

Autoritatea de înregistrare

Ghid FirmaCerta pentru MacOS

Categorie	TSP-Digital Signature	ID document	NAM-User Guide MacOS	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



– Această pagină este lăsată necompletată în mod intenționat –



INDEX

Index	3
Istoricul modificărilor	6
1 Introducere	7
1.1 Scopul documentului și domeniul de aplicare	7
1.2 Definiții și acronime utilizate în document	8
2 Instalarea	9
3 Interfața grafică	11
4 Funcții principale	11
4.1 Semnarea	11
4.2 Sign and Timestamp (Semnare și marcare temporală).....	12
4.3 Countersign (Contrasemnare).....	12
4.4 Timestamp (Marcaj temporal).....	12
4.5 Verify (Verificare).....	12
4.6 View (Vizualizare).....	12
5 Tools (Instrumente)	13
5.1 Afișarea certificatelor în dispozitivul de semnare	13
5.2 Check Signature Device (Verificarea dispozitivului de semnare).....	14
5.3 Change PIN (Modificare PIN).....	14
5.4 Unlock PIN (Deblocare PIN)	15
5.5 Change PUK (Modificare PUK)	15
5.6 Renew Certificates (Reînnoire certificate).....	16
5.7 Options (Opțiuni).....	16
5.7.1 General (Generalități)	16



5.7.2	File (Fișier).....	17
5.7.3	Verify (Verificare).....	17
5.7.4	TimeStamp (Marcaj temporal).....	18
5.7.5	Updates (Actualizări).....	18
6	Anexa:.....	19
6.1	Anexa A: Modul de semnare a unui document.....	19
6.1.1	Selectarea formatului semnăturii.....	19
6.1.2	Select signature motivation (Only PDF FILE) (Se selectează motivul semnării (numai FIȘIER PDF)).....	20
6.1.3	Confirmarea procesului de semnare.....	20
6.2	Anexa B: Modul de contrasemnare a unui document.....	22
6.2.1	Confirmarea procesului de semnare.....	22
6.3	Anexa C: Configurarea parametrilor de marcare temporală.....	24
6.3.1	Anexa C1: Modul de marcare temporală a unui fișier.....	25
6.3.2	Anexa C2: Modul de semnare și aplicare a marcajului temporal într-un document.....	28
6.4	Anexa D: Modul de verificare a unui fișier.....	31
6.5	Anexa E: Reînnoirea certificatului.....	32
6.5.1	Configurarea serverului proxy.....	32
6.5.2	Reînnoirea smartcardului și tokenului.....	33
6.6	Anexa F: Ghid de semnare la distanță.....	35
6.6.1	Modul de semnare a unui fișier.....	35
6.6.2	Procedura OTP virtual: Namirial OTP.....	37
6.6.3	Procedura OTP SMS.....	41
6.6.4	Procedura Hardware OTP.....	42
6.7	Anexa H: Bit4id – MacOS.....	44
6.7.1	Change PIN (Modificare PIN).....	45
6.7.2	Unlock PIN (Deblocare PIN).....	45



6.7.3	Change PUK (Modificare PUK)	46
Referințe		47
Index tabele		48
Index figuri		48



ISTORICUL MODIFICĂRILOR

VERSIUNEA	1.0
Data	01/02/2019
Motive	Prima ediție a documentului
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 acestei semnături și oferă posibilitatea de a atribui documentului o anumită dată și oră, prin mecanismul de marcare temporală.

Firma Certa 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 Firma Certa și driverele bit4id pentru recunoașterea certificatelor; descrie, de asemenea, funcțiile Clientului Firma Certa, 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, Firma Certa va eșua în timpul operațiunii de verificare a documentului.



1.2 DEFINIȚII ȘI ACRONIME UTILIZATE ÎN DOCUMENT

TERMEN	DEFINIȚIE
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
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 pentru citirea documentelor PDF.
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, 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	Pentru semnătura electronică, legea se referă la un set de date în formă electronică, atașate sau conectate prin asociere logică cu alte date electronice, utilizate ca metodă de identificare computerizată.
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.
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.

Tabelul 1 - Definiții și acronime



2 INSTALAREA

Descărcați software-ul de pe următorul site www.firmacerta.it, secțiunea *Download > Software Firmacerta*, > Versiune Desktop per Mac (Descărcare > Software Firmacerta > Versiune desktop pentru Mac) ([LINK](#)).

După aceea, deschideți fișierul FirmaCerta.dmg și:

1. Trageți fișierul Firmacerta în folderul **Applicazioni** (Aplicații);
2. Deschideți pachetul *hid-switch-signed.pkg*
3. Deschideți pachetul *bit4id-middleware-user-signed.pkg* (după finalizarea instalării acestui pachet, sistemul trebuie repornit).



Figura 1 - Instalarea Firmacerta

Notă: Pentru dispozitivele cu numerele de serie 2203... 2204..., instalați [SafeDive](#).

Atenție: La prima pornire a software-ului FirmaCerta, un mesaj de avertizare va fi afișat pentru a informa utilizatorul următoarele: „FirmaCerta software belongs to a non-identified developer” (Software-ul FirmaCerta aparține unui dezvoltator neidentificat).

Acest mesaj apare pentru toate aplicațiile care nu aparțin Apple Store.



Figura 2 - Avertisment: dezvoltator neidentificat



Pentru a ignora setarea de securitate la deschiderea oricărei aplicații:

1. În Finder > Applications (Instrument de găsim > Aplicații), găsiți aplicația pe care doriți să o deschideți. Vă rugăm să nu utilizați Launchpad (Zonă de lansare) pentru această operațiune, deoarece Launchpad (Zonă de lansare) nu permite accesul la meniul rapid.
2. Dați clic pe pictograma aplicației, apăsând tasta **Ctrl** (alternativ, dați clic pe butonul din dreapta), apoi selectați **Open** (Deschidere) din meniul rapid.
3. Dacă dați clic pe Open (Deschidere) veți confirma deschiderea aplicației care va fi salvată ca excepție în setările de securitate, astfel încât în viitor utilizatorul va putea să o deschidă cu un dublu clic pe aplicația însăși, ca aplicație autorizată.

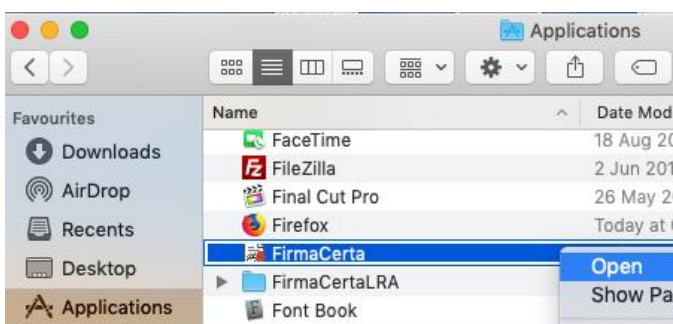


Figura 3 - Soluția 1a de instalare FirmaCerta

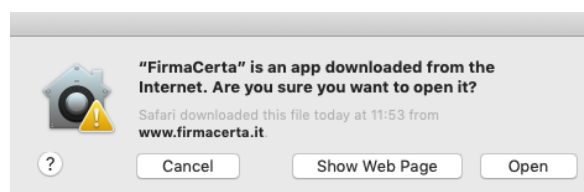


Figura 4 - Soluția 1b de instalare FirmaCerta

Notă:

Utilizatorul poate autoriza o excepție pentru o aplicație blocată anterior, dând clic pe butonul „**Open Anyway**” (Deschideți oricum) din panoul General (Generalități), panoul de preferințe „Security & Privacy” (Securitate și confidențialitate). Pentru a deschide acest panou, selectați meniul **Apple > System Preferences...** (Apple > Preferințe de sistem...) și dați clic pe „**Security & Privacy**” (Securitate și confidențialitate), apoi dați clic pe **General** (Generalități). După ce ati încercat să deschideți aplicația, acest buton este disponibil aproximativ o oră

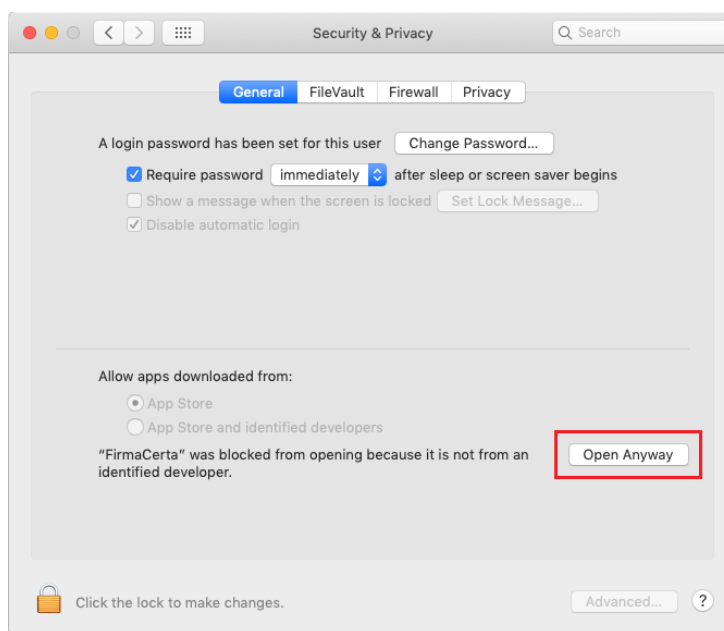


Figura 5 - Soluția 2 de instalare FirmaCerta



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;
- Vizualizați și verificați fișierele semnate digital;



Figura 6 - Interfața grafică FirmaCerta

Pentru informații suplimentare despre funcțiile principale, consultați [Capitolul 4](#)

În bara de activități puteți să administrați setările software-ului și utilizarea funcțiilor specifice, cum ar fi:

- Activarea dispozitivului de semnare
- Afișarea certificatelor dispozitivului de semnare
- Verificarea dispozitivului de semnare
- Reînnoirea certificatelor



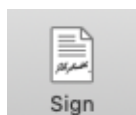
Figura 7 - FirmaCerta: Bara de instrumente

Pentru mai multe setări software și utilizarea funcțiilor specifice, consultați [Capitolul 5](#)

4 FUNCȚII PRINCIPALE

4.1 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 Software și dați clic pe pictograma „Sign” (Semnare).

Din bara de instrumente **File > Add File** (Fișier > Adăugare fișier) veți putea să căutați fișierul pe care doriți să îl semnați în folderele computerului.

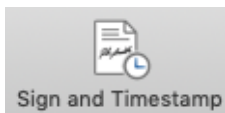
Din software: Dacă dați clic pe pictograma Sign (Semnare), puteți căuta fișierul pe care doriți să îl semnați în folderele computerului.

După ce apăsați pe „Sign” (Semnare), software-ul vă va cere să selectați directorul pentru salvarea fișierului/fișierelor 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 F: Semnătura la distanță](#)



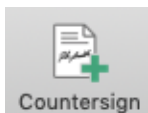
4.2 SIGN AND TIMESTAMP (SEMNARE ȘI MARCARE TEMPORALĂ)



Prin această funcție este posibilă semnarea și marcarea temporală, într-o singură operațiune, a unui sau mai multor documente digitale. Clientul Signature (Semnătură) vă solicită să selectați folderul de destinație pentru fișierul semnat. După ce apăsați pe „Sign and Timestamp” (Semnare și marcarea temporală) și introduceți codul PIN, software-ul vă va solicita să introduceți acreditările „Username” (Nume de utilizator) și „Password” (Parolă) pentru a utiliza marcasele temporale.

Consultați întreaga procedură pentru semnarea și marcarea temporală a unui document [Anexa C2: Modul de semnare și aplicare a marcatului temporal pe un document](#)

4.3 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 B: Modul de contrasemnare](#)

4.4 TIMESTAMP (MARCAJ TEMPORAL)



După selectarea unui fișier, cu această caracteristică puteți marca temporal fișierul respectiv, aplicând o anumită dată/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 C1: Modul de marcarea temporală a unui fișier](#)

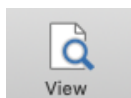
4.5 VERIFY (VERIFICARE)



Funcția 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 **Details** (Detalii) pentru a 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 D: Modul de verificare și vizualizare a unui fișier](#)

4.6 VIEW (VIZUALIZARE)



Această funcție vă permite să vizualizați documente semnate digital în format .p7m



5 TOOLS (INSTRUMENTE)

5.1 AFIȘAREA CERTIFICATELOR ÎN DISPOZITIVUL DE SEMNARE

În coloana din stânga sunt menționate cele două certificate:

Authentication (Autentificare) (Cod FISCAL) și
Subscription (Abonament) (Prenume și nume de familie).

În coloana din dreapta este afișat elementul **Result** (Rezultat) al verificării, iar în **Details** (Detalii) aceasta este detaliată.

