

Registration Authority

Guida FirmaCerta per MacOS

Categoria	TSP-Firma Digitale	Codice Documento	NAM-Guida Utente	Namirial S.p.A.
Redatto da	Michelangelo Bonvini	Nota di riservatezza	Documento Pubblico	Registration Authority
Verificato da	Gabriele Bocchini	Versione	1.0	Gabriele Bocchini
Approvato da	Gabriele Bocchini	Data di emissione	01/02/2019	



– Questa pagina è lasciata intenzionalmente in bianco –



INDICE

Indice	3
Storia delle modifiche apportate	6
1 Introduzione	7
1.1 Scopo del documento e campo di applicazione.....	7
1.2 Definizioni ed Acronimi usati all'interno del documento	7
2 Installazione	9
3 Interfaccia grafica	11
4 Funzioni Principali.....	11
4.1 Firma	11
4.2 Firma e Marca.....	12
4.3 Controfirma	12
4.4 Marca	12
4.5 Verifica.....	12
4.6 Visualizza.....	12
5 Strumenti.....	13
5.1 Visualizza Certificati	13
5.2 Verifica dispositivo di firma	14
5.3 Cambio PIN	14
5.4 Sblocca PIN	15
5.5 Cambio PUK	15
5.6 Rinnovo Certificati	16
5.7 Opzioni.....	16
5.7.1 Generale	16



5.7.2	Gestione File	17
5.7.3	Verifica	17
5.7.4	Marche	18
5.7.5	Aggiornamenti	18
6	Appendice:	19
6.1	Appendice A: Come Firmare un File	19
6.1.1	Selezione del formato di firma	19
6.1.2	Selezione del motivo di Firma	20
6.1.3	Conclusione processo di firma	20
6.2	Appendice B: Come Controfirmare un documento	22
6.2.1	Conclusione processo di controfirma	22
6.3	Appendice C: Configurazione Parametri Marche Temporalì	24
6.3.1	Appendice C1: Come Marcare un file	25
6.3.2	Appendice C2: Come Firmare e Marcare un documento	28
6.4	Appendice D: Come Verificare un file	31
6.5	Appendice E: Rinnovo Certificati	32
6.5.1	Configurazione del Proxy	32
6.5.2	Modalità di Rinnovo SmartCard e Token	33
6.6	Appendice F: Guida Firma Remota	35
6.6.1	Come Firmare un File	35
6.6.2	Procedura OTP Virtuale: Namirial OTP	37
6.6.3	Procedura OTP SMS	41
6.6.4	Procedura con OTP Hardware	42
6.7	Appendice G: Autenticazione WEB	44
6.8	Appendice H: Bit4id – MacOS	44
6.8.1	Cambio Pin	45



6.8.2	Sblocco Pin.....	45
6.8.3	Cambio PUK.....	46
Riferimenti		47
Indice delle Tabelle.....		48
Indice delle Figure		48



STORIA DELLE MODIFICHE APPORTATE

VERSIONE	1.0
Data	01/02/2019
Motivazione	Prima emissione del documento.
Modifiche	---



1 INTRODUZIONE

Nell'Ordinamento Giuridico Italiano il termine FIRMA DIGITALE sta a indicare un tipo di firma elettronica qualificata, alla quale si attribuisce piena efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa. Così come la firma autografa sul documento cartaceo, la firma digitale può essere apposta su un documento informatico.

La tecnologia alla base della firma digitale garantisce, inoltre, che il documento firmato non possa essere in seguito modificato senza invalidare la firma stessa, e consente di associare al documento una data e un'ora certe, attraverso il meccanismo della marca temporale.

FirmaCerta è lo strumento ideale per:

- firmare contemporaneamente grandi volumi di documenti digitali, come fatture, polizze, ricevute di pagamenti, bonifici e qualsiasi altro documento digitale;
- Firmare i documenti mantenendo il formato originale (il .PDF o .XML dopo essere stato firmato mantenendo lo stesso formato);
- La possibilità di poter scegliere il dispositivo hardware col quale si desidera apporre la firma (Smart Card - Token);
- La possibilità di apporre/associare una marca temporale ad un documento o a una firma (Grafometrica);

1.1 SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE

Il presente documento, identificato mediante il codice riportato nel frontespizio, descrive le operazioni da seguire per l'installazione del Client FirmaCerta, e il driver Bit4id per il riconoscimento dei certificati; descrive inoltre le funzioni del Client FirmaCerta, il software per la gestione delle firme digitali e le marche temporali personali.

Un documento firmato non può più essere modificato dal software usato per crearlo. In ogni caso, qualora si riesca ad alterare il file con qualunque strumento, per i principi della crittografia asimmetrica non ci potrà più essere corrispondenza tra contenuto del documento e firme associate, FirmaCerta nelle operazioni di verifica del documento darà esito negativo.

1.2 DEFINIZIONI ED ACRONIMI USATI ALL'INTERNO DEL DOCUMENTO

TERMINE	SIGNIFICATO
Firma Digitale	è un particolare tipo di firma elettronica qualificata e rappresenta l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Marca Temporale (timestamp)	è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione è detta timestamping. Un file marcato temporalmente ha estensione .m7m
PDF: (Portable Document Format)	Formato per file grafici elaborato dalla Adobe Systems. Questo standard viene utilizzato per rendere disponibili documenti rappresentanti pagine stampate di libri, riviste, depliant, cataloghi, listini, ecc. e per tutti quei documenti per cui è importante che venga mantenuto l'aspetto grafico. Le pagine visibili a video possono essere, di norma (ma non sempre), stampate ma non modificate utilizzando Acrobat Reader, che è il programma gratuito utilizzato per leggere i documenti pdf.
Smart Card	è un dispositivo hardware delle dimensioni di una carta di credito che possiede potenzialità di elaborazione e memorizzazione dati ad alta sicurezza.
Token USB	Sono quelle chiavette che comprendono un chip analogo a quello di una smart card e si inseriscono direttamente in una porta USB: hanno quindi le stesse funzioni della smart card con lo stesso chip, driver e software di corredo ma non necessitano di un lettore avendo una connessione diretta al PC tramite la porta USB.



Drag and Drop	Trascina e lascia. Tecnica che consente di trasferire i file da un punto all'altro di un programma mediante il semplice trascinamento, tenendo premuto il tasto sinistro del mouse (drag: trascinare - drop: cadere).
PIN	(Personal Identification Number) codice univoco per l'identificazione di un utente.
Firma Elettronica	Per firma elettronica la legge intende l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo d'identificazione informatica.
Proxy	Sistema di protezione della rete locale dall'accesso da parte di altri utenti Internet. Il server proxy funziona come una barriera di sicurezza tra la rete interna e Internet, impedendo ad altri utenti Internet di accedere alle informazioni riservate della rete interna. Il server inoltre riduce notevolmente il traffico in rete memorizzando localmente nella memoria cache i documenti utilizzati di frequente.
Base64	è un sistema di numerazione posizionale che usa 64 simboli. Viene usato principalmente come codifica di dati binari nelle e-mail, per convertire i dati nel formato ASCII. La codifica Base64 provoca un aumento globale del 33% del volume dei dati da decodificare.

Tabella 1 - Definizioni ed Acronimi



2 INSTALLAZIONE

Scaricare il software di Firma dal sito www.firmacerta.it, sezione *Download > Software Firmacerta*, > Versione Desktop per Mac ([LINK](#)).

Attenzione: *Compatibile con MacOS 10.11 o superiore., per le versioni precedenti (10.10 e 10.9.5) non garantiamo il corretto funzionamento.*

Avviare il file FirmaCerta.dmg

1. Trascinare il file Firmacerta nella cartella Applicazioni;
2. Avviare il pacchetto *hid-switch-signed.pkg*
3. Avviare il pacchetto *bit4id-middleware-user-signed.pkg* (al termine dell'installazione di questo pacchetto sarà richiesto il riavvio del computer).

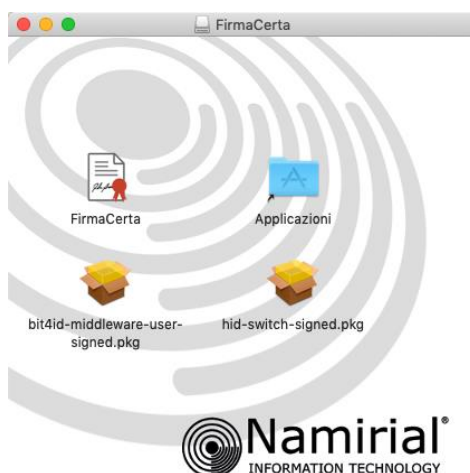


Figura 1 - installazione firmacerta

Nota: Per dispositivi con numero di Serie 2203... 2204... Installare [SafeDive](#).

Attenzione: Al primo avvio del software FirmaCerta sarà mostrato un messaggio di Warning in cui viene comunicato all'utente che: "il software FirmaCerta proviene da uno sviluppatore non identificato". Questo messaggio viene comunicato per tutte le applicazioni non presenti nell'APP store di Apple.



Figura 2 - installazione firmacerta Warning



Per scegliere di ignorare le impostazioni sulla sicurezza e aprire comunque l'app.

1. Nel Finder > Applicazioni, trovare l'app che desideri aprire. *Non utilizzare Launchpad per realizzare questa operazione. Launchpad non consente di accedere al menu di scelta rapida.*
2. Fai clic sull'icona dell'app tenendo premuto il tasto Ctrl (in alternativa click con il tasto DX), quindi scegli **Apri** dal menu di scelta rapida.
3. Cliccando su Apri si conferma di volerlo aprire comunque e L'app verrà salvata come eccezione alle impostazioni sulla sicurezza e si potrà aprire in futuro facendo doppio clic su di essa, proprio come un'app autorizzata.

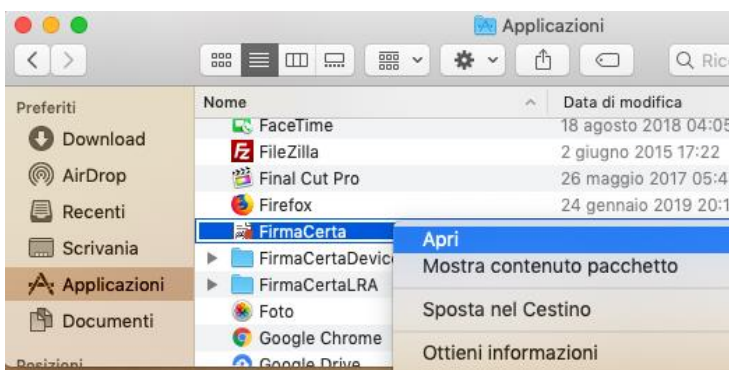


Figura 3 - installazione firmacerta soluzione 1a



Figura 4 - installazione firmacerta soluzione 1b

Nota:

Puoi anche concedere un'eccezione per un app bloccata facendo clic sul pulsante "Apri comunque" nel pannello Generali delle preferenze "Sicurezza e Privacy".

Per aprire questo pannello, scegli menu **Apple > Preferenze di Sistema**, fai clic su **"Sicurezza e Privacy"**, quindi fai clic su **Generali**.

Questo pulsante è disponibile per circa un'ora dopo che tenti di aprire l'app.

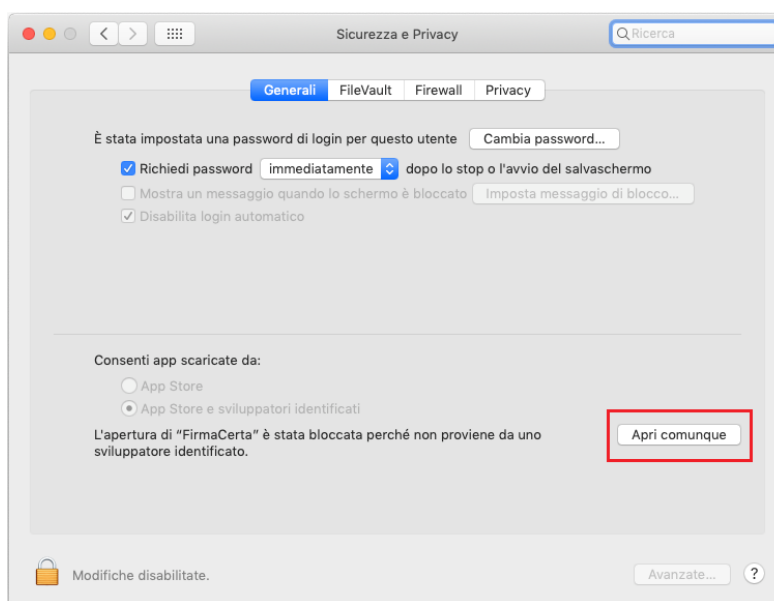


Figura 5 - installazione firmacerta soluzione 2



3 INTERFACCIA GRAFICA

L'interfaccia grafica di FirmaCerta è semplice e intuitiva. Il menù è composto dalle principali funzioni d'utilizzo del software:

- Firmare digitalmente qualsiasi File;
- Apporre la Marca temporale;
- Visualizzare e Verificare i file firmati digitalmente;



Figura 6 - interfaccia grafica

Le principali funzioni saranno dettagliate nel [Capitolo 4](#)

Nella Barra degli Strumenti: è possibile gestire le impostazioni del software e l'utilizzo di funzioni specifiche quali:

- Attiva Dispositivo di firma
- Visualizza Certificati Contenuti nel Dispositivo di Firma
- Verifica Dispositivo di Firma
- Rinnovo Certificati



Figura 7 - barra degli strumenti

Le impostazioni del software e l'utilizzo delle funzioni specifiche saranno dettagliate nel [Capitolo 5](#)

4 FUNZIONI PRINCIPALI

4.1 FIRMA

Con FirmaCerta è possibile firmare un qualsiasi documento con una delle seguenti modalità:



Drag & Drop: Trascinando (*drag & drop*) contemporaneamente uno o più file da firmare digitalmente all'interno della finestra del software FirmaCerta e fare click sull'icona "Firma".

