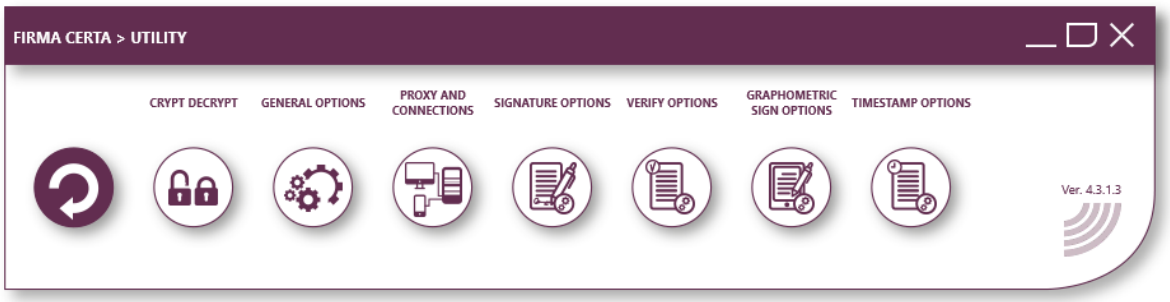


Figura 23 - Panoul Utility (Utilitar)

4.3.1 ENCRYPT AND DECRYPT (CRIPTARE ȘI DECRIPTARE)

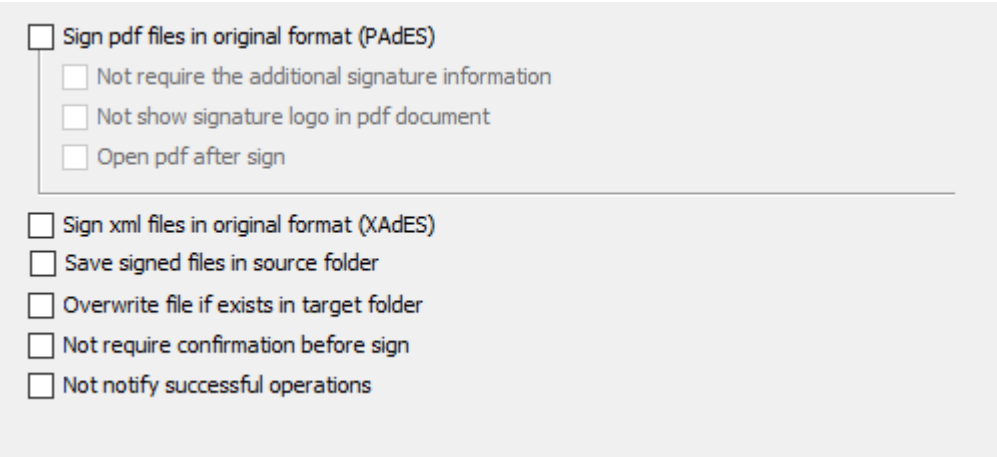
Aceasta este o aplicație utilă pentru criptarea fișierelor de toate tipurile și dimensiunile, în conformitate cu reglementările actuale și referințele normativelor tehnice.
Foarte adaptabilă și ușor de utilizat, Firma Certa Protect este disponibilă pentru Windows.
Pentru a utiliza Firma Certa Protect, consultați **ghidul** pentru a găsi informațiile de bază (consultați Anexa D).

Figura 24 - Accesarea aplicației FirmaCerta Protect

4.3.2 GENERAL OPTIONS (OPȚIUNI GENERALE)

În această secțiune puteți gestiona setările software-ului Firmacerta.
Atenție: folosind săgețile pe care le puteți găsi în colțul din dreapta sus puteți răsfoi diferite profiluri.

Puteți efectua câteva operațiuni pentru personalizarea semnăturii.



Signature of pdf files maintaining the format (PAdES) (Semnarea fișierelor PDF cu păstrarea formatului (PAdES)):	Păstrează formatul fișierului original (în caz contrar, convertit în format .p7m), oferind posibilitatea de a vizualiza documente chiar și pentru un utilizator care nu deține un software specific de semnare digitală.
• **Do not request additional signature information (Nu se solicită informații suplimentare despre semnătură):**	Informațiile opționale nu vor fi afișate în documentul semnat;
• **Do not show the signature logo in PDF documents (Nu se afișează logotipul semnăturii în documente PDF):**	Dacă setați această preferință înainte de semnare și apoi vizualizați fișierul PDF semnat digital, logotipul semnăturii cu informațiile semnatarului nu va fi raportat. **NB:** Puteți personaliza logotipul prin intermediul setării corespunzătoare, **Logo pdf** (Logotip pdf); în lipsa acestui tip de personalizare, software-ul va utiliza un logotip în mod implicit
• **Open the PDF after the signing process (Se deschide fișierul PDF după procesul de semnare)**	Fișierul PDF va fi deschis cu programul implicit al computerului după aplicarea semnăturii digitale.
Signature of xml files maintaining the original format (XAdES) (Semnarea fișierelor XML cu păstrarea formatului original (XAdES)):	Păstrează formatul fișierului original, oferind posibilitatea de a vizualiza documentul chiar și pentru un utilizator care nu deține un software specific de semnare digitală.
Save signed files in the same folder of the original file (Se salvează fișierele semnate în același folder cu fișierul original):	Permite salvarea fișierului semnat în același director în care se află și fișierul original;
Overwrite files if already existing in the destination folder (Fișierele se suprascriu dacă există deja în folderul de destinație):	Mesajul care informează cu privire la prezența fișierului original va fi ignorat;
Do not ask any confirmation before signing a file (Nu se solicită confirmarea înainte de semnarea unui fișier):	Omite solicitarea confirmării ori de câte ori semnatarul aplică o semnătură pe document.
Do not notify the successful outcome of the operations (Nu se anunță rezultatul reușit al operațiunilor):	Mesajul de succes de la sfârșitul procedurii nu va fi afișat.

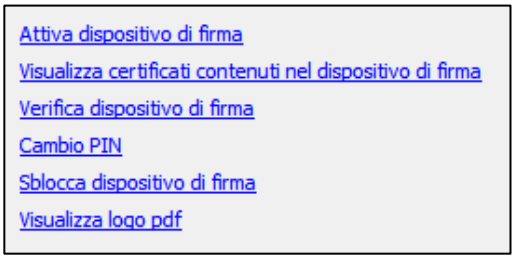


Figura 25 - Panoul General Options (Opțiuni generale)

4.3.2.1 GESTIONAREA FIȘIERELOR

Următoarele opțiuni vă oferă aceste posibilități:

- utilizați Firma Certa ca program implicit pentru a deschide fișiere semnate digital (.p7m), fișiere marcate temporal (.tsd, .tsr, .tst) și fișiere protejate (.p7e).
- codificați fișiere semnate digital (.p7m), fișiere marcate temporal (.tsd, .tsr, .tst) și fișiere protejate (.p7e) în format Base64.
- Creați fișierul care conține marcajul unui fișier marcat temporal.

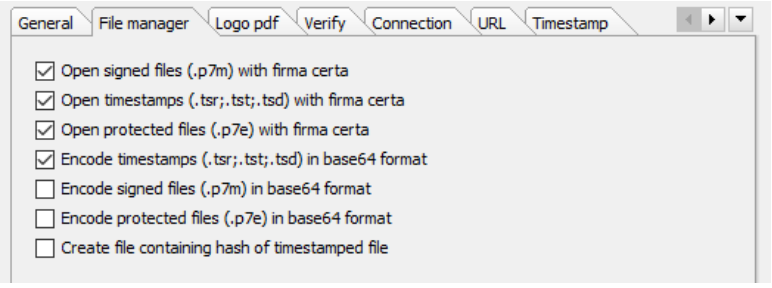


Figura 26 - Opțiuni: Gestionarea fișierelor

4.3.2.2 ADRESA URL

Afișează adresa la care se conectează software-ul pentru a descărca actualizări (se recomandă cu fermitate să nu modificați datele implicite).

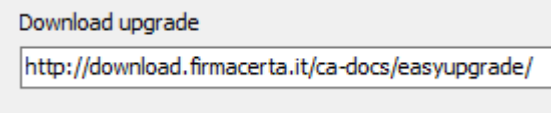


Figura 27 - Opțiuni: Adresa URL

4.3.2.3 SERVICII WEB

În această secțiune puteți activa pluginul pentru a utiliza serviciul Remote Signature (Semnătură la distanță), prin selectarea serviciul și dând clic pe Enabled/Disabled (Activat/Dezactivat).

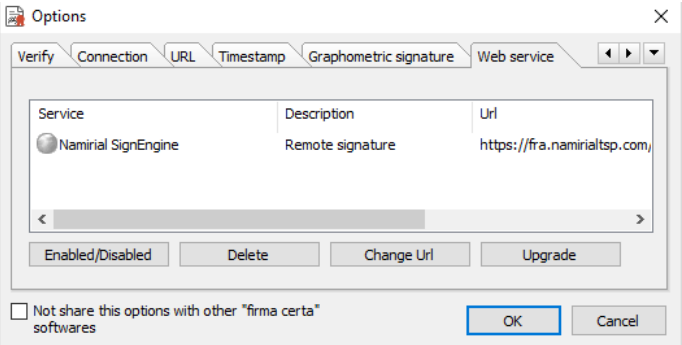


Figura 28 - Opțiuni servicii web

4.3.2.4 INFORMATION (INFORMAȚII)

Secțiune în care puteți verifica informațiile Firmacerta, cum ar fi ultima versiune de software, configurarea limbii etc.

Atenție: vă recomandăm cu fermitate să mențineți software-ul la zi, pentru a asigura conformitatea cu reglementările și îmbunătățirile.

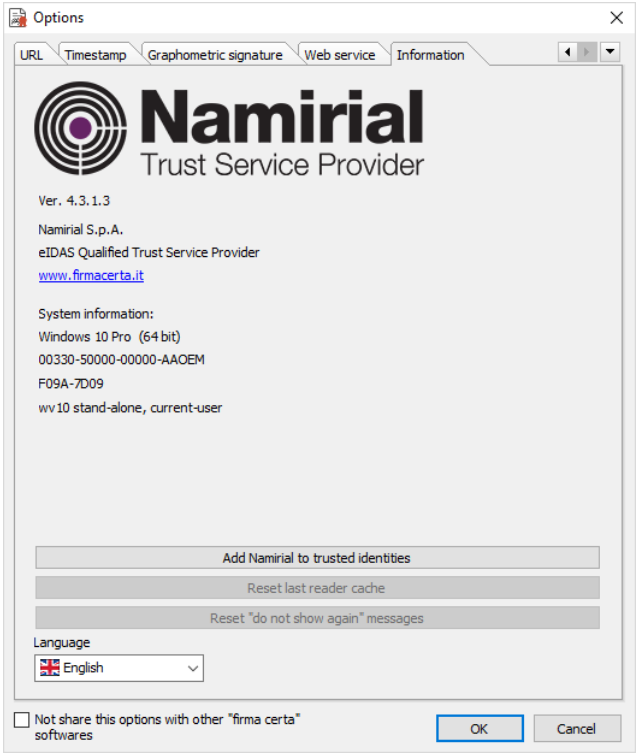


Figura 29 - Opțiuni Information (Informații)

4.3.3 PROXY ȘI CONEXIUNI

Această caracteristică trebuie utilizată numai dacă accesul la internet pentru protocolul HTTP este accesibil prin server proxy. Sistemul permite setarea numelui, a portului pentru asocierea la web, precum și a ID-ului și parolei pentru accesul la internet ale unui utilizator FirmaCerta.

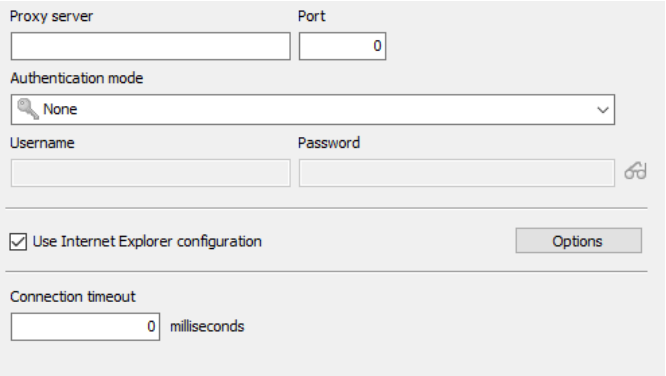


Figura 30 - Opțiuni: Configurarea proxy

4.3.4 SIGNATURE OPTIONS (OPȚIUNI DE SEMNARE)

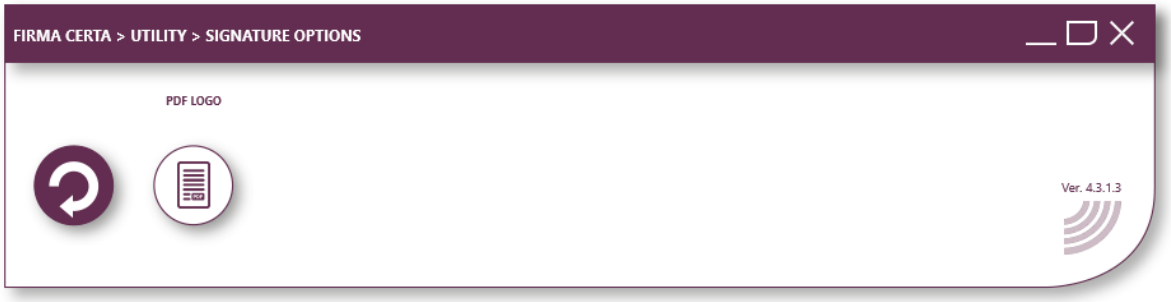


Figura 31 - Panoul Signature Options (Opțiuni de semnare)

4.3.4.1 PDF LOGO (LOGOTIP PDF)

Vă permite să schimbați logotipul implicit al Namirial și să configurați un logotip personal într-un document PDF, în timpul aplicării semnăturii în acest tip de document.
Puteți seta efectul de transparență prin selectarea a două culori diferite, personalizați textul care urmează să fie aplicat peste logotip, încorporați fontul în sistemul de operare pentru o compatibilitate mai bună cu PDF/A.

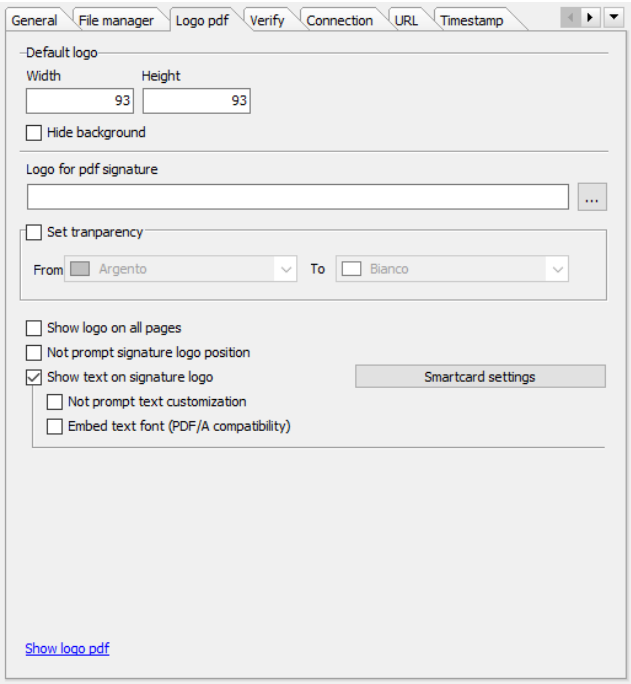


Figura 32 - Opțiuni: PDF Logo (Logotip PDF)

4.3.5 VERIFY (VERIFICARE)

Pentru a verifica și a afișa simultan starea certificatului (active (activ)/revoked (revocat)/suspended (suspendat)) a unui fișier semnat digital.

Figura 33 - Opțiuni: Opțiuni de verificare

4.3.6 GRAPHOMETRIC SIGNATURE OPTIONS (OPȚIUNI DE SEMNARE GRAFOMETRICĂ)

Această caracteristică îi permite utilizatorului să acceseze Utilitarele numite dispozitive de semnare grafometrică.

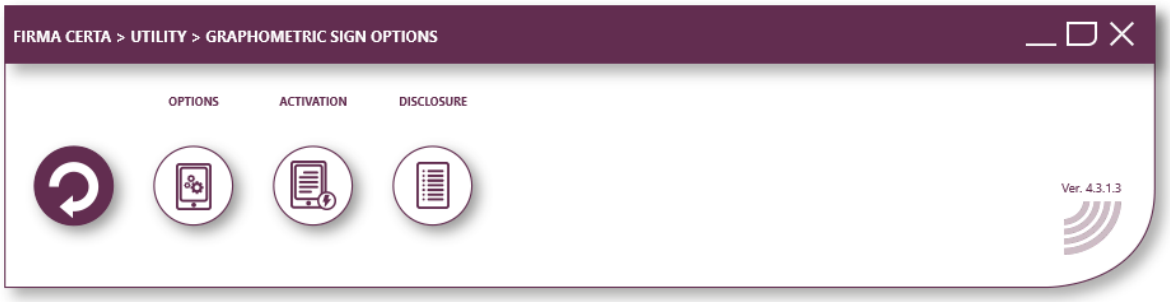


Figura 34 - Panoul Graphometric Signature Options (Opțiuni de semnare grafometrică)

4.3.6.1 OPTIONS (OPȚIUNI)

În cadrul preferințelor de semnare grafometrică puteți utiliza unul dintre cele trei modele de tablete Wacom din meniul vertical și, alternativ, una dintre tabletele certificate pentru această operațiune (pentru mai multe informații vizitați www.firmagrafometrica.it, secțiunea „Dispositivi Utilizzabili" (Dispozitive utilizabile)).

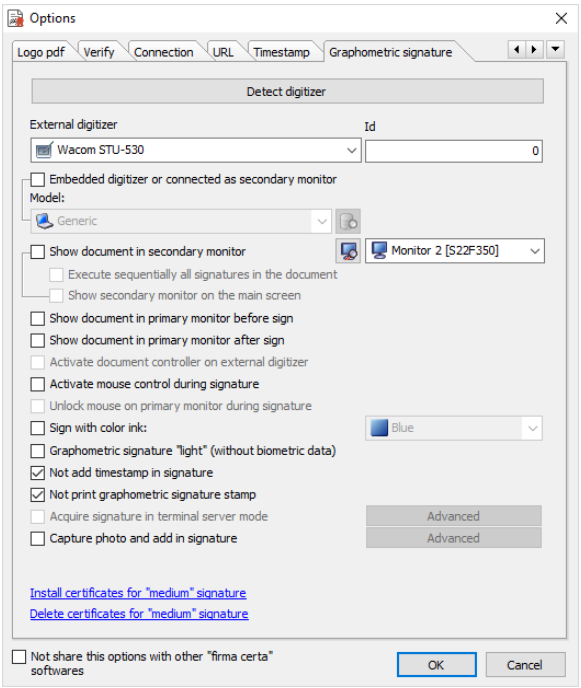


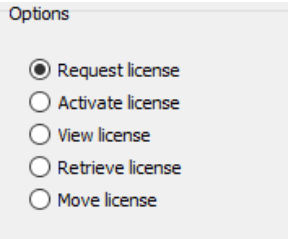
Figura 35 - (Opțiuni) Graphometric Signature (Semnătură grafometrică)

4.3.6.2 ACTIVAREA

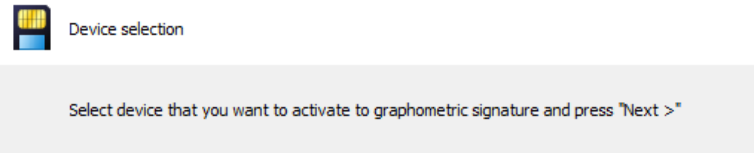
Utilizatorul care dorește să activeze software-ul primește prin poștă un certificat tehnic de criptare care trebuie instalat pe computer.
Acest certificat este obligatoriu pentru activarea licenței de semnare grafometrică.