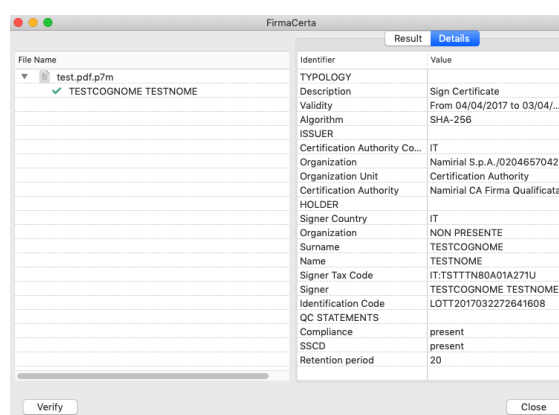
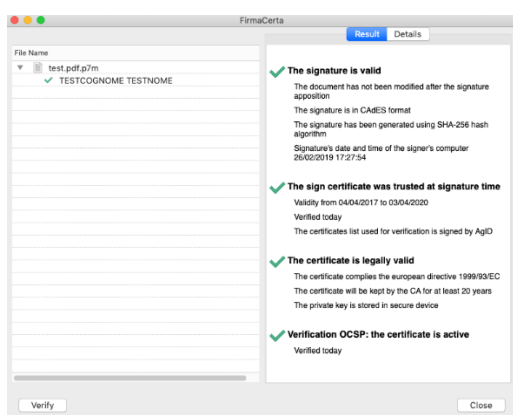
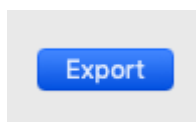


Figura 8 - Afișarea certificatelor în dispozitivul de semnare



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

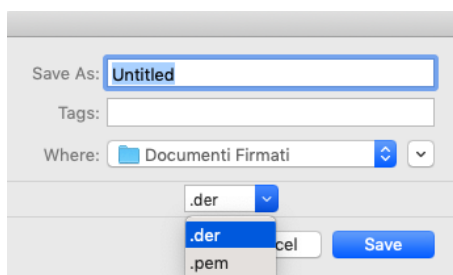


Figura 9 - Exportul certificatelor

.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.

.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 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.



5.2 CHECK SIGNATURE DEVICE (VERIFICAREA DISPOZITIVULUI DE SEMNARE)

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).

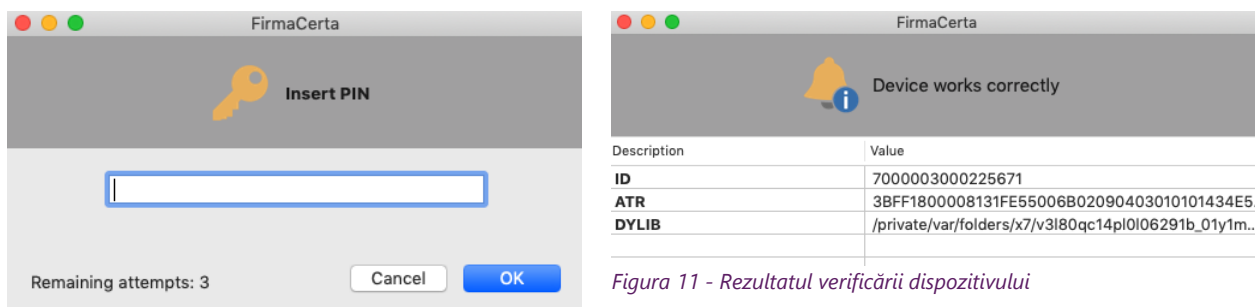


Figura 11 - Rezultatul verificării dispozitivului

Figura 10 - Introducerea codului PIN pentru verificarea dispozitivului de semnare

5.3 CHANGE PIN (MODIFICARE PIN)

Permite editarea codului PIN curent prin introducerea unui nou PIN (introducere și verificare).

Notă:

- Pentru posesorii de semnături digitale la distanță, aceștia pot modifica codul PIN prin accesarea [User Private Area](#) > User > Digital signature > Management (Spațiul privat al utilizatorului > Utilizator > Semnătură digitală > Administrare).
- Puteți utiliza opțiunea [Change PIN](#) (Modificare PIN) și cu Middleware Bit4id, așa cum se menționează în [Anexa H](#)

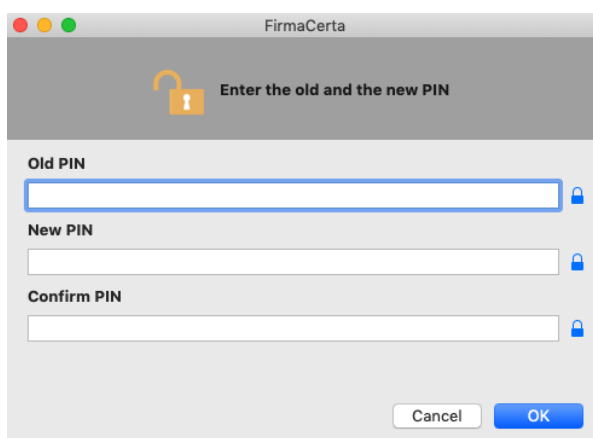


Figura 12 - Change PIN (Modificare PIN)



5.4 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.

Puteți utiliza opțiunea Unlock PIN (Deblocare PIN) și cu Middleware Bit4id, așa cum se menționează în [Anexa H](#)

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 13 - Unlock PIN (Deblocare PIN)

5.5 CHANGE PUK (MODIFICARE PUK)

Permite editarea codului PUK curent prin introducerea unui nou cod PUK (introducere și verificare).

Notă:

- Pentru posesorii de semnături digitale la distanță, aceștia pot modifica codul PIN prin accesarea [User Private Area](#) > User > Digital signature > Management (Spațiul privat al utilizatorului > Utilizator > Semnătură digitală > Administrare).
- Puteți utiliza opțiunea Change PUK (Modificare PUK) și cu Middleware Bit4id, așa cum se menționează în [Anexa H](#)

Figura 14 - Change PUK (Modificare PUK)



5.6 RENEW CERTIFICATES (REÎNNOIRE CERTIFICATE)

Funcție necesară pentru reînnoirea certificatelor de semnătură digitală pentru încă trei ani.
Consultați **ghidul** cu toate informațiile de bază pentru reînnoirea certificatelor, în [Anexa H](#).

ATENȚIE:

1. Dacă utilizatorul nu a fost deblocat de RAO, reînnoirea nu poate fi finalizată;
2. Certificatele nu pot fi reînnoite de două ori.

5.7 OPTIONS (OPȚIUNI)

În această secțiune puteți gestiona setările software-ului FirmaCerta.

5.7.1 GENERAL (GENERALITĂȚI)

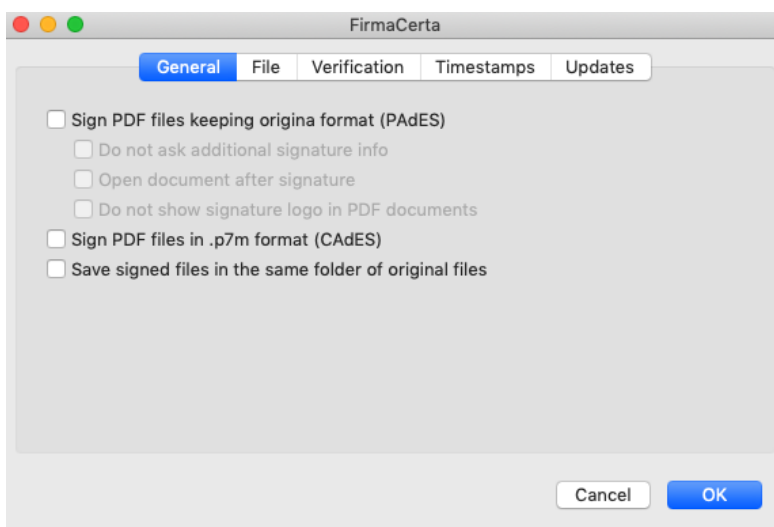


Figura 15 - Opțiuni: General (Generalități)

Signature of pdf files maintaining the format (PAdES) (Semnarea fișierelor PDF cu păstrarea formatului (PAdES)):	Fișierele .pdf vor fi semnate automat în format PAdES fără a-i permite utilizatorului să aleagă între formatul .p7m sau .pdf Păstrează formatul original al fișierului semnat (în caz contrar, convertit în format .p7m), oferindu-le utilizatorilor fără un software specific de semnare digitală posibilitatea de a vizualiza documentul.
• Do not request additional signature information (Nu se solicită informații suplimentare despre semnătură):	Informațiile opționale nu vor fi afișate în documentul semnat;
• 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.



• 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. Notă: Puteți personaliza logotipul prin intermediul setării Logo pdf (Logotip pdf) ; în lipsa acestui tip de personalizare, software-ul va utiliza un logotip în mod implicit
Signature of pdf files into .p7m format (CAAdES) (Semnarea fișierelor PDF în format .p7m (CAAdES)):	Fișierele .pdf vor fi semnate automat în format CAAdES fără a-i permite utilizatorului să aleagă între formatul .p7m sau .pdf.
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;

5.7.2 FILE (FIȘIER)

În această secțiune puteți să codificați fișiere semnate digital (.p7m), fișiere marcate temporal (.tsd, .tsr, .tst) și fișiere protejate (.p7e) în format Base64.

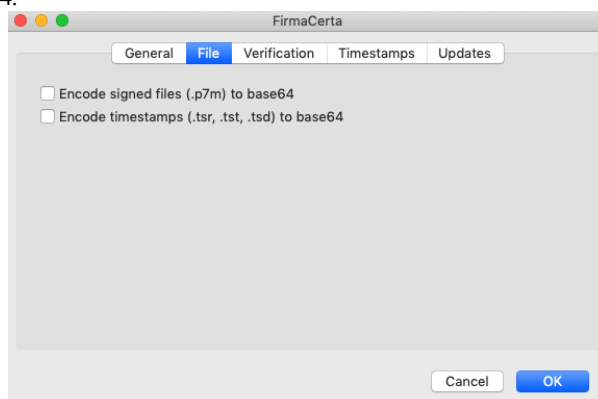


Figura 16 - Opțiuni: File (Fișier)

5.7.3 VERIFY (VERIFICARE)

Funcție pentru verificarea și afișarea simultană a stării certificatului (active (activ)/revoked (revocat)/suspended (suspendat)) și pentru verificarea fișierului la inițierea funcției Verify (Verificare).

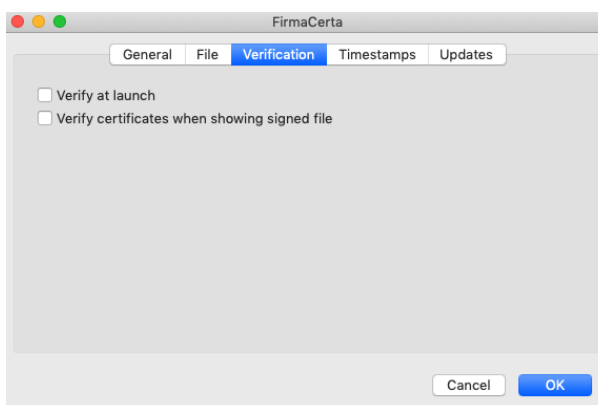


Figura 17 - Opțiuni: Verification (Verificare)



5.7.4 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.

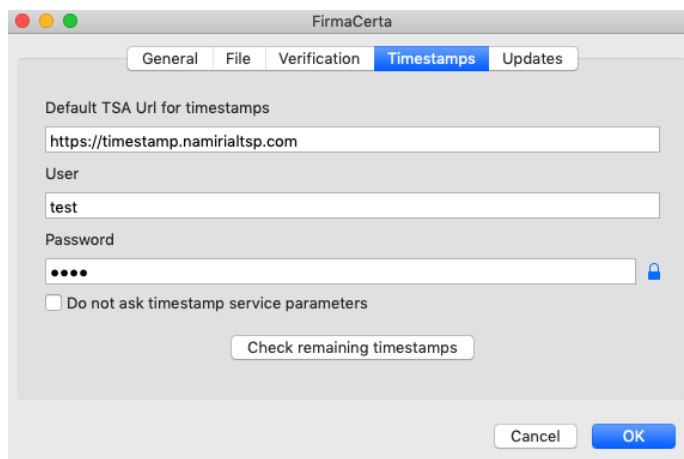


Figura 18 - Opțiuni: Timestamps (Marcaje temporale)

LINK de utilizare a serviciului de marcare temporală <https://timestamp.namirialtsp.com>
<http://timestamp.namirialtsp.com>

5.7.5 UPDATES (ACTUALIZĂRI)

Funcție pentru activarea/dezactivarea verificării actualizărilor, puteți alege dacă permiteți instalarea automată a actualizărilor atunci când sunt disponibile, în modul silențios.