Dalla barra degli strumenti **File > Aggiungi File** sarà possibile ricercare all'interno del vostro computer il file che desiderate firmare.

Dal Software: Cliccando direttamente sull'icona di Firma sarà possibile ricercare all'interno del vostro computer il file che si desidera firmare.

Una volta premuto "Firma" il software chiederà di scegliere la directory in cui si vuole memorizzare il/i file/s firmato/i, e successivamente il PIN del proprio dispositivo di firma (Smart card/Token Sim card).

- Vedi la procedura completa per firmare un documento [Appendice A: Come firmare un documento](#)
- Vedi la procedura per i possessori di Firma Remota [Appendice F: Firma Remota](#)



4.2 FIRMA E MARCA



Attraverso questa funzione è possibile firmare e marcare temporalmente in un'unica operazione un/più documento/i digitale/i.

Il client di Firma chiede di selezionare la cartella di destinazione del file firmato. Una volta premuto "Firma e Marca" e digitato il PIN verrà richiesto di inserire la "User" e la "Password" per l'utilizzo delle marche temporali.

Vedi la procedura completa per Firmare e Marcare un documento: [Appendice C2: Come Firmare e Marcare un documento](#)

4.3 CONTROFIRMA



Con questa funzione è possibile controfirmare una firma già presente, vale a dire conferire a quest'ultima una sorta di validazione gerarchica.

Una volta premuto *Controfirma* il software richiederà prima la destinazione della cartella dove si desidera salvare il file controfirmato, in seguito la conferma che sia il documento selezionato quello da firmare ed infine l'inserimento del PIN del dispositivo di firma connesso al computer.

Vedi la procedura completa per controfirmare un documento [Appendice B: Come controfirmare](#)

4.4 MARCA



Dopo aver selezionato un file con questa funzione è possibile marcarlo temporalmente, in questo modo associamo al documento una data ed un'ora certa, opponibile a terzi.

Anche a seguito di questa operazione verrà richiesta la cartella di destinazione del file *Marcato* e l'inserimento del PIN associato al dispositivo di firma.

Vedi la procedura completa per Marcare un documento: [Appendice C1: Come Marcare un file](#)

4.5 VERIFICA



Questa funzione permette di verificare lo stato della firma/firme apposte sul documento. La finestra **Esito** darà conferma sull'integrità della firma, l'attendibilità del certificato, la validità legale del certificato e la verifica della CRL e OCSP ossia che il certificato è attivo.

È possibile inoltre, all'interno di questa funzione, aprire la finestra dei **Dettagli** che mostrerà le principali caratteristiche del certificato (Tipologia, Ente Emittente, Titolare, Validità del certificato)

Vedi la procedura completa per Verificare un documento: [Appendice D: Come verificare e visualizzare un file](#)

4.6 VISUALIZZA



Questa funzione permette di visualizzare i documenti firmati digitalmente in formato .p7m



5 STRUMENTI

5.1 VISUALIZZA CERTIFICATI

Nella colonna di sinistra vengono valorizzati i due certificati:

Autenticazione (Codice Fiscale) e **Sottoscrizione** (Nome e Cognome).

Nella colonna di destra viene mostrato l'**Esito** della verifica effettuata e in **Dettagli** viene approfondita.

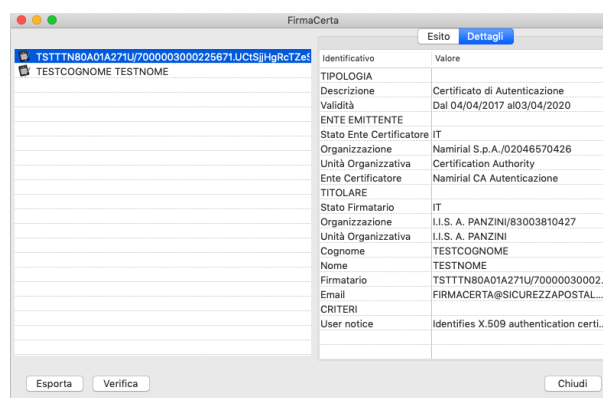
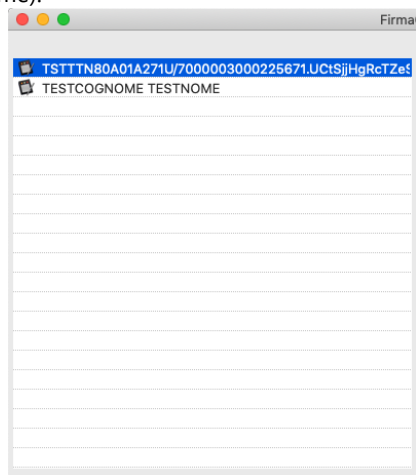
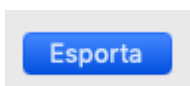


Figura 8 - Visualizza Certificati

Nota:

- Verificare di avere Adobe Reader aggiornato all'ultima versione, per utilizzare questa procedura;
- Soltanto per i file firmati digitalmente in PAdES sarà visibile un logo PDF.



Tramite questa funzione è possibile esportare i certificati della propria Smart Card nei seguenti formati:

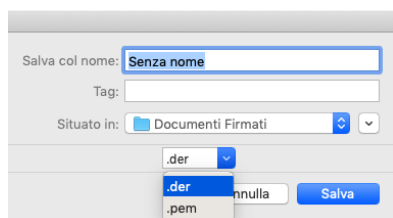


Figura 9 - esporta certificati

- **.der** Sono semplicemente una versione binaria del formato PEM. Hanno estensione .der ma talvolta anche .cer; in quest'ultimo caso l'unico modo per distinguere il formato è di aprire il file con un editor per vedere se sia in formato ASCII o binario.
- **.pem** Formato più comunemente utilizzato dalle Certification Authorities per emettere i certificati, solitamente utilizzando le estensioni convenzionali .pem, .crt, e .cer. Sono files ASCII con codifica Base64 e contengono "-----BEGIN CERTIFICATE-----" all'inizio e "-----END CERTIFICATE-----" alla fine. Possono essere in formato PEM sia certificati server, che certificati intermedi e chiavi private.



Premendo il tasto **verifica** viene effettuata la verifica dei certificati presenti nel dispositivo di firma. Cliccando sulle etichette **Esito** e **Dettagli** è possibile visualizzare il risultato del test eseguito e le particolarità del Certificato selezionato



5.2 VERIFICA DISPOSITIVO DI FIRMA

Tramite questa funzione è possibile compiere un test sul lettore di Smart Card, digitando il *Pin* verrà fornita all'utente informazioni sullo stato dell'hardware (ammesso che la carta sia attivata correttamente).

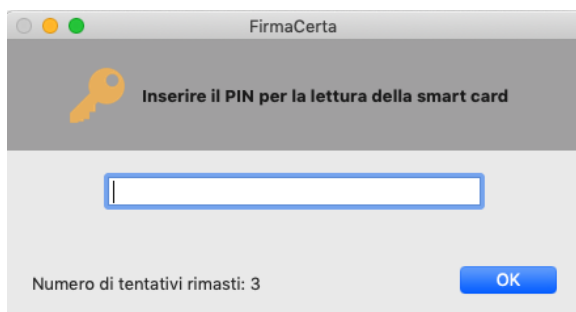


Figura 10 - inserimento Pin: verifica dispositivo



Descrizione	Valore
ID	7000003000225671
ATR	3BFF1800008131FE55006B020904030...
DYLIB	/Applications/FirmaCerta.app/Contents/...

Figura 11 - esito verifica dispositivo

5.3 CAMBIO PIN

Consente di modificare il PIN attuale attraverso l'inserimento di un nuovo PIN (inserimento e verifica).

Nota:

- Per i possessori di Firma Remota è possibile modificare il PIN dalla propria [Area Privata Utente](#) nella sezione > Utente > Firma digitale > Gestione.
- È possibile eseguire il Cambio PIN anche con il Middleware Bit4id come indicato nell' [Appendice H](#)

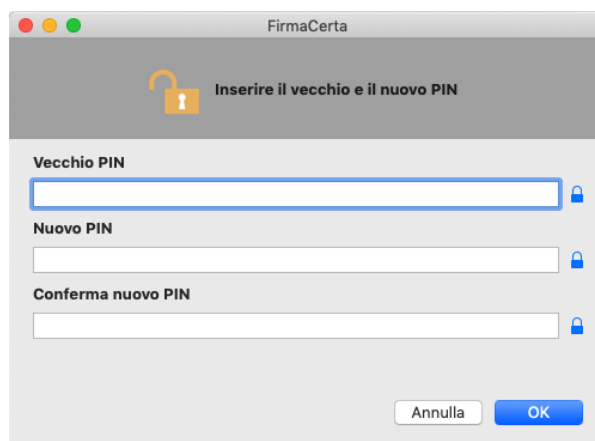


Figura 12 - Cambio PIN



5.4 SBLOCCA PIN

Funzione necessaria per sbloccare il codice PIN. Inserire il Codice PUK (codice numerico di 8 cifre) presente nella busta cieca.

Nota: È possibile eseguire lo Sblocco PIN anche con il Middleware Bit4id come indicato nell' [Appendice H](#)

ATTENZIONE: prima di eseguire la procedura di sblocco è necessario possedere la Busta Cieca che è stata fornita in fase di Emissione.

Dopo 3 tentativi errati del Codice PUK il dispositivo si bloccherà irrimediabilmente e sarà necessario richiedere un nuovo dispositivo di firma.

Figura 13 - Sblocca PIN

5.5 CAMBIO PUK

Consente di modificare il PUK attuale attraverso l'inserimento di un nuovo PUK (inserimento e verifica).

Nota:

- È possibile eseguire il Cambio PUK anche con il Middleware Bit4id come indicato nell' [Appendice H](#)

Figura 14 - Cambio PUK



5.6 RINNOVO CERTIFICATI

Funzione necessaria per poter rinnovare i certificati di firma digitale, per ulteriori tre anni.
Consultare la **guida** con le informazioni essenziali per eseguire il rinnovo (Vedi [Appendice E](#)).

ATTENZIONE:

1. Se l'utente non viene sbloccato dal RAO, non sarà possibile completare il rinnovo;
2. Non è possibile eseguire un secondo rinnovo di firma digitale.

5.7 OPZIONI

In questa sezione è possibile gestire le impostazioni di firmacerta.

5.7.1 GENERALE

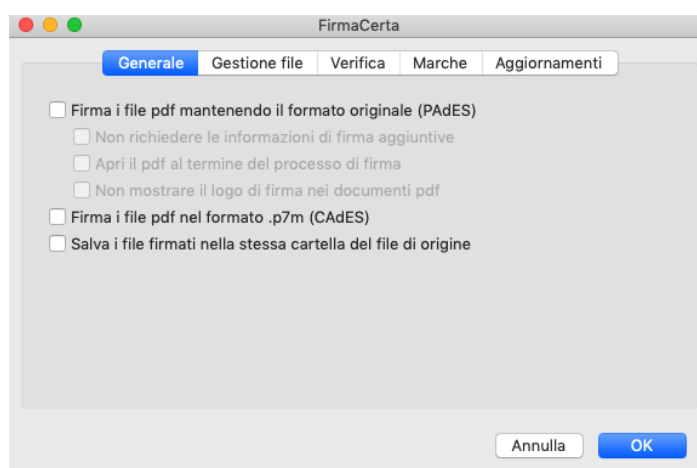


Figura 15 - Opzioni: Generali

Firma i file pdf mantenendo il formato (PAdES):	i File .pdf vengono firmati in automatico in formato PAdES senza permettere all'utente di scegliere tra il formato .p7m e .pdf mantiene il formato originale del file firmato (altrimenti convertito in formato .p7m), fornendo la possibilità di visualizzare i documenti anche ad un utente non forniti di software per la firma digitale.
• Non richiedere le informazioni di firma aggiuntive:	Non saranno visualizzate alcune informazioni facoltative nella firma del documento;
• Apri il pdf al termine del processo di firma	Viene aperto il file PDF con il programma predefinito dopo l'applicazione della firma digitale.
• Non mostrare il logo di firma nei documenti pdf:	Utilizzando questa preferenza prima della firma e visualizzando in seguito il file PDF firmato digitalmente, non sarà mostrato il logo di firma con i dati del firmatario.