Pentru a solicita activarea funcției de semnare grafometrică, procedați după cum urmează:

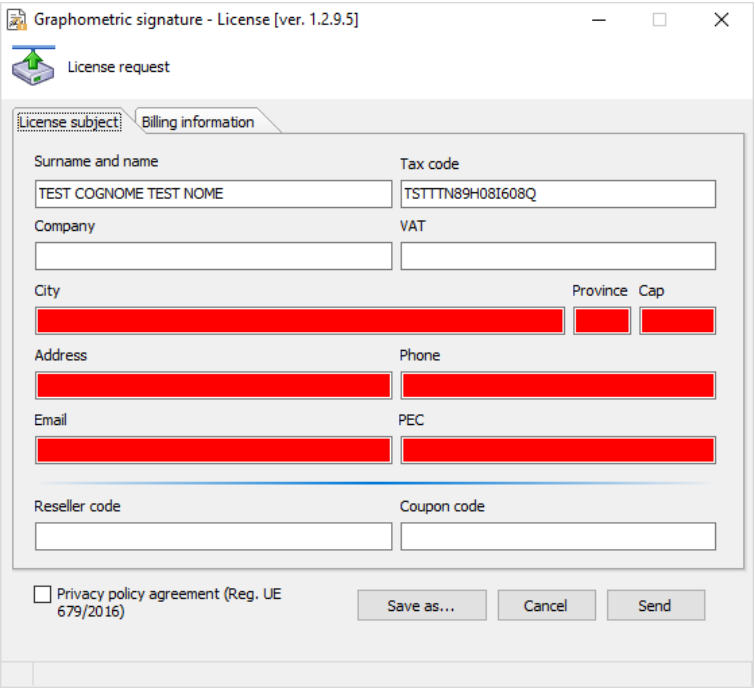
Selectați opțiunea Request License (Solicitare licență) și apăsați pe **Next** (Înainte);



Apăsați pe **Next** (Înainte);



Completați câmpurile cu datele posesorului licenței și apăsați pe **Send** (Trimitere).



La sfârșitul procedurii, CA Namirial va procesa cererea și în câteva ore va activa dispozitivul digital pentru semnătura biometrică.

Figura 36 - Opțiuni grafometrice: Activarea licenței

4.3.6.3 INFORMAȚII

Funcția îi permite semnatarului compilarea, elaborarea și semnarea cu semnătura grafometrică a unui document PDF informativ despre funcționarea generală a semnăturii grafometrice și prelucrarea documentelor electronice în locul celor pe hârtie, utilizând un dispozitiv digital conectat (tabletă grafică sau alt hardware acceptat). Pentru a efectua operațiunea, solicitantului i se va cere, după introducerea Tax code (Cod fiscal) și Name (Nume) într-o fereastră inițială (fig. din dreapta), să utilizeze procedurile aplicate semnăturii grafometrice și să înscrie data și semnătura pe dispozitiv. Dacă nu permiteți utilizarea acestui proces prin accesarea acestui meniu, acest tip de cerere se va afișa pentru semnatar în timpul primei operațiuni de semnare.

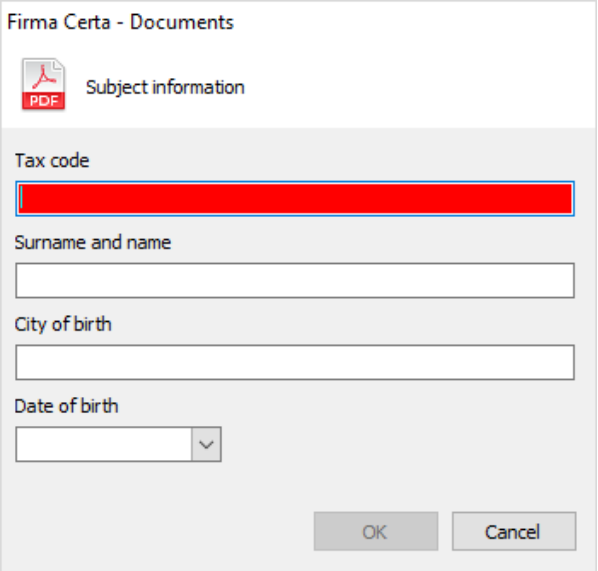
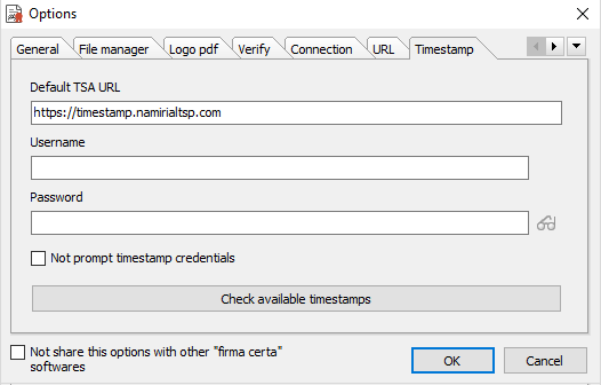


Figura 37 - Opțiuni grafometrice: Confidențialitatea informațiilor

4.3.7 OPTIONS (OPȚIUNI) TIMESTAMP (MARCAJ TEMPORAL)

Această secțiune permite salvarea acreditărilor Username (Nume de utilizator) și Password (Parolă) pentru a utiliza marcajele temporale (dacă posesorul le deține) fără a le introduce de fiecare dată când utilizatorul dorește să utilizeze un marcaj temporal.

Dacă dați clic pe **Check Available timestamps** (Se verifică marcajele temporale disponibile), puteți verifica numărul de marcaje temporale rămase.



LINK către serviciul de marcare temporală

https://timestamp.namirialtsp.com
http://timestamp.namirialtsp.com

Figura 38 - Options (Opțiuni) Time Stamp (Marcaj temporal)

4.4 HELP (AJUTOR)

Secțiunea în care puteți găsi Ghidul utilizatorului software-ului, puteți verifica manual actualizările disponibile dând clic pe **Check Upgrade** (Verificare upgrade).

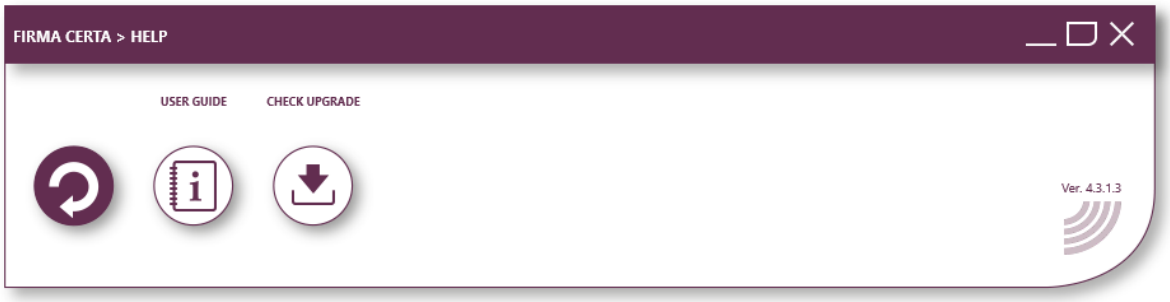


Figura 39 - Panoul: Help (Ajutor)

Figura 39: Panoul: Help (Ajutor)

5 ANEXA A: MODUL DE SEMNARE ȘI CONTRASEMNARE

5.1 MODUL DE SEMNARE A UNUI DOCUMENT

Selectați fișierul de semnat și dați clic pe **Sign** (Semnare).

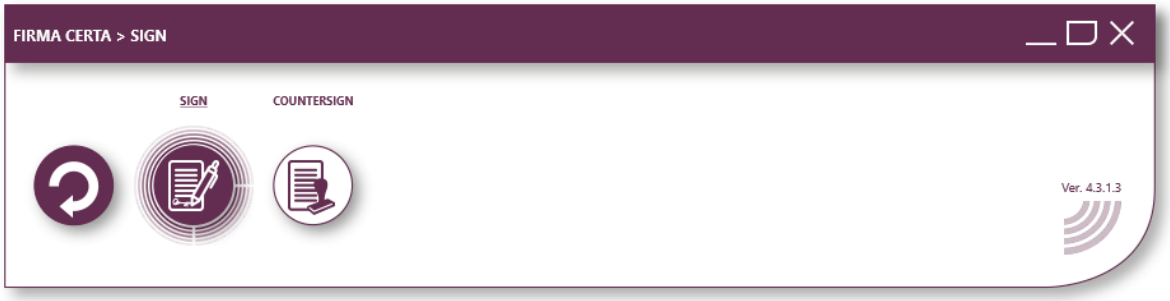


Figura 40 - Panoul Sign (Semnare)

Atenție: Software-ul Firmacerta permite semnarea oricărui tip de fișier în format CAdES.p7m, dar numai pentru fișierele PDF sau XML software-ul îi va solicita utilizatorului să aleagă dacă dorește să semneze în .p7m sau să păstreze formatul original.

5.1.1 SEMNAREA ÎN CADES - XADES

După ce dați clic pe „Sign" (Semnare), se va deschide o fereastră pentru a vă solicita formatul de semnare a documentului.

- Apăsați Yes (Da) pentru o semnătură XAdES, păstrând formatul .xml (valabil numai pentru fișierele XML)
- Apăsați No (Nu) pentru o semnătură CAdES într-un format .p7m

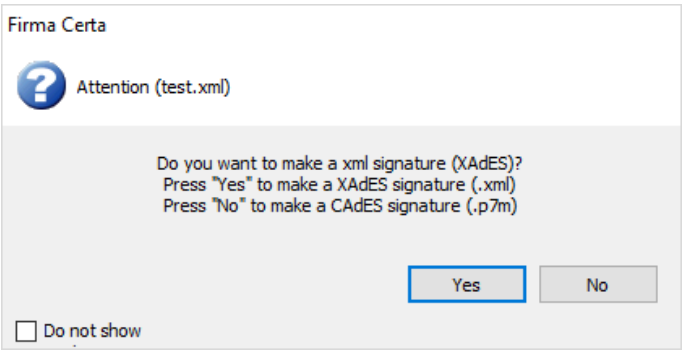


Figura 41 - Selectarea formatului de semnătură Cades-XAdES

Selectați folderul de destinație al fișierului semnat, apoi dați clic pe OK.

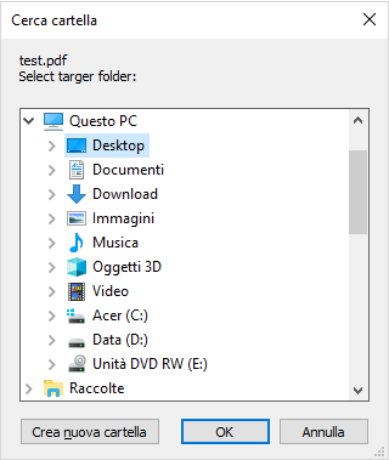


Figura 42 - Selectați folderul de destinație

Continuați operațiunea de semnare, prin apăsare pe Yes (Da).

Atenție: Vă recomandăm să creați un folder specific pentru fișierul semnat digital, pentru a evita problemele.

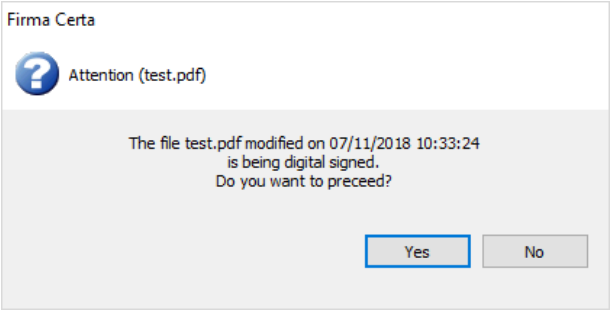


Figura 43 - Confirmarea semnăturii

Introduceți codul PIN al dispozitivului de semnare digitală și dați clic pe OK.

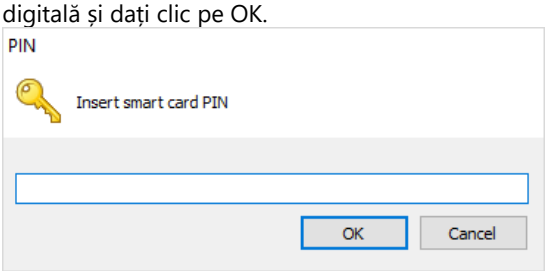


Figura 44 - Introducerea codului PIN

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.

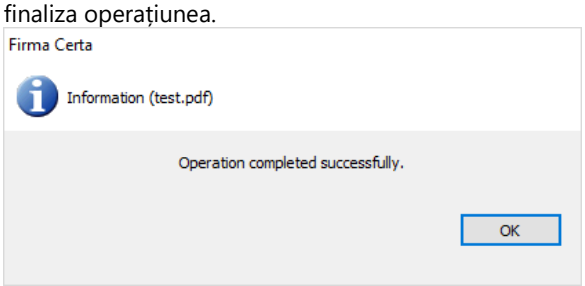


Figura 45 - Operation completed (Operațiunea a fost finalizată)

5.1.2 SEMNAREA ÎN PADES

După ce dați clic pe „Sign" (Semnare), se va deschide o fereastră pentru a vă solicita formatul de semnare a documentului.

- Apăsați Yes (Da) pentru o semnătură PAdES, păstrând formatul .pdf (valabil numai pentru fișierele PDF)

- Apăsați No (Nu) pentru o semnătură CAdES într-un format .p7m

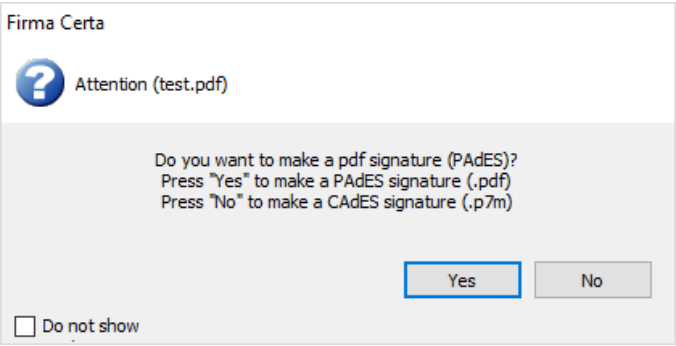


Figura 46 - Selectarea formatului de semnătură Cades-Pades

Selectați folderul de destinație al fișierului semnat, apoi dați clic pe OK.

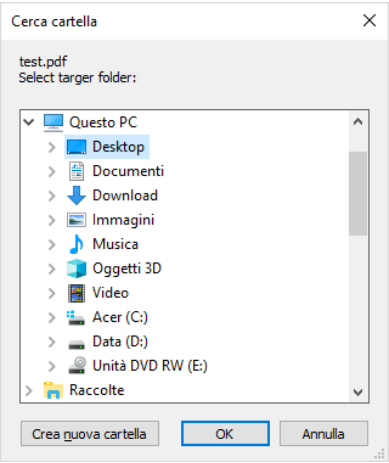


Figura 47: Selectați folderul de destinație

Introduceți codul PIN al dispozitivului de semnare digitală și dați clic pe OK.

Continuați operațiunea de semnare, prin apăsare pe Yes (Da).

NB: Vă recomandăm să creați un folder specific pentru fișierele semnate digital, pentru a evita problemele.

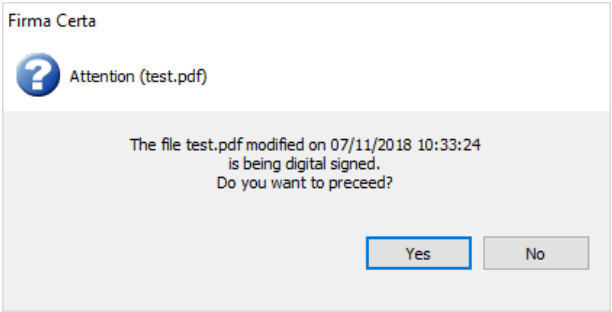


Figura 48: Confirmarea semnăturii

Selectați motivul semnării (opțional).

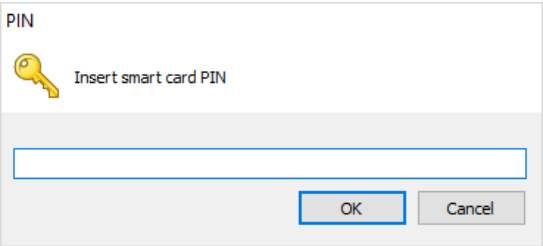


Figura 49: Introducerea codului PIN

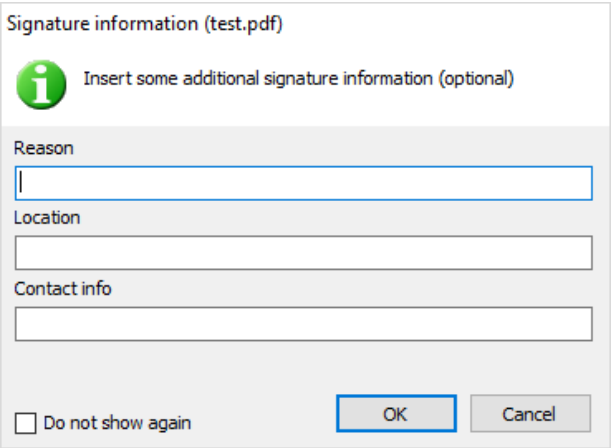


Figura 50: Signature information (Informații despre semnătură)

Selectați poziția logotipului folosind marcatorul verde

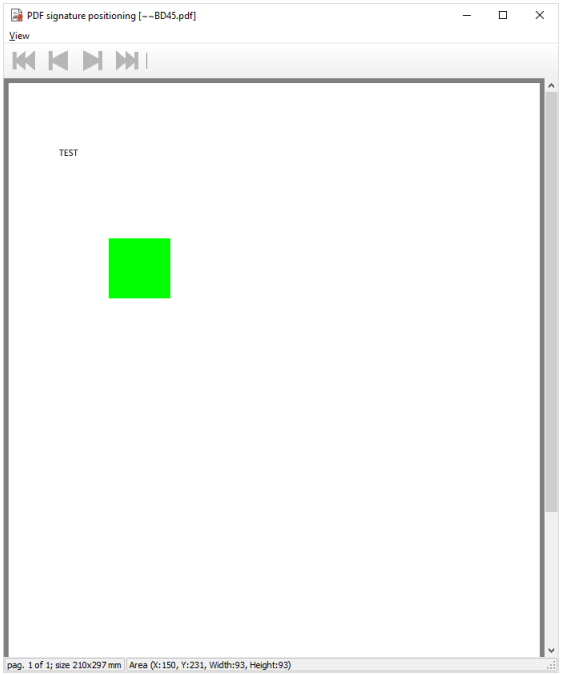


Figura 51: Poziționarea marcatorului de semnare

Pentru a confirma operațiunea, apăsați pe „Yes" (Da).

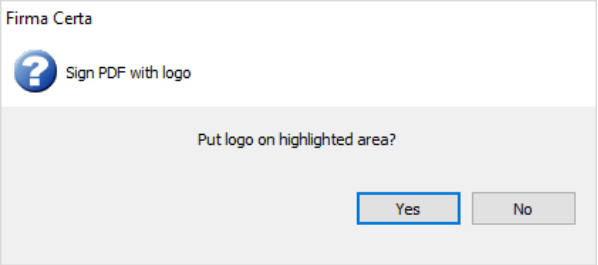


Figura 52: Confirmarea poziționării

Pentru a personaliza logotipul (opțional), apăsați pe OK.

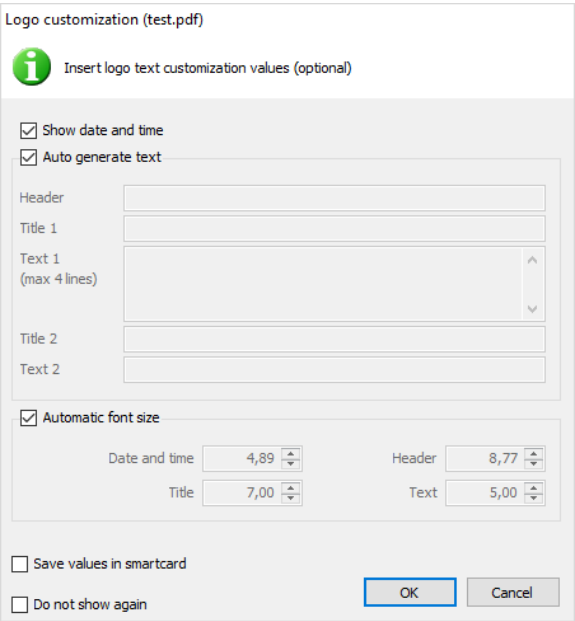


Figura 53: Logotip personalizat

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.

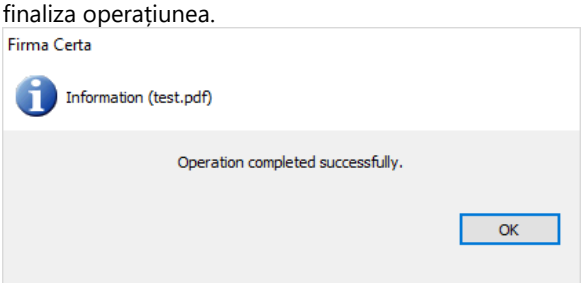


Figura 54: Operation completed (Operațiunea a fost finalizată)

5.2 MODUL DE CONTRASEMNARE

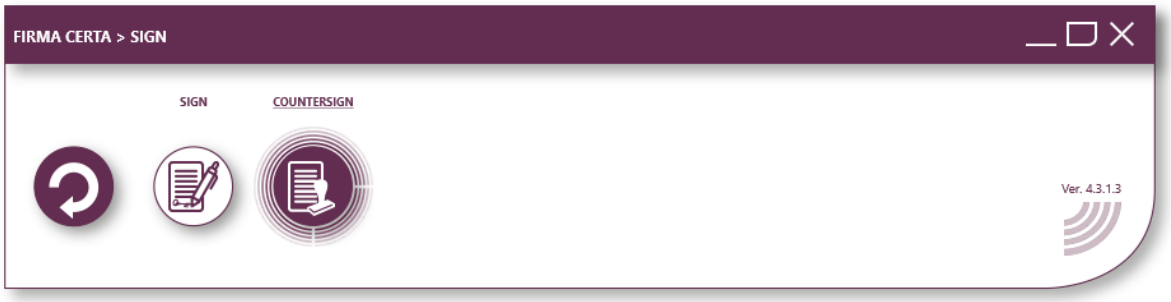


Figura 47 - Panoul Countersign (Contrasemnare)

Cu această funcție este posibilă contrasemnarea unei semnături deja prezente în document, oferindu-i acesteia din urmă un fel de validare ierarhică.

