Registration Authority

Guida FirmaCerta per Windows

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	**2.0**	**Gabriele Bocchini**
Approvato da	**Gabriele Bocchini**	Data di emissione	**31/10/2018**	_____

Namirial S.p.A.

Sede legale, direzione e amministrazione 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
C.F./ISCR. REG. IMPR. ANCONA N.02046570426 - P.I. IT02046570426 - CAP. SOC. € 6.500.000,00 i.v.
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com

UNI EN ISO 9001:2015 - Certificato N. 223776 | **UNI EN ISO 27001:2013** - Certificato N. IT280490

– Questa pagina è lasciata intenzionalmente in bianco –

INDICE

Indice **3**

Storia delle modifiche apportate **7**

Riferimenti **8**

Indice delle Figure **9**

1 Introduzione **14**

1.1 Scopo del documento e campo di applicazione 14

1.2 Definizioni ed Acronimi usati all'interno del documento 15

2 Installazione **17**

3 Interfaccia Grafica **20**

4 Funzioni Principali **21**

4.1 Firma: 21

4.1.1 Firma 21

4.1.2 ControFirma 21

4.2 Firma E Marca 22

4.3 Verifica 22

4.4 Marca 22

4.5 Gestione Dispositivo 23

4.5.1 Cambio Pin 23

4.5.2 Sblocco Pin 24

4.5.3 Attivazione Dispositivo 24

4.5.4 Visualizza Certificati 25

4.5.5 Verifica Dispositivo 26

4.5.6 Rinnovo Certificati 26

4.6 Firma Grafometrica ... 27
4.6.1 Firma Documento ... 27
4.6.2 Template di Firma ... 27
4.7 Utilità ... 30
4.7.1 Cifra e Decifra ... 30
4.7.2 Opzioni Generali ... 30
4.7.3 Proxy e Connessioni ... 34
4.7.4 Opzioni Firma ... 34
4.7.5 Opzioni Verifica ... 35
4.7.6 Opzioni Firma Grafometrica ... 36
4.7.7 Opzioni Marca Temporale ... 38
4.8 Help ... 39
5 Appendice A: Come Firmare e Controfirmare ... 40
5.1 Come firmare un documento ... 40
5.1.1 Firmare in CAdES - XAdES ... 40
5.1.2 Firmare in PAdES ... 42
5.2 Come Controfirmare ... 44
6 Appendice B: Come Marcare un file ... 47
6.1 Configurazione Parametri Marche Temporali ... 47
6.2 Come Firmare e Marcare ... 48
6.3 Come Separare la Marca ... 50
6.3.1 Firmare un documento in .p7m ... 50
6.3.2 Marcare un file Firmato in .p7m ... 51
6.3.3 Separare la Marca Temporale ... 53
7 Appendice C: Come verificare e Visualizzare un file ... 54

7.1 Per impostare in automatico l'avvio della verifca delle Firme ... 56

7.2 Come visualizzare un file firmato ... 56

8 Appendice D: Come Cifrare e Decifrare un file ... 57

8.1 Come Cifrare un file ... 57

8.2 Come Decifrare un file ... 58

9 Appendice F: Riga di Comando ... 59

9.1 Comandi e Parametri ... 59

9.2 Esempi: ... 60

10 Appendice G: Funzioni Avanzate ... 61

10.1 Firma di più Documenti ... 61

10.2 Marca di più documenti ... 62

10.3 Firma e Marca di più documenti ... 63

11 Appendice H: Rinnovo Certificati ... 64

11.1 Configurazione del Proxy ... 64

11.2 Modalità di Rinnovo ... 65

12 Appendice I : Configurazione Firma remota ... 68

12.1 Introduzione all'applicazione Namirial Otp ... 68

12.1.1 Come Aprirla ... 68

12.1.2 Configurazione l'Applicazione Namirial OTP ... 68

12.1.3 Android ... 69

12.1.4 iOS ... 70

12.2 Abilitazione Servizio Namirial SignEngine ... 71

12.3 Come firmare un documento ... 72

12.3.1 Username ... 73

12.3.2 Selezione Dispositivo Remoto ... 74

12.3.3 Firmare in formato PAdES 75

12.4 Procedura con OTP SMS 76

12.5 Procedura con OTP Mobile: Namirial OTP 77

12.6 Procedura con OTP Fisico 78

12.7 Attivazione OTP 78

13 Autenticazione WEB 80

STORIA DELLE MODIFICHE APPORTATE

VERSIONE	**2.0**
Data	31/10/2018
Motivazione	Aggiornamento del documento, con le nuove schermate del Software
Modifiche	

RIFERIMENTI

NUMERO	DESCRIZIONE
[I]	Guida Utente: Windows e Mac OS
[II]	<…>

INDICE DELLE FIGURE

Figura 1: installazione guidata firmacerta 17

Figura 2: seleziona cartella di destinazione 18

Figura 3: conferma d'installazione 18

Figura 4: messaggio di avvenuta installazione 19

Figura 5: interfaccia grafica firmacerta 20

Figura 6: sottomenù di firma 21

Figura 7: Introduzione funzione di firma 21

Figura 8: Introduzione funzione di controfirma 22

Figura 9: Introduzione funzione di firma e Marca 22

Figura 10: Introduzione funzione di verifica 22

Figura 11: Introduzione funzione di MArca 22

Figura 12: Pannello di Gestione Dispositivo 23

Figura 13: Funzione Cambio PIN 23

Figura 14: funzione di Sblocco PIN 24

Figura 15: funzione di attivazione dispositivo di firma 24

Figura 16: funzione di visualizza certificati 25

Figura 17: funzione di verifica dispositivo 26

Figura 18: Introduzione funzione di rinnovo certificati 26

Figura 19: Marcatore nel template 28

Figura 20: Sfondo Firma 28

Figura 21: Generale Proprietà di Firma 29

Figura 22: Chiavi di ricerca 29

Figura 23: Pannello di Utilità 30

Figura 24: Introduzione a FirmaCerta Protect 30

Figura 25: Pannello delle opzioni generali 32

Figura 26: Opzioni: Gestione File 32

Figura 27: Opzioni:URL 32

Figura 28: Opzioni Servizi Web 33

Figura 29: Opzioni: informazioni 33

Figura 30: Opzioni: Configurazione del Proxy 34

Figura 31: Pannello di Opzioni Firma 34

Figura 32: Opzioni: Logo PDF 35

Figura 33: Opzioni: Opzioni di Verifica 35

Figura 34: Pannello Opzioni firma Grafometrica 36

Figura 35: Opzioni Firma grafometrica 36

Figura 36: Opzioni Grafometrica: Attivazione Licenza 37

Figura 37: Opzioni Grafometrica: informativa Privacy 38

Figura 38: Opzioni Marca temporale 38

Figura 39: Pannello: Help 39

Figura 40: Pannello di Firma 40

Figura 41: Scelta formato di firma Cades-Xades 40

Figura 42: Selezione cartella di destinazione 41

Figura 43: Conferma di firma 41

Figura 44: Inserimento PIN 41

Figura 45: Operazione Completata 41

Figura 46: Scelta formato di firma Cades-Pades 42

Figura 47: Selezione cartella di destinazione 42

Figura 48: Conferma di firma 42

Figura 49: Inserimento PIN 43

Figura 50: informazioni di firma 43

Figura 51: Posizionamento del marcatore di firma 43

Figura 52: Conferma di posizionamento 43

Figura 53: Personalizzazione del logo 44

Figura 54: Operazione Completata 44

Figura 55: Pannello di Controfirma 44

Figura 56: Selezione cartella di destinazione 45

Figura 57: Conferma di sovrascrizione 45

Figura 58: Schermata di esempio: verifica file controfirmato 45

Figura 59: Conferma di firma 46

Figura 60: Inserimento Pin 46

Figura 61: Operazione Completata 46

Figura 62: Pannello di Utilità 47

Figura 63: Opzioni Configurazione Marche 47

Figura 64: Controllo Marche temporali 48

Figura 65: Selezione cartella di destinazione 49

Figura 66: Conferma di firma 49

Figura 67: Inserimento del PIN 49

Figura 68: Conferma credenziali Marche 49

Figura 69: Operazione Completata 49

Figura 70: Pannello di Firma 50

Figura 52: Selezione del formato di firma Cades 50

Figura 72: Pannello FirmaCerta 51

Figura 73: Scelta formato marca temporale 51

Figura 52: Scelta cartella di destinazione 51

Figura 75: conferma dati di configurazione Marche 52

Figura 76: Operazione Completata 52

Figura 77: Esempio: file marcato temporalmente 52

Figura 78: Pannello di Firma Certa 53

Figura 79: Separazione marca temporale 53

Figura 80: Selezionare il formato di marca 53

Figura 81: Esempio di file marcati 53

Figura 82: Pannello di Firmacerta 54

Figura 83: Schermata di verifica 54

Figura 84: Schermata di Esito 55

Figura 85: Schermata di Dettagli 55

Figura 86: Impostazioni di Verifica 56

Figura 87: schermata per visualizzare il file firmato 56

Figura 88: Schermata di Verifica con esempio 58

Figura 52: Accesso Negato 58

Figura 90: Configurazione per firma Pades 61

Figura 91: Configurazione per firma Cades 61

Figura 92: Schermata opzioni Generale 62

Figura 93: Schermata opzioni Marche 62

Figura 94: Schermata formato Marche 62

Figura 95: Schermata opzioni generali 63

Figura 96: Schermata opzioni Marche 63

Figura 97: Inserimento PIN 63

Figura 98: Schermata Clausole Vessatorie 64

Figura 99: Configurazione Proxy 64

Figura 100: Schermata Clausole Vessatorie 65

Figura 101: Schermata Inserimento PIN 66

Figura 102: Rinnovo Certificati 66

Figura 103: Messaggio di visualizzazione del contratto 66

Figura 104: Conferma apposizione della firma 67

Figura 105: Rinnovo completato con successo 67

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;

- La firma dei 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);
- Consente il drag & drop di uno o più file all'interno della stessa finestra di firma.
- Consente la firma di documenti .PDF protetti da password.

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 princìpi 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 detto timestamping. Un file marcato temporalmente ha estensione .m7m
Firma Grafometrica	è una modalità di firma elettronica che è realizzata secondo un processo che è in grado di associare ad un documento elettronico un insieme di dati ottenuti campionando una comune firma autografa
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.
XML: (eXtensible Markup Language)	è un metalinguaggio per la definizione di linguaggi di markup basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.
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.
Tool	Strumento, attrezzo.
Template	Sagoma. Si tratta di modelli predefiniti che rendono molto più semplice e veloce la composizione di una lettera, la creazione di un piccolo archivio ecc.
Adobe	è un'applicazione realizzata dalla Adobe Systems per creare e modificare file PDF. Adobe Acrobat, in quanto prodotto dalla stessa società che ha sviluppato il PDF, è stato il primo programma in grado di lavorare su questo formato.
Screenshot	Questo termine indica un'immagine, o una porzione d'immagine, "catturata" dallo schermo (screen).
Label	Etichetta, contrassegno
Bmp	File Bitmap. È il formato ufficiale di grafica per Windows (vedi Bitmap)

Bitmap	Letteralmente: "mappa di bit". Formato grafico (raster), tra i più diffusi, supportato in sostanza da tutti gli applicativi. Permette una memorizzazione dell'immagine senza perdita di informazioni. Alcune estensioni tipiche di file bitmap sono .BMP, .GIF, .JPG, .PNG, .TIFF.
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.
PDF/A	Standard internazionale (ISO19005), sottoinsieme dello standard PDF, appositamente pensato per l'archiviazione nel lungo periodo di documenti elettronici che devono poter essere visualizzabili sempre allo stesso modo, anche a distanza di tempo e con programmi software diversi.
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.
Add-on	Accessorio. In ambito hardware può rappresentare un qualunque dispositivo "esterno" (modem, scanner, monitor mouse, ecc.) da aggiungere al computer, in ambito software, invece, indica un modulo che aggiunge o estende le funzionalità di un dato programma base.

Tabella 1: Definizioni ed Acronimi

2 INSTALLAZIONE

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

Dopo aver eseguito il download del software, procedere con l'installazione guidata.

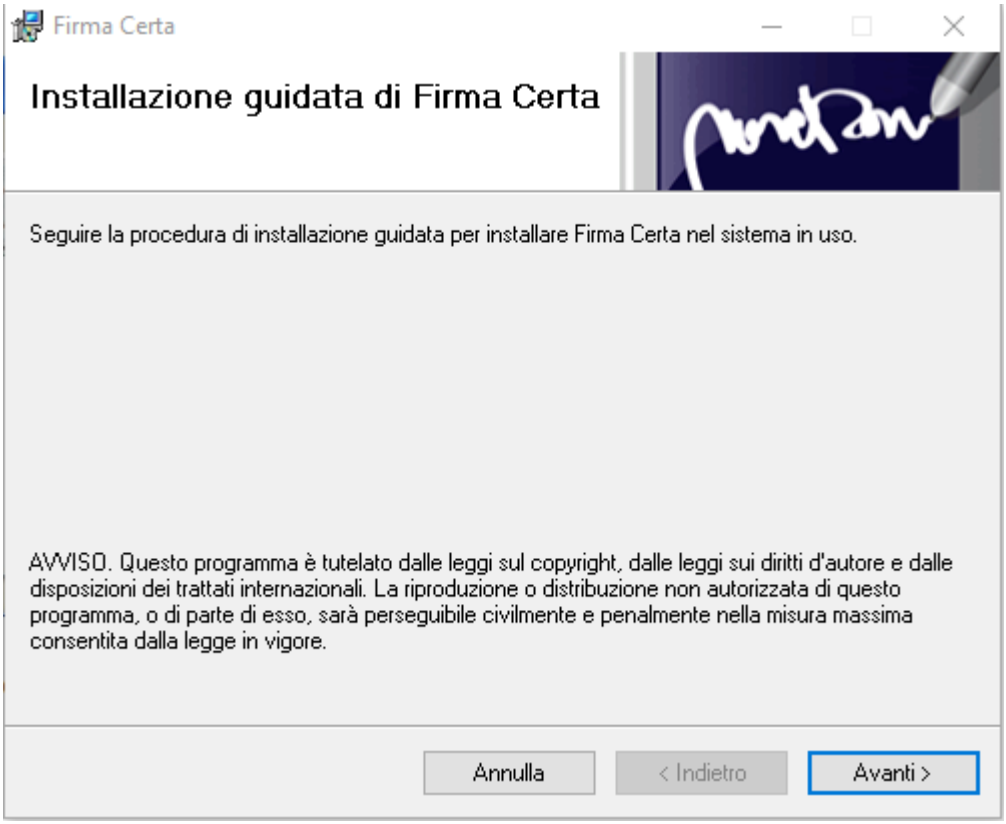


Figura 1: installazione guidata firmacerta

Dopo aver confermato le leggi sul copyright del software.
Il programma d'installazione proporrà di default la cartella dell'utente.

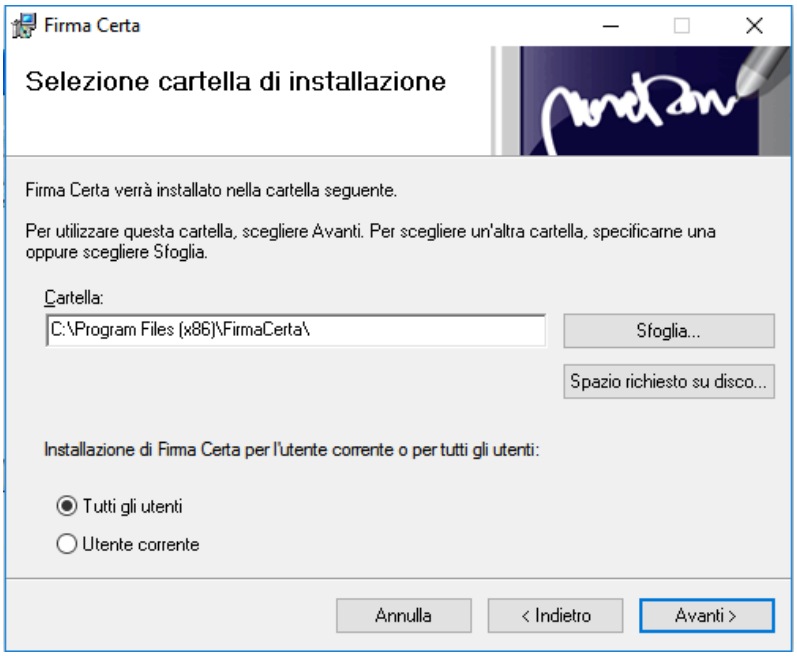


Figura 2: seleziona cartella di destinazione

IMPORTANTE: *se si desidera modificare la cartella di destinazione accertarsi di avere i permessi necessari o chiedere il supporto dell'amministratore di sistema.*
Premere avanti per avviare l'installazione.

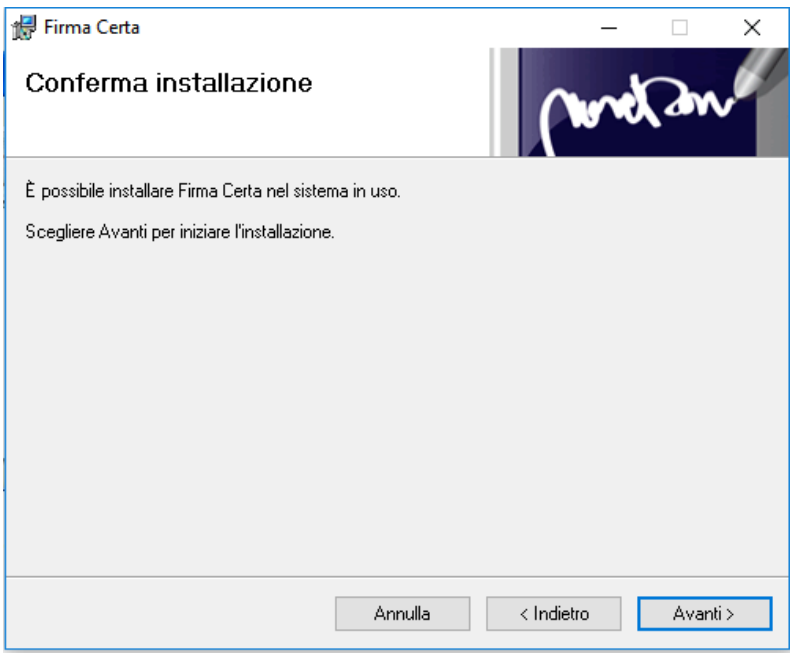


Figura 3: conferma d'installazione

Attendere fino al completamento dell'installazione.