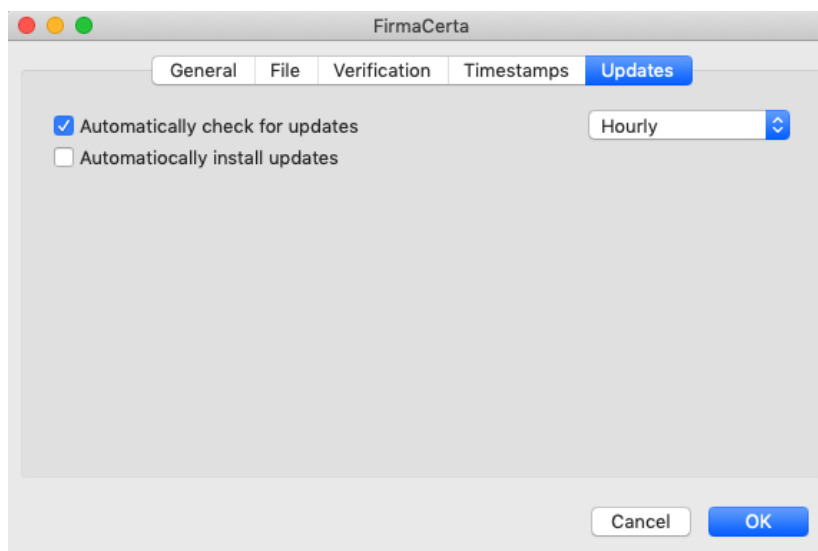


Figura 19 - Opțiuni: Updates (Actualizări)



6 ANEXA:

6.1 ANEXA A: MODUL DE SEMNARE A UNUI DOCUMENT

După încărcarea fișierului care urmează să fie semnat și dacă dați clic pe funcția **Signature** (Semnătură), utilizatorul va fi rugat să selecteze un folder de destinație pentru a salva documentul semnat.

În exemplul următor, a fost creat anterior un folder specific pentru fișierele semnate digital; selectați Signed Documents (Documente semnate) și dați clic pe **Open** (Deschidere).

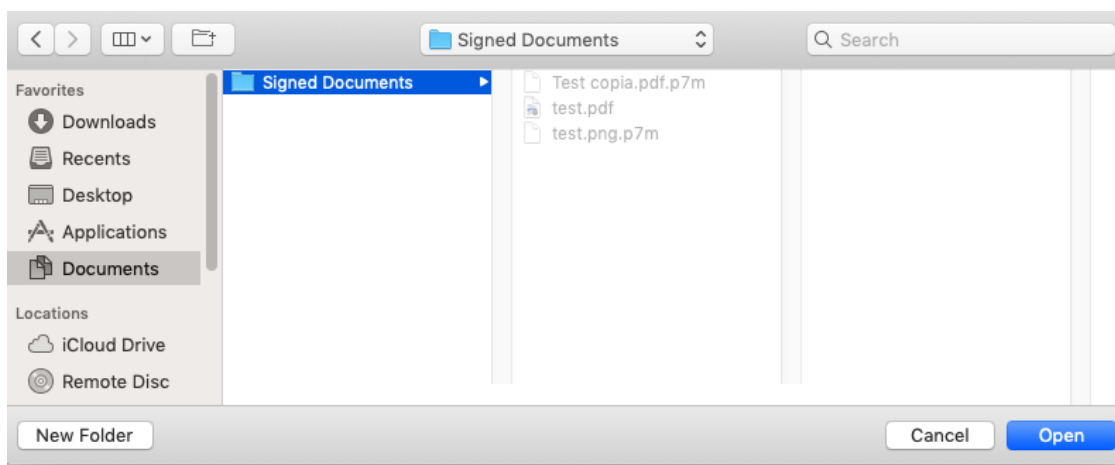


Figura 20 - Selectarea folderului de destinație

6.1.1 SELECTAREA FORMATULUI SEMNĂTURII

Selectați formatul CADES pentru a semna fișierul în format .p7m

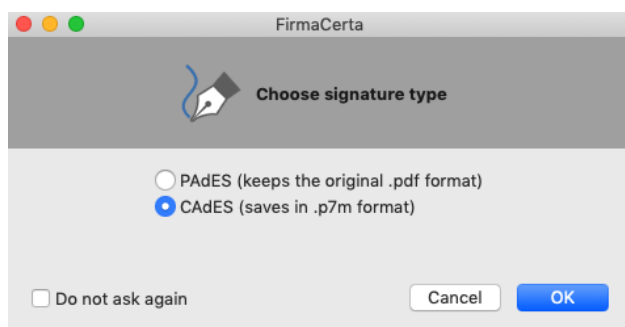


Figura 21 - Selectare: Format CADES

Selectați formatul PAdES pentru a semna fișierul în format .pdf

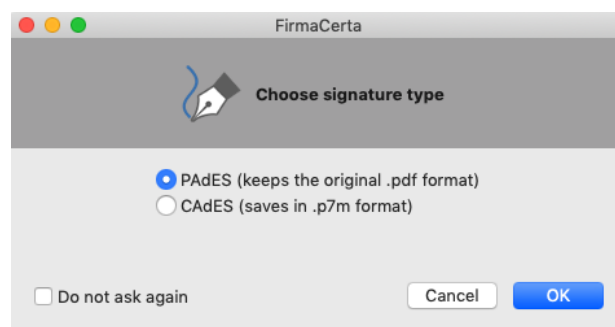


Figura 22 - Selectare: Format PAdES

Notă: selectarea formatului semnăturii este disponibilă numai pentru .pdf, pentru orice alt format software-ul va aplica automat extensia .p7m

Preferința **Do not ask anymore** (Nu mai întreba) va fi setată automat să nu mai afișeze mesajul și va trebui să modificați setările din [Options](#) (Opțiuni) pentru a avea posibilitatea de a vizualiza din nou mesajul.



6.1.2 SELECT SIGNATURE MOTIVATION (ONLY PDF FILE) (SE SELECTEAZĂ MOTIVUL SEMNĂRII (NUMAI FIȘIER PDF))

Această funcție îi permite utilizatorului să adauge informații opționale, precum *motivation* (motiv), *location* (locație), *contact information* (informații de contact) înainte de a finaliza semnarea documentului.

Notă: Această funcție este disponibilă numai pentru documentele .p7m.
Utilizarea acestei funcții este la alegerea utilizatorului, ca Optional Operation (Operațiune opțională).

The dialog box is titled 'FirmaCerta' and contains the text 'Specify some additional information that will be displayed in the document signature (optional)'. It has three input fields: 'Reason', 'Location', and 'Contact Info'. At the bottom, there is a checkbox labeled 'Do not ask again' and two buttons: 'Cancel' and 'OK'.

Figura 23 - Informații despre semnătură

6.1.3 CONFIRMAREA PROCESULUI DE SEMNARE

Confirmarea aplicării semnăturii.

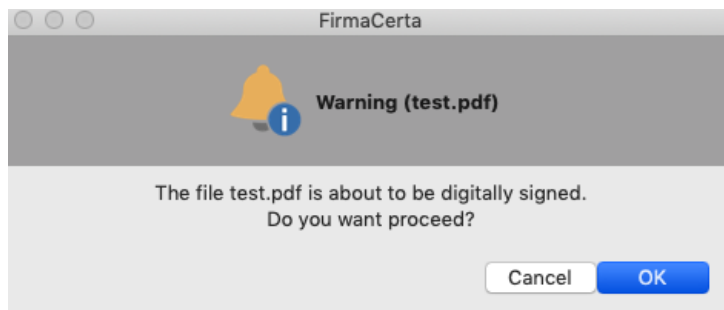


Figura 24 - Confirmarea procesului de semnare

Selectarea dispozitivului de citire USB/tokenului USB

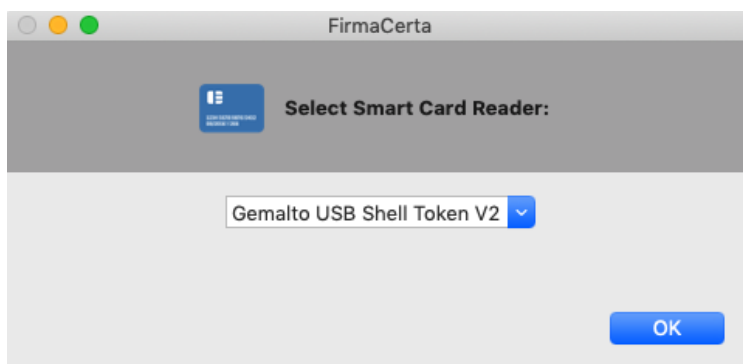


Figura 25 - Selectare: dispozitiv de citire a semnăturii



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

Notă:

Codul PIN a fost furnizat împreună cu plicul neinscripționat

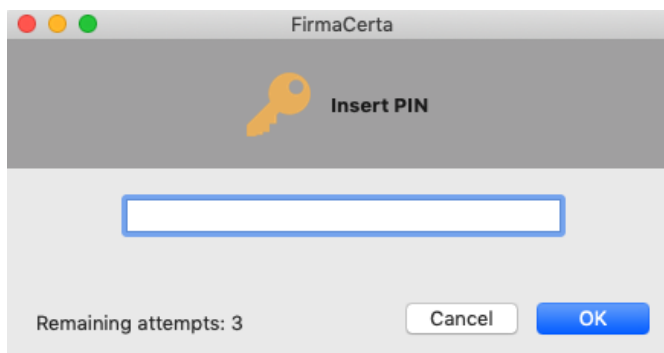


Figura 26 - Introducerea codului PIN

Așteptați terminarea procesării și apăsați **OK** pentru a finaliza operațiunea de semnare.



Figura 27 - Încheierea procesului de semnare



6.2 ANEXA B: MODUL DE CONTRASEMNARE A UNUI DOCUMENT

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).

În exemplul următor, a fost creat anterior un folder specific pentru fișierele semnate digital; selectați Signed Documents (Documente semnate) și dați clic pe **Open** (Deschidere).

Notă: operațiunea de contrasemnare este posibilă numai pentru fișierul semnat digital în format .p7m

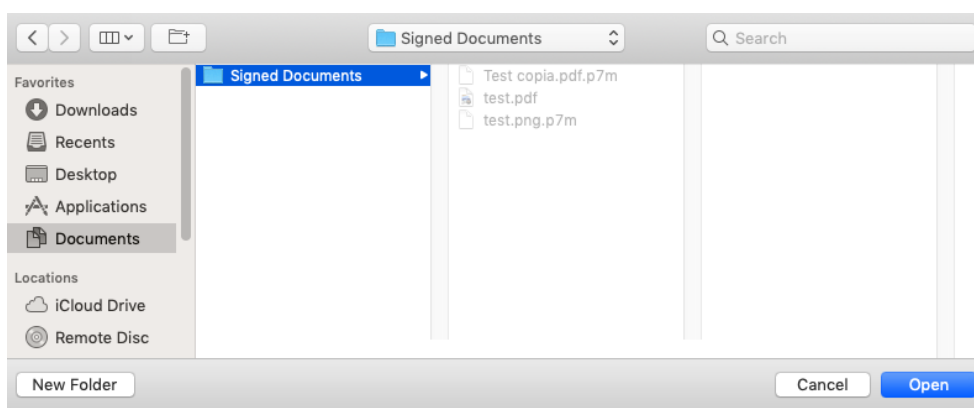


Figura 28 - Selectarea folderului de destinație

6.2.1 CONFIRMAREA PROCESULUI DE SEMNARE

Confirmarea aplicării semnăturii.

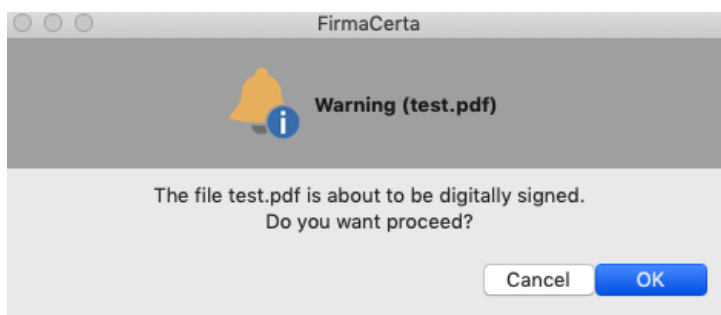


Figura 29 - Confirmarea procesului



Selectarea dispozitivului de citire
USB/tokenului USB

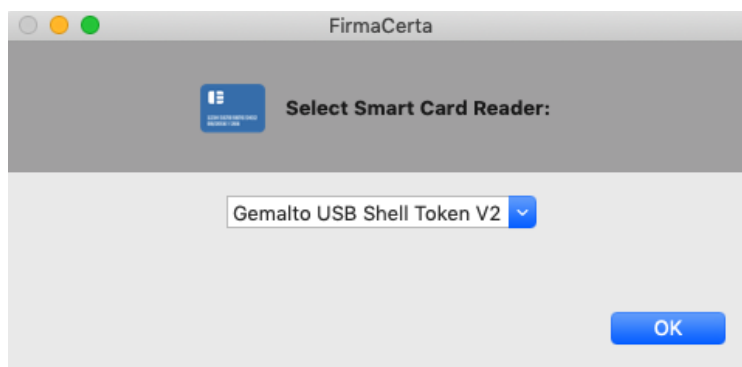


Figura 30 - Selectarea dispozitivului de citire a semnăturii

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

Notă:

Codul PIN a fost furnizat împreună cu plicul
neinscripționat

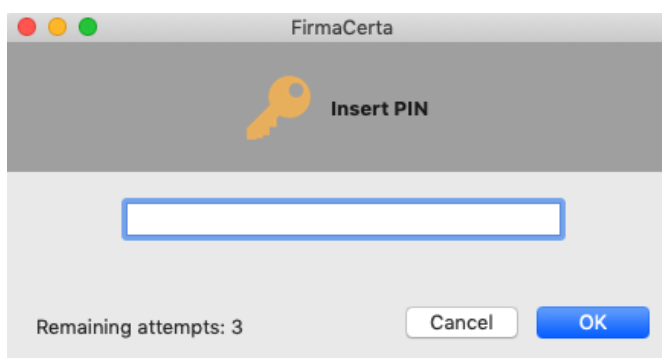


Figura 31 - Introducerea codului PIN

Așteptați terminarea procesării și apăsați **OK** pentru a finaliza operațiunea de semnare.