După încărcarea fișierului semnat digital pe care doriți să îl contrasemnați, dați clic pe butonul „Countersign" (Contrasemnare).

ATENȚIE: Puteți contrasemna un fișier semnat digital cu formatul .p7m

Selectați folderul de destinație al fișierului semnat, apoi dați clic pe OK.

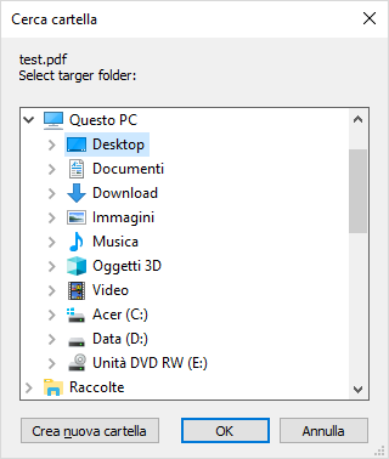


Figura 48 - Selectați folderul de destinație

Confirmați dacă doriți să suprascrieți fișierul existent și dați clic pe Yes (Da).

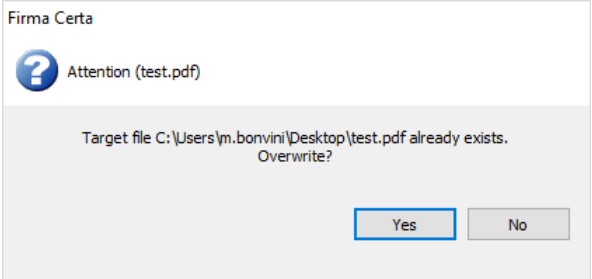


Figura 49 - Confirmarea suprascrierii

Selectați semnătura pe care doriți să o contrasemnați și dați clic pe OK.

Exemplu: În imaginea următoare, utilizatorul TEST COGNOME TEST NOME 2 contrasemnează semnătura utilizatorului TEST COGNOME TEST NOME 1

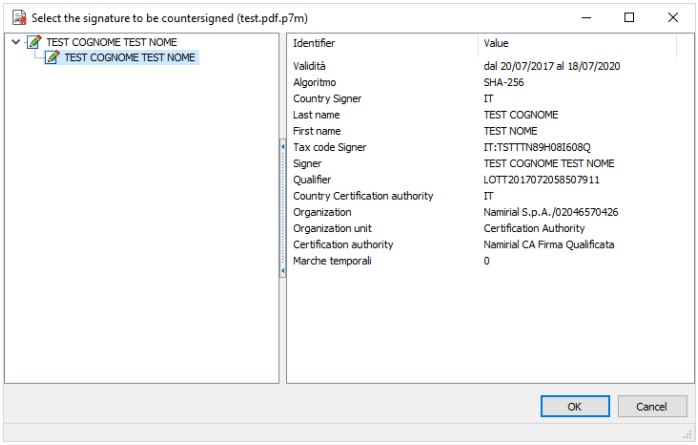


Figura 50 - Ecran exemplificativ: verificarea fișierului contrasemnat

Continuați operațiunea de semnare, prin apăsare pe Yes (Da).

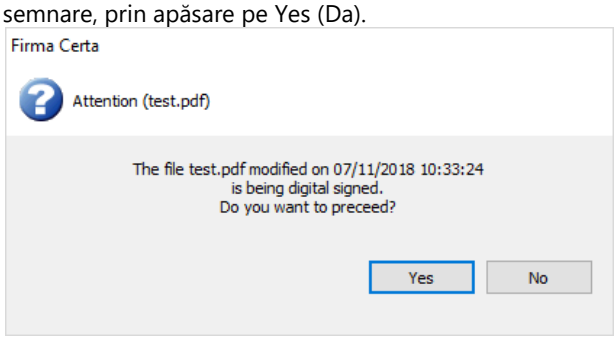


Figura 51 - Confirmarea semnăturii

Introduceți codul PIN al dispozitivului de semnare digitală și dați clic pe OK.

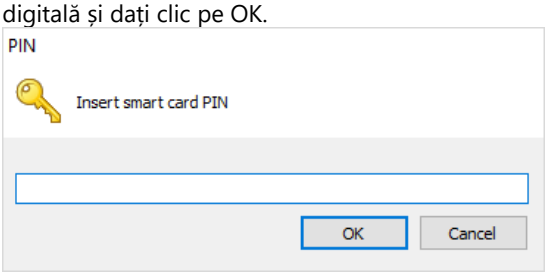


Figura 52 - Introducerea codului PIN

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.

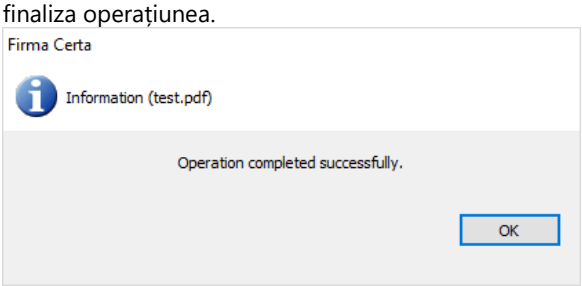


Figura 53 - Operation completed (Operațiunea a fost finalizată)

6 ANEXA B: MODUL DE MARCARE TEMPORALĂ A UNUI FIȘIER

Înainte de a utiliza serviciul Timestamp (Marcare temporală), trebuie să configurați software-ul FirmaCerta.

ATENȚIE: Semnătura digitală nu include serviciul de marcare temporală. Marcajele temporale pot fi achiziționate din Magazinul nostru.
Pentru a configura marcajul temporal, deschideți FirmaCerta Software > Utility > Timestamp Options (Software FirmaCerta > Utilitar > Opțiuni de marcare temporală)

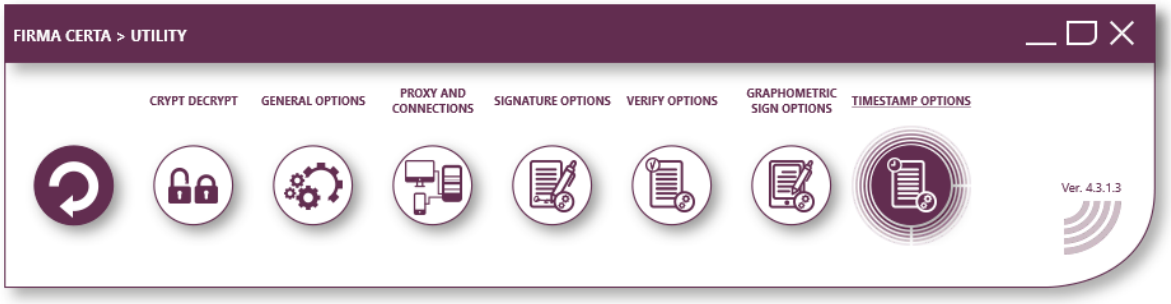


Figura 54 - Panoul Utility (Utilitar)

6.1 CONFIGURAREA PARAMETRILOR DE MARCARE TEMPORALĂ

Din meniul **Utility** (Utilitar) ->**opțiunea Timestamp (Marcaj temporal)**

- Verificați dacă adresa URL este http://timestamp.namirialtsp.com sau https://timestamp.namirialtsp.com
- Introduceți Username (Nume de utilizator) și Password (Parolă), apoi dați clic pe OK.

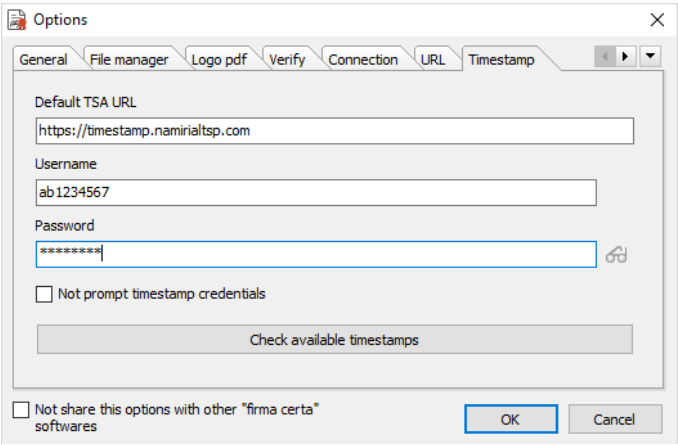


Figura 55 - Opțiuni de configurare a marcajului temporal

ATENȚIE:

- Dacă dați clic pe pictograma din dreptul câmpului Password (Parolă), este posibil să vizualizați clar parola pe care o introduceți.
- În cazul pierderii acreditărilor pentru marcajul temporal, utilizatorul le poate solicita prin trimiterea unui PEC (e-mail certificat) la firmacerta@sicurezzapostale.it sau un e-mail la helpdesk@firmacerta.it, cu specificarea numelui de utilizator și/sau a codului fiscal.

Funcția **Check Available Timestamp** (Se verifică marcajele temporale disponibile) verifică marcajele temporale rămase (în cazul în care interogarea eșuează, trebuie să verificați introducerea corectă a acreditărilor)

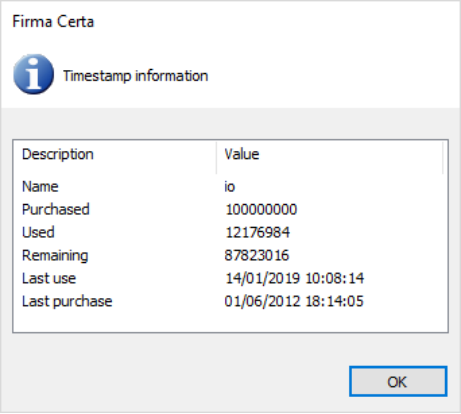


Figura 56 - Verificarea marcajelor temporale

6.2 MODUL DE SEMNARE ȘI APLICARE A MARCAJULUI TEMPORAL

După selectarea unui fișier, puteți alege această funcție pentru a semna și a marca temporal, într-o sesiune unică. Fișierul semnat și marcat temporal va fi în format CADES-T (fișier marcat temporal .pdf.P7M).
În formatul CADES-T (formatul implicit), marcajul temporal este asociat unei singure semnături și *NU poate fi separat*.

Pentru semnare și aplicarea marcajului temporal, parcurgeți următorii pași:

- Selectați Sign and Timestamp (Semnare și aplicarea marcajului temporal) în software,

Selectați folderul de destinație al fișierului semnat, apoi dați clic pe OK.

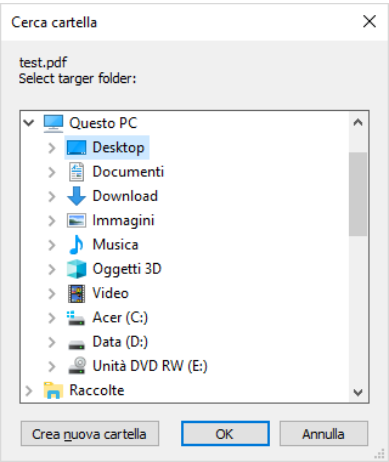


Figura 57 - Selectați folderul de destinație

Continuați operațiunea de semnare, prin apăsare pe „Yes" (Da).

NB: Vă recomandăm să creați un folder specific pentru fișiere, pentru a evita problemele.

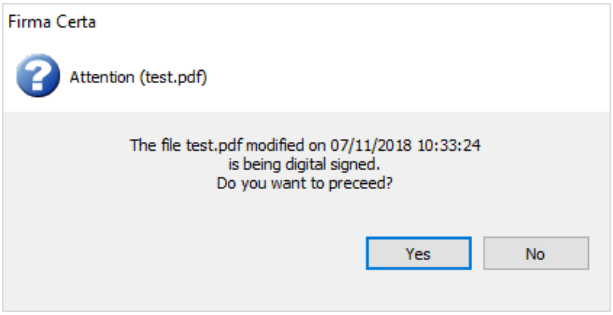


Figura 58 - Confirmarea semnăturii

Introduceți codul PIN al dispozitivului de semnare digitală, apoi dați clic pe „OK".

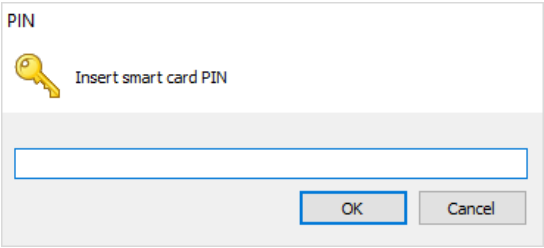


Figura 59 - Introducerea codului PIN

Confirmați aplicarea marcajului temporal, apoi dați clic pe OK.

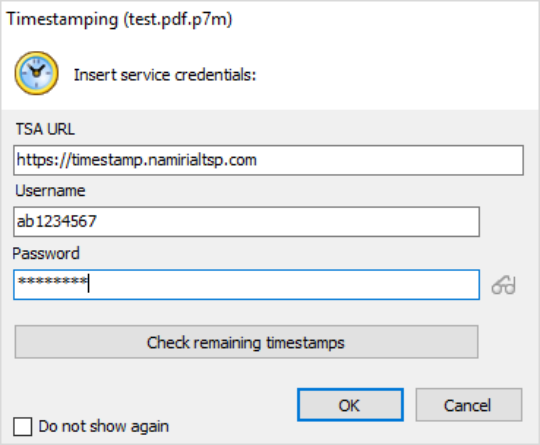


Figura 60 - Confirmarea acreditărilor introduse pentru marcajul temporal

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.

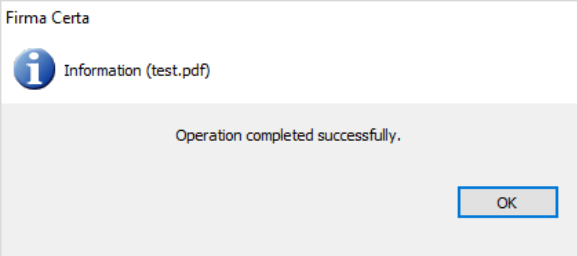


Figura 61 - Operation completed (Operațiunea a fost finalizată)

6.3 MODUL DE SEPARARE A MARCAJULUI TEMPORAL

Această caracteristică îi permite utilizatorului să separe marcajul temporal dintr-un fișier într-un format .TSD (timestamped-date).
ATENȚIE: *puteți face această operațiune doar pentru fișierele semnate în .p7m*

6.3.1 MODUL DE SEMNARE A UNUI FIȘIER ÎN .P7M

Încărcați fișierul care va fi semnat și dați clic pe „Sign" (Semnare).

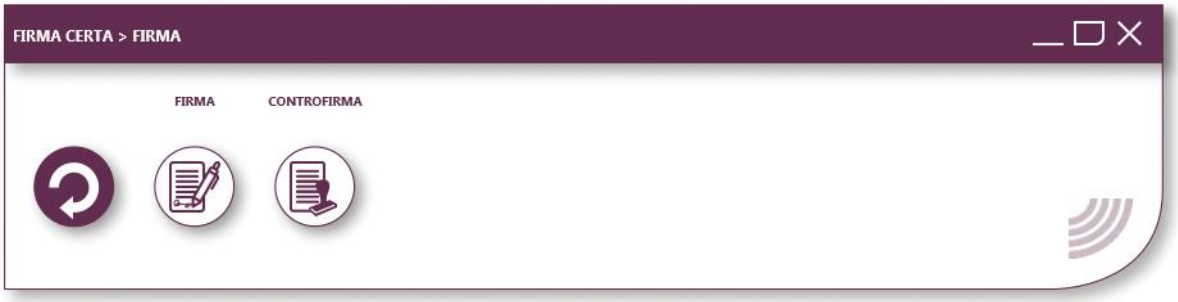


Figura 62 - Tablou de bord pentru semnare

ATENȚIE: Software-ul Firmacerta permite semnarea oricărui tip de fișier în format CAdES, numit și .p7m.
Numai pentru fișierele PDF sau XML software-ul îi va solicita utilizatorului să aleagă dacă dorește să semneze în .p7m sau să păstreze formatul original.

După ce dați clic pe Sign (Semnare), software-ul va deschide o fereastră pentru a vă întreba în ce format doriți să semnați documentul.
Apăsați **No** (Nu) pentru o semnătură CAdES (format .p7m)

Figura 63 - Selectarea formatului de semnătură Cades

Urmați procedura descrisă în Anexa A: Modul de semnare a unui document.

6.3.2 MODUL DE MARCARE TEMPORALĂ A UNUI FIȘIER .P7M SEMNAT

Încărcați fișierul pentru a semna în software și dați clic pe **Timestamp** (Marcaj temporal).

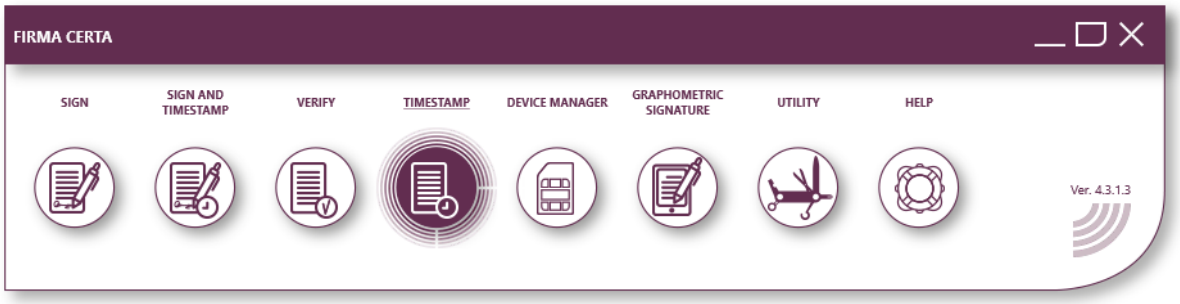


Figura 64 - Panoul Timestamp (Marcaj temporal) FirmaCerta

Selectați formatul .TSD pentru Timestamp (Marcaj temporal).

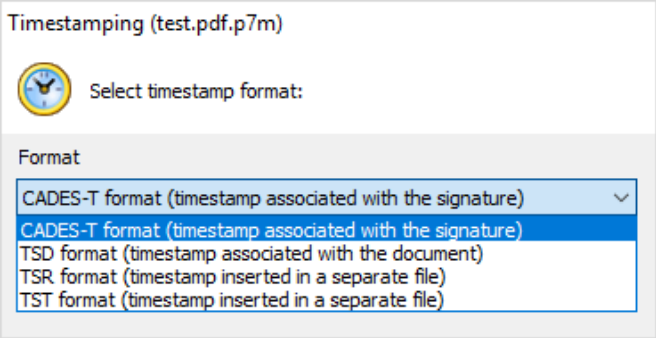


Figura 65 - Selectarea formatului pentru marcaj temporal

Selectați folderul de destinație pentru fișierul semnat, apoi dați clic pe OK.

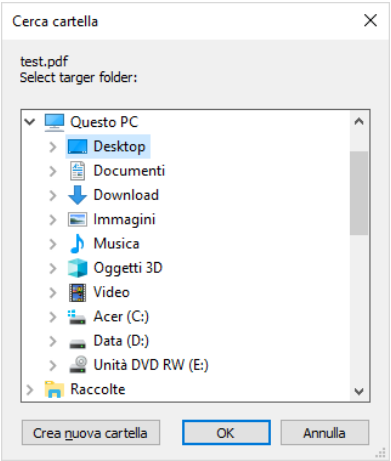


Figura 66 - Selectarea folderului de destinație

Confirmați aplicarea marcajului temporal, apoi dați clic pe OK.

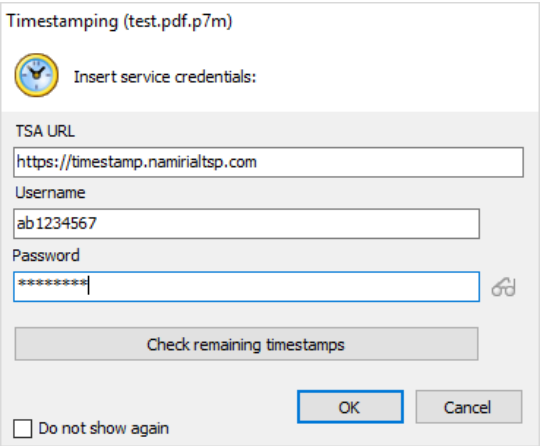


Figura 67 - Confirmarea configurației pentru marcajul temporal

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.