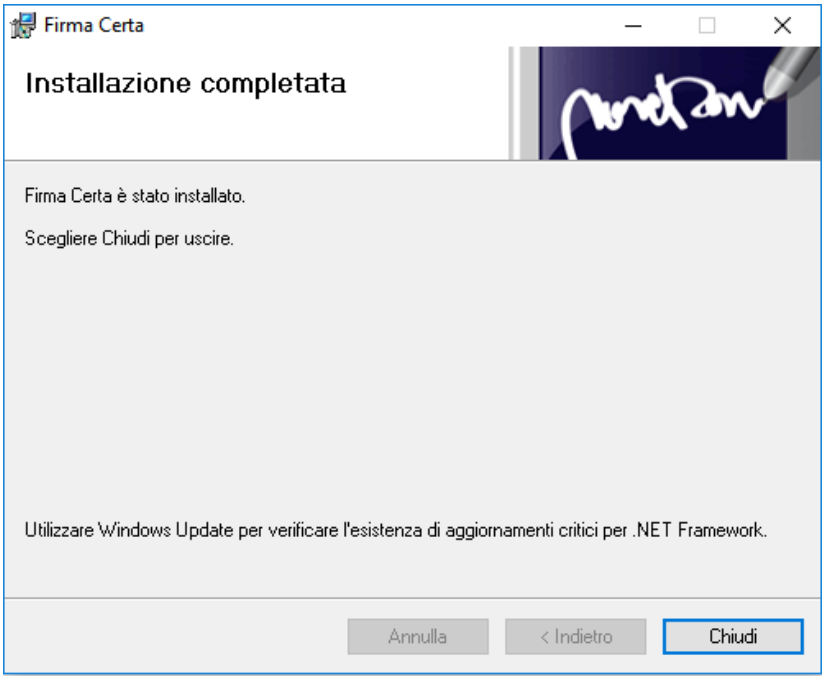


Figura 4: messaggio di avvenuta installazione

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;
- Utilizzare la Firma Grafometrica;
- Visualizzare e Verificare i file firmati digitalmente;

Figura 5: interfaccia grafica firmacerta

4 FUNZIONI PRINCIPALI

4.1 FIRMA:

Cliccando sull'icona Firma si avrà la scelta di Firmare o Controfirmare il file

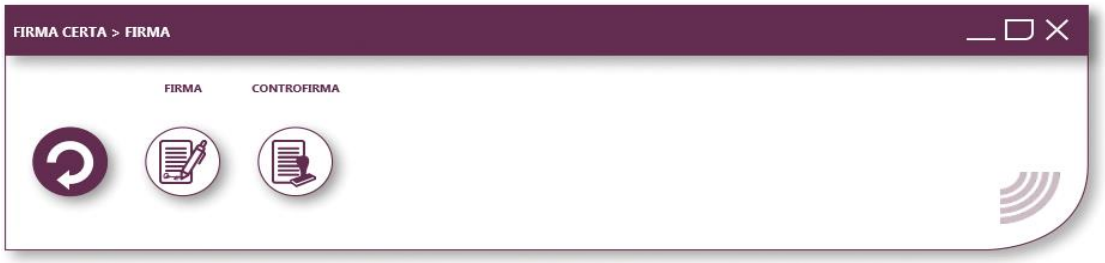


Figura 6: sottomenù di firma

4.1.1 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"*.
Dal File: Cliccando con il tasto destro del mouse direttamente sull'icona del/i file/s da firmare e selezionando all'interno del menu a tendina la voce *"Firma"*.
Dal Software: Cliccando direttamente sull'icona di Firma potrete ricercare all'interno del vostro computer il file che desiderate firmare.

Figura 7: Introduzione funzione di firma

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 I: Firma Remota

4.1.2 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 A: Come controfirmare

Figura 8: Introduzione funzione di controfirma

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 B: Come Firmare e marcare un documento

Figura 9: Introduzione funzione di firma e Marca

4.3 VERIFICA

Attraverso questa funzione si verifica e visualizza 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.
E' 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 C: Come verificare e visualizzare un file

Figura 10: Introduzione funzione di verifica

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 B: Come Marcare un file

Figura 11: Introduzione funzione di Marca

4.5 GESTIONE DISPOSITIVO

Questa funzione permette all'utente di accedere alle impostazioni del dispositivo di firma.

Figura 12: Pannello di Gestione Dispositivo

4.5.1 CAMBIO PIN

Consente di modificare il PIN attuale attraverso l'inserimento di un nuovo PIN (inserimento e verifica).
N.B: *per i possessori di Firma Remota non è possibile modificare il PIN.*

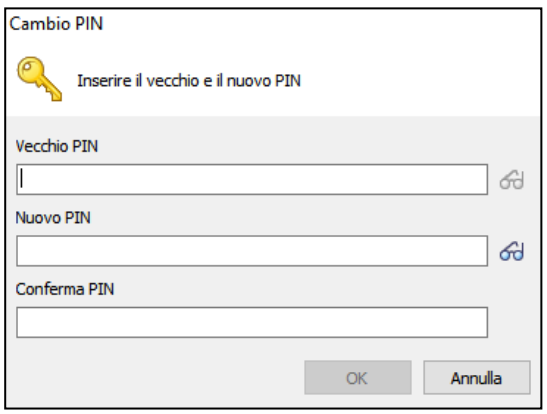


Figura 13: Funzione Cambio PIN

4.5.2 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.

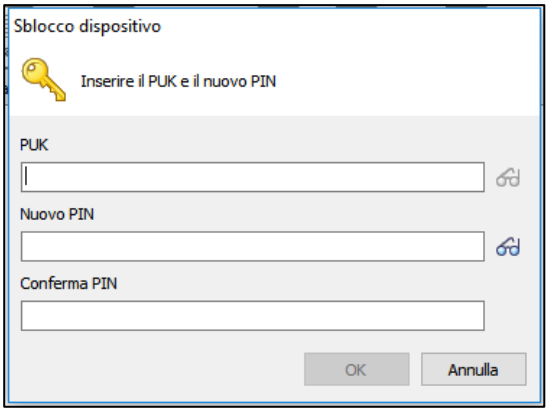
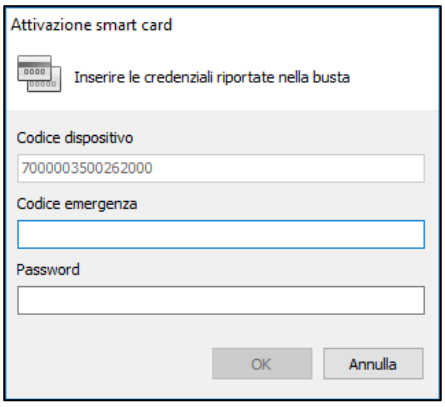


Figura 14: funzione di Sblocco PIN

4.5.3 ATTIVAZIONE DISPOSITIVO

Funzione necessaria per attivare i certificati presenti nel Dispositivo (Smartcard/Token), rilasciati con busta cieca cartacea, l'utente dovrà inserire Password e Cod. Emergenza.

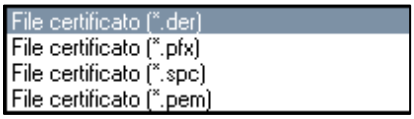


N.B: *Tutti i certificati emessi con busta cieca cartacea a partire dal 20/07/2017 non devono più essere attivati in quanto vengo rilasciati immediatamente attivi.*

Figura 15: funzione di attivazione dispositivo di firma

4.5.4 VISUALIZZA CERTIFICATI

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



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. Sono tipicamente usati nella piattaforma Java

PFX: **:** Il formato PKCS#12 o PFX è un formato binario che permette di salvare in modo criptato sia il certificato server e quelli intermedi, che la chiave privata. L'estensione utilizzata è solitamente .pfx o .p12. I file PFX sono di solito usati su macchine Windows per effettuare backup e migrazioni da un server all'altro di certificati con le loro rispettive chiavi private.

SPC: Formato più comunemente utilizzato dalle Certification Authorities per test

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 questo tasto si esegue semplicemente una cancellazione dell'elenco dei certificati rilevati nella smart card dalla finestra attiva (senza alcuna rimozione degli stessi dal supporto collegato).

Consente di accedere alle Opzioni di Verifica, accessibili anche dal menù di Firmacerta > Utilità.

Premendo questo tasto viene effettuata la verifica dei certificati presenti nella smart card. Cliccando sulle etichette *Esito* e *Dettagli* è possibile visualizzare il risultato del test eseguito e le particolarità del Certificato selezionato.

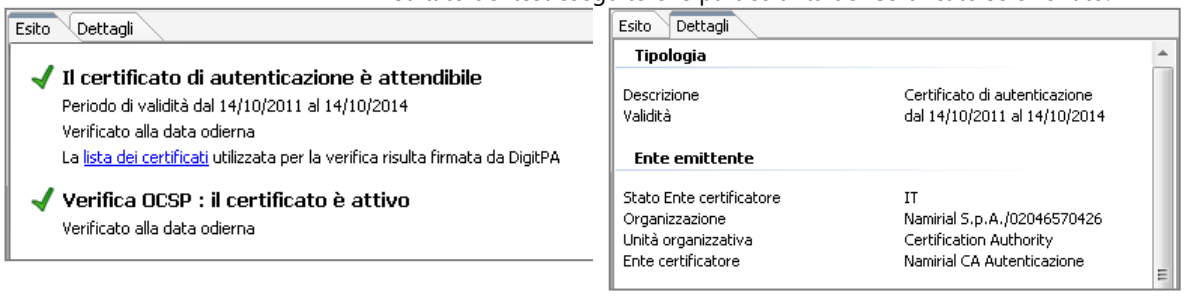


Figura 16: funzione di visualizza certificati

4.5.5 VERIFICA DISPOSITIVO

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).

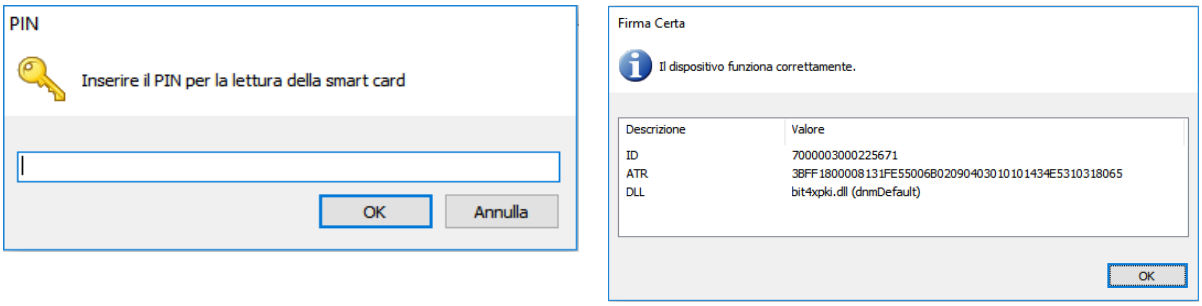


Figura 17: funzione di verifica dispositivo

4.5.6 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 H).

ATTENZIONE:

1. Se non compare nel menù, scaricare il software FirmaCerta Device Manager;
2. Se l'utente non viene sbloccato dal RAO, non sarà possibile completare il rinnovo;
3. Non è possibile rinnovare la firma remota;
4. Non è possibile eseguire un secondo rinnovo di firma digitale.

Figura 18: Introduzione funzione di rinnovo certificati

4.6 FIRMA GRAFOMETRICA

La firma grafometrica è una modalità di firma elettronica che è realizzata secondo un processo in grado di associare ad un documento elettronico un insieme di dati ottenuti campionando una comune firma autografa.

Tali dati sono ottenuti utilizzando un dispositivo che rileva e digitalizza l'immagine grafica di una firma apposta da una persona cui generalmente si aggiungono, secondo le caratteristiche del dispositivo utilizzato, altri parametri biometrici come pressione e velocità del tratto grafico. Il dispositivo è costituito da una tavoletta grafica che è in grado di mostrare al sottoscrittore il documento che sta firmando, ricreando così un'esperienza molto simile a quella della firma di un documento cartaceo.

4.6.1 FIRMA DOCUMENTO

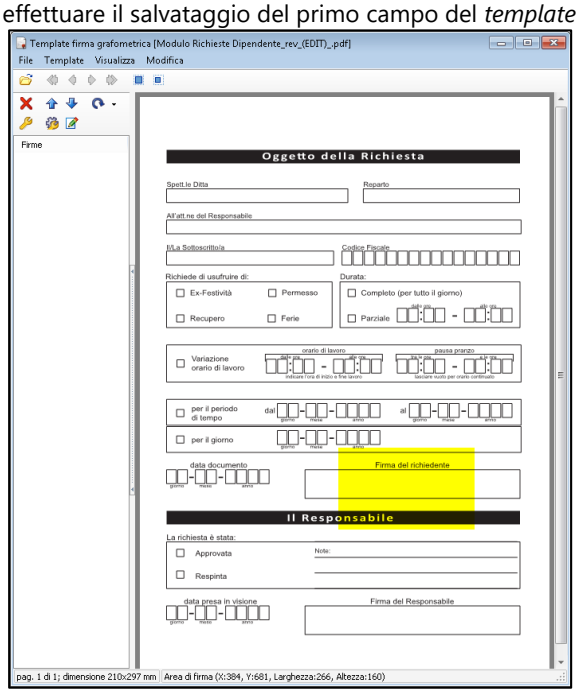
Con questa funzione è possibile caricare un file PDF che si desidera firmare con la firma grafometrica.

4.6.2 TEMPLATE DI FIRMA

Il presente *tool* consente la creazione di diversi modelli da utilizzare con l'abbinamento di documenti PDF durante la fase effettiva di firma grafometrica. I *template* permetteranno, selezionando un determinato documento, di rilevare immediatamente i campi di firma e quindi evidenziarli su tavoletta grafica senza che l'utente debba scorrere il PDF. Per capirne il funzionamento, si utilizzerà come esempio un documento generico per la richiesta di ferie e permessi (fig. sotto).

Dopo aver lanciato il *tool*, aprire da *File* il PDF che si desidera parametrizzare. In corrispondenza del puntatore comparirà un rettangolo giallo corrispondente all'area di firma, la cui superficie può essere aumentata o diminuita premendo i tasti corrispondenti sulla *Barra degli Strumenti* (fig. sotto).

Cliccare con il tasto sinistro (o destro) del mouse per effettuare il salvataggio del primo campo del *template*



Una volta selezionato il campo comparirà la seguente finestra.

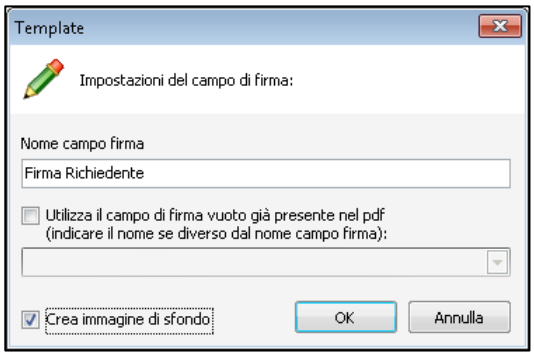
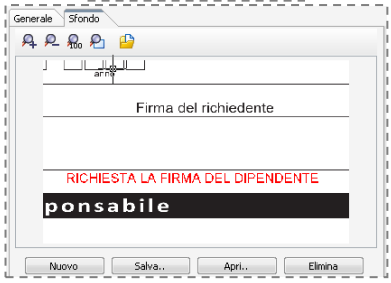


Figura 19: Marcatore nel template

Utilizza il campo di firma vuoto già presente nel pdf
Vengono rilevati eventuali campi di firma creati in precedenza sul documento tramite da *Adobe Acrobat*.

Crea Immagine di sfondo
Grazie a questa funzione è possibile realizzare uno *screenshot* dell'area di firma selezionata che può essere prima personalizzato e poi presentato con le modifiche effettuate durante la fase di firma autografa, in questo modo l'utente che si appresta a firmare su tavoletta grafica vedrà comparire sul display non solo la porzione corrispondente all'area selezionata ma anche le indicazioni inserite manualmente dall'operatore.

Per modificare lo sfondo occorre accedere alle *Proprietà* del campo firma salvato cliccando sull'icona corrispondente (fig. a lato) e spostarsi quindi sulla *Label* denominata *Sfondo*.

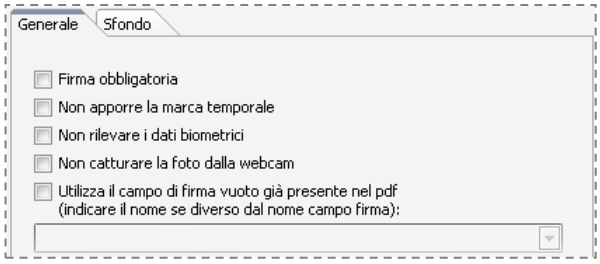


Premere il tasto *Salva* per eseguire il salvataggio dell'immagine in formato *.bmp*. A questo punto è possibile modificare il file con un qualsiasi editor grafico oppure utilizzarne uno già presente nel sistema operativo come *Paint*. Terminate le modifiche basterà richiamare l'immagine all'interno del campo firma utilizzando il tasto *Apri* (fig. a lato) e premere infine *OK* per la conferma delle operazioni.