Figura 32 – Finalizarea procesului de semnare



6.3 ANEXA C: CONFIGURAREA PARAMETRILOR DE MARCARE TEMPORALĂ

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

ATENȚIE: Semnătura digitală nu include serviciul de marcare temporală; marcasele temporale pot fi achiziționate din magazinul nostru.

Pentru a configura serviciul de marcare temporală, deschideți FirmaCerta Software > Utility > Timestamp Options (Software FirmaCerta > Utilitar > Opțiuni de marcare temporală)

Deschideți FirmaCerta > Tools > Options > Timestamps (FirmaCerta > Instrumente > Opțiuni > Marcaje temporale)

- 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**.
- Dacă setați opțiunea „Do not ask timestamp service parameters” (Nu se solicită parametrii serviciului de marcare temporală), nu va fi necesară confirmarea datelor în timpul procesului de marcare temporală.

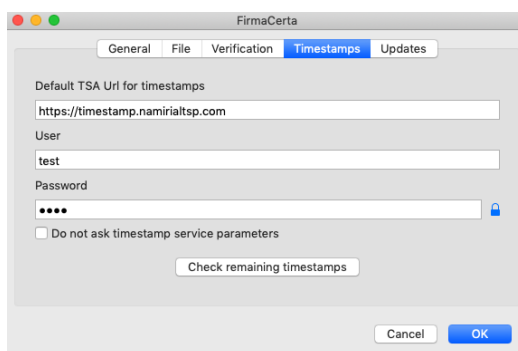


Figura 33 - Configurarea marcajelor temporale

- **Notă:** 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 marcasele temporale disponibile) verifică marcasele temporale rămase (în cazul în care interogarea eșuează, trebuie să verificați introducerea corectă a acreditărilor).

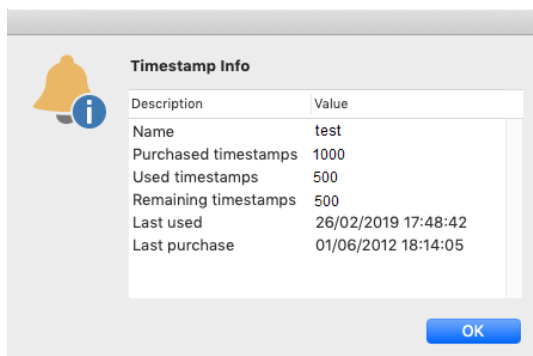


Figura 34 - Verificarea marcajelor temporale disponibile



6.3.1 ANEXA C1: MODUL DE MARCARE TEMPORALĂ A UNUI FIȘIER

După încărcarea fișierului care urmează să fie marcat temporal și dacă dați clic pe funcția **Timestamp** (Marcaj temporal), utilizatorul va fi rugat să selecteze un folder de destinație pentru a salva documentul.

În exemplul următor, a fost creat anterior un folder specific pentru fișierele semnate digital; selectați **Timestamped Documents** (Documente marcate temporal) și dați clic pe **Open** (Deschidere).

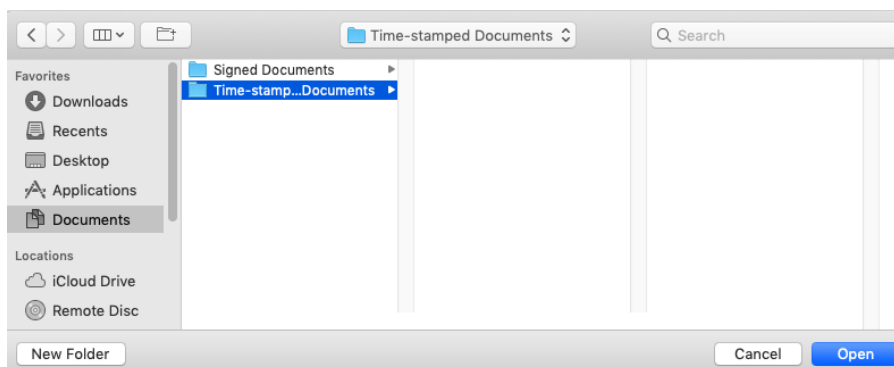


Figura 35 - Selectarea folderului de destinație

Selectați formatul pentru marcarea documentului.

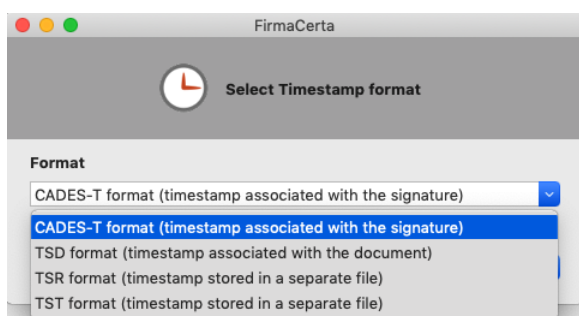


Figura 36 - Selectarea formatului de marcare temporală

.TSD (TimeStamp Document): este formatul standard care contine atât marcajul temporal, cât și fișierul original care urmează să fie marcat temporal, deci permite verificarea acurateții marcajului temporal și a conținutului fișierului original. Marcajul temporal este asociat cu documentul.

.TSR (TimeStamp Response): este similar cu formatul .TST, dar, în plus, cu codul de răspuns de la serverul de marcare temporală al Autorității de certificare. Testul IT, obținut datorită verificării, se referă numai la acuratețea marcajului temporal, în timp ce este necesar să aveți fișierul original pentru a verifica relația dintre acesta și fișierul .tsr.

.TST (TimeStamp Token): este un fișier care contine amprenta documentului sau fișierul marcat, nu conținutul documentului în sine.

CADES-T sau **PADES-T:** demonstrează că semnătura a existat într-adevăr, la o anumită dată/oră. Marcajul temporal este asociat cu o semnătură unică și nu poate fi separat.



Atenție: dacă documentul a fost deja semnat și doriți să introduceți marcajul temporal în acesta, software-ul permite alegerea **formatului CADES-T** (pentru fișierul .p7m) și a **formatului PADES-T** (pentru fișierul .pdf).

Exemplu: marcajul temporal al unui fișier .p7m

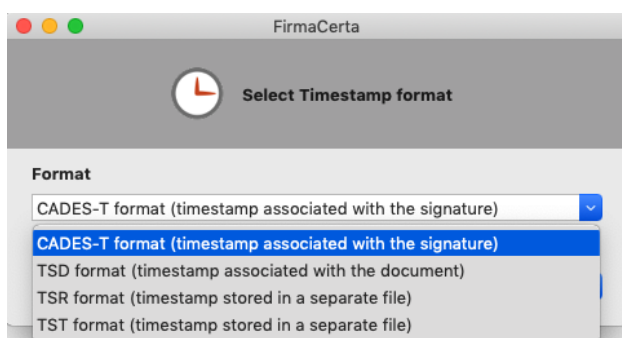


Figura 37 – Selectarea formatului marcajului temporal pentru fișierul .p7m

Exemplu: marcajul temporal al unui fișier .pdf

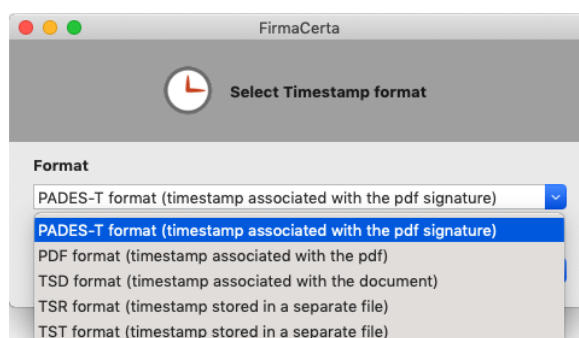


Figura 38 – Selectarea formatului marcajului temporal pentru fișierul .pdf

6.3.1.1 CONFIGURAREA PARAMETRILOR DE MARCARE TEMPORALĂ

Trebuie să configurați parametrii pentru serviciul Timestamp (Marcaj temporal).

Notă:

- Dacă s-a realizat configurarea marcajului temporal, câmpurile **URL**, **Username (Nume de utilizator)** și **Password (Parolă)** vor fi completate.
- Dacă setați opțiunea „**Do not ask access parameters anymore**” (Nu se mai solicită parametrii de acces), confirmarea datelor în timpul procesului de marcare temporală nu va fi necesară; *pentru a seta din nou această opțiune, va trebui să modificați setările din [Options Timestamps](#) (Opțiuni marcaje temporale).*

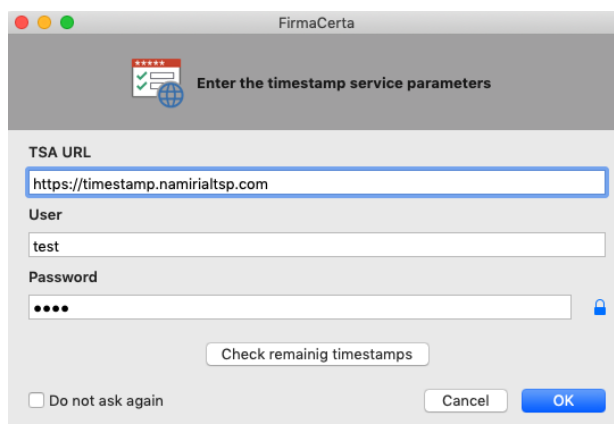


Figura 39 - Introducerea parametrilor de marcare temporală



6.3.1.2 ÎNCHEIEREA PROCESULUI DE MARCARE TEMPORALĂ

Confirmarea aplicării semnăturii.

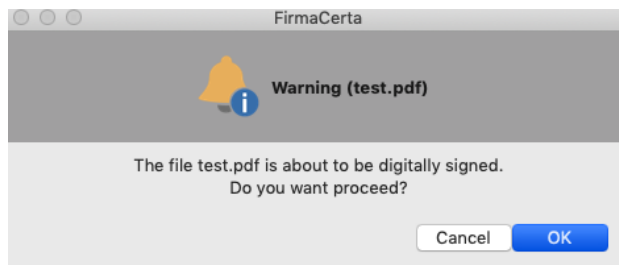


Figura 40 - Confirmarea procesului de semnare

Selectarea dispozitivului de citire USB/tokenului USB

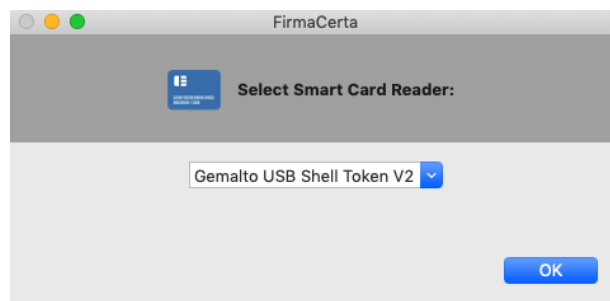


Figura 41 - Selectarea dispozitivului de citire a semnăturii

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

Notă:

Codul PIN a fost furnizat împreună cu plicul neinscripționat

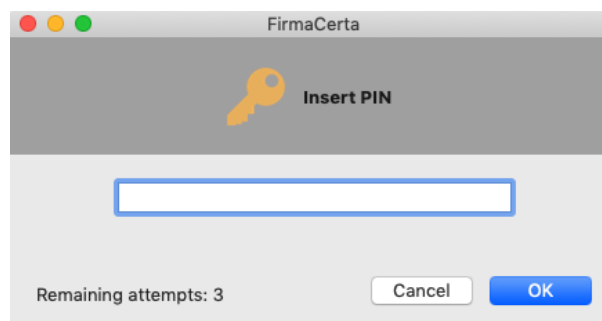


Figura 42 - Introducerea codului PIN

Așteptați terminarea procesării și apăsați **OK** pentru a finaliza operațiunea de semnare.