	N.B: È possibile personalizzare il logo in assenza del quale sarebbe impiegato quello predefinito utilizzando le opzioni della sezione corrispondente denominata Logo pdf .
Firma i file pdf nel formato .p7m (CAdES):	i File .pdf vengono firmati in automatico in formato CAdES senza permettere all'utente di scegliere tra il formato .p7m e .pdf
Salva i file firmati nella stessa cartella del file originale:	consente il salvataggio del file firmato nella stessa directory del file originale;

5.7.2 GESTIONE FILE

In questa sezione è possibile codificare i file firmati digitalmente (.p7m), i file marcati temporalmente (.tsd, .tsr, .tst) e i file protetti(.p7e) in formato *Base64*

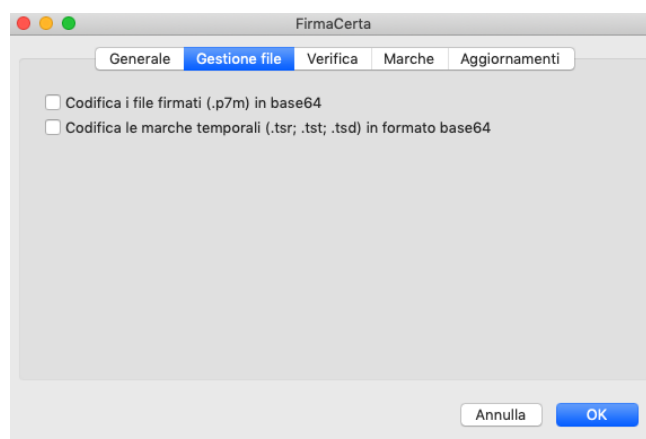


Figura 16 - Opzioni: Gestione File

5.7.3 VERIFICA

Permette di verificare contestualmente alla visualizzazione di un file firmato digitalmente lo stato del certificato (attivo/revocato/sospeso) e di eseguire la verifica del file all'avvio della funzione [Verifica](#).

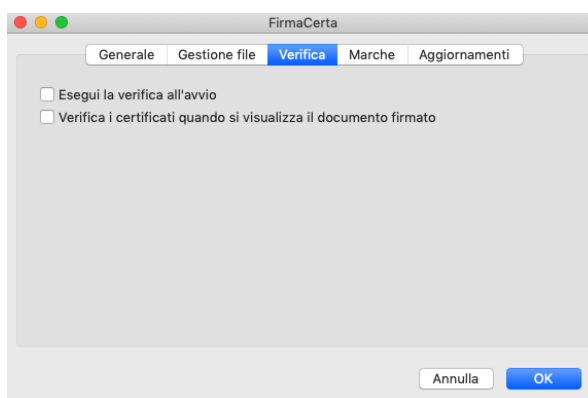


Figura 17 - Opzioni: Verifica



5.7.4 MARCHE

La sezione permette di memorizzare il nome *Utente* e la *Password* per l'utilizzo di marche temporali (ammesso che l'operatore ne sia in possesso) senza dover digitare ogni volta le credenziali durante la fase di *timestamping*.

Cliccando su Controlla Marche Residue è possibile verificare il numero delle marche temporali residue.

Figura 18 - Opzioni: Marche Temporali

LINK per l'utilizzo delle Marche Temporali

<https://timestamp.namiraltsp.com>
<http://timestamp.namiraltsp.com>

5.7.5 AGGIORNAMENTI

Consente di abilitare/disabilitare il controllo degli aggiornamenti e di scegliere se far installare in autonomia gli aggiornamenti quando disponibili, in modalità silente.

Figura 19 - Opzioni: Aggiornamenti



6 APPENDICE:

6.1 APPENDICE A: COME FIRMARE UN FILE

Dopo aver caricato il file da firmare e cliccato sulla funzione di **Firma**, sarà richiesto all'utente di selezionare una cartella di destinazione dove salvare il documento firmato.

*In questo esempio è stata creata in precedenza una cartella dedicata per i file firmati digitalmente, quindi **selezionare** Documenti Firmati e poi click su **Apri**.*

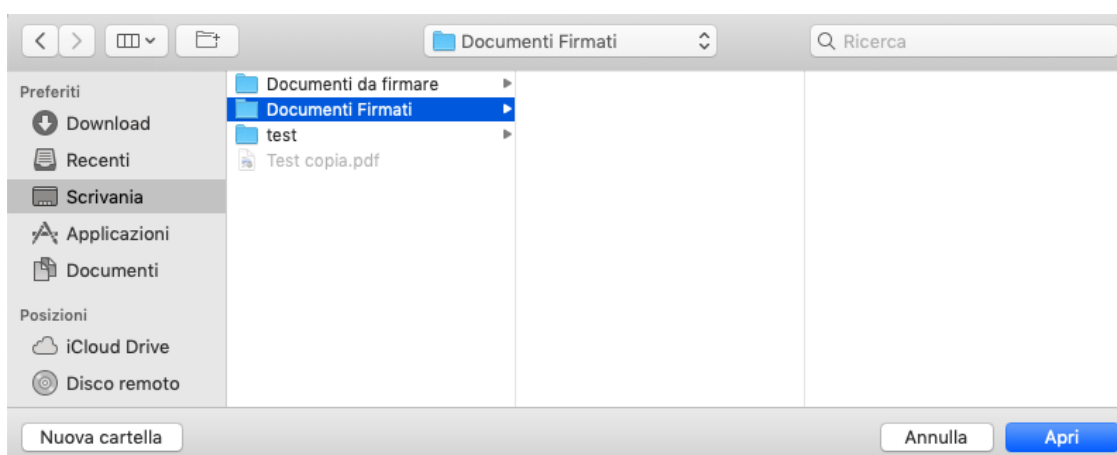


Figura 20 – selezione cartella di destinazione

6.1.1 SELEZIONE DEL FORMATO DI FIRMA

Selezionare il formato CADES per firmare il file in formato .p7m.

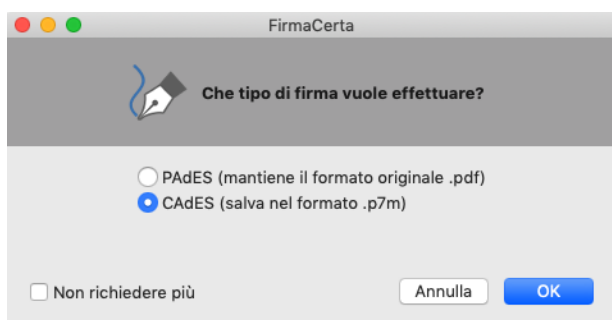


Figura 21 - selezione formato CADES

Selezionare il formato PAdES per firmare il file in formato .pdf.

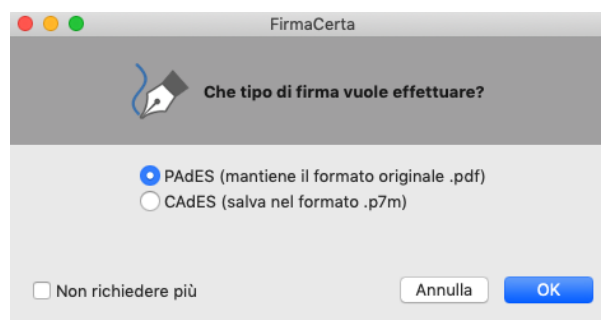


Figura 22 - selezione formato PAdES

Nota: la scelta del formato con cui firmare il documento è disponibile solo per i file con estensione .pdf, per tutti gli altri formati sarà automaticamente applicata l'estensione .p7m

Contrassegnando con una spunta la voce **Non richiedere più**, verrà impostato l'automatismo e per rimuoverlo sarà necessario modificare le impostazioni nelle [Opzioni](#)



6.1.2 SELEZIONE DEL MOTIVO DI FIRMA

Questa funzione permette l'aggiunta di informazioni aggiuntive quali, il *motivo*, la *località* e le *informazioni di contatto* alla firma del documento.

Nota: Questa funzione è disponibile solamente per i documenti in formato .pdf
L'utilizzo di questa funzione è una scelta dell'utente in quanto è un Operazione Facoltativa.

FirmaCerta

Indicare alcune informazioni aggiuntive che verranno visualizzate nella firma del documento (facoltativo)

Motivo di Firma

Località

Informazioni di contatto

☐ Non richiedere più

Annulla OK

Figura 23 - Motivo della Firma

6.1.3 CONCLUSIONE PROCESSO DI FIRMA

Confermare l'apposizione della firma

FirmaCerta

Attenzione (Test copia.pdf)!

Il file Test copia.pdf sta per essere firmato digitalmente.
Si desidera procedere?

Annulla OK

Figura 24 - Conferma apposizione firma

Selezione del Lettore USB/Token USB

FirmaCerta

Selezione il lettore smart card:

Gemalto USB Shell Token V2

OK

Figura 25 - Selezione Lettore



Inserire il PIN del dispositivo di Firma Digitale e cliccare su **OK**.

Nota:

Il codice PIN è stato fornito con la busta cieca

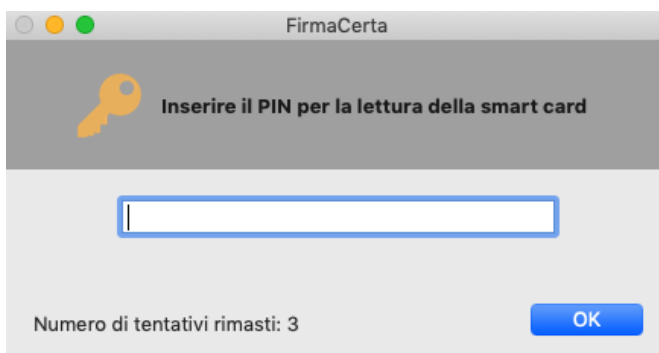


Figura 26 - inserimento PIN

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.



Figura 27 - Completamento processo di firma



6.2 APPENDICE B: COME CONTROFIRMARE UN DOCUMENTO

Con questa funzione è possibile controfirmare una firma già presente, vale a dire conferire a quest'ultima una sorta di validazione gerarchica.

Dopo aver caricato il *File Firmato Digitalmente* che si desidera Controfirmare, **Cliccare sul pulsante Controfirma**. In questo esempio è stata creata in precedenza una cartella dedicata per i file firmati digitalmente, quindi **selezionare Documenti Firmati** e poi click su **Apri**.

