CAMERE DI COMMERCIO
D'ITALIA

firma4ng

Manuale Utente

v.6 (ultimo aggiornamento 11/10/2022)

Powered by Bit4id

InfoCamere

Sommario

1. INTRODUZIONE

Il presente manuale d'uso descrive le principali funzionalità dell'applicazione di firma digitale ***firma4ng***. In particolare, il documento si propone di supportare l'utente nello svolgimento delle seguenti operazioni:

- Attivazione dispositivi
- Apposizione di firme digitali in formato .P7M
- Apposizione di firme digitali in formato .PDF
- Apposizione di firme digitali in formato .XML
- Apposizione di firme digitali in formato PAdES LTV (Long Term Validation)
- Apposizione di marche temporali
- Verifica di firme digitali in formato .P7M
- Verifica di firme digitali in formato .PDF
- Verifica di firme digitali in formato .XML
- Verifica di marche temporali
- Cifratura e decifratura di file
- Gestione PIN e PUK del dispositivo crittografico (smart card o token USB)
- Consultazione e sincronizzazione dello Storico

2. CARATTERISTICHE DEL SOFTWARE

2.1 Distribuzioni disponibili e requisiti

L'applicazione *firma4ng* viene distribuita nelle seguenti versioni:

- *firma4ng* per Windows 64 bit, installazione disponibile per ambienti desktop Windows 10 e Windows 11
- *firma4ng* per Mac OS X, installazione disponibile per ambienti desktop Mac OS X(11.X.X e 12.X.X);
- *firma4ng* per Linux 64, distribuito come archivio tar.gz per ambienti desktop Linux (Ubuntu 22.04 LTS);

Uso dal PC tramite USB

Requisiti HW

- Porta USB disponibile
- Connettività Internet

Requisiti SW

- MS Windows 10| 11
- Mac OSx 11.X.X (Big Sur) MacOS X 12.X.X (Monterey)
- Linux 22.04 LTS

Uso dal PC tramite Bluetooth

Requisiti HW

- Bluetooth 4.1 o superiore

Requisiti SW

- MS Windows 10 | 11
- Mac OSx 11.X.X (Big Sur) MacOS X 12.X.X (Monterey)

2.2 Requisiti di sistema

Prima di utilizzare *firma4ng*, a garanzia del corretto funzionamento dell'applicazione, è bene verificare:

- La disponibilità di connessione Internet;
- La possibilità di instaurare connessioni HTTP, HTTPS e LDAP.

Inoltre, per una corretta visualizzazione, si suggerisce di impostare una risoluzione dello schermo pari almeno a 1024x768.

2.3 Procedura di installazione

Windows

Per installare l'applicazione su sistemi operativi Windows (a 64 bit), avviare il programma di installazione (con estensione "**.exe**") con doppio click e seguirne tutti i passi.

Occorre accettare, per presa visione, le condizioni ed i termini di utilizzo per poter procedere con l'installazione di firma4ng.

Mac OS X

Per installare l'applicazione su sistemi operativi Mac OS X avviare il programma di installazione individuato dall'estensione "**.pkg**" e seguirne tutti i passi.

Occorre accettare, per presa visione, le condizioni ed i termini di utilizzo per poter procedere con l'installazione di firma4ng.

Linux

Per installare l'applicazione su sistemi operativi Linux (a 64 bit) occorre estrarre il contenuto dell'archivio individuato dal file con estensione "**.tar.gz**" nella home dell'utente ed eseguire lo script setup.run con opzione i ("*setup.run –i*") e seguire le opzioni a video.

2.4 Aggiornamento automatico

Il software *firma4ng* è dotato della funzionalità di aggiornamento automatico: ad ogni avvio dell'applicativo viene effettuato un controllo sulla disponibilità di nuove versioni e, a seguito dell'autorizzazione da parte dell'utente, viene effettuato l'aggiornamento.

Tale funzionalità è attiva se il PC è collegato ad Internet.

3. INIZIO

Una volta completata l'installazione, è sufficiente fare doppio click sull'icona di avvio per aprire il programma di firma digitale. Apparirà sullo schermo il menu principale di *firma4ng* (Figura 1), da cui accedere alle diverse funzioni dell'applicazione.

Figura 1

Il menu contiene le seguenti voci:

- Firma
- Verifica
- Marca Temporale
- Gestione Dispositivo
- Applicazioni
- Gestione DigitalDNA
- Cassetto digitale dell'imprenditore

ATTENZIONE

Prima di avviare una o più operazioni, verificare di aver collegato correttamente il token DigitalDNA al computer in uso. Il dispositivo può essere utilizzato in due modalità:

USB: collegando il token alla porta USB del computer, il software *firma4ng* riconoscerà automaticamente il dispositivo DigitalDNA e i certificati in esso contenuti.

Bluetooth: per utilizzare il token via Bluetooth, è necessario completare prima l'associazione descritta nel capitolo dedicato a "Gestione DigitalDNA".

3.1 Attivazione

Il paragrafo è dedicato agli utenti che hanno richiesto il dispositivo (smart card o Token DigitalDNA) tramite piattaforma id.infocamere.it e ricevuto a domicilio.

L'attivazione del dispositivo è una procedura obbligatoria e deve essere effettuata solo una volta alla ricezione del dispositivo e se il dispositivo non è stato mai attivato tramite altra modalità (es. via app per il token DigitalDNA).

Tramite la procedura di invio del dispositivo inattivo e conseguente attivazione, il Titolare ha la certezza di essere l'utilizzatore esclusivo dei certificati, avendo accesso esclusivo ai relativi codici di attivazione, inviati telematicamente su contatto verificato.

La procedura di attivazione del dispositivo è effettuabile da PC tramite software di firma Firma4NG, disponibile per Smart Card e Token Digital DNA, e da smartphone o tablet tramite app DigitalDNA IC, disponibile esclusivamente per il Token Digital DNA.

La procedura di attivazione è un'attività propedeutica all'utilizzo dei certificati sul dispositivo.

3.1.1 Acquisto online: emissione certificati

A seguito dell'emissione dei certificati CNS e firma digitale, vengono inviate due e-mail sull'indirizzo di posta elettronica del titolare: un'e-mail con le istruzioni per procedere all'attivazione del dispositivo ed una con i segreti, con oggetto **Nuova richiesta CNS: riferimenti per l'uso.**

All'interno del testo email, cliccando su **Vai al PDF**, si accede alle credenziali per l'attivazione e l'utilizzo del dispositivo. L'accesso al contenuto è protetto dalla pass-phrase scelta in fase di richiesta.

Le informazioni contenute nel pdf cifrato sono le seguenti (Figura 2):

- **SERIALE DISPOSITIVO** nel formato numerico, che identifica il dispositivo fisico in cui sono contenuti i certificati
- **ID SCRATCH-CARD** necessario per la gestione del ciclo di vita dei certificati, secondo le indicazioni riportate sul portale id.infocamere.it
- **PUK** codice segreto necessario per l'attivazione del dispositivo.
- **CODICE DI EMERGENZA** necessario per la gestione del ciclo di vita del certificato, secondo le indicazioni riportate sul portale id.infocamere.it

Gentile Signora, Egregio Signore,

Le comunichiamo i CODICI per l'utilizzo dei certificati collegati alla Sua Carta Nazionale dei Servizi.

SERIALE: 7420063000277611

ID SCRATCH CARD: 1000361657

PUK: 22222222

CODICE di EMERGENZA: 0000000000

Il codice PUK è necessario per l'attivazione del dispositivo ricevuto. Durante l'attivazione è richiesta la scelta del codice PIN.

Il PIN è indispensabile per firmare digitalmente un documento. Dopo tre tentativi falliti consecutivi di inserimento del PIN, il dispositivo si blocca. Per sbloccarlo, è necessario utilizzare il codice PUK. Tre tentativi falliti consecutivi di inserimento del PUK, bloccano il dispositivo definitivamente.

Il SERIALE identifica il dispositivo.

Il codice ID_SCRATCH e il CODICE UTENTE di EMERGENZA potranno essere utilizzati nel caso fosse necessario sospendere il servizio di certificazione, secondo le indicazioni riportate sul sito id.infocamere.it.

I CODICI sono strettamente riservati e personali. Le raccomandiamo di conservarli separatamente dal dispositivo di firma e di non comunicarli a nessuno.

Figura 2

3.1.2 Requisiti per l'attivazione

Per procedere all'attivazione della smart card è necessario avere a disposizione:

- **Lettore smart card** compatibile collegato al PC;
- **Dispositivo da attivare** ricevuto a domicilio;
- PDF con i **segreti** (figura 2);
- **PC** connesso ad internet;
- Software **Firma4NG** installato sulla postazione.

Per procedere all'attivazione del token Digital DNA è necessario avere a disposizione:

- **Porta USB** a cui collegare il token;
- **Dispositivo da attivare** ricevuto a domicilio;
- PDF con i **segreti** (figura 2);
- **PC** connesso ad internet;

- Software **Firma4NG** installato sulla postazione.

3.2 Procedura di attivazione

Inserire la smart card nel lettore o il token Digital DNA nella porta USB, assicurandosi che il dispositivo da attivare sia l'unico collegato al PC, e avviare il software Firma4NG (Figura 1).

Attendere la verifica degli aggiornamenti e sullo stato di attivazione del dispositivo. Se il software rileva un dispositivo da attivare, viene mostrato a video l'alert di attivazione (Figura 3).

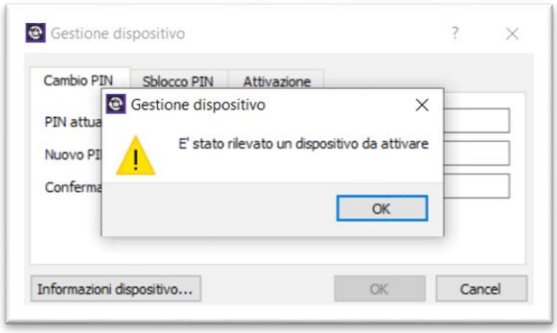


Figura 3

Cliccando su **OK** è possibile accedere alla finestra di attivazione (Figura 4), dove viene richiesto di inserire il PUK (disponibile nel PDF cifrato – Figura 1) e la scelta e conferma del nuovo PIN.

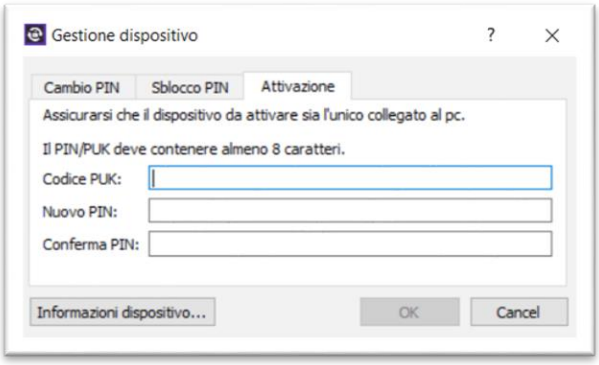


Figura 4

Il PIN è il codice segreto che consente di accedere alla chiave privata del dispositivo durante le operazioni di sottoscrizione dei documenti e accesso ai siti web. Il codice PIN e gli altri segreti devono essere conservati separatamente dal dispositivo di firma e non vanno comunicati a terzi.

Una volta scelto il PIN, cliccare su **OK** per concludere l'operazione (Figura 5).

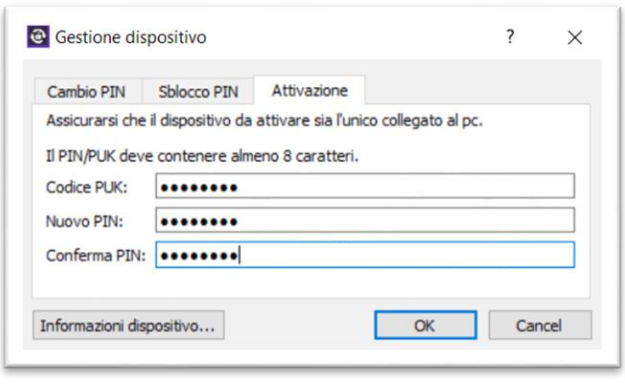


Figura 5

ATTENZIONE: 3 tentativi consecutivi di inserimento PUK errato bloccano definitivamente il dispositivo.

Terminata la fase di attivazione del dispositivo, è possibile procedere alle operazioni di firma e autenticazione.

4. FIRMA DIGITALE

La funzione **"Firma digitale"** permette di firmare digitalmente uno o più documenti con certificati digitali.

4.1 Firma con DigitalDNA

Se si è in possesso di un dispositivo DigitalDNA seguire la procedura di firma illustrata nelle fasi di seguito.

FASE 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Firma attraverso una delle seguenti modalità:

- Selezionando e trascinando uno o più documenti sul pulsante "Firma" presente nel menu principale (drag&drop);

- Cliccando sul pulsante "Firma" presente nel menu principale e selezionando uno o più documenti da firmare dalla finestra di navigazione del PC (Figura 6).

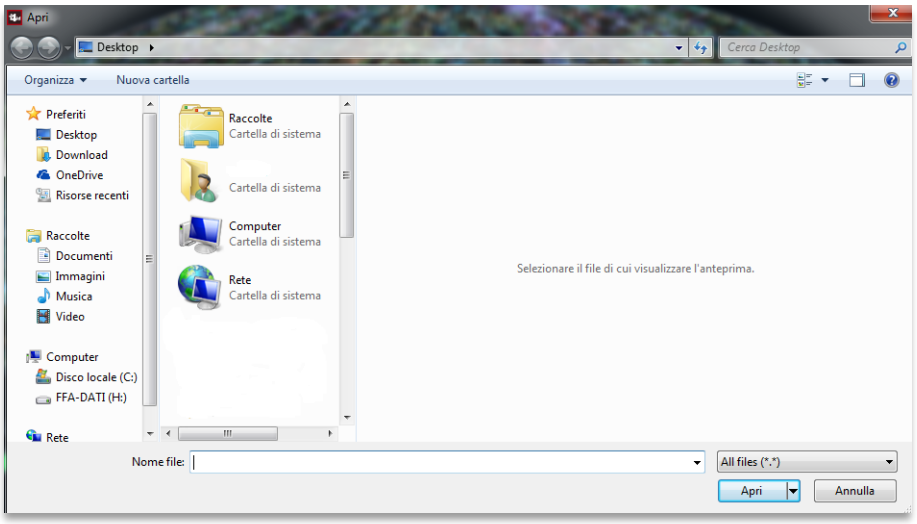


Figura 6

FASE 2

Attendere il caricamento dei certificati (Figura 7).