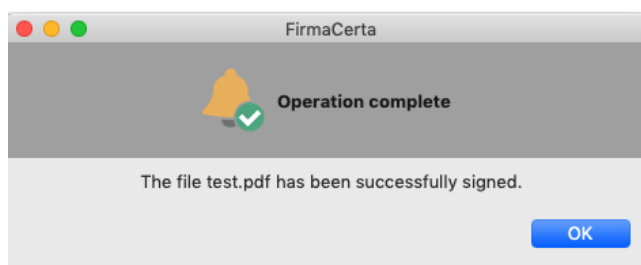


Figura 43 - Procesul de semnare a fost finalizat



6.3.2 ANEXA C2: MODUL DE SEMNARE ȘI APLICARE A MARCAJULUI TEMPORAL ÎNTR-UN DOCUMENT

După încărcarea fișierului, selectați această funcție pentru a semna și a aplica marcajul temporal într-o singură operațiune. După semnarea și marcarea temporală a fișierului, formatul va fi **CADES-T** (de exemplu, filename.pdf.P7M). Cu un format CADES-T (format implicit) sau PAdES-T (format disponibil numai pentru documentul PDF), marcajul temporal este asociat cu o semnătură unică și nu poate fi separat.

După încărcarea fișierului și selectarea funcției **Sign and Timestamp** (Semnare și marcarea temporală), utilizatorul va trebui să selecteze un folder de destinație pentru a salva fișierul.

*În exemplul următor, a fost creat anterior un folder specific pentru fișierele semnate digital; selectați Timestamped Documents (Documente marcate temporal) și dați clic pe **Open** (Deschidere).*

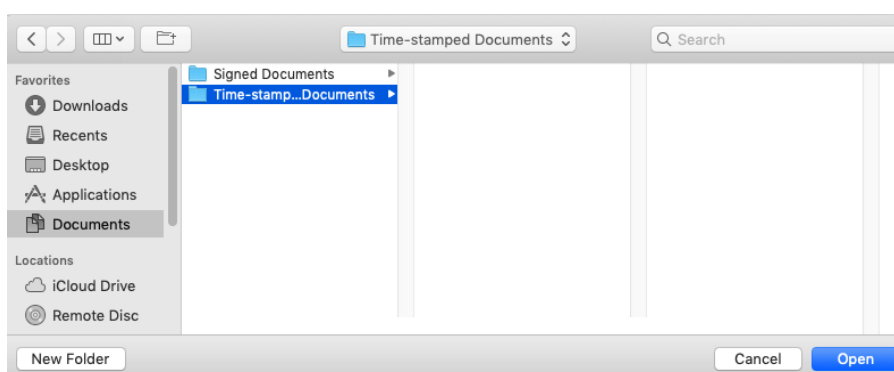


Figura 44 - Selectarea folderului de destinație

6.3.2.1 SELECTAREA FORMATULUI SEMNĂTURII

Selectați formatul CADES pentru a semna fișierul în format .p7m

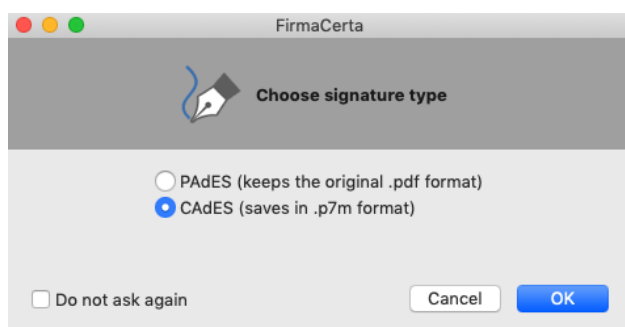


Figura 45 - Selectarea formatului CADES

Selectați formatul PAdES pentru a semna fișierul în format .pdf

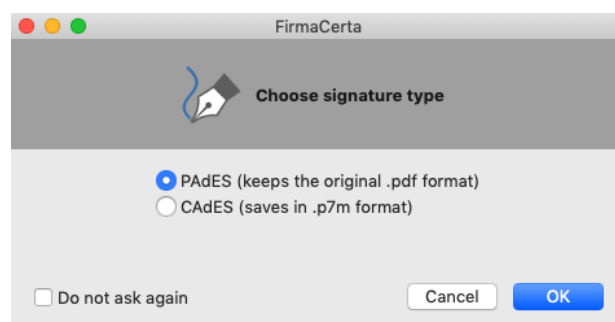


Figura 46 - Selectarea formatului PAdES

Notă: selectarea formatului semnăturii este disponibilă numai pentru .pdf, pentru orice alt format software-ul va aplica automat extensia .p7m

Bifarea preferinței **Do not ask anymore** (Nu mai întreba) va fi setată automat; pentru eliminare, va trebui să modificați setările din [Options](#) (Opțiuni).



6.3.2.2 SELECT SIGNATURE MOTIVATION (ONLY PDF FILE) (SE SELECTEAZĂ MOTIVUL SEMNĂRII (NUMAI FIȘIER PDF))

Această funcție îi permite utilizatorului să adauge informații opționale, precum *motivation* (motiv), *location* (locatie), *contact information* (informații de contact) înainte de a finaliza semnarea documentului.

Notă: Această funcție este disponibilă numai pentru documentele .pdf.
Utilizarea acestei funcții este la alegerea utilizatorului, ca Optional Operation (Operațiune opțională).

The dialog box is titled 'FirmaCerta' and contains the text 'Specify some additional information that will be displayed in the document signature (optional)'. It has three input fields: 'Reason', 'Location', and 'Contact Info'. At the bottom, there is a checkbox labeled 'Do not ask again', a 'Cancel' button, and an 'OK' button.

Figura 47 - Informații despre semnătură

6.3.2.3 CONFIGURAREA PARAMETRILOR DE MARCARE TEMPORALĂ

Trebuie să configurați parametrii pentru serviciul Timestamp (Marcaj temporal).

Notă:

- Dacă s-a realizat configurarea marcajului temporal, câmpurile **URL**, **Username (Nume de utilizator)** și **Password (Parolă)** vor fi completate.
- Dacă setați opțiunea „**Do not ask access parameters anymore**” (Nu se mai solicită parametrii de acces), confirmarea datelor în timpul procesului de marcare temporală nu va fi necesară; *pentru a seta din nou această opțiune, va trebui să modificați setările din [Option Timestamps](#) (Opțiune marcaje temporale).*

The dialog box is titled 'FirmaCerta' and contains the text 'Enter the timestamp service parameters'. It has three input fields: 'TSA URL' (containing 'https://timestamp.namirialtsp.com'), 'User' (containing 'test'), and 'Password' (masked with dots). There is a 'Check remainig timestamps' button. At the bottom, there is a checkbox labeled 'Do not ask again', a 'Cancel' button, and an 'OK' button.

Figura 48 - Parametrii marcajelor temporale



6.3.2.4 ÎNCHEIEREA PROCESULUI DE SEMNARE ȘI DE MARCARE TEMPORALĂ

Confirmarea aplicării semnăturii.

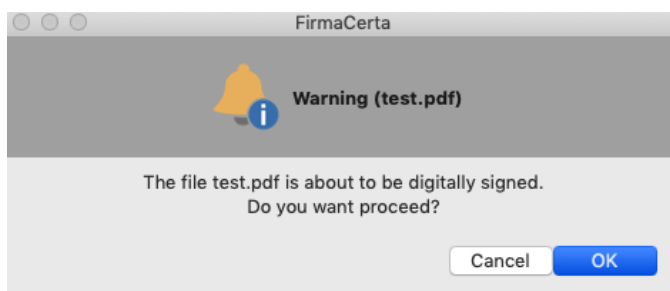


Figura 49 - Confirmarea procesului de semnare

Selectarea dispozitivului de citire USB/tokenului USB

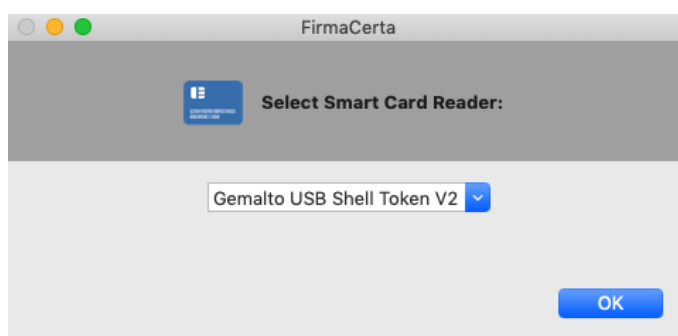


Figura 50 - Selectarea dispozitivului de citire a semnăturii

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

Notă:

Codul PIN a fost furnizat împreună cu plicul neinscripționat

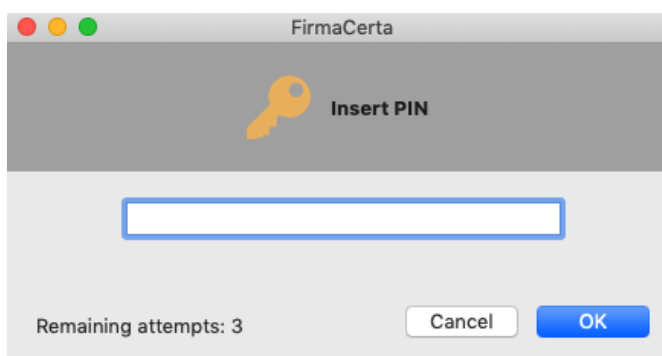


Figura 51 - Introducerea codului PIN

Așteptați să treacă timpul de procesare și apăsați pe **OK** pentru a finaliza procesul de semnare.

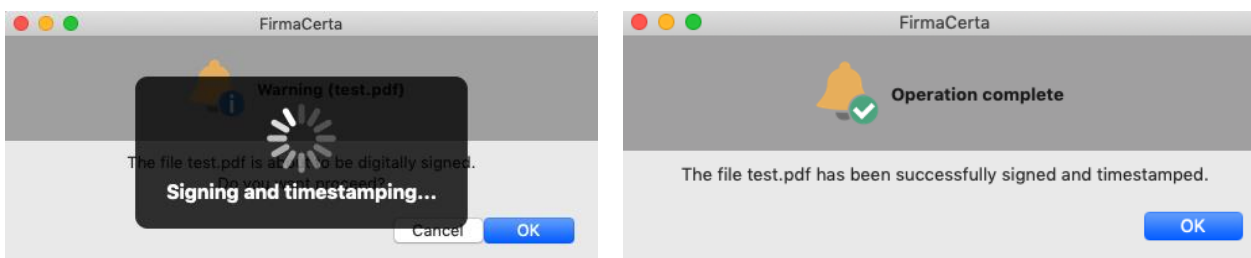


Figura 52 - Încheierea procesului de semnare



6.4 ANEXA D: MODUL DE VERIFICARE A UNUI FIȘIER

După încărcarea fișierului de verificat și dacă dați clic pe funcția **Verify** (Verificare) se va deschide o fereastră rezumativă.

Notă:

Dacă apare mesajul ***the signature certificate has not been verified*** (certificatul de semnătură nu a fost verificat), înseamnă că verificarea nu a fost inițiată automat (pentru a activa automat verificarea la deschiderea fișierului va fi necesară modificarea manuală, în [Verification Options](#) (Opțiuni de verificare)); în caz contrar, verificarea semnăturilor trebuie inițiată manual dând clic pe butonul **Verify** (Verificare).

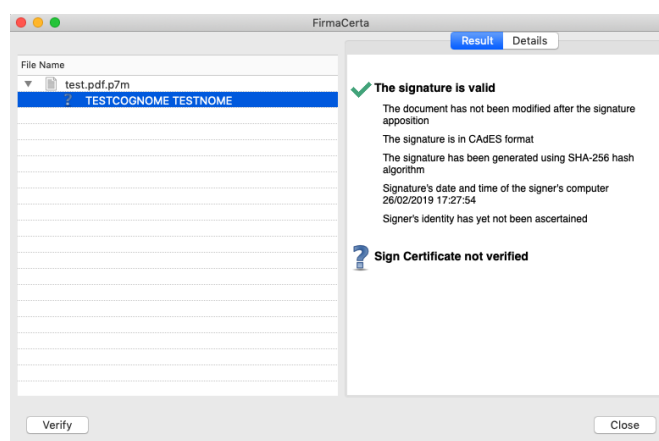


Figura 53 - Verificarea

Exemplu: În acest caz, fișierul semnat este test.png.p7m și a fost semnat de utilizatorul TESTCOGNOME TESTNOME.

În coloana din stânga puteți găsi fișierul semnat digital și semnatarul.

