

# Registration Authority

## Guida FirmaCerta per Windows

|               |                             |                      |                           |                          |
|---------------|-----------------------------|----------------------|---------------------------|--------------------------|
| Categoria     | <b>TSP-Firma Digitale</b>   | Codice Documento     | <b>NAM-Guida Utente</b>   | <b>Namirial S.p.A.</b>   |
| Redatto da    | <b>Michelangelo Bonvini</b> | Nota di riservatezza | <b>Documento Pubblico</b> | Registration Authority   |
| Verificato da | <b>Gabriele Bocchini</b>    | Versione             | <b>2.0</b>                | <b>Gabriele Bocchini</b> |
| Approvato da  | <b>Gabriele Bocchini</b>    | Data di emissione    | <b>18/01/2019</b>         | <hr/>                    |



– Questa pagina è lasciata intenzionalmente in bianco –



## INDICE

|  |           |
|--|-----------|
| <b>Indice.....</b>   | <b>3</b>  |
| <b>Storia delle modifiche apportate.....</b>                     | <b>7</b>  |
| <b>1 Introduzione.....</b>                                       | <b>8</b>  |
| 1.1 Scopo del documento e campo di applicazione.....             | 8         |
| 1.2 Definizioni ed Acronimi usati all'interno del documento..... | 9         |
| <b>2 Installazione .....</b>                                     | <b>11</b> |
| <b>3 Interfaccia Grafica.....</b>                                | <b>14</b> |
| <b>4 Funzioni Principali .....</b>                               | <b>15</b> |
| 4.1 Firma: .....   | 15        |
| 4.1.1 Firma.....   | 15        |
| 4.1.2 ControFirma.....   | 15        |
| 4.2 Firma E Marca .....  | 16        |
| 4.3 Verifica .....   | 16        |
| 4.4 Marca.....   | 16        |
| 4.5 Gestione Dispositivo .....                                   | 17        |
| 4.5.1 Cambio Pin.....  | 17        |
| 4.5.2 Sblocco Pin.....   | 18        |
| 4.5.3 Cambio PUK.....  | 18        |
| 4.5.4 Visualizza Certificati.....                                | 19        |
| 4.5.5 Verifica Dispositivo .....                                 | 20        |
| 4.5.6 Rinnovo Certificati.....                                   | 20        |
| 4.6 Firma Grafometrica .....                                     | 21        |
| 4.6.1 Firma Documento .....                                      | 21        |



|          |  |           |
|----------|--|-----------|
| 4.6.2    | Template di Firma .....  | 21        |
| 4.7      | Utilità .....  | 24        |
| 4.7.1    | Cifra e Decifra .....  | 24        |
| 4.7.2    | Opzioni Generali .....   | 25        |
| 4.7.3    | Proxy e Connessioni .....  | 27        |
| 4.7.4    | Opzioni Firma .....  | 28        |
| 4.7.5    | Opzioni Verifica .....   | 29        |
| 4.7.6    | Opzioni Firma Grafometrica .....                                     | 29        |
| 4.7.7    | Opzioni Marca Temporale .....  | 32        |
| 4.8      | Help .....   | 32        |
| <b>5</b> | <b>Appendice A: Come Firmare e Controfirmare .....</b>               | <b>33</b> |
| 5.1      | Come firmare un documento .....                                      | 33        |
| 5.1.1    | Firmare in CADES - XAdES .....                                       | 33        |
| 5.1.2    | Firmare in PAdES .....   | 35        |
| 5.2      | Come Controfirmare .....   | 38        |
| <b>6</b> | <b>Appendice B: Come Marcare un file .....</b>                       | <b>40</b> |
| 6.1      | Configurazione Parametri Marche Temporalì .....                      | 40        |
| 6.2      | Come Firmare e Marcare .....   | 41        |
| 6.3      | Come Separare la Marca .....   | 43        |
| 6.3.1    | Firmare un documento in .p7m .....                                   | 43        |
| 6.3.2    | Marcare un file Firmato in .p7m .....                                | 44        |
| 6.3.3    | Separare la Marca Temporale .....                                    | 46        |
| <b>7</b> | <b>Appendice C: Come Verificare e Visualizzare un file .....</b>     | <b>47</b> |
| 7.1      | Per impostare in automatico l'avvio della verifica delle Firme ..... | 49        |
| 7.2      | Come visualizzare un file firmato .....                              | 49        |



|           |  |           |
|-----------|--|-----------|
| <b>8</b>  | <b>Appendice D: Come Cifrare e Decifrare un file .....</b> | <b>50</b> |
| 8.1       | Come Cifrare un file.....                                  | 50        |
| 8.2       | Come Decifrare un file.....                                | 51        |
| <b>9</b>  | <b>Appendice F: Riga di Comando .....</b>                  | <b>52</b> |
| 9.1       | Comandi e Parametri .....                                  | 52        |
| 9.2       | Esempi:.....   | 53        |
| <b>10</b> | <b>Appendice G: Funzioni Avanzate.....</b>                 | <b>54</b> |
| 10.1      | Firma di più Documenti .....                               | 54        |
| 10.2      | Marca di più documenti .....                               | 55        |
| 10.3      | Firma e Marca di più documenti.....                        | 56        |
| <b>11</b> | <b>Appendice H: Rinnovo Certificati.....</b>               | <b>57</b> |
| 11.1      | Configurazione del Proxy .....                             | 57        |
| 11.2      | Modalità di Rinnovo SmartCard e Token .....                | 58        |
| 11.3      | Modalità di Rinnovo Remota e Automatica.....               | 60        |
| <b>12</b> | <b>Appendice I: Firma remota .....</b>                     | <b>62</b> |
| 12.1      | Seleziona la tipologia di Firma.....                       | 62        |
| 12.2      | Scegliere cartella di destinazione .....                   | 63        |
| 12.3      | Inserimento parametri firma remota.....                    | 64        |
| 12.4      | Selezione dispositivo remoto .....                         | 65        |
| 12.5      | Firma PAdES:.....  | 66        |
| 12.6      | Seleziona la procedura di firma.....                       | 67        |
| 12.6.1    | Procedura con OTP SMS.....                                 | 68        |
| 12.6.2    | Procedura con Namirial OTP .....                           | 69        |
| 12.6.3    | Procedura con OTP Fisico.....                              | 70        |
| <b>13</b> | <b>Autenticazione WEB .....</b>                            | <b>71</b> |



|           |   |           |
|-----------|---|-----------|
| <b>14</b> | <b>Appendice J: Bit4id – Linux.....</b> | <b>72</b> |
| 14.1      | Cambio Pin.....                         | 73        |
| 14.2      | Sblocco Pin.....                        | 74        |
| 14.3      | Cambio PUK.....                         | 74        |
|           | <b>Riferimenti.....</b>                 | <b>75</b> |
|           | <b>Indice delle Figure.....</b>         | <b>76</b> |



## STORIA DELLE MODIFICHE APPORTATE

| VERSIONE    | 2.0  |
|-------------|--|
| Data        | 18/01/2019   |
| Motivazione | Aggiornamento del documento, con le nuove schermate del Software |
| Modifiche   |  |



# 1 INTRODUZIONE

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

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

FirmaCerta è lo strumento ideale per:

- firmare contemporaneamente grandi volumi di documenti digitali, come fatture, polizze, ricevute di pagamenti, bonifici e qualsiasi altro documento digitale;
- Firmare i documenti mantenendo il formato originale (il .PDF o .XML dopo essere stato firmato mantenendo lo stesso formato);
- La possibilità di poter scegliere il dispositivo hardware col quale si desidera apporre la firma (Smart Card - Token);
- La possibilità di apporre/associare una marca temporale ad un documento o a una firma (Grafometrica);
- 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 principi della crittografia asimmetrica non ci potrà più essere corrispondenza tra contenuto del documento e firme associate, FirmaCerta nelle operazioni di verifica del documento darà esito negativo.



## 1.2 DEFINIZIONI ED ACRONIMI USATI ALL'INTERNO DEL DOCUMENTO

| TERMINE                           | SIGNIFICATO  |
|-----------------------------------|--|
| Firma Digitale                    | è un particolare tipo di firma elettronica qualificata e rappresenta l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.   |
| Marca Temporale (timestamp)       | è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione è 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

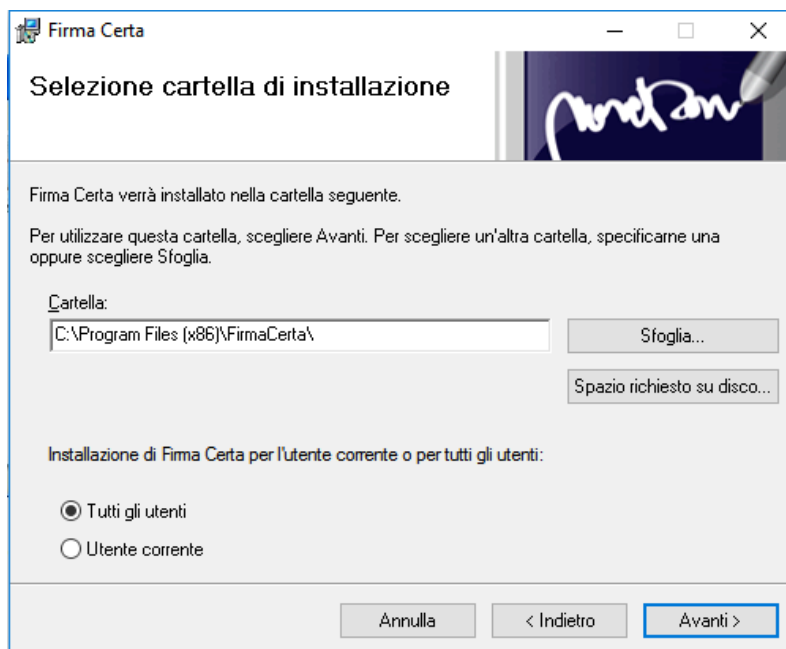
Scaricare il software di Firma dal sito [www.firmacerta.it](http://www.firmacerta.it), sezione *Download Software Firmacerta*, > Versione Desktop per Windows ([LINK](#)).

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



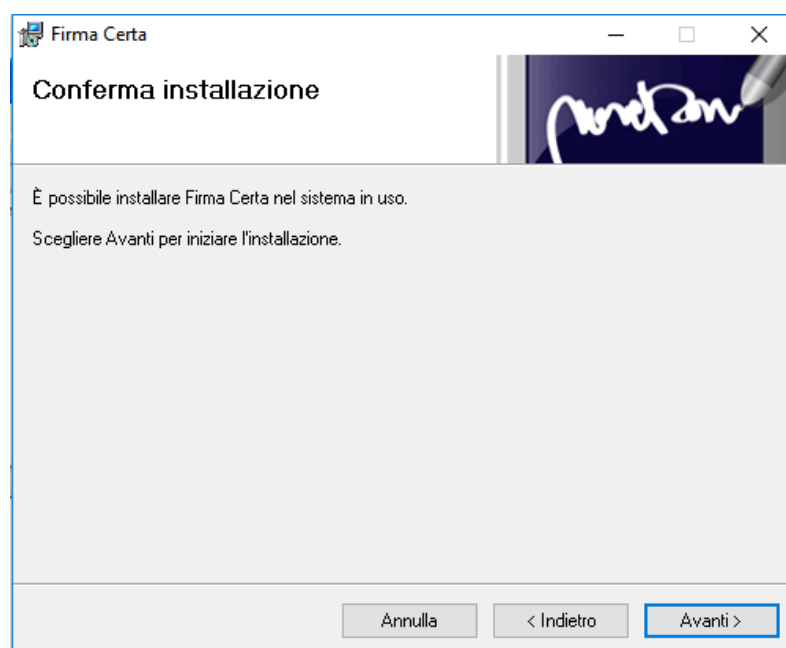
Figura 1 - installazione guidata firmacerta

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



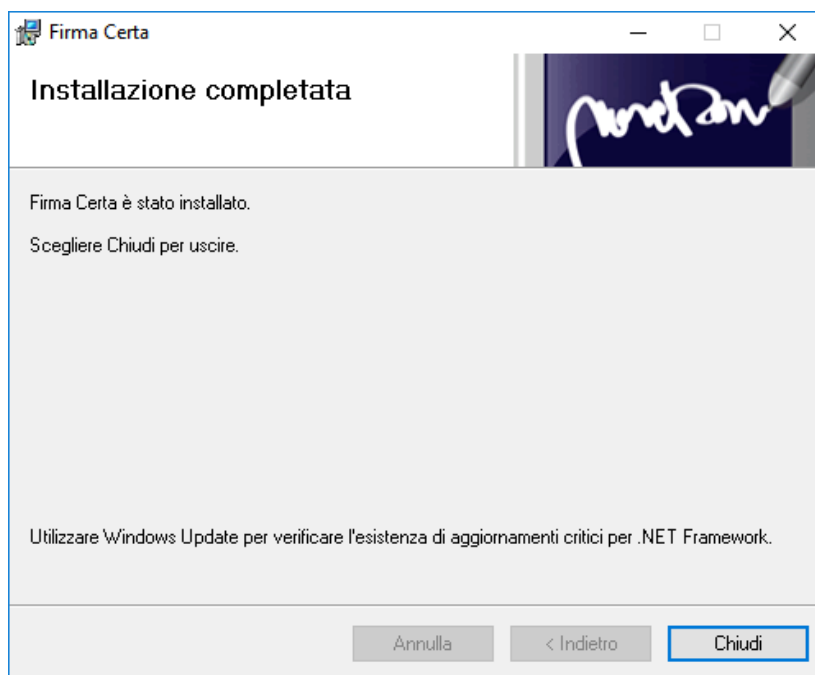
*Figura 2 - seleziona cartella di destinazione*

**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

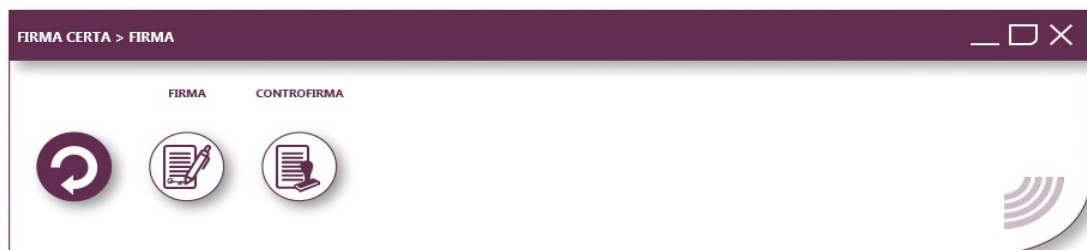


Figura 6 - sottomenù di firma

#### 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.

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

Vedi la procedura completa per Verificare un documento: [Appendice 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 è possibile modificare il PIN dalla propria [Area Privata Utente](#) nella sezione > Utente > Firma digitale > Gestione.

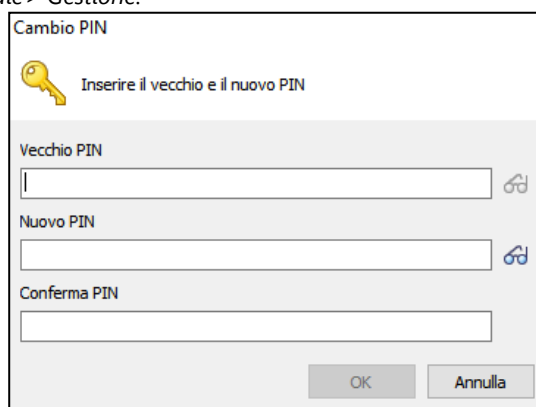


Figura 13 - Funzione Cambio PIN

## 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.**

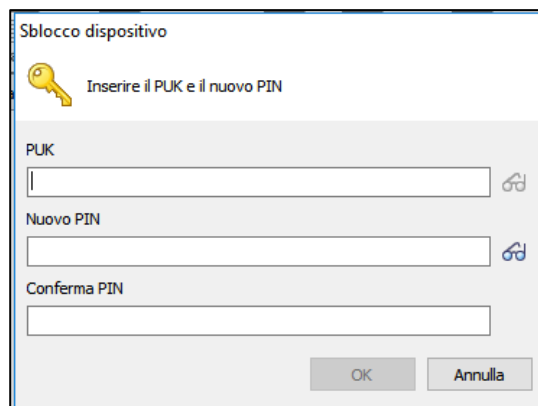


Figura 14 - funzione di Sblocco PIN

## 4.5.3 CAMBIO PUK

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

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

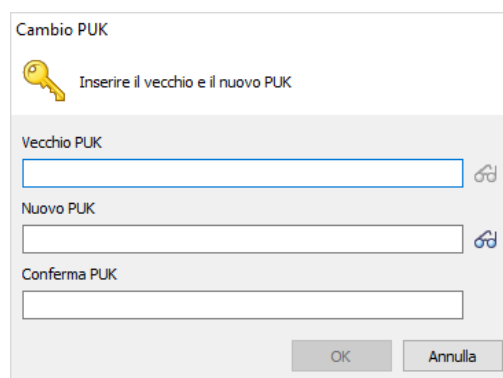


Figura 15 - funzione di Cambio PUK

#### 4.5.4 VISUALIZZA CERTIFICATI



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

|                          |
|--------------------------|
| File certificato (*.der) |
| File certificato (*.pfx) |
| File certificato (*.spc) |
| File certificato (*.pem) |

##### 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:

##### PEM:

Formato più comunemente utilizzato dalle Certification Authorities per test  
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).