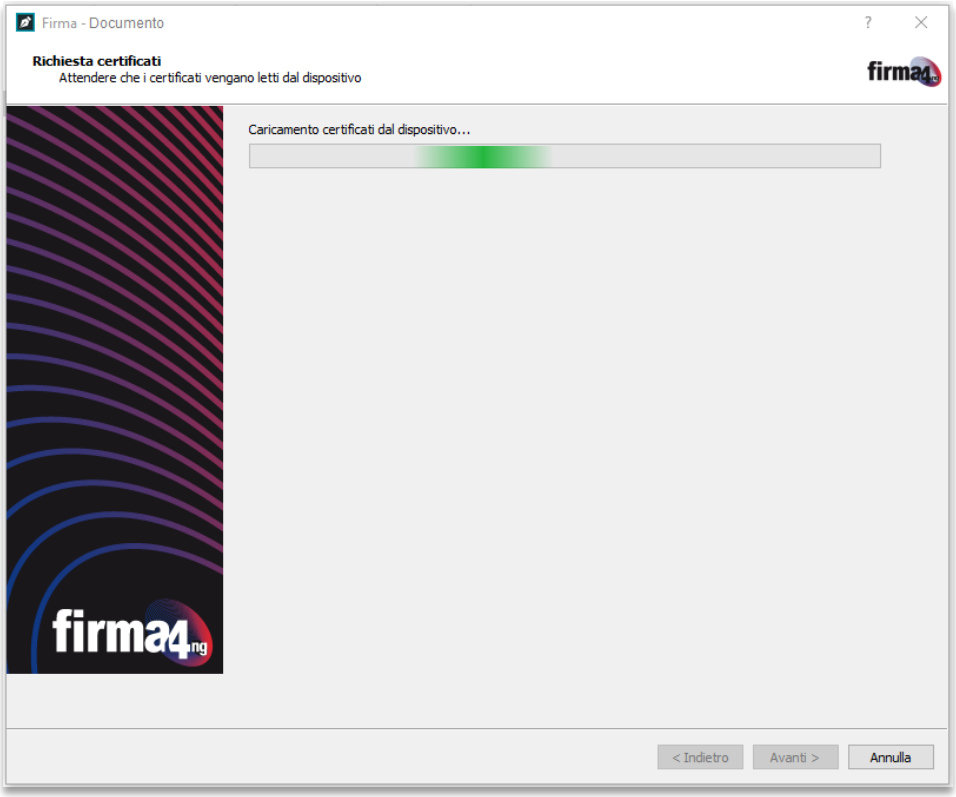


Figura 7

FASE 3 (Firma in formato P7M o XML)

Al termine del caricamento dei certificati, si apre la finestra di configurazione in cui inserire i parametri e le preferenze da applicare alla firma che si sta effettuando (Figura 8):

Seleziona il certificato: risulterà automaticamente selezionato il certificato di firma digitale a validità legale (o di "non ripudio") identificato da Nome e Cognome dell'intestatario. Per utilizzare un certificato diverso da quello preimpostato, selezionare una voce dal menu a tendina.

Inserisci il PIN: Inserire il PIN riportato sulla Scratch card virtuale ricevuta via email o sulla cartellina fisica consegnata in fase di rilascio.

Salva come: selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "...". Lasciando invariato questo campo, il file firmato verrà salvato automaticamente nella stessa cartella in cui si trova il file originale non firmato.

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Cifra il documento al termine della firma
Distruggi il documento al termine della firma

Tipologia di firma: selezionare dal menu a tendina la tipologia di firma che si vuole apporre al documento. I formati di firma disponibili sono:

- *Busta crittografica P7M (CAdES)* - formato valido per qualunque tipo di documento;
- *Documento XML* – formato valido per qualunque tipo di documento (eccetto quando l'operazione di firma viene lanciata dai pulsanti "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica");

Richiedi Timestamp*: attivare l'opzione per aggiungere una marca temporale, ovvero per associare una data e un'ora precisa alla firma che si sta effettuando. Selezionare dal menu a tendina il formato con cui si vuole apporre la marca digitale al documento (formato .M7M, .TSD o .P7M).

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Codifica in Base64
Separa la firma dal documento (firma "detached")

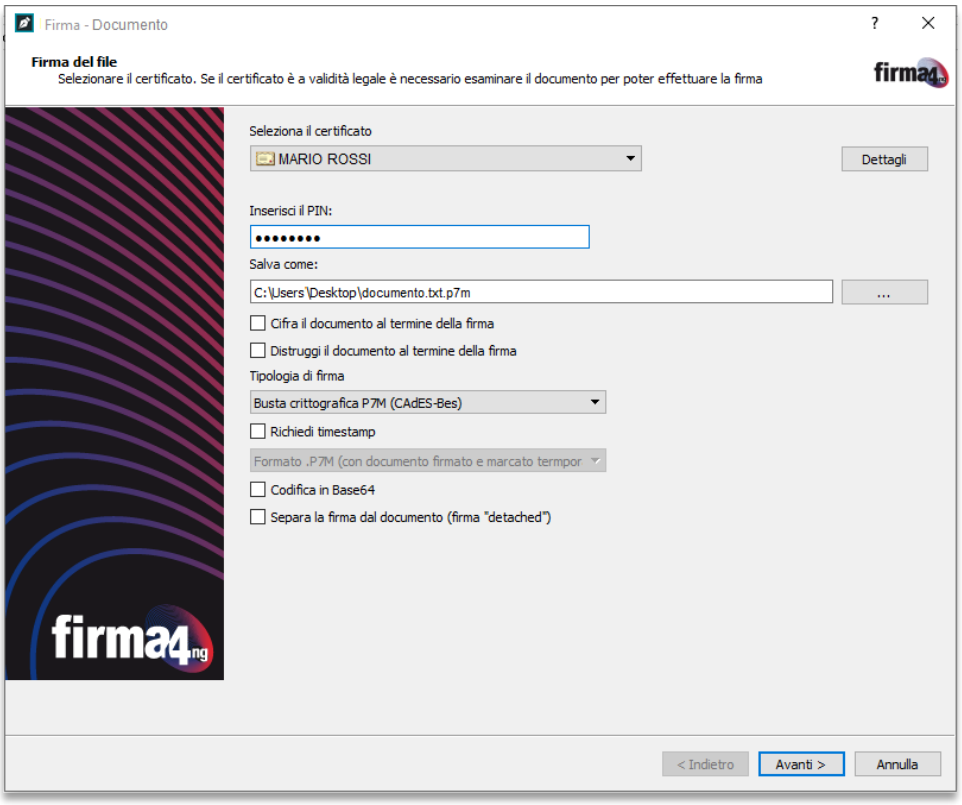


Figura 8

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

FASE 3 (Firma in formato PDF)

Questa configurazione riguarda solo la firma PDF. Si tratta infatti di un formato valido solo nel caso in cui il documento da firmare sia un file PDF.
Al termine del caricamento dei certificati (Figura 7), appare la finestra di configurazione in cui inserire parametri e preferenze da applicare alla firma che si sta effettuando (Figura 9):

Seleziona il certificato: risulterà automaticamente selezionato il certificato di firma digitale a validità legale (o di "non ripudio") identificato da Nome e Cognome dell'intestatario. Per utilizzare un certificato diverso da quello preimpostato, selezionare una voce dal menu a tendina.

Inserisci il PIN: Inserire il PIN riportato sulla Scratch card virtuale ricevuta via email o sulla Cartellina fisica consegnata in fase di rilascio.

Salva come: selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "...". Lasciando invariato questo campo, il file firmato verrà salvato automaticamente nella stessa cartella in cui si trova il file originale non firmato.

Questa sezione riporta due opzioni facoltative da attivare/disattivare:

Cifra il documento al termine della firma

Distruggi il documento al termine della firma

Tipologia di firma: selezionare dal menu a tendina la tipologia di firma che si vuole apporre al documento. I formati di firma disponibili sono:

- *Busta crittografica P7M (CAdES)* - formato valido per qualunque tipo di documento;
- *Aggiungi la firma al PDF* (PAdES)- formato selezionabile solo nel caso in cui il documento da firmare sia un file PDF (anche nella modalità di firma di più documenti, questo formato sarà presente solo se tutti i documenti selezionati sono esclusivamente documenti PDF);
- *Documento XML* – formato valido per qualunque tipo di documento (eccetto quando l'operazione di firma viene lanciata dai bottoni "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica");

Richiedi Timestamp: attivare l'opzione per aggiungere una marca temporale, ovvero per associare una data e un'ora precisa alla firma che si sta effettuando.*

Scegliere come rappresentare la firma nel documento PDF selezionando una delle opzioni:
Firma invisibile: il PDF verrà firmato senza aggiungere alcun dettaglio di tipo "grafico" al documento;
Firma grafica (modalità avanzata): è possibile selezionare la posizione della firma ed eventualmente aggiungere un'immagine (opzione non disponibile per firma multipla di più documenti PDF);

Firma grafica (con opzioni di default): il PDF verrà firmato aggiungendo i dettagli e la grafica definiti nella sezione "Firma PDF" del menu "Opzioni" (par. 8.4.4); sarà comunque possibile modificare le impostazioni spuntando la casella "Modifica opzioni" e personalizzando al momento le opzioni di firma PDF.

Incorpora informazioni di verifica (formato PAdES-LTV): attivare l'opzione per creare una firma in formato PAdES-LTV (Long Term Validation) e rendere la firma valida a lungo termine. Tramite questa opzione, la firma risulterà sempre valida in qualunque verifica futura, anche dopo la scadenza dei certificati. Attenzione: la funzione è disponibile solo dopo aver precedentemente selezionato la casella "Richiedi timestamp".*

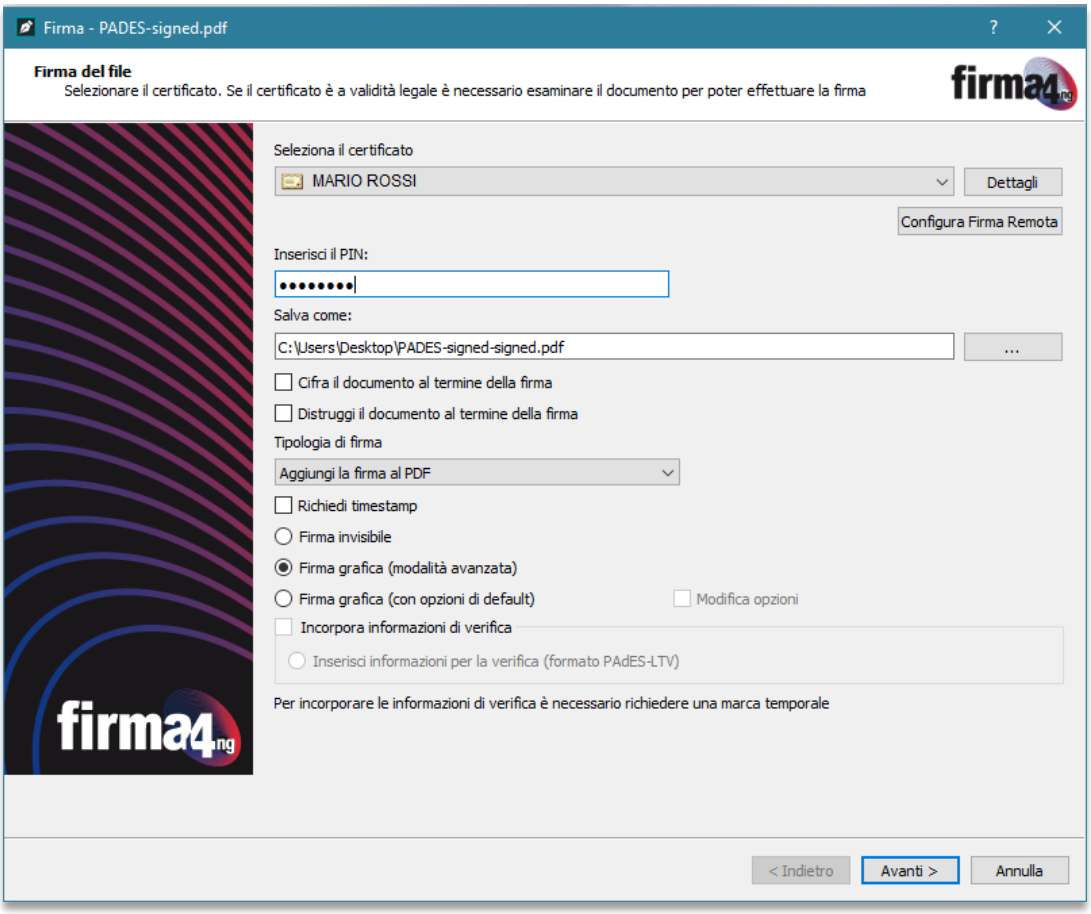


Figura 9

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

***** Per utilizzare il servizio di **Timestamp** o **LTV** è necessario possedere un certificato di marca temporale. Attivando una di queste opzioni durante la procedura di firma (Figura 9), dopo aver cliccato su "Avanti" si aprirà una schermata in cui selezionare dalla tendina il proprio servizio di Timestamp (Figura 10). Se è la prima volta che si utilizza questa funzione e il servizio non risulta ancora configurato, cliccare su "Configura" e inserire le seguenti informazioni:

Nome del servizio
Indirizzo della Timestamp Authority
Username (opzionale)
Password (opzionale)

Quindi cliccare su "Salva" poi su "Chiudi" e proseguire nella procedura di firma cliccando su 'Avanti'.

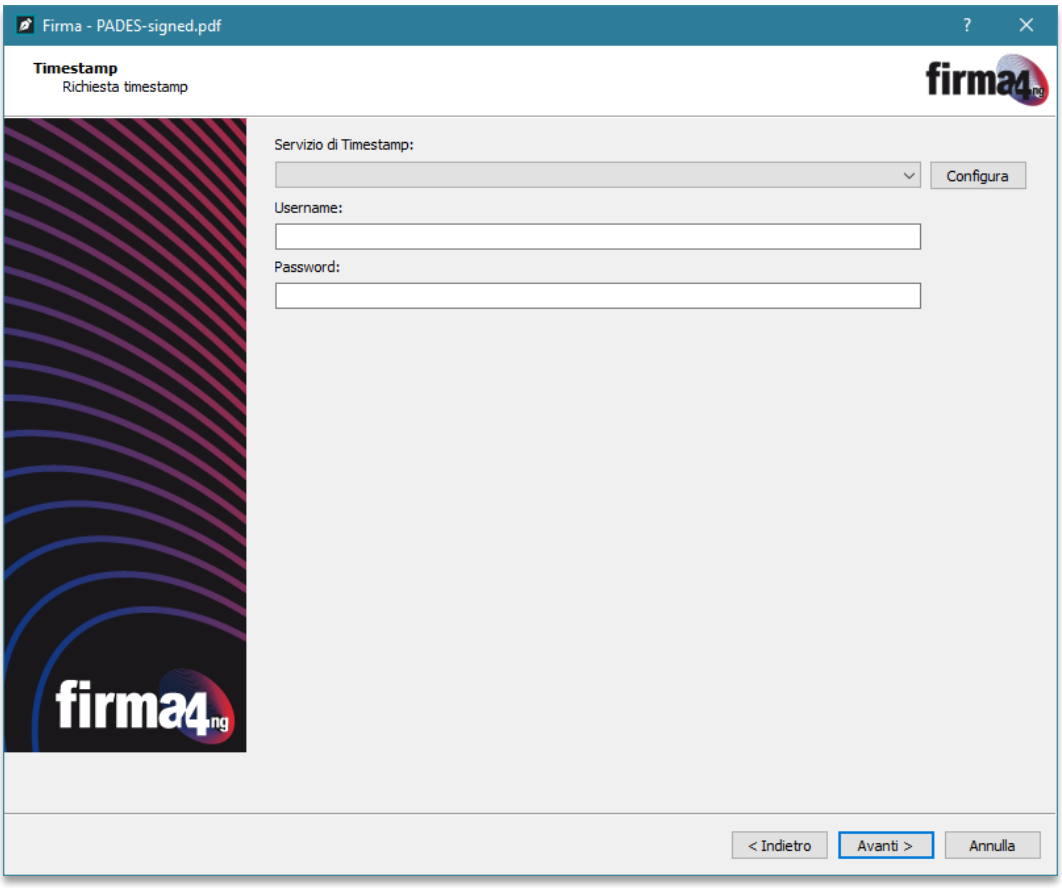


Figura 10

FASE 4 (Firma in formato P7M o XML)

Nel caso in cui si stia firmando un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante "Apri documento".