Nota: è possibile controfirmare soltanto i *File Firmati Digitalmente* in formato .p7m

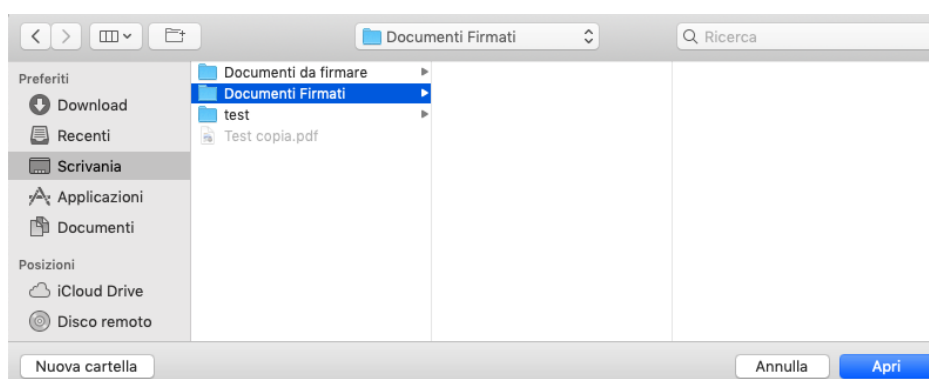


Figura 28 - Selezione cartella di destinazione

6.2.1 CONCLUSIONE PROCESSO DI CONTROFIRMA

Confermare l'apposizione della firma

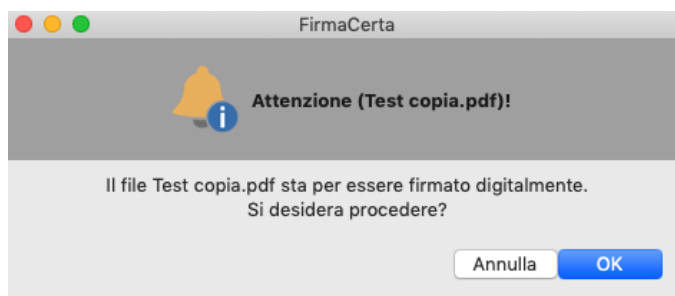


Figura 29 - Conferma firma

Selezione del Lettore USB/Token USB

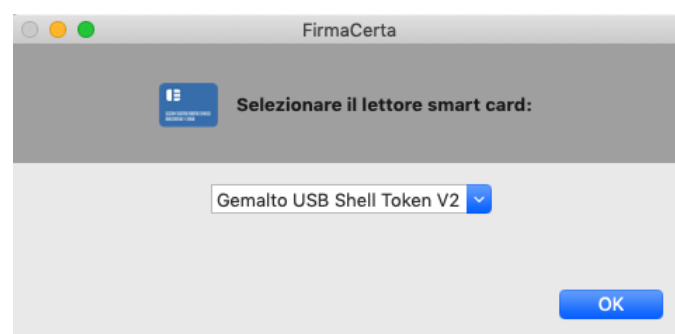


Figura 30 - selezione Lettore



Inserire il PIN del dispositivo di Firma Digitale e cliccare su **OK**.

Nota:

Il codice PIN è stato fornito con la busta cieca

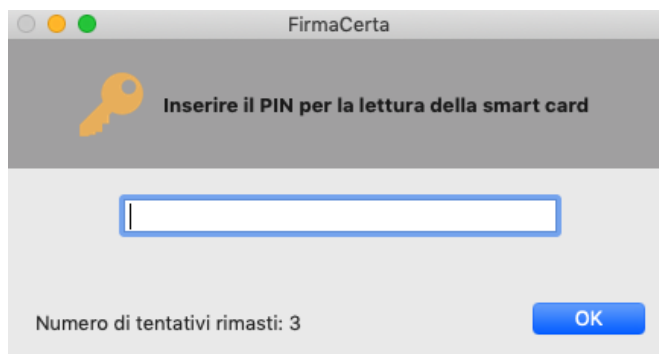


Figura 31 - Inserimento PIN

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.



Figura 32 - Completamento processo di controfirma



6.3 APPENDICE C: CONFIGURAZIONE PARAMETRI MARCHE TEMPORALI

Prima di utilizzare il servizio di Marche Temporalì si deve configurare il programma FirmaCerta.

Nota:

Il Servizio di Marcatura Temporale, non è compreso con la Firma Digitale. Le marche temporalì possono essere acquistate nel nostro [Shop](#).

Da FirmaCerta > Strumenti > Opzioni > Marche

- Verificare che l'URL sia <http://timestamp.namirialtsp.com> o <https://timestamp.namirialtsp.com>
- Inserire **Utente** e **Password** e infine cliccare su **OK**.
- Contrassegnando con una spunta la voce "Non richiedere parametri di accesso", non sarà richiesto la conferma dei dati nel processo di marcatura temporale.

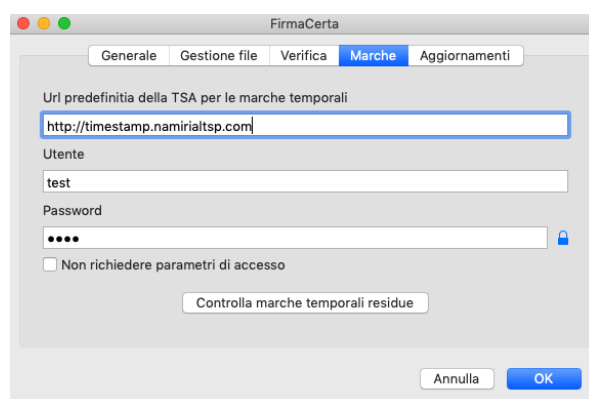


Figura 33 - Configurazione Marche

Nota: in caso di smarrimento delle credenziali per l'utilizzo delle Marche - Il Cliente deve richiederle inviando una PEC all'indirizzo: firmacerta@sicurezzapostale.it o una email a helpdesk@firmacerta.it indicando l'Username e/o Codice Fiscale.

La funzione **Controlla marche temporalì residue** verifica l'acquisto, l'uso e il residuo di marche temporalì (nel caso in cui l'interrogazione fallisse controllare il corretto inserimento delle credenziali)

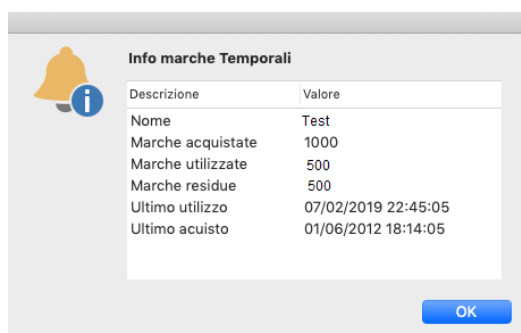


Figura 34 - esito marche residue



6.3.1 APPENDICE C1: COME MARCARE UN FILE

Dopo aver caricato il file da marcare e cliccato sulla funzione di **Marca**, sarà richiesto all'utente di selezionare una cartella di destinazione dove salvare il file marcato.

*In questo esempio è stata creata in precedenza una cartella dedicata per i file firmati e marcati, quindi **selezionare** Documenti Marcati e poi click su **Apri**.*

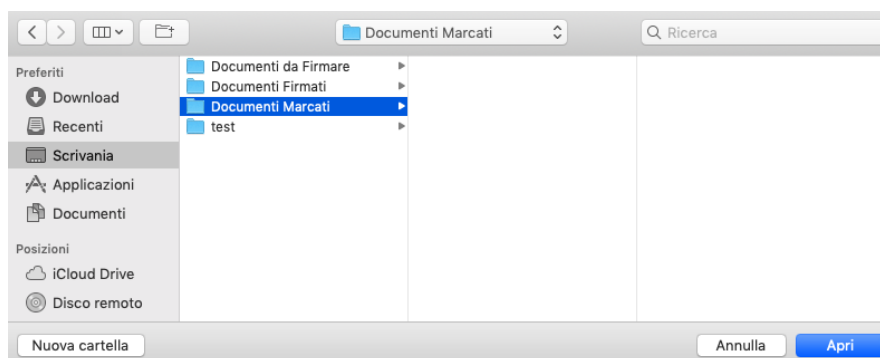


Figura 35 - Selezione cartella di destinazione

Indicare il formato con cui si desidera Marcare il documento.

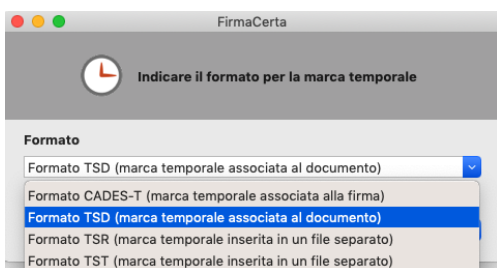


Figura 36 - selezione formato Marca temporale

.TSD (TimeStamp Document): è il **formato standard** che contiene sia marca temporale che il file originale oggetto di marcatura, e consente quindi di verificare sia la correttezza della marca temporale che il contenuto del file originale. La Marca Temporale è associata al documento.

.TSR (TimeStamp Response): è simile al formato .TST con in aggiunta il codice di risposta del Server TimeStamp dell'ente certificatore.

L'evidenza informatica che si ottiene attraverso la verifica è solo sulla correttezza della marca temporale mentre *è necessario avere il file originale per verificare la corrispondenza tra quest'ultimo e il file .tsr*.

.TST (TimeStamp Token): è un file contenente l'impronta del documento o file marcato non il contenuto dello stesso.

CADES-T o PADES-T: dimostra che la firma stessa è effettivamente esistita in una determinata data e ora. La marca temporale è associata alla singola firma e NON separabile.



Attenzione: se il documento è stato già firmato e si desidera marcare temporalmente il file il software permetterà anche la scelta del formato **CADES-T** (per i file .p7m) e **PADES-T** (per i file .pdf).

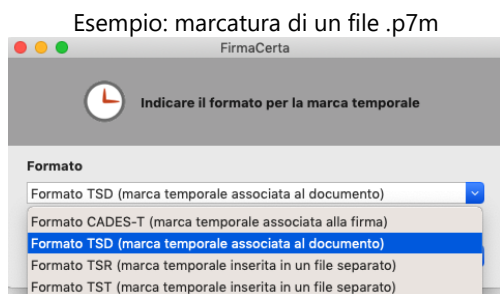


Figura 37 - File .p7m da marcare

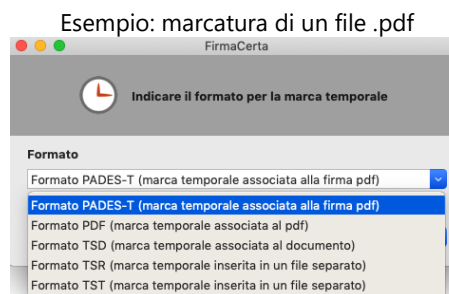


Figura 38 - file .pdf da marcare

6.3.1.1 INDICARE I PARAMETRI DI MARCATURA TEMPORALE

Indicare i parametri del servizio di marche temporali.

Nota:

- se è stata eseguita la configurazione delle Marche temporali i campi **URL**, **Username** e **Password** saranno precompilati.
- Contrassegnando con una spunta la voce "Non richiedere parametri di accesso", non sarà più richiesto la conferma dei dati nel processo di marcatura temporale, e per rimuoverlo sarà necessario modificare le impostazioni nelle [Opzioni](#).

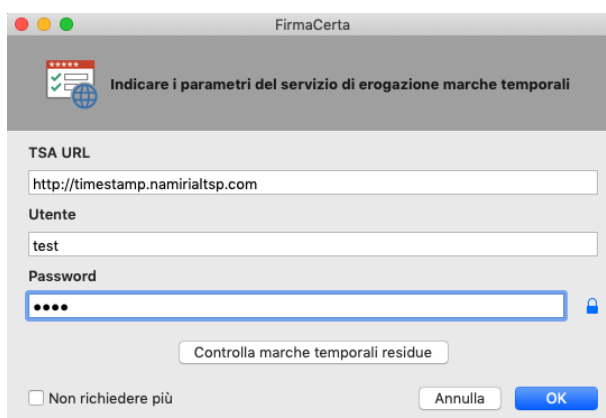


Figura 39 - inserimento parametri Marche



6.3.1.2 CONCLUSIONE PROCESSO DI MARCATURA TEMPORALE

Confermare l'apposizione della firma

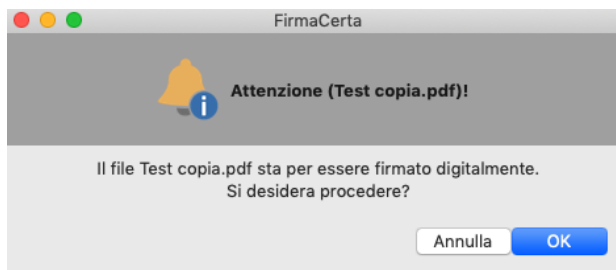


Figura 40 - conferma apposizione firma

Selezione del Lettore USB/Token USB



Figura 41 - selezione lettore

Inserire il PIN del dispositivo di Firma Digitale e cliccare su **OK**.

Nota:

Il codice PIN è stato fornito con la busta cieca

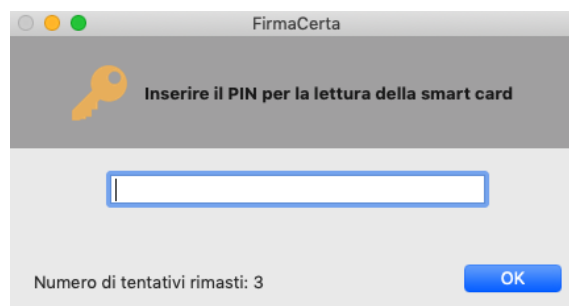


Figura 42 - inserimento PIN

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.