Verifica

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

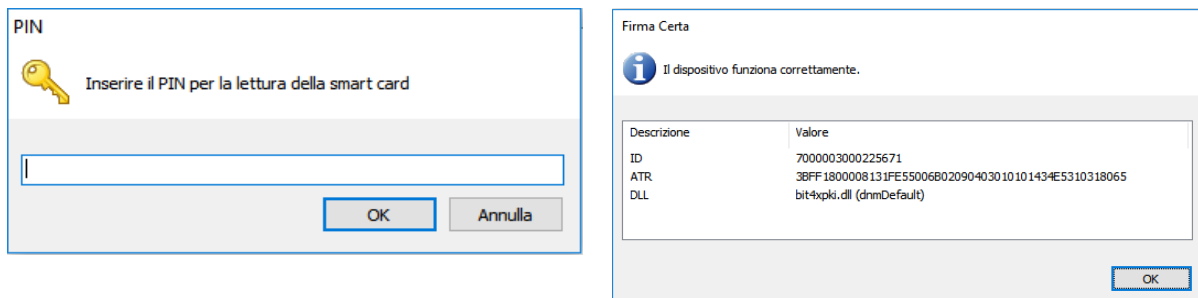
Premendo questo tasto viene effettuata la verifica dei certificati presenti nella smart card. Cliccando sulle etichette *Esito* e *Dettagli* è possibile visualizzare il risultato del test eseguito e le particolarità del Certificato selezionato.

| Esito  | Dettagli   |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
|--|--|-----------|--|-------------|-------------------------------|----------|------------------------------|----------------|--|--------------------------|----|----------------|-----------------------------|---------------------|-------------------------|--------------------|----------------------------|
| <p>✓ <b>Il certificato di autenticazione è attendibile</b><br/>Periodo di validità dal 14/10/2011 al 14/10/2014<br/>Verificato alla data odierna<br/>La <a href="#">lista dei certificati</a> utilizzata per la verifica risulta firmata da DigitPA</p> <p>✓ <b>Verifica OCSP : il certificato è attivo</b><br/>Verificato alla data odierna</p> | <table border="1"><thead><tr><th colspan="2">Tipologia</th></tr></thead><tbody><tr><td>Descrizione</td><td>Certificato di autenticazione</td></tr><tr><td>Validità</td><td>dal 14/10/2011 al 14/10/2014</td></tr><tr><th colspan="2">Ente emittente</th></tr><tr><td>Stato Ente certificatore</td><td>IT</td></tr><tr><td>Organizzazione</td><td>Namirial S.p.A./02046570426</td></tr><tr><td>Unità organizzativa</td><td>Certification Authority</td></tr><tr><td>Ente certificatore</td><td>Namirial CA Autenticazione</td></tr></tbody></table> | Tipologia |  | Descrizione | Certificato di autenticazione | Validità | dal 14/10/2011 al 14/10/2014 | Ente emittente |  | Stato Ente certificatore | IT | Organizzazione | Namirial S.p.A./02046570426 | Unità organizzativa | Certification Authority | Ente certificatore | Namirial CA Autenticazione |
| Tipologia  |  |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Descrizione  | Certificato di autenticazione  |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Validità   | dal 14/10/2011 al 14/10/2014   |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Ente emittente   |  |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Stato Ente certificatore   | IT   |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Organizzazione   | Namirial S.p.A./02046570426  |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Unità organizzativa  | Certification Authority  |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |
| Ente certificatore   | Namirial CA Autenticazione   |           |  |             |                               |          |                              |                |  |                          |    |                |                             |                     |                         |                    |                            |

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).



The image shows two side-by-side windows from the FirmaCerta software. The left window, titled 'PIN', contains a key icon and the text 'Inserire il PIN per la lettura della smart card'. Below this is a text input field and two buttons: 'OK' and 'Annulla'. The right window, titled 'Firma Certa', displays an information icon and the message 'Il dispositivo funziona correttamente.' Below this is a table showing device details.

| Descrizione | Valore   |
|-------------|--|
| ID          | 7000003000225671                                   |
| ATR         | 3BFF1800008131FE55006B02090403010101434E5310318065 |
| DLL         | bit4xpki.dll (dnnDefault)                          |

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 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.

*Figura 19 - Introduzione funzioni: firma grafometrica*

### 4.6.1 FIRMA DOCUMENTO



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

*Figura 20 - Introduzione funzione di 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).

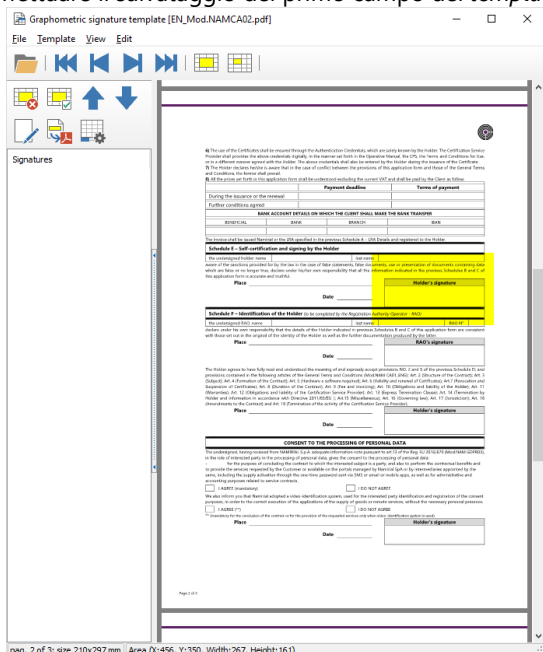
Dopo aver lanciato il *tool*, aprire da *File* il PDF che si desidera parametrizzare. In corrispondenza del puntatore comparirà un rettangolo giallo corrispondente all'area di firma, la cui superficie può essere aumentata o diminuita premendo i tasti corrispondenti sulla *Barra degli Strumenti* (fig.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



*Figura 21 - Template di firma*



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.

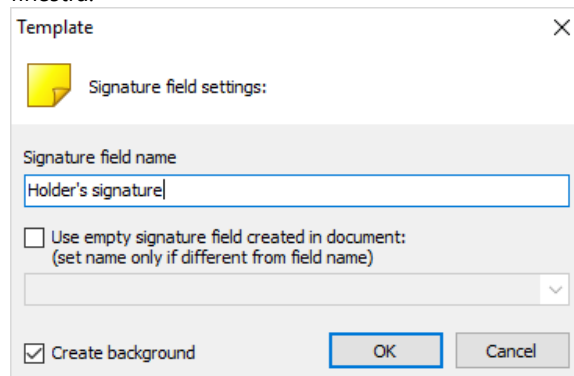


Figura 22 - Marcatore nel template

### 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.

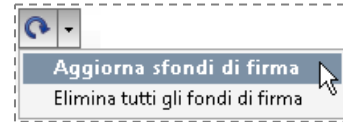


Per modificare lo sfondo occorre accedere alle *Proprietà* del campo firma salvato cliccando sull'icona corrispondente (fig. a lato) e spostarsi quindi sulla *Label* denominata *Sfondo*.

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.

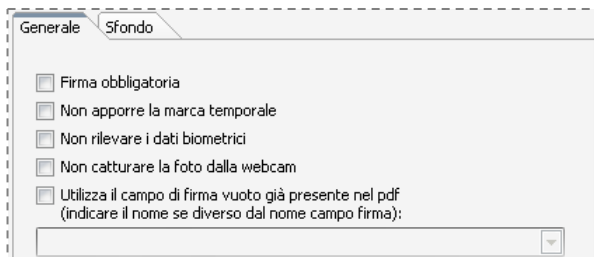
Figura 23: Sfondo Firma

Si consiglia sempre di salvare i 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 24 - Generale Proprietà di Firma

### Non apporre la marca temporale

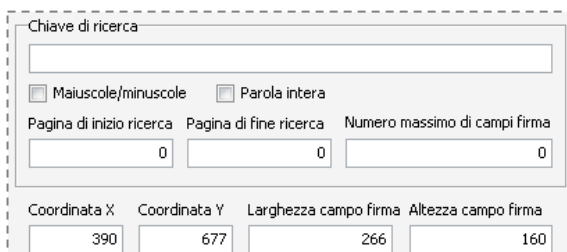
Tramite il software Firma Certa è anche possibile apporre la Marca Temporale sull'intero documento o sulle singole firme presenti all'interno di esso, selezionando il *check-box* in questione non verrà effettuato alcun *timestamping* sul campo firma selezionato.

### 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 25 - 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 26 - Pannello di Utilità

### 4.7.1 CIFRA E DECIFRA



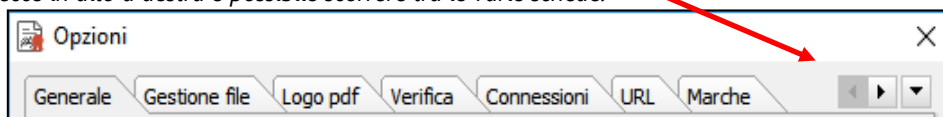
È un'applicazione che consente la cifratura di file di ogni tipo e dimensione, nel rispetto della normativa vigente e degli standard tecnici di riferimento. Molto versatile e di facile uso, Firma Certa Protect è disponibile per ambiente Windows. Consultare la **guida** con le informazioni essenziali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

Figura 27 - Introduzione a FirmaCerta Protect

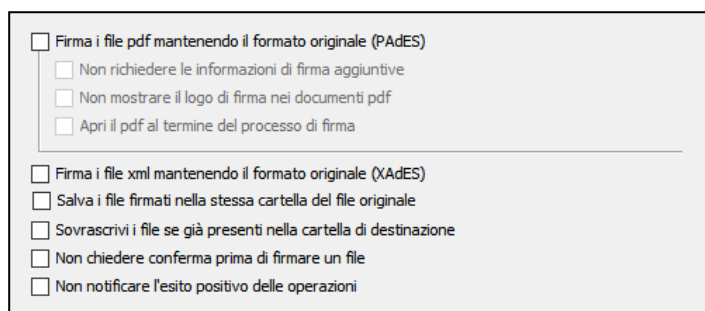
## 4.7.2 OPZIONI GENERALI

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 originale (PAdES)
  - ☐ Non richiedere le informazioni di firma aggiuntive
  - ☐ Non mostrare il logo di firma nei documenti pdf
  - ☐ Apri il pdf al termine del processo di firma
- ☐ Firma i file xml mantenendo il formato originale (XAdES)
  - ☐ Salva i file firmati nella stessa cartella del file originale
  - ☐ Sovrascrivi i file se già presenti nella cartella di destinazione
  - ☐ Non chiedere conferma prima di firmare un file
  - ☐ Non notificare l'esito positivo delle operazioni

### **Firma i file pdf mantenendo il formato (PAdES):**

- **Non richiedere le informazioni di firma aggiuntive:**
- **Non mostrare il logo di firma nei documenti pdf:**

mantiene il formato originale del file firmato (altrimenti convertito in formato .p7m), fornendo la possibilità di visualizzare i documenti anche ad un utente non fornito di software per la firma digitale.

Non saranno visualizzate alcune informazioni facoltative nella firma del documento;

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.

Figura 28 - 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.*

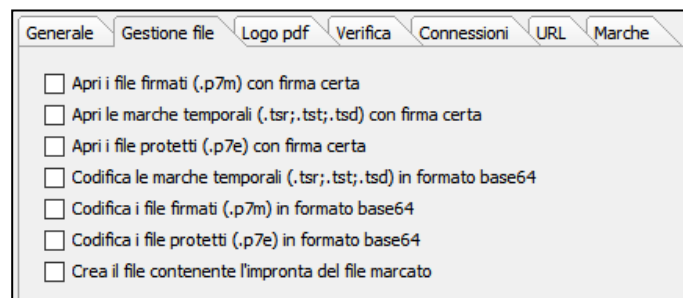


Figura 29 - Opzioni: Gestione File

#### 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*).

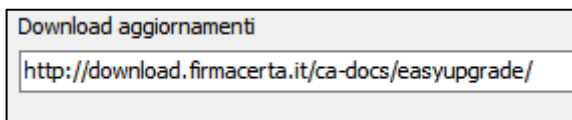


Figura 30 - Opzioni:URL

#### 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.

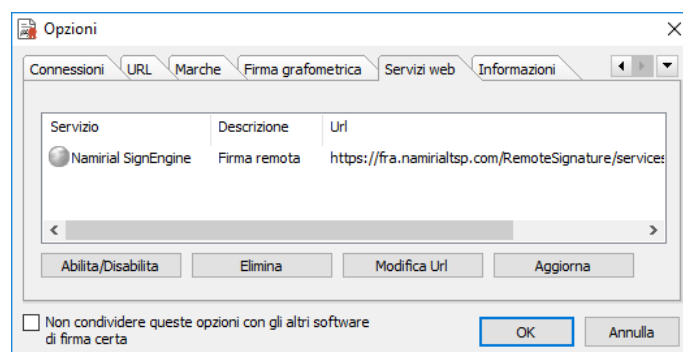


Figura 31 - Opzioni Servizi Web

#### 4.7.2.4 INFORMAZIONI

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

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

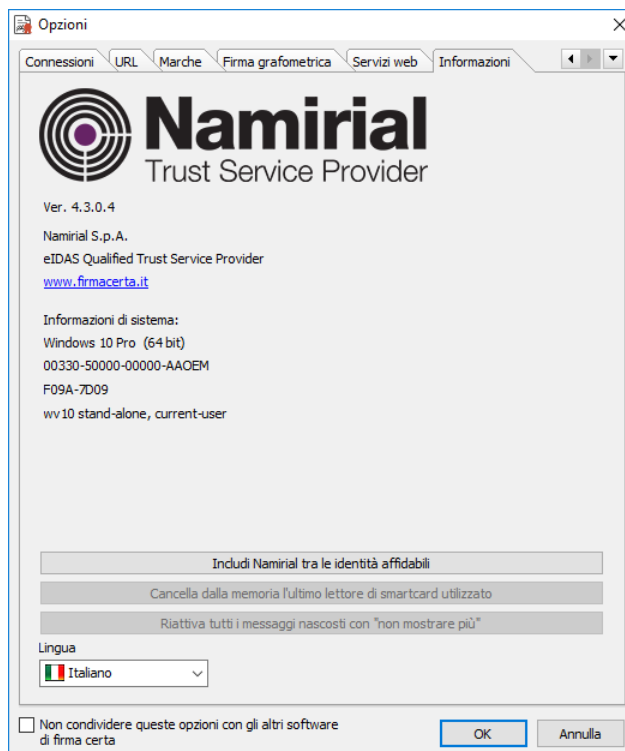


Figura 32 - Opzioni: informazioni

#### 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.

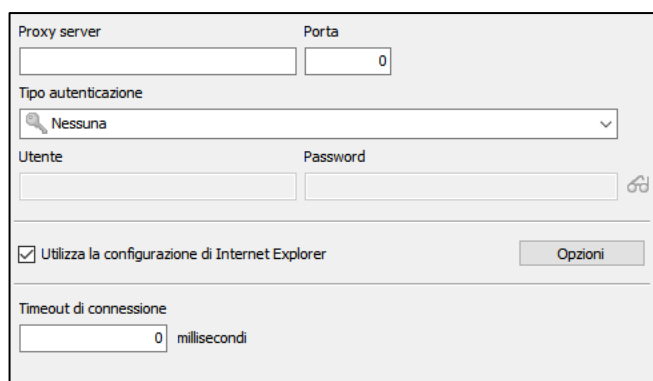


Figura 33 - Opzioni: Configurazione del Proxy

## 4.7.4 OPZIONI FIRMA



Figura 34 - 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*.