Quindi selezionare la checkbox "Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta." e cliccare su "Avanti" (Figura 11).

Figura 7

FASE 4 (Firma in formato PDF)

Nel caso in cui si stia firmando un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante "*Apri documento*". Quindi selezionare la checkbox "Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta." e cliccare su "Avanti" (Figura 7).

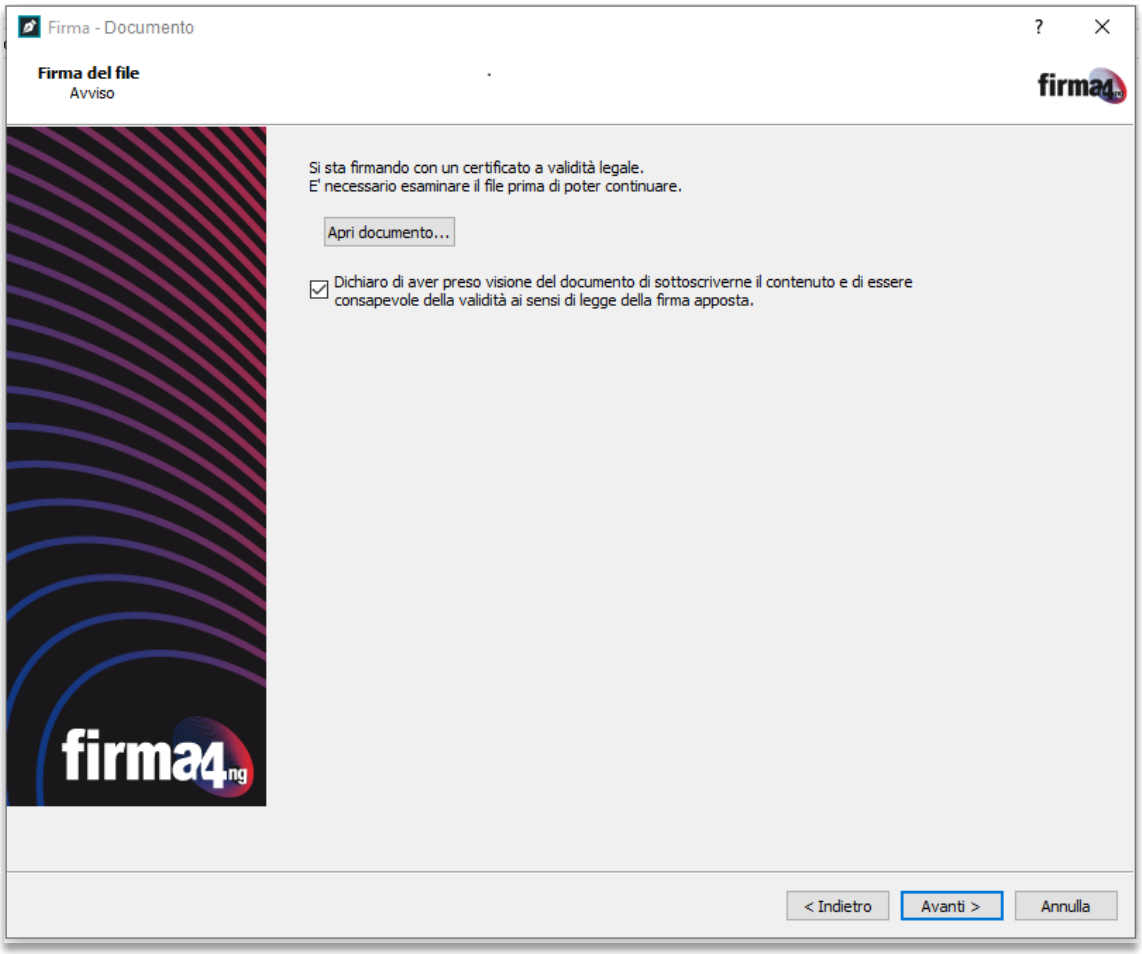


Figura 11

- Se nella Fase 3 è stata selezionata l'opzione **"Firma grafica (modalità avanzata)"** verrà mostrata la schermata per la selezione e il posizionamento della grafica (Figura 12):

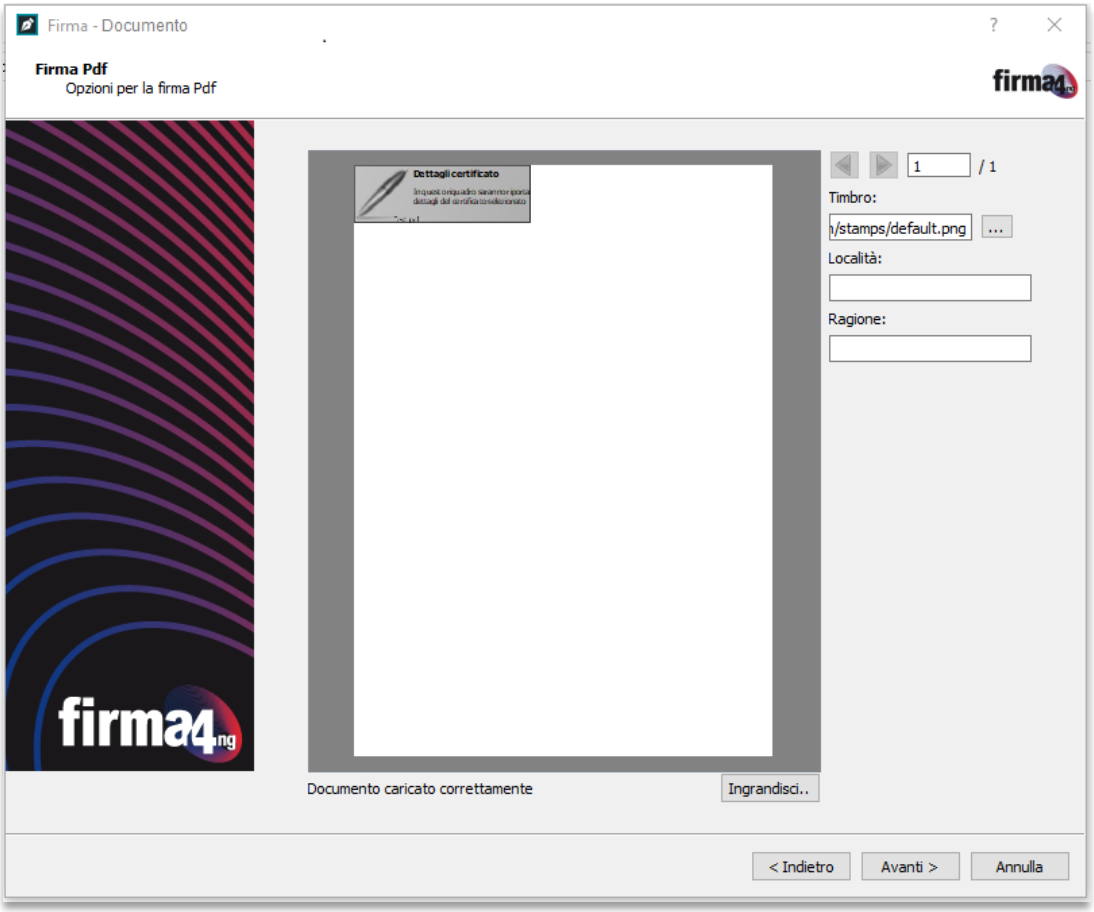


Figura 12

In questa schermata è possibile:

a. Sfogliare le pagine del documento per scegliere dove apporre la firma;
b. Selezionare un'immagine da associare alla firma (facoltativo);
c. Inserire i campi "Località" e "Ragione" da aggiungere alla firma (facoltativo).

- Se nella Fase 3 è stata selezionata l'opzione **"Firma grafica (con opzioni di default)"** con la spunta sulla voce "Modifica opzioni" verrà mostrata la schermata in cui modificare gli standard della firma grafica (Figura 13).

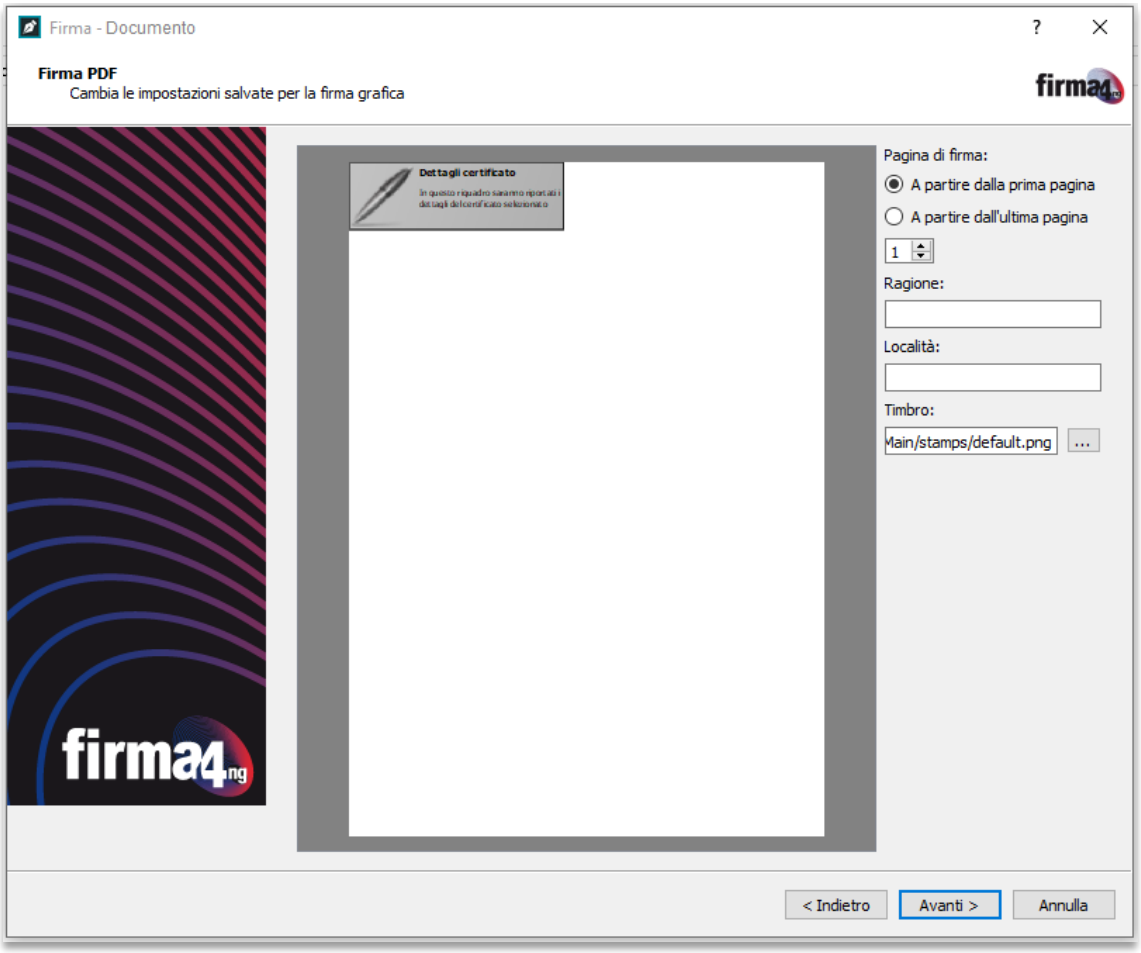


Figura 13

In questa schermata è possibile modificare/inserire:

a) la posizione della firma
b) le dimensioni della firma grafica da apporre
c) la pagina del documento su cui apporre la firma
d) la Ragione e Località
e) l'immagine da includere nella firma.

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

FASE 5

Al termine dell'operazione di firma, il documento firmato viene salvato sul PC, al percorso indicato nella schermata "Operazione conclusa" (Figura 14). Cliccando sul percorso del documento firmato si avvia automaticamente l'operazione di "Verifica" della firma digitale.

Per chiudere la schermata, cliccare su "Termina".

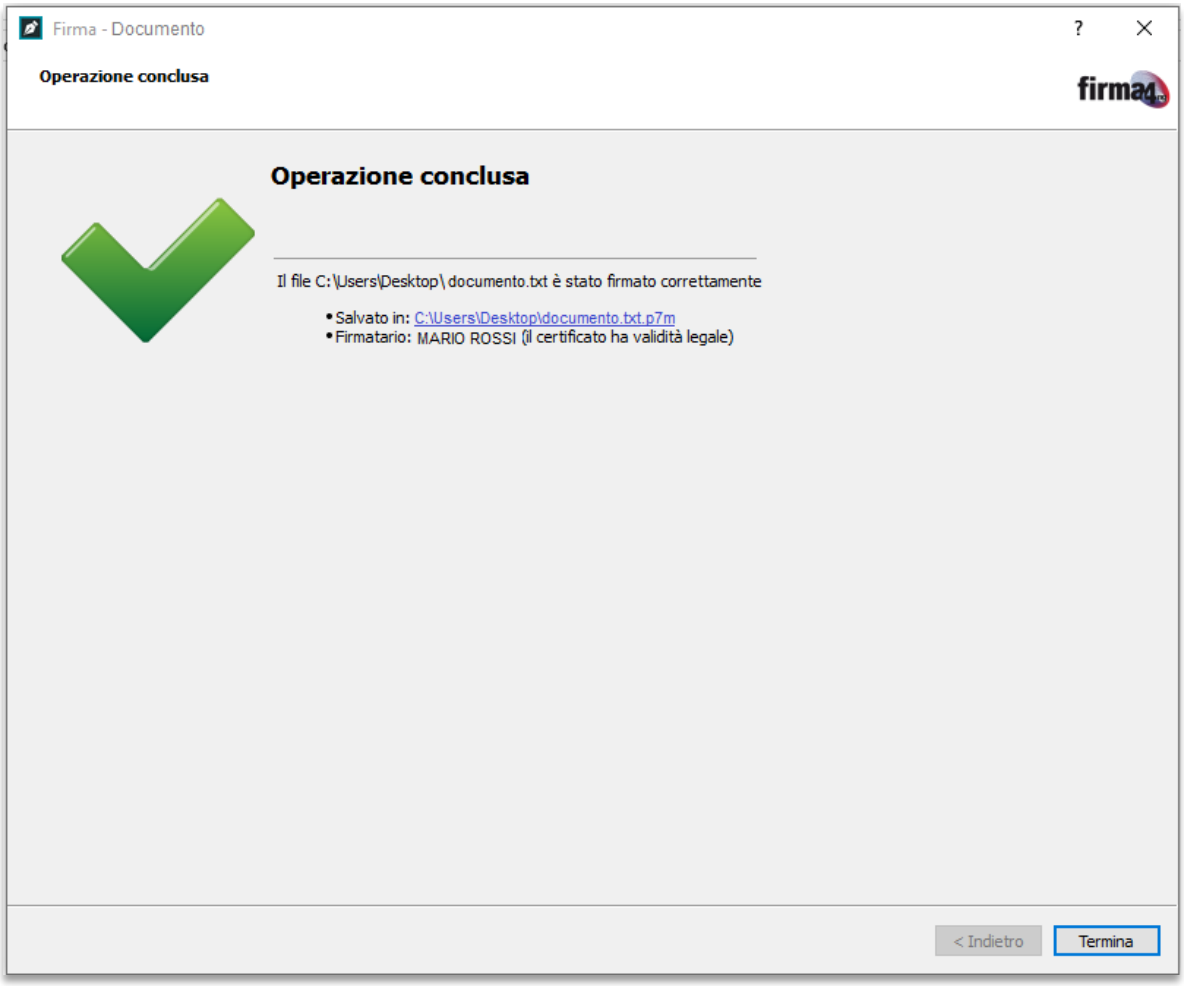


Figura 14

4.2 Firma con certificato di Firma Remota

Se si è in possesso di un certificato di **Firma Remota** seguire la procedura di firma illustrata nelle fasi di seguito.