Figura 20: Sfondo Firma

Si consiglia sempre di salvare le *bitmap* di un template nella stessa cartella, poiché in qualsiasi momento, dopo essere state modificate, potranno essere aggiornate all'interno del modello con la voce **Aggiorna sfondi di firma**.

Non utilizzare lo sfondo per la firma
Lo sfondo salvato non verrà mostrato sul display della tavoletta grafica in fase di firma autografa



Nella parte *Generale* delle *Proprietà firma* sono presenti le seguenti opzioni:

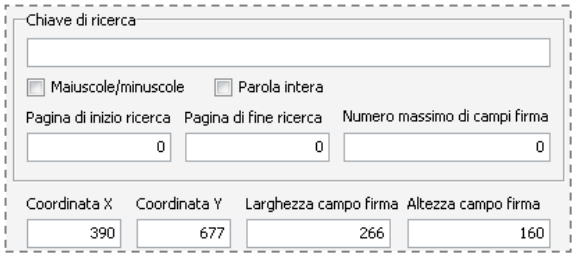
Firma obbligatoria
Obbliga l'utente a tracciare una firma autografa su tavoletta in corrispondenza del campo selezionato, senza consentire la possibilità di procedere al campo successivo o al salvataggio del documento.

Figura 21: Generale Proprietà di Firma

Non apporre la marca temporale
Tramite il software Firma Certa è anche possibile apporre la Marca Temporale sull'intero documento o sulle singole firme presenti all'interno di esso, selezionando il *check-box* in questione non verrà effettuato alcun *timestamping* sul campo firma selezionato.

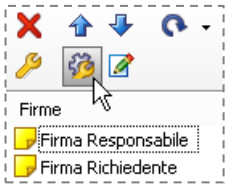
Non rilevare dati biometrici
Questa funzione impedisce al software di rilevare dalla firma i dati che contraddistinguono il soggetto firmatario acquisendo il solo tratto grafico.

Non catturare la foto dalla webcam
La scelta può essere valorizzata ad esempio nel caso in cui il pc non sia dotato di *webcam* o non sia necessario acquisire una foto del soggetto firmatario (che comunque sarebbe cifrata all'interno del documento)



Chiave di ricerca
Inserendo una parola presente all'interno del documento da firmare o indicando coordinate precise, sarà possibile creare dei campi firma liberi da altri parametri che compariranno al firmatario durante la fase di firma autografa. Ad esempio tale funzione avrebbe la sua utilità maggiore applicando un'etichetta con titolo su un modello .PDF utilizzato come "base" per altre

Figura 22: Chiavi di ricerca



Questa funzionalità consente di estendere due importanti preferenze (descritte in precedenza) a tutti i campi firma salvati nel *template*:

- ☐ Non utilizzare lo sfondo per la firma
- ☐ Non catturare la foto dalla webcam

4.7 UTILITÀ

Questa funzione permette di accedere alle principali impostazioni del software Firmacerta.

Figura 23: Pannello di Utilità

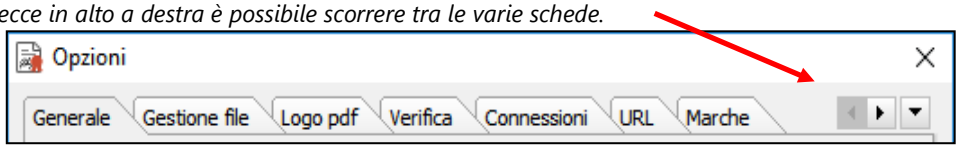
4.7.1 CIFRA E DECIFRA

È un'applicazione che consente la cifratura di file di ogni tipo e dimensione, nel rispetto della normativa vigente e degli standard tecnici di riferimento.
Molto versatile e di facile uso, Firma Certa Protect è disponibile per ambiente Windows.
Consultare la **guida** con le informazioni essenziali per l'uso di Firma Certa Protect (Vedi Appendice D).

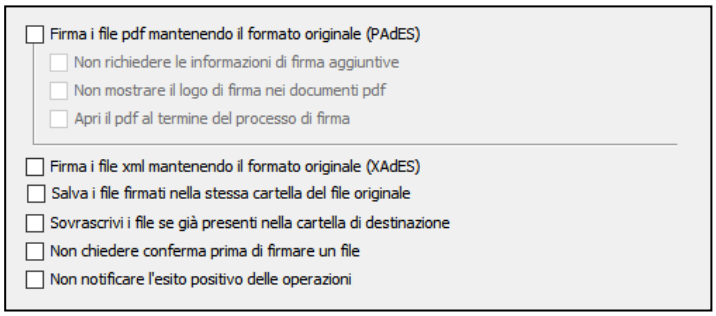
Figura 24: Introduzione a FirmaCerta Protect

4.7.2 OPZIONI GENERALI

In questa sezione è possibile modificare le impostazioni del software firmacerta.
N.B: *utilizzando le frecce in alto a destra è possibile scorrere tra le varie schede.*



è possibile eseguire alcune operazioni per la personalizzazione della firma.



Firma i file pdf mantenendo il formato (PAdES): 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;
- **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****.*
- **Apri il pdf al termine del processo di firma** Viene aperto il file PDF con il programma predefinito dopo l'applicazione della firma digitale.

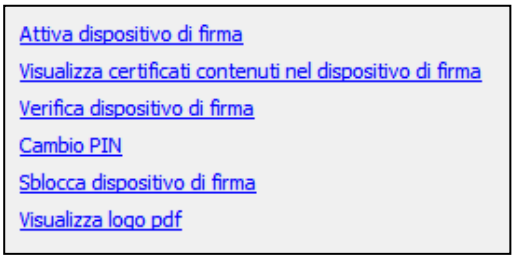
Firma i file xml mantenendo il formato originale (XAdES): mantiene il formato originale del file firmato, fornendo la possibilità di visualizzare i documenti anche ad un utente non fornito di software per la firma digitale.

Salva i file firmati nella stessa cartella del file originale: consente il salvataggio del file firmato nella stessa directory del file originale;

Sovrascrivi i file se già presenti nella cartella di destinazione: viene omesso il messaggio che segnala la presenza del file originale;

Non chiedere conferma prima di firmare un file: evita all'operatore di confermare la scelta ogni qualvolta effettui la firma di un documento.

Non notificare l'esito positivo delle operazioni: non mostra il messaggio di successo al termine della procedura.



Attiva dispositivo di firma: con l'inserimento del codice d'emergenza e della Password
N.B: operazione necessaria solo per i dispositivi richiesti con busta cieca cartacea.

Visualizza certificati contenuti nel dispositivo di firma: Consente di verificare i certificati contenuti nel dispositivo di firma e la validità degli stessi.

Verifica dispositivo di firma:	Consente di verificare attraverso l'immissione del PIN se il dispositivo di firma funziona correttamente.
Cambio Pin:	Consente di modificare il PIN attuale attraverso l'inserimento di un nuovo PIN (inserimento e verifica).
Sblocco dispositivo di firma:	Questa funzione permette di sbloccare attraverso l'inserimento del *PUK* e di un nuovo PIN (inserimento e conferma) il dispositivo di firma.
Visualizza logo pdf:	apre un pop-up in cui viene mostrato il logo pdf che è stato configurato nel software, dall'utente.

Figura 25: Pannello delle opzioni generali

4.7.2.1 GESTIONE FILE

Grazie alle scelte qui presenti è possibile:

- utilizzare Firma Certa come programma predefinito sia per aprire i file firmati digitalmente (.p7m), i file marcati temporalmente (.tsd, .tsr, .tst) e i file protetti(.p7e).
- codificare i file firmati digitalmente (.p7m), i file marcati temporalmente (.tsd, .tsr, .tst) e i file protetti(.p7e) in formato *Base64*.
- *Creare il file contenente l'impronta del file marcato.*

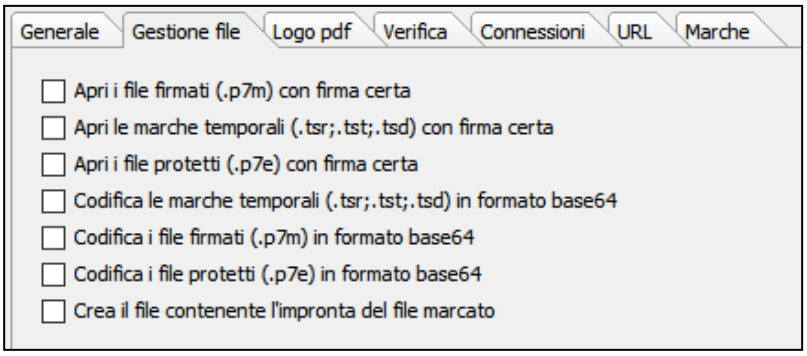


Figura 26: Opzioni: Gestione File

4.7.2.2 URL

Il percorso indica l'indirizzo web al quale il software si collega per scaricare eventuali aggiornamenti (si consiglia di non modificare mai i dati presenti di *default*).

Figura 27: Opzioni:URL

4.7.2.3 SERVIZI WEB

Nella sezione Servizi Web è possibile attivare il plug-in per l'utilizzo della Firma Remota. Per Abilitare il servizio è necessario selezionarlo e cliccare su Abilita/Disabilita.

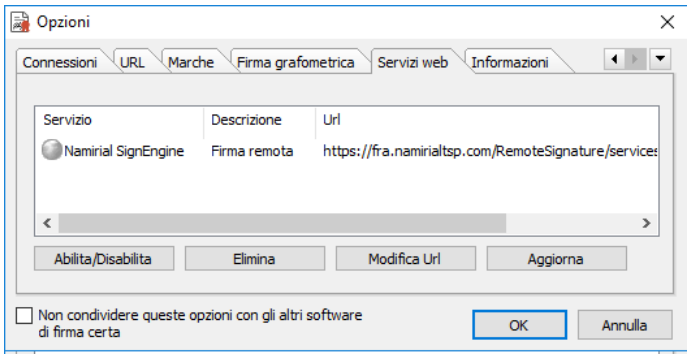


Figura 28: Opzioni Servizi Web

4.7.2.4 INFORMAZIONI

In questa sezione è possibile verificare le informazioni del software Firmacerta, quali la versione del installato, modificare la lingua del software;

N.B: *E' buona norma tenere sempre aggiornato il software, per garantire gli adempimenti normativi ed eventuali migliorie apportate.*

Figura 29: Opzioni: informazioni

4.7.3 PROXY E CONNESSIONI

Questa funzionalità deve essere utilizzata solo se l'accesso ad Internet per il protocollo HTTP è effettuato tramite un server *Proxy*. Il sistema permette di impostarne il nome, la porta a cui è collegato, l'identificativo e la password di accesso ad Internet dell'utente di FirmaCerta.

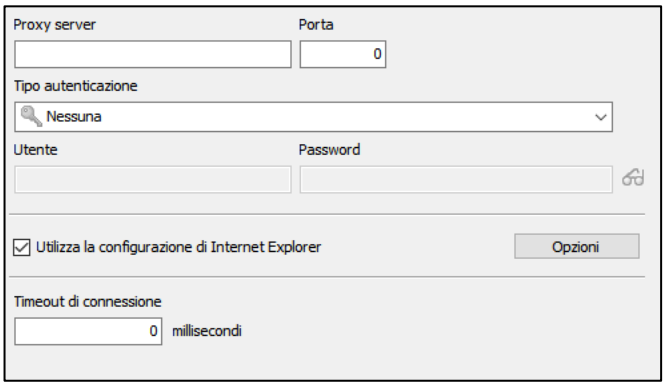


Figura 30: Opzioni: Configurazione del Proxy

4.7.4 OPZIONI FIRMA

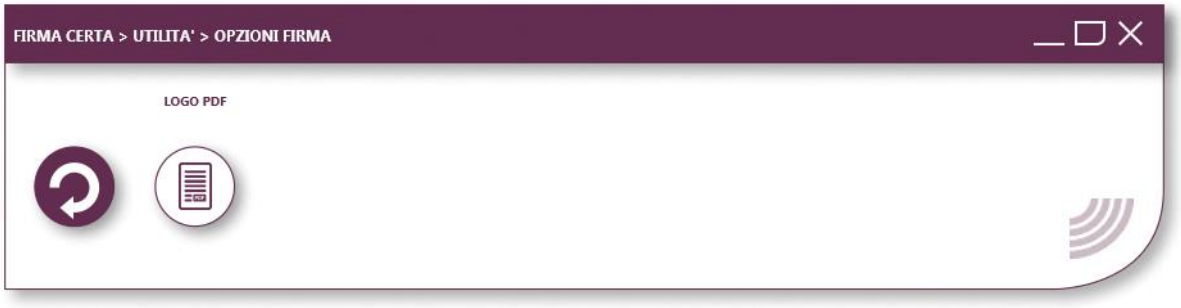


Figura 31: Pannello di Opzioni Firma

4.7.4.1 LOGO PDF

Consente di Modificare il logo predefinito di Namirial e permette l'inserimento di un logo personale in un documento PDF quando si applica la firma a questo tipo di documenti.

È possibile impostare l'effetto trasparenza selezionando due colorazioni diverse, personalizzare il testo da applicare sopra il logo, incorporare il *font,* nel sistema operativo per maggiore compatibilità con i *PDF/A*.

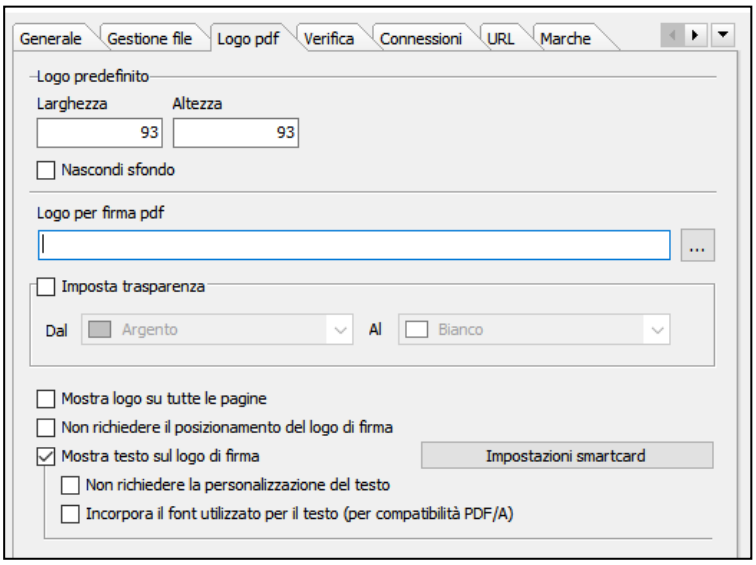


Figura 32: Opzioni: Logo PDF

4.7.5 OPZIONI VERIFICA

Permette di verificare, contestualmente alla visualizzazione di un file firmato digitalmente, lo stato del certificato (attivo/revocato/sospeso).

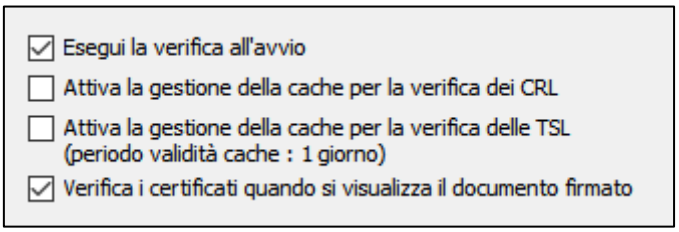


Figura 33: Opzioni: Opzioni di Verifica

4.7.6 OPZIONI FIRMA GRAFOMETRICA

Questa funzione permette all'utente di accedere alle Utilità relative ai dispositivi di firma grafometrica.

Figura 34: Pannello Opzioni firma Grafometrica

4.7.6.1 OPZIONI

Nelle preferenze per la Firma Grafometrica è possibile utilizzare sia uno dei tre modelli di tavoletta *Wacom* in elenco, sia, in alternativa, uno dei *tablet* certificati per tale operazione (per maggiori informazioni visitare la pagina Dispositivi Utilizzabili del sito www.firmagrafometrica.it).

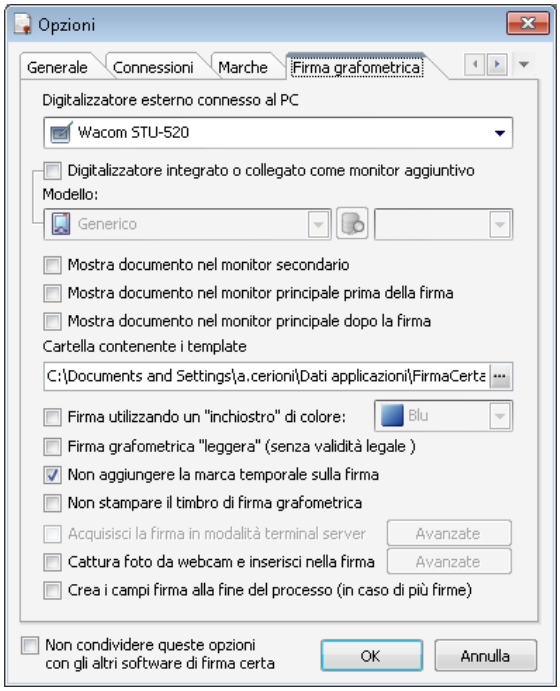


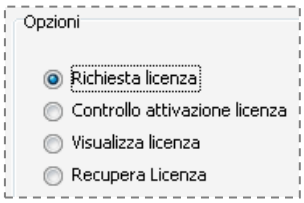
Figura 35: Opzioni Firma grafometrica

4.7.6.2 ATTIVAZIONE

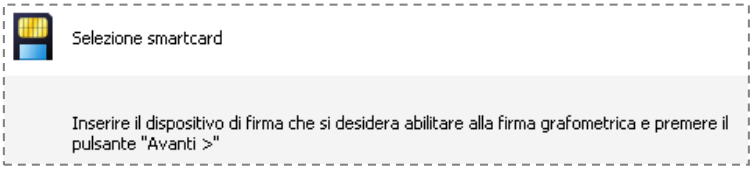
L'utente che desidera attivare il software riceve tramite mail un certificato di cifratura tecnico che deve essere installato nel pc.
Questo certificato è necessario per l'attivazione della licenza di firma grafometrica.