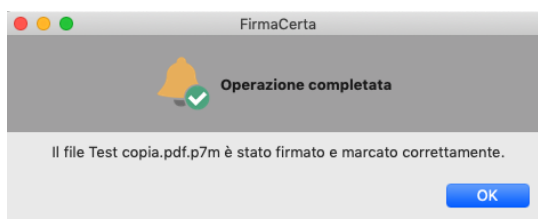


Figura 43 - operazione completata



6.3.2 APPENDICE C2: COME FIRMARE E MARCARE UN DOCUMENTO

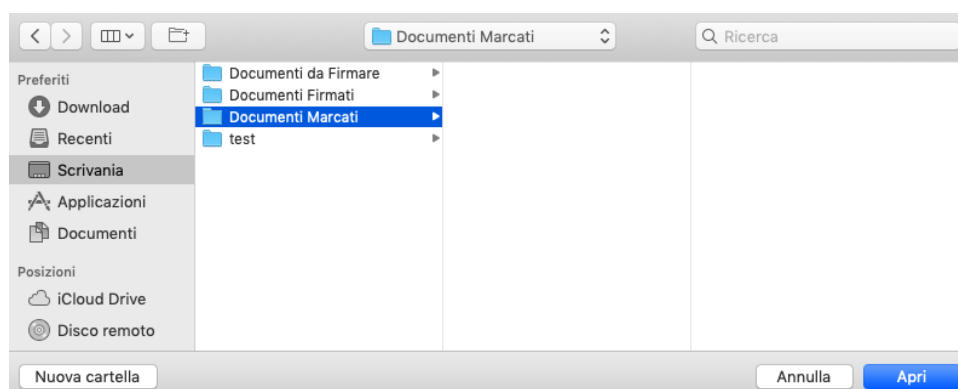
Dopo aver selezionato un file, si sceglie questa funzione per firmare e marcare temporalmente in un'unica sessione.

Il file così firmato e marcato sarà in formato **CADES-T** (file marcato.pdf.P7M).

Nel formato CADES-T (formato di default) o PAdES-T (formato disponibile solo per i documenti PDF) la marca è associata alla singola firma e NON separabile.

Dopo aver caricato il file da firmare e cliccato sulla funzione di **Firma e Marca**, sarà richiesto all'utente di selezionare una cartella di destinazione dove salvare il documento firmato e marcato.

*In questo esempio è stata creata in precedenza una cartella dedicata per i file firmati e marcati, quindi **selezionare** Documenti Marcati e poi click su **Apri**.*



ATTENZIONE: Se il file che si desidera firmare e marcare temporalmente non è un file PDF [passare direttamente al punto 6.3.2.3](#)

6.3.2.1 SELEZIONE DEL FORMATO DI FIRMA

Selezionare il formato CAdES per firmare il file in formato .p7m.

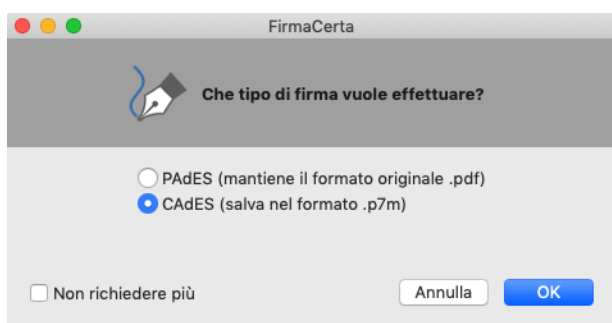


Figura 44 - selezione formato Cades

Selezionare il formato PAdES per firmare il file in formato .pdf.

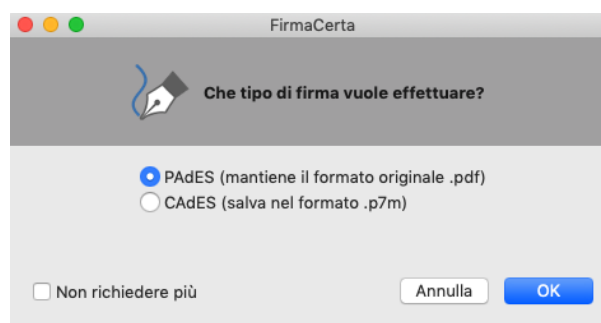


Figura 45 - selezione formato Pades

Nota: la scelta del formato con cui firmare il documento è disponibile solo per i file con estensione .pdf, per tutti gli altri formati sarà automaticamente applicata l'estensione .p7m

Contrassegnando con una spunta la voce **Non richiedere più**, verrà impostato l'automatismo e per rimuoverlo sarà necessario modificare le impostazioni nelle [Opzioni](#)



6.3.2.2 SELEZIONE DEL MOTIVO DI FIRMA

Questa funzione permette l'aggiunta di informazioni aggiuntive quali, il *motivo*, la *località* e le *informazioni di contatto* alla firma del documento.

Nota: Questa funzione è disponibile solamente per i documenti in formato .pdf
L'utilizzo di questa funzione è una scelta dell'utente in quanto è un Operazione Facoltativa.

FirmaCerta

Indicare alcune informazioni aggiuntive che verranno visualizzate nella firma del documento (facoltativo)

Motivo di Firma

Località

Informazioni di contatto

☐ Non richiedere più

Annulla OK

Figura 46 - inserimento motivo della firma

6.3.2.3 INDICARE I PARAMETRI DI MARCATURA TEMPORALE

Indicare i parametri del servizio di marche temporali.

Nota:

- se è stata eseguita la configurazione delle Marche temporali i campi **URL**, **Username** e **Password** saranno precompilati.
- Contrassegnando con una spunta la voce "Non richiedere parametri di accesso", non sarà più richiesto la conferma dei dati nel processo di marcatura temporale, e per rimuoverlo sarà necessario modificare le impostazioni nelle [Opzioni](#).

FirmaCerta

Indicare i parametri del servizio di erogazione marche temporali

TSA URL

http://timestamp.namirialtsp.com

Utente

test

Password

Controlla marche temporali residue

☐ Non richiedere più

Annulla OK

Figura 47 - Parametri Marche



6.3.2.4 CONCLUSIONE PROCESSO DI FIRMA E MARCA TEMPORALE

Confermare l'apposizione della firma

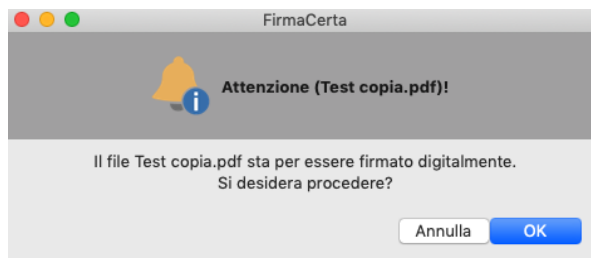


Figura 48 - Conferma firma

Selezione del Lettore USB/Token USB

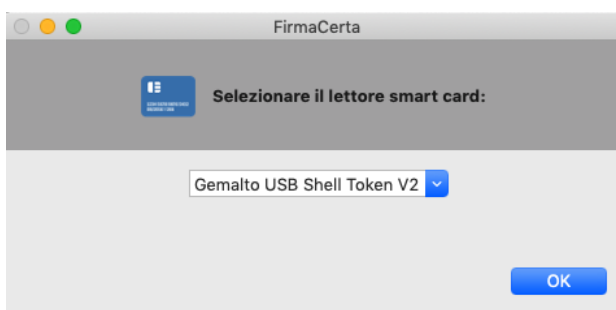


Figura 49 - selezione lettore

Inserire il PIN del dispositivo di Firma Digitale e cliccare su **OK**.

Nota:

Il codice PIN è stato fornito con la busta cieca

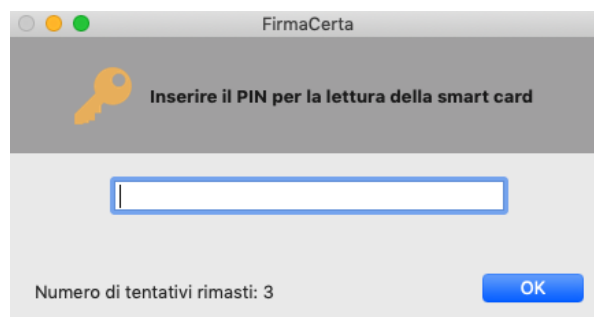


Figura 50 - inserimento PIN

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.



Figura 51 - completamento processo firma



6.4 APPENDICE D: COME VERIFICARE UN FILE

Dopo aver caricato il file da verificare e cliccato sulla funzione di **Verifica**, si aprirà una finestra di riepilogo.

Nota:

se compare la dicitura **il certificato di firma non è stato verificato** significa che non si è avviato in automatico (per avviare in automatico la verifica all'apertura è necessario andare a modificare [le opzioni di verifica](#)) la verifica delle firme, quindi deve essere avviato manualmente cliccando nel pulsante **Verifica**.

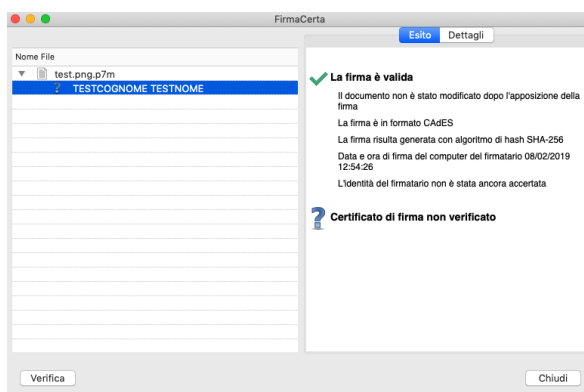


Figura 52 - Verify Panel

Nota:

se compare la dicitura **il certificato di firma non è stato verificato** significa che non si è avviato in automatico (per avviare in automatico la verifica all'apertura è necessario andare a modificare [le opzioni di verifica](#)) la verifica delle firme, quindi deve essere avviato manualmente cliccando nel pulsante **Verifica**.

Nella colonna di sinistra è mostrato il file che è stato firmato digitalmente e chi lo ha firmato.
esempio: in questo caso il file firmato è test.png.p7m ed è stato firmato TESTCOGNOME TESTNOME.

Nella colonna di destra viene mostrato l'**Esito** della verifica effettuata e in **Dettagli** viene approfondita indicando ad esempio:

- la tipologia di firma e la sua validità;
- l'ente che ha emesso il certificato;
- i dati del titolare;

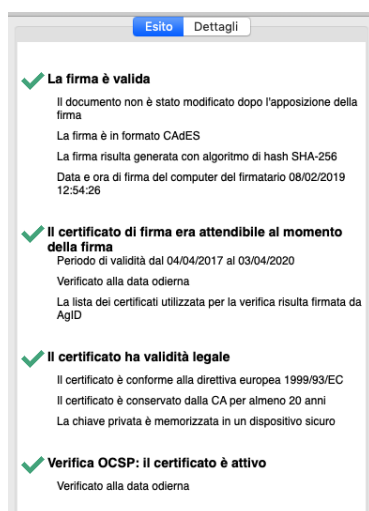


Figura 53 - esito verifica

Esito	
Identificativo	Valore
TIPOLOGIA	
Descrizione	Certificato di firma
Validità	Dal 04/04/2017 al 03/04/2020
Algoritmo	SHA-256
ENTE EMITTENTE	
Stato Ente Certificatore	IT
Organizzazione	Namirial S.p.A./02046570426
Unità Organizzativa	Certification Authority
Ente Certificatore	Namirial CA Firma Qualificata
TITOLARE	
Stato Firmatario	IT
Organizzazione	NON PRESENTE
Cognome	TESTCOGNOME
Nome	TESTNOME
Codice Fiscale Firmatario	IT:TSTTTN80A01A271U
Firmatario	TESTCOGNOME TESTNOME
Codice Identificativo	LOTT2017032272641608
QC STATEMENTS	
Compliance	presente
SSCD	presente
Retention period	20

Figura 54 - dettagli verifica



6.5 APPENDICE E: RINNOVO CERTIFICATI

Prima di procedere, verificare di avere installato e aggiornato all'ultima versione disponibile il software [FirmaCerta](#).
In caso di utilizzo del proxy si consiglia di chiedere i parametri di configurazione al proprio amministratore di rete.

6.5.1 CONFIGURAZIONE DEL PROXY

Accedere al software Firmacerta e nella barra degli strumenti cliccare su **Strumenti** > **Rinnovo certificati**, confermare le clausole e cliccare su **Avanti**.