FASE 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Firma attraverso una delle seguenti modalità:

- Selezionando e trascinando uno o più documenti sul pulsante "Firma" presente nel menu principale (drag&drop);

- Cliccando sul pulsante "Firma" presente nel menu principale e selezionando uno o più documenti da firmare dalla finestra di navigazione del PC (Figura 15).

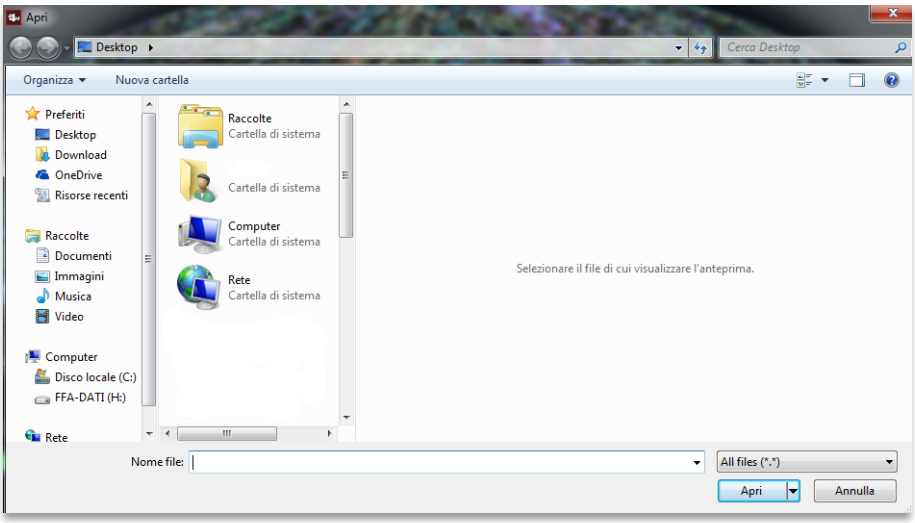


Figura 15

FASE 2

Attendere il caricamento dei certificati (Figura 16).

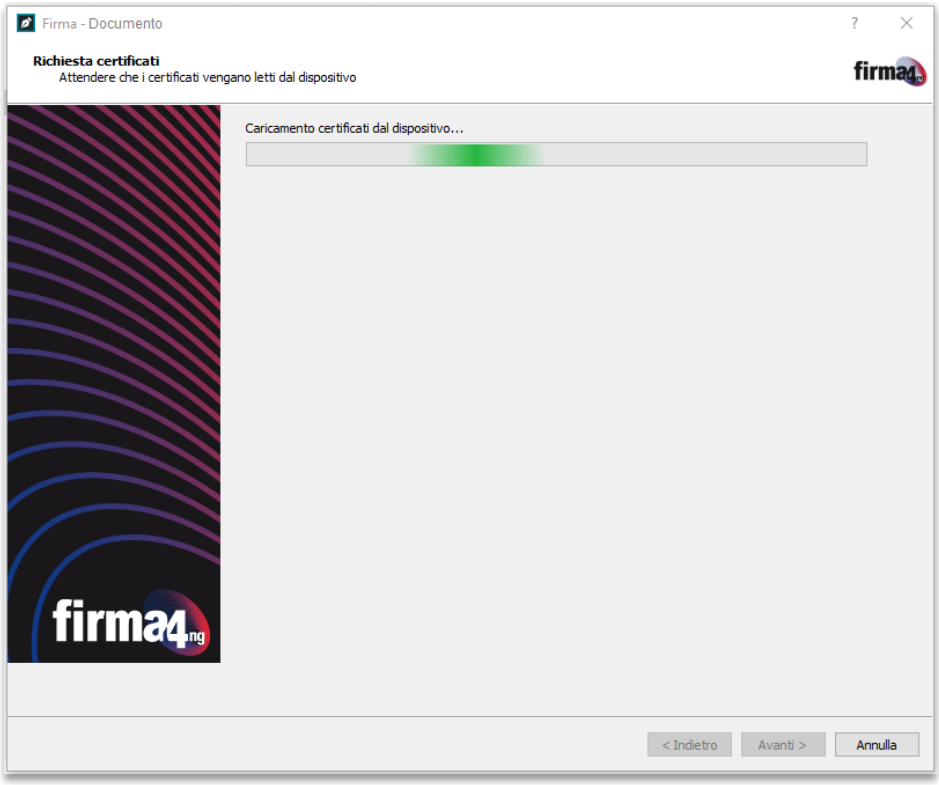


Figura 16

Se è la prima volta che si utilizza la Firma Remota all'interno del software *firma4ng*, appare la finestra di avviso "Non sono stati rilevati Certificati" (Figura 17).
Cliccare su **"Configura Certificati Remoti"** per impostare correttamente la Firma Remota. Se invece la configurazione è già stata effettuata in precedenza, cliccare su **"Ricarica Certificati"** per ripristinare il certificato impostato.

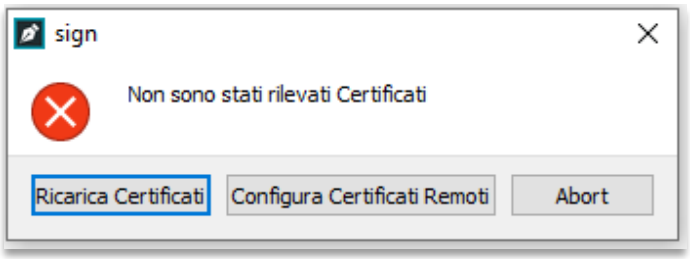


Figura 17

Dopo aver cliccato su **"Configura Certificati Remoti"**, inserire nei campi corrispondenti le credenziali *Username* e *Password* associate al proprio certificato di Firma Remota, quindi cliccare su OK (Figura 18).

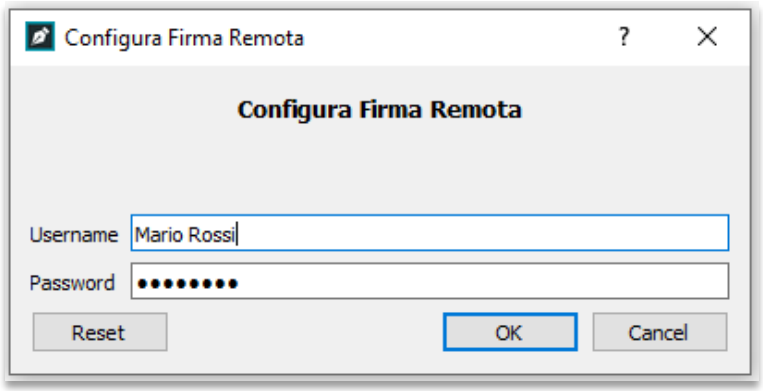


Figura 18

FASE 3 (Firma in formato P7M o XML)

Al termine del caricamento dei certificati, si apre la finestra di configurazione in cui inserire i parametri e le preferenze da applicare alla firma che si sta effettuando (Figura 19):

Seleziona il certificato: risulterà automaticamente selezionato il certificato di firma digitale a validità legale (o di "non ripudio") identificato da Nome e Cognome dell'intestatario. Per utilizzare un certificato diverso da quello preimpostato, selezionare una voce dal menu a tendina.
Firma4ng consente di configurare una singola firma remota alla volta, per sostituire l'account di firma remota cliccare su Configura Firma Remota (Figura 19) e inserire IDlogin e password del certificato di firma remota che intende utilizzare.

Salva come: selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "...". Lasciando invariato questo campo, il file firmato verrà salvato automaticamente nella stessa cartella in cui si trova il file originale non firmato.

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Cifra il documento al termine della firma
Distruggi il documento al termine della firma

Tipologia di firma: selezionare dal menu a tendina la tipologia di firma che si vuole apporre al documento. I formati di firma disponibili sono:

- *Busta crittografica P7M (CAdES)* - formato valido per qualunque tipo di documento;

- *Documento XML* – formato valido per qualunque tipo di documento (eccetto quando l'operazione di firma viene lanciata dai pulsanti "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica");

Richiedi Timestamp: attivare l'opzione per aggiungere una marca, ovvero per associare una data e un'ora precisa alla firma che si sta effettuando. Selezionare dal menu a tendina il formato con cui si vuole apporre la marca digitale al documento (formato .M7M, .TSD o .P7M).

Questa sezione riporta due opzioni facoltative da attivare/disattivare:

Codifica in Base64 (solo per formato P7M)
Separa la firma dal documento (firma "detached")

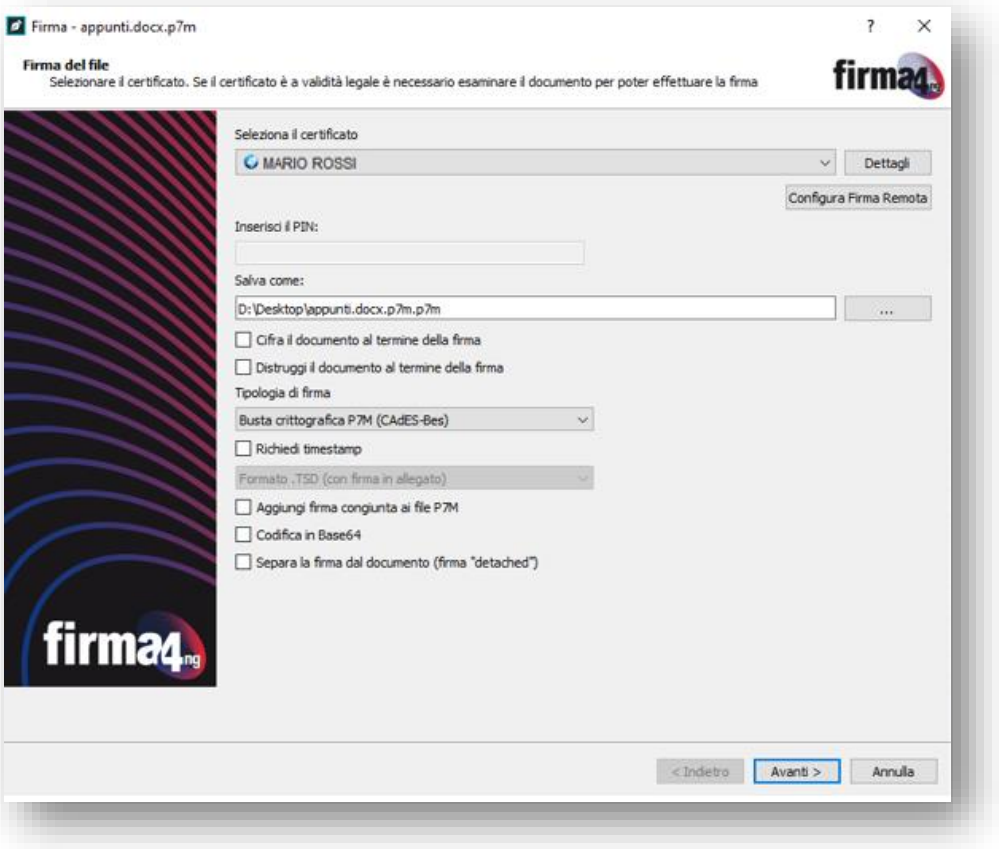


Figura 19

Al termine delle modifiche, cliccare su "Avanti" per proseguire.
Per la Firma Remota configurata non bisognerà inserire la password (PIN) associata, ma verrà richiesto solo l'inserimento del codice OTP associato alle credenziali (Figura 23).

FASE 3 (Firma in formato PDF)

Questa configurazione riguarda solo la firma PDF. Si tratta infatti di un formato valido solo nel caso in cui il documento da firmare sia un file PDF.
Al termine del caricamento dei certificati (Figura 16), appare la finestra di configurazione in cui inserire parametri e preferenze da applicare alla firma che si sta effettuando (Figura 20):

Seleziona il certificato: risulterà automaticamente selezionato il certificato di firma digitale a validità legale (o di "non ripudio") identificato da Nome e Cognome dell'intestatario. Per utilizzare un certificato diverso da quello preimpostato, selezionare una voce dal menu a tendina.

Salva come: selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "...". Lasciando invariato questo campo, il file firmato verrà salvato automaticamente nella stessa cartella in cui si trova il file originale non firmato.

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Cifra il documento al termine della firma
Distruggi il documento al termine della firma

Tipologia di firma: selezionare dal menu a tendina la tipologia di firma che si vuole apporre al documento. I formati di firma disponibili sono:

- *Busta crittografica P7M (CAdES)* - formato valido per qualunque tipo di documento;
- *Aggiungi la firma al PDF* - formato selezionabile solo nel caso in cui il documento da firmare sia un file PDF (anche nella modalità di firma di più documenti, questo formato sarà presente solo se tutti i documenti selezionati sono esclusivamente documenti PDF);
- *Documento XML* – formato valido per qualunque tipo di documento (eccetto quando l'operazione di firma viene lanciata dai bottoni "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica");

Richiedi Timestamp: attivare l'opzione per aggiungere una marca temporale, ovvero per associare una data e un'ora precisa alla firma che si sta effettuando.*

Scegliere come rappresentare la firma nel documento PDF selezionando una delle opzioni:
Firma invisibile: il PDF verrà firmato senza aggiungere alcun dettaglio di tipo "grafico" al documento;
Firma grafica (modalità avanzata): è possibile selezionare la posizione della firma ed eventualmente aggiungere un'immagine (opzione non disponibile per firma multipla di più documenti PDF);

Firma grafica (con opzioni di default): il PDF verrà firmato aggiungendo i dettagli e la grafica definiti nella sezione "Firma PDF" del menu "Opzioni" (par. 8.4.4); sarà comunque possibile modificare le impostazioni spuntando la casella "Modifica opzioni" e personalizzando al momento le opzioni di firma PDF.