Per *richiedere l'attivazione* della funzionalità di Firma Grafometrica, procedere come descritto:

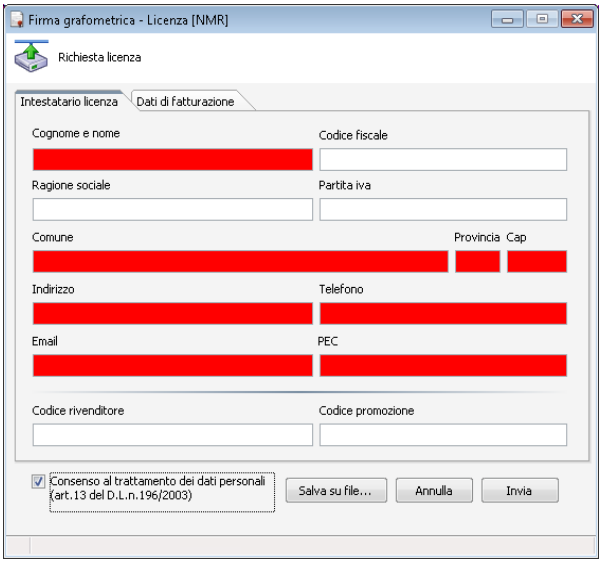
Selezionare l'opzione *Richiesta Licenza* e premere il pulsante *Avanti;*



Premere il pulsante *Avanti;*



Compilare i campi in finestra con i dati dell'intestatario della licenza e premere il pulsante *Invia*.



Al termine della procedura la CA Namirial prenderà in carico la richiesta ed entro poche ore abiliterà il dispositivo digitale alla Firma Biometrica.

Figura 36: Opzioni Grafometrica: Attivazione Licenza

4.7.6.3 INFORMATIVA

La funzione consente la compilazione da parte del firmatario di redigere e firmare grafometricamente, mediante dispositivo digitale collegato (tavoletta grafica o altro hardware supportato) un documento PDF informativo sul funzionamento della Firma grafometrica in genere e sul trattamento dei documenti informatici in sostituzione del cartaceo. Per portare a termine l'operazione verrà richiesto al firmatario, dopo l'inserimento del proprio *Codice Fiscale* e *Nominativo* in una finestra iniziale (fig. a lato), di utilizzare le procedure applicate alle operazioni di firma grafometrica scrivendo sul display del dispositivo prima la data e poi la propria firma. Se non si dovesse utilizzare la presente procedura accedendo direttamente da questo menù, tale richiesta verrà comunque presentata al firmatario alla prima operazione di firma di un qualsiasi documento.

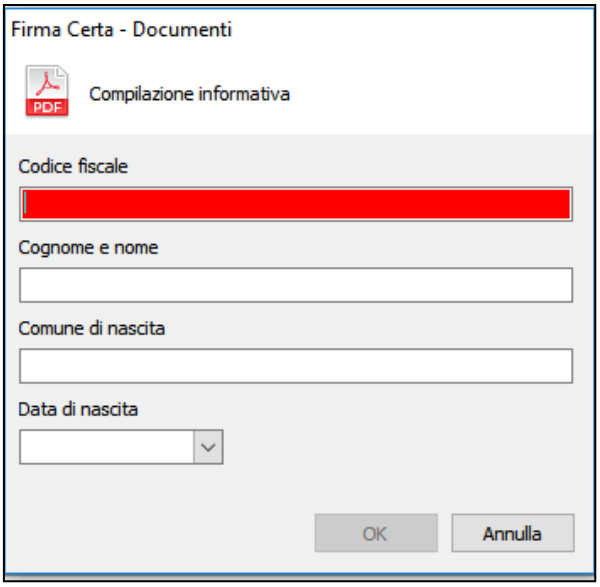
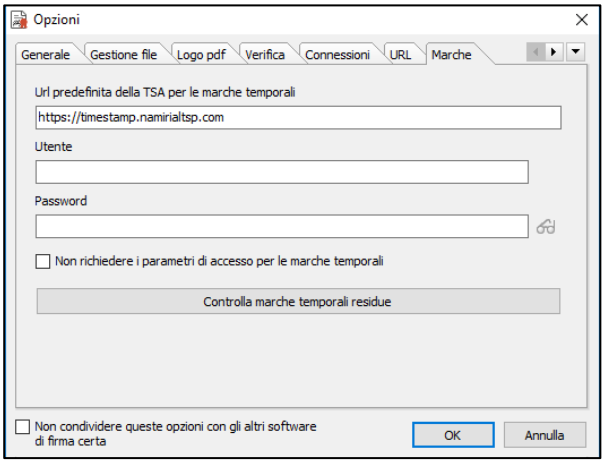


Figura 37: Opzioni Grafometrica: informativa Privacy

4.7.7 OPZIONI MARCA TEMPORALE

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.



LINK per l'utilizzo delle Marche Temporali

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

Figura 38: Opzioni Marca temporale

4.8 HELP

In questa sezione è possibile consultare la *Guida Utente* del software sempre aggiornata inoltre è possibile eseguire un controllo manuale di eventuali aggiornamenti disponibili per il software Firma Certa, cliccando su *Controllo Aggiornamenti*

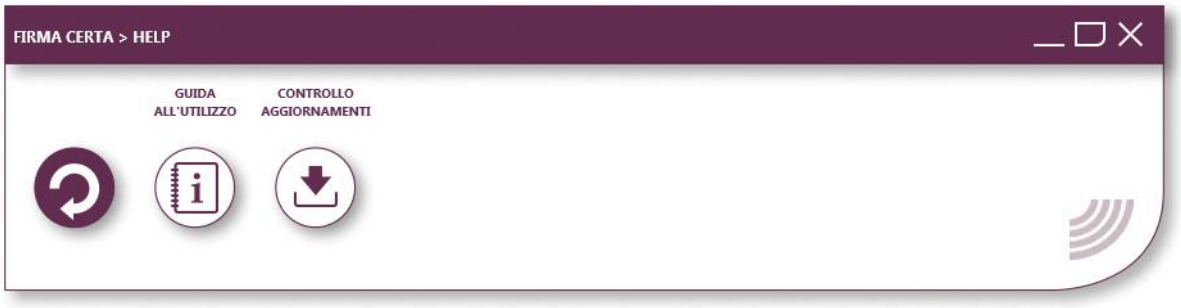


Figura 39: Pannello: Help

5 APPENDICE A: COME FIRMARE E CONTROFIRMARE

5.1 COME FIRMARE UN DOCUMENTO

Caricare il file da firmare all'interno del programma e cliccare su ***Firma***.

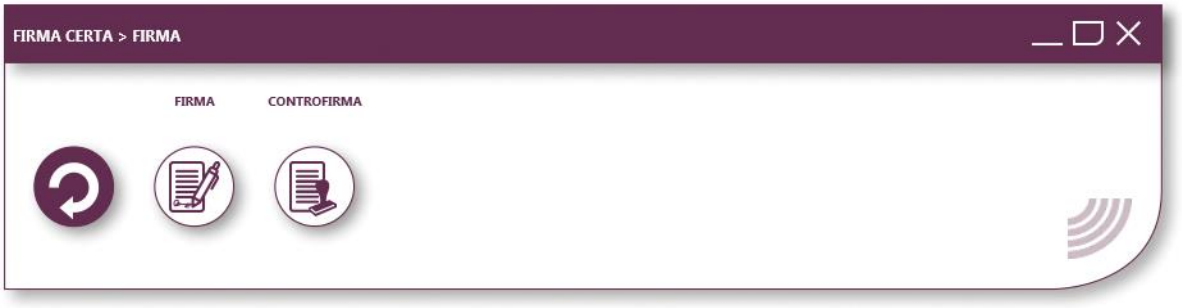


Figura 40: Pannello di Firma

N.B: Il software Firmacerta permette di firmare qualsiasi tipo di file in formato CAdES ovvero in .p7m, soltanto per i file PDF o XML chiederà all'utente con un messaggio a video se firmare in .P7M o mantenere il formato originale.

5.1.1 FIRMARE IN CADES - XADES

Dopo aver cliccato su firma si aprirà una finestra che vi chiede in che formato firmare il documento.

- Premere ***Si***, per effettuare una firma XAdES, mantenendo il formato .xml (valido solo per file XML)
- Premere ***No***, per effettuare una firma CAdES con il formato .p7m

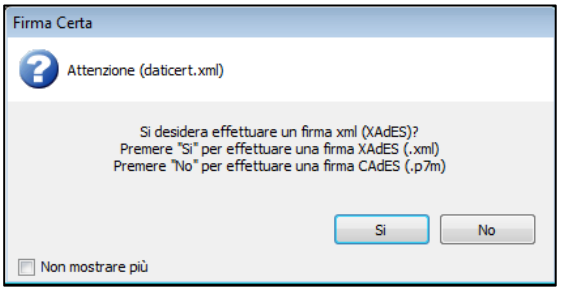


Figura 41: Scelta formato di firma Cades-Xades

Selezionare la Cartella di destinazione del File Firmato, infine cliccare ***OK***.

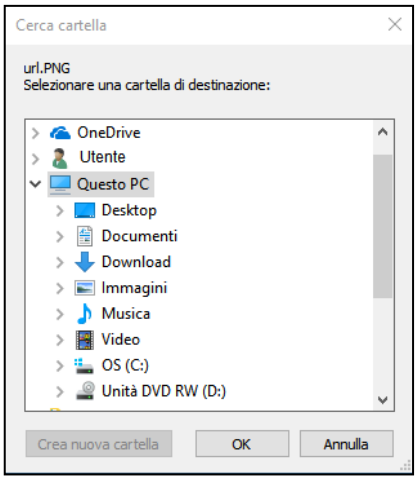


Figura 42: Selezione cartella di destinazione

Procedere con l'operazione di Firma premendo ***Si.***

N.B: *Consigliamo di creare una cartella dedicata per i File Firmati Digitalmente, così da evitare problemi.*

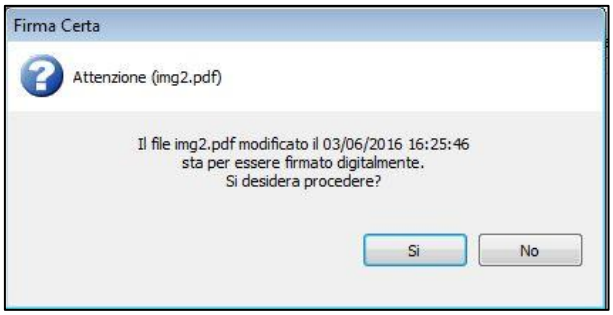


Figura 43: Conferma di firma

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

Figura 44: Inserimento PIN

Attendere il tempo di elaborazione e premere ***OK*** per concludere la procedura.

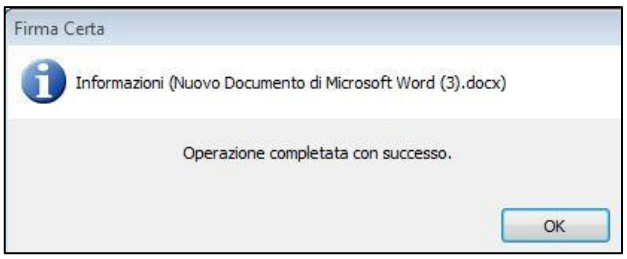


Figura 45: Operazione Completata

5.1.2 FIRMARE IN PADES

Dopo aver cliccato su firma si aprirà una finestra che vi chiede in che formato firmare il documento.

- Premere ***Si***, per effettuare una firma PAdES, mantenendo il formato .xml (valido solo per file PDF)
- Premere ***No***, per effettuare una firma CAdES con il formato .p7m

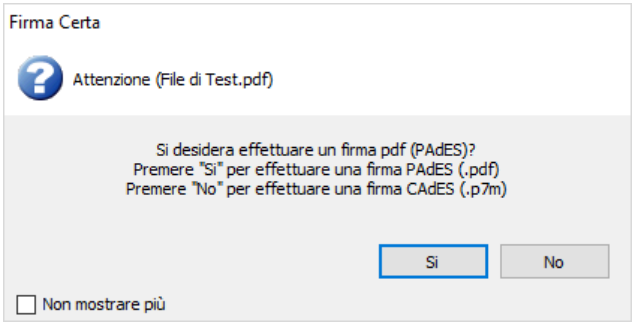


Figura 46: Scelta formato di firma Cades-Pades

Selezionare la Cartella di destinazione del File Firmato, infine cliccare ***OK***.

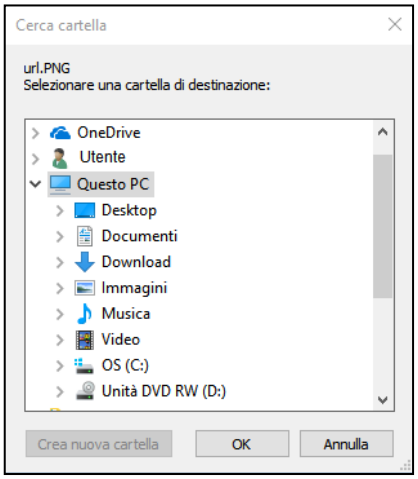


Figura 47: Selezione cartella di destinazione

Procedere con l'operazione di Firma premendo ***Si.***

N.B: *Consigliamo di creare una cartella dedicata per i File Firmati Digitalmente, così da evitare problemi.*

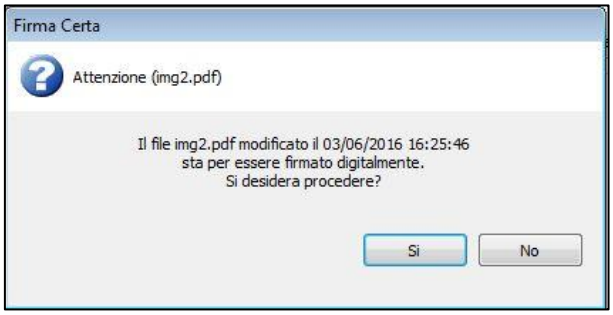


Figura 48: Conferma di firma

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

Figura 49: Inserimento PIN

Selezionare il Motivo della Firma (facoltativo).

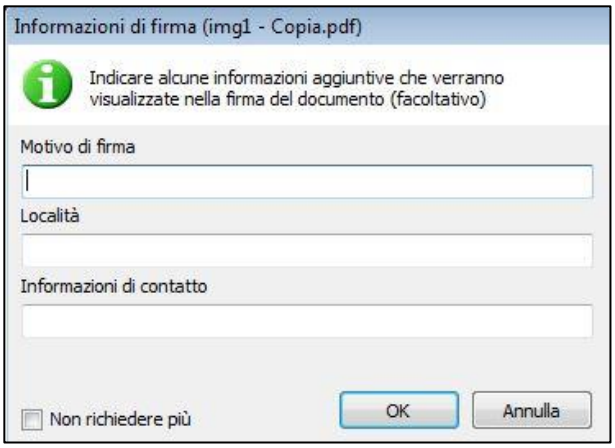


Figura 50: informazioni di firma

Selezionare dove apporre il Logo utilizzando il Marcatore Verde

Figura 51: Posizionamento del marcatore di firma

Confermare l'apposizione premendo ***Si***.

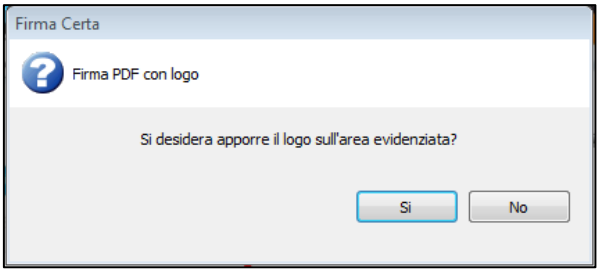


Figura 52: Conferma di posizionamento

Personalizzazione della visualizzazione del Logo(facoltativo), premere ***Ok.***

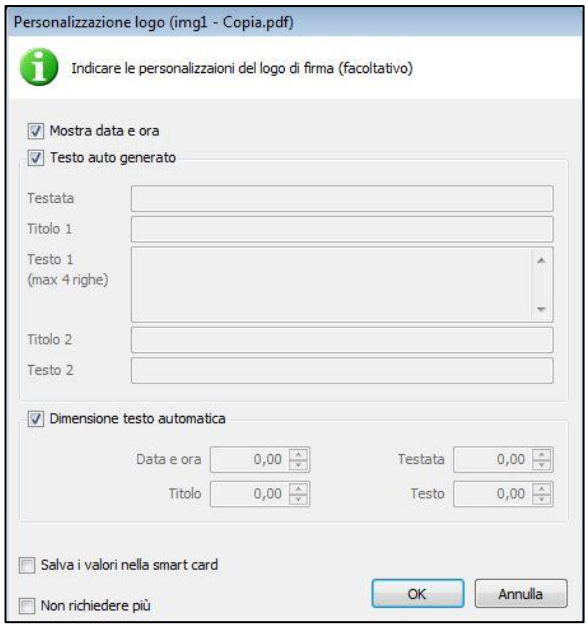


Figura 53: Personalizzazione del logo

Attendere il tempo di elaborazione e premere ***OK*** per concludere la procedura.