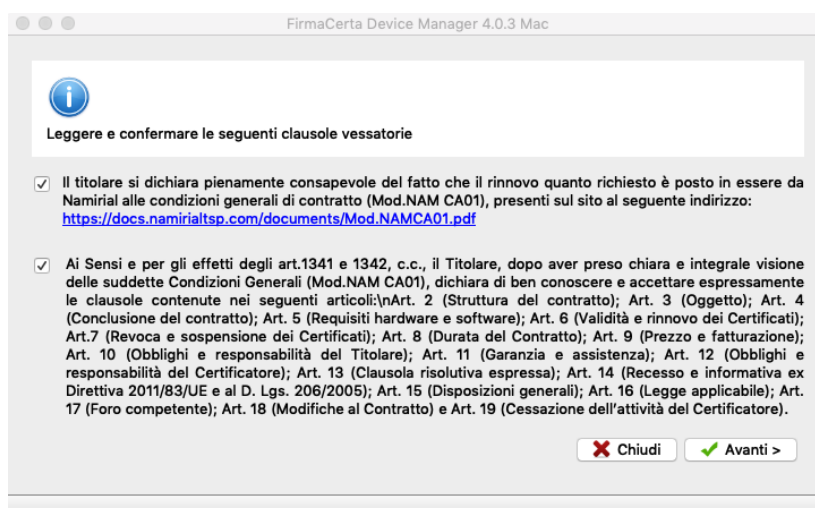


Figura 55 - Schermata Clausole Vessorie

Selezionare **Strumenti** > **Opzioni** ed impostare il proxy (per i parametri rivolgersi al proprio amministratore di rete). Cliccare su **Salva**.

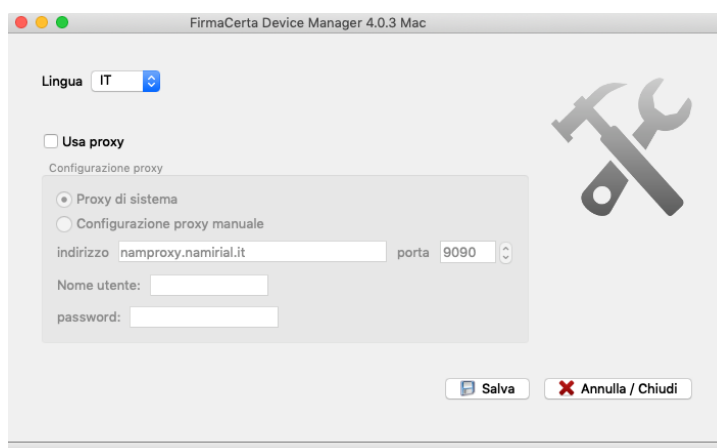


Figura 56 - Configurazione Proxy



6.5.2 MODALITÀ DI RINNOVO SMARTCARD E TOKEN

Con il dispositivo di Firma inserito aprire il software, *FirmaCerta*, quindi cliccare su **"Strumenti > Rinnovo Certificati"**. Leggere e confermare le clausole vessatorie quindi cliccare sul pulsante.

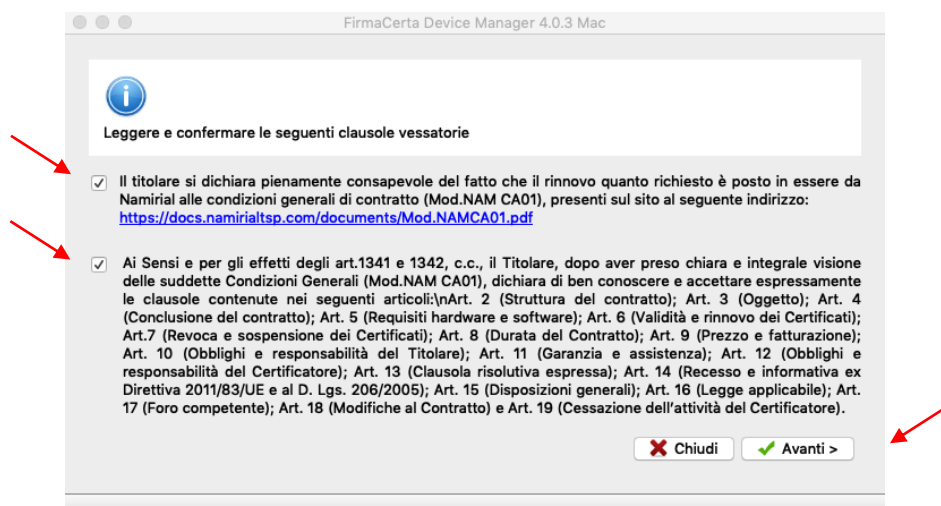


Figura 57 - Schermata Clausole Vessatorie

Quindi **"Selezionare il dispositivo"** ed immettere il **"Pin"** per il riconoscimento dello stesso e la lettura dei certificati.

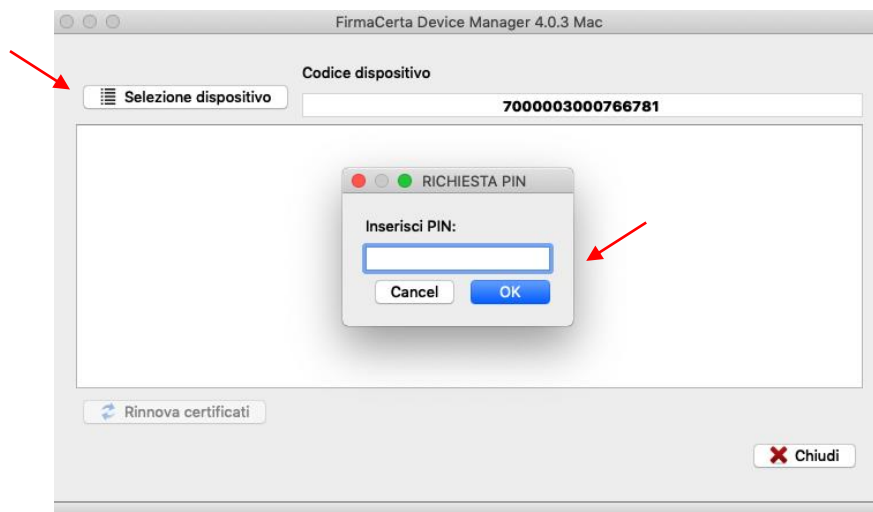


Figura 58 - Schermata Inserimento PIN

Nel processo di rinnovo certificati il Tool Device Manager proporrà di visualizzare (facoltativo) e firmare digitalmente (obbligatorio) un file .pdf di richiesta rinnovo. Selezionare **"OK"**, quando richiesto, per effettuare l'operazione di firma.



Attendere il completamento della procedura di rinnovo.

Cliccare su **"Rinnova Certificati"**.

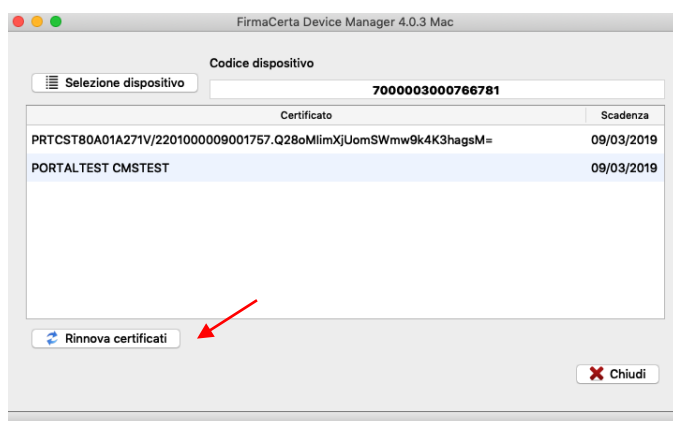


Figura 59 - Rinnovo Certificati

Premere Sì, se si desidera visualizzare il contratto
Premere No, per non visualizzarlo

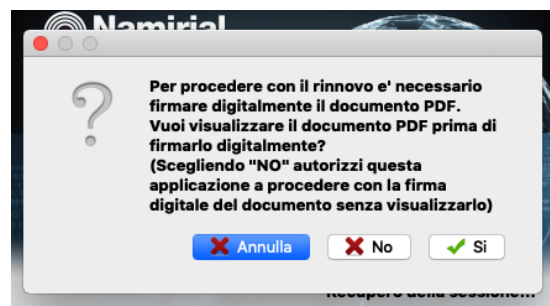


Figura 60 - Messaggio di visualizzazione del contratto

ATTENZIONE: Se è stato selezionato di visualizzare il Documento PDF, il programma mostrerà il contratto di rinnovo dei certificati.

Per concludere la procedura l'utente dovrà apporre la firma cliccando nel file che viene mostrato.

Attendere il completamento della procedura di rinnovo e concludere premendo OK.

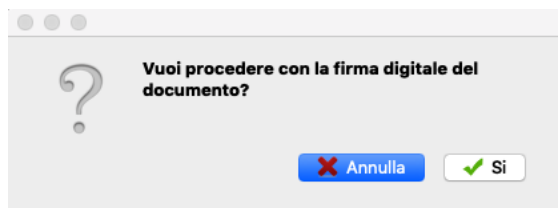


Figura 61 - Conferma apposizione della firma

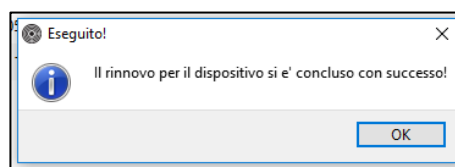


Figura 62 - Rinnovo completato con successo



6.6 APPENDICE F: GUIDA FIRMA REMOTA

6.6.1 COME FIRMARE UN FILE

Dopo aver caricato il file da firmare e cliccato sulla funzione di **Firma**, sarà richiesto all'utente di selezionare una cartella di destinazione dove salvare il documento firmato.

*In questo esempio è stata creata in precedenza una cartella dedicata per i file firmati digitalmente, quindi **selezionare** Documenti Firmati e poi click su **Apri**.*

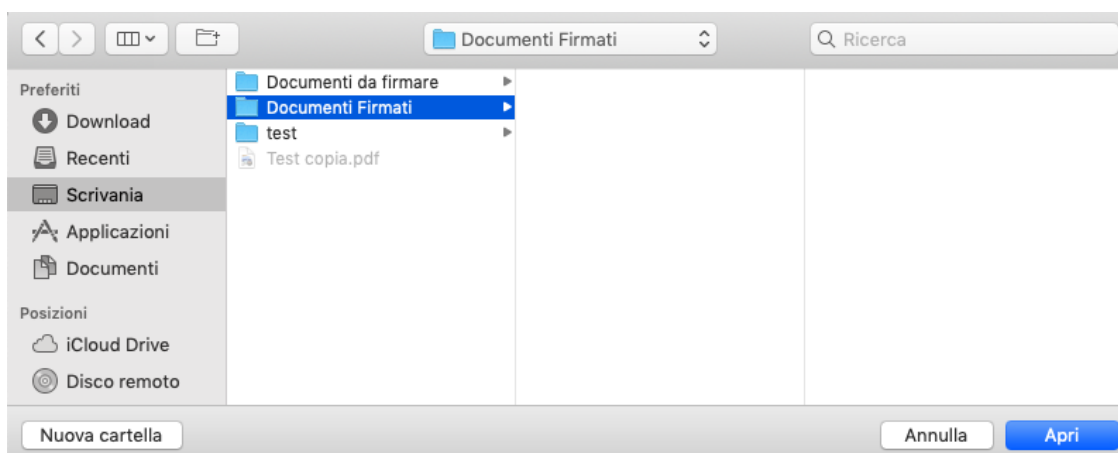


Figura 63 - selezione cartella di destinazione

6.6.1.1 SELEZIONE DEL FORMATO DI FIRMA

Selezionare il formato CAdES per firmare il file in formato .p7m.

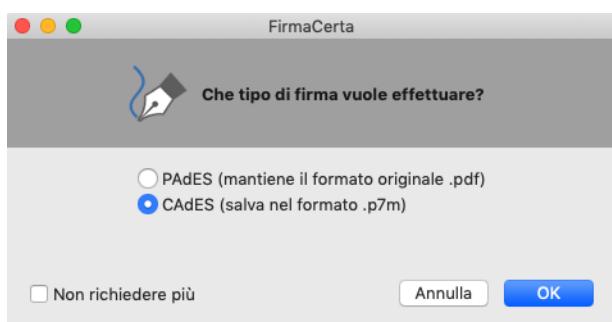


Figura 64 - selezione formato Cades

Selezionare il formato PAdES per firmare il file in formato .pdf.