Incorpora informazioni di verifica (formato PAdES-LTV): attivare l'opzione per creare una firma in formato LTV (Long Term Validation) e rendere la firma valida a lungo termine. Tramite questa opzione, la firma risulterà sempre valida in qualunque verifica futura, anche dopo la scadenza dei certificati. Attenzione: la funzione è disponibile solo dopo aver precedentemente selezionato la casella "Richiedi timestamp".*

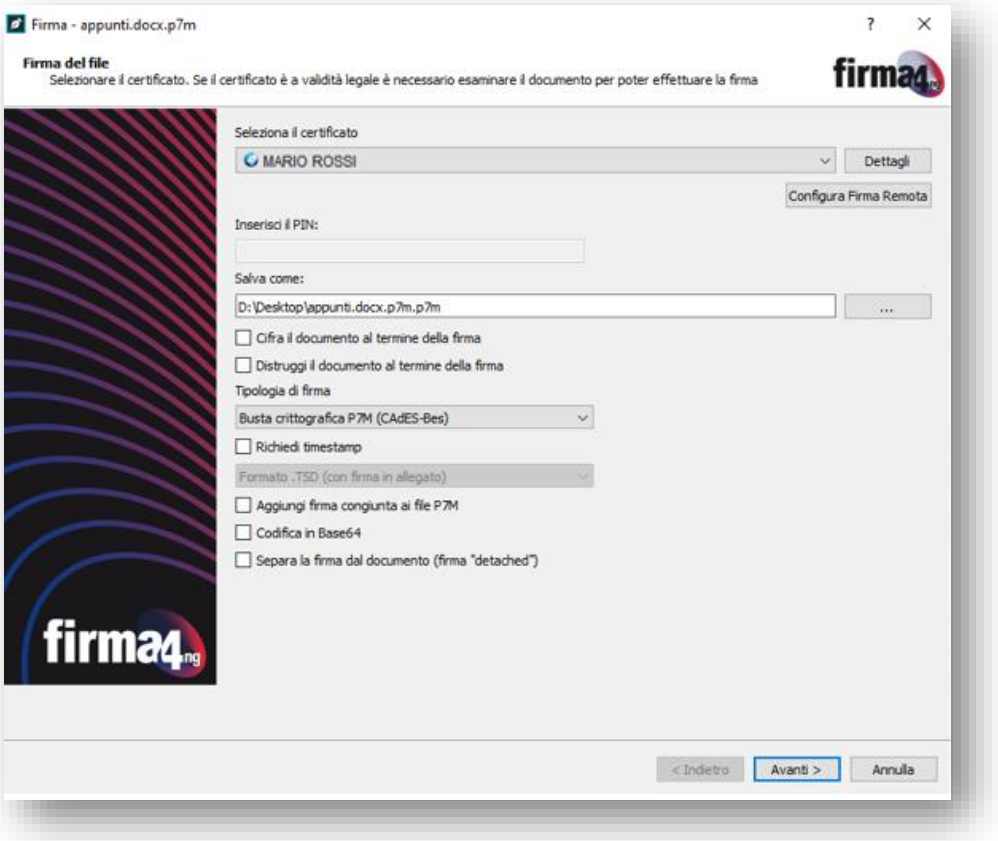


Figura 20

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

***** Per utilizzare il servizio di **Timestamp** o **LTV** è necessario possedere un certificato di marca temporale. Attivando una di queste opzioni durante la procedura di firma (Figura 20), dopo aver cliccato su "Avanti" si aprirà una schermata in cui selezionare dalla tendina il proprio servizio di Timestamp (Figura 21). Se è la prima volta che si utilizza questa funzione e il servizio non risulta ancora configurato, cliccare su "Configura" e inserire le seguenti informazioni:

Nome del servizio
Indirizzo della Timestamp Authority
Username (opzionale)
Password (opzionale)

Quindi cliccare su "Salva" poi su "Chiudi" e proseguire nella procedura di firma cliccando su 'Avanti'.

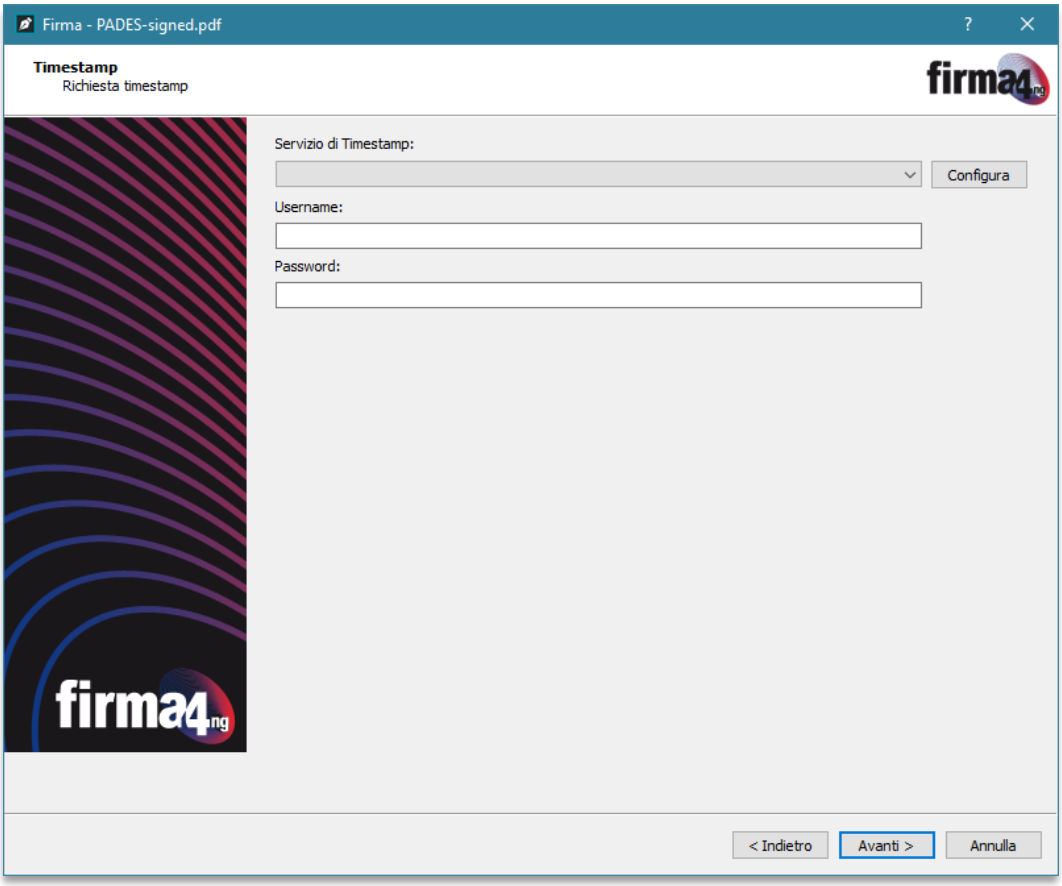


Figura 21

FASE 4 (Firma in formato P7M o XML)

Nel caso in cui si stia firmando un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante "*Apri documento*". Quindi selezionare la checkbox "Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta." e cliccare su "Avanti" (Figura 22).

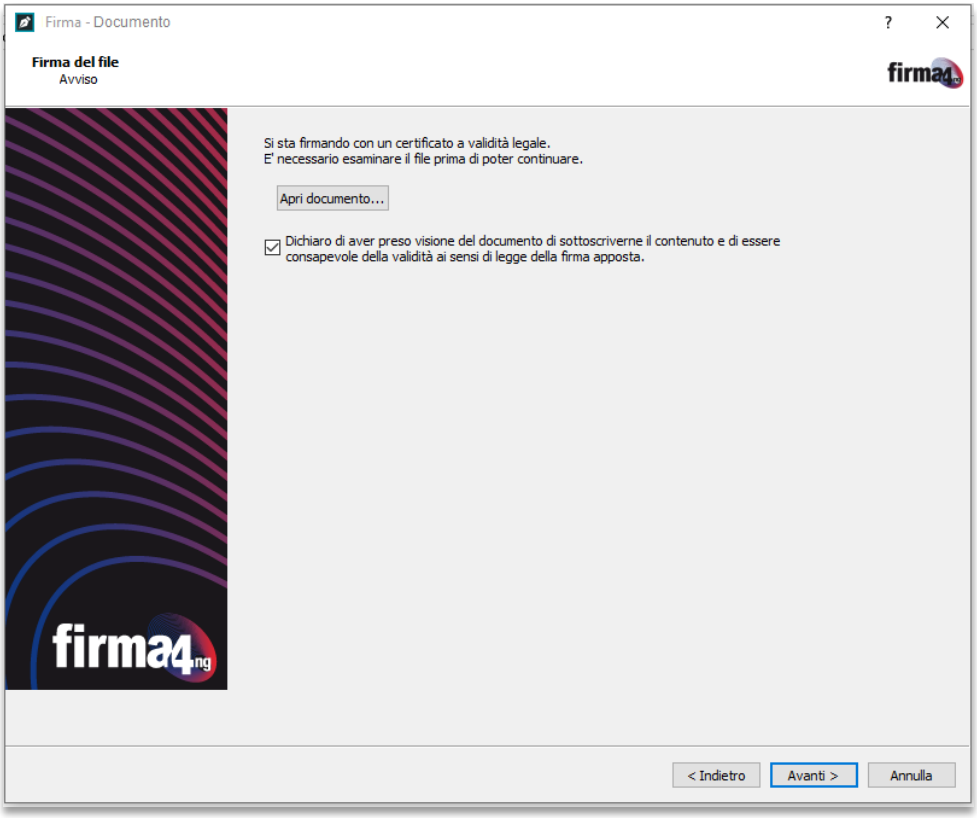


Figura 22

Apparirà una finestra in cui inserire il **codice OTP** generato dall'applicazione DigitalDNA IC oppure richiederlo via sms (Figura 23).

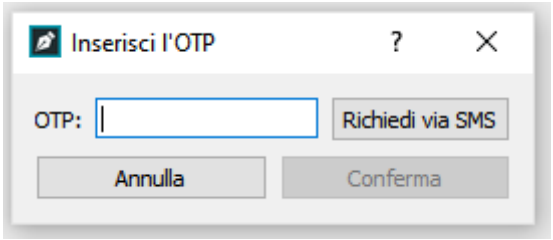


Figura 23

Apparirà una finestra in cui inserire il **codice OTP** ricevuto via sms (Figura 24).

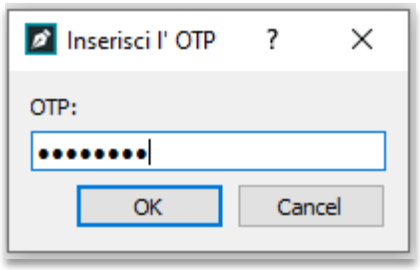


Figura 24

FASE 4 (Firma in formato PDF)

Nel caso in cui si stia firmando un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante "*Apri documento*". Quindi selezionare la checkbox "Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta." e cliccare su "Avanti" (Figura 22).

- Se nella Fase 3 è stata selezionata l'opzione **"Firma grafica (modalità avanzata)"** verrà mostrata la schermata per la selezione e il posizionamento della grafica (Figura 25):

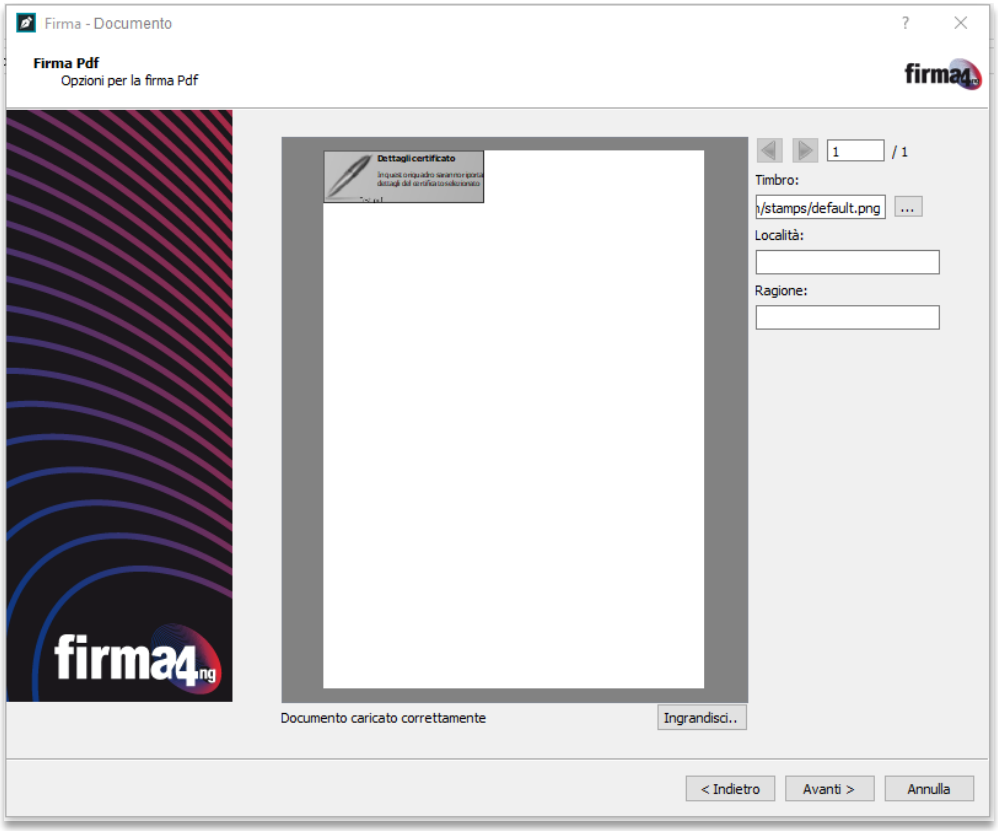


Figura 25

In questa schermata è possibile:

a) Sfogliare le pagine del documento per scegliere dove apporre la firma;
b) Selezionare un'immagine da associare alla firma (facoltativo);
c) Inserire i campi "Località" e "Ragione" da aggiungere alla firma (facoltativo).

- Se nella Fase 3 è stata selezionata l'opzione **"Firma grafica (con opzioni di default)"** con la spunta sulla voce "Modifica opzioni" verrà mostrata la schermata in cui modificare gli standard della firma grafica (Figura 26).