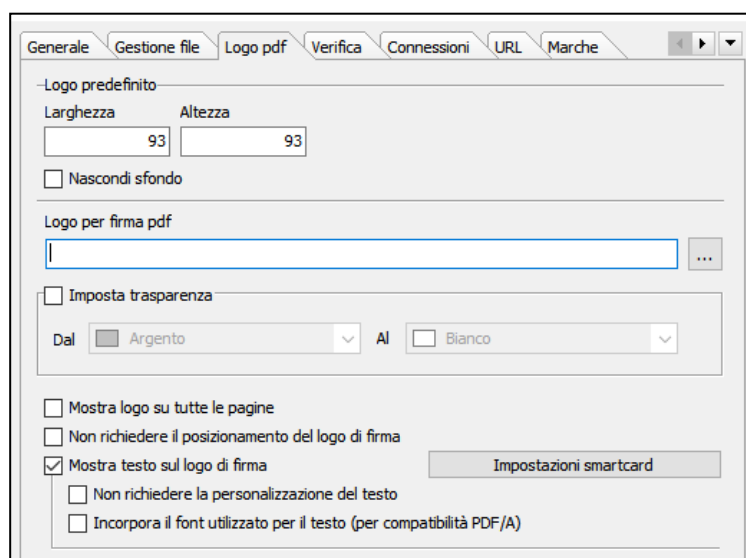


Figura 35 - Opzioni: Logo PDF



#### 4.7.5 OPZIONI VERIFICA

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

- ☒ Esegui la verifica all'avvio
- ☐ Attiva la gestione della cache per la verifica dei CRL
- ☐ Attiva la gestione della cache per la verifica delle TSL (periodo validità cache : 1 giorno)
- ☒ Verifica i certificati quando si visualizza il documento firmato

Figura 36 - 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 37 - 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](http://www.firmagrafometrica.it)).

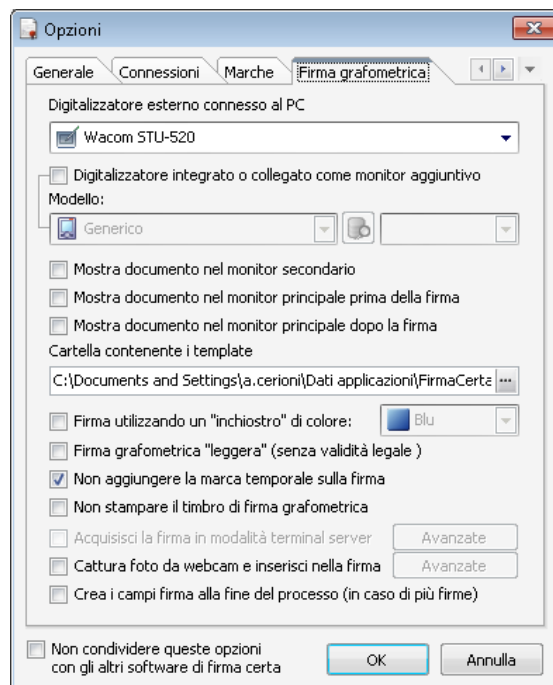


Figura 38 - Opzioni Firma grafometrica

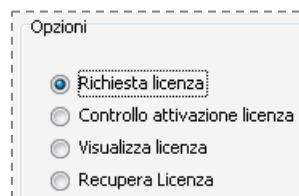
#### 4.7.6.2 ATTIVAZIONE

L'utente che desidera attivare il software riceve tramite mail un certificato di cifratura tecnico che deve essere installato nel pc.

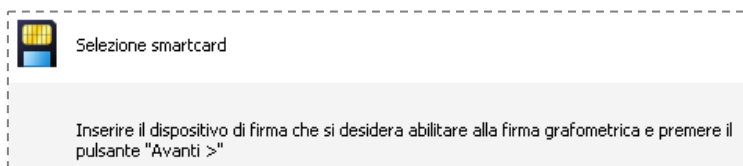
Questo certificato è necessario per l'attivazione della licenza di firma grafometrica.

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 39 - Opzioni Grafometrica: Attivazione Licenza*

#### 4.7.6.3 INFORMATIVA

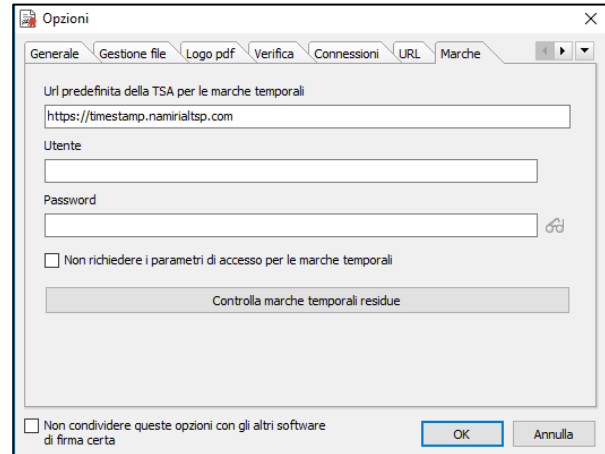
La funzione consente la compilazione da parte del firmatario di redigere e firmare grafometricamente, mediante dispositivo digitale collegato (tavoletta grafica o altro hardware supportato) un documento PDF informativo sul funzionamento della Firma grafometrica in genere e sul trattamento dei documenti 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 40 - 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 Temporal

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

Figura 41 - 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

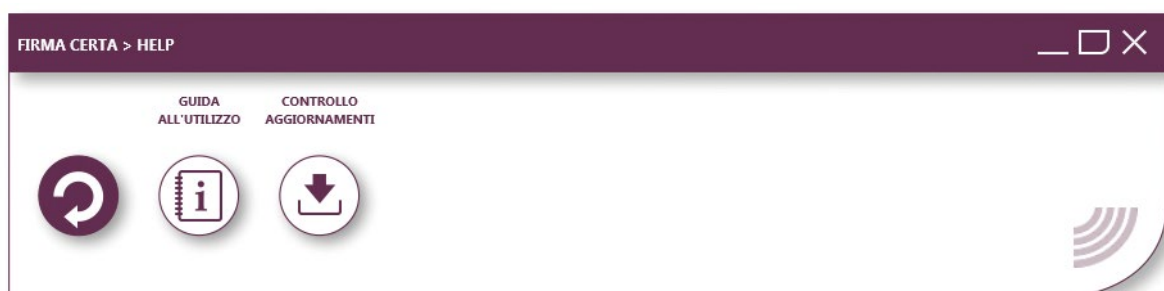


Figura 42 - Pannello: Help

## 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**.

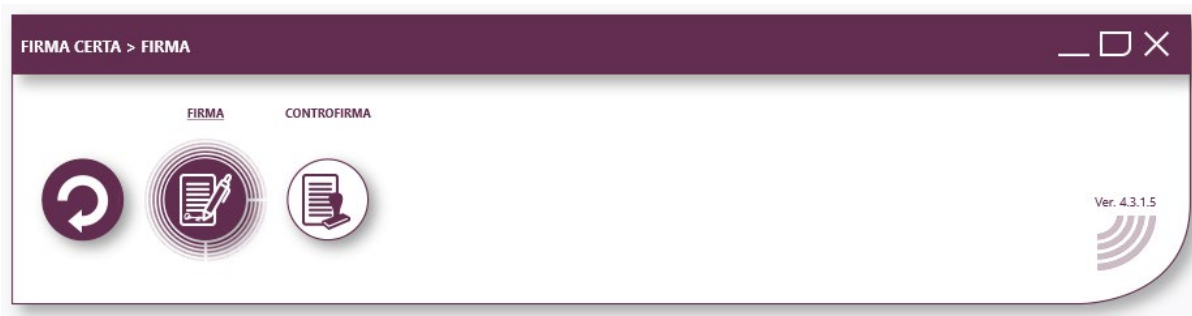


Figura 43 - Pannello di Firma

**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

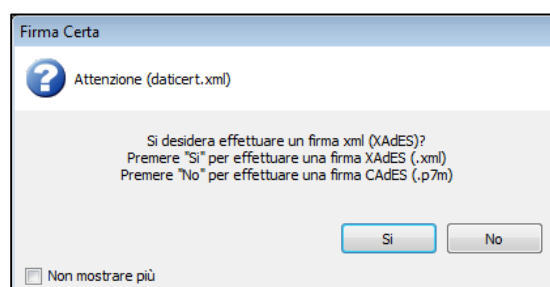


Figura 44 - Scelta formato di firma Cades-Xades

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

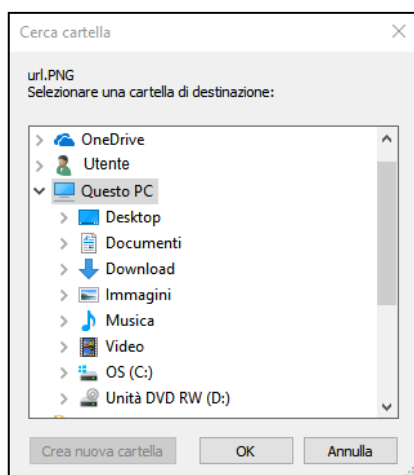


Figura 45 - Selezione cartella di destinazione

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.

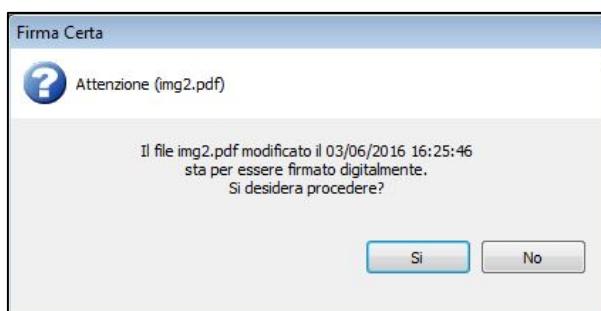


Figura 46 - Conferma di firma

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

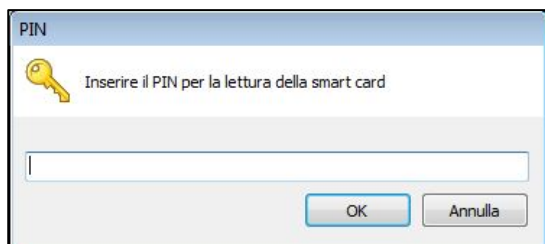


Figura 47 - Inserimento PIN

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

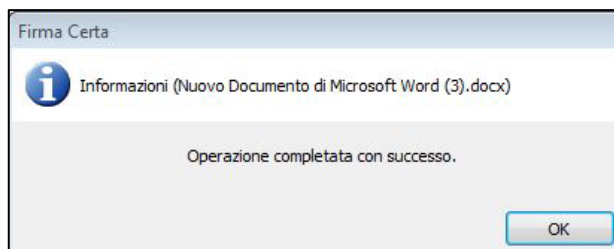


Figura 48 - Operazione completata

## 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

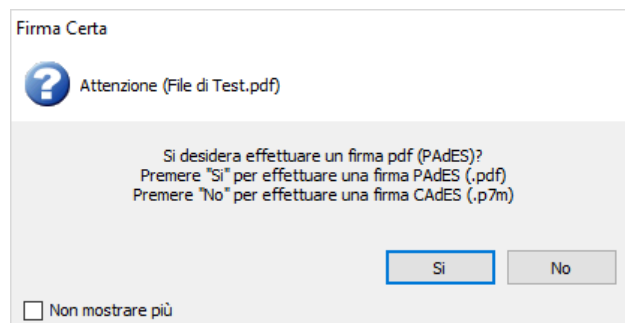


Figura 49 - Scelta formato di firma Cades-Pades

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.

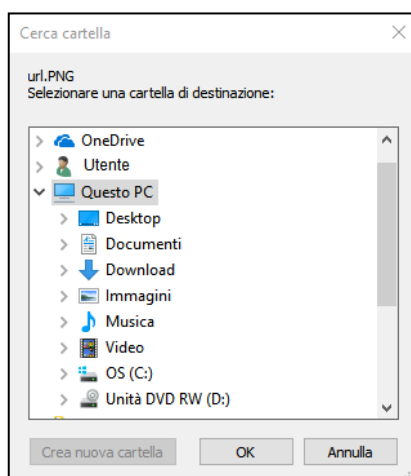


Figura 50 - Selezione cartella di destinazione

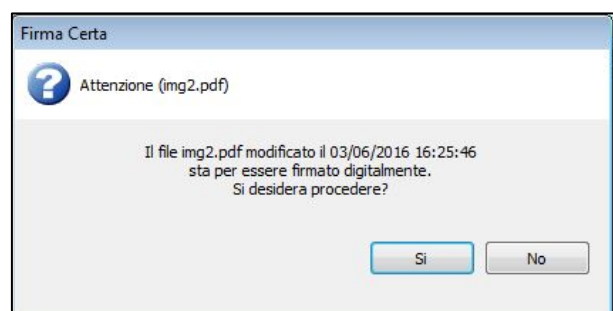
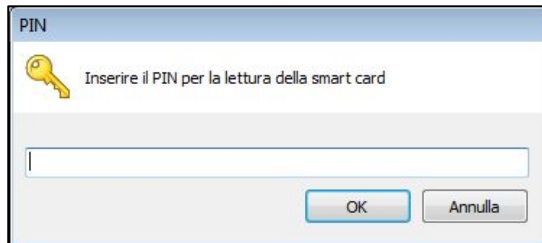


Figura 51 - Conferma di firma

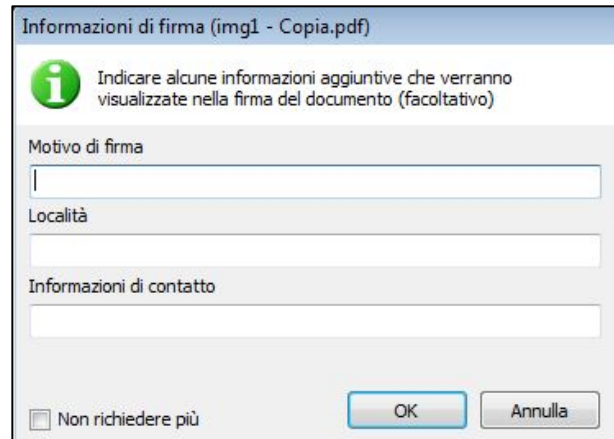
Inserire il PIN del dispositivo di Firma Digitale e cliccare su **OK**.



A dialog box titled "PIN" with a key icon. It contains the text "Inserire il PIN per la lettura della smart card" and a text input field. At the bottom are "OK" and "Annulla" buttons.

Figura 52 - Inserimento PIN

Selezionare il Motivo della Firma (facoltativo).



A dialog box titled "Informazioni di firma (img1 - Copia.pdf)". It contains an information icon and the text "Indicare alcune informazioni aggiuntive che verranno visualizzate nella firma del documento (facoltativo)". Below are three text input fields labeled "Motivo di firma", "Località", and "Informazioni di contatto". At the bottom is a checkbox "Non richiedere più" and "OK" and "Annulla" buttons.

Figura 53 - informazioni di firma

Selezionare dove apporre il Logo utilizzando il Marcatore Verde

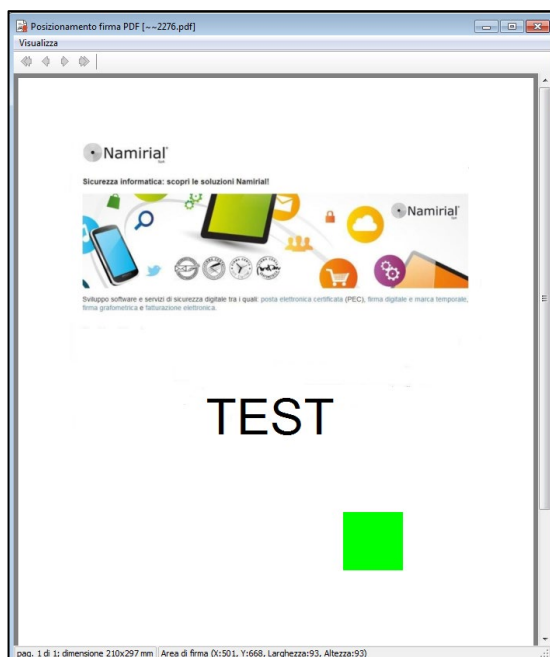
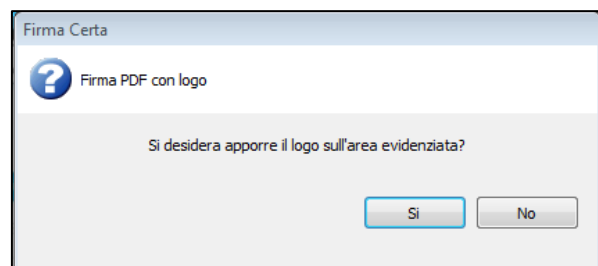


Figura 54 - Posizionamento del marcatore di firma

Confermare l'apposizione premendo **Sì**.