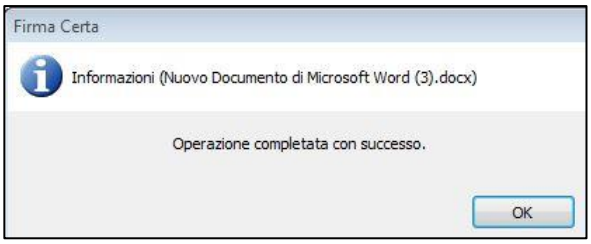


Figura 54: Operazione Completata

5.2 COME CONTROFIRMARE

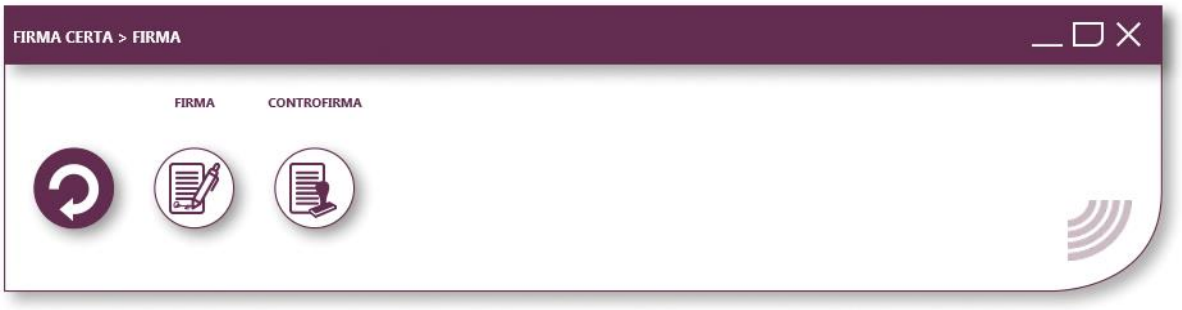


Figura 55: Pannello di Controfirma

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.**

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

Selezionare la Cartella di destinazione del File Firmato, infine cliccare ***OK***.

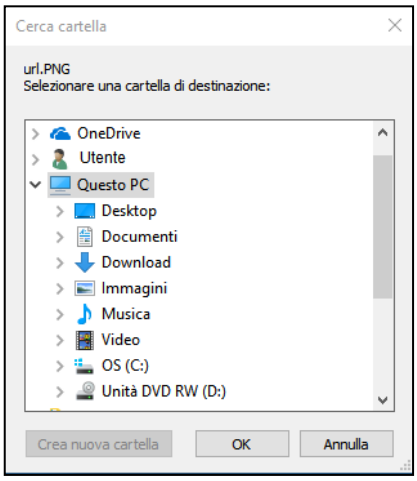


Figura 56: Selezione cartella di destinazione

Confermare che si desidera sovrascrivere il file già esistente, cliccando su ***Si***.

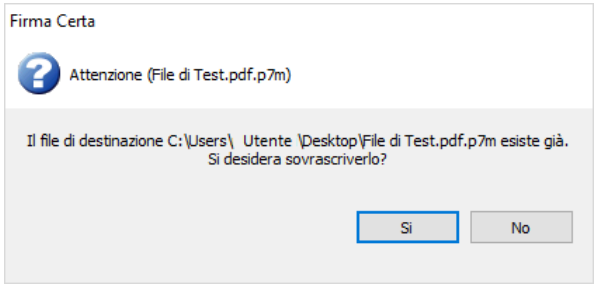


Figura 57: Conferma di sovrascrizione

Selezionare la firma che si desidera Controfirmare e procedere cliccando su ***OK***.

Esempio: *nell'immagine seguente l'utente TEST NOME COGNOME 2 ha controfirmato la firma di TEST NOME COGNOME 1*

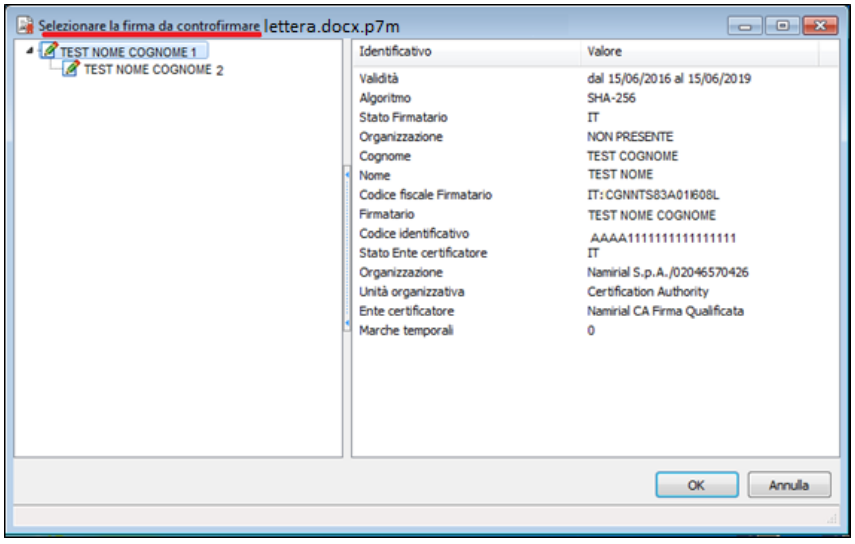


Figura 58: Schermata di esempio: verifica file controfirmato

Procedere con l'operazione di Firma premendo ***Si.***

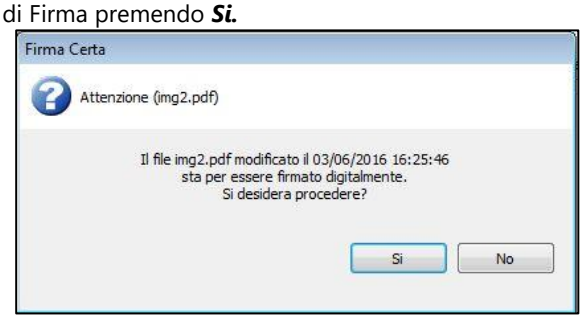


Figura 59: Conferma di firma

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

Figura 60: Inserimento Pin

Attendere il tempo di elaborazione e premere ***OK*** per concludere la procedura.

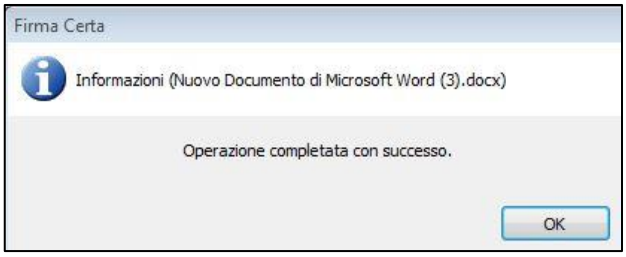


Figura 61: Operazione Completata

6 APPENDICE B: COME MARCARE UN FILE

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

N.B:
Il Servizio di Marcatura Temporale, non è compreso con la Firma Digitale.
Le marche temporali possono essere acquistate nel nostro Shop.
Da FirmaCerta > Utilità > Opzioni Marca Temporale

Figura 62: Pannello di Utilità

6.1 CONFIGURAZIONE PARAMETRI MARCHE TEMPORALI

Dal Menu Opzioni, scorrere tra le schede utilizzando le frecce apposite e cliccare sulla scheda Marche.

- Verificare che l'URL sia http://timestamp.namirialtsp.com o https://timestamp.namirialtsp.com
- Inserire ***Utente*** e ***Password*** e infine cliccare su ***OK.***

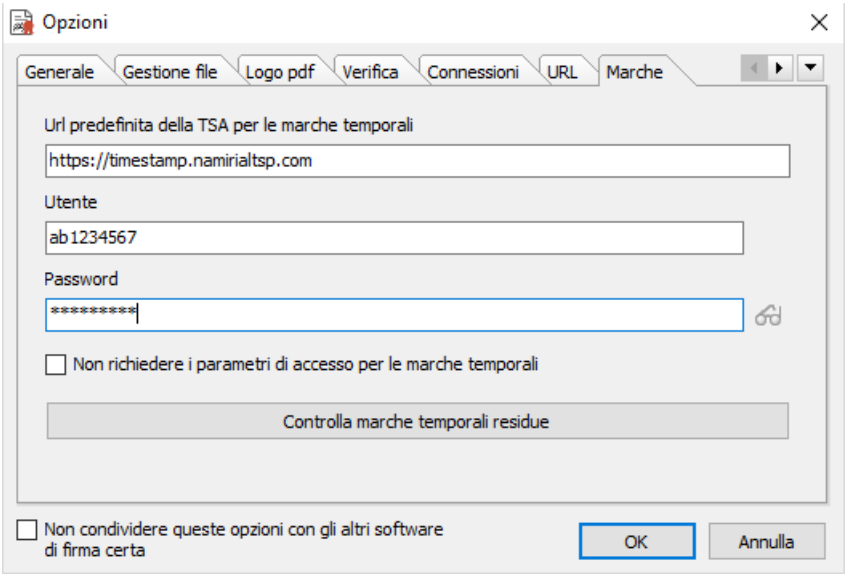


Figura 63: Opzioni Configurazione Marche

N.B :

- *Cliccando sull'icona a fianco del campo Password è possibile visualizzare in chiaro la password che si sta inserendo.*
- *- in caso di smarrimento delle credenziali per l'utilizzo delle Marche - Il Cliente deve richiederle inviando una PEC all'indirizzo: firmacerta@sicurezzapostale.it o un email a helpdesk@firmacerta.it indicando l'Username e/o Codice Fiscale.*

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

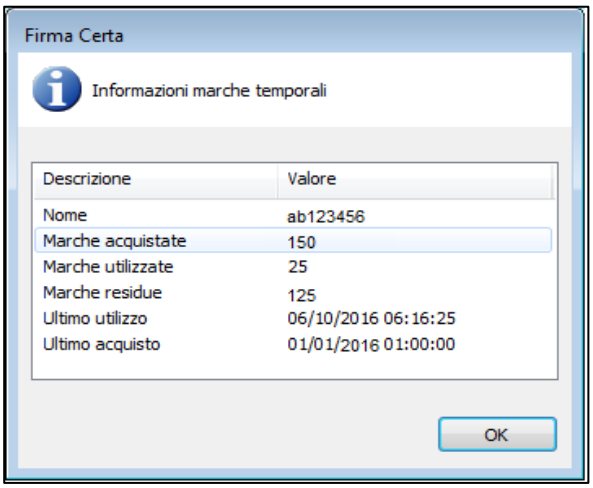


Figura 64: Controllo Marche temporali

6.2 COME FIRMARE E MARCARE

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) la marca è associata alla singola firma e
NON separabile.

Per apporre la Firma Digitale e la Marca Temporale ad un documento, effettuare la seguente procedura:

- Cliccare su ***Firma e Marca*** all'interno del programma,

Selezionare la Cartella di destinazione del File Firmato, infine cliccare ***OK***.

Procedere con l'operazione di Firma premendo ***Si.***

N.B: *Consigliamo di creare una cartella dedicata per i File Firmati Digitalmente, così da evitare problemi.*

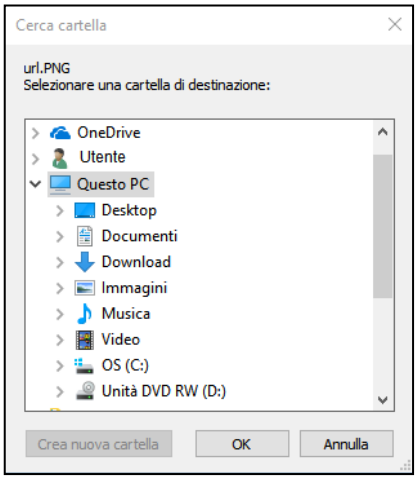


Figura 65: Selezione cartella di destinazione

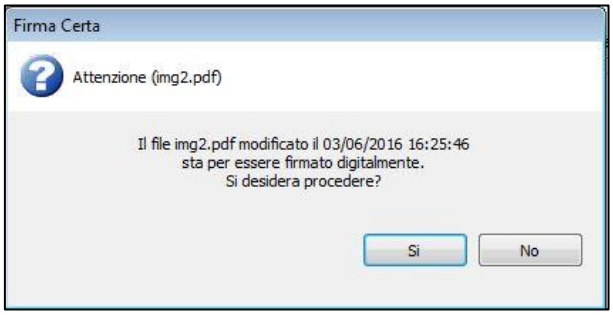


Figura 66: Conferma di firma

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

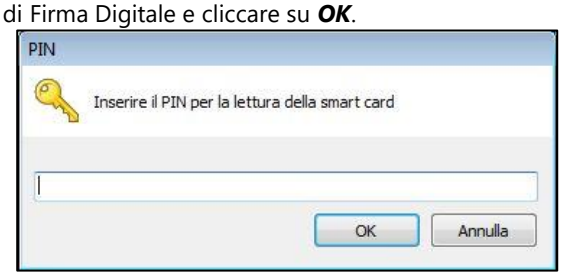


Figura 67: Inserimento del PIN

Confermare l'apposizione della marca cliccando sul pulsante ***OK.***

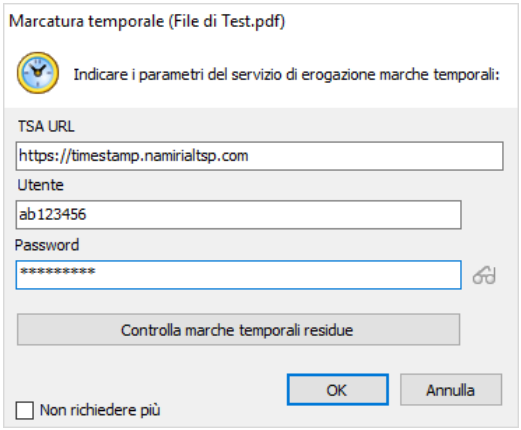


Figura 68: Conferma credenziali Marche

Attendere il tempo di elaborazione e premere ***OK*** per concludere la procedura.

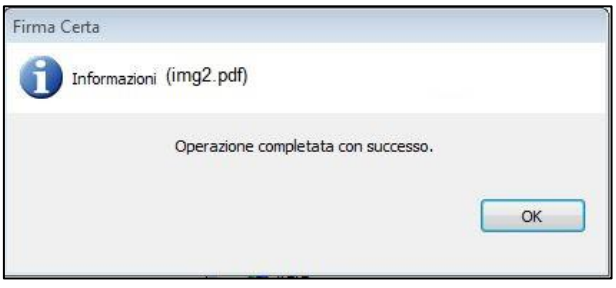


Figura 69: Operazione Completata

6.3 COME SEPARARE LA MARCA

Questa funzionalità permette di separare da un file di tipo, .TSD (TimeStamped-Data) la marca temporale.
N.B: *è possibile eseguire questa operazione soltanto per i file firmati in .p7m*

6.3.1 FIRMARE UN DOCUMENTO IN .P7M

Caricare il file da firmare all'interno del programma e cliccare su ***Firma***.

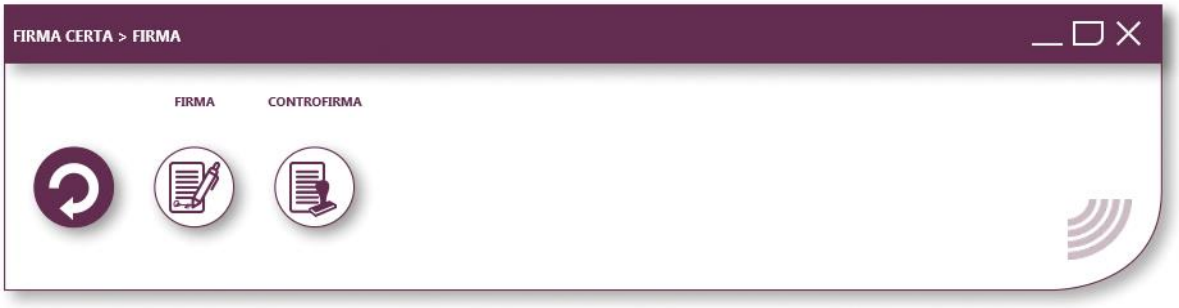


Figura 70: Pannello di Firma

N.B: Il software Firmacerta permette di firmare qualsiasi tipo di file in formato CAdES ovvero in .p7m, soltanto per i file PDF o XML chiederà all'utente con un messaggio a video se firmare in .P7M o mantenere il formato originale.

Dopo aver cliccato su firma si aprirà una finestra che vi chiede in che formato firmare il documento.
Premere ***No***, per effettuare una firma CAdES con il formato .p7m

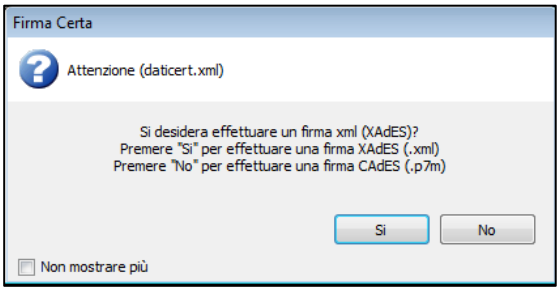


Figura 71: Selezione del formato di firma Cades

Seguire la procedura come indicato al punto Appendice A: Come firmare un documento.

6.3.2 MARCARE UN FILE FIRMATO IN .P7M

Caricare il file da marcare all'interno del programma e cliccare su ***Marca***.

Figura 72: Pannello FirmaCerta

Selezionare il formato .TSD per la Marca Temporale.

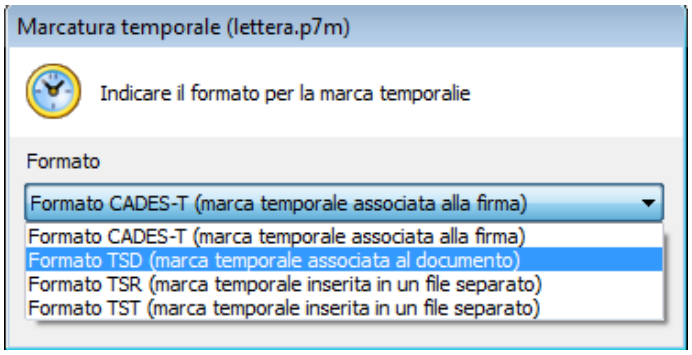


Figura 73: Scelta formato marca temporale

Selezionare la Cartella di destinazione del File Firmato, infine cliccare ***OK***.