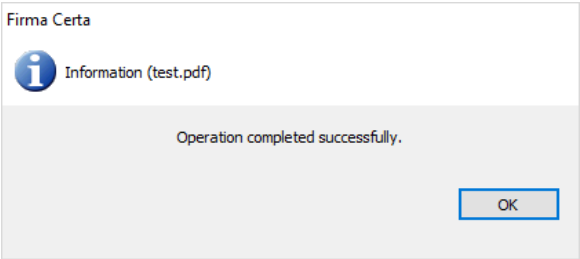


Figura 68 - Operation completed (Operațiunea a fost finalizată)

La sfârșitul operațiunii, software-ul FirmaCerta va crea un fișier nou.

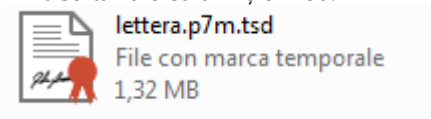


Figura 69 - Exemplu: fișier marcat temporal

6.3.3 SEPARAREA MARCAJULUI TEMPORAL

Încărcați fișierul marcat temporal în software, apoi dați clic pe **Verify** (Verificare).

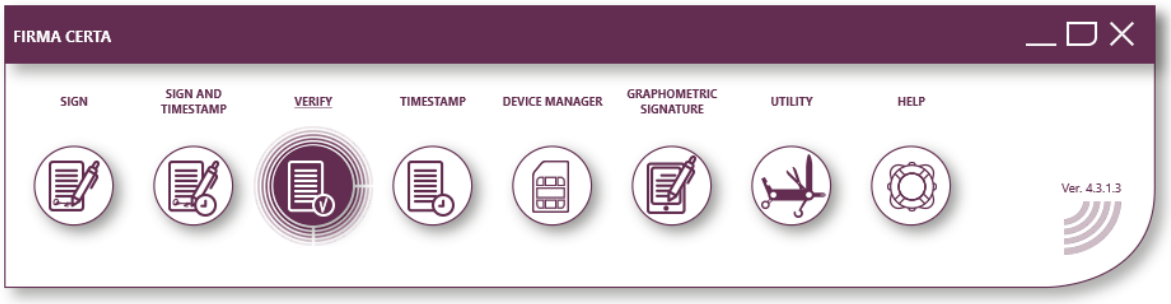


Figura 70 - Panoul Verify (Verificare) FirmaCerta Panel pentru separarea marcajului temporal

În profilul „Verify" (Verificare), selectați Timestamp (Marcaj temporal), iar din meniul Tools (Instrumente) dați clic pe „**Split timestamp și document**" (Separare marcaj temporal și document).

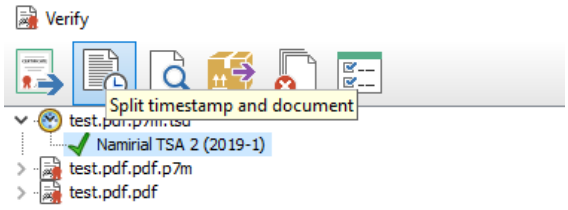


Figura 71 - Separarea marcajului temporal

Selectați formatul dorit al marcajului temporal, .TSR/.TST, apoi apăsați pe OK.

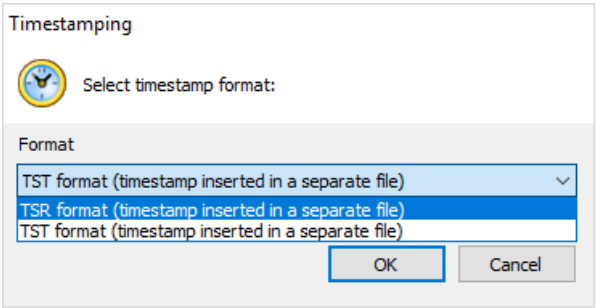


Figura 72 - Selectarea formatului

La sfârșitul operațiunii, utilizatorul va avea două fișiere:

- Un fișier .TSR sau .TST care conține marcajul temporal.
- Un fișier .p7m care conține fișierul semnat digital.

Figura 73 - Exemplu de fișiere marcate temporal

7 ANEXA C: MODUL DE VERIFICARE ȘI VIZUALIZARE A UNUI FIȘIER

Pentru a verifica validitatea unei semnături digitale într-un document, parcurgeți pașii următori:

Încărcați fișierul semnat digital în program și dați clic pe **Verify** (Verificare).

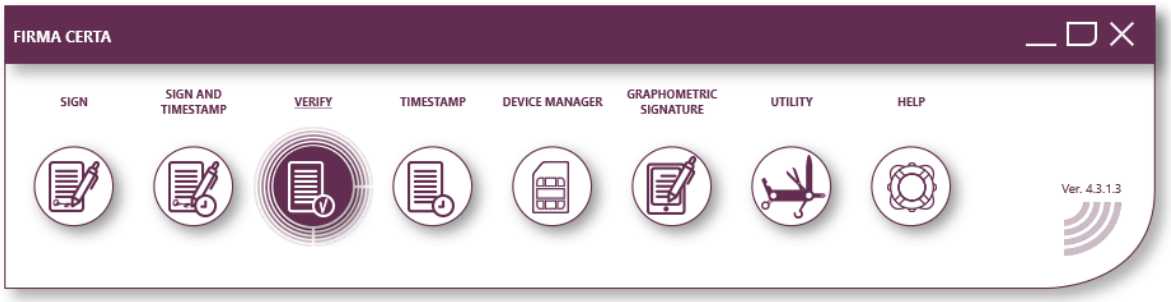


Figura 74 - Panoul Verify (Verificare) FirmaCerta

După ce dați clic pe **Verify** (Verificare) se va deschide o fereastră rezumativă, după cum urmează:

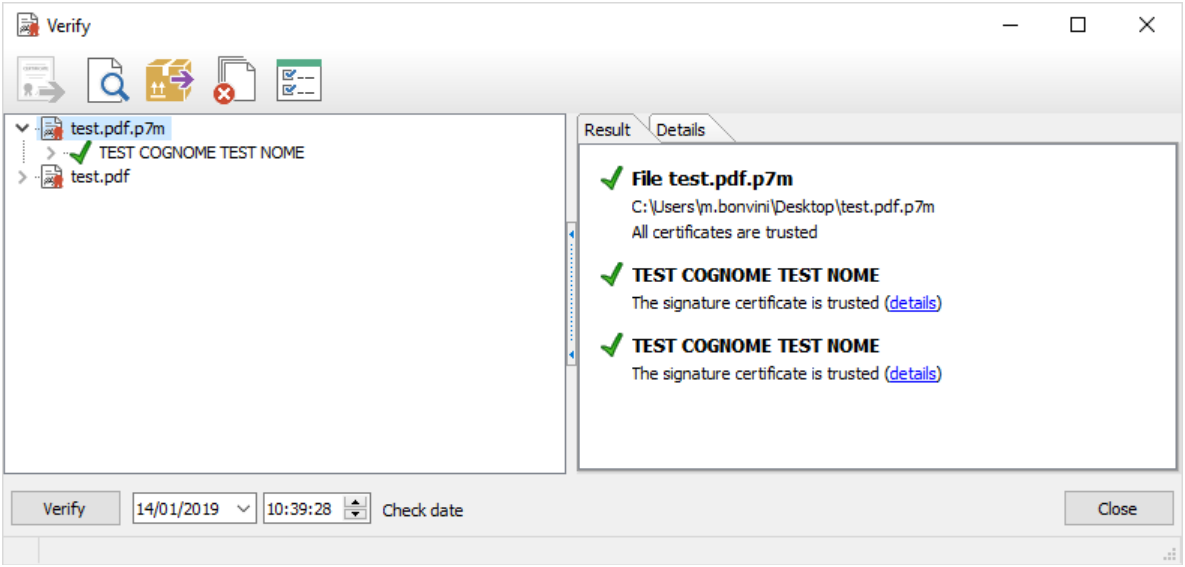


Figura 75 - Ecranul de verificare

ATENȚIE: dacă apare textul „**the certificate has not been verified**" (certificatul nu a fost verificat) înseamnă că verificarea semnăturii nu a fost inițiată automat, deci se recomandă inițierea manuală a verificării, dând clic pe butonul **Verify** (Verificare).
În coloana din stânga este posibil să vizualizați fișierul care a fost semnat digital și persoana care l-a semnat.

Exemplu: În acest caz, fișierul semnat este „test.pdf.p7m" și a fost semnat de doi utilizatori: TEST COGNOME1 și TEST NOME COGNOME2

În coloana din dreapta puteți găsi elementul **Result** (Rezultat) al verificării și **Details** (Detalii) pentru certificat, adică:

- tipul semnăturii și valabilitatea acesteia;
- entitatea care a emis certificatul;
- datele posesorului;

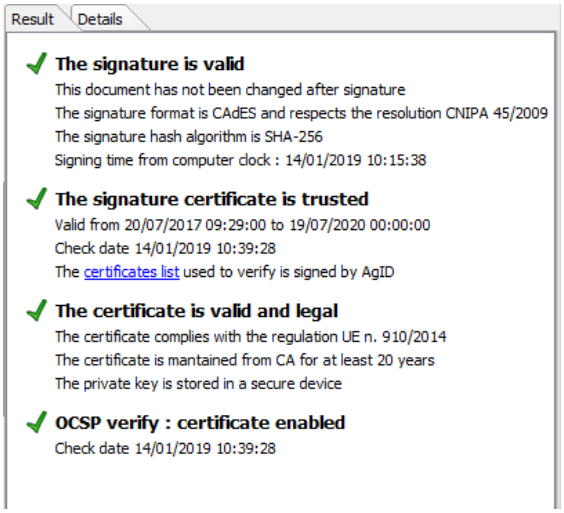


Figura 76 - Ecranul filei Result (Rezultat)

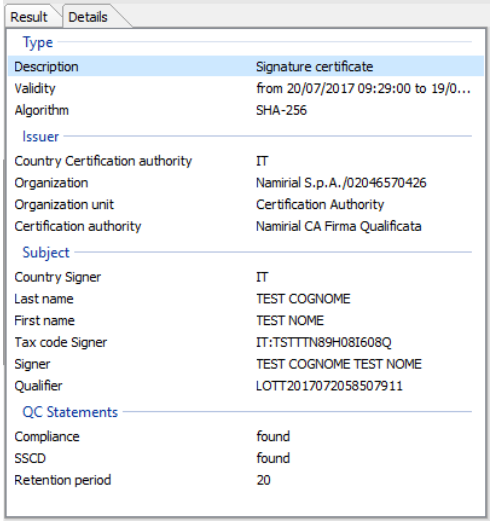


Figura 77 - Ecranul filei Details (Detalii)

7.1 MODUL DE SETARE AUTOMATĂ A LANSĂRII VERIFICĂRII SEMNĂTURILOR

Dați clic pe **Utility -> Verify options** (Utilitar -> Opțiuni Verificare).

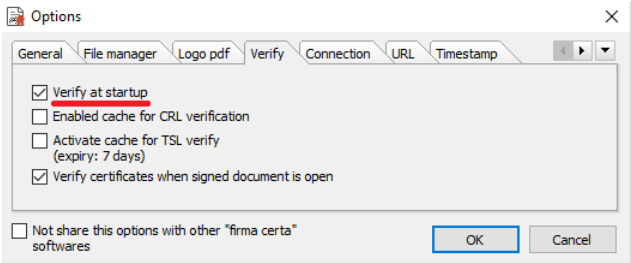


Figura 78 - Setări de verificare

7.2 MODUL DE VIZUALIZARE A UNUI FIȘIER SEMNAT

Pentru vizualizarea unui document semnat digital, parcurgeți următorii pași:

Adăugați fișierul în software și dați clic pe **Verify** (Verificare);
Dați clic pe pictograma de mai jos:

Figura 79 - Ecran pentru vizualizarea fișierului semnat în opțiunea Verify (Verificare)

ATENȚIE:

- Utilizatorul trebuie să verifice dacă are cea mai recentă versiune de Adobe Reader pentru a utiliza această opțiune;
- Va fi posibil să vizualizați un logotip PDF doar pentru fișierele .PDF semnate digital.

8 ANEXA D: MODUL DE CRIPTARE ȘI DECRIPTARE A UNUI FIȘIER

Criptarea unui document (numită și criptografie) este o operațiune specială prin care documentul va fi complet ilizibil pentru oricine, cu excepția celor care au cheia de decriptare, pentru readucerea acestuia într-o „formă lizibilă". Prin urmare, criptarea face posibilă garantarea caracterului privat al informațiilor confidențiale.
Pentru a cripta un document astfel încât numai un anumit destinatar să îl poată citi, expeditorul trebuie să aibă certificatul digital al destinatarului, deoarece operațiunea de criptare impune utilizarea cheii publice.
Pentru a decripta un document, destinatarul trebuie să aibă propriul dispozitiv de semnare SmartCard/Token, deoarece decriptarea impune utilizarea cheii private.

Semnarea digitală și operațiunea de criptare pot fi combinate, adică: un document poate fi semnat și apoi criptat pentru a asigura atât calitatea de autor, cât și secretul.
Pictograma unui document criptat cu Firma Certa Protect arată astfel:

8.1 MODUL DE CRIPTARE A UNUI FIȘIER

Rețineți că, **pentru a cripta un document, trebuie să aveți certificatul de criptare al destinatarului** (al utilizatorului, deoarece vrem să fim singurii care pot decripta documentul).

Acesta poate fi obținut prin solicitarea certificatului digital al destinatarului, apoi prin importul manual al acestuia în propria bază de date de certificate Firma Certa Protect.

Puteți cripta simultan un document pentru mai mulți utilizatori, deci pentru diferite persoane.

Pentru a cripta un document, dați clic pe „Protect Document" (Protejați documentul) în fereastra principală a Firma Certa Protect.

La sfârșitul operațiunii, fișierul criptat va fi creat în aceeași poziție în care documentul este salvat inițial.

8.2 MODUL DE DECRIPTARE A UNUI FIȘIER

Deschizând documentul cu un dublu clic, vi se va solicita să introduceți codul PIN pentru a deschide atât fereastra de verificare, cât și fereastra de vizualizare.

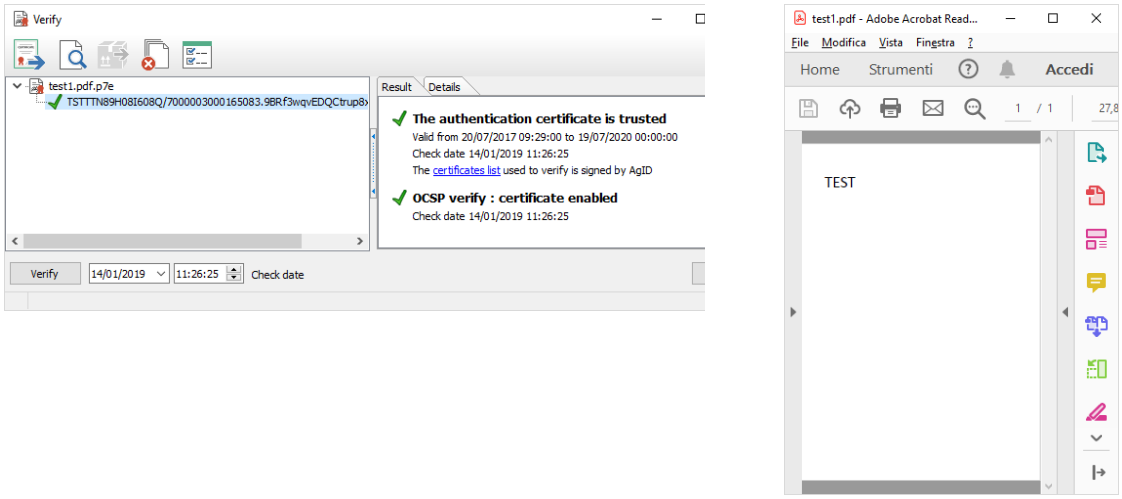


Figura 80 - Exemplu de fereastră de verificare

ATENȚIE:
Dacă nu aveți cheia privată necesară pentru decriptarea fișierului, va apărea un mesaj de eroare:

Figura 81 - Access denied (Acces interzis)

9 ANEXA F: LINIA DE COMANDĂ

Clientul FirmaCerta poate fi utilizat din linia de comandă pentru a permite integrarea cu aplicații care necesită semnături și marcaje temporale fără asistența operatorului. În mediul Windows, pentru a verifica poziția FirmaCerta, citiți valoarea PathApp a următoarei chei:

```
[HKEY_CURRENT_USER\Software\Namirial\Firmacerta\fcsign.exe] "PathApp" = ""
```

9.1 COMENZI ȘI PARAMETRI

fcsign.exe: <file> <action> <mode> <params>

<File>calea completă a fișierului de manipulat
<Action>0 = Semnătură 1 = Semnătură și marcaj temporal 2 = Contrasemnătură 3 = Marcaj temporal 4 = Verificare 5 = Afișare 7 = Opțiuni
<Mode>m dacă este necesară o semnătură în masă; în acest caz, trebuie să fie un fișier text care să conțină lista fișierelor care urmează a fi procesate câte una pe fiecare linie
<Params>

- **TargetDir**= <folder de destinație pentru fișiere procesate>
- **LogFileName**= <fișier jurnal al procesului, care rulează în modul silențios (fără afișarea ferestrelor inutile)>
- OverwriteLog= <File>
- **Pin**= <cod PIN pentru accesul la dispozitivul de semnare>
- **UrlTSA**= <adresă URL server pentru marcaje de timp>

NOTĂ: Dacă nu o configurați, configurația adresei URL va fi preluată în timpul configurării

- **UsernameTSA**= <utilizator pentru acces la serviciile de marcaj de timp>
- **PasswordTSA**= <parolă pentru acces la serviciile de marcaj de timp>
- **OverwriteFile**= <1 Suprascrierea fișierului procesat, dacă există; 0 adăugarea unui caracter de subliniere (_) în nume (implicit)>

IMPORTANT: Parametrii sub forma "key1=value1;key2=value2" (separați prin punct și virgulă (;) și încadrați de ghilimele (")).

9.2 EXEMPLE:

În cele ce urmează, vă prezentăm câteva exemple pentru ca utilizarea comenzilor să fie mai simplă și intuitivă.

Semnarea unui document fcsign.exe "C: \ Documents and Settings \ User \ Desktop \ Documento.pdf" 1

Semnarea unui document fără o interfață grafică

```
fcsign.exe "C:\Documents and Settings\User\Desktop\Documento.pdf" 1
"TargetDir=C:\Folder\;LogFileName=C:\firmacerta.log;Pin = 999999”
```

Semnarea mai multor documente

```
fcsign.exe "C:\temp\list.txt" 1 m
```

fișierul "C: \ temp \ list.txt" conține:

```
C:\Documents and Settings\User\Desktop\Documento1.pdf
C:\Documents and Settings\User\Desktop\Documento2.pdf
C:\Documents and Settings\User\Desktop\Documento3.pdf
```

10 ANEXA G: CARACTERISTICI AVANSATE

Clientul FirmaCerta are o serie de caracteristici neobișnuite, care le permit posesorilor să faciliteze operațiunile de semnare.

IMPORTANT: ***toate funcțiile de semnare a mai multor documente în același timp sunt posibile numai cu certificate emise de Autoritatea de certificare Namirial SpA***

10.1 SEMNAREA MAI MULTOR DOCUMENTE

Clientul îi permite utilizatorului să selecteze mai multe documente simultan, prin introducerea codului PIN o singură dată și semnarea consecutivă a documentelor.

Înainte de a efectua procedura Massive Signature (Semnare în masă), trebuie să configurați programul din Utility> General Options> General (Utilitar> Opțiuni generale> Generalități):

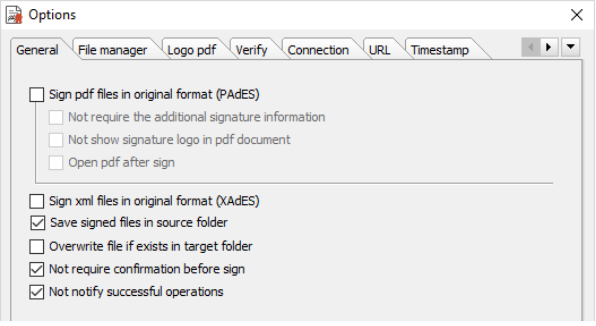


Figura 82 - Configurarea semnăturii automate Pades

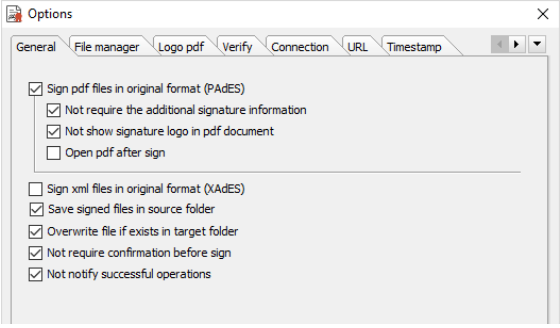


Figura 83 - Configurarea semnăturii automate Cades

10.2 MARCAREA TEMPORALĂ A MAI MULTOR DOCUMENTE

Clientul îi permite utilizatorului să selecteze mai multe documente simultan și să aplice marcajul temporal consecutiv.