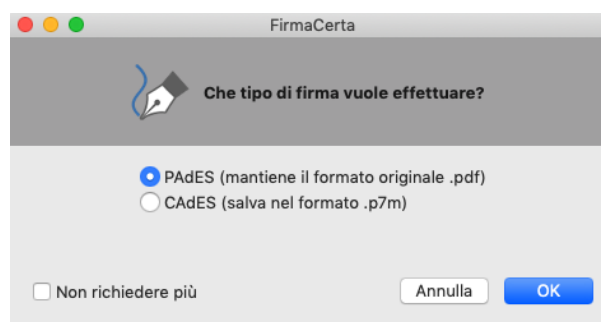


Figura 65 - selezione formato Pades

Nota: la scelta del formato con cui firmare il documento è disponibile solo per i file con estensione .pdf, per tutti gli altri formati sarà automaticamente applicata l'estensione .p7m

Contrassegnando con una spunta la voce **Non richiedere più**, verrà impostato l'automatismo e per rimuoverlo sarà necessario modificare le impostazioni nelle [Opzioni](#)



6.6.1.2 SELEZIONE DEL MOTIVO DI FIRMA

Questa funzione permette l'aggiunta di informazioni aggiuntive quali, il *motivo*, la *località* e le *informazioni di contatto* alla firma del documento.

Nota: Questa funzione è disponibile solamente per i documenti in formato .pdf
L'utilizzo di questa funzione è una scelta dell'utente in quanto è un Operazione Facoltativa.

Figura 66 - Motivo della firma

6.6.1.3 CONCLUSIONE PROCESSO DI FIRMA

Confermare l'apposizione della firma

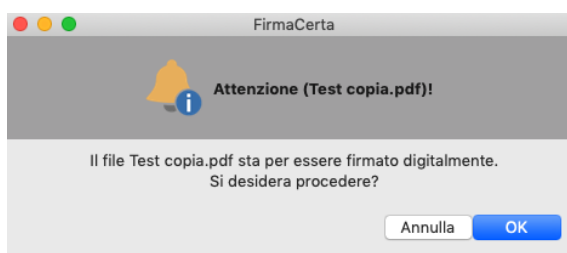


Figura 67 - conferma apposizione firma

Selezionare nel menu a discesa Firma Remota

Nota: la scelta tra quale dispositivo selezionare sarà disponibile solamente se è inserito un lettore USB o TokenUSB nel computer.



Figura 68 - selezione lettore: firma remota

Per continuare il processo di firma seguire le istruzioni in base al tipo di OTP che è stato selezionato in fase di registrazione:

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



6.6.2 PROCEDURA OTP VIRTUALE: NAMIRIAL OTP

6.6.2.1 INTRODUZIONE ALL'APPLICAZIONE NAMIRIAL OTP

Namirial Virtual OTP, un'applicazione per dispositivi mobile per l'utilizzo delle così dette One Time Password (o password usa-e-getta) e un primo utilizzo del software Firma Certa per utilizzare la firma remota su sistemi operativi Windows.

Questo tipo di password sono utilizzate quando è richiesta un'autenticazione con alto livello di sicurezza (autenticazione forte).

Il Virtual OTP può essere necessario:

- Per l'utilizzo della firma digitale di tipo remoto (brevemente Firma Remota);
- Per l'accesso SPID di livello 2 o superiore mediante servizio Namirial ID;
- Per l'accesso all'area privata dei servizi Namirial TS.

6.6.2.2 COME APRIRLA

Per questioni di sicurezza, l'apertura dell'App è possibile solo previa operazione di sblocco. Questo avviene:

- Se già impostato dall'utente, attraverso il meccanismo standard gestito dello Smartphone. Sui moderni cellulare sono normalmente utilizzabili le seguenti modalità:
 - Digitazione PIN;
 - Esecuzione del Segno;
 - Riconoscimento Biometrico: Impronta digitale (Touch ID), Riconoscimento del volto (Face ID)
- Se l'utente non ha impostato alcun meccanismo di blocco/sblocco, l'applicazione richiede di scegliere un apposito PIN da utilizzare.

6.6.2.3 ATTIVAZIONE NAMIRIAL OTP

Per eseguire la prima attivazione, l'utente deve avviare l'applicazione ed inserire il codice ricevuto via SMS al numero di cellulare registrato in fase di richiesta per l'attivazione del servizio (Firma Remota, SPID o altro servizio Namirial TSP). Di seguito, al solo titolo d'esempio, è mostrato un messaggio SMS per l'attivazione del Virtual OTP.

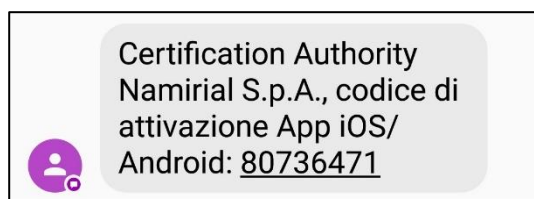


Figura 69 - SMS attivazione APP



6.6.2.4 ANDROID

Per l'attivazione del Virtual OTP è necessario fare tap su *Aggiungi OTP*

Di seguito, sono invece rappresentate la sequenza di azioni su Android che illustrano come procedere.



Figura 70 - Interfaccia Namirial OTP

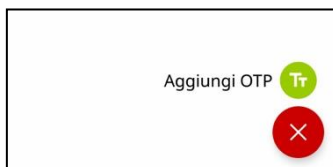


Figura 71 - Aggiungi OTP

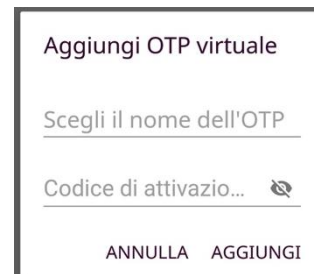


Figura 72 - Creazione OTP

6.6.2.5 IOS

Per l'attivazione del Virtual OTP è necessario fare tap su *Aggiungi OTP*

Di seguito, sono invece rappresentate la sequenza di azioni su iOS che illustrano come procedere.

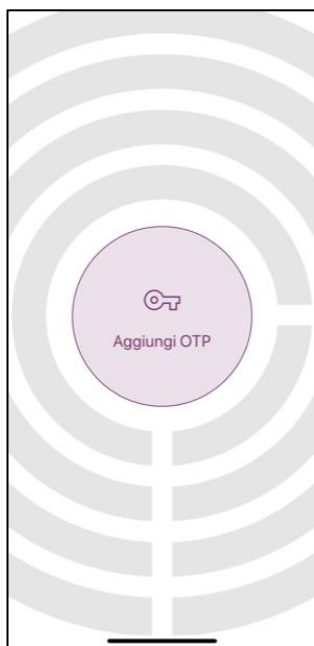


Figura 73 - Aggiungi OTP



Figura 74 - Creazione OTP



Nell'ultima schermata:

- **Virtual OTP Name:** è l'etichetta attribuibile al singolo token OTP per la quale può essere scelto un nome a piacimento (es. Firma). L'etichetta è di aiuto nell'individuare il token da utilizzare nel caso in cui sull'applicazione vengano attivati più token simultaneamente.
- **Codice di attivazione App:** qui va inserito il codice di attivazione ricevuto tramite SMS. nel campo *Token* (numero di 8 cifre), e infine cliccare su *Aggiungi*.

N.B: cliccando sull' icona  vedrete in chiaro il codice che inserito.

Al termine della procedura sarà mostrato a video un codice di 6 cifre che si aggiorna ogni 30 sec.

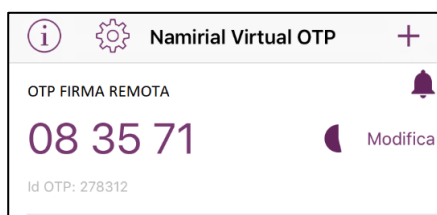


Figura 75 - Generazione OTP virtuale

6.6.2.6 INSERIMENTO PARAMETRI FIRMA REMOTA

Per recuperare i dati del certificato di firma remota è necessario Inserire l'Username fornito in fase di registrazione dei dati.

ATTENZIONE: In caso di smarrimento dell'username

Accedere alla propria area riservata al seguente indirizzo: <https://portal.namirialtsp.com>

Cliccare su "Non ricordo il nome utente" e seguire le indicazioni riportate.

Se il problema persiste contattare il supporto tecnico per e-mail all'indirizzo: helpdesk@firmacerta.it

Cliccando sul pulsante **Recupera**, verranno auto compilati i campi **Dispositivi virtuali** e **Tipo OTP**.

Figura 76 - Parametri Firma Remota: inserimento username

Figura 77 - Parametri Firma Remota: recupera dispositivi



Inserire il PIN ricevuto tramite Busta Cieca Digitale o Cartacea nel campo PIN.
Cliccare su Invia SMS e inserire il codice ricevuto **nel campo OTP**
Completare la procedura cliccando su **OK**.

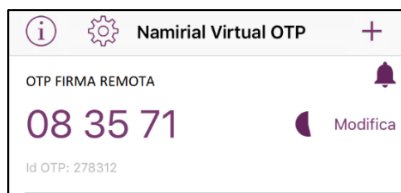


Figura 78 - OTP Generator

Figura 79 - inserimento PIN Parametri Firma remota

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.

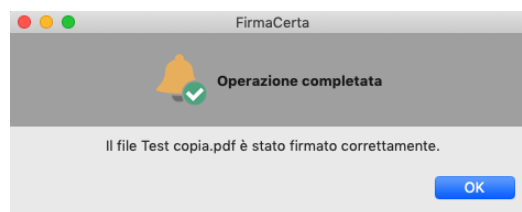


Figura 80 - Completamento Processo di firma



6.6.3 PROCEDURA OTP SMS

6.6.3.1 INSERIMENTO PARAMETRI FIRMA REMOTA

Per recuperare i dati del certificato di firma remota è necessario Inserire l'Username fornito in fase di registrazione dei dati.

ATTENZIONE: In caso di smarrimento dell'username

Accedere alla propria area riservata al seguente indirizzo: <https://portal.namirialtsp.com>

Cliccare su "Non ricordo il nome utente" e seguire le indicazioni riportate.

Se il problema persiste contattare il supporto tecnico per e-mail all'indirizzo: helpdesk@firmacerta.it

Cliccando sul pulsante **Recupera**, verranno auto compilati i campi **Dispositivi virtuali** e **Tipo OTP**.

Username: test

Dispositivi virtuali: [empty]

Tipo OTP: [empty]

OTP: [empty]

PIN: [empty]

Recupera

Invia SMS

Annulla OK

Figura 81 - Parametri Firma Remota: inserimento username

Username: test

Dispositivi virtuali: RHI1234567890123

Tipo OTP: 8381 12345678-1751115CGPI - SMS (Namirial)

OTP: [empty]

PIN: [empty]

Recupera

Invia SMS

Annulla OK

Figura 82 Parametri Firma Remota: recupero dati

Inserire il PIN ricevuto tramite Busta Cieca Digitale o Cartacea nel campo PIN.

Cliccare su Invia SMS e inserire il codice ricevuto nel campo OTP

Completare la procedura cliccando su **OK**.

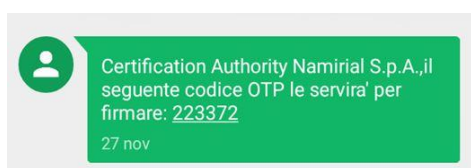


Figura 83 - SMS OTP

Username: test

Dispositivi virtuali: RHI1234567890123

Tipo OTP: 8381 12345678-1751115CGPI - SMS (Namirial)

OTP: 123456

PIN: *****

Recupera

Invia SMS

Annulla OK

Figura 84 - inserimento PIN firma remota

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.



Figura 85 - operazione completata





6.6.4 PROCEDURA CON OTP HARDWARE

6.6.4.1 ATTIVAZIONE OTP

Accedere all'[Area Privata Utente](#), inserendo le credenziali Username e Password che sono stati inviate all'indirizzo e-mail fornito in fase di registrazione.

RECUPERO CREDENZIALI AREA PRIVATA: In caso di smarrimento della username e/o della password, si può procedere al recupero dei singoli dati cliccando su "Non ricordo il nome utente" o "Non ricordo la password" e seguendo le indicazioni riportate, se il problema persiste contattare il supporto tecnico per e-mail all'indirizzo: helpdesk@firmacerta.it indicando il codice fiscale del titolare.

Al primo accesso il portale riconoscerà che il dispositivo OTP non è ancora attivo.

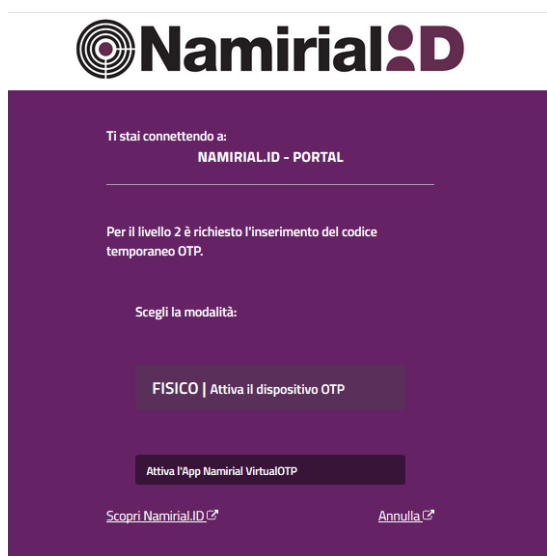


Figura 86 - attivazione OTP fisico

Generare il codice con l'OTP, premendo il pulsante sul dispositivo, infine aggiungere il codice generato nel campo *Codice OTP* e premere **Attiva OTP**.