A dialog box titled "Firma Certa" with a question mark icon. It contains the text "Firma PDF con logo" and "Si desidera apporre il logo sull'area evidenziata?". At the bottom are "Sì" and "No" buttons.

Figura 55 - Conferma di posizionamento



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

Personalizzazione logo (img1 - Copia.pdf)

Indicare le personalizzazioni del logo di firma (facoltativo)

☒ Mostra data e ora

☒ Testo auto generato

Testata

Titolo 1

Testo 1 (max 4 righe)

Titolo 2

Testo 2

☒ Dimensione testo automatica

Data e ora  Testata

Titolo  Testo

☐ Salva i valori nella smart card

☐ Non richiedere più

Figura 56 - Personalizzazione del logo

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

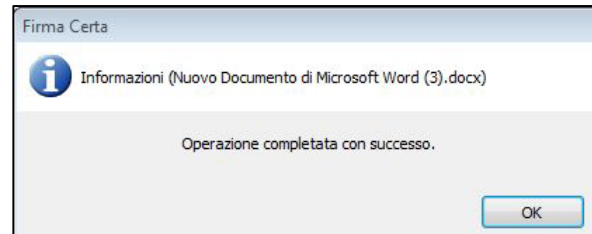


Figura 57 - Operazione Completata

## 5.2 COME CONTROFIRMARE

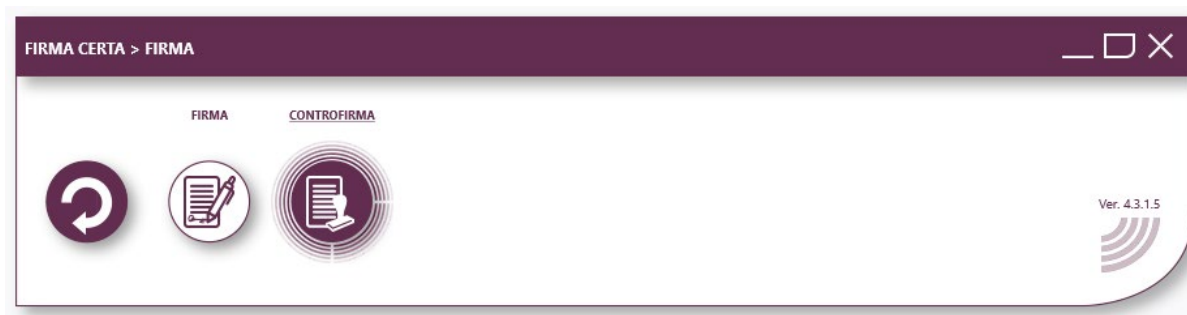


Figura 58 - Pannello di Controfirma

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**.

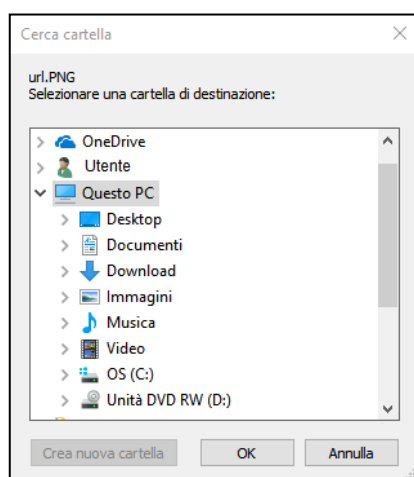


Figura 59 - Selezione cartella di destinazione

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

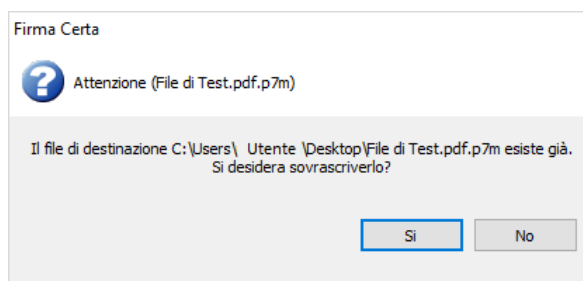


Figura 60 - Conferma di sovrascrizione

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

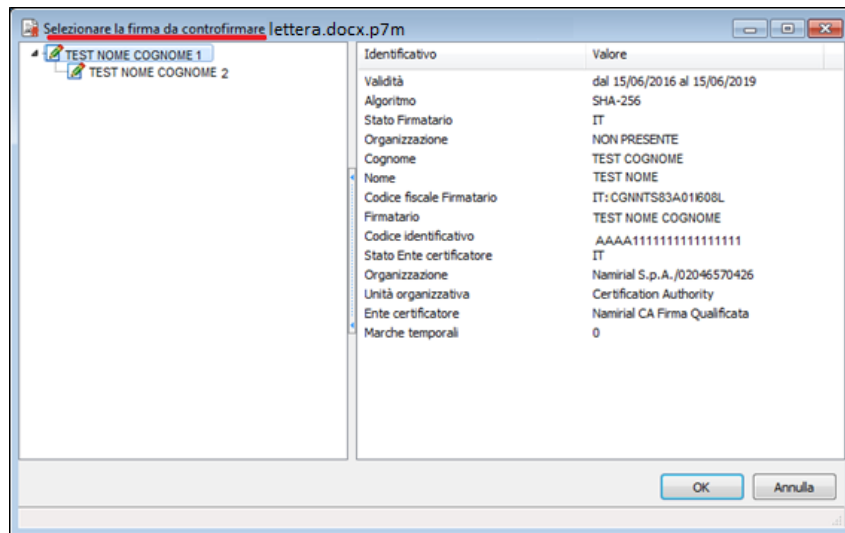


Figura 61 - Schermata di esempio: verifica file controfirmato

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

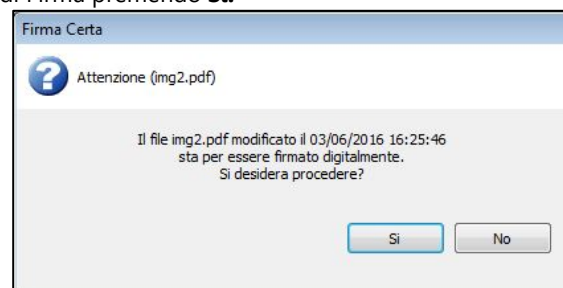


Figura 62 - Conferma di firma

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

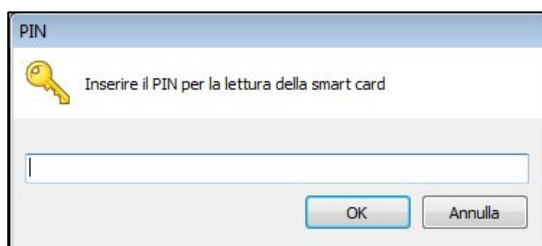


Figura 63 - Inserimento Pin

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

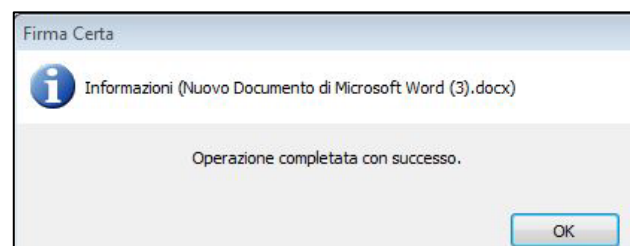


Figura 64 - Operazione Completata

## 6 APPENDICE B: COME MARCARE UN FILE

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

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



Figura 65 - Pannello di Utilità

### 6.1 CONFIGURAZIONE PARAMETRI MARCHE TEMPORALI

#### **Da FirmaCerta > Utilità > Opzioni Marca Temporale**

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

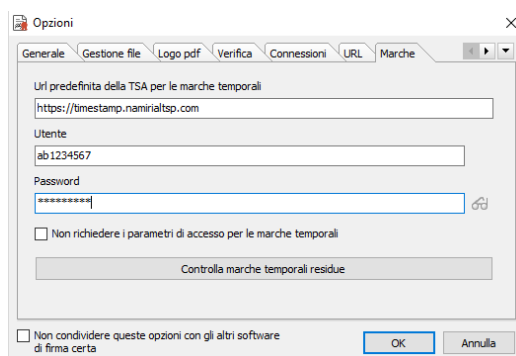


Figura 66 - Opzioni Configurazione Marche

Cliccando sull'icona a fianco del campo Password è possibile visualizzare in chiaro la password che si sta inserendo.



possibile visualizzare in chiaro la password che si sta inserendo.

**RECUPERO CREDENZIALI MARCHE TEMPORALI:** In caso di smarrimento della username e/o della password, contattare il supporto tecnico per e-mail all'indirizzo: [supportoca@namirial.com](mailto:supportoca@namirial.com) indicando nell'OGGETTO: **RECUPERO CREDENZIALI TIMESTAMP** – 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)

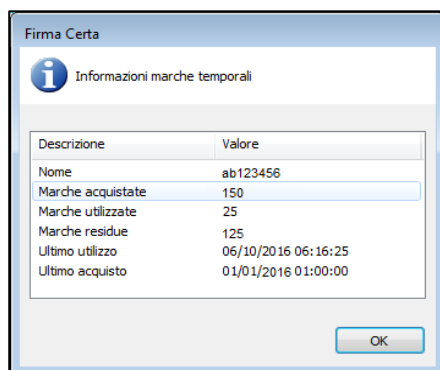


Figura 67 - Controllo Marche temporali

## 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.

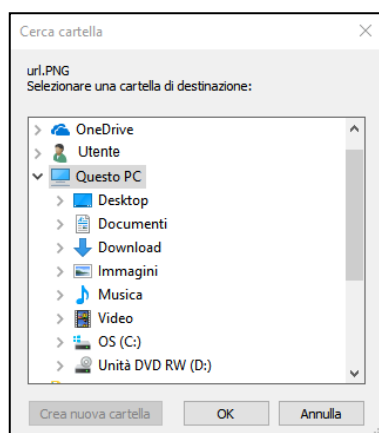


Figura 68 - Selezione cartella di destinazione

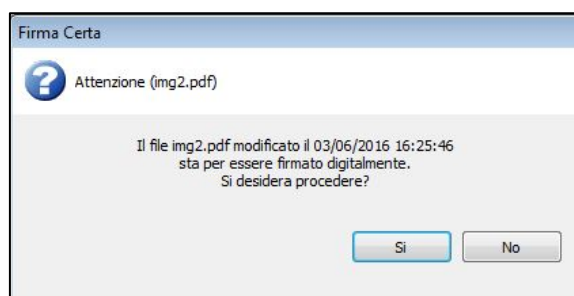


Figura 69 - Conferma di firma

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

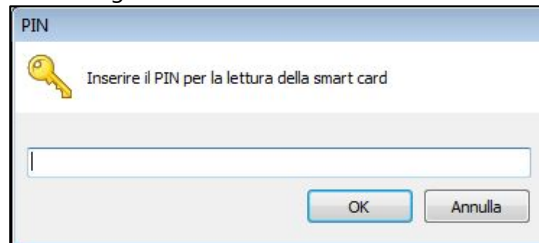


Figura 70 - Inserimento del PIN

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

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

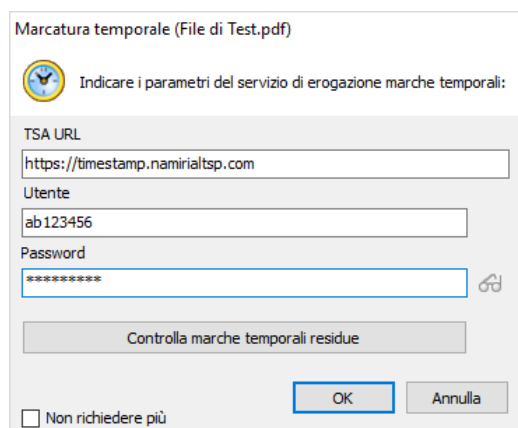


Figura 71 - Conferma credenziali Marche

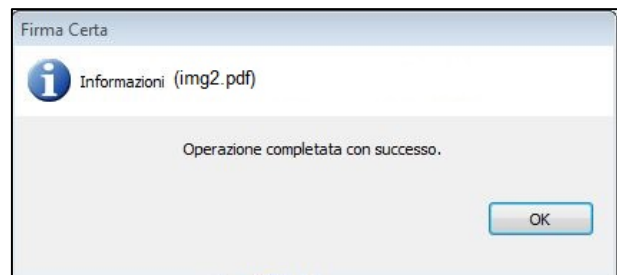


Figura 72 - Operazione Completata

## 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**.

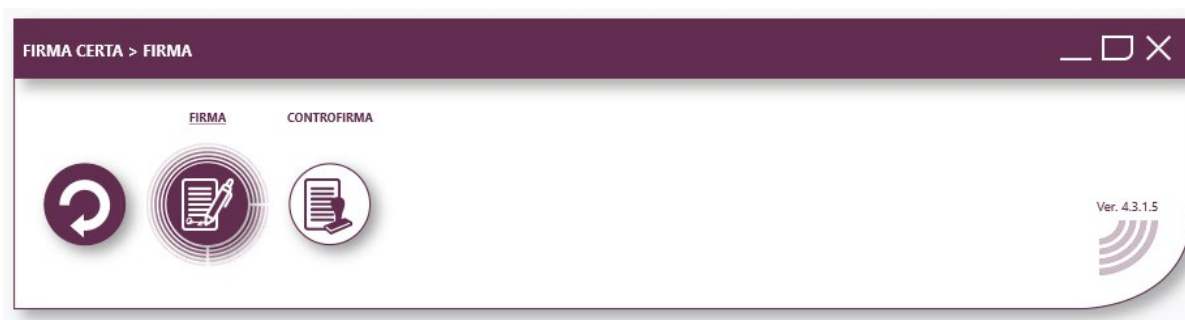


Figura 73 - Pannello di Firma

**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

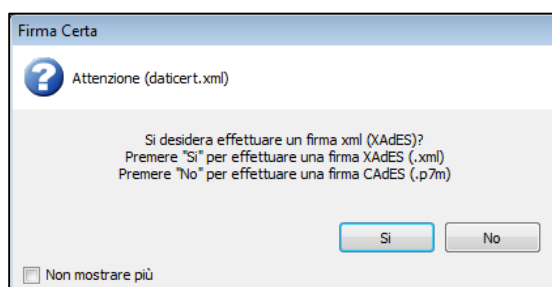


Figura 74 - Selezione del formato di firma Cades

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 75 - Pannello FirmaCerta

Selezionare il formato .TSD per la Marca Temporale.