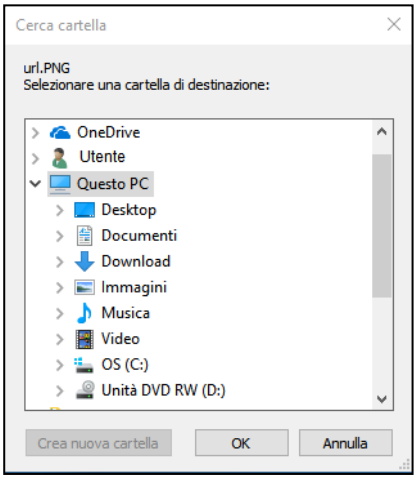


Figura 74: Scelta cartella di destinazione

Confermare l'apposizione della marca cliccando sul pulsante ***OK.***

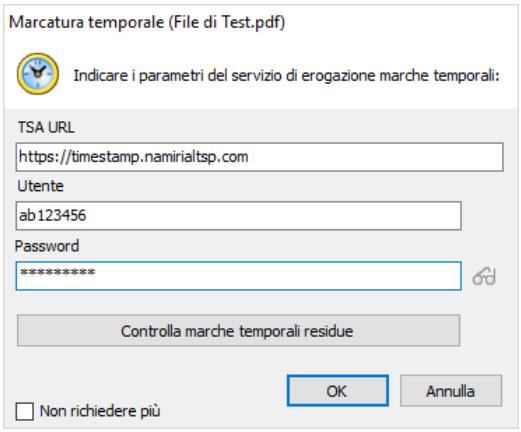


Figura 75: conferma dati di configurazione Marche

Attendere il tempo di elaborazione e premere ***OK*** per concludere la procedura.

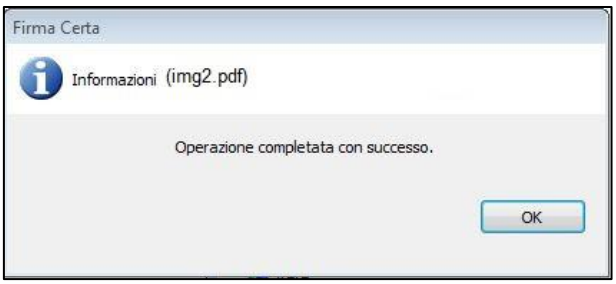


Figura 76: Operazione Completata

Al termine della procedura il software FirmaCerta avrà creato un nuovo file.

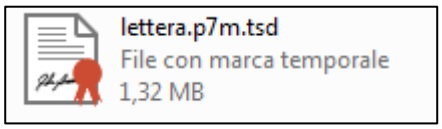


Figura 77: Esempio: file marcato temporalmente

6.3.3 SEPARARE LA MARCA TEMPORALE

Caricare il file *Marcato Temporalmente* all'interno del programma e cliccare su V***erifica***.

Figura 78: Pannello di Firma Certa

Nella Scheda di verifica, Selezionare la Marca Temporale e nel Menu degli strumenti cliccare sull'icona ***Separa marca e documento.***

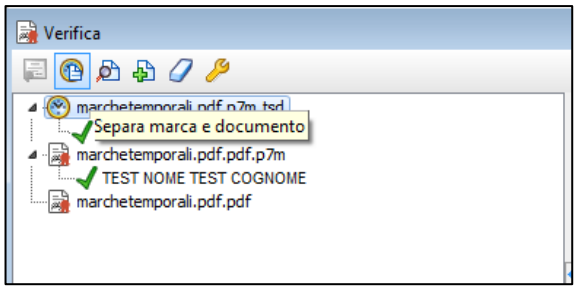


Figura 79: Separazione marca temporale

Selezionare il formato della marca richiesto, **.TSR/.TST**, e infine premere ***OK***.

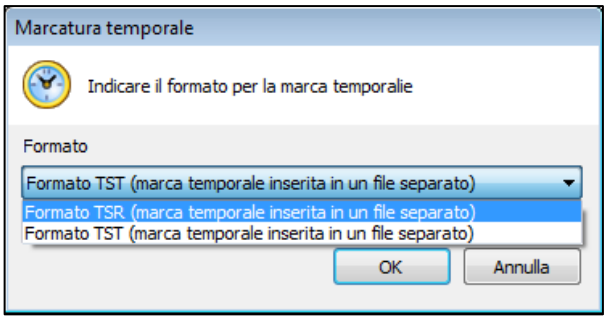


Figura 80: Selezionare il formato di marca

Al termine dell'operazione l'utente avrà due file:

- Un file di tipo .TSR o .TST contenente la *marca temporale*.
- Un file di tipo .P7m contenente il *file firmato digitalmente*.

Figura 81: Esempio di file marcati

7 APPENDICE C: COME VERIFICARE E VISUALIZZARE UN FILE

Per Verificare la validità della Firma Digitale di un documento, effettuare la seguente procedura:

Caricare il file *da Verificare* all'interno del programma e cliccare su ***Verifica***.

Figura 82: Pannello di Firmacerta

Dopo aver cliccato su ***Verifica*** si aprirà una finestra di riepilogo dove:

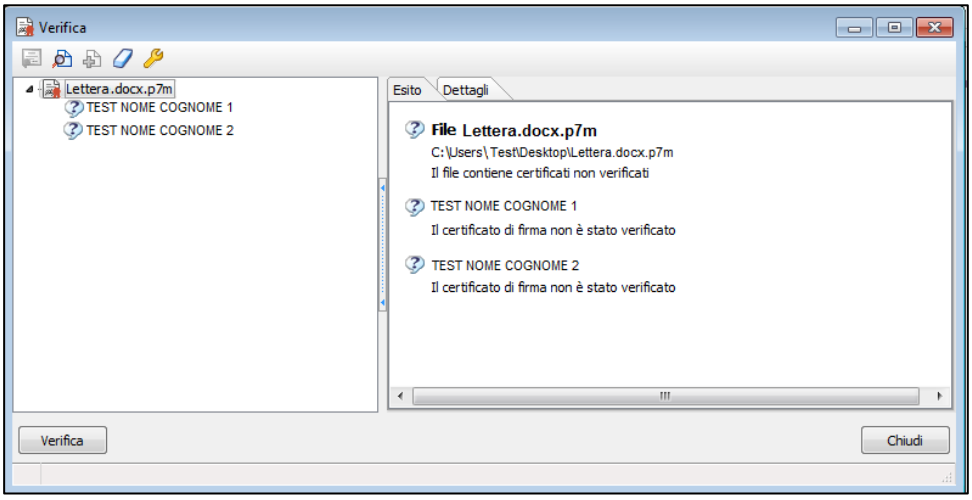


Figura 83: Schermata di verifica

N.B:
se compare la dicitura *il certificato di firma non è stato verificato* significa che non si è avviato in automatico 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 lettera.docx.p7m ed è stato firmato da due Utenti Test Nome Cognome 1 e Test Cognome 2.*

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

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

Figura 84: Schermata di Esito

Figura 85: Schermata di Dettagli

7.1 PER IMPOSTARE IN AUTOMATICO L'AVVIO DELLA VERIFCA DELLE FIRME

*Cliccare in **Utilità** > **Opzioni Verifica**.*

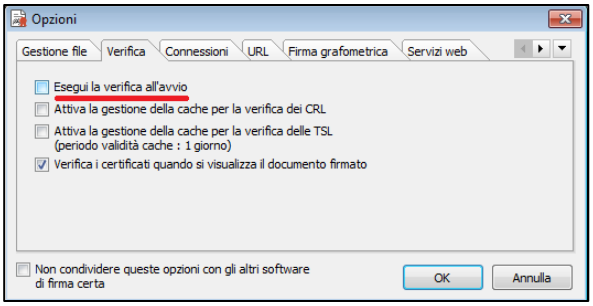


Figura 86: Impostazioni di Verifica

7.2 COME VISUALIZZARE UN FILE FIRMATO

Per Visualizzare un documento firmato digitalmente, effettuare la seguente procedura:

Aggiungere il file che si desidera all'interno del programma, e cliccare su ***Verifica***;
Nella scheda di verifica cliccare sull'icona

Figura 87: schermata per visualizzare il file firmato

N.B:

- 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.

8 APPENDICE D: COME CIFRARE E DECIFRARE UN FILE

La **cifratura** (detta anche crittografia) di un documento è un'operazione con la quale si rende quel documento completamente illeggibile per chiunque, ad eccezione di chi possiede la chiave che permette di decifrarlo, ossia riportarlo "in chiaro". La cifratura, dunque, permette di assicurare la confidenzialità di informazioni riservate.

Per cifrare un documento in modo che solo un particolare destinatario possa leggerlo, il mittente deve avere a disposizione il certificato di quel destinatario, poiché l'operazione di cifratura richiede l'uso della chiave pubblica.

Per poter **de**cifrare un documento, il destinatario deve avere a disposizione il proprio dispositivo di firma SmartCard/Token, in quanto l'operazione di decifratura richiede l'uso della chiave privata.
Le operazioni di firma digitale e cifratura possono essere combinate tra loro: in altre parole, un documento può essere firmato e successivamente cifrato, così da garantirne sia la paternità che la segretezza.

L' icona di un documento cifrato con Firma Certa Protect assume il seguente aspetto:

8.1 COME CIFRARE UN FILE

Ricordiamo che **per cifrare un documento è necessario possedere il certificato di cifratura del destinatario** (ossia dell'utente che vogliamo sia l'unico a poter decifrare il documento).

Si ottiene richiedendo il certificato al destinatario e poi importarlo manualmente nel proprio database di certificati di Firma Certa Protect.

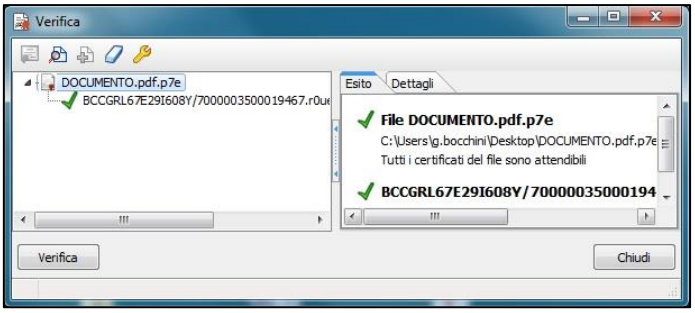
È possibile cifrare un documento per più utenti contemporaneamente, ossia in modo tale che diverse persone e solo loro possano decifrarlo.

Per cifrare un documento, cliccare sul bottone "**Proteggi Documenti**" nella finestra principale di Firma Certa Protect.

Al termine verrà creato, nella stessa posizione in cui il documento si trova, il file cifrato.

8.2 COME DECIFRARE UN FILE

Aprendo il documento desiderato con il doppio click si apparirà sia la finestra di Verifica che la visualizzazione del documento



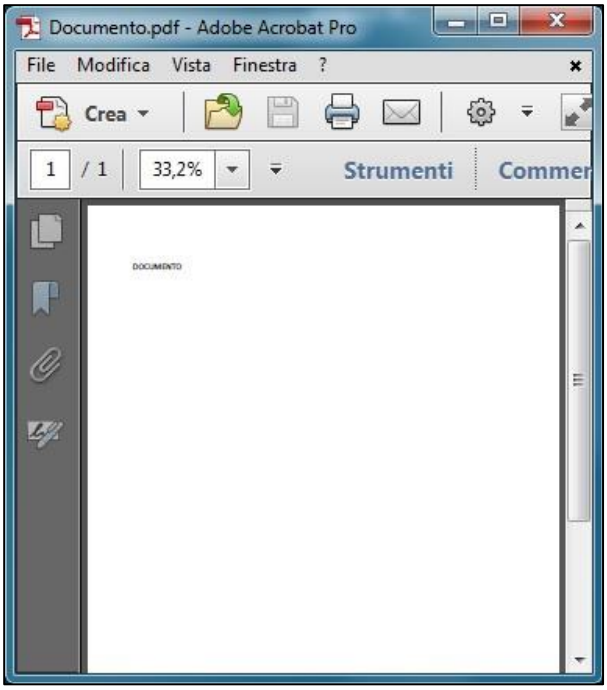


Figura 88: Schermata di Verifica con esempio

Attenzione:
Se non si possiede la chiave privata necessaria per decifrare, apparirà un messaggio d'errore:

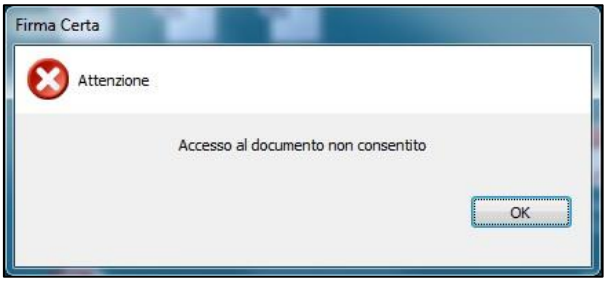


Figura 89: Accesso Negato

9 APPENDICE F: RIGA DI COMANDO

Il client FirmaCerta può essere utilizzato da riga di comando per consentire l'integrazione con applicativi che richiedono firme e marche senza l'ausilio dell'operatore. In ambiente Windows per la rilevazione della posizione di FirmaCerta, leggere il valore PathApp della seguente chiave:

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

9.1 COMANDI E PARAMETRI

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

<file>path completo del file su cui operare

<action>0=Firma 1=Firma e marca 2=Controfirma 3=Marca 4=Verifica 5=Visualizza 7=Opzioni

<mode>m se si richiede la firma massiva in tal caso deve essere un file di testo contenente la lista dei file da processare uno per riga.

<params>

- **TargetDir**=<cartella di destinazione dei file processati>
- **LogFileName**=<file di log del processo che è eseguito in modalità silent(senza mostrare finestre non necessarie)>
- **OverwriteLog**=<file>
- **Pin**=<codice pin per l'accesso al dispositivo di firma>
- **UrlTSA**=<url del server per le marche temporali>
  N.B: se non viene impostato viene preso quello inserito in configurazione
- **UsernameTSA**=<utente per l'accesso ai servizi di marche temporali>
- **PasswordTSA**=<password per l'accesso ai servizi di marche temporali>
- **OverwriteFile** =<**1** Sovrascrivere il file processato se presente; **0** aggiunge un underscore(_) nel nome (valore di default)>

IMPORTANTE: i parametri nella forma "chiave1=valore1;chiave2=valore2" (separati dal punto e virgola (;) e racchiusi da doppie virgole (")).

9.2 ESEMPI:

Di seguito sono riportati alcuni esempi per rendere più semplice e intuitive l'utilizzo dei comandi.
Firma di un documento fcsign.exe "C:\Documents and Settings\Utente\Desktop\Documento.pdf" 1

Firma di un documento senza interfaccia grafica

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

Firma di più documenti

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

il file "C:\temp\lista.txt" contiene:

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

10 APPENDICE G: FUNZIONI AVANZATE

Il Client FirmaCerta ha una serie di funzioni non comuni che consentono ai Titolari di rendere più agevole le operazioni di firma.

IMPORTANTE: *tutte le funzioni di firma di più documenti contemporaneamente sono possibili solo con certificati rilasciati dalla Certification Authority di Namirial S.p.A.*

10.1 FIRMA DI PIÙ DOCUMENTI

Il client consente di selezionare più documenti contemporaneamente inserendo una sola volta il PIN e firmarli consecutivamente gli stessi.

Prima di eseguire la procedura di *Firma Massiva* è necessario configurare il programma Firmacerta, da *Utilità* > *Opzioni Generali*:

Figura 90: Configurazione per firma Pades

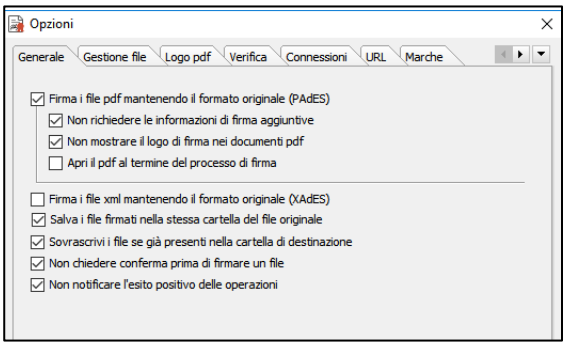


Figura 91: Configurazione per firma Cades

10.2 MARCA DI PIÙ DOCUMENTI

Il client consente di selezionare più documenti contemporaneamente ed apporre la marcatura temporale consecutivamente gli stessi.

Prima di eseguire la procedura di *Marcatura Massiva* è necessario configurare il programma Firmacerta, da *Utilità* > *Opzioni Generali* e Marche:

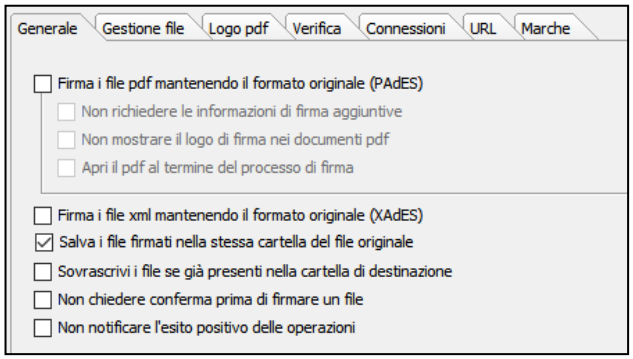


Figura 92: Schermata opzioni Generale

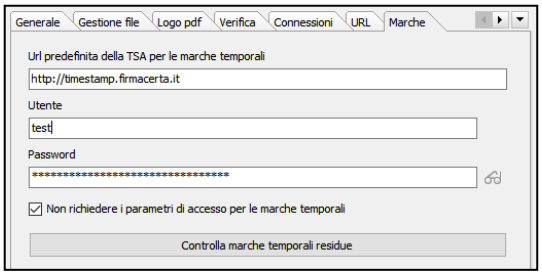


Figura 93: Schermata opzioni Marche

Selezionare il formato di Marcatura e selezionare la voce "*Mantieni i valori per tutte le marche*" se si desidera mantenere lo stesso valore per tutti file da marcare.