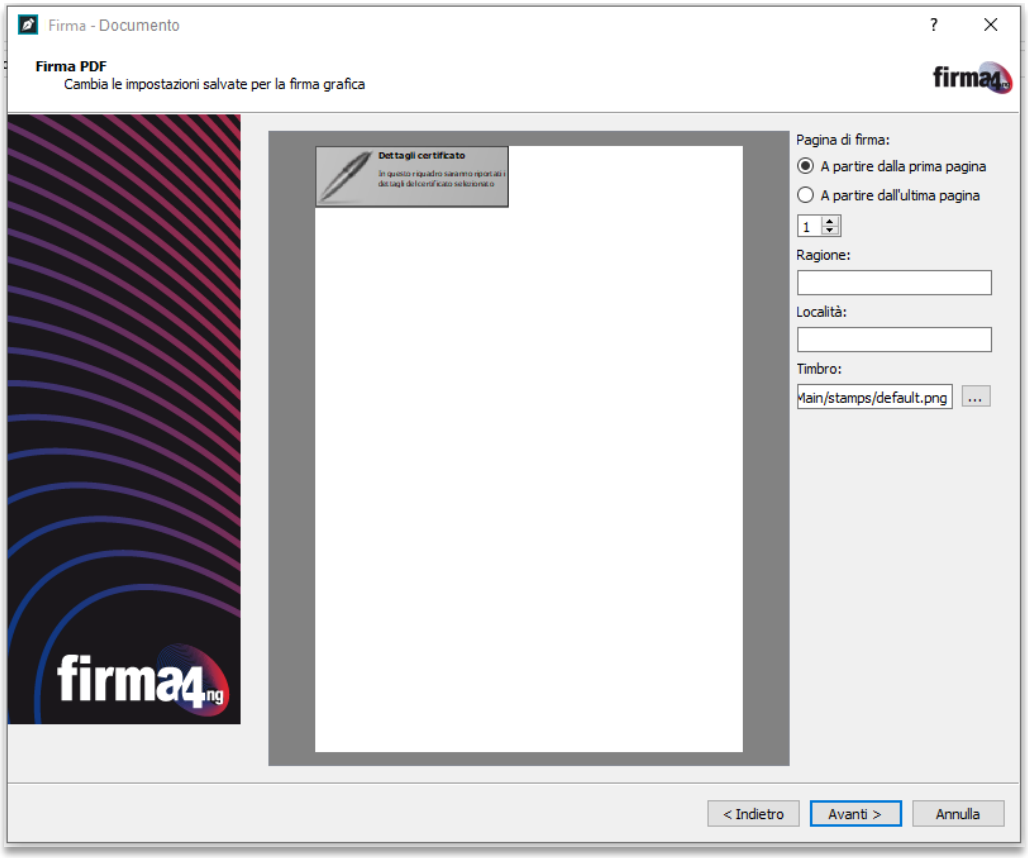


Figura 26

In questa schermata è possibile modificare/inserire:

a) la posizione della firma
b) le dimensioni della firma grafica da apporre
c) la pagina del documento su cui apporre la firma
d) la Ragione e Località
e) l'immagine da includere nella firma.

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

FASE 5

Al termine dell'operazione di firma, il documento firmato viene salvato sul PC, al percorso indicato nella schermata "Operazione conclusa" (Figura 27). Cliccando sul percorso del documento firmato si avvia automaticamente l'operazione di "Verifica" della firma digitale.

Per chiudere la schermata, cliccare su "Termina".

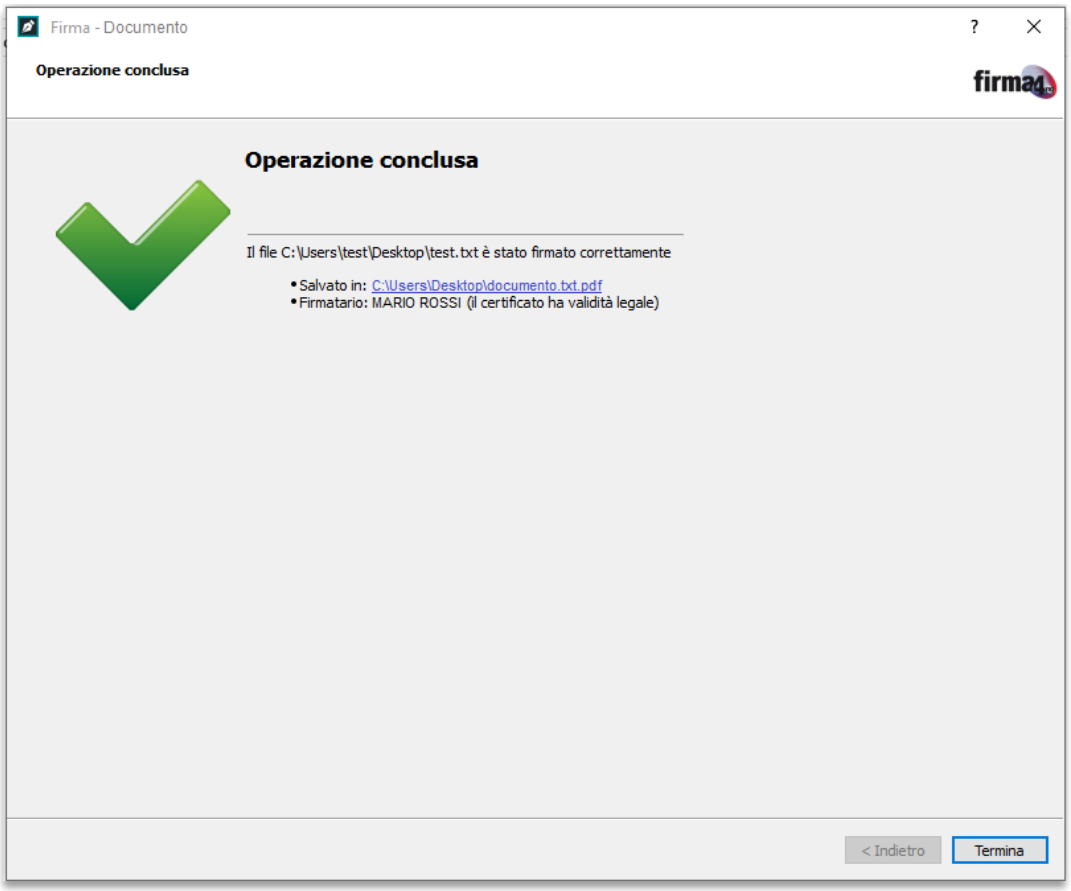


Figura 27

4.3 Firma tramite un applicativo esterno

Se si è in possesso di un dispositivo DigitalDNA o di un certificato di Firma Remota, è possibile firmare digitalmente i documenti anche attraverso un **applicativo esterno** a *firma4ng* (es. Adobe Acrobat Reader).

Prima di iniziare è necessario associare la propria firma digitale al PC in uso, collegando il dispositivo DigitalDNA tramite USB o Bluetooth (paragrafo 9.1) oppure configurando la Firma Remota (paragrafo 4.2). Una volta riconosciuta dal software *firma4ng* installato sul PC, la firma digitale risulterà automaticamente integrata anche in applicativi esterni che supportano la funzione di firma.

Esempio di firma tramite applicativo esterno: Adobe Acrobat Reader

1. Aprire un file PDF tramite Adobe Acrobat Reader
2. Cliccare sulla voce del menu "Altri strumenti" (Figura 28)

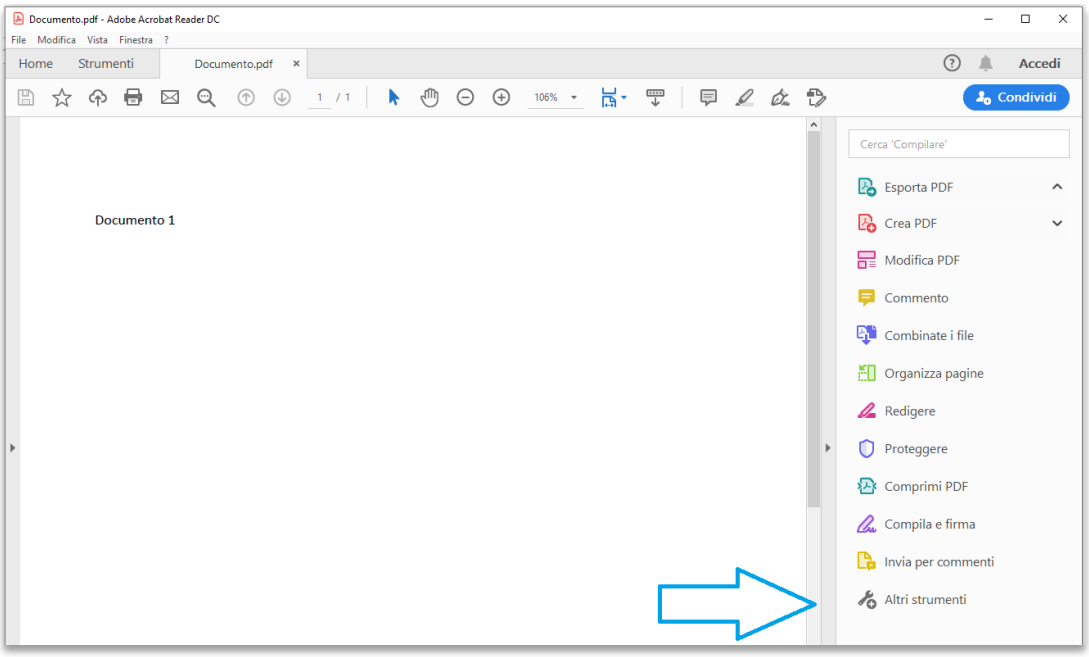


Figura 28

3. Cliccare sul pulsante "Apri" posizionato sotto l'icona "Certificati" (Figura 29)

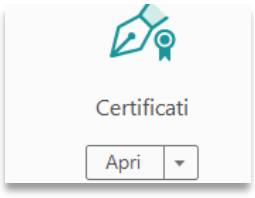


Figura 29

4. Cliccare su “Firma digitalmente” (Figura 30)

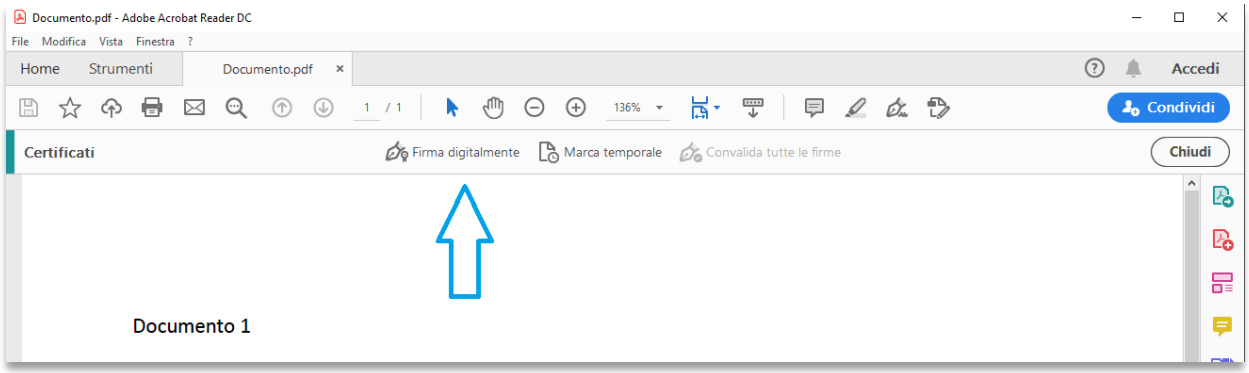


Figura 30

5. Seguire le istruzioni contenute all’interno della finestra per selezionare e delimitare l’area in cui posizionare graficamente la firma (Figura 31)

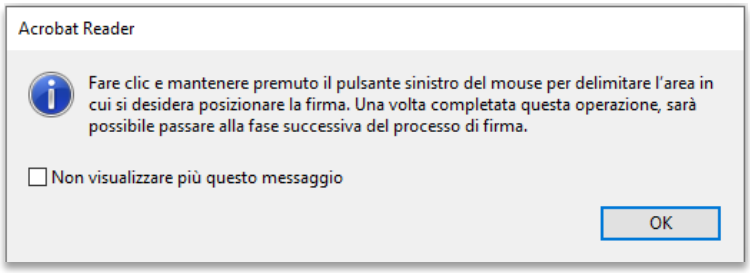


Figura 31

6. Selezionare il certificato da utilizzare per la firma digitale e cliccare su “Continua” (Figura 32)

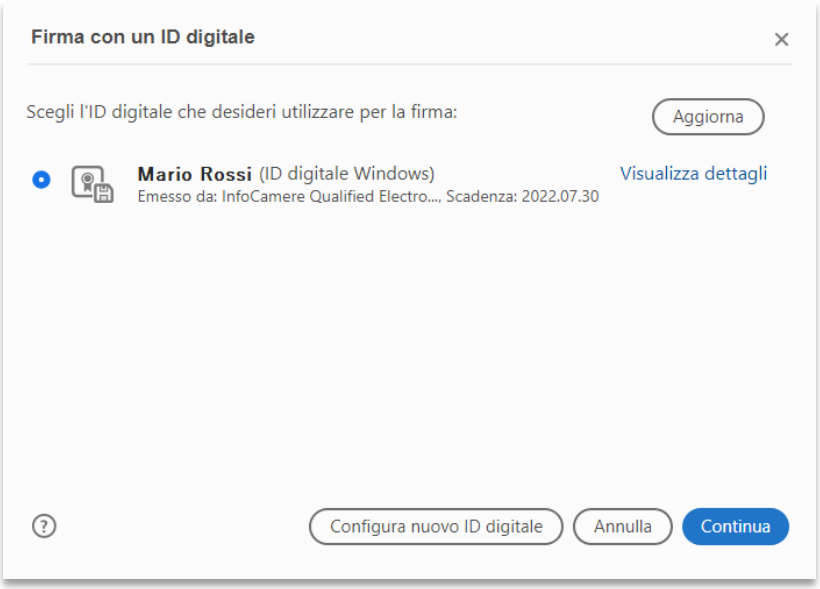


Figura 32

7. Verificare l'anteprima della firma che si è sul punto di apporre sul documento, quindi cliccare su "Firma" per confermare (Figura 33)

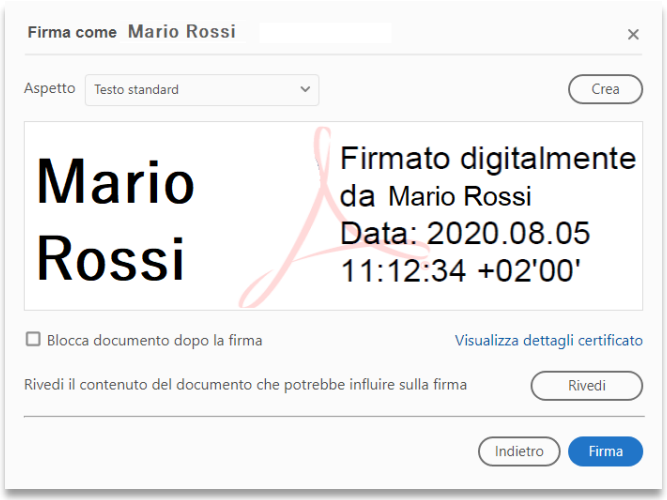


Figura 33

8. Selezionare la cartella del PC in cui si desidera salvare il documento firmato.
9. Inserire il **codice OTP** ricevuto tramite SMS (Figura 34)

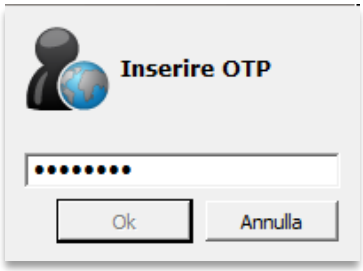


Figura 34

10. Il documento è stato firmato correttamente (Figura 35)

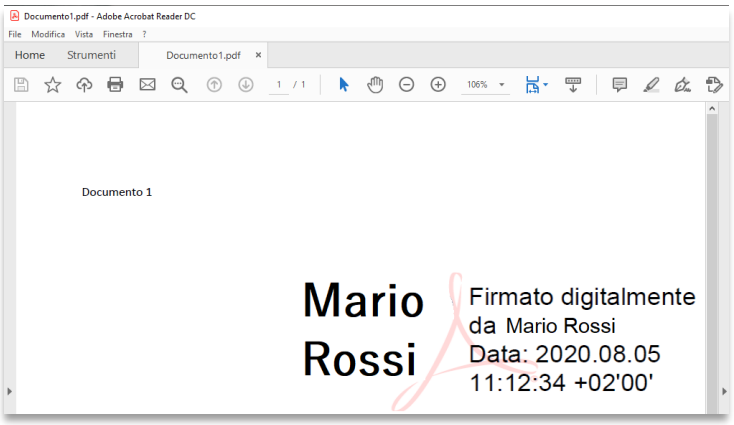


Figura 35

5. VERIFICA

La funzione **"Verifica"** permette di verificare la validità di un file firmato e/o marcato temporalmente.