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;

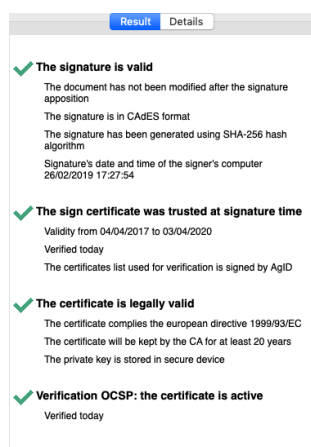


Figura 54 - Verify Result (Verificare rezultat)

Identifier	Value
TYPOLOGY	
Description	Sign Certificate
Validity	From 04/04/2017 to 03/04/20...
Algorithm	SHA-256
ISSUER	
Certification Authority Co...	IT
Organization	Namirial S.p.A./02046570426
Organization Unit	Certification Authority
Certification Authority	Namirial CA Firma Qualificata
HOLDER	
Signer Country	IT
Organization	NON PRESENTE
Surname	TESTCOGNOME
Name	TESTNOME
Signer Tax Code	IT:TSTTTN80A01A271U
Signer	TESTCOGNOME TESTNOME
Identification Code	LOTT2017032272641608
QC STATEMENTS	
Compliance	present
SSCD	present
Retention period	20

Figura 55 - Verify Details (Verificare detalii)



6.5 ANEXA E: REÎNNOIREA CERTIFICATULUI

Înainte de a continua, asigurați-vă că ați instalat software-ul de semnare [FirmaCerta](#), actualizat corect. Dacă utilizați un proxy, vă rugăm să solicitați configurația parametrilor de la administratorul de rețea.

6.5.1 CONFIGURAREA SERVERULUI PROXY

Deschideți software-ul Firmacerta și dați clic pe bara de instrumente: Tools> Certificate Renewal (Instrumente > Reînnoire certificat), confirmați termenii și dați clic pe **Next** (Înainte).

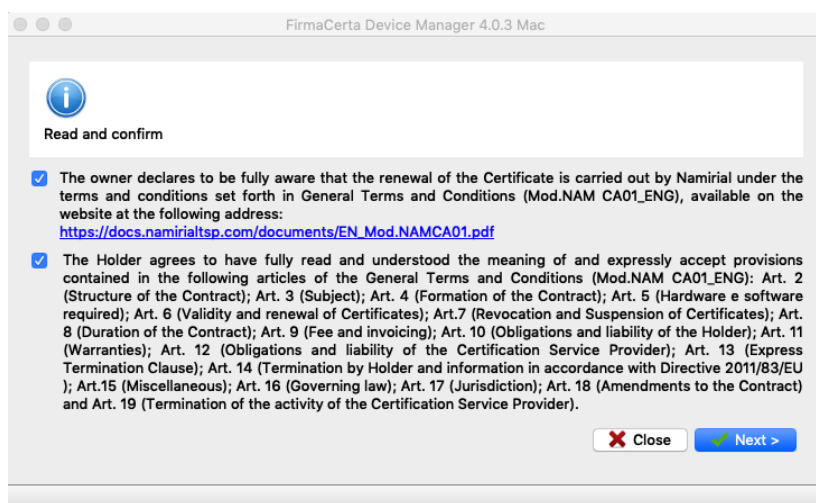


Figura 56 - Termeni și condiții

Selectați **Firmacerta DeviceManager > Preferences** (Manager dispozitive Firmacerta > Preferințe) și continuați cu configurarea proxy (pentru parametri, contactați administratorul de rețea) Apoi dați clic pe **SAVE** (SALVARE).



Figura 57 - Configurarea serverului proxy



6.5.2 REÎNNOIREA SMARTCARDULUI ȘI TOKENULUI

Deschideți FirmaCerta cu dispozitivul de semnare conectat la computer, apoi dați clic pe *Tools > Certificates Renewal* (Instrumente > Reînnoire certificate).

Citiți și confirmați termenii restrictivi și dați clic pe **NEXT** (ÎNAINTE)

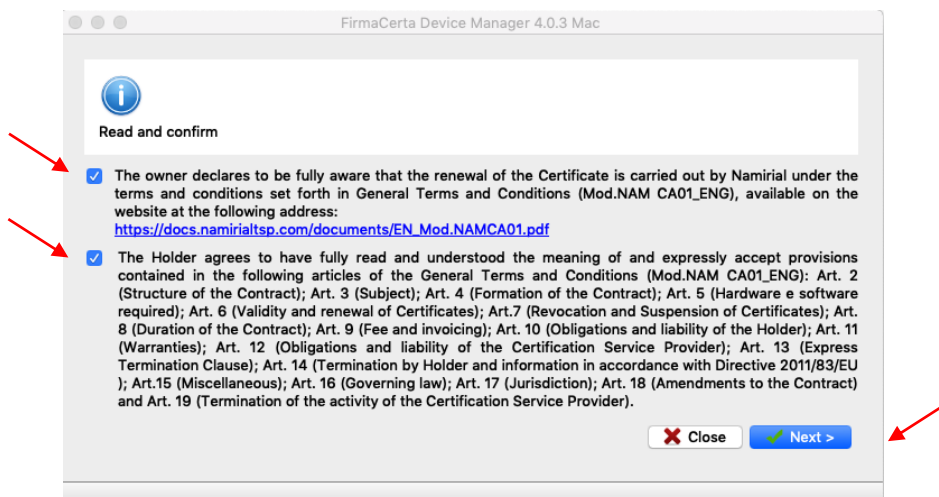


Figura 58 - Termeni și condiții

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

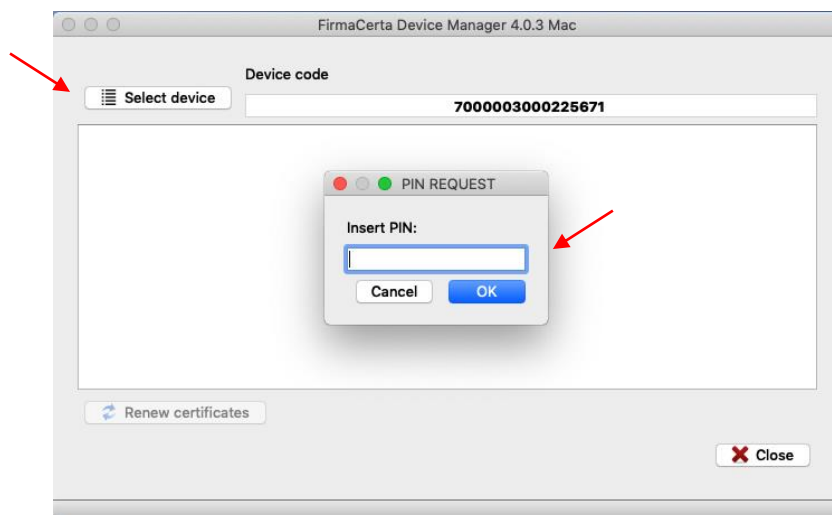


Figura 59 - Selectarea dispozitivului de semnare și introducerea codului PIN



Instrumentul Device Manager (Manager dispozitive) 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.

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

Apăsați Yes (Da), dacă doriți să vedeți contractul, în caz contrar, apăsați No (Nu).

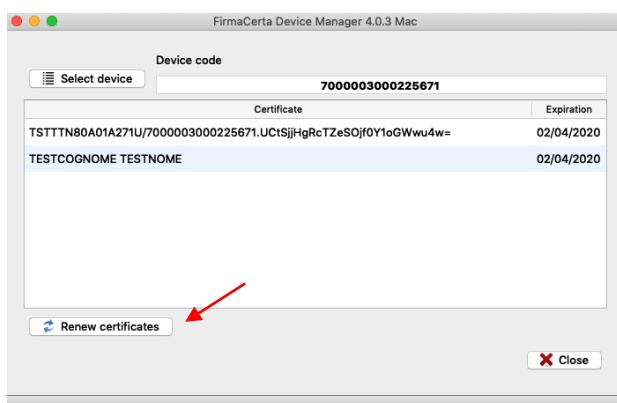


Figura 60 - Renew Certificates (Reînnoire certificate)

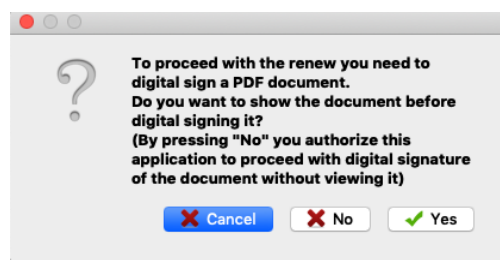


Figura 61 - Cerere de vizualizare a contractului înainte de semnarea acestuia

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

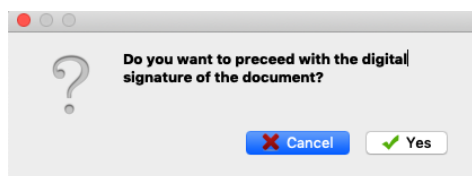


Figura 62 - Confirmarea procesului de semnare

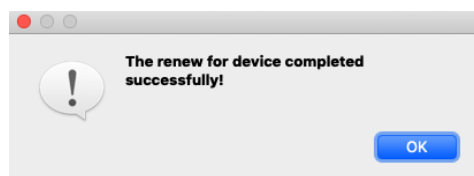


Figura 63 - Reînnoirea dispozitivului de semnare a fost finalizată



6.6 ANEXA F: GHID DE SEMNARE LA DISTANȚĂ

6.6.1 MODUL DE SEMNARE A UNUI FIȘIER

După încărcarea fișierului care urmează să fie semnat și dacă dați clic pe funcția **Sign** (Semnare), utilizatorul va fi rugat să selecteze un folder de destinație pentru a salva documentul semnat.

În exemplul următor, a fost creat anterior un folder specific pentru fișierele semnate digital; selectați *Signed Documents* (Documente semnate) și dați clic pe **Open** (Deschidere).

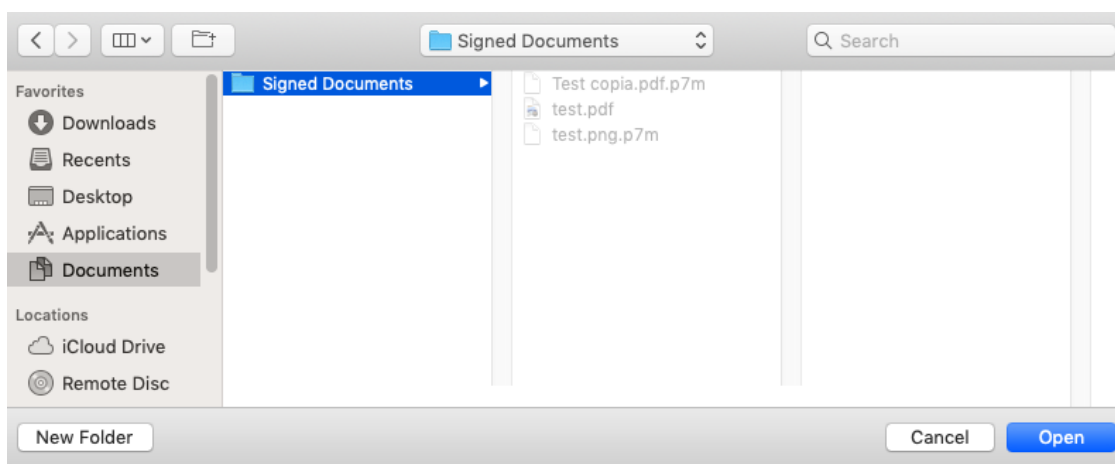


Figura 64 - Selectarea folderului de destinație

6.6.1.1 SELECTAREA FORMATULUI SEMNĂTURII

Selectați formatul CADES pentru a semna fișierul în format .p7m

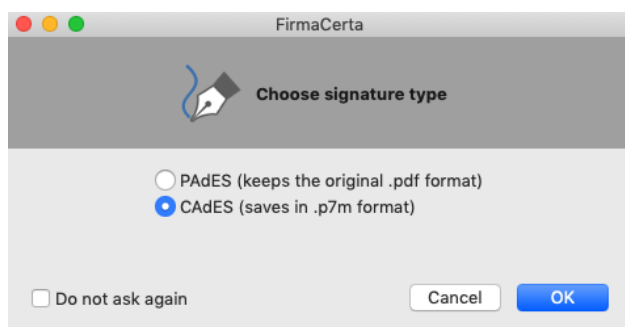


Figura 65 - Selectare: Format CADES

Selectați formatul PAdES pentru a semna fișierul în format .pdf

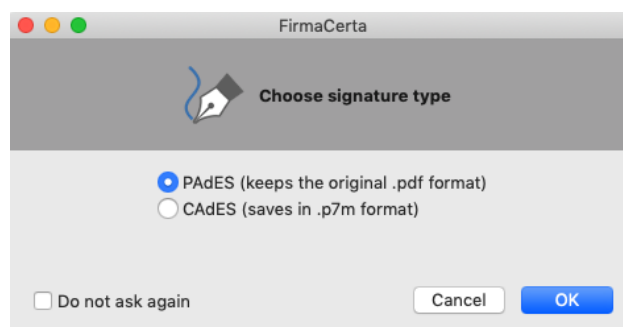


Figura 66 - Selectare: Format PAdES

Notă: selectarea formatului semnăturii este disponibilă numai pentru .pdf, pentru orice alt format software-ul va aplica automat extensia .p7m

Bifați preferința **Do not ask anymore** (Nu mai întreba), care va fi setată automat să nu mai afișeze mesajul și va trebui să modificați setările din [Options](#) (Opțiuni)



6.6.1.2 SELECT SIGNATURE MOTIVATION (ONLY PDF FILE) (SE SELECTEAZĂ MOTIVUL SEMNĂRII (NUMAI FIȘIER PDF))

Această funcție îi permite utilizatorului să adauge informații opționale, precum *motivation* (motiv), *location* (locatie), *contact information* (informații de contact) înainte de a finaliza semnarea documentului.