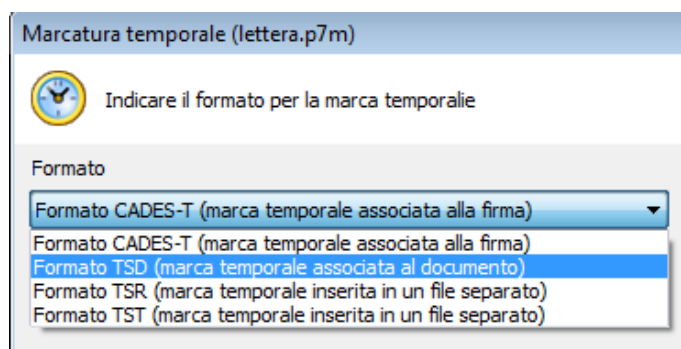


Figura 76 - Scelta formato marca temporale

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

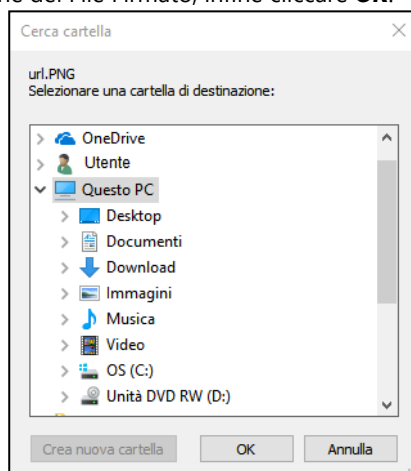


Figura 77 - Scelta cartella di destinazione

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

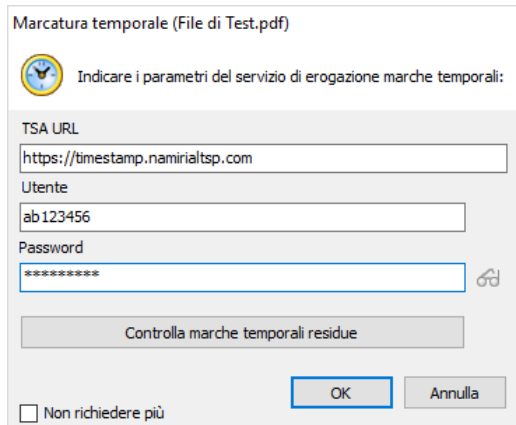


Figura 78 - conferma dati di configurazione Marche

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

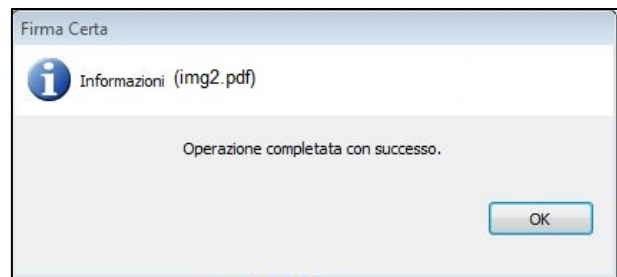


Figura 79 - Operazione Completata

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

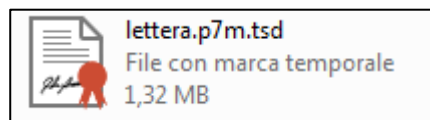


Figura 80 - Esempio: file marcato temporalmente



### 6.3.3 SEPARARE LA MARCA TEMPORALE

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



Figura 81 - Pannello di FirmaCerta

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

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

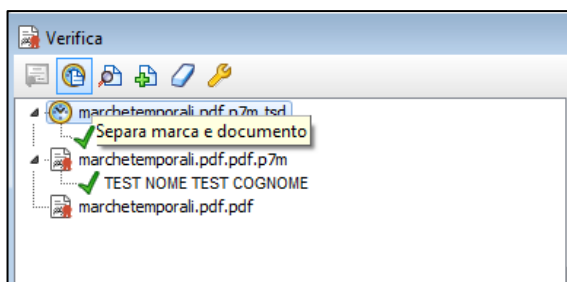


Figura 82 - Separazione marca temporale

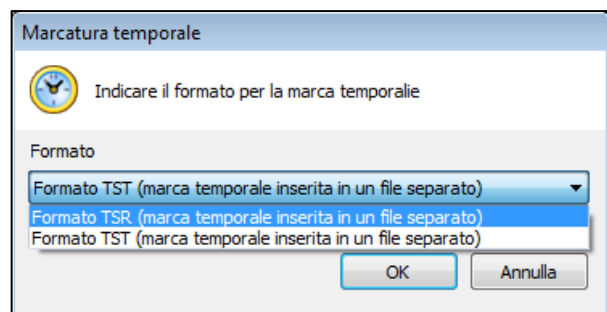


Figura 83 - Selezionare il formato di marca

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 84 - 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 85 - Pannello di Firmacerta

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

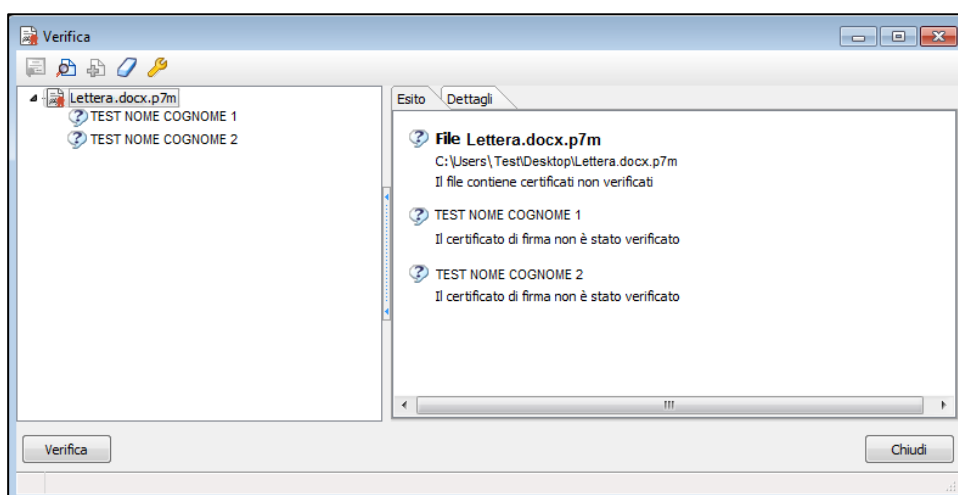


Figura 86 - Schermata di verifica



**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;

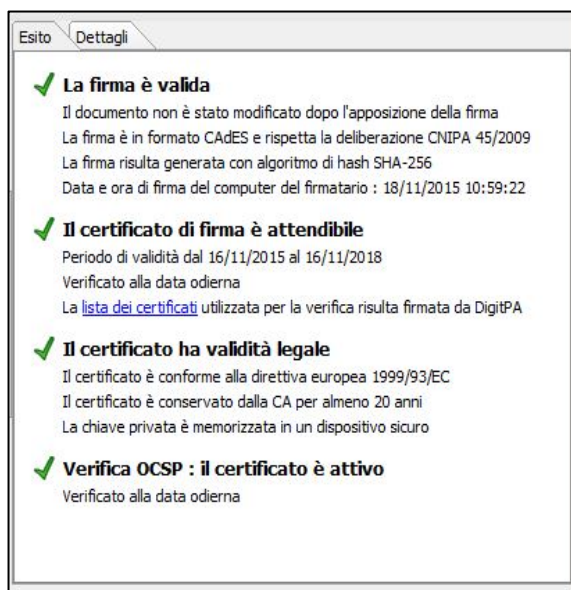


Figura 87 - Schermata di Esito

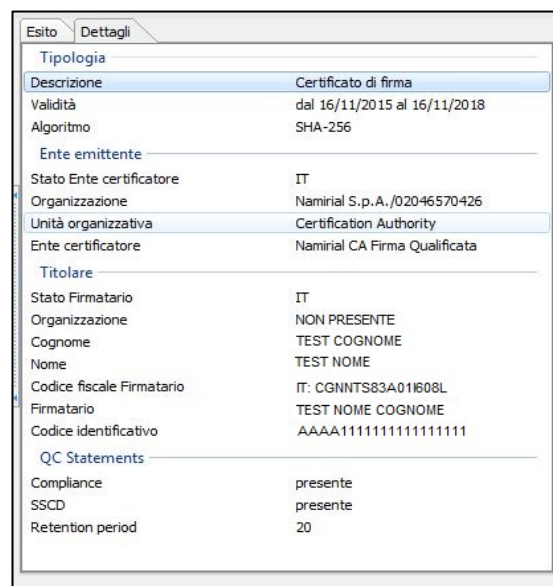


Figura 88 - Schermata di Dettagli

## 7.1 PER IMPOSTARE IN AUTOMATICO L'AVVIO DELLA VERIFICA DELLE FIRME

Cliccare in **Utilità > Opzioni Verifica**.

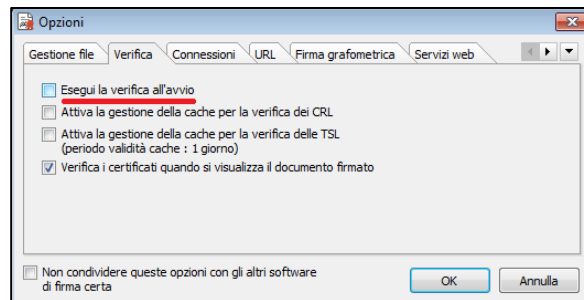


Figura 89 - Impostazioni di Verifica

## 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 90 - 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

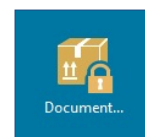
La **cifratura** (detta anche crittografia) di un documento è un'operazione con la quale si rende quel documento completamente illeggibile per chiunque, ad eccezione di chi possiede la chiave che permette di decifrarlo, ossia riportarlo "in chiaro". La cifratura, dunque, permette di assicurare la confidenzialità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

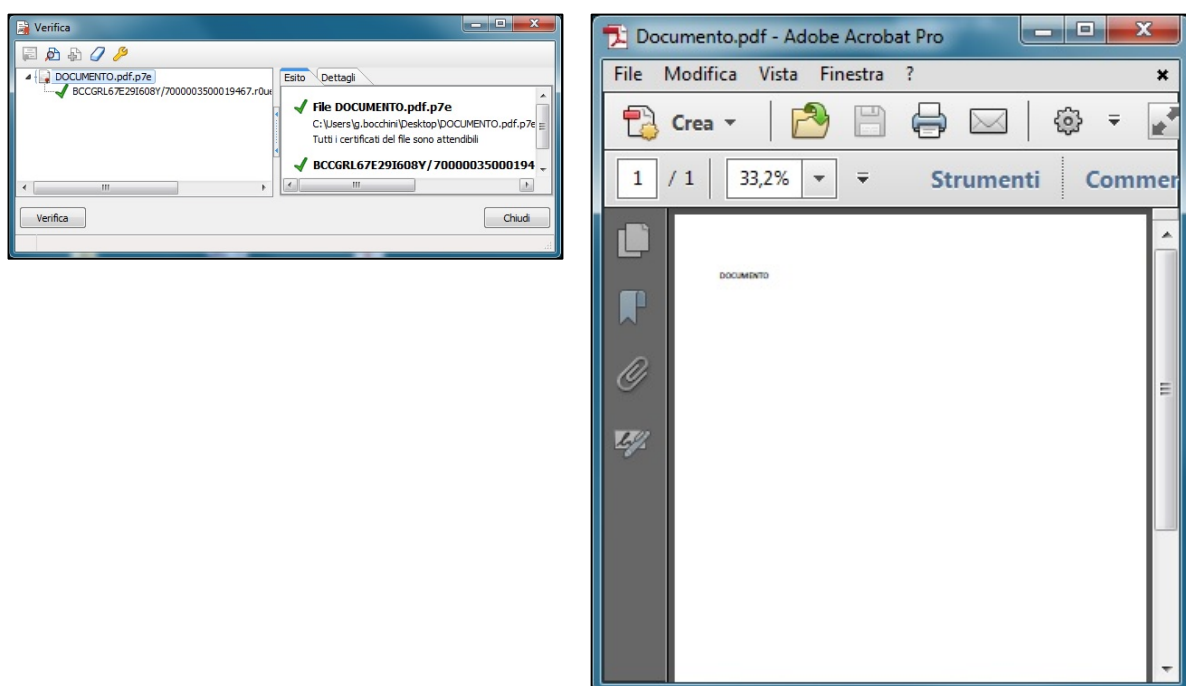


Figura 91 - Schermata di Verifica con esempio

### **Attenzione:**

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

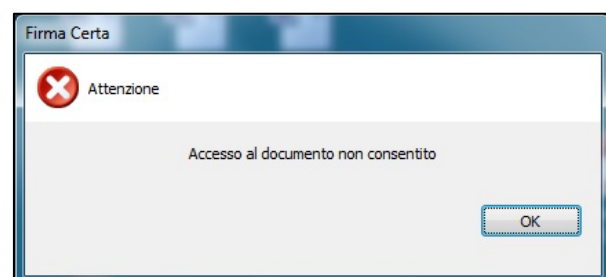


Figura 92 - Accesso Negato



## 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*:

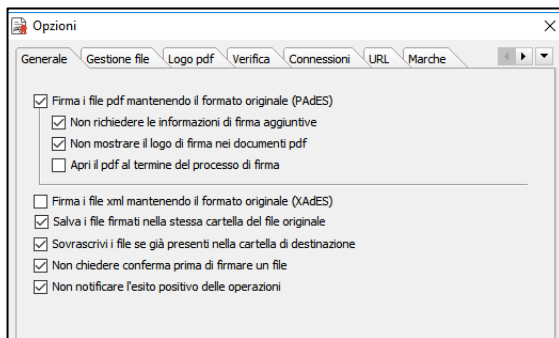


Figura 93 - Configurazione per firma Pades

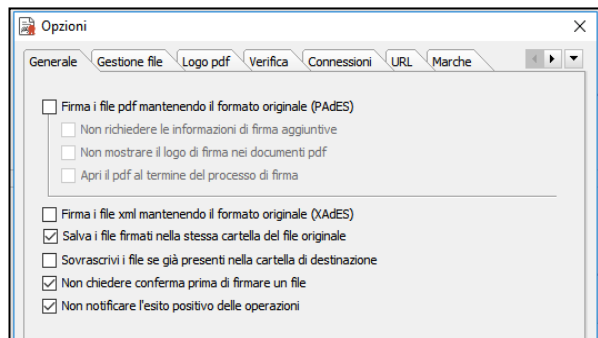


Figura 94 - Configurazione per firma Cades

## 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:

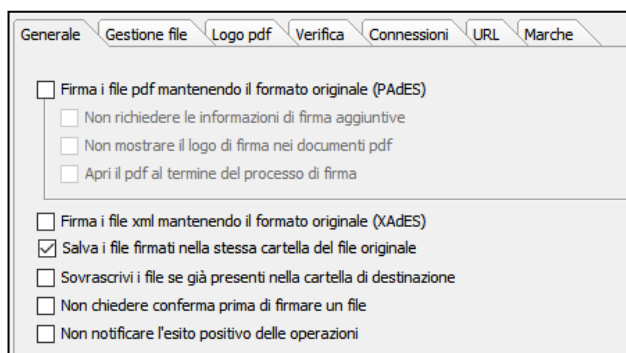


Figura 95 - Schermata opzioni Generale

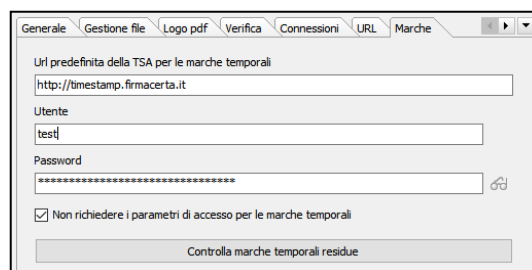


Figura 96 - Schermata opzioni Marche

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.

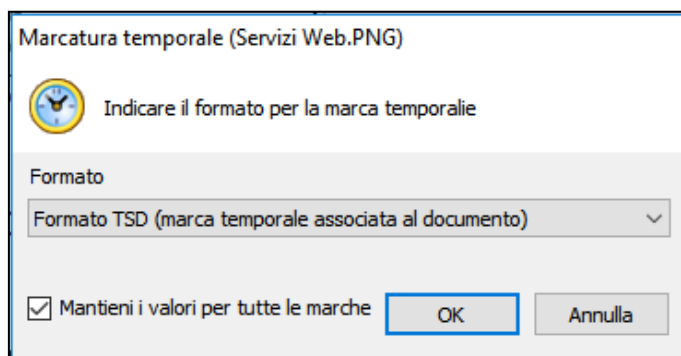


Figura 97 - Schermata formato Marche

## 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 98 - Schermata opzioni generali

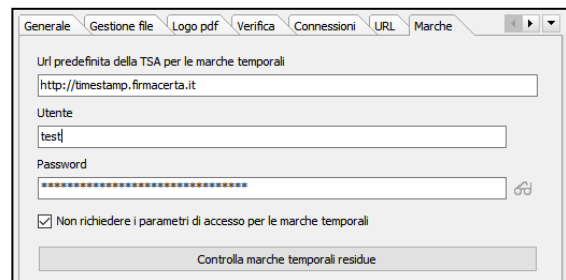


Figura 99 - Schermata opzioni Marche

Sarà richiesto di inserire il codice PIN una sola volta.