FASE 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Verifica attraverso una delle seguenti modalità:

- Selezionando e trascinando il documento sul pulsante "Verifica" presente nel menu principale (drag&drop);
- Cliccando sul pulsante "Verifica" presente nel menu principale e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 36).

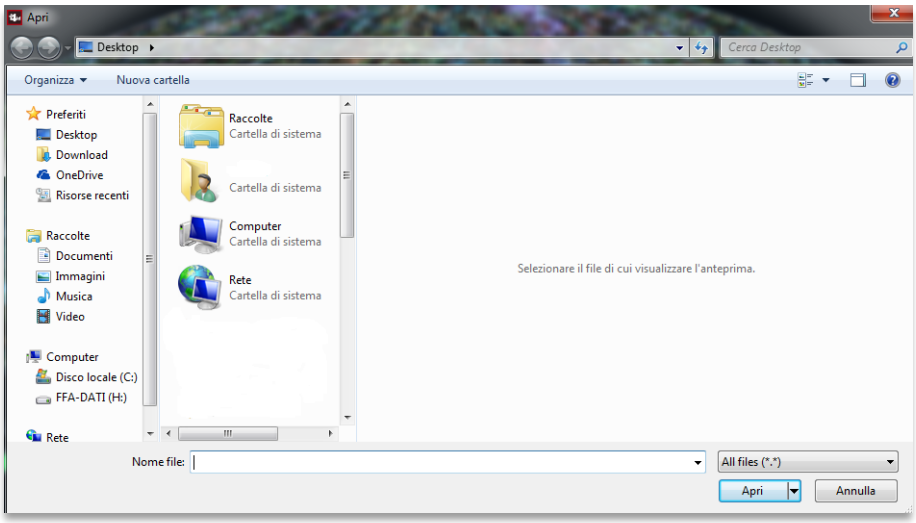


Figura 36

FASE 2

Attendere il completamento dell'operazione. Al termine dell'analisi, la schermata riporta l'esito della verifica (Figura 37).

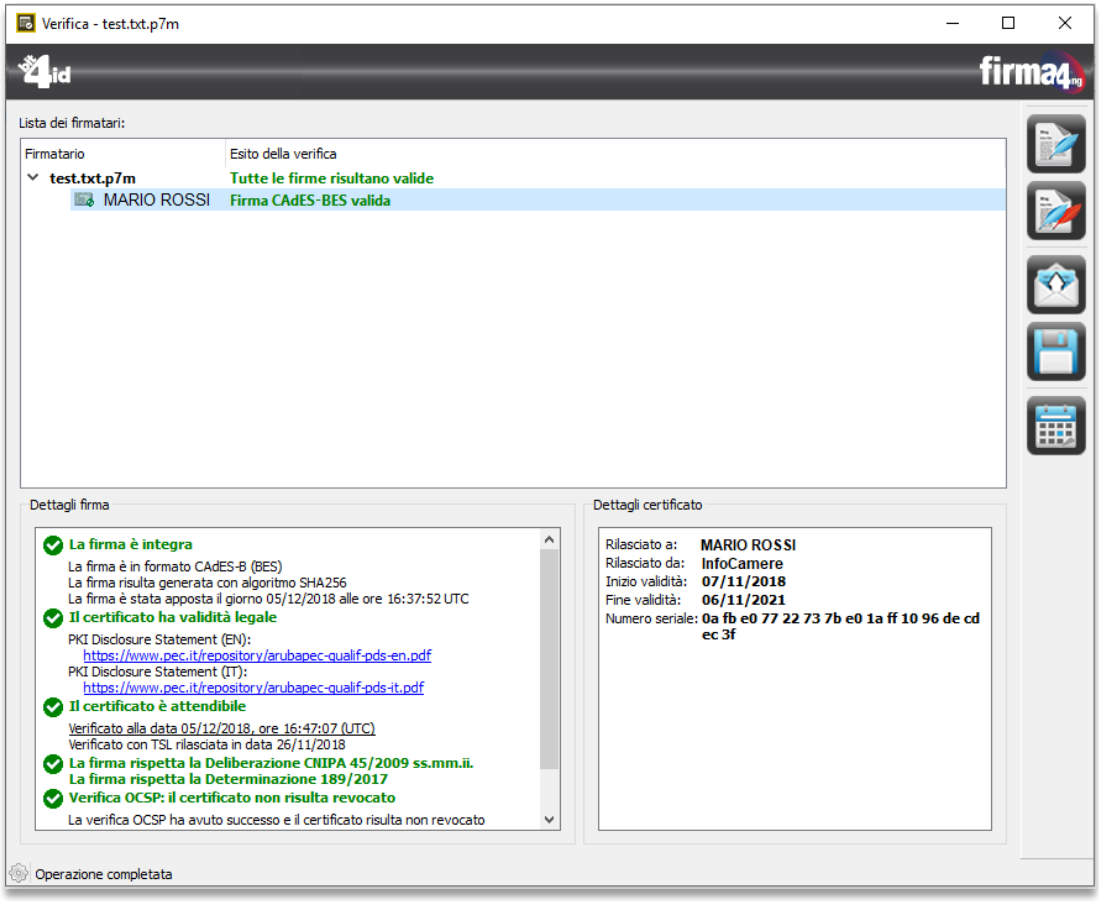


Figura 37

- Nella sezione in alto viene mostrato l'elenco delle firme apposte sul documento, insieme a eventuali marche temporali o firme LTV (Long Term Validation). Sono riportati anche i certificati dei firmatari del documento (Figura 38). È possibile visualizzare i dettagli di un certificato con un doppio clic su ognuno di essi.

Figura 38

- Nella sezione in basso a sinistra della schermata sono mostrati i dettagli delle verifiche effettuate su una specifica firma/marca temporale (Figura 39):

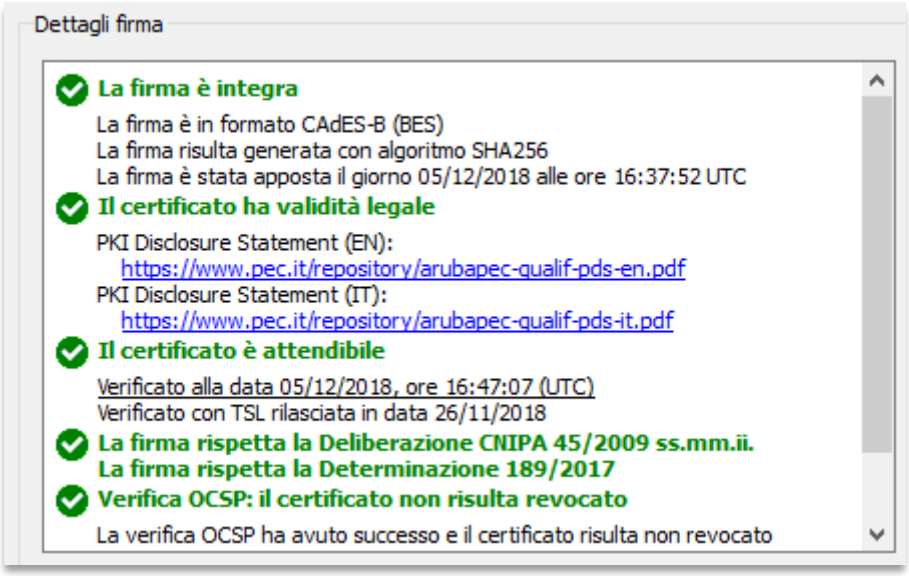


Figura 39

Integrità: viene mostrato l'esito della verifica di integrità del documento firmato, per controllare che non sia stato alterato dopo la firma. Vengono inoltre visualizzati i dettagli relativi al formato di firma, l'algoritmo utilizzato e la data in cui è stata realizzata la firma. In caso di esito positivo viene mostrato il messaggio: "La firma è integra".

Validità legale: viene mostrato l'esito del controllo effettuato sull'attributo del certificato (Key Usage) che ne definisce l'utilizzo. Per la normativa italiana, il certificato di firma digitale deve avere il Key Usage valorizzato con il solo valore "Non Repudiation". In caso di esito positivo viene mostrato il messaggio: "Il certificato ha validità legale".

Attendibilità: viene mostrato l'esito del controllo effettuato sul Certificatore che ha emesso il certificato del firmatario. In caso di esito positivo, ossia nel caso in cui il Certificatore emittente sia presente nella lista dei Certificatori Accreditati presso l'AgID (Agenzia per l'Italia Digitale), viene mostrato il messaggio: "Il certificato è attendibile".

Aderenza alle Regole Tecniche previste dalla Normativa vigente: viene mostrato l'esito del controllo relativo all'aderenza e al rispetto della Normativa Vigente. In caso di esito positivo viene mostrato il messaggio: "La firma rispetta la Deliberazione CNIPA 45/2009 ss.mm.ii". La firma rispetta la Determinazione 189/2017".

Stato di revoca/sospensione del certificato: viene mostrato l'esito del controllo sullo stato di validità del certificato, per verificare che non sia scaduto temporalmente e, attraverso le CRL (Certificate Revocation Lists), che non sia stato sospeso o revocato. Se lo stato del certificato è valido viene mostrato il messaggio: "Il certificato non risulta revocato".

- Nella sezione in basso a destra vengono mostrati i dettagli del certificato con cui è stato firmato il documento selezionato (Figura 40).

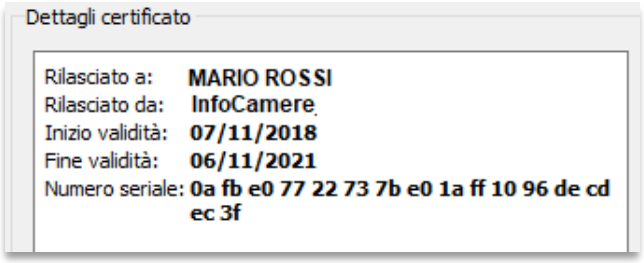


Figura 40

FASE 3

Dal menu verticale presente sul bordo destro della schermata di Verifica (Figura 33), è possibile effettuare le seguenti operazioni:

Aggiungi firma:

Per aggiungere un'ulteriore firma al documento.

Aggiungi controfirma:

Per aggiungere una controfirma alla firma selezionata.

Apri contenuto:

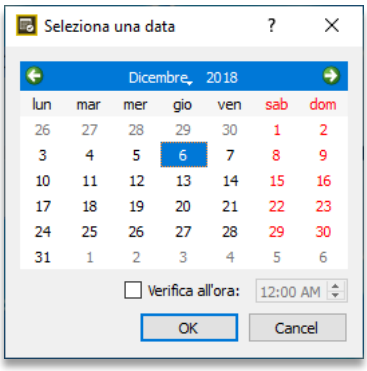
Per visualizzare il contenuto del documento firmato o marcato temporalmente.

Salva contenuto:

Per salvare il documento originale oggetto della verifica. Nel caso in cui si stia verificando una marca temporale apposta al documento, questa funzione è disponibile solo se il formato della marca temporale è ".tsd".

Verifica alla data:

Per effettuare la verifica a una specifica data selezionata. Cliccando sul pulsante si apre un calendario da cui selezionare una data (se il documento firmato contiene delle firme marcate temporalmente, la verifica di tali firme viene sempre effettuata alla data indicata nella marca temporale).



6. MARCA TEMPORALE

La funzione **"Marca temporale"** permette di apporre una marca temporale su un documento. Il software *firma4ng* supporta tutti formati di marche temporali previsti dagli standard e dalla normativa Nazionale attualmente in vigore.

FASE 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Marca temporale attraverso una delle seguenti modalità:

- Selezionando e trascinando il documento sul pulsante "Marca temporale" presente nel menu principale (drag&drop);
- Cliccando sul pulsante "Marca temporale" presente nel menu principale e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 41).

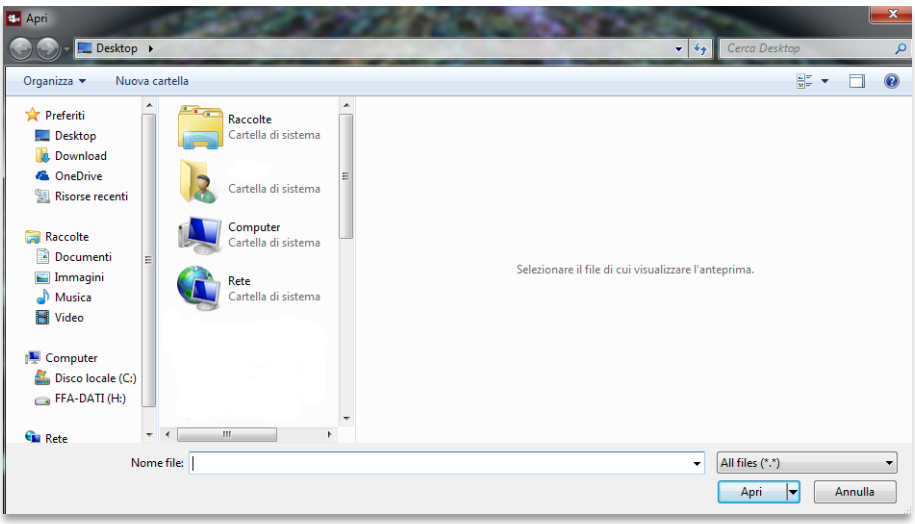


Figura 41

Nota: è possibile appore una marca temporale anche contestualmente all'operazione di firma (vedi paragrafo 4.4 fase 3).