Notă: Această funcție este disponibilă numai pentru documentele .p7m.
Utilizarea acestei funcții este la alegerea utilizatorului, ca Optional Operation (Operațiune opțională).

Figura 67 - Informații despre semnătură

6.6.1.3 ÎNCHEIEREA PROCESULUI DE SEMNARE

Confirmarea aplicării semnăturii.

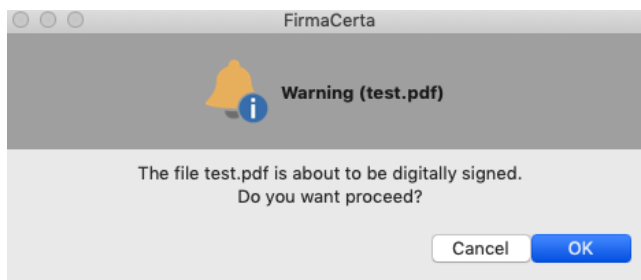


Figura 68 - Confirmarea procesului de semnare

Selectați **Remote Signature** (Semnătură la distanță) din meniul vertical

Notă: selectarea dispozitivelor va fi disponibilă numai dacă un cititor USB sau un token USB sunt conectate la computer.

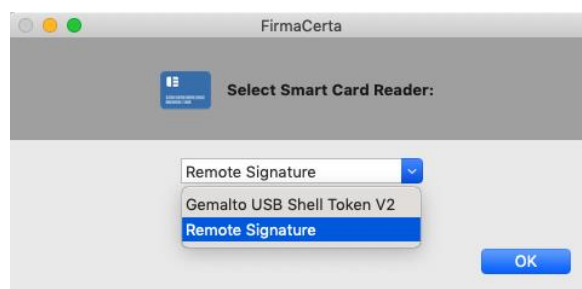


Figura 69 - Selectarea dispozitivului de citire a semnăturii

Pentru a finaliza procesul de semnare, urmați instrucțiunile în funcție de tipul de OTP atribuit în timpul înregistrării:

- [Procedura OTP virtual](#)
- [Procedura OTP SMS](#)
- Procedura OTP [HARDWARE](#)



6.6.2 PROCEDURA OTP VIRTUAL: NAMIRIAL OTP

6.6.2.1 INTRODUCERE ÎN APLICAȚIA PENTRU MOBIL 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.

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.

6.6.2.2 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 deschide acestea.

6.6.2.3 ACTIVAREA NAMIRIAL OTP

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.

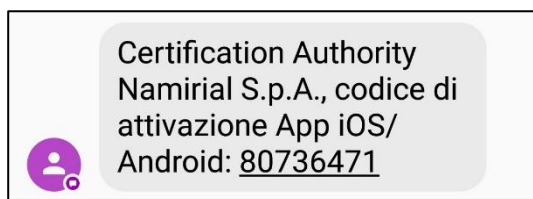


Figura 1 - SMS de activare aplicație



6.6.2.4 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 70 – Interfața Namirial OTP

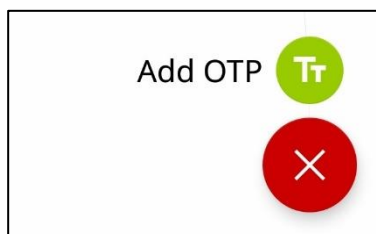


Figura 71 – Add OTP (Adăugare OTP)

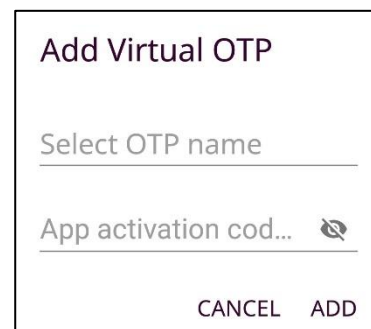


Figura 72 – Activarea OTP

6.6.2.5 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 73 – Add OTP (Adăugare OTP)

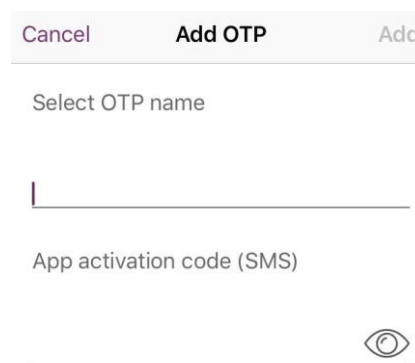


Figura 74 – Activarea OTP



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.

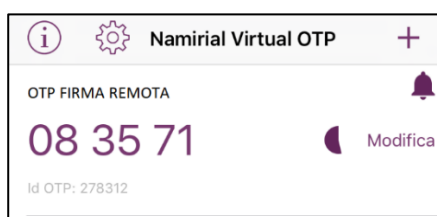


Figura 75 - Generator OTP virtual

6.6.2.6 CONFIGURAREA PARAMETRILOR DE SEMNARE LA DISTANȚĂ

Pentru a recupera datele certificatului de semnătură la distanță este necesar să introduceți **Username** (Nume de utilizator) atribuit în timpul înregistrării serviciului.

RECUPERAREA ACREDITĂRIILOR: În cazul pierderii numelui de utilizator, vă rugăm să accesați spațiul privat <https://portal.namirialtsp.com> și să dați clic pe „I don't remember the username” (Am uitat numele de utilizator) și să urmați instrucțiunile.

Dacă problema persistă, acreditările pot fi solicitate prin trimiterea unui e-mail la: helpdesk@firmacerta.it, cu menționarea codului fiscal al posesorului de semnătură.

Dacă dați clic pe tasta **Recover** (Recuperare), câmpurile **virtual devices** (dispozitive virtuale) și **OTP type** (tip OTP) vor fi completate automat.

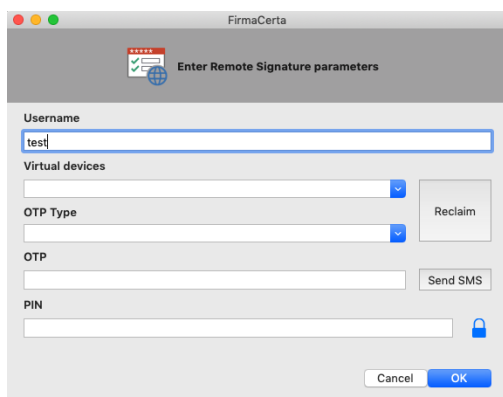


Figura 76 - Parametri de semnare la distanță: username (nume de utilizator)

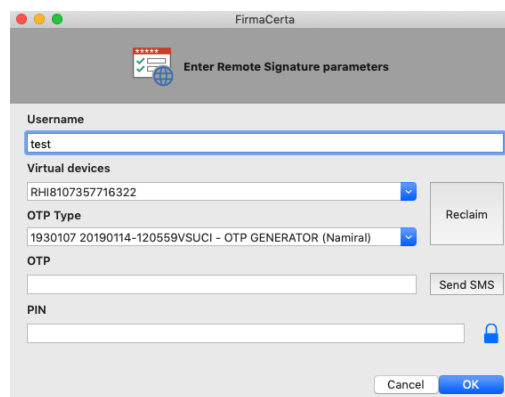


Figura 77 - Parametri de semnare la distanță: devices recovery (recuperare dispozitive)



Introduceți codul PIN în câmpul pentru PIN, primit în plicul neînscrisționat digital sau din hârtie
Deschideți aplicația mobilă și introduceți codul indicat pe afișaj, în câmpul OTP
Finalizați procesul dând clic pe **OK**.

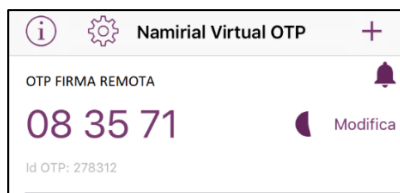


Figura 78 - Generator OTP virtual

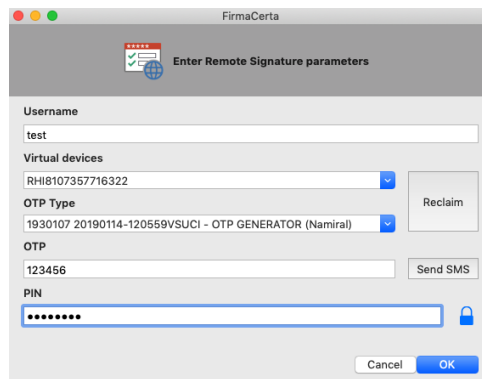
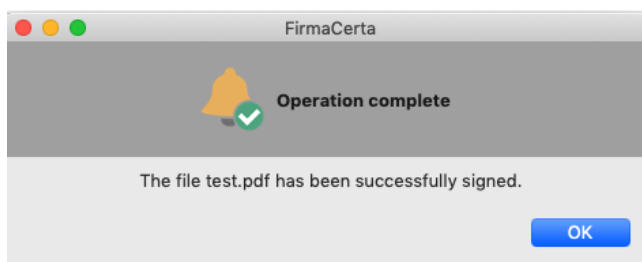


Figura 79 - Parametri de semnare la distanță: PIN

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.



Figura 80 - Încheierea procesului de semnare





6.6.3 PROCEDURA OTP SMS

6.6.3.1 CONFIGURAREA PARAMETRILOR DE SEMNARE LA DISTANȚĂ

Pentru a recupera datele certificatului de semnătură la distanță este necesar să introduceți **Username** (Nume de utilizator) atribuit în timpul înregistrării serviciului.

RECUPERAREA ACREDITĂRIILOR: În cazul pierderii numelui de utilizator, vă rugăm să accesați spațiul privat <https://portal.namirialtsp.com> și să dați clic pe „I don't remember the username” (Am uitat numele de utilizator) și să urmați instrucțiunile.

Dacă problema persistă, acreditările pot fi solicitate prin trimiterea unui e-mail la: helpdesk@firmacerta.it, cu menționarea codului fiscal al posesorului de semnătură.

Dacă dați clic pe tasta **Reclaim** (Recuperare), câmpurile **virtual devices** (dispozitive virtuale) și **OTP type** (tip OTP) vor fi completate automat.

Figura 2 - Parametri de semnare la distanță: introducerea numelui de utilizator

Figura 3 - Parametri de semnare la distanță: recuperarea datelor

Introduceți codul PIN în câmpul pentru PIN, primit în plicul neinscripționat digital sau din hârtie

Dați clic pe Send SMS (Trimitere SMS) și introduceți codul primit în câmpul OTP

Finalizați procesul dând clic pe **OK**.

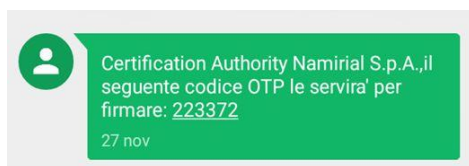


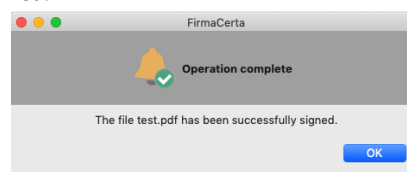
Figura 4 - OTP SMS

Figura 5 - Introducerea codului PIN semnătură la distanță

Așteptați terminarea procesării și apăsați OK pentru a finaliza operațiunea.



Figura 6 - Operațiune finalizată





6.6.4 PROCEDURA HARDWARE OTP

6.6.4.1 ACTIVARE OTP

Accesați [Private User Area](#) (Spațiul privat al utilizatorului), prin introducerea acreditărilor Username (Nume de utilizator) și Password (Parolă) primite prin e-mail, la adresa de e-mail furnizată în timpul înregistrării.

RECUPERAREA ACREDITĂRIILOR: În cazul pierderii numelui de utilizator/parolei, vă rugăm să accesați spațiul privat <https://portal.namirialtsp.com> și să dați clic pe „I don't remember the username” (Am uitat numele de utilizator) sau pe „I don't remember the password” (Am uitat parola) și să urmați instrucțiunile.

Dacă problema persistă, acreditările pot fi solicitate prin trimiterea unui e-mail la: helpdesk@firmacerta.it, cu menționarea codului fiscal al posesorului de semnătură.

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

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).