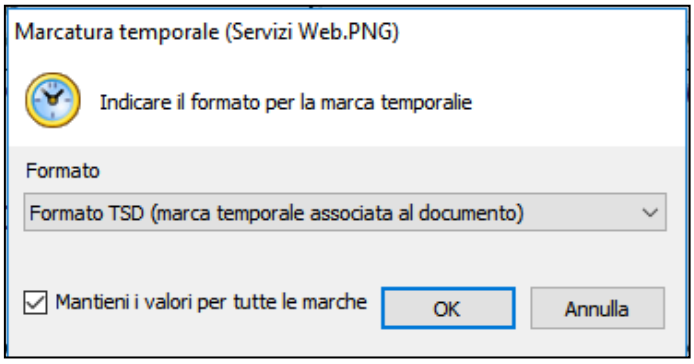


Figura 94: Schermata formato Marche

10.3 FIRMA E MARCA DI PIÙ DOCUMENTI

Il client consente di selezionare più documenti contemporaneamente inserendo una sola volta il PIN e firmarli e marcando consecutivamente gli stessi.

Prima di eseguire la procedura di *Firma e Marca in modo Massivo* è necessario configurare il programma Firmacerta, da *Utilità* > *Opzioni Generali* e Marche:

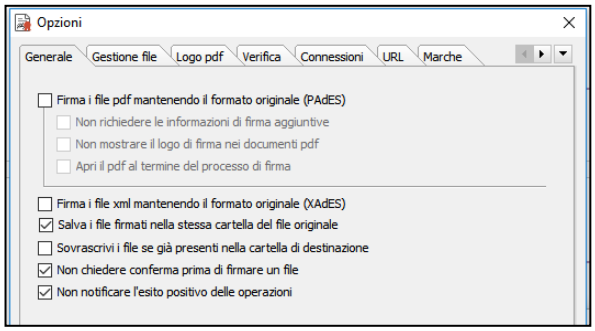


Figura 95: Schermata opzioni generali

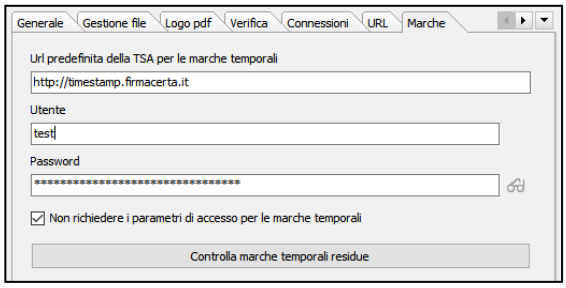


Figura 96: Schermata opzioni Marche

Sarà richiesto di inserire il codice PIN una sola volta.

Figura 97: Inserimento PIN

11 APPENDICE H: RINNOVO CERTIFICATI

Prima di procedere, verificare di avere installato sulla propria postazione il software di firma **FirmaCerta** e che questo sia correttamente aggiornato.
In caso di utilizzo del proxy si consiglia di chiedere i parametri di configurazione al proprio amministratore di rete.
In caso non sia presente la voce *Rinnovo certificati* è necessario scaricare il software **FirmaCerta Device Manager**.

11.1 CONFIGURAZIONE DEL PROXY

Accedere al software Firmacerta e cliccare su ***Gestione Dispositivo > Rinnovo certificati***, confermare le clausole e cliccare su ***Avanti***.

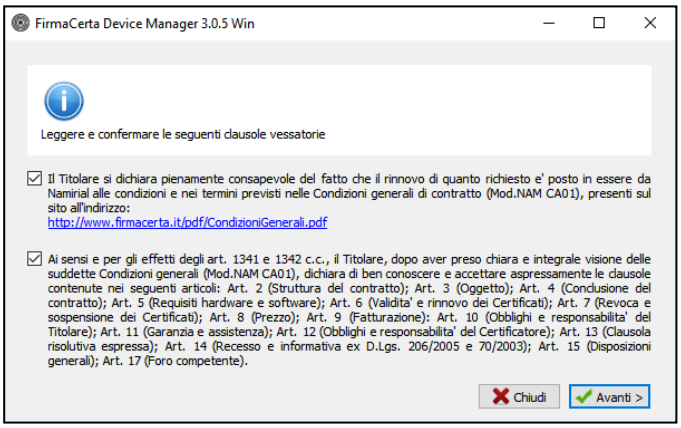


Figura 98: Schermata Clausole Vessatorie

Selezionare ***Utilità > Proxy e Connessioni*** ed impostare il proxy (per i parametri rivolgersi al proprio amministratore di rete. Cliccare su ***Salva.***

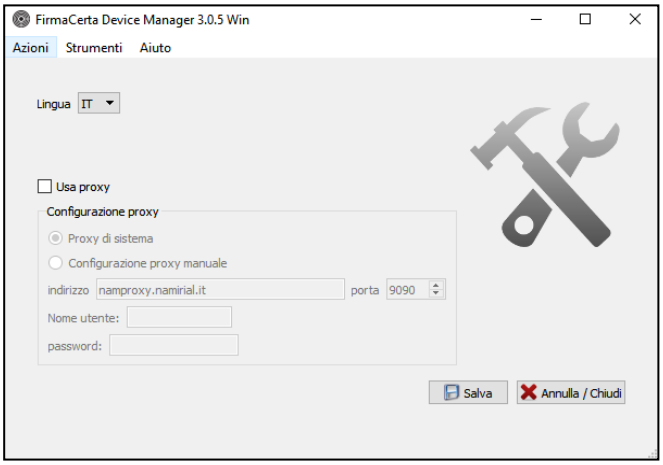


Figura 99: Configurazione Proxy

11.2 MODALITÀ DI RINNOVO

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

Figura 100: Schermata Clausole Vessatorie

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

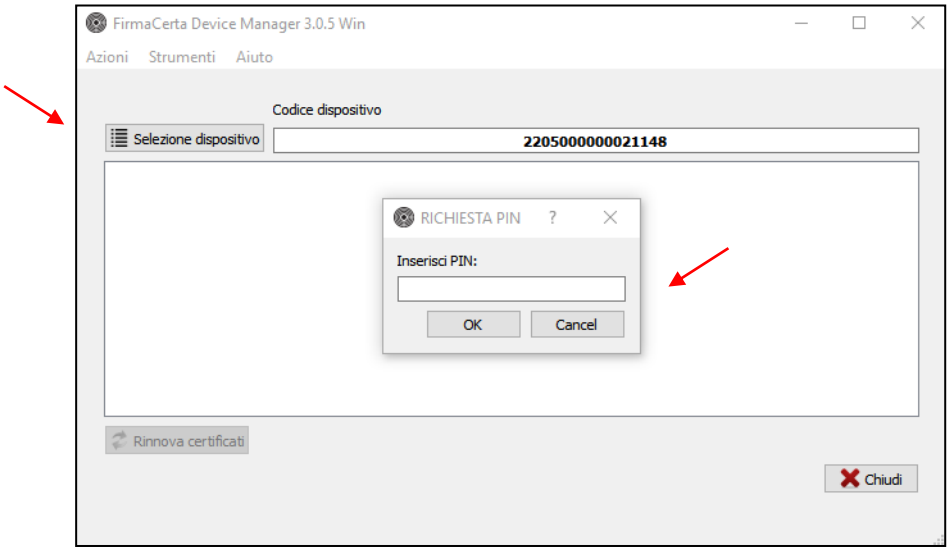


Figura 101: Schermata Inserimento PIN

A questo punto, il tool 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.

A questo punto, il tool proporrà di firmare il contratto di rinnovo automaticamente e proporrà all'utente se desidera visualizzarlo o meno.

Selezionare il certificato e infine cliccare su "***Rinnova Certificati***".

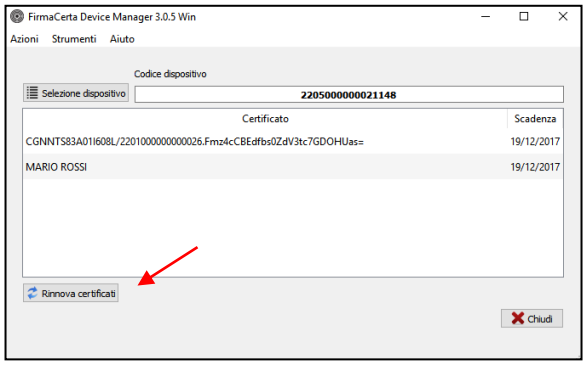


Figura 102: Rinnovo Certificati

A questo punto, il tool proporrà di visualizzare o meno la richiesta di rinnovo, in entrambi i casi il file sarà firmato digitalmente.

Figura 103: Messaggio di visualizzazione del contratto

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.

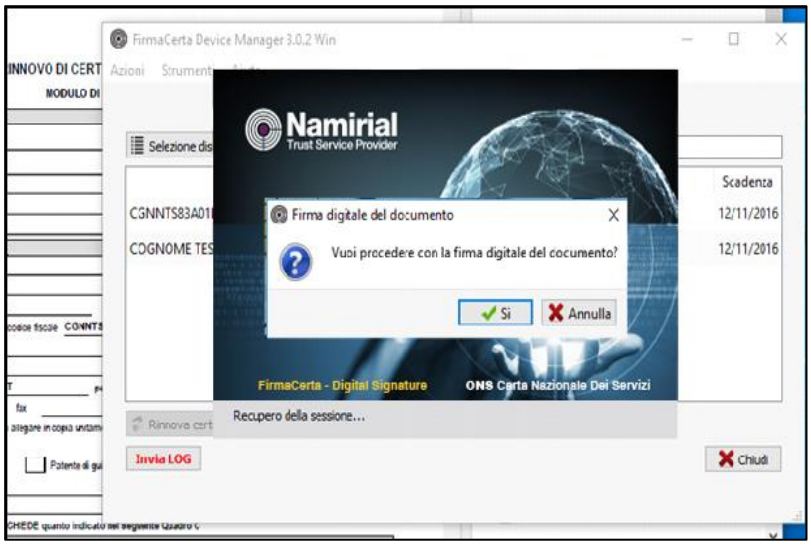


Figura 104: Conferma apposizione della firma

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

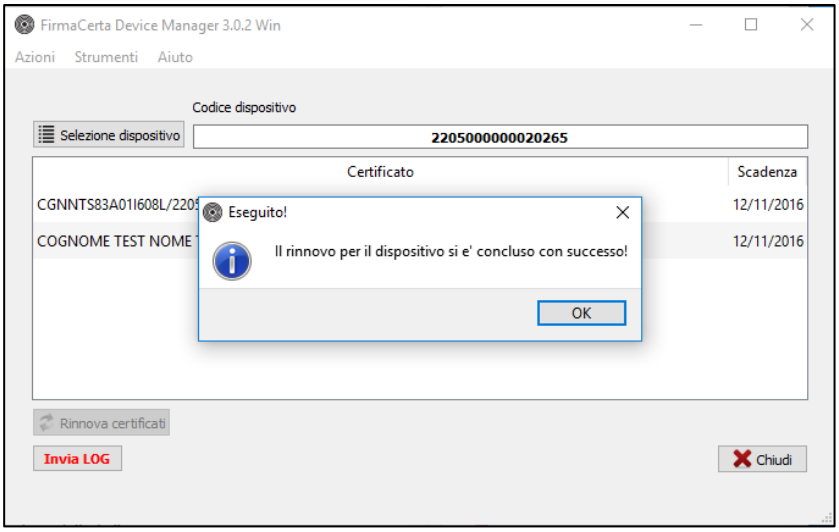


Figura 105: Rinnovo completato con successo

12 APPENDICE I : CONFIGURAZIONE FIRMA REMOTA

12.1 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.

12.1.1 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.

12.1.2 CONFIGURAZIONE L'APPLICAZIONE NAMIRIAL OTP

Per eseguire la prima attivazione, l'utente deve avviare l'applicazione ed inserire il codice ricevuto via SMS al numero di cellullare 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.

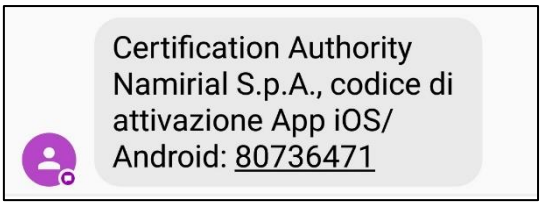


Figura 106: Esempio SMS con codice attivazione

12.1.3 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 107: Schermata iniziale di Virtual OTP. Fare tap sul bottone rosso

Figura 108: Fare tap sul bottone verde (Aggiungi OTP)

Figura 109: Inserimento codice ed assegnazione etichetta

12.1.4 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 110: Schermata iniziale di Virtual OTP. Fare tap su Aggiungi OTP

Figura 111: Inserimento codice ed assegnazione etichetta

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.

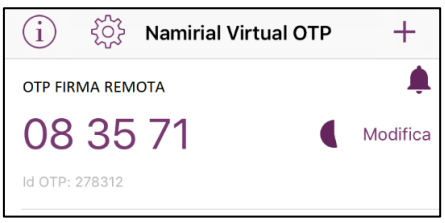


Figura 112: Schermata codice OTP generato dall'APP

12.2 ABILITAZIONE SERVIZIO NAMIRIAL SIGNENGINE

Scaricare il software FirmaCerta al seguente Link

Per abilitare la Firma Remota: *verificare in FirmaCerta -> Utilità -> Opzioni Generali -> Servizi Web. Selezionare Namirial SignEngine e cliccare su Abilita.*

N.B.
Se il servizio non è presente, Installare il Plugin per la Firma Remota tramite il seguente link:
http://download.assistenzatelematica.it/FileDwn/FCService_NamirialSignEngine.EXE

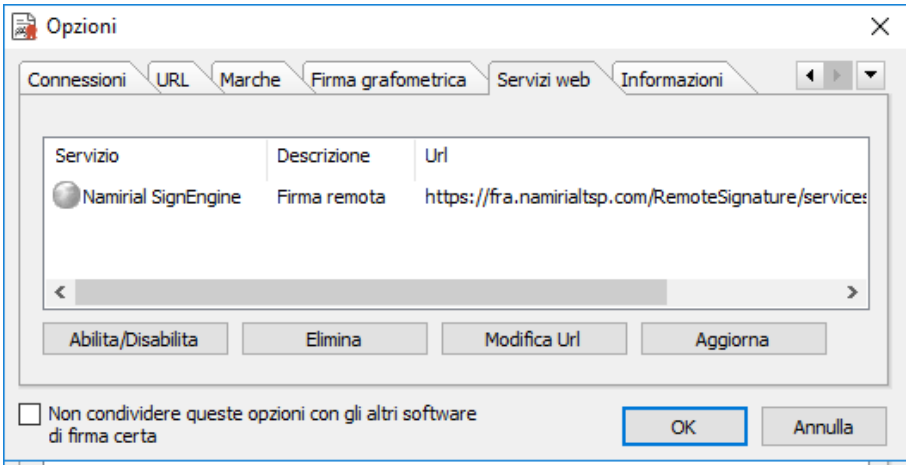


Figura 113: Abilitazione Servizio SignEngine

12.3 COME FIRMARE UN DOCUMENTO

Caricare il file da firmare all'interno del programma e cliccare su ***Firma***.

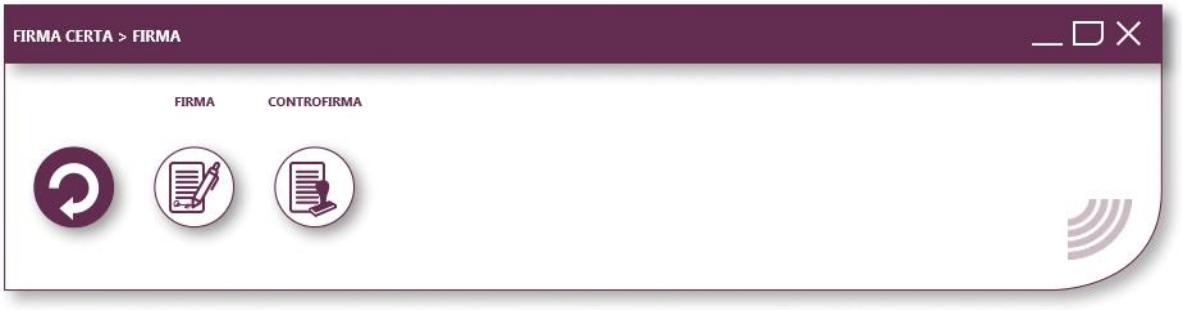


Figura 114: Pannello di Firma

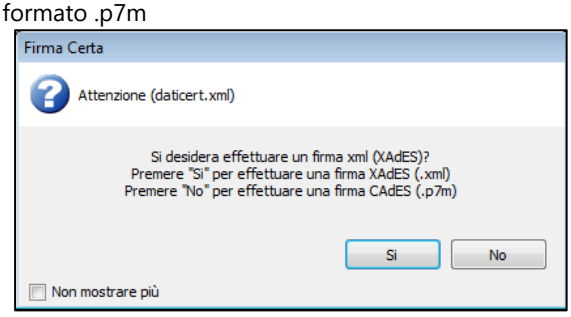
N.B: Il software Firmacerta permette di firmare qualsiasi tipo di file in formato CAdES ovvero in .p7m, soltanto per i file PDF o XML chiederà all'utente con un messaggio a video se firmare in .P7M o mantenere il formato originale.

Dopo aver cliccato su firma si aprirà una finestra che vi chiede in che formato firmare il documento.