Înainte de a efectua procedura Massive Timestamp (Marcare temporală în masă), trebuie să configurați programul din Utility> General Options> Timestamp (Utilitar> Opțiuni generale> Marcare temporală):

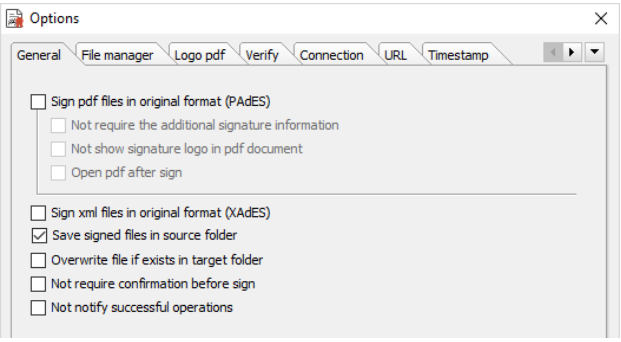


Figura84 - Opțiuni generale pentru marcarea temporală a mai multor documente

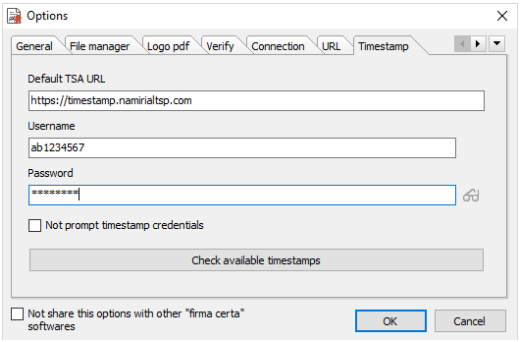


Figura 85 - Configurarea opțiunii Timestamp (Marcaj temporal)

Selectați formatul marcajului temporal și selectați „Keep values for all timestamps" (Se păstrează valorile pentru toate marcajele temporale) dacă doriți să păstrați aceeași valoare pentru toate fișierele care trebuie marcate temporal.

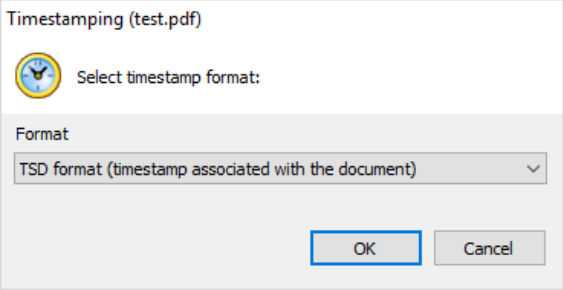


Figura 86 - Selectarea formatului marcajului temporal

10.3 SEMNAREA ȘI MARCAREA TEMPORALĂ A MAI MULTOR DOCUMENTE

Clientul îi permite utilizatorului să selecteze mai multe documente simultan și să aplice marcajul temporal consecutiv, prin introducerea codului PIN o singură dată pentru semnarea și marcarea temporală consecutivă a documentelor.

Înainte de a efectua procedura Massive Signature and Timestamp (Semnare și marcare temporală în masă), trebuie să configurați programul din Utility> General Options> General (Utilitar> Opțiuni generale> Generalități) mai întâi, apoi Timestamp (Marcare temporală):

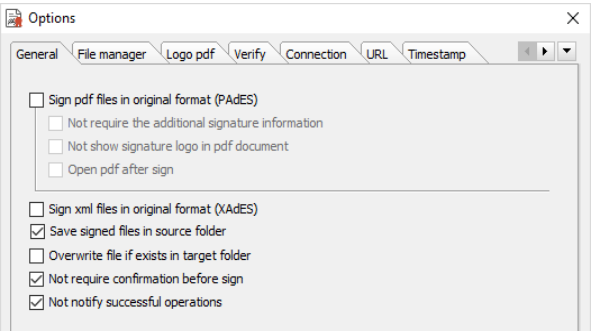


Figura 87 - Configurație pentru semnarea și marcarea temporală a mai multor documente

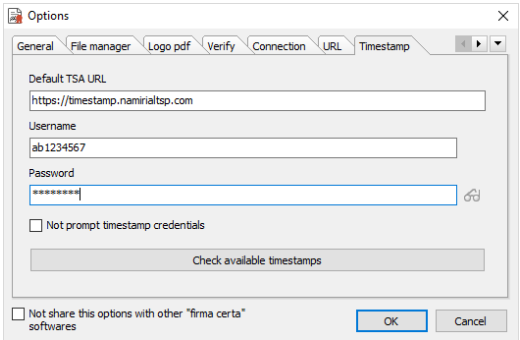


Figura 88 - Configurarea opțiunii Timestamp (Marcaj temporal)

Software-ul va solicita introducerea codului PIN o singură dată.

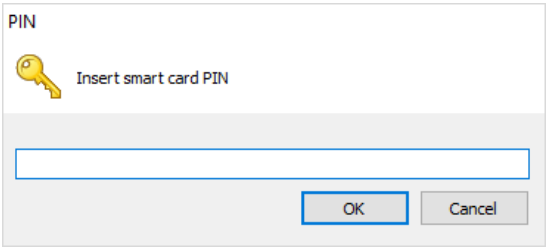


Figura 89 - Introducerea codului PIN

11 ANEXA H: REÎNNOIREA CERTIFICATULUI

Înainte de a continua, asigurați-vă că ați instalat pe computer software-ul de semnare **FirmaCerta**, actualizat corect.
Dacă utilizați un proxy, vă rugăm să solicitați configurația parametrilor de la administratorul de rețea.
Dacă nu există nicio reînnoire a certificatului, trebuie să descărcați software-ul FirmaCerta Device Manager (Manager dispozitive FirmaCerta).

11.1 CONFIGURAREA SERVERULUI PROXY

Deschideți software-ul Firmacerta și dați clic pe Device Manager> Certificate Renewal (Manager dispozitive> Reînnoire certificat), confirmați termenii și dați clic pe **Next** (Înainte).

Figura 90 - Clauze restrictive

Selectați „ACTION" (ACȚIUNE) și setați proxy-ul (pentru parametri, contactați administratorul de rețea) Dați clic pe SAVE (SALVARE).

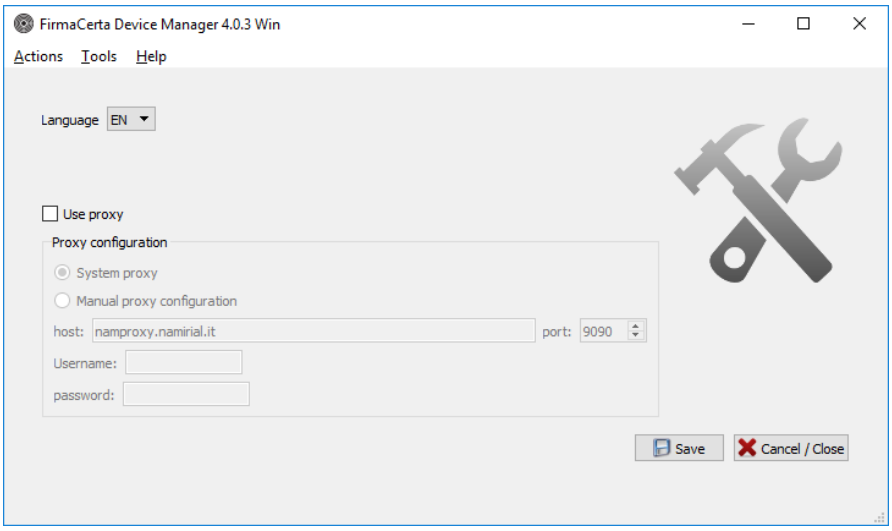


Figura 91 - Configurarea serverului proxy

11.2 METODE DE REÎNNOIRE: SMARTCARD ȘI TOKEN

Deschideți FirmaCerta cu dispozitivul de semnare conectat la computer, apoi dați clic pe „*Device Manager* > *Certificates Renewal*" (Manager dispozitive > Reînnoire certificate).
Citiți și confirmați termenii restrictivi și dați clic pe **NEXT** (ÎNAINTE).

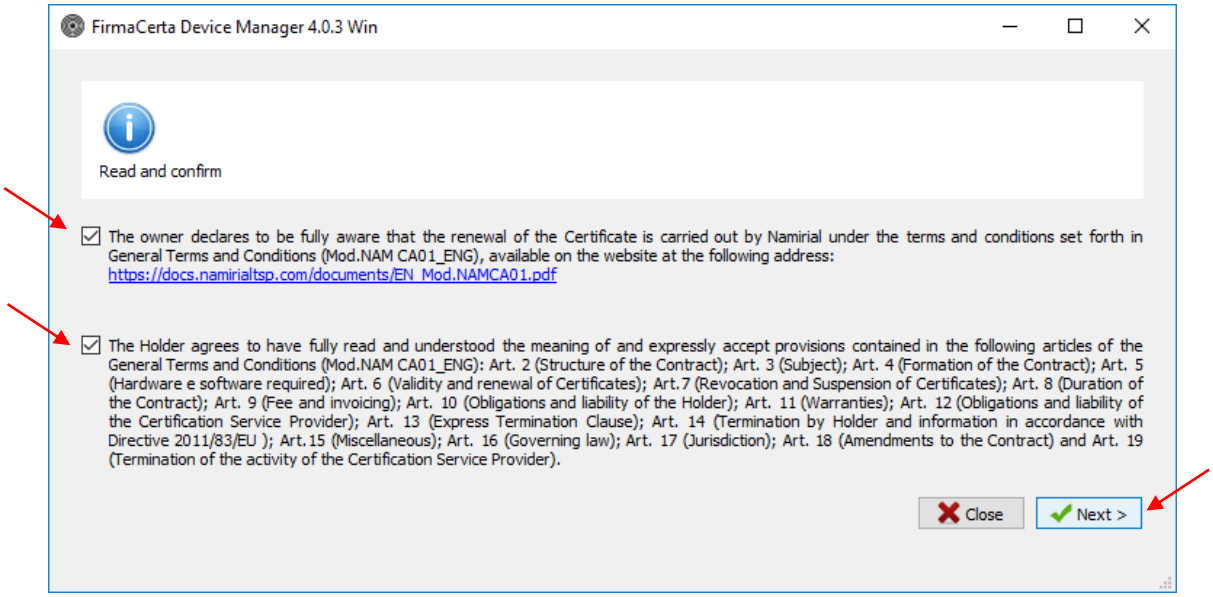


Figura 92 - Clauze restrictive

Apoi dați clic pe „**Select Device**" (Selectare dispozitiv) și introduceți codul PIN pentru recunoașterea dispozitivului și citirea certificatelor.

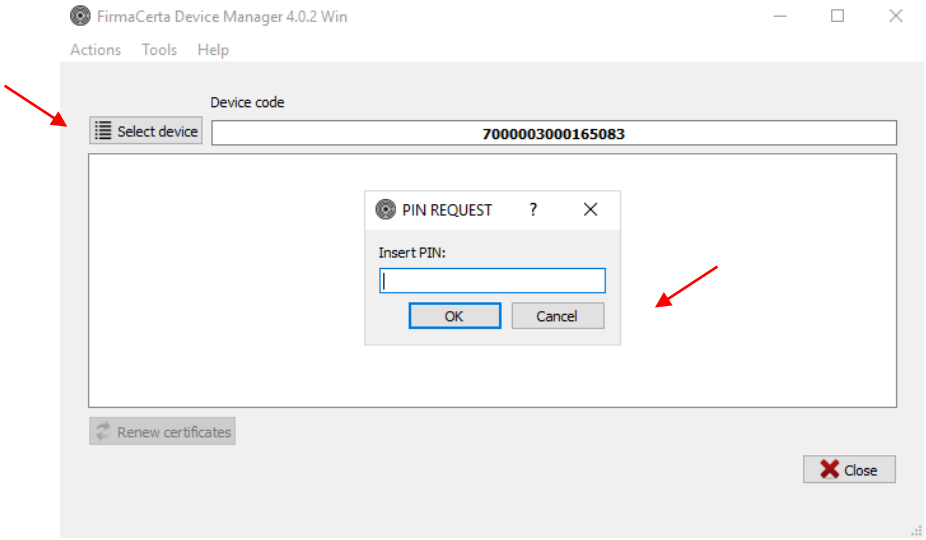


Figura 93 - Introducerea codului PIN

Instrumentul va propune afișarea (opțională) și semnarea digitală (obligatorie) a unui fișier .pdf pentru cererea de reînnoire a certificatelor. Selectați „OK", atunci când vi se solicită, pentru a finaliza operațiunea de semnare.

Așteptați până la finalizarea procedurii de reînnoire.

În acest moment, instrumentul va propune semnarea automată a contractului pentru certificatele de reînnoire, întrebând utilizatorul dacă dorește să îl vizualizeze sau nu.

După afișarea certificatelor, selectați **„Renew Certificates"** (Reînnoire certificate).

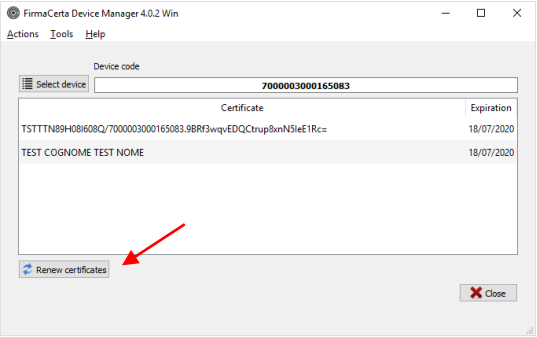


Figura 94 - Renew Certificates (Reînnoire certificate)

Apoi, instrumentul va propune afișarea sau nu a cererii de reînnoire, în ambele cazuri, fișierul va fi semnat digital.

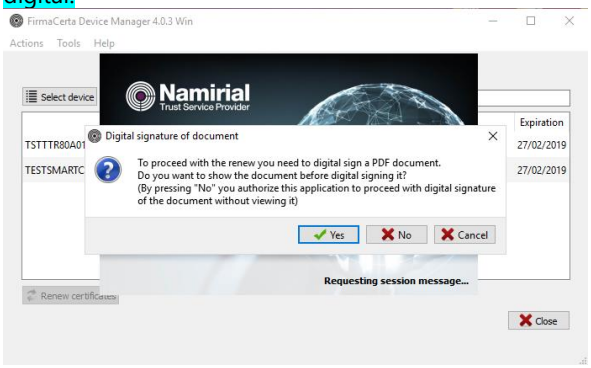


Figura 95 - Cerere de vizualizare a contractului înainte de semnarea acestuia

Dacă ați selectat vizualizarea documentului PDF, programul va afișa contractul de reînnoire a certificatului. Pentru a finaliza întregul proces, utilizatorul trebuie să-și aplice semnătura dând clic pe fișierul afișat.

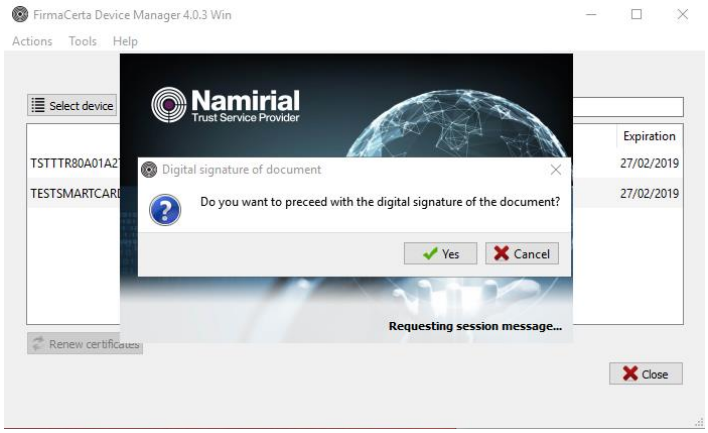


Figura 96 - Confirmarea aplicării semnăturii

Așteptați finalizarea procesului de reînnoire și încheierea operațiunii, prin apăsare pe **OK**.

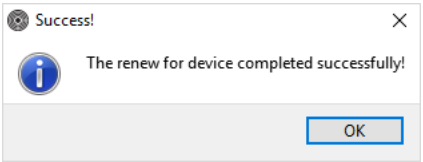


Figura 97 - Renewal successfully completed (Reînnoire finalizată cu succes)

11.3 METODE DE REÎNNOIRE: CERTIFICATE AUTOMATE ȘI LA DISTANȚĂ

Acces la spațiul personal, la următoarea adresă: https://portal.namirialtsp.com
Dați clic pe LOGIN (CONECTARE) și introduceți numele de utilizator și parola primite anterior prin e-mail în momentul emiterii certificatului de semnătură digitală.

Figura 98 - Private User Area (Spațiul privat al utilizatorului) Namirial

ATENȚIE: *În cazul pierderii acreditărilor, puteți recupera datele individuale dând clic pe „I don't remember the username" (Am uitat numele de utilizator) sau „I don't remember the password" (Am uitat parola), apoi urmați instrucțiunile. Dacă problema persistă, acreditările pot fi solicitate prin e-mail la helpdesk@firmacerta.it, cu specificarea codului fiscal al posesorului de semnătură.*

După reușita conectării.

- În pagina de pornire, găsiți caseta *Functionality or services to activate* (Funcționalitate sau servicii de activat) în partea dreaptă> *dați clic pe Renew certificates (Reînnoire certificate)*;
- Alternativ, dați clic pe *User* > *Digital Signature* > *Management* (Utilizator > Semnătură digitală > Administrare) din partea stângă;

Pentru a continua, vi se va solicita să introduceți codul OTP.

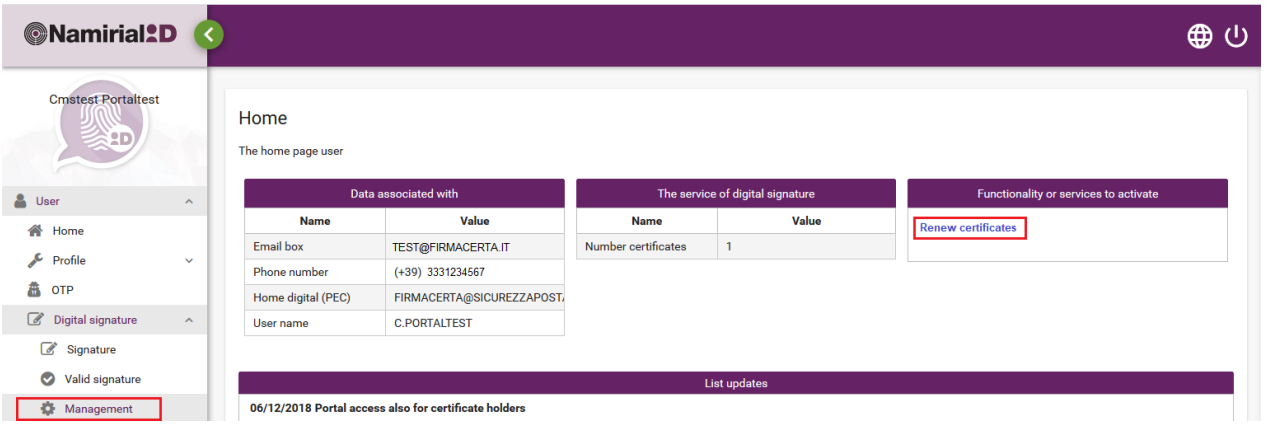


Figura 99 - Tabloul de bord personal al utilizatorului

În ***Certificate Management*** (Administrare certificate) vor fi afișate toate certificatele asociate utilizatorului, în coloana Renewable (Cu posibilitate de reînnoire) veți putea selecta certificatul pe care doriți să îl reînnoiți.

Se va deschide panoul *Selecting the certificate and click on the **RENEW** button* (Selectați certificatul și dați clic pe butonul REÎNNOIRE): Procedura de reînnoire autonomă a certificatului cu abonament; va trebui să introduceți mai întâi codul PIN al certificatului (prezent în plicul neinscripționat digital primit la emiterea certificatului), apoi codul OTP de verificare (în acest caz, SMS OTP).