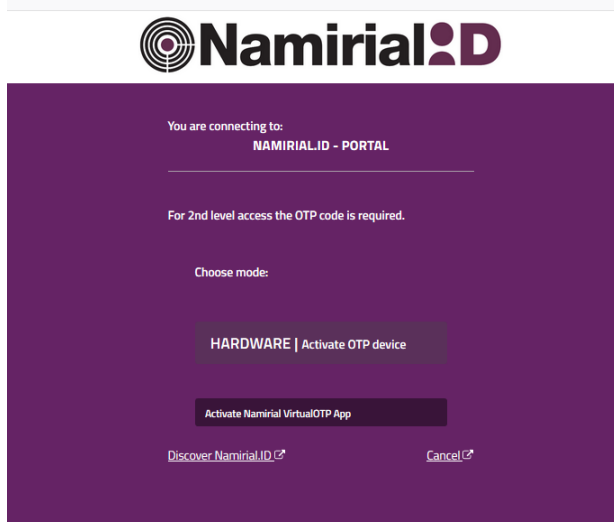


Figura 7 – Activarea OTP hardware



Figura 8 – Accesarea OTP hardware



6.6.4.2 CONFIGURAREA PARAMETRILOR DE SEMNARE LA DISTANȚĂ

Pentru a recupera datele certificatului de semnătură la distanță este necesar să introduceți **Username** (Nume de utilizator) atribuit în timpul înregistrării serviciului.

RECUPERAREA ACREDITĂRIILOR: În cazul pierderii numelui de utilizator, vă rugăm să accesați spațiul privat <https://portal.namirialtsp.com> și să dați clic pe „I don't remember the username” (Am uitat numele de utilizator) și să urmați instrucțiunile.

Dacă problema persistă, acreditările pot fi solicitate prin trimiterea unui e-mail la: helpdesk@firmacerta.it, cu menționarea codului fiscal al posesorului de semnătură.

Dacă dați clic pe tasta **Recover** (Recuperare), câmpurile **virtual devices** (dispozitive virtuale) și **OTP type** (tip OTP) vor fi completate automat.

Figura 9 - Parametri de semnare la distanță: introducerea numelui de utilizator

Figura 10 - Parametri de semnare la distanță: recuperarea datelor de utilizator

Introduceți codul PIN în câmpul pentru PIN, primit în plicul neinscripționat digital sau din hârtie

Generați codul OTP folosind dispozitivul hardware atribuit, apoi introduceți-l în câmpul OTP

Finalizați procesul dând clic pe **OK**.

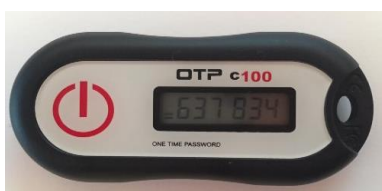


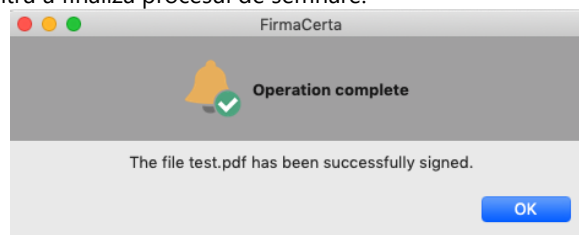
Figura 11 - OTP hardware

Figura 12 - Introducerea codului PIN

Așteptați să treacă timpul de procesare și apăsați pe **OK** pentru a finaliza procesul de semnare.



Figura 13 - Operațiune finalizată





6.7 ANEXA H: BIT4ID – MACOS

Descărcați și instalați Bit4id PKI Manager Driver Manager, la următorul [link](#):

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

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

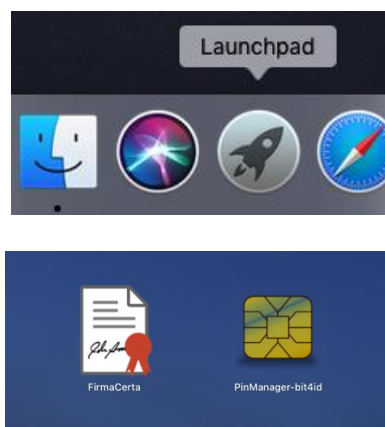
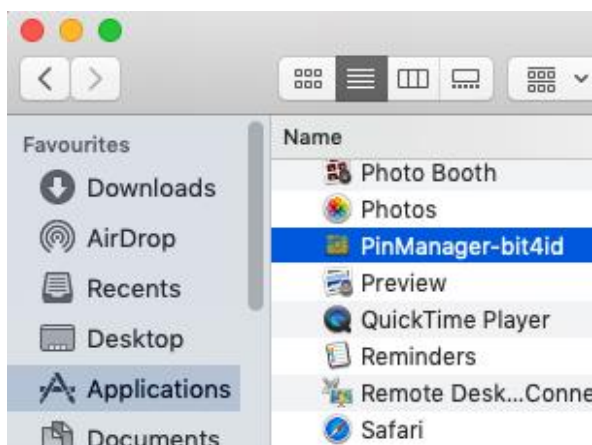


Figura 14 - PIN Manager: Deschidere

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**

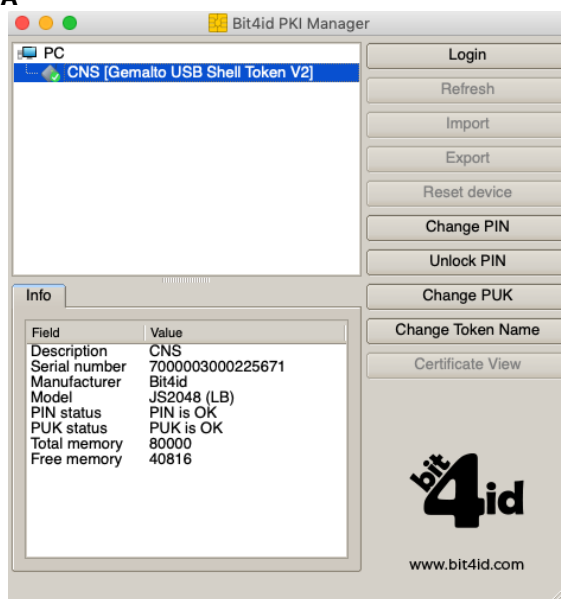


Figura 15 - Funcții avansate Bit4id PKI Manager



6.7.1 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).

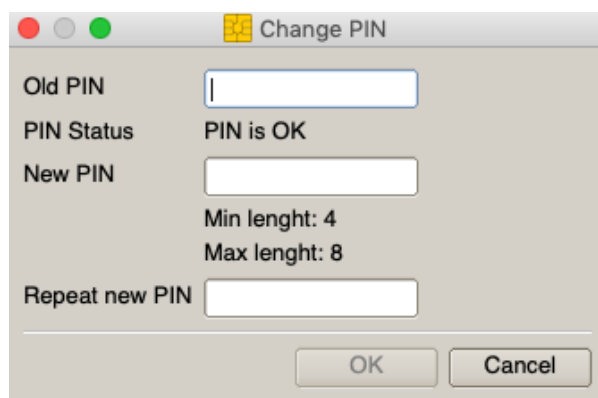


Figura 16 - Funcția de modificare a codului PIN

6.7.2 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.

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

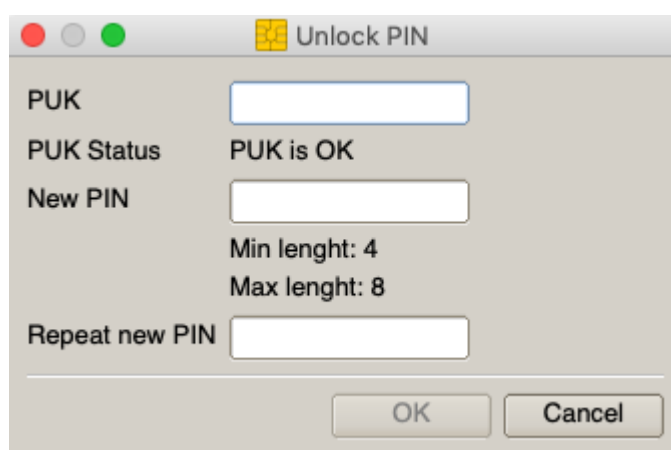


Figura 17 - Unlock PIN (Deblocare PIN)



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

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

Change PUK

Old PUK

PUK Status PUK is OK

New PUK

Min lenght: 4
Max lenght: 8

Repeat new PUK

OK Cancel

Figura 18 - Change PUK (Modificare PUK)



REFERINȚE

NUMĂR	DESCRIERE
[I]	<...>
[II]	<...>



INDEX TABELE

Tabelul 1 - Definiții și acronime	8
---	---

INDEX FIGURI

Figura 1 - Instalarea Firmacerta	9
Figura 2 - Avertisment: dezvoltator neidentificat	9
Figura 3 - Soluția 1a de instalare FirmaCerta	10
Figura 4 - Soluția 1b de instalare FirmaCerta	10
Figura 5 - Soluția 2 de instalare FirmaCerta	10
Figura 6 - Interfața grafică FirmaCerta	11
Figura 7 - FirmaCerta: Bara de instrumente	11
Figura 8 - Afișarea certificatelor în dispozitivul de semnare	13
Figura 9 - Exportul certificatelor	13
Figura 10 - Introducerea codului PIN pentru verificarea dispozitivului de semnare	14
Figura 11 - Rezultatul verificării dispozitivului	14
Figura 12 - Change PIN (Modificare PIN)	14
Figura 13 - Unlock PIN (Deblocare PIN)	15
Figura 14 - Change PUK (Modificare PUK)	15
Figura 15 - Opțiuni: General (Generalități)	16
Figura 16 - Opțiuni: File (Fișier)	17
Figura 17 - Opțiuni: Verification (Verificare)	17
Figura 18 - Opțiuni: Timestamps (Marcaje temporale)	18
Figura 19 - Opțiuni: Updates (Actualizări)	18
Figura 20 - Selectarea folderului de destinație	19
Figura 21 - Selectare: Format CADES	19



Figura 22 - Selectare: Format PAdES	19
Figura 23 - Informații despre semnătură	20
Figura 24 - Confirmarea procesului de semnare	20
Figura 25 - Selectare: dispozitiv de citire a semnăturii	20
Figura 26 - Introducerea codului PIN	21
Figura 27 - Încheierea procesului de semnare	21
Figura 28 - Selectarea folderului de destinație	22
Figura 29 - Confirmarea procesului	22
Figura 30 - Selectarea dispozitivului de citire a semnăturii	23
Figura 31 - Introducerea codului PIN	23
Figura 32 - Finalizarea procesului de semnare	23
Figura 33 - Configurarea marcajelor temporale	24
Figura 34 - Verificarea marcajelor temporale disponibile	24
Figura 35 - Selectarea folderului de destinație	25
Figura 36 - Selectarea formatului de marcare temporală	25
Figura 37 - Selectarea formatului marcajului temporal pentru fișierul .p7m	26
Figura 38 - Selectarea formatului marcajului temporal pentru fișierul .pdf	26
Figura 39 - Introducerea parametrilor de marcare temporală	26
Figura 40 - Confirmarea procesului de semnare	27
Figura 41 - Selectarea dispozitivului de citire a semnăturii	27
Figura 42 - Introducerea codului PIN	27
Figura 43 - Procesul de semnare a fost finalizat	27
Figura 44 - Selectarea folderului de destinație	28
Figura 45 - Selectarea formatului CAdES	28
Figura 46 - Selectarea formatului PAdES	28



Figura 47 - Informații despre semnătură	29
Figura 48 - Parametrii marcajelor temporale	29
Figura 49 - Confirmarea procesului de semnare	30
Figura 50 - Selectarea dispozitivului de citire a semnăturii	30
Figura 51 - Introducerea codului PIN	30
Figura 52 - Încheierea procesului de semnare	30
Figura 53 - Verificarea	31
Figura 54 - Verify Result (Verificare rezultat)	31
Figura 55 - Verify Details (Verificare detalii)	31
Figura 56 - Termeni și condiții	32
Figura 57 - Configurarea serverului proxy	32
Figura 58 - Termeni și condiții	33
Figura 59 - Selectarea dispozitivului de semnare și introducerea codului PIN	33
Figura 60 - Renew Certificates (Reînnoire certificate)	34
Figura 61 - Cerere de vizualizare a contractului înainte de semnarea acestuia	34
Figura 62 - Confirmarea procesului de semnare	34
Figura 63 - Reînnoirea dispozitivului de semnare a fost finalizată	34
Figura 64 - Selectarea folderului de destinație	35
Figura 65 - Selectare: Format CAdES	35
Figura 66 - Selectare: Format PAdES	35
Figura 67 - Informații despre semnătură	36
Figura 68 - Confirmarea procesului de semnare	36
Figura 69 - Selectarea dispozitivului de citire a semnăturii	36
Figura 70 – Interfața Namirial OTP	38
Figura 71 – Add OTP (Adăugare OTP)	38



Figura 72 – Activarea OTP.....	38
Figura 73 – Add OTP (Adăugare OTP)	38
Figura 74 – Activarea OTP.....	38
Figura 75 - Generator OTP virtual.....	39
Figura 76 - Parametri de semnare la distanță: username (nume de utilizator)	39
Figura 77 - Parametri de semnare la distanță: devices recovery (recuperare dispozitive).....	39
Figura 78 - Generator OTP virtual.....	40
Figura 79 - Parametri de semnare la distanță: PIN	40
Figura 80 - Încheierea procesului de semnare	40