Figura 100 - 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 101 - Schermata Clausole Vessatorie

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

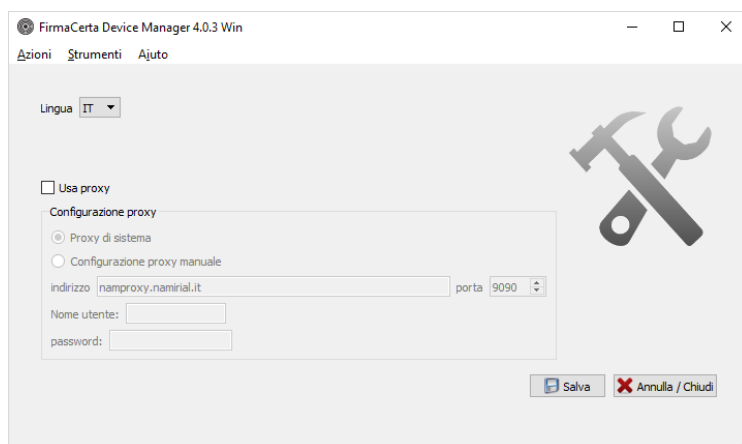


Figura 102 - Configurazione Proxy

## 11.2 MODALITÀ DI RINNOVO SMARTCARD E TOKEN

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.

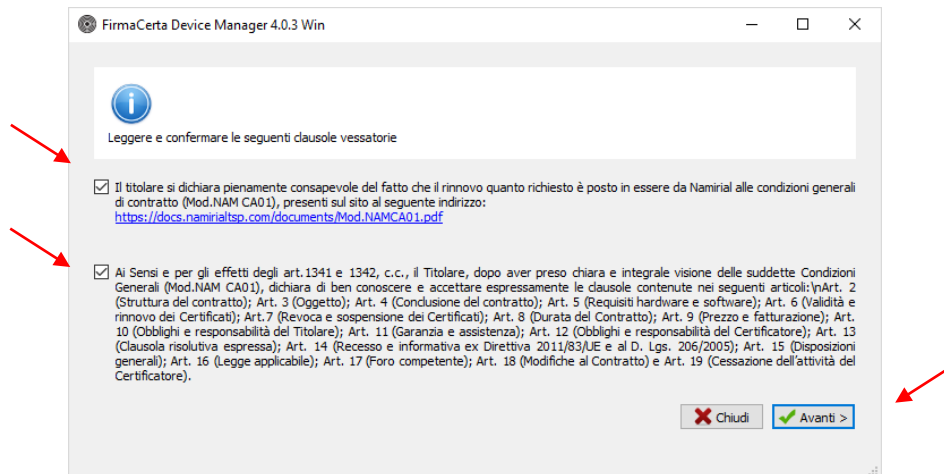


Figura 103 - Schermata Clausole Vessatorie

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

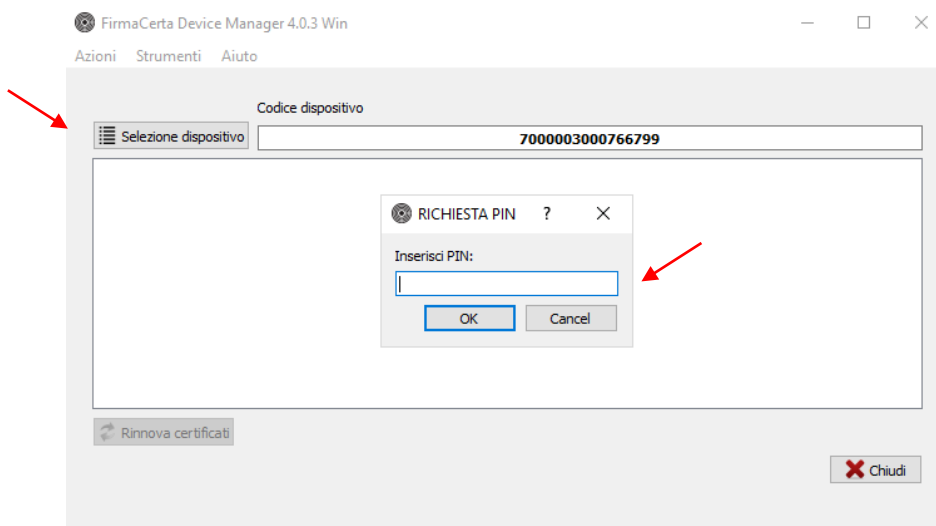


Figura 104 - Schermata Inserimento PIN

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

**Attendere il completamento della procedura di rinnovo.**

Cliccare su **"Rinnova Certificati"**.

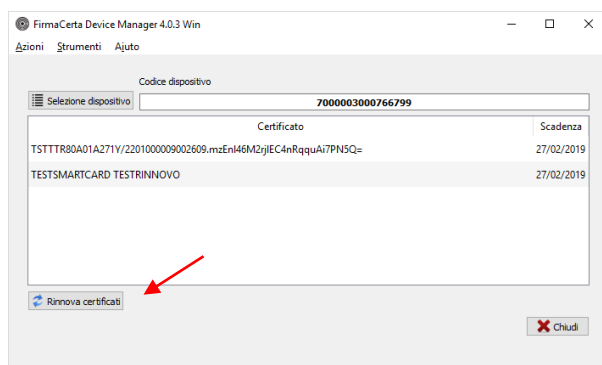


Figura 105 - Rinnovo Certificati

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

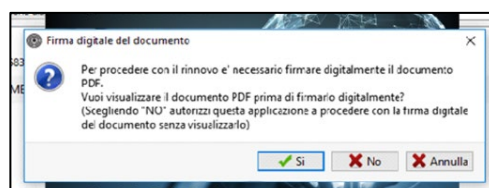


Figura 106 - Messaggio di visualizzazione del contratto

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

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

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

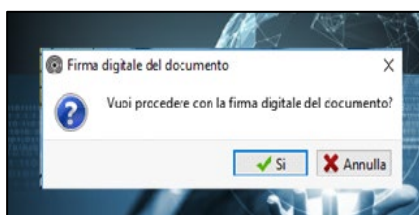


Figura 107 - Conferma apposizione della firma

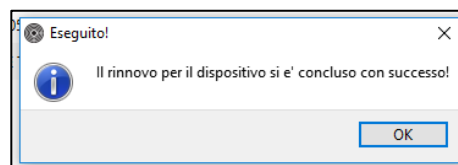


Figura 108 - Rinnovo completato con successo

## 11.3 MODALITÀ DI RINNOVO REMOTA E AUTOMATICA

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

Cliccare su **ACCEDI** ed inserire *username* e *password* ricevuti via mail contestualmente al rilascio del certificato digitale di firma.



Figura 109: Area Privata Namirial

**RECUPERO CREDENZIALI AREA PRIVATA:** In caso di smarrimento della username e/o della password, si può procedere al recupero dei singoli dati cliccando su "Non ricordo il nome utente" o "Non ricordo la password" e seguendo le indicazioni riportate. In caso di problematiche contattare il supporto tecnico per e-mail all'indirizzo: [supportoca@namirial.com](mailto:supportoca@namirial.com) indicando il codice fiscale del titolare e nell'oggetto: **RESET CREDENZIALI AREA PRIVATA**.

Dopo aver eseguito correttamente il login,

- Nella Home nella categoria *Funzionalità o servizi da attivare* > cliccare su *Esegui rinnovo certificato*;
- In alternativa cliccare su *Utente* > *Firma Digitale* > *Gestione*;

Per procedere verrà richiesto l'inserimento del codice OTP.

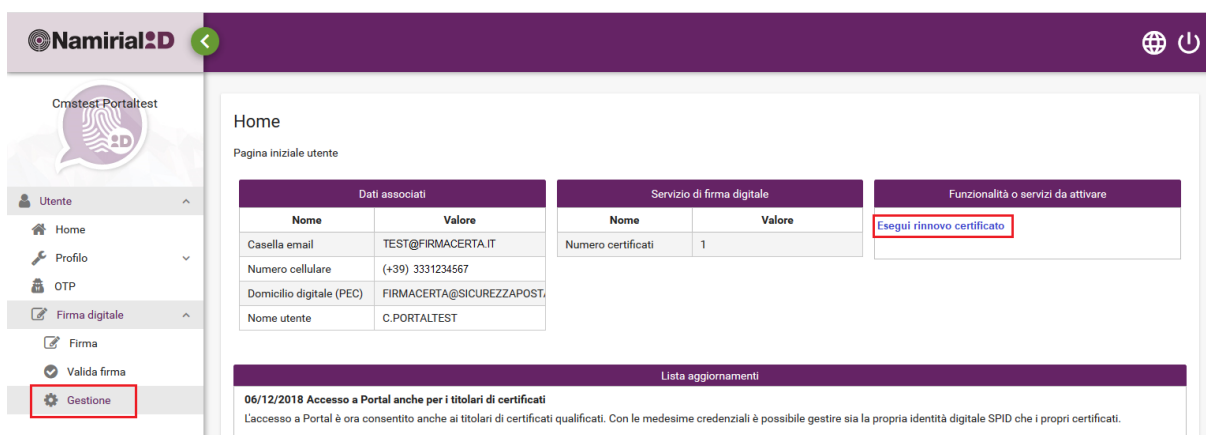


Figura 110: Dashboard Area Privata

In **Gestione certificati** sono visualizzati tutti i certificati associati all'utenza, e sotto la colonna *Rinnovabile* è possibile determinare quale certificato è in fase di rinnovo.

Selezionare il certificato > cliccare sul tasto **RINNOVA**, si aprirà il pannello: Procedura rinnovo in autonomia di certificato di sottoscrizione, dove sarà necessario inserire il PIN del Certificato (presente nella busta cieca digitale ricevuta al rilascio del certificato stesso) ed il codice OTP di verifica (in questo caso OTP SMS).



Figura 111: Gestione Certificati

Dopo aver Inserito tutti i dati, cliccare su "**FIRMA E RINNOVA**" e attendere il completamento della procedura di rinnovo del certificato.

The screenshot shows the 'Procedura rinnovo in autonomia di certificato di sottoscrizione' (Autonomous renewal procedure of a subscription certificate) form. It includes a header with the title and a brief explanation of the process. Below the header, there are several input fields and buttons. A 'Scarica contratto precompilato' button is at the top. Below it, there's a 'PIN' input field. Then, there's a dropdown menu showing 'SMS - 324282'. To the right of this dropdown is a green button labeled 'Invia con SMS'. Next to it is a 'Codice OTP' input field. Below these fields, there are two buttons: 'Firma e rinnovo' (highlighted with a red box) and 'Scarica contratto firmato'. At the bottom, there's a legend section titled 'Legenda rinnovabilità certificati'.

Figura 112: Processo di firma e rinnovo

## 12 APPENDICE I: FIRMA REMOTA

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

**NOTA:** 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.

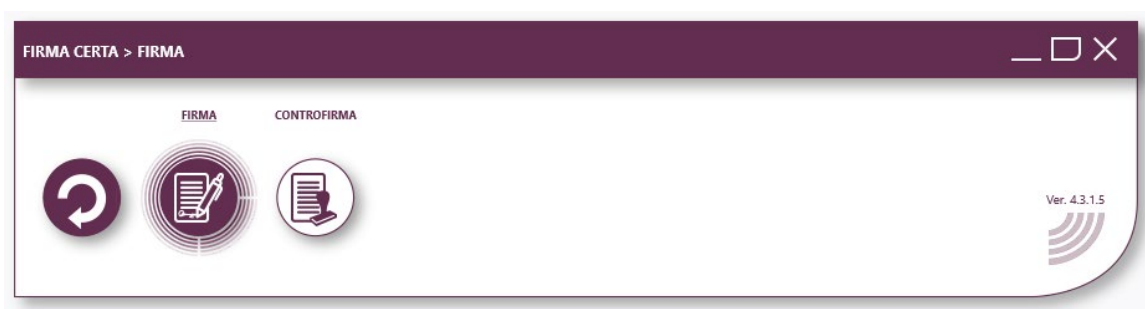


Figura 113 - come firmare

### 12.1 SELEZIONA LA TIPOLOGIA DI FIRMA

Il software Firmacerta permette di firmare qualsiasi tipo di file generico in formato CAdES (.p7m);

Per i file PDF o XML sarà mostrato con un messaggio a video se firmare in .P7M o mantenere il formato originale(pdf o xml).

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

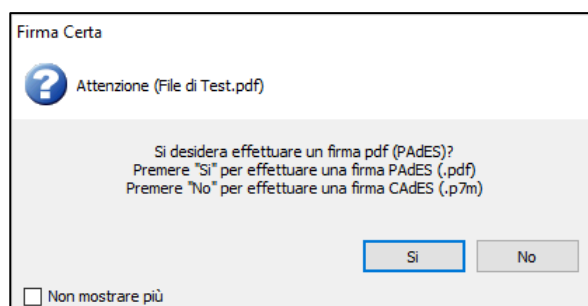


Figura 114 - schermata file pdf

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

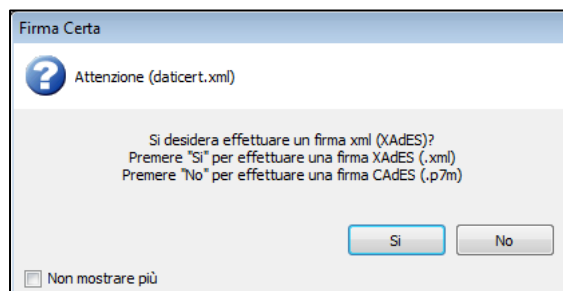


Figura 115 - schermata file xml

## 12.2 SCEGLIERE CARTELLA DI DESTINAZIONE

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

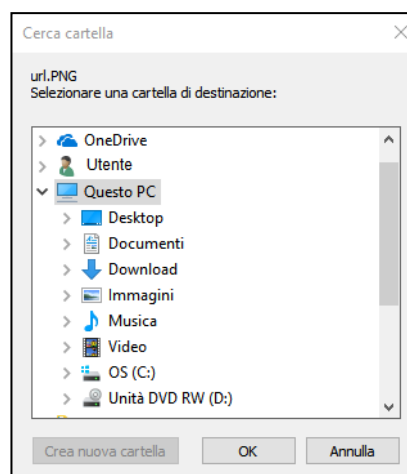


Figura 116 - selezione cartella

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

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

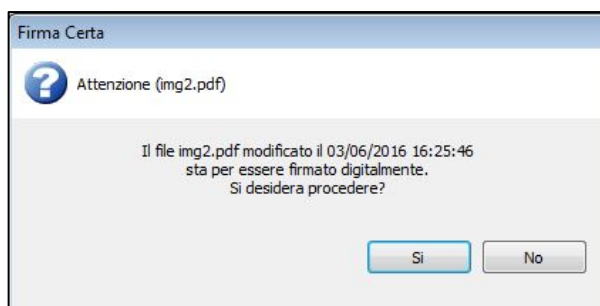


Figura 117 - conferma processo

## 12.3 INSERIMENTO PARAMETRI FIRMA REMOTA

Al primo avvio di FirmaCerta è necessario configurare il nome utente per l'utilizzo della firma remota.  
In **Impostazioni** inserire il nome utente fornito in fase di emissione del certificato.

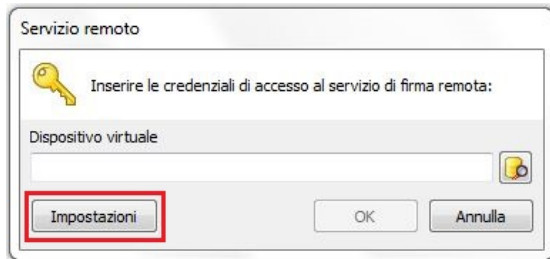


Figura 118 - inserimento user parte 1

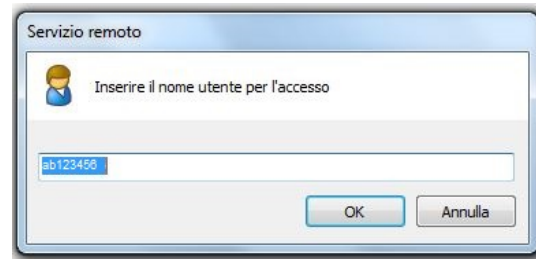


Figura 119 - inserimento user parte 2

### RECUPERO CREDENZIALI FIRMA REMOTA

In caso di smarrimento accedere alla propria area riservata al seguente indirizzo: <https://portal.namirialtsp.com>  
Cliccare su "Non ricordo il nome utente" e seguire le indicazioni riportate.  
Se il problema persiste contattare il supporto tecnico per e-mail all'indirizzo: [supportoca@namirial.com](mailto:supportoca@namirial.com) indicando nell'OGGETTO: **RECUPERO USERNAME FIRMA REMOTA** – Codice fiscale.