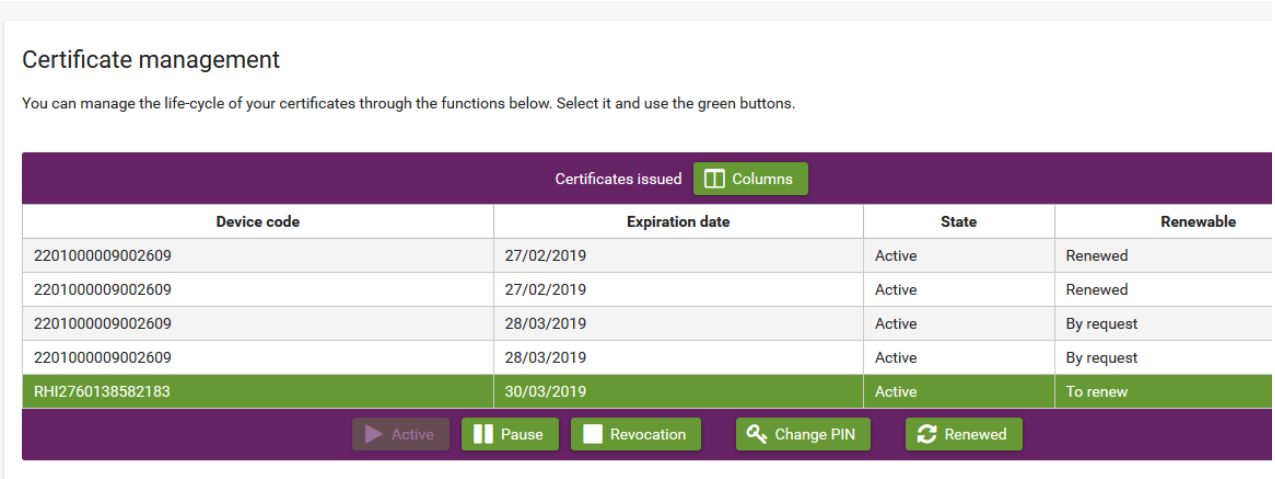


Figura 100 - Certificate Management (Administrare certificate)

După introducerea tuturor datelor, dați clic pe „**SIGN AND RENEW**" (SEMNARE ȘI REÎNNOIRE) și așteptați până când procedura de reînnoire a certificatului va fi finalizată.

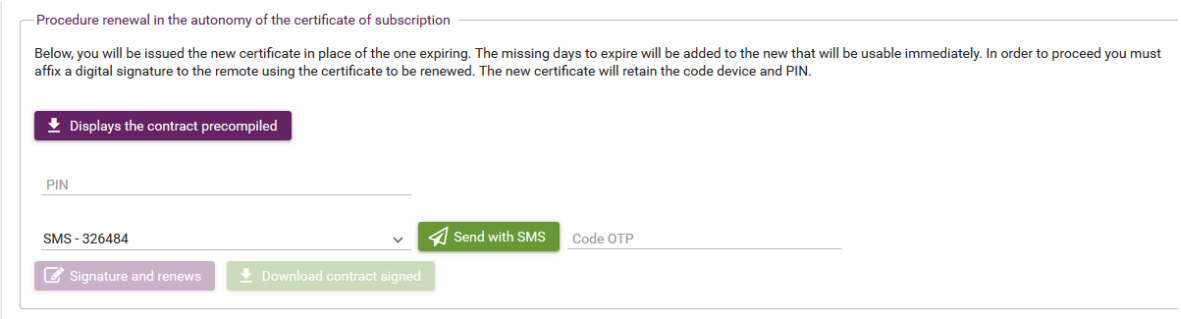


Figura 101 - Procesul de semnare și reînnoire

12 ANEXA I: CONFIGURAREA SEMNĂTURII LA DISTANȚĂ

12.1 INTRODUCERE ÎN APLICAȚIA NAMIRIAL OTP

Namirial OTP este o aplicație pentru dispozitive mobile care generează o parolă unică (sau parole de unică folosință) și este utilă pentru prima utilizare a semnăturii la distanță a software-ului Firma Certa pentru sistemele de operare Windows.
Acest tip de parolă este utilizat în mod normal pentru a finaliza o autentificare cu un nivel ridicat de securitate (autentificare puternică).

OTP-ul virtual poate fi necesar în următoarele scopuri:

- utilizarea semnăturii digitale la distanță (pe scurt, semnătura la distanță);
- acces SPID de nivel 2 sau superior, prin intermediul serviciilor de identificare Namirial;
- accesarea spațiului privat pentru serviciile TS Namirial.

12.1.1 MODUL DE DESCHIDERE A APLICAȚIEI

Din motive de securitate, deschiderea aplicației este posibilă numai după deblocarea dispozitivului.

Cu alte cuvinte:

- Dacă este deja configurată de utilizator, printr-un mecanism standard gestionat de smartphone.

În mod normal, telefoanele mobile de ultimă generație oferă următoarele opțiuni:

  - Introducerea unui cod PIN;
  - Utilizarea unei semnături;
  - Recunoaștere biometrică: amprentă digitală (Touch ID), detectarea feței (Face ID)

- Dacă utilizatorul nu a configurat niciun mecanism de blocare/deblocare, aplicația va solicita selectarea/configurarea unui cod PIN adecvat pentru a deschiderea acesteia.

12.1.2 CONFIGURAREA OTP NAMIRIAL

Pentru a continua cu prima activare, utilizatorul trebuie să lanseze aplicația și să introducă codul primit anterior prin SMS pe numărul de telefon mobil înregistrat în timpul procesului de solicitare de activare a serviciului (Remote Signature (Semnătură la distanță), SPID Namirial TSP sau alt serviciu).
În continuare, vă prezentăm un exemplu de mesaj pentru activarea OTP virtual.

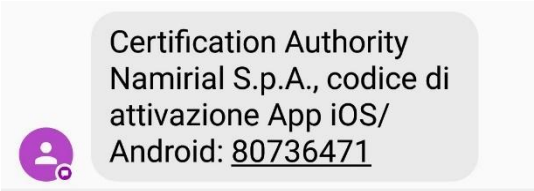


Figura 102 - Exemplu de SMS cu cod de activare

12.1.3 ANDROID

Pentru activarea OTP virtual trebuie să apăsați pe Add OTP (Adăugare OTP)
Mai jos vă prezentăm o secvență de acțiuni care vă arată cum să procedați:

Figura 103 - Ecran de pornire OTP virtual. Atingeți butonul roșu

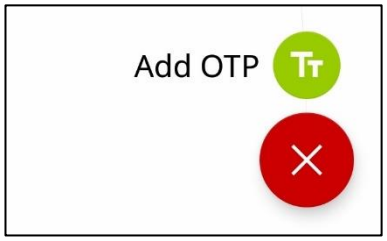


Figura 104 - Atingeți butonul verde (Add OTP (Adăugare OTP))

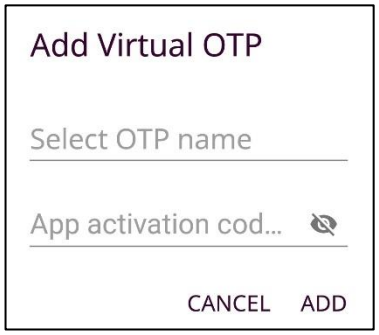


Figura 105 - Introducerea codului și alocarea etichetei

12.1.4 IOS

Pentru activarea OTP virtual trebuie să apăsați pe Add OTP (Adăugare OTP)
Mai jos vă prezentăm o secvență de acțiuni care vă arată cum să procedați:

Figura 106 - Ecran de pornire OTP virtual. Atingeți Add OTP (Adăugare OTP)

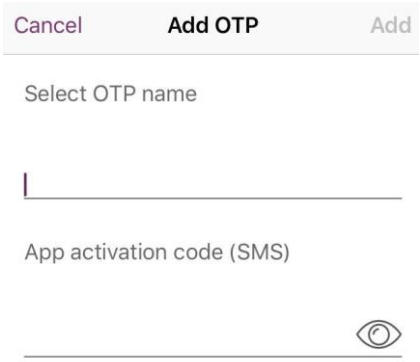


Figura 107 - Introducerea codului și alocarea etichetei

Afișarea în ultimul ecran:

- ***Virtual OTP Name*** **(Nume OTP virtual):** este eticheta de identificare asociată unui singur OTP (de exemplu, Signature (Semnătură)). Eticheta este utilă pentru a identifica tokenul pe care doriți să îl utilizați dacă mai multe tokenuri au fost activate simultan în cadrul aplicației.
- ***Activation SMS Code (Cod SMS de activare)/Codice attivazione app*****:** este codul de activare primit prin SMS, trebuie introdus în câmpul Codice attivazione App SMS (număr format din 8 cifre), apoi dați clic pe Add (Adăugare).

Atenție: dacă dați clic pe pictogramă, veți vedea clar codul de-abia introdus.

La sfârșitul procedurii, un cod din 6 cifre (actualizat la fiecare 30 de secunde) va fi afișat pe ecran.

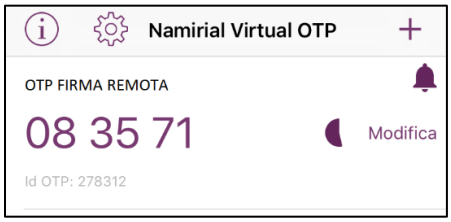


Figura 108 - Captură de ecran cod OTP generat din aplicație

12.2 ACTIVAREA SERVICIULUI NAMIRIAL SIGNENGINE

Descărcați software-ul Firma Certa de la următorul link

Pentru a activa serviciul Remote Signature (Semnătură la distanță), deschideți **FirmaCerta -> Utility -> General Options -> Web Services** (FirmaCerta -> Utilitar -> Opțiuni generale -> Servicii web).
Selectați Namirial SignEngine și dați clic pe **Enabled/Disabled** (Activat/Dezactivat).

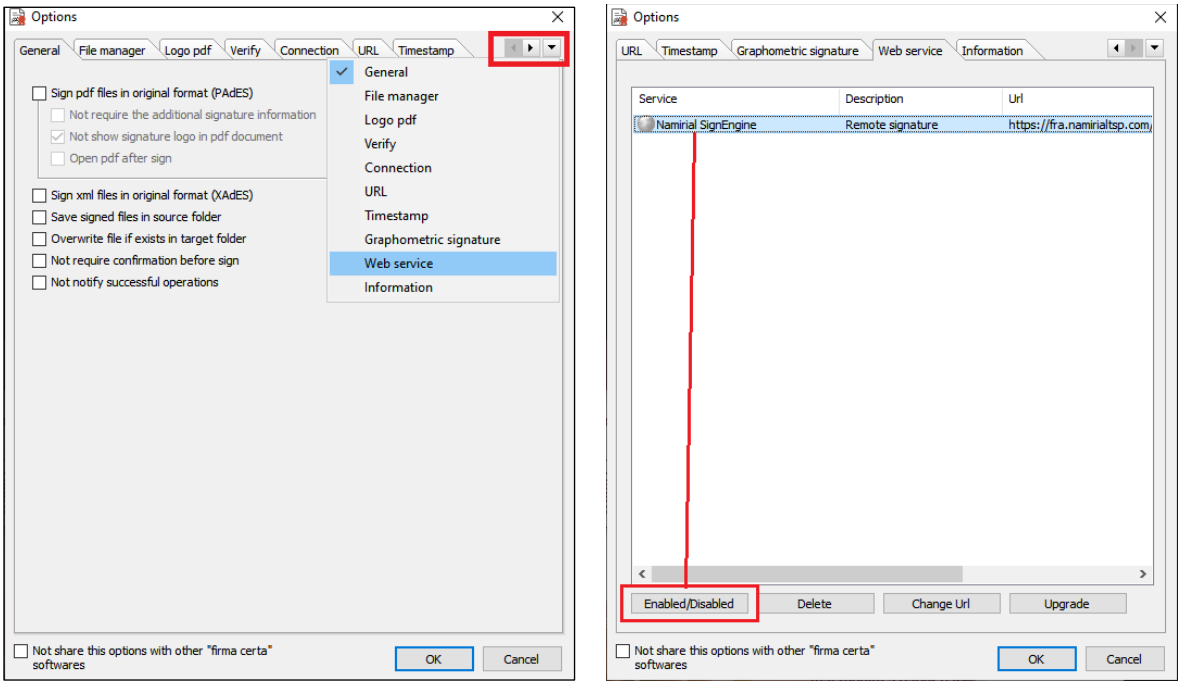


Figura 109 - Activarea serviciului SignEngine

12.3 MODUL DE SEMNARE A UNUI DOCUMENT

Selectați fișierul pe care doriți să îl semnați și dați clic pe **Sign** (Semnare).

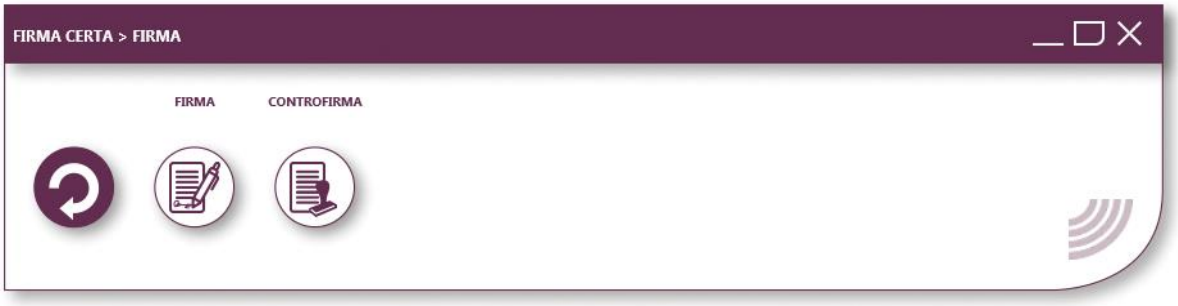
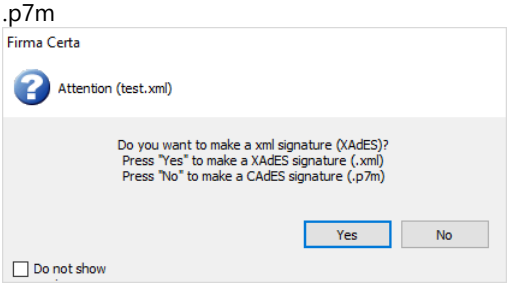


Figura 110 - Panoul Sign (Semnare)

ATENȚIE: Software-ul Firmacerta permite semnarea oricărui tip de fișier în format CAdES.p7m, numai pentru fișierele PDF sau XML software-ul îi va solicita utilizatorului să aleagă dacă dorește să semneze în .p7m sau să păstreze formatul original.

Apăsați **Yes** (Da) pentru o semnătură XAdES, păstrând formatul .xml (valabil numai pentru fișierele XML)

Apăsați **No** (Nu) pentru o semnătură CAdES în format .p7m



Apăsați **Yes** (Da) pentru o semnătură PAdES, păstrând formatul .pdf (numai pentru fișierele PDF)

Apăsați **No** (Nu) pentru o semnătură CAdES în format .p7m

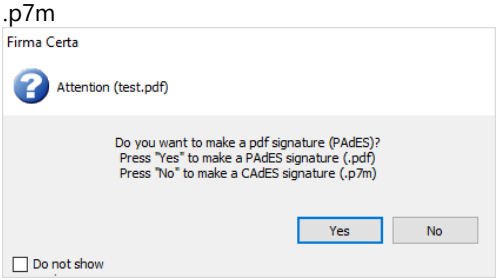


Figura 111 - Alegerea formatului de semnătură

Selectați folderul de destinație pentru fișierul semnat, apoi, la final, dați clic pe **OK**.

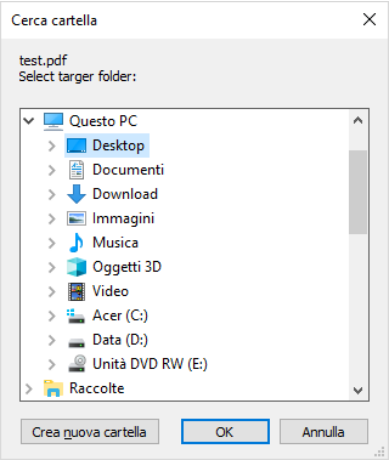


Figura 112 - Selectarea folderului de destinație

Continuați operațiunea de semnare, prin apăsare pe **Yes** (Da).

Atenție: Vă recomandăm să creați un folder specific pentru fișierul semnat digital, pentru a evita problemele.

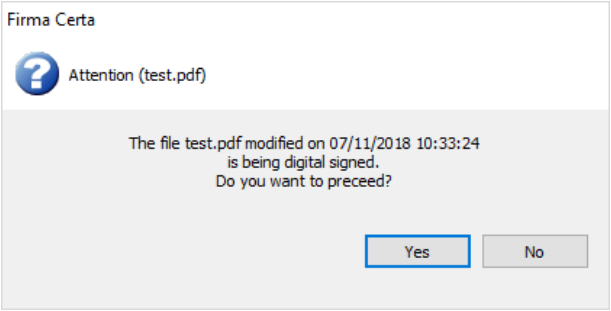


Figura 113 - Confirmarea semnăturii

12.3.1 USERNAME (NUME DE UTILIZATOR)

Dați clic pe **Settings** (Setări) pentru a introduce numele de utilizator:

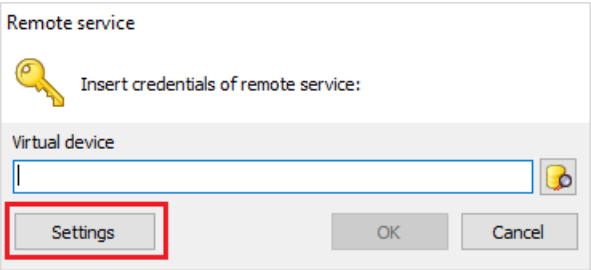


Figura 114 - Configurarea serviciului Remote Signature (Semnătură la distanță)

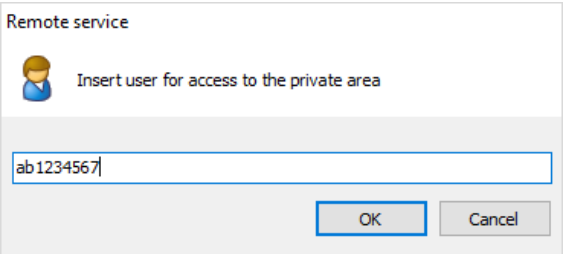


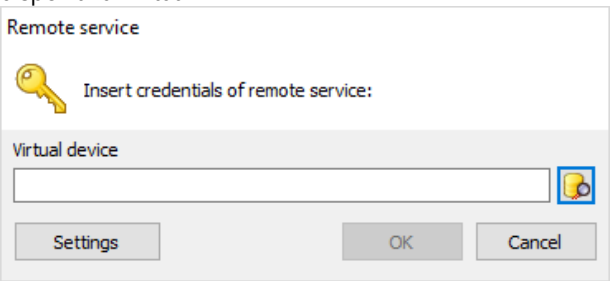
Figura 115 - Introducerea numelui de utilizator

ATENȚIE: În cazul pierderii numelui de utilizator: accesați spațiul dvs. personal, la următoarea adresă: https://portal.namirialtsp.com
Dați clic pe „*I don't remember the user name*" (Am uitat numele de utilizator) și urmați instrucțiunile.
Dacă problema va persista, contactați asistența tehnică prin e-mail la: helpdesk@firmacerta.it

12.3.2 SELECTAREA REMOTE DEVICE (DISPOZITIV LA DISTANȚĂ)

Pentru a configura dispozitivul virtual, selectați pictograma afișată în caseta roșie pentru a recupera dispozitivul virtual

Următoarea fereastră conține toate informațiile despre dispozitivele de semnare virtuală, utilizatorul trebuie să selecteze dispozitivul, apoi să dea clic pe OK.