- Premere ***Si***, per effettuare una firma XAdES, mantenendo il formato .xml (valido solo per file XML)
- Premere ***Si***, per effettuare una firma PAdES, mantenendo il formato .pdf (valido solo per file PDF)

Premere ***Si***, per effettuare una firma XAdES, mantenendo il formato .xml (valido solo per file XML)

Premere ***No***, per effettuare una firma CAdES con il formato .p7m



Premere ***Si***, per effettuare una firma PAdES, mantenendo il formato .pdf (valido solo per file PDF)

Premere ***No***, per effettuare una firma CAdES con il formato .p7m

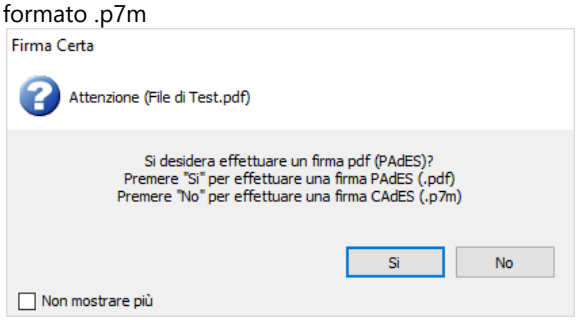


Figura 115: Scelta formato di firma

Selezionare la Cartella di destinazione del File Firmato, infine cliccare ***OK***.

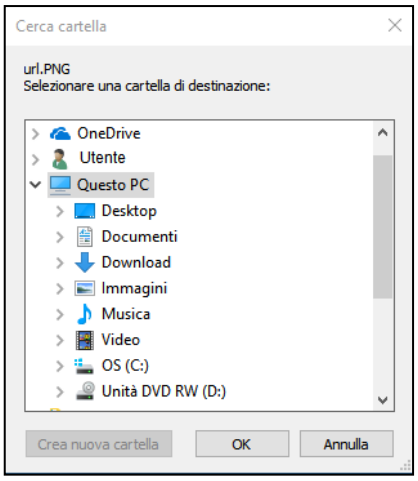


Figura 116: Selezione cartella di destinazione

Procedere con l'operazione di Firma premendo ***Si.***

N.B: *Consigliamo di creare una cartella dedicata per i File Firmati Digitalmente, così da evitare problemi.*

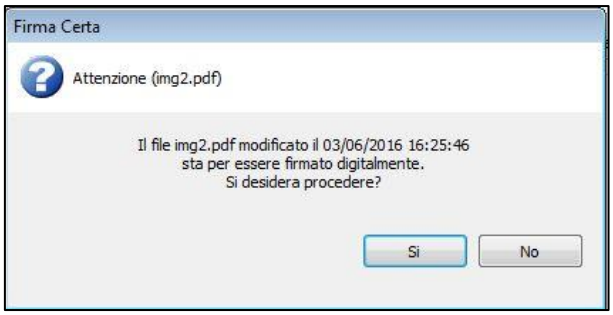


Figura 117: Conferma di firma

12.3.1 USERNAME

*Verificare in **Impostazioni** che il nome utente sia corretto.*

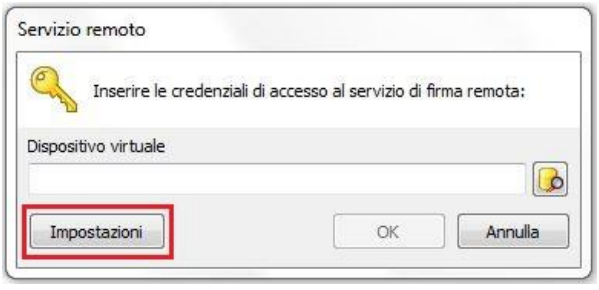


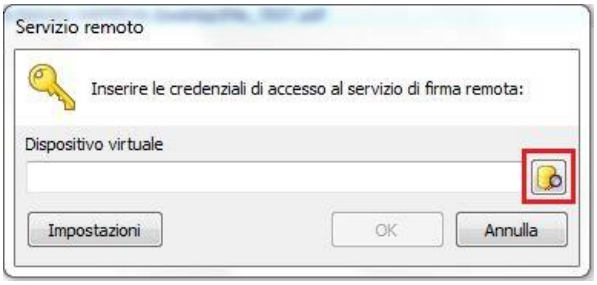
Figura 118: configurazione servizio remoto

Figura 119: inserimento nome utente

Recupero USERNAME
Il nome utente, può essere richiesto tramite e-mail all'indirizzo: helpdesk@firmacerta.it indicando il codice fiscale del titolare del dispositivo.

12.3.2 SELEZIONE DISPOSITIVO REMOTO

Cliccare sulla figura nel riquadro rosso, per inserire il vostro *Dispositivo virtuale* di Firma.



Nella seguente finestra sono presenti tutti i vostri dispositivi virtuali di Firma, quindi selezionare quello desiderato e poi click *Ok*.

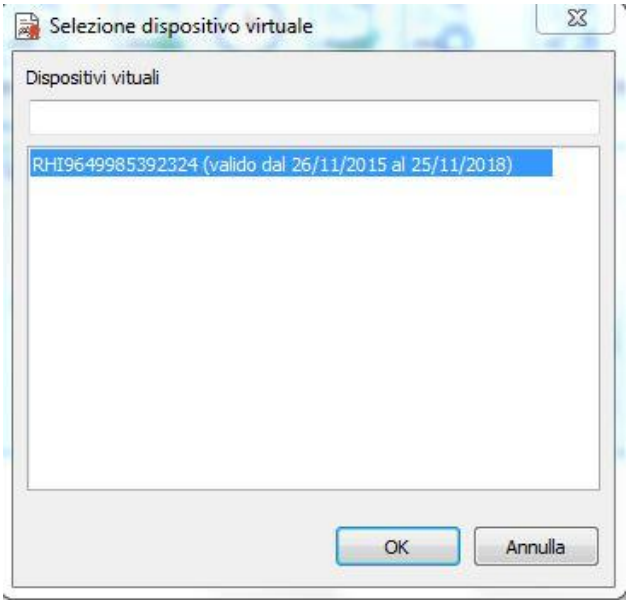


Figura 120: selezione del dispositivo virtuale remoto

Inserito il dispositivo virtuale confermare cliccando su OK.

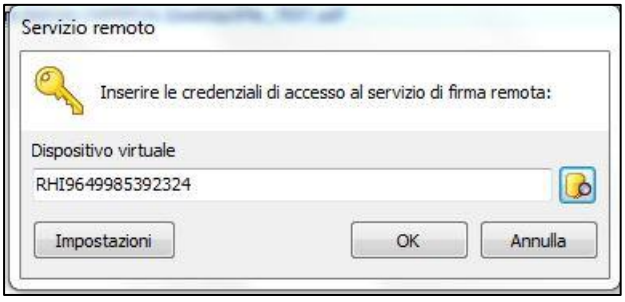


Figura 121: installazione guidata firmacerta

12.3.3 FIRMARE IN FORMATO PADES

Attenzione: Le Informazioni di firma è un'*operazione facoltativa selezionabile soltanto se è stato scelto il formato **PAdES***).

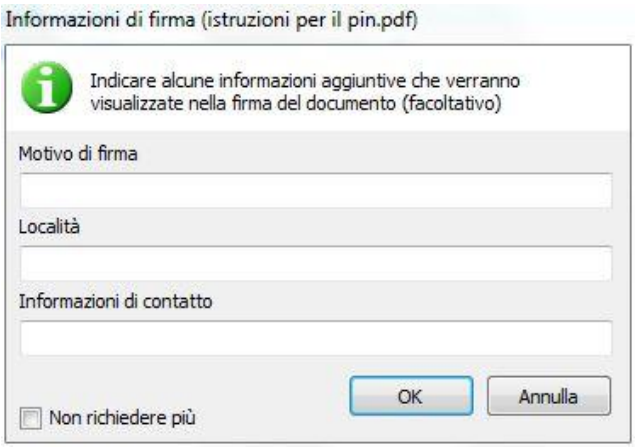


Figura 122: installazione guidata firmacerta

Email di Esempio con le credenziali per l'Area Privata

Gentile NOME COGNOME,

grazie per aver scelto i nostri prodotti di Firma Digitale.

Con la presente Le comunichiamo USERNAME e PASSWORD per accedere alla sua area privata dalla sezione ACCESSO UTENTI:

USERNAME: yxxyyxxy

PASSWORD: yyyxxxxy

All'interno di quest'area sono possibili una serie di operazioni direttamente riconducibili al tipo di dispositivo/i posseduti:

- Prima Attivazione - Proceduta obbligatoria solo per i certificati emessi su smartcard, token USB o microSD per i quali si è ricevuta una busta cieca cartacea;
- Sospensione - Utilizzabile tutte le volte in cui si rende necessario sospendere la validità dei certificati;
- Riattivazione - Utilizzabile solo sui certificati precedentemente sospesi;
- Revoca - Richiedibile quando si rende necessario interrompere definitivamente la validità dei certificati prima della scadenza naturale degli stessi;
- Modifica PIN - Permette di modificare il codice PIN dei certificati di firma remota e firma automatica;
- Modifica Codice Emergenza - Permette di modificare il Codice Emergenza utilizzato per il certificato di firma remota e firma automatica;
- Resetta OTP - Permette di resettare il token OTP (non si applica per OTP di tipo SMS);
- Verifica Dispositivo - Permette di eseguire un controllo sui dispositivi fisici (smartcard, token USB o microSD);

Si ricorda che lo USERNAME è altresì necessaria per la configurazione del software di firma "FirmaCerta" per l'utilizzo della firma remota.
Mediante lo USERNAME, FirmaCerta (disponibile sia per PC e Mac che come App per iPhone/iPad) è in grado di associare automaticamente il dispositivo OTP in possesso.
Per eseguire la configurazione fare riferimento alla relativa guida d'uso.

Attenzione: Non rispondere a questa e-mail. Il messaggio e' generato automaticamente.
Cordiali Saluti
Namirial S.p.A.
helpdesk@firmacerta.it
www.firmacerta.it

Figura 123: esempio busta cieca

12.4 PROCEDURA CON OTP SMS

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

Cliccare sulla figura nel riquadro rosso, Selezionare il Dispositivo OTP poi cliccare OK

Da questa schermata si legge la tipologia di OTP in questo caso SMS

Figura 124: selezionare dispositivo OTP

Cliccare sul pulsante **Invia SMS**, per ricevere al numero di telefono fornito in fase di registrazione un SMS contenente il codice OTP, da inserire nel riquadro. OTP

Figura 125: Invio SMS OTP

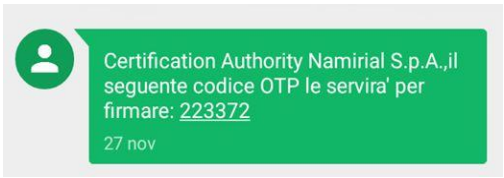


Figura 126: SMS ricevuto

Alla fine della procedura comparirà il seguente messaggio di Conferma.

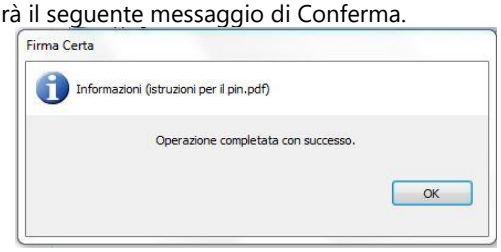


Figura 127: Messaggio di conferma

12.5 PROCEDURA CON OTP MOBILE: NAMIRIAL OTP

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

Cliccare sulla figura nel riquadro rosso, Selezionare il Dispositivo OTP poi cliccare OK

Da questa schermata si legge la tipologia di OTP in questo caso GENERATOR

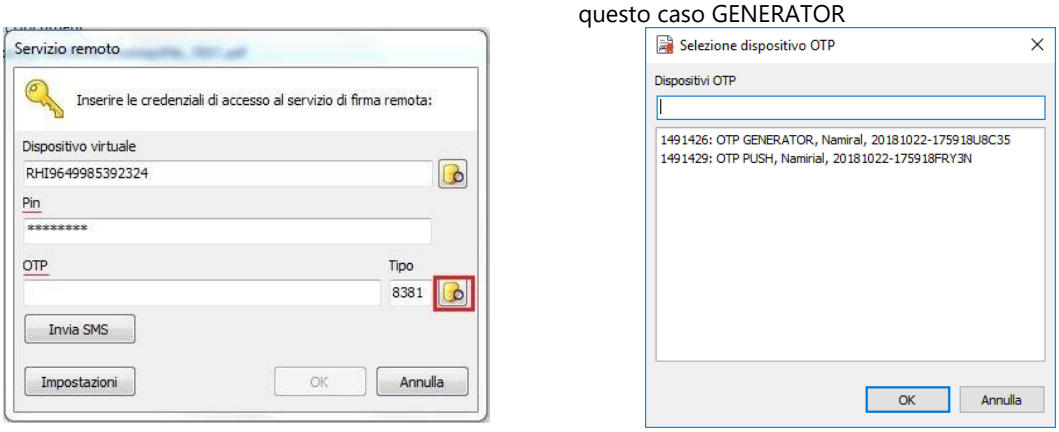


Figura 128: selezionare dispositivo OTP

Aprire l'applicazione Namirial OTP, e inserire il codice nel riquadro. OTP.

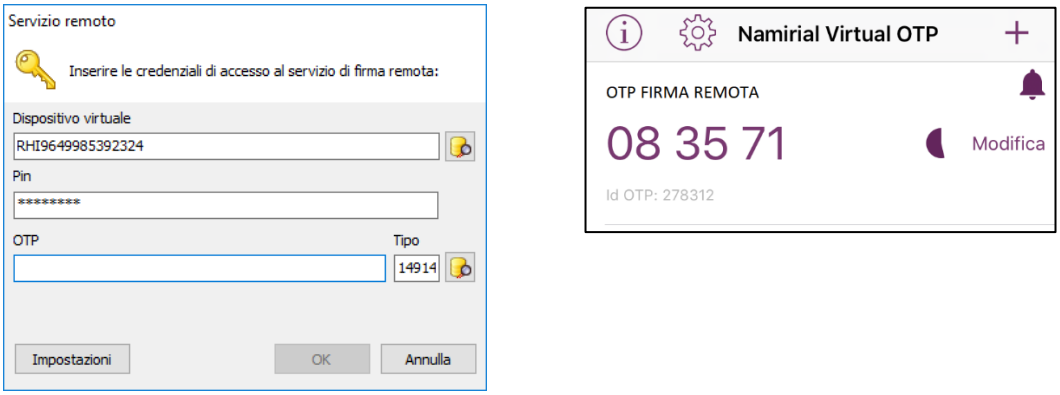


Figura 129: OTP Generator

Alla fine della procedura comparirà il seguente messaggio di Conferma.

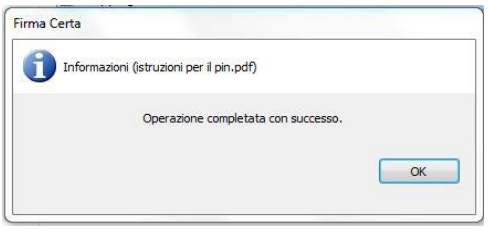


Figura 130: Messaggio di conferma

12.6 PROCEDURA CON OTP FISICO

12.7 ATTIVAZIONE OTP

Accedere all'areaPrivata, inserendo le credenziali Username e Password che sono stati inviate all'indirizzo email fornito in fase di registrazione.

> **RECUPERO CREDENZIALI AREA PRIVATA**: possono *essere richieste tramite e-mail all'indirizzo: helpdesk@firmacerta.it indicando il codice fiscale del titolare del dispositivo.*

Nel Menù laterale a destra, sotto la categoria FIRMA REMOTA cliccare su Attivazione.
Verificare che il numero di serie coincide con il numero di serie presente nel OTP FISICO.

Figura 131: 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.**

Figura 132: Schermata Area Privata

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

Cliccare sulla figura nel riquadro rosso, Selezionare il Dispositivo OTP poi cliccare OK

Da questa schermata si legge la tipologia di OTP in questo caso FISICO

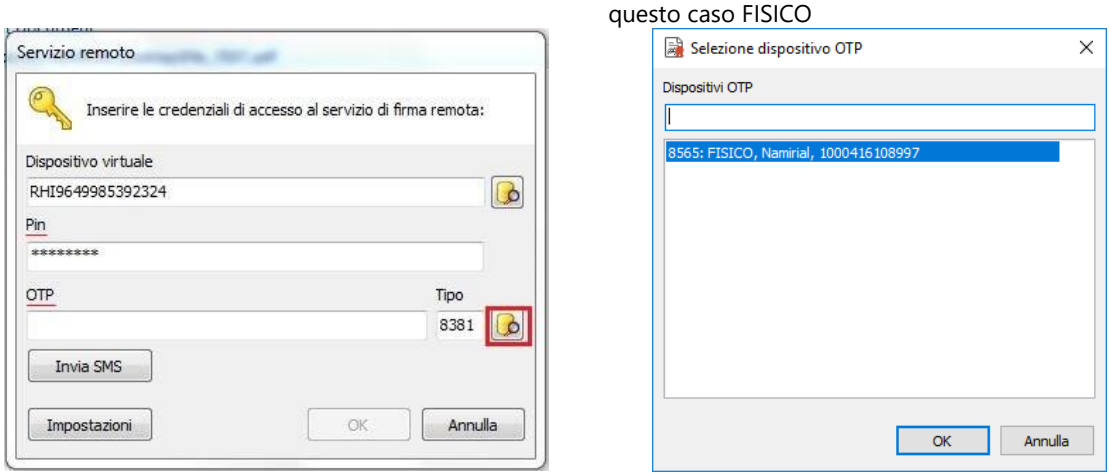


Figura 133: selezionare dispositivo OTP

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

Figura 134: OTP Fisico Generato

Alla fine della procedura comparirà il seguente messaggio di Conferma.

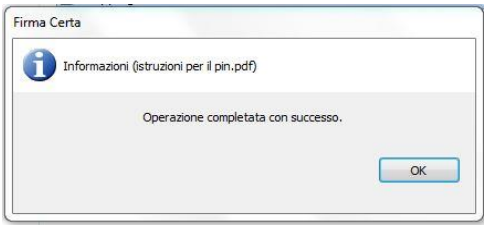


Figura 135: Messaggio di conferma

13 AUTENTICAZIONE WEB

Per l'importazione dei certificati vi invitiamo a seguire la guida citata in [I], pubblicata nel nostro portale al seguente link: http://download.firmacerta.it/pdf/manualeAutenticazioneWeb.pdf