### ATTENZIONE – SMARTCARD NON PRESENTE

Il Messaggio d'errore **Smartcard non presente** viene mostrato all'utente prima di inserire i parametri della firma remota solamente se il servizio NamirialSignEngine non è stato abilitato, quindi il software Firmacerta si aspetta di recuperare i certificati da un dispositivo fisico non presente.

Per risolvere questa problematica, assicurarsi che il servizio NamirialSignEngine risulti abilitato.

Dal software **Firmacerta** > **Utilità** > **Opzioni Generali** > **Servizi Web** > **click sul tasto Abilita/Disabilita**.

Se l'icona del servizio diventa colorata significa che il servizio è attivo.

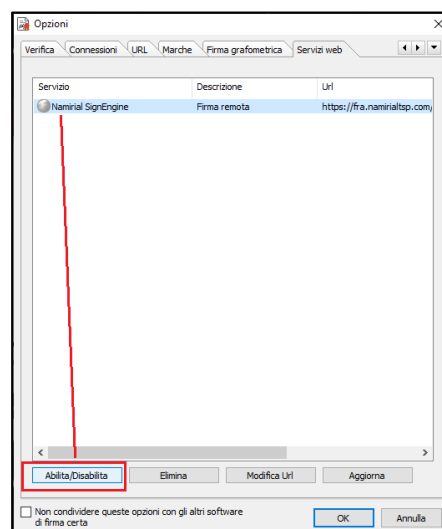
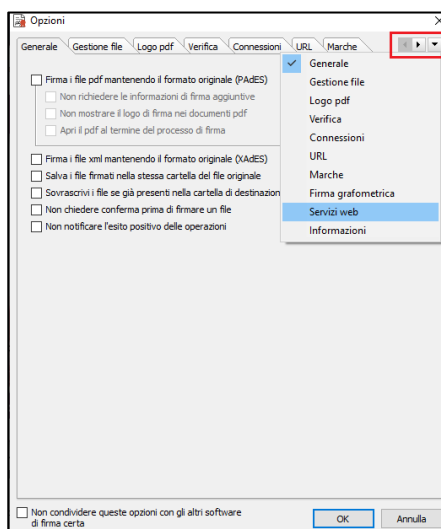


Figura 120 - Servizi Web

## 12.4 SELEZIONE DISPOSITIVO REMOTO

Cliccare sulla figura nel riquadro rosso, per selezionare il vostro *Dispositivo virtuale* di Firma, in alternativa potete inserirlo manualmente, recuperando il codice dall'email di emissione certificato.

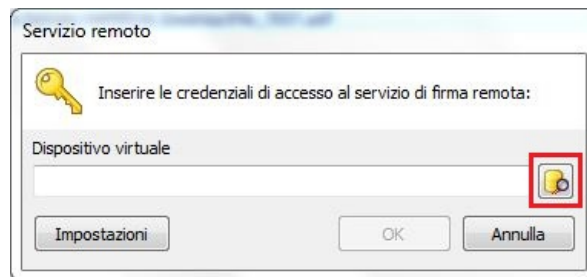


Figura 121 - inserimento dispositivo remoto

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

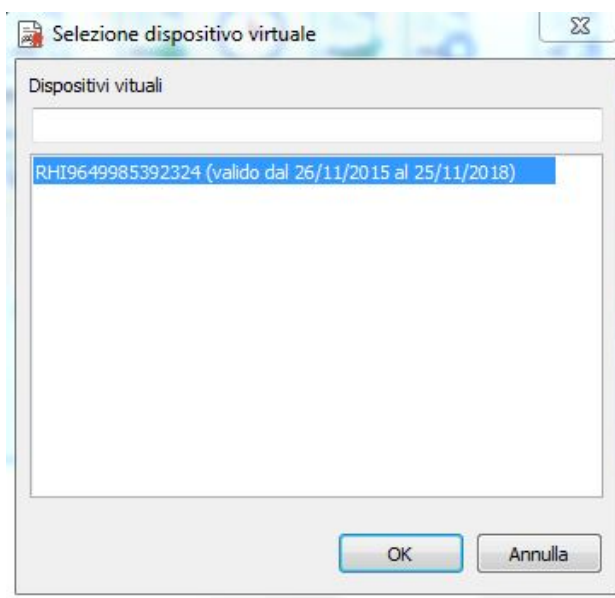


Figura 122 - selezione dispositivo virtuale

Inserito il dispositivo virtuale confermare cliccando su *OK*.

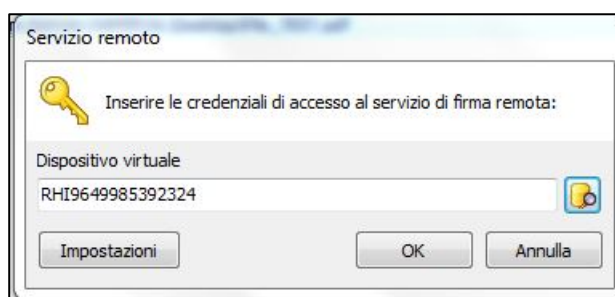


Figura 123 - esempio numero dispositivo inserito



## 12.5 FIRMA PADES:

Solo se l'utente ha selezionato il formato PAdES, il programma mostrerà a video le seguenti schermate aggiuntive in successione.

### ATTENZIONE:

Le Informazioni di firma è un'operazione facoltativa.

### NOTA:

Cliccando sulla casella *Non richiedere più* questa schermata non sarà più proposta.

Questa opzione può essere riattivata da:  
Utilità > Opzioni Generali > deselezionare: Non richiedere le informazioni di firma aggiuntive.

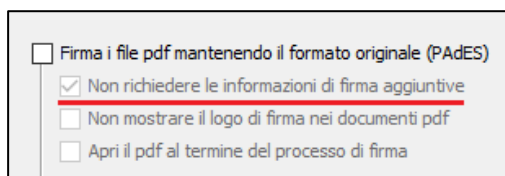


Figura 124 - opzioni generali - pdf

Informazioni di firma (test.pdf)

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

Motivo di firma

Località

Informazioni di contatto

☐ Non richiedere più

OK Annulla

Figura 125 - informazioni di firma

In questa schermata viene mostrato a video il documento PDF caricato e permette di scegliere dove posizionare il logo pdf con il marcatore verde. (vedi immagine).

Al termine della procedura sarà richiesto un messaggio di conferma.

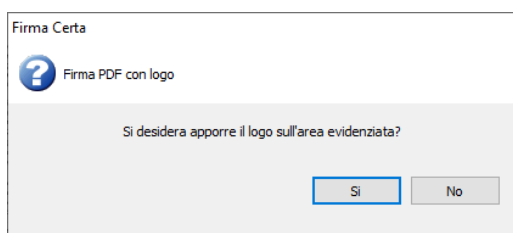


Figura 126 - conferma area evidenziata

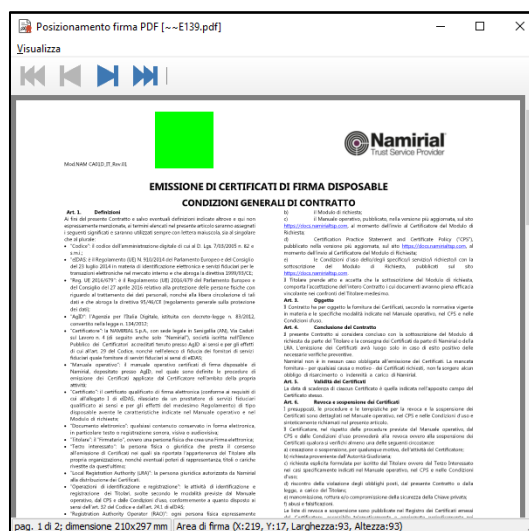


Figura 127 -posizionamento marcatore

### NOTA:

l'utente deve essere in possesso di Adobe Reader aggiornato;  
il file non deve essere protetto altrimenti non permetterà di visualizzare il contenuto.

**ATTENZIONE:**

La personalizzazione del logo è un'operazione facoltativa.

**NOTA:**

Cliccando sulla casella *Non richiedere più* questa schermata non sarà più proposta se non necessaria. Questa opzione può essere riattivata da: Utilità > Opzioni Firma > logo PDF > deselezionare: Non richiedere la personalizzazione del testo.

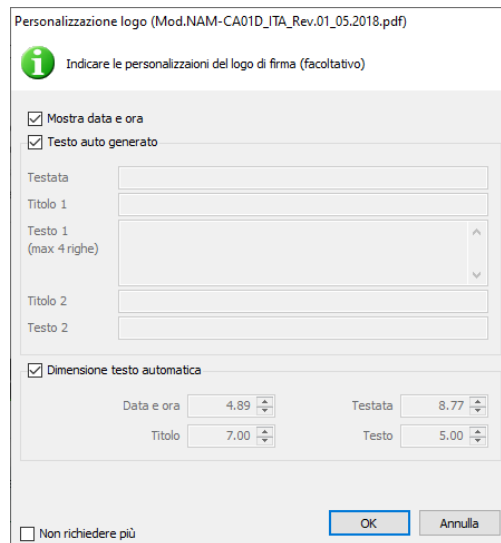


Figura 128 - personalizzazione logo

## 12.6 SELEZIONA LA PROCEDURA DI FIRMA

- [Firmare un file con OTP SMS](#)
- [Firmare un file con OTP VIRTUALE](#)
- [Firmare un file con OTP FISICO](#)

## 12.6.1 PROCEDURA CON OTP SMS

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

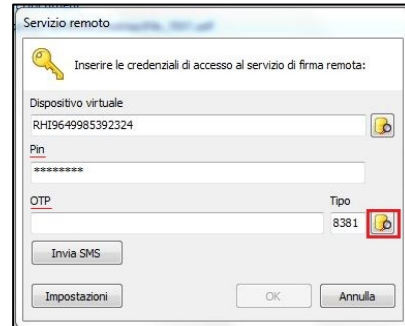


Figura 129 - inserimento PIN OTP SMS

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

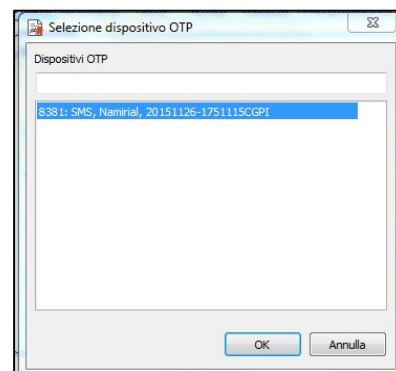


Figura 130 - selezione OTP [OTP SMS]

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

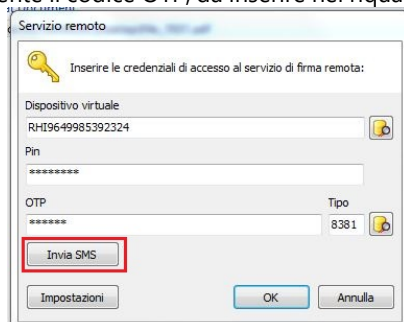


Figura 131 -invio OTP SMS

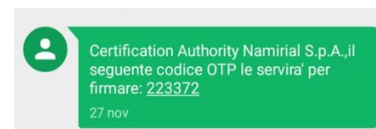


Figura 132 - esempio otp SMS

Alla fine della procedura comparirà il seguente messaggio di Conferma.

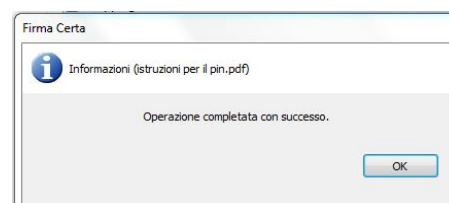


Figura 133 - operazione completata otp sms

## 12.6.2 PROCEDURA CON NAMIRIAL OTP

Prima di procedere con la firma assicurarsi di aver attivato l'OTP Virtuale.

Per i possessori dell'app Namirial OTP versione iOS - 3.3.0 e Android - 1.6.5.1: [Configurazione OTP Virtuale](#).

Per i possessori dell'app Namirial OTP versione iOS - 4.2.2.0 e Android - 4.2.0.5 o versioni successive:

- **iOS:** [Attivazione OTP iOS](#)
- **Android:** [Attivazione OTP Android](#)

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**.

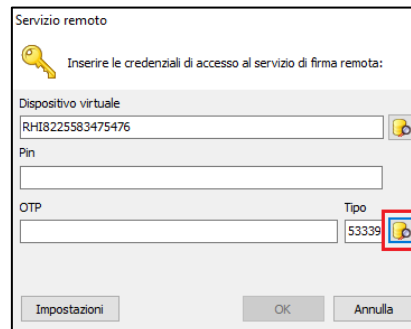


Figura 134 - inserimento PIN OTP virtuale

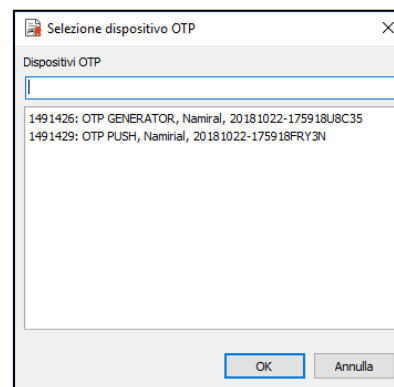


Figura 135 - selezione OTP virtuale

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

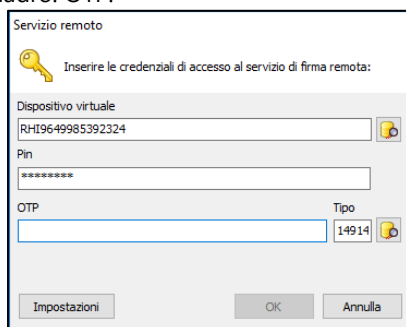


Figura 136 -inserimento otp virtuale



Figura 137 - esempio OTP virtuale

Alla fine della procedura comparirà il seguente messaggio di Conferma.

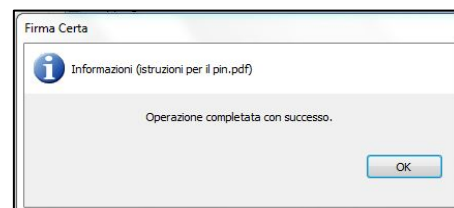


Figura 138 - operazione completata otp sms

### 12.6.3 PROCEDURA CON OTP FISICO

**NOTA:** Prima di procedere con la firma assicurarsi di aver attivato l'OTP Fisico vedi: [Configurazione OTP FISICO](#).

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

Figura 139- inserimento PIN OTP fisico

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 140 - selezione OTP fisico

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

Figura 141 -inserimento otp fisico



Figura 142 - esempio otp fisico

Alla fine della procedura comparirà il seguente messaggio di Conferma.

Figura 143 - operazione completata otp sms



## 13 AUTENTICAZIONE WEB

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



## 14 APPENDICE J: BIT4ID – LINUX

Scaricare e installare il Driver Manager Bit4id PKI Manager, al seguente link:

### File .deb:

- Versione **64bit**: [ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id\\_middleware/Linux/deb/libbit4xpki-bit4id-user-amd64.1.4.10-464.deb](ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id_middleware/Linux/deb/libbit4xpki-bit4id-user-amd64.1.4.10-464.deb)
- Versione **32bit**: [ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id\\_middleware/Linux/deb/libbit4xpki-bit4id-user-i386.1.4.10-464.deb](ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id_middleware/Linux/deb/libbit4xpki-bit4id-user-i386.1.4.10-464.deb)

### File .rpm:

- Versione **64bit**: [ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id\\_middleware/Linux/rpm/libbit4xpki-1.4.10-464-bit4id-user.x86\\_64.rpm](ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id_middleware/Linux/rpm/libbit4xpki-1.4.10-464-bit4id-user.x86_64.rpm)
- Versione **32bit**: [ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id\\_middleware/Linux/rpm/libbit4xpki-1.4.10-464-bit4id-user.i386.rpm](ftp://dwnfirmacerta@ftpdwn.firmacerta.it/bit4id_middleware/Linux/rpm/libbit4xpki-1.4.10-464-bit4id-user.i386.rpm)

Aprire **Mostra Applicazioni** e cercare il software **Bit4id PKI Manager**.