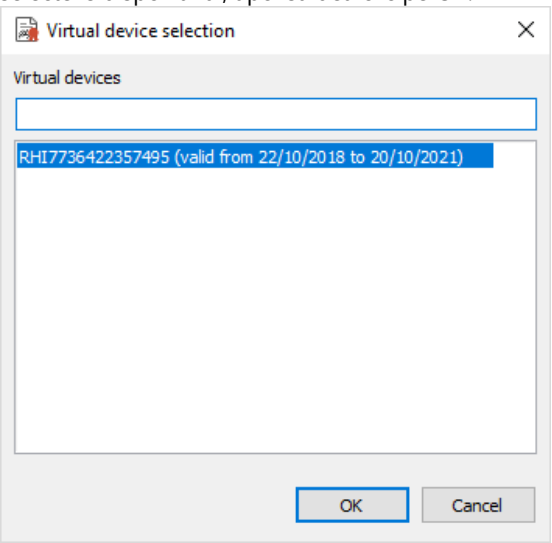


Figura 116 - Selectarea dispozitivului virtual la distanță

După adăugarea dispozitivului virtual, confirmați dând clic pe OK

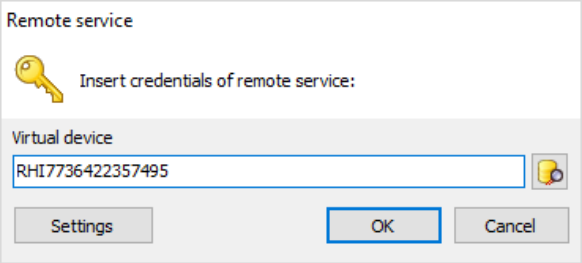


Figura 117 - Expert Remote Service (Serviciu la distanță)

12.3.3 SEMNAREA ÎN FORMAT PADES

ATENȚIE: Informațiile despre semnătură sunt opționale și sunt selectabile numai dacă formatul PAdES a fost selectat anterior.

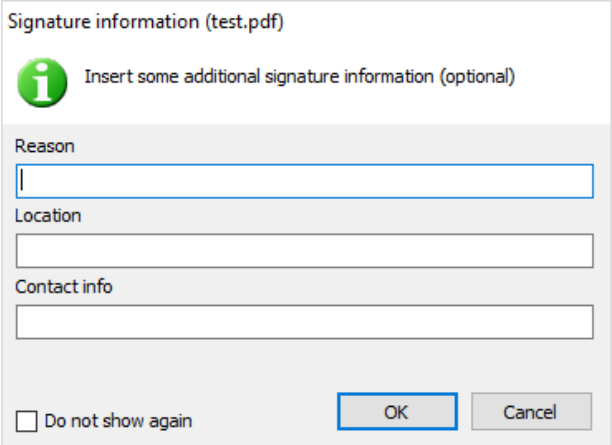


Figura 118 - Informații despre semnătură

Exemplu de e-mail cu acreditări pentru acces la Private Area (Spațiu privat):

Dear TEST NOME TEST COGNOME

thank you for choosing our digital signature products.

We herewith advise you of the USERNAME and the PASSWORD for accessing to your private area from the ACCESSO UTENTI section:

USERNAME: USERNAME

PASSWORD: PASSWORD

Within this area you can perform a series of operations directly related to the type of your device:

- Suspension - It may be used as often as it is necessary to suspend the validity of the certificates;
- Reactivation - It may be used on previously suspended certificates;
- Revoke - Require to interrupt permanently discontinue the validity of the certificates before their expiry date;
- Change PIN - It allows you to change the PIN code of the remote/automatic signature certificates;
- Change Emergency Code - It allows you to change the emergency number used for the remote/automatic signature certificates;
- Reset OTP - It allows you to reset the OTP token (does not apply to SMS OTP type);
- Check Signature - It allows you to run a check on the physical devices (smart cards, USB tokens or microSD);

Please note that the USERNAME is also necessary for the configuration of the \"FirmaCerta\" signature software for using the remote signature.
Through the USERNAME, FirmaCerta (available both for PC and Mac and for iPhone/iPad App) is able to automatically associate the holding OTP device.
To run the configuration please refer to the relative user guide.

Attention: This is an automatically generated email, please do not reply.

Best Regards,
Namirial S.p.A.
Email: helpdesk@firmacerta.it
Web: www.firmacerta.it

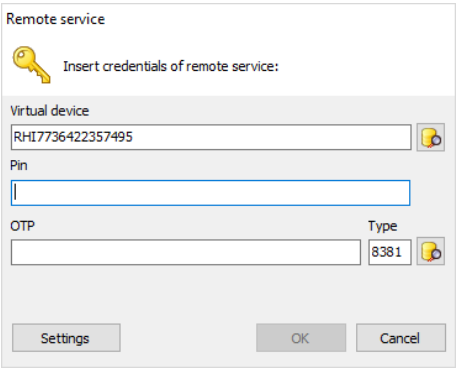
Safeguard clause
The information contained in this message are confidential and its diffusion, in any case, is strictly forbidden.
In the case you are not the intended recipient, we kindly ask you to delete this e-mail after having informed the sender and to not use, in any case, its content.

NamirialSpa
Trust Service Provider

Figura 119 - Exemplu de plic neinscripționat

12.4 PROCEDURA OTP SMS

Introduceți codul PIN primit într-un plic neinscripționat digital.



Dați clic pe pictograma din caseta roșie pentru a selecta dispozitivul OTP, apoi dați clic pe OK

Acest ecran afișează tipul de OTP (în acest caz, SMS)

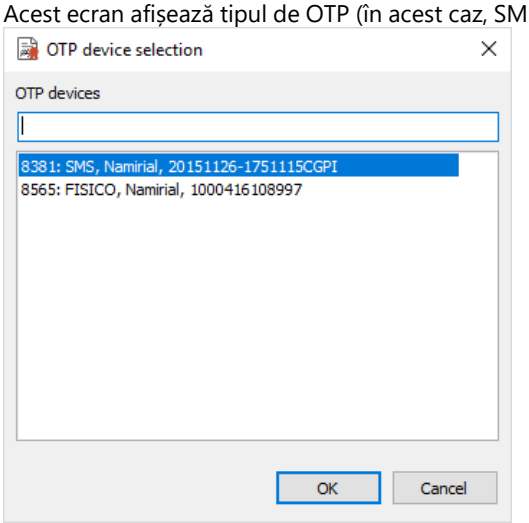


Figura 120 - Selectați dispozitivul OTP

Dați clic pe butonul **Send SMS** (Trimitere SMS) pentru a primi la numărul de telefon mobil furnizat în timpul înregistrării un SMS care conține codul OTP care trebuie introdus în caseta OTP

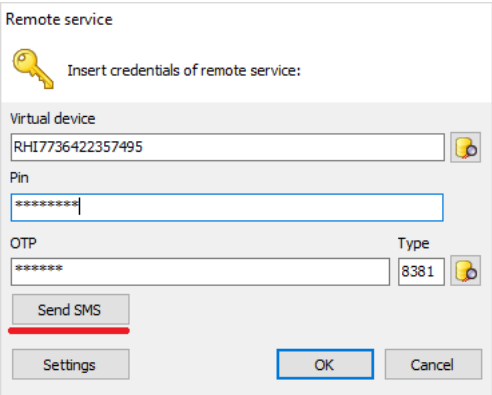


Figura 121 - Trimiterea SMS OTP

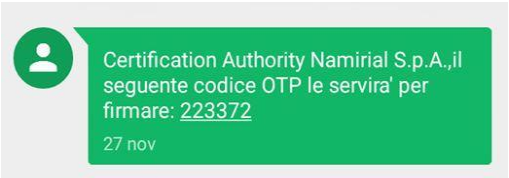


Figura 122 - SMS primit

La sfârșitul operațiunii va apărea următorul mesaj.

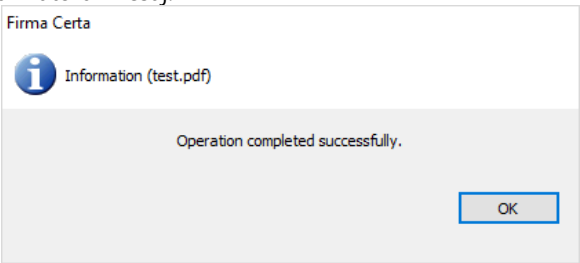
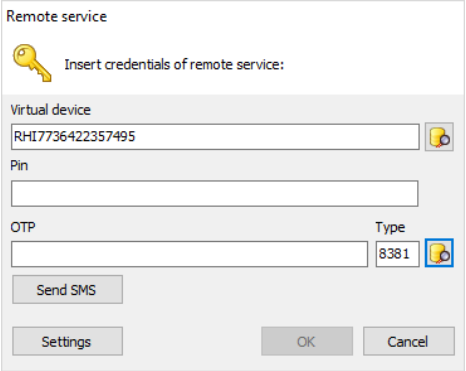


Figura 123 - Mesaj de confirmare

12.5 PROCEDURĂ OTP PENTRU MOBIL: OTP NAMIRIAL

Introduceți codul PIN primit într-un plic neinscripționat digital.



Dați clic pe pictograma din caseta albastră pentru a selecta dispozitivul OTP, apoi dați clic pe OK

Acest ecran afișează tipul de OTP (în acest caz, GENERATOR)

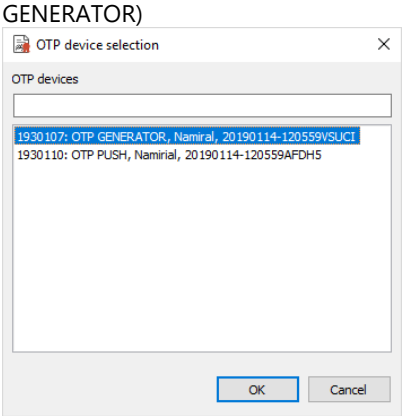
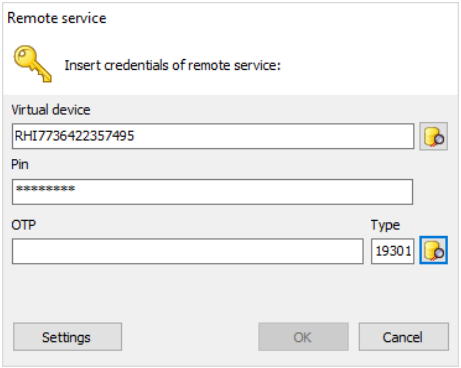


Figura 124 - Selectați dispozitivul OTP

Deschideți aplicația OTP Namirial și introduceți codul în caseta OTP



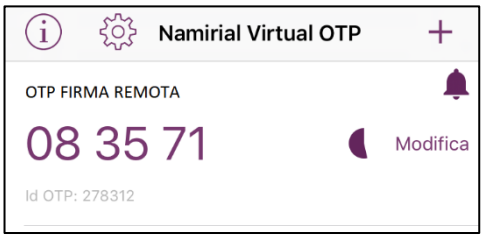


Figura 125 - Generator OTP

La sfârșitul operațiunii va apărea următorul mesaj.

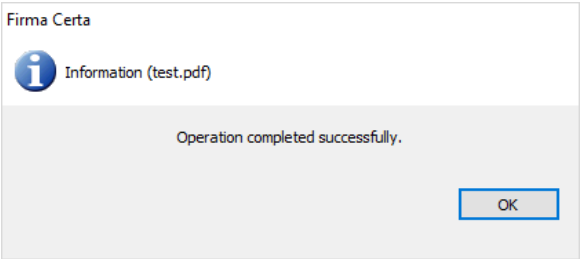


Figura 126 - Mesaj de confirmare

12.6 PROCEDURA HARDWARE OTP

12.6.1 ACTIVARE OTP

Autentificați-vă în User Private Area (Spațiul privat al utilizatorului), utilizând acreditările Username (Nume de utilizator) și Password (Parolă) primite prin e-mail la adresa de e-mail furnizată în timpul înregistrării.

RECUPERAREA ACREDITĂRILOR PENTRU PRIVATE AREA (SPAȚIUL PRIVAT): *În cazul pierderii numelui de utilizator și/sau parolei, le puteți recupera dând clic pe „I don't remember the username" (Am uitat numele de utilizator) sau „I don't remember the password" (Am uitat parola), apoi urmați instrucțiunile. Dacă problema persistă, acreditările pot fi solicitate prin trimiterea unui e-mail la: helpdesk@firmacerta.it, menționând codul fiscal al posesorului semnăturii.*

La prima accesare, portalul va recunoaște dacă dispozitivul OTP nu este încă activ.

Figura 127 – Activarea OTP

Generați codul cu OTP, prin apăsarea butonului de pe dispozitiv, apoi adăugați codul generat în câmpul de cod OTP și apăsați **Activate OTP** (Activare OTP).

Figura 128 - Private User Area (Spațiul privat al utilizatorului)

Introduceți codul PIN al dispozitivului primit într-un plic neinscripționat digital.

Dați clic pe pictograma din caseta roșie pentru a selecta dispozitivul OTP, apoi dați clic pe OK

Acest ecran afișează tipul de OTP (în acest caz, HARDWARE-FISICO)

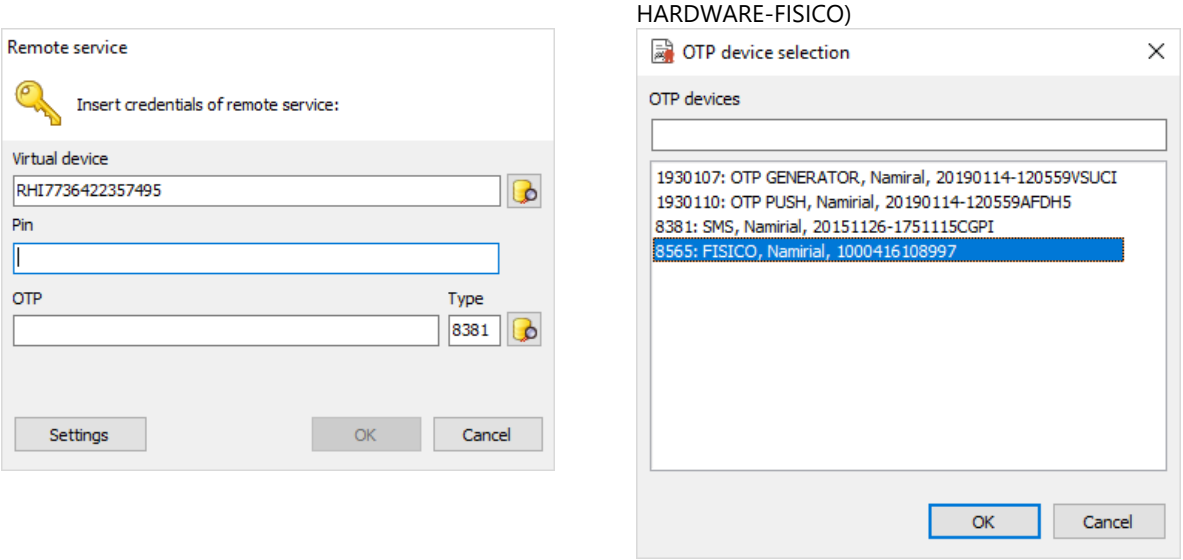


Figura 129 - Selectați dispozitivul OTP

După generarea codului prin intermediul dispozitivului atribuit, introduceți-l în câmpul OTP

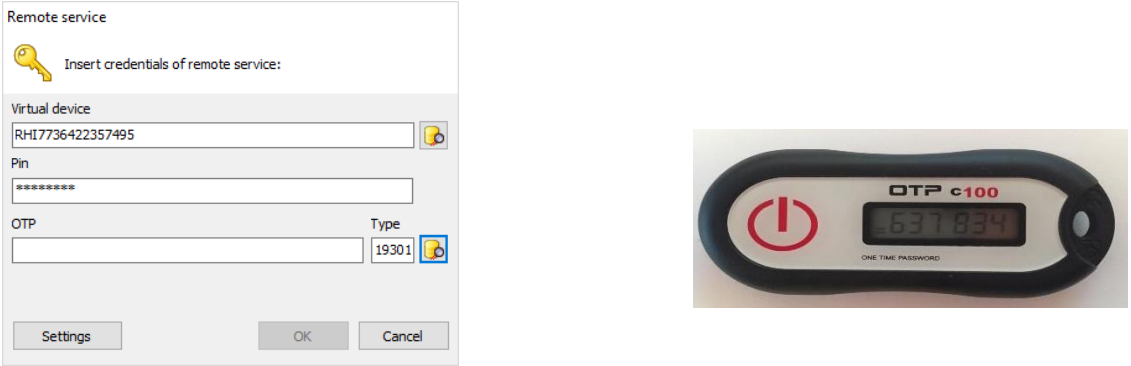


Figura 130 - Cod OTP generat

La sfârșitul operațiunii va apărea următorul mesaj.

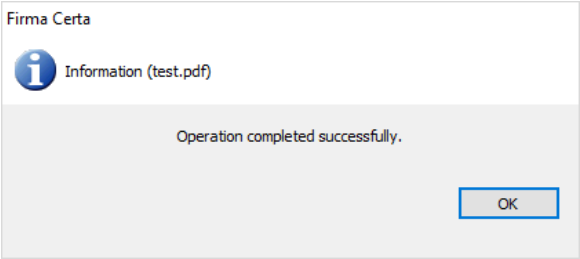


Figura 131 - Mesaj de confirmare

13 AUTENTIFICARE WEB

Pentru a importa certificatele, vă invităm să urmați ghidul publicat pe portalul nostru la următorul link: http://download.firmacerta.it/pdf/manualeAutenticazioneWeb.pdf

14 ANEXA J: BIT4ID – LINUX

Descărcați și instalați Bit4id PKI Manager Driver Manager, la următorul link:

- File . deb: 64 bit e file .deb 32bit
- File . rpm 64bit e file rpm 32bit

Deschideți Show Applications (Afișare aplicații) și căutați software-ul Bit4id PKI Manager.

Figura 132 - Tabloul de bord Linux

Software-ul Bi4id îi permite utilizatorului să folosească funcțiile Change PIN (Modificare PIN) și PIN unblock (Deblocare PIN), pentru dispozitivele de semnare smartcard și token.

PUK Change (Modificare PUK) este o funcție care poate fi activată numai cu combinația de taste **Ctrl + A**

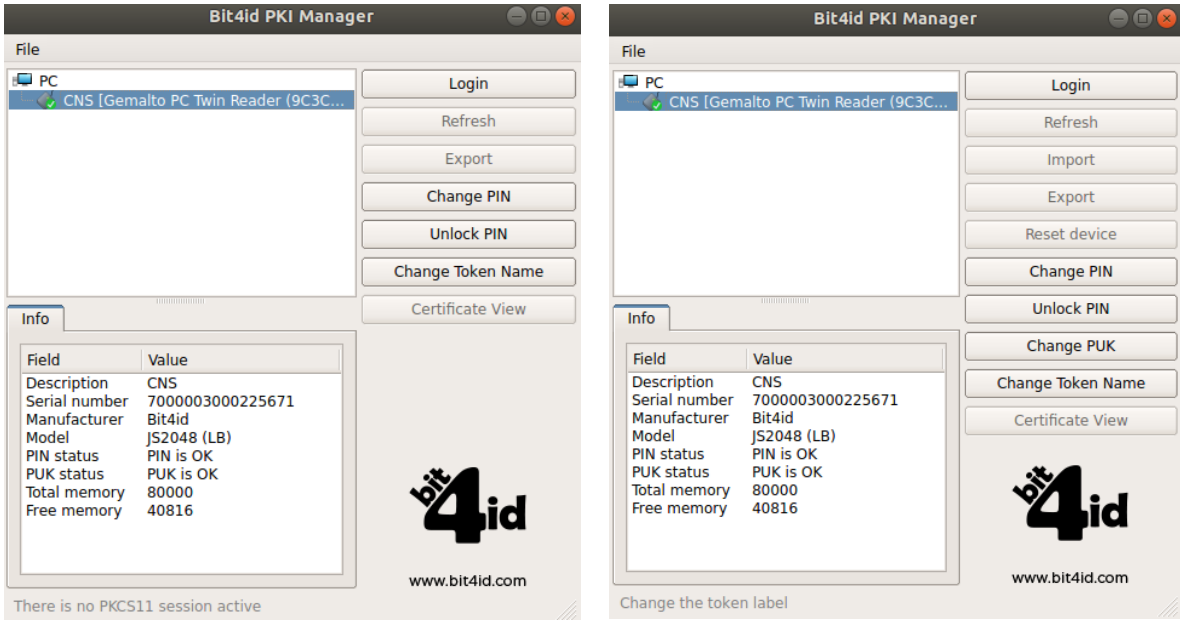


Figura 133 - Funcții avansate Bit4id PKI Manager

14.1 CHANGE PIN (MODIFICARE PIN)

Modificați codul PIN curent prin introducerea unui cod PIN nou (introducere și verificare).

ATENȚIE: Posesorul semnăturii la distanță poate modifica codul PIN din Private User Area (Spațiul privat al utilizatorului) din secțiunea > User > Digital Signature > Management (> Utilizator > Semnătură digitală > Administrare).