Dopo aver selezionato il documento, appare una finestra (Figura 42) nella quale indicare:

Servizio di marcatura temporale da utilizzare;

Username;

Password;

Cartella di destinazione;

Formato della marca temporale tra quelli presenti nel menu a tendina:

- .M7M: unisce al suo interno sia il documento elettronico firmato (di tipo .p7m), che la relativa Marca Temporale (in formato .tsr);
- .TSD: formato che racchiude il documento originale e la marca temporale;
- .TSR: formato che racchiude la sola marca temporale;
- .TST: formato che racchiude la sola marca temporale;
- .PDF: inglobando la marca temporale nel file pdf in cui è apposta la firma.

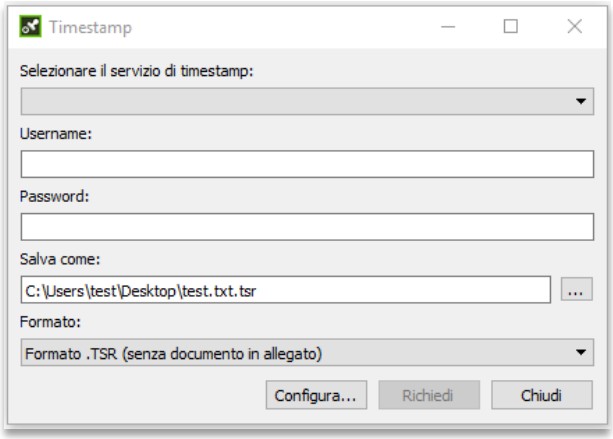


Figura 42

L'operazione di marcatura temporale necessita della connessione a Internet in quanto per completare tale operazione *firma4ng* comunica con il servizio di Timestamp selezionato. È possibile modificare la configurazione cliccando sul pulsante "Configura".

Al termine delle modifiche, cliccare sul pulsante **"Richiedi"** per inviare la richiesta di marcatura temporale.

FASE 3

Al termine dell'operazione di marcatura temporale, appare un messaggio con l'esito dell'operazione. Cliccare su "OK" per chiudere il messaggio; per chiudere la finestra "Timestamp" cliccare su "Chiudi".

7. GESTIONE DISPOSITIVO

Cliccando sul pulsante **"Gestione Dispositivo"** presente nel menu principale (Figura 1), si apre una finestra che contiene le seguenti schede:

- Cambio PIN
- Sblocco PIN

7.1 Cambio PIN

Nella finestra **"Cambio PIN"** è possibile cambiare il codice PIN del dispositivo, inserendo negli appositi campi il PIN attuale e il nuovo PIN scelto, confermando nuovamente quest'ultimo (Figura 43). Al termine delle modifiche, cliccare su "OK" per cambiare il PIN.

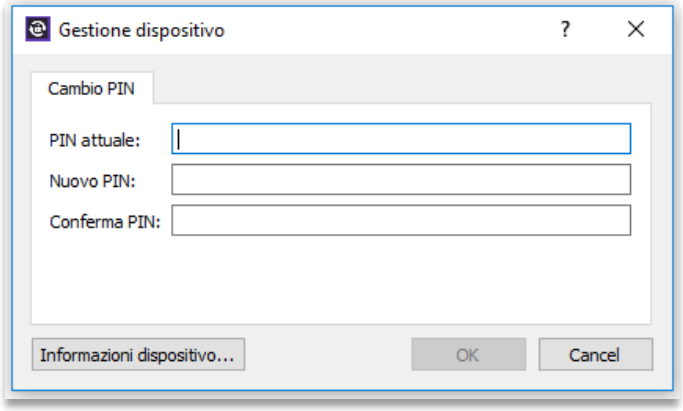


Figura 43

7.2 Sblocco PIN

Nella finestra **"Sblocco PIN"** è possibile sbloccare il codice PIN del dispositivo (a seguito di tre tentativi errati di inserimento PIN) inserendo negli appositi campi il codice PUK del dispositivo, un nuovo PIN di otto cifre numeriche e confermando nuovamente quest'ultimo (Figura 44). Al termine delle modifiche, cliccare su "OK" per sbloccare il PIN.

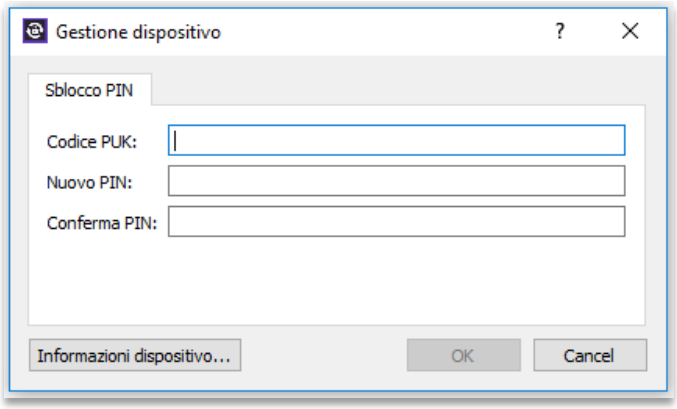


Figura 44

7.3 Informazioni dispositivo

Cliccando sul pulsante "Informazioni dispositivo" presente nella schermata di Cambio PIN/Sblocco PIN, vengono visualizzate informazioni relative al dispositivo di firma collegato (numero seriale, certificati, ecc.) (Figura 45).

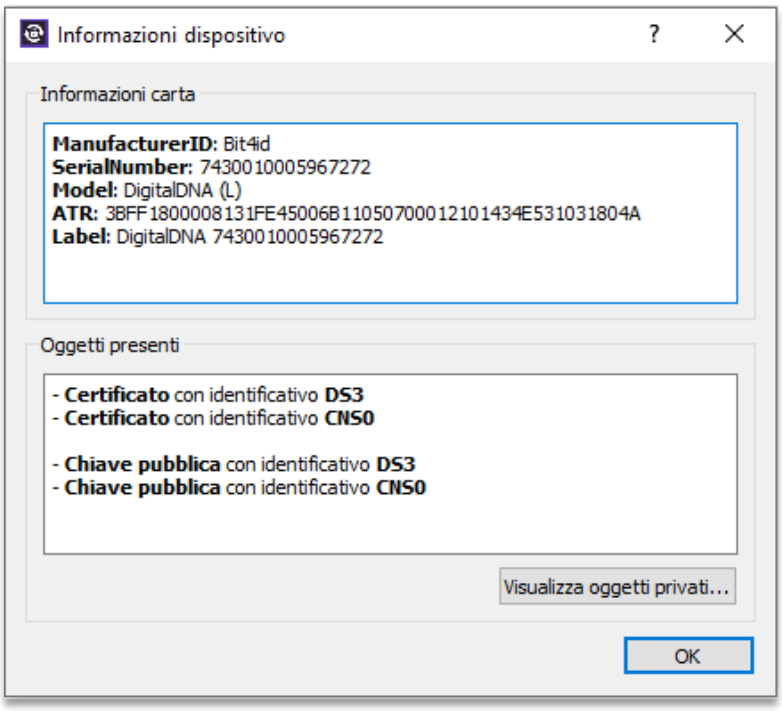


Figura 45

8. APPLICAZIONI

Cliccando sul pulsante **"Applicazioni"** presente nel menu principale (Figura 1) si apre un menu secondario che contiene le seguenti voci (Figura 46):

- Cifra
- Decifra
- Storico
- Impostazioni

Figura 46

8.1 Cifratura

Al pulsante **"Cifra"** corrisponde la funzione di cifratura di uno o più documenti.

FASE 1

A partire dal menu secondario "Applicazioni" (Figura 46), è possibile avviare l'operazione di cifratura attraverso una delle seguenti modalità:

- Selezionando e trascinando il documento sul pulsante "Cifra" presente nel menu secondario (drag&drop);
- Cliccando sul pulsante "Cifra" presente nel menu secondario e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 47).

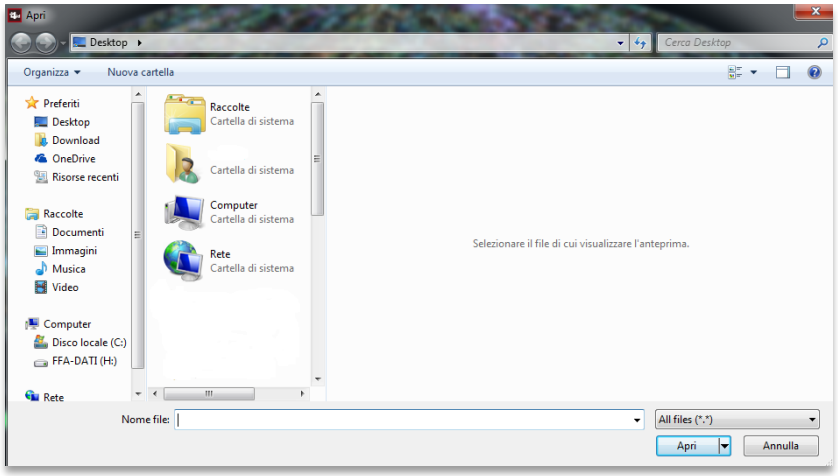


Figura 47

FASE 2

Attendere il caricamento dei certificati. Terminato il caricamento, i certificati vengono visualizzati nella schermata all'interno della sezione **"Contatti"** (Figura 48).

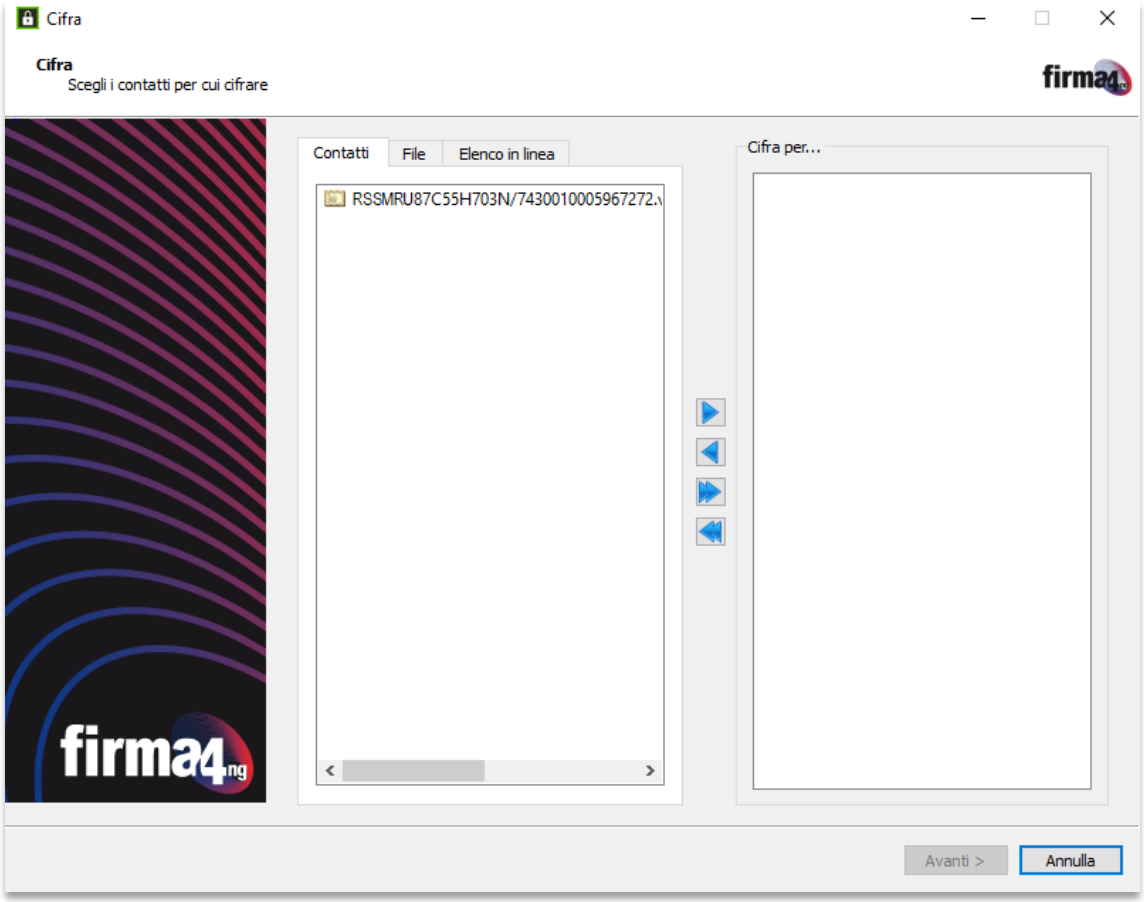


Figura 48

La rubrica di contatti permette di memorizzare i certificati dei contatti per i quali cifrare un documento.
Se si desidera cifrare un documento per un destinatario specifico, è possibile importare contatti all'interno della rubrica sia caricandoli dal PC, sia ricercandoli sul Registro pubblico dei certificati gestito dal Certificatore, tramite le seguenti modalità:

File

Per inserire nella rubrica dei Contatti un destinatario il cui certificato è disponibile su file, dalla sezione "File" cliccare su "Importa da file" e scegliere il certificato (.cer) da importare (Figura 49).
Una volta che il file del certificato è stato correttamente 'caricato', cliccando con il tasto destro del mouse su di esso e scegliendo "Aggiungi ai contatti...", il contatto verrà inserito nei "Contatti personali" (Figura 51).

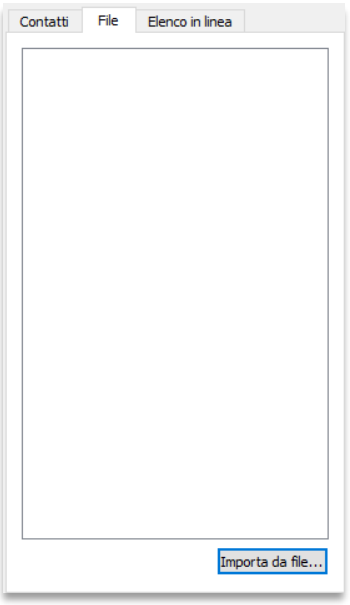


Figura 49

Elenco in linea

È possibile importare il certificato di un contatto cercandolo sul Registro pubblico dei certificati gestito dal Certificatore, impostando i parametri di ricerca presenti nella sezione e cliccando su "Cerca" (Figura 50).
Al termine della ricerca, nel riquadro in basso verrà mostrata la lista dei certificati ottenuti come risultato. Dopo aver selezionato il certificato di interesse, cliccando con il tasto destro del mouse su di esso e scegliendo "Aggiungi ai contatti...", questo verrà inserito nei "Contatti personali" (Figura 51).

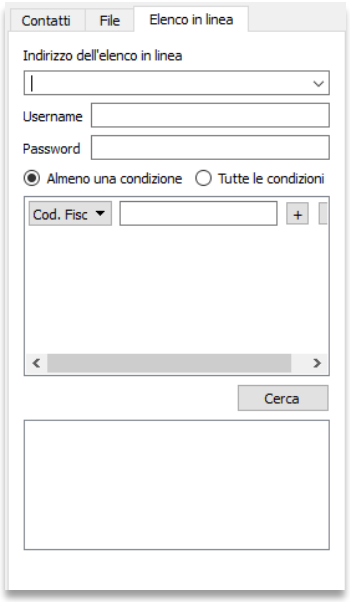


Figura 50