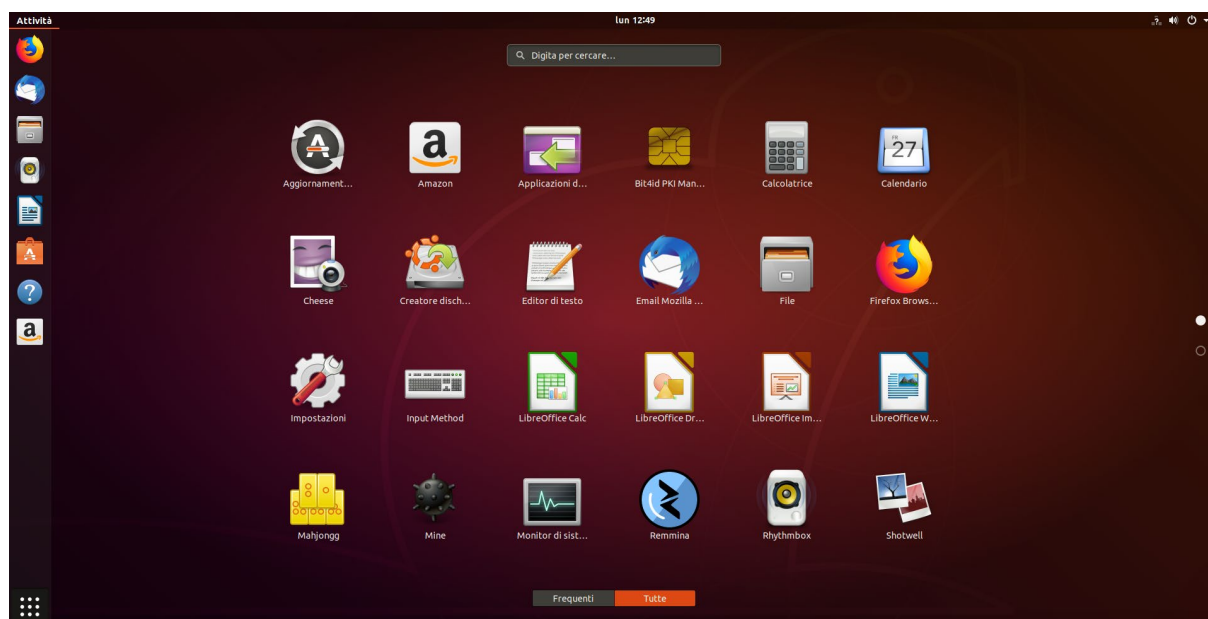


Figura 144 - Dashboard Linux

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

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

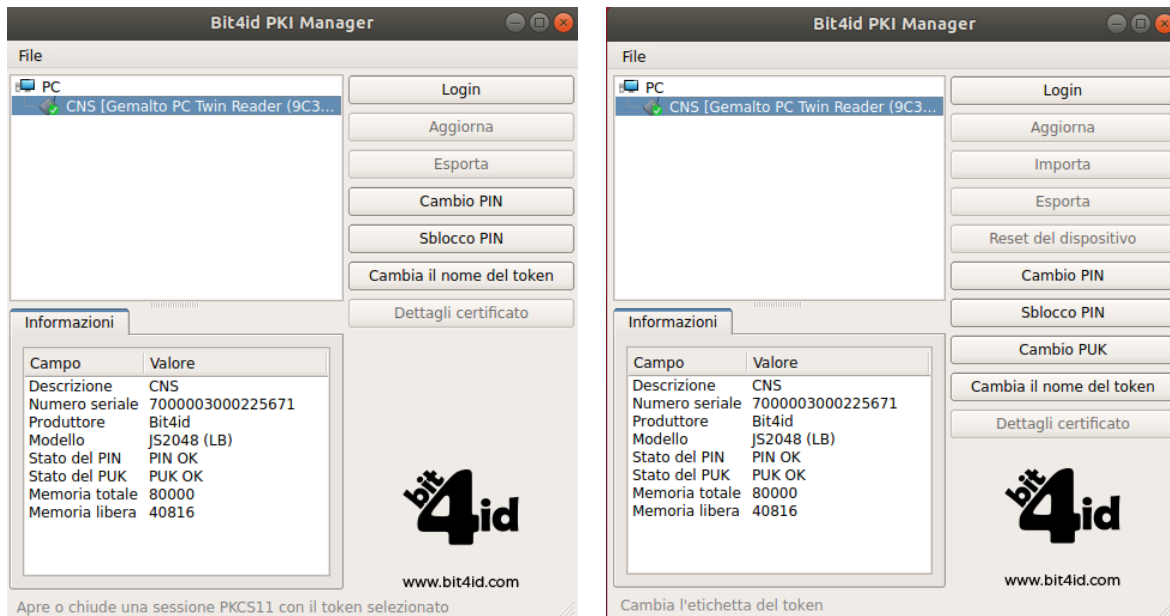


Figura 145 - Funzione avanzate PIN Manager

## 14.1 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 è possibile modificare il PIN dalla propria [Area Privata Utente](#) nella sezione > Utente > Firma digitale > Gestione.



Figura 146 - Funzione Cambio PIN

## 14.2 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 147 - funzione di Sblocco PIN

## 14.3 CAMBIO PUK

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

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

**ATTENZIONE:**

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

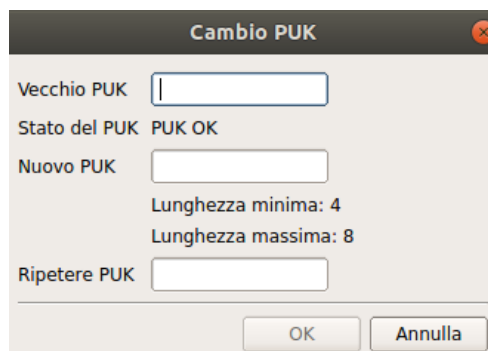


Figura 148 - funzione di Cambio PUK



## RIFERIMENTI

| NUMERO | DESCRIZIONE                    |
|--------|--------------------------------|
| [I]    | Guida Utente: Windows e Mac OS |
| [II]   | <...>                          |



## INDICE DELLE FIGURE

|  |    |
|--|----|
| Figura 1 - installazione guidata firmacerta.....               | 11 |
| Figura 2 - seleziona cartella di destinazione.....             | 12 |
| Figura 3 - conferma d'installazione .....                      | 12 |
| Figura 4 - messaggio di avvenuta installazione .....           | 13 |
| Figura 5 - interfaccia grafica firmacerta.....                 | 14 |
| Figura 6 - sottomenù di firma.....                             | 15 |
| Figura 7 - Introduzione funzione di firma.....                 | 15 |
| Figura 8 - Introduzione funzione di controfirma .....          | 15 |
| Figura 9 - Introduzione funzione di firma e Marca.....         | 16 |
| Figura 10 - Introduzione funzione di verifica .....            | 16 |
| Figura 11 - Introduzione funzione di Marca .....               | 16 |
| Figura 12 - Pannello di Gestione Dispositivo .....             | 17 |
| Figura 13 - Funzione Cambio PIN .....                          | 17 |
| Figura 14 - funzione di Sblocco PIN.....                       | 18 |
| Figura 15 - funzione di Cambio PUK.....                        | 18 |
| Figura 16 - funzione di visualizza certificati .....           | 19 |
| Figura 17 - funzione di verifica dispositivo .....             | 20 |
| Figura 18 - Introduzione funzione di rinnovo certificati ..... | 20 |
| Figura 19 - Introduzione funzioni: firma grafometrica.....     | 21 |
| Figura 20 - Introduzione funzione di firma grafometrica.....   | 21 |
| Figura 21 - Template di firma.....                             | 21 |
| Figura 22 - Marcatore nel template.....                        | 22 |
| Figura 23: Sfondo Firma .....                                  | 23 |



|   |    |
|---|----|
| Figura 24 - Generale Proprietà di Firma .....               | 23 |
| Figura 25 - Chiavi di ricerca .....                         | 23 |
| Figura 26 - Pannello di Utilità.....                        | 24 |
| Figura 27 - Introduzione a FirmaCerta Protect .....         | 24 |
| Figura 28 - Pannello delle opzioni generali .....           | 25 |
| Figura 29 - Opzioni: Gestione File .....                    | 26 |
| Figura 30 - Opzioni:URL.....                                | 26 |
| Figura 31 - Opzioni Servizi Web.....                        | 26 |
| Figura 32 - Opzioni: informazioni.....                      | 27 |
| Figura 33 - Opzioni: Configurazione del Proxy .....         | 27 |
| Figura 34 - Pannello di Opzioni Firma.....                  | 28 |
| Figura 35 - Opzioni: Logo PDF.....                          | 28 |
| Figura 36 - Opzioni: Opzioni di Verifica.....               | 29 |
| Figura 37 - Pannello Opzioni firma Grafometrica.....        | 29 |
| Figura 38 - Opzioni Firma grafometrica .....                | 30 |
| Figura 39 - Opzioni Grafometrica: Attivazione Licenza ..... | 31 |
| Figura 40 - Opzioni Grafometrica: informativa Privacy ..... | 31 |
| Figura 41 - Opzioni Marca temporale .....                   | 32 |
| Figura 42 - Pannello: Help .....                            | 32 |
| Figura 43 - Pannello di Firma .....                         | 33 |
| Figura 44 - Scelta formato di firma Cades-Xades.....        | 33 |
| Figura 45 - Selezione cartella di destinazione.....         | 34 |
| Figura 46 - Conferma di firma.....                          | 34 |
| Figura 47 - Inserimento PIN.....                            | 34 |
| Figura 48 - Operazione completata.....                      | 34 |



|  |    |
|--|----|
| Figura 49 - Scelta formato di firma Cades-Pades.....               | 35 |
| Figura 50 - Selezione cartella di destinazione.....                | 35 |
| Figura 51 - Conferma di firma.....                                 | 35 |
| Figura 52 - Inserimento PIN.....                                   | 36 |
| Figura 53 - informazioni di firma.....                             | 36 |
| Figura 54 - Posizionamento del marcatore di firma.....             | 36 |
| Figura 55 - Conferma di posizionamento .....                       | 36 |
| Figura 56 - Personalizzazione del logo .....                       | 37 |
| Figura 57 - Operazione Completata .....                            | 37 |
| Figura 58 - Pannello di Controfirma.....                           | 38 |
| Figura 59 - Selezione cartella di destinazione.....                | 38 |
| Figura 60 - Conferma di sovrascrizione .....                       | 38 |
| Figura 61 - Schermata di esempio: verifica file controfirmato..... | 39 |
| Figura 62 - Conferma di firma.....                                 | 39 |
| Figura 63 - Inserimento Pin.....                                   | 39 |
| Figura 64 - Operazione Completata .....                            | 39 |
| Figura 65 - Pannello di Utilità.....                               | 40 |
| Figura 66 - Opzioni Configurazione Marche .....                    | 40 |
| Figura 67 - Controllo Marche temporali.....                        | 41 |
| Figura 68 - Selezione cartella di destinazione.....                | 41 |
| Figura 69 - Conferma di firma.....                                 | 41 |
| Figura 70 - Inserimento del PIN .....                              | 42 |
| Figura 71 - Conferma credenziali Marche.....                       | 42 |
| Figura 72 - Operazione Completata .....                            | 42 |
| Figura 73 - Pannello di Firma .....                                | 43 |



|   |    |
|---|----|
| Figura 74 - Selezione del formato di firma Cades.....       | 43 |
| Figura 75 - Pannello FirmaCerta .....                       | 44 |
| Figura 76 - Scelta formato marca temporale.....             | 44 |
| Figura 77 - Scelta cartella di destinazione .....           | 44 |
| Figura 78 - conferma dati di configurazione Marche .....    | 45 |
| Figura 79 - Operazione Completata.....                      | 45 |
| Figura 80 - Esempio: file marcato temporalmente.....        | 45 |
| Figura 81 - Pannello di FirmaCerta .....                    | 46 |
| Figura 82 - Separazione marca temporale .....               | 46 |
| Figura 83 - Selezionare il formato di marca.....            | 46 |
| Figura 84 - Esempio di file marcati .....                   | 46 |
| Figura 85 - Pannello di Firmacerta .....                    | 47 |
| Figura 86 - Schermata di verifica .....                     | 47 |
| Figura 87 - Schermata di Esito .....                        | 48 |
| Figura 88 - Schermata di Dettagli .....                     | 48 |
| Figura 89 - Impostazioni di Verifica.....                   | 49 |
| Figura 90 - schermata per visualizzare il file firmato..... | 49 |
| Figura 91 - Schermata di Verifica con esempio.....          | 51 |
| Figura 92 - Accesso Negato.....                             | 51 |
| Figura 93 - Configurazione per firma Pades.....             | 54 |
| Figura 94 - Configurazione per firma Cades.....             | 54 |
| Figura 95 - Schermata opzioni Generale .....                | 55 |
| Figura 96 - Schermata opzioni Marche.....                   | 55 |
| Figura 97 - Schermata formato Marche.....                   | 55 |
| Figura 98 - Schermata opzioni generali.....                 | 56 |



|   |    |
|---|----|
| Figura 99 - Schermata opzioni Marche.....                     | 56 |
| Figura 100 - Inserimento PIN .....                            | 56 |
| Figura 101 - Schermata Clausole Vessatorie .....              | 57 |
| Figura 102 - Configurazione Proxy .....                       | 57 |
| Figura 103 - Schermata Clausole Vessatorie .....              | 58 |
| Figura 104 - Schermata Inserimento PIN .....                  | 58 |
| Figura 105 - Rinnovo Certificati.....                         | 59 |
| Figura 106 - Messaggio di visualizzazione del contratto ..... | 59 |
| Figura 107 - Conferma apposizione della firma.....            | 59 |
| Figura 108 - Rinnovo completato con successo .....            | 59 |
| Figura 109: Area Privata Namirial .....                       | 60 |
| Figura 110: Dashboard Area Privata.....                       | 60 |
| Figura 111: Gestione Certificati .....                        | 61 |
| Figura 112: Processo di firma e rinnovo .....                 | 61 |
| Figura 113 - come firmare.....                                | 62 |
| Figura 114 - schermata file pdf .....                         | 62 |
| Figura 115 - schermata file xml.....                          | 63 |
| Figura 116 - selezione cartella .....                         | 63 |
| Figura 117 - conferma processo .....                          | 63 |
| Figura 118 - inserimento user parte 1 .....                   | 64 |
| Figura 119 - inserimento user parte 2.....                    | 64 |
| Figura 120 - Servizi Web .....                                | 64 |
| Figura 121 - inserimento dispositivo remoto .....             | 65 |
| Figura 122 - selezione dispositivo virtuale .....             | 65 |
| Figura 123 - esempio numero dispositivo inserito .....        | 65 |



|  |    |
|--|----|
| Figura 124 - opzioni geenrali - pdf.....         | 66 |
| Figura 125 - informazioni di firma .....         | 66 |
| Figura 126 - conferma area evidenziata .....     | 66 |
| Figura 127 -posizionamento marcatore .....       | 66 |
| Figura 128 - personalizzazione logo .....        | 67 |
| Figura 129 - inserimento PIN OTP SMS.....        | 68 |
| Figura 130 - selezione OTP [OTP SMS].....        | 68 |
| Figura 131 -invio OTP SMS .....                  | 68 |
| Figura 132 - esempio otp SMS.....                | 68 |
| Figura 133 - operazione completata otp sms ..... | 68 |
| Figura 134 - inserimento PIN OTP virtuale.....   | 69 |
| Figura 135 - selezione OTP virtuale.....         | 69 |
| Figura 136 -inserimento otp virtuale .....       | 69 |
| Figura 137 - esempio OTP virtuale .....          | 69 |
| Figura 138 - operazione completata otp sms ..... | 69 |
| Figura 139- inserimento PIN OTP fisico.....      | 70 |
| Figura 140 - selezione OTP fisico .....          | 70 |
| Figura 141 -inserimento otp fisico.....          | 70 |
| Figura 142 - esempio otp fisico.....             | 70 |
| Figura 143 - operazione completata otp sms ..... | 70 |
| Figura 143 - Dashboard Linux.....                | 72 |
| Figura 144 - Funzione avanzate PIN Manager.....  | 73 |
| Figura 145 - Funzione Cambio PIN.....            | 73 |
| Figura 146 - funzione di Sblocco PIN .....       | 74 |
| Figura 147 - funzione di Cambio PUK.....         | 74 |



– Questa pagina è lasciata intenzionalmente in bianco –