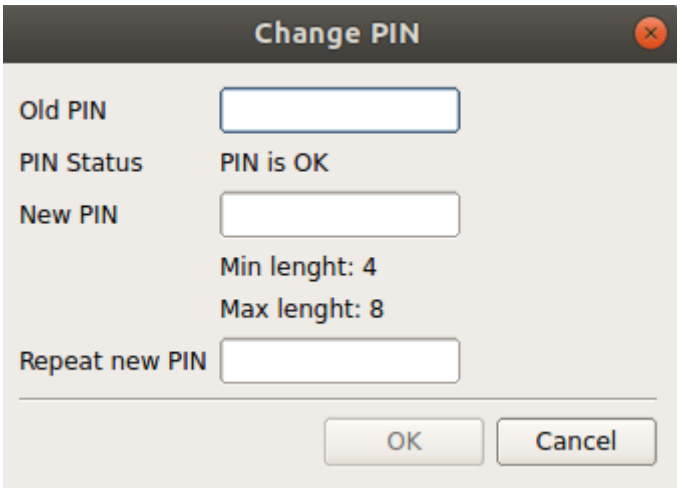


Figura 134 - Change PIN (Modificare PIN)

14.2 UNLOCK PIN (DEBLOCARE PIN)

Funcție necesară pentru deblocarea codului PIN. Introduceți codul PUK (codul numeric format din 8 cifre) din plicul neinscripționat.

ATENȚIE: înainte de procedura de deblocare, este obligatoriu ca plicul neinscripționat să vă fie pus la dispoziție după emiterea dispozitivului.

<u>După 3 încercări incorecte de scriere a codului PUK,</u> dispozitivul va fi blocat definitiv și va fi necesar să solicitați un nou dispozitiv de semnare.

Figura 135 - Unlock PIN (Deblocare PIN)

14.3 CHANGE PUK (MODIFICARE PUK)

Permite modificarea codului PUK curent atribuit de Namirial prin introducerea unui nou cod PUK, ales de utilizator (introducere și verificare).

ATENȚIE: Posesorul semnăturii la distanță nu poate fi modificat.

Firma Namirial nu este responsabilă pentru utilizarea improprie a acestei funcții. În cazul pierderii codului PUK, nu îl veți putea recupera și va trebui să solicitați un nou dispozitiv de semnare.

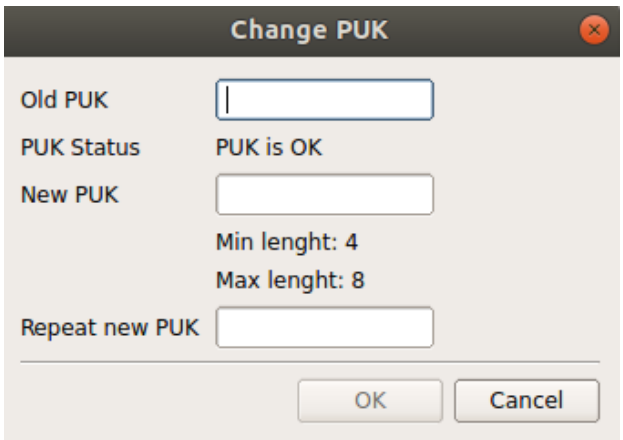


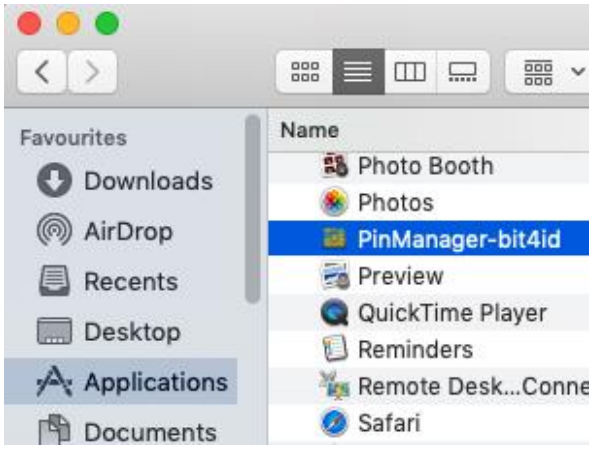
Figura 136 - Change PUK (Modificare PUK)

15 ANEXA K: BIT4ID – MACOS

Descărcați și instalați Bit4id PKI Manager Driver Manager, la următorul link:

Deschideți **Finder > Applications** (Instrument de găsire > Aplicații) sau dați clic pe **Launchpad** (Zonă de lansare) și căutați software-ul **PIN Manager** în lista de aplicații.

Deschideți **Finder** > **Applications** > **PIN Manager** (Instrument de găsire > Aplicații > PIN Manager)



Dați clic pe **Launchpad** (Zonă de lansare) și căutați software-ul **PIN Manager** în lista de aplicații

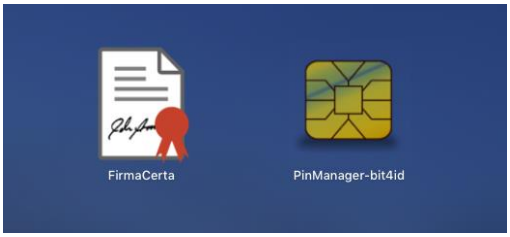
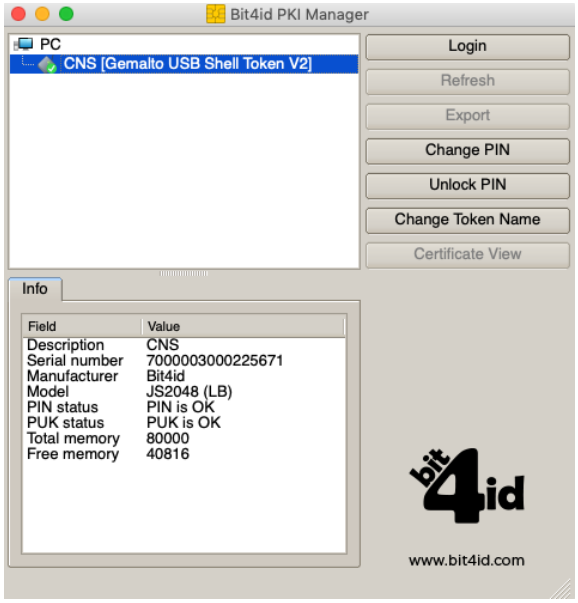


Figura 137 - Deschiderea PIN Manager

Software-ul Bi4id permite utilizarea funcțiilor Change PIN (Modificare PIN) și Unlock PIN (Deblocare PIN).



PUK Change (Modificare PUK) este o funcție care poate fi activată numai cu combinația de taste **CMD + A**

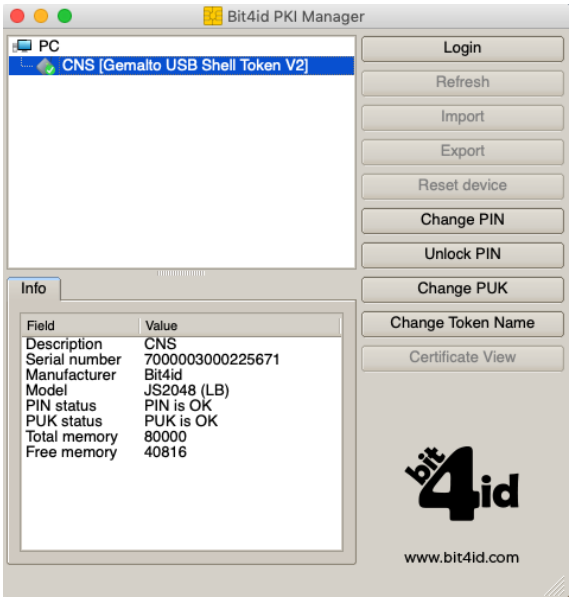


Figura 138 - Funcții avansate Bit4id PKI Manager

15.1 CHANGE PIN (MODIFICARE PIN)

Modificați codul PIN curent prin introducerea unui cod PIN nou (introducere și verificare).
ATENȚIE: Posesorul semnăturii la distanță poate modifica codul PIN din Private User Area (Spațiul privat al utilizatorului) din secțiunea > User > Digital Signature > Management (> Utilizator > Semnătură digitală > Administrare).

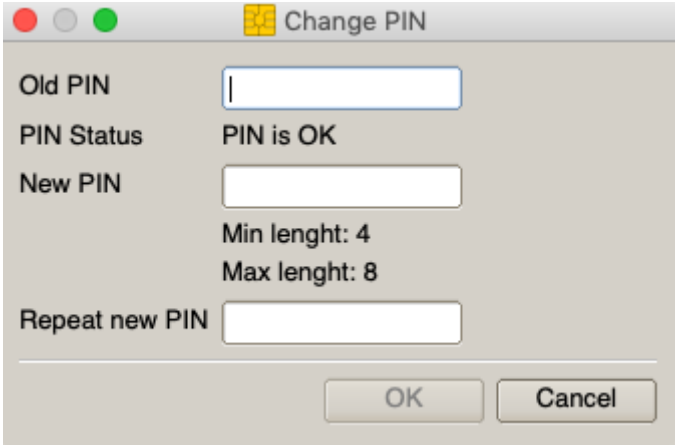


Figura 139 - Change PIN (Modificare PIN)

15.2 UNLOCK PIN (DEBLOCARE PIN)

Funcție necesară pentru deblocarea codului PIN. Introduceți codul PUK (codul numeric format din 8 cifre) din plicul neinscripționat.

ATENȚIE: înainte de procedura de deblocare, este obligatoriu ca plicul neinscripționat să vă fie pus la dispoziție după emiterea dispozitivului.
<u>După 3 încercări incorecte de scriere a codului PUK,</u> dispozitivul va fi blocat definitiv și va fi necesar să solicitați un nou dispozitiv de semnare.

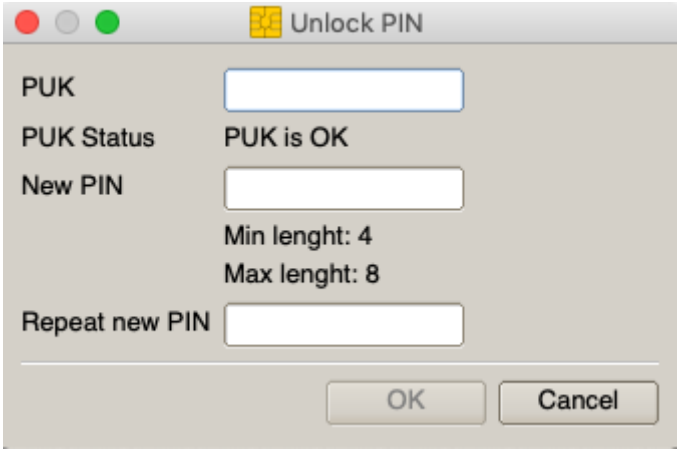


Figura 140 - Unlock PIN (Deblocare PIN)

15.3 CHANGE PUK (MODIFICARE PUK)

Permite modificarea codului PUK curent atribuit de Namirial prin introducerea unui nou cod PUK, ales de utilizator (introducere și verificare).

ATENȚIE: Posesorul semnăturii la distanță nu poate fi modificat.

Firma Namirial nu este responsabilă pentru utilizarea improprie a acestei funcții. În cazul pierderii codului PUK, nu îl veți putea recupera și va trebui să solicitați un nou dispozitiv de semnare.

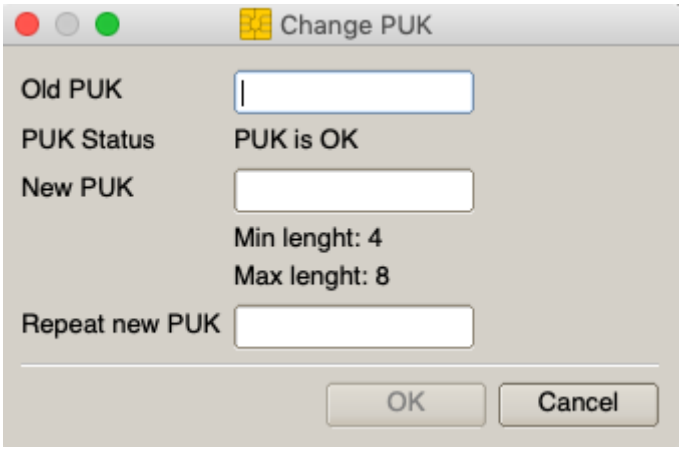


Figura 141 - Change PUK (Modificare PUK)

REFERINȚE

NUMĂR	DESCRIERE
[I]	<...>
[II]	<...>

INDEX TABELE

Tabelul 1 - Definiții și acronime 9

INDEX FIGURI

Figura 1 - Expertul firmacerta 10

Figura 2 - Selectați folderul de destinație 10

Figura 3 - Confirmarea instalării 11

Figura 4 - Mesaj pentru instalare reușită 11

Figura 5 - Interfața grafică FirmaCerta 12

Figura 6 - Submeniu pentru semnătură 12

Figura 7 - Accesarea funcției de semnare 13

Figura 8 - Accesarea funcției de contrasemnare 13

Figura 9 - Accesarea funcției de semnare și marcare 13

Figura 10 - Accesarea funcției de verificare 13

Figura 11 - Accesarea funcției de marcare 14

Figura 12 - Panoul de administrare a dispozitivelor 14

Figura 13 - Funcția de modificare a codului 14

Figura 14 - Funcția de deblocare a codului PIN 15

Figura 15 - Funcția de modificare a codului PUK 15

Figura 16 - Funcția de afișare a certificatelor 16

Figura 17 - Funcția de verificare a dispozitivului 17

Figura 18 - Accesarea funcției de reînnoire a certificatelor 17

Figura 19 - Marcator în șablon 18

Figura 20 - Fundal pentru semnătură 19

Figura 21 - General (Generalități) Signature Properties (Proprietăți semnătură) 19

Figura 22 - Cuvinte cheie de căutare....20

Figura 23 - Panoul Utility (Utilitar)....21

Figura 24 - Accesarea aplicației FirmaCerta Protect....21

Figura 25 - Panoul General Options (Opțiuni generale)....22

Figura 26 - Opțiuni: Gestionarea fișierelor....23

Figura 27 - Opțiuni: Adresa URL....23

Figura 28 - Opțiuni servicii web....23

Figura 29 - Opțiuni Information (Informații)....24

Figura 30 - Opțiuni: Configurarea proxy....24

Figura 31 - Panoul Signature Options (Opțiuni de semnare)....25

Figura 32 - Opțiuni: PDF Logo (Logotip PDF)....26

Figura 33 - Opțiuni: Opțiuni de verificare....26

Figura 34 - Panoul Graphometric Signature Options (Opțiuni de semnare grafometrică)....27

Figura 35 - (Opțiuni) Graphometric Signature (Semnătură grafometrică)....27

Figura 36 - Opțiuni grafometrice: Activarea licenței....28

Figura 37 - Opțiuni grafometrice: Confidențialitatea informațiilor....29

Figura 38 - Options (Opțiuni) Time Stamp (Marcaj temporal)....29

Figura 39 - Panoul: Help (Ajutor)....30

Figura 40 - Panoul Sign (Semnare)....31

Figura 41 - Selectarea formatului de semnătură Cades-XAdES....31

Figura 42 - Selectați folderul de destinație....32

Figura 43 - Confirmarea semnăturii....32

Figura 44 - Introducerea codului PIN....32

Figura 45 - Operation completed (Operațiunea a fost finalizată)....32

Figura 46 - Selectarea formatului de semnătură Cades-Pades....33

Figura 47 - Panoul Countersign (Contrasemnare) 35

Figura 48 - Selectați folderul de destinație 36

Figura 49 - Confirmarea suprascrierii 36

Figura 50 - Ecran exemplificativ: verificarea fișierului contrasemnat 36

Figura 51 - Confirmarea semnăturii 37

Figura 52 - Introducerea codului PIN 37

Figura 53 - Operation completed (Operațiunea a fost finalizată) 37

Figura 54 - Panoul Utility (Utilitar) 38

Figura 55 - Opțiuni de configurare a marcajului temporal 38

Figura 56 - Verificarea marcajelor temporale 39

Figura 57 - Selectați folderul de destinație 39

Figura 58 - Confirmarea semnăturii 39

Figura 59 - Introducerea codului PIN 40

Figura 60 - Confirmarea acreditărilor introduse pentru marcajul temporal 40

Figura 61 - Operation completed (Operațiunea a fost finalizată) 40

Figura 62 - Tablou de bord pentru semnare 40

Figura 63 - Selectarea formatului de semnătură Cades 41

Figura 64 - Panoul Timestamp (Marcaj temporal) FirmaCerta 42

Figura 65 - Selectarea formatului pentru marcaj temporal 42

Figura 66 - Selectarea folderului de destinație 42

Figura 67 - Confirmarea configurației pentru marcajul temporal 43

Figura 68 - Operation completed (Operațiunea a fost finalizată) 43

Figura 69 - Exemplu: fișier marcat temporal 43

Figura 70 - Panoul Verify (Verificare) FirmaCerta Panel pentru separarea marcajului temporal 44

Figura 71 - Separarea marcajului temporal 44

Figura 72 - Selectarea formatului....44

Figura 73 - Exemplu de fișiere marcate temporal....44

Figura 74 - Panoul Verify (Verificare) FirmaCerta....45

Figura 75 - Ecranul de verificare....45

Figura 76 - Ecranul filei Result (Rezultat)....46

Figura 77 - Ecranul filei Details (Detalii)....46

Figura 78 - Setări de verificare....46

Figura 79 - Ecran pentru vizualizarea fișierului semnat în opțiunea Verify (Verificare)....46

Figura 80 - Exemplu de fereastră de verificare....48

Figura 81 - Access denied (Acces interzis)....48

Figura 82 - Configurarea semnăturii automate Pades....50

Figura 83 - Configurarea semnăturii automate Cades....50

Figura84 - Opțiuni generale pentru marcarea temporală a mai multor documente....50

Figura 85 - Configurarea opțiunii Timestamp (Marcaj temporal)....50

Figura 86 - Selectarea formatului marcajului temporal....51

Figura 87 - Configurație pentru semnarea și marcarea temporală a mai multor documente....51

Figura 88 - Configurarea opțiunii Timestamp (Marcaj temporal)....51

Figura 89 - Introducerea codului PIN....51

Figura 90 - Clauze restrictive....52

Figura 91 - Configurarea serverului proxy....52

Figura 92 - Clauze restrictive....53

Figura 93 - Introducerea codului PIN....53

Figura 94 - Renew Certificates (Reînnoire certificate)....54

Figura 95 - Cerere de vizualizare a contractului înainte de semnarea acestuia....54

Figura 96 - Confirmarea aplicării semnăturii....54

Figura 97 - Renewal successfully completed (Reînnoire finalizată cu succes) 54

Figura 98 - Private User Area (Spațiul privat al utilizatorului) Namirial 55

Figura 99 - Tabloul de bord personal al utilizatorului 55

Figura 100 - Certificate Management (Administrare certificate) 56

Figura 101 - Procesul de semnare și reînnoire 56

Figura 102 - Exemplu de SMS cu cod de activare 57

Figura 103 - Ecran de pornire OTP virtual. Atingeți butonul roșu 58

Figura 104 - Atingeți butonul verde (Add OTP (Adăugare OTP)) 58

Figura 105 - Introducerea codului și alocarea etichetei 58

Figura 106 - Ecran de pornire OTP virtual. Atingeți Add OTP (Adăugare OTP) 58

Figura 107 - Introducerea codului și alocarea etichetei 58

Figura 108 - Captură de ecran cod OTP generat din aplicație 59

Figura 109 - Activarea serviciului SignEngine 59

Figura 110 - Panoul Sign (Semnare) 60

Figura 111 - Alegerea formatului de semnătură 60

Figura 112 - Selectarea folderului de destinație 61

Figura 113 - Confirmarea semnăturii 61

Figura 114 - Configurarea serviciului Remote Signature (Semnătură la distanță) 61

Figura 115 - Introducerea numelui de utilizator 61

Figura 116 - Selectarea dispozitivului virtual la distanță 62

Figura 117 - Expert Remote Service (Serviciu la distanță) 62

Figura 118 - Informații despre semnătură 63

Figura 119 - Exemplu de plic neinscripționat 63

Figura 120 - Selectați dispozitivul OTP 64

Figura 121 - Trimiterea SMS OTP 64

Figura 122 - SMS primit 64

Figura 123 - Mesaj de confirmare 64

Figura 124 - Selectați dispozitivul OTP 65

Figura 125 - Generator OTP 65

Figura 126 - Mesaj de confirmare 65

Figura 127 – Activarea OTP 66

Figura 128 - Private User Area (Spațiul privat al utilizatorului) 66

Figura 129 - Selectați dispozitivul OTP 67

Figura 130 - Cod OTP generat 67

Figura 131 - Mesaj de confirmare 67

Figura 132 - Tabloul de bord Linux 68

Figura 133 - Funcții avansate Bit4id PKI Manager 69

Figura 134 - Change PIN (Modificare PIN) 69

Figura 135 - Unlock PIN (Deblocare PIN) 70

Figura 136 - Change PUK (Modificare PUK) 70

Figura 137 - Deschiderea PIN Manager 71

Figura 138 - Funcții avansate Bit4id PKI Manager 71

Figura 139 - Change PIN (Modificare PIN) 72

Figura 140 - Unlock PIN (Deblocare PIN) 72

Figura 141 - Change PUK (Modificare PUK) 73