Figura 87 - inserimento OTP fisico generato

6.6.4.2 INSERIMENTO PARAMETRI FIRMA REMOTA

Per recuperare i dati del certificato di firma remota è necessario Inserire l'Username fornito in fase di registrazione dei dati.

ATTENZIONE: In caso di smarrimento dell'username

Accedere alla propria area riservata al seguente indirizzo: <https://portal.namirialtsp.com>

Cliccare su "Non ricordo il nome utente" e seguire le indicazioni riportate.

Se il problema persiste contattare il supporto tecnico per e-mail all'indirizzo: helpdesk@firmacerta.it



Cliccando sul pulsante **Recupera**, verranno auto compilati i campi **Dispositivi virtuali** e **Tipo OTP**.

Figura 88 - Parametri Firma Remota: inserimento username

Figura 89 - Parametri Firma Remota: recupera dati

Inserire il PIN ricevuto tramite Busta Cieca Digitale o Cartacea nel campo PIN.

Generare il codice OTP utilizzando il dispositivo assegnato e **inserirlo nel campo OTP**

Completare la procedura cliccando su **OK**.



Figura 90 - OTP FISICO

Figura 91 - inserimento PIN

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.

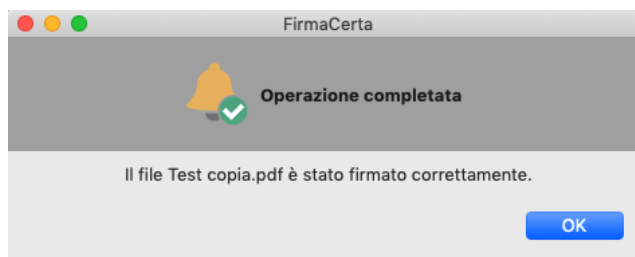


Figura 92 - operazione completata



6.7 APPENDICE G: AUTENTICAZIONE WEB

Per l'importazione dei certificati vi invitiamo a seguire la guida pubblicata nel nostro portale al seguente link: al punto 2.2 del manuale. <http://download.firmacerta.it/pdf/manualeAutenticazioneWeb.pdf>

6.8 APPENDICE H: BIT4ID – MACOS

Scaricare e installare il Driver Manager Bit4id PKI Manager, al seguente [link](#):

Aprire **Finder** > **Applicazioni**, altrimenti cliccare su **Launchpad** e ricercare il software **PIN Manager** nell'elenco delle applicazioni.

Aprire **Finder** > **Applicazioni** > **PIN Manager**

Cliccare su **Launchpad** e ricercare il software **PIN Manager** nell'elenco delle applicazioni.

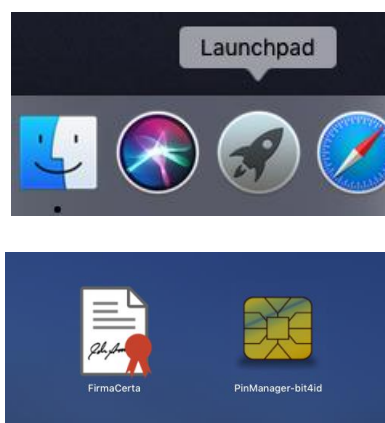
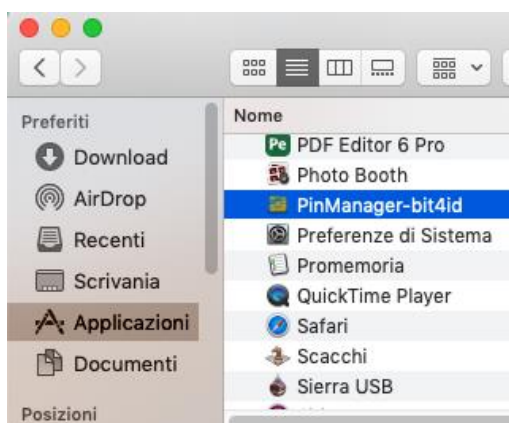


Figura 93 - PIN Manager: Launchpad

Il software Bi4id permette l'utilizzo delle funzioni Cambio PIN e Sblocco PIN sul dispositivo di firma Smartcard e token.

Il cambio PUK è una funzione attivabile solamente con la combinazione di tasti **CMD + A**

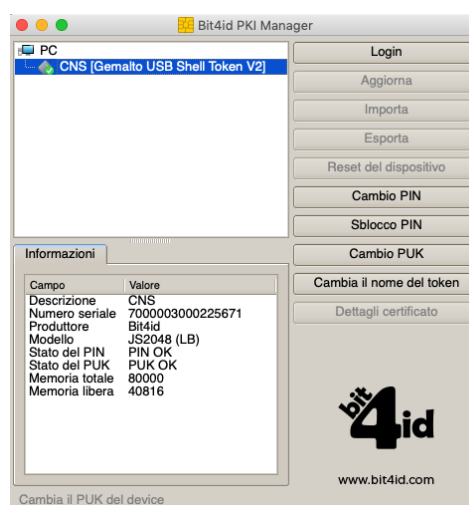
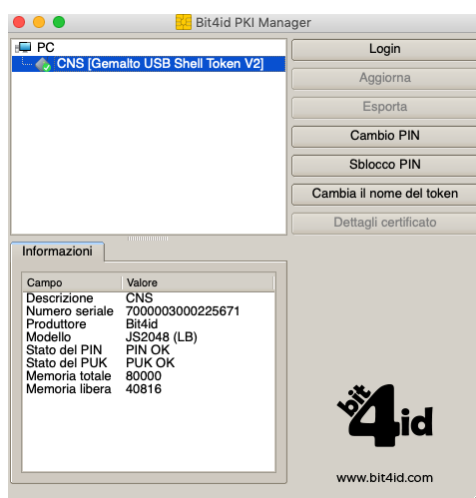


Figura 94 - Funzione Avanzate PIN Manager



6.8.1 CAMBIO PIN

Consente di modificare il PIN attuale attraverso l'inserimento di un nuovo PIN (inserimento e verifica).

Nota: Per i possessori di Firma Remota è possibile modificare il PIN dalla propria [Area Privata Utente](#) nella sezione > Utente > Firma digitale > Gestione.

Figura 95 - Funzione Cambio PIN

6.8.2 SBLOCCO PIN

Funzione necessaria per sbloccare il codice PIN. Inserire il Codice PUK (codice numerico di 8 cifre) presente nella busta cieca.

ATTENZIONE: prima di eseguire la procedura di sblocco è necessario possedere la Busta Cieca che è stata fornita in fase di Emissione.

Dopo 3 tentativi errati del Codice PUK il dispositivo si bloccherà irrimediabilmente e sarà necessario richiedere un nuovo dispositivo di firma.

Figura 96 - funzione di Sblocco PIN



6.8.3 CAMBIO PUK

Consente di modificare il PUK attuale assegnato da Namirial attraverso l'inserimento di un nuovo PUK a scelta dell'utente (inserimento e verifica).

N.B: per i possessori di Firma Remota non è possibile modificare il PUK.

ATTENZIONE:

Namirial non si ritiene responsabile dell'uso improprio di questa funzione. In caso di smarrimento del codice non sarà più possibile recuperarlo e sarà necessario richiedere un nuovo dispositivo di firma.

Figura 97 - funzione di Cambio PUK



RIFERIMENTI

NUMERO	DESCRIZIONE
[I]	<...>
[II]	<...>



INDICE DELLE TABELLE

Tabella 1 - Definizioni ed Acronimi.....	8
--	---

INDICE DELLE FIGURE

Figura 1 - installazione firmacerta	9
Figura 2 - installazione firmacerta Warning	9
Figura 3 - installazione firmacerta soluzione 1a	10
Figura 4 - installazione firmacerta soluzione 1b.....	10
Figura 5 - installazione firmacerta soluzione 2.....	10
Figura 6 - interfaccia grafica.....	11
Figura 7 - barra degli strumenti.....	11
Figura 8 - Visualizza Certificati	13
Figura 9 - esporta certificati	13
Figura 10 - inserimento Pin: verifica dispositivo.....	14
Figura 11 - esito verifica dispositivo	14
Figura 12 - Cambio PIN.....	14
Figura 13 - Sblocca PIN.....	15
Figura 14 - Cambio PUK.....	15
Figura 15 - Opzioni: Generali.....	16
Figura 16 - Opzioni: Gestione File	17
Figura 17 - Opzioni: Verifica.....	17
Figura 18 - Opzioni: Marche Temporal.....	18
Figura 19 - Opzioni: Aggiornamenti	18
Figura 20 - selezione cartella di destinazione	19
Figura 21 - selezione formato CAAdES.....	19



Figura 22 - selezione formato PAdES.....	19
Figura 23 - Motivo della Firma.....	20
Figura 24 - Conferma apposizione firma	20
Figura 25 - Selezione Lettore.....	20
Figura 26 - inserimento PIN	21
Figura 27 - Completamento processo di firma	21
Figura 28 - Selezione cartella di destinazione	22
Figura 29 - Conferma firma	22
Figura 30 - selezione Lettore	22
Figura 31 - Inserimento PIN	23
Figura 32 - Completamento processo di controfirma	23
Figura 33 - Configurazione Marche	24
Figura 34 - esito marche residue.....	24
Figura 35 - Selezione cartella di destinazione	25
Figura 36 - selezione formato Marca temporale.....	25
Figura 37 - File .p7m da marcare	26
Figura 38 - file .pdf da marcare.....	26
Figura 39 - inserimento parametri Marche	26
Figura 40 - conferma apposizione firma.....	27
Figura 41 - selezione lettore	27
Figura 42 - inserimento PIN	27
Figura 43 - operazione completata.....	27
Figura 44 - selezione formato Cades.....	28
Figura 45 - selezione formato Pades	28
Figura 46 - inserimento motivo della firma.....	29



Figura 47 - Parametri Marche	29
Figura 48 - Conferma firma	30
Figura 49 - selezione lettore	30
Figura 50 - inserimento PIN	30
Figura 51 - completamento processo firma	30
Figura 52 - Verify Panel	31
Figura 53 - esito verifica	31
Figura 54 - dettagli verifica	31
Figura 55 - Schermata Clausole Vessatorie	32
Figura 56 - Configurazione Proxy	32
Figura 57 - Schermata Clausole Vessatorie	33
Figura 58 - Schermata Inserimento PIN	33
Figura 59 - Rinnovo Certificati	34
Figura 60 - Messaggio di visualizzazione del contratto	34
Figura 61 - Conferma apposizione della firma	34
Figura 62 - Rinnovo completato con successo	34
Figura 63 - selezione cartella di destinazione	35
Figura 64 - selezione formato Cades	35
Figura 65 - selezione formato Pades	35
Figura 66 - Motivo della firma	36
Figura 67 - conferma apposizione firma	36
Figura 68 - selezione lettore: firma remota	36
Figura 69 - SMS attivazione APP	37
Figura 70 - Interfaccia Namirial OTP	38
Figura 71 - Aggiungi OTP	38



Figura 72 - Creazione OTP	38
Figura 73 - Aggiungi OTP.....	38
Figura 74 - Creazione OTP	38
Figura 75 - Generazione OTP virtuale	39
Figura 76 - Parametri Firma Remota: inserimento username	39
Figura 77 - Parametri Firma Remota: recupera dispositivi	39
Figura 78 - OTP Generator.....	40
Figura 79 - inserimento PIN Parametri Firma remota	40
Figura 80 - Completamento Processo di firma	40
Figura 81 - Parametri Firma Remota: inserimento username	41
Figura 82 Parametri Firma Remota: recupero dati.....	41
Figura 83 - SMS OTP	41
Figura 84 - inserimento PIN firma remota	41
Figura 85 - operazione completata.....	41
Figura 86 - attivazione OTP fisico	42
Figura 87 - inserimento OTP fisico generato	42
Figura 88 - Parametri Firma Remota: inserimento username	43
Figura 89 - Parametri Firma Remota: recupera dati.....	43
Figura 90 - OTP FISICO.....	43
Figura 91 - inserimento PIN	43
Figura 92 - operazione completata.....	43
Figura 93 - PIN Manager: Launchpad	44
Figura 94 - Funzione Avanzate PIN Manager	44
Figura 95 - Funzione Cambio PIN.....	45
Figura 96 - funzione di Sblocco PIN	45



Figura 97 - funzione di Cambio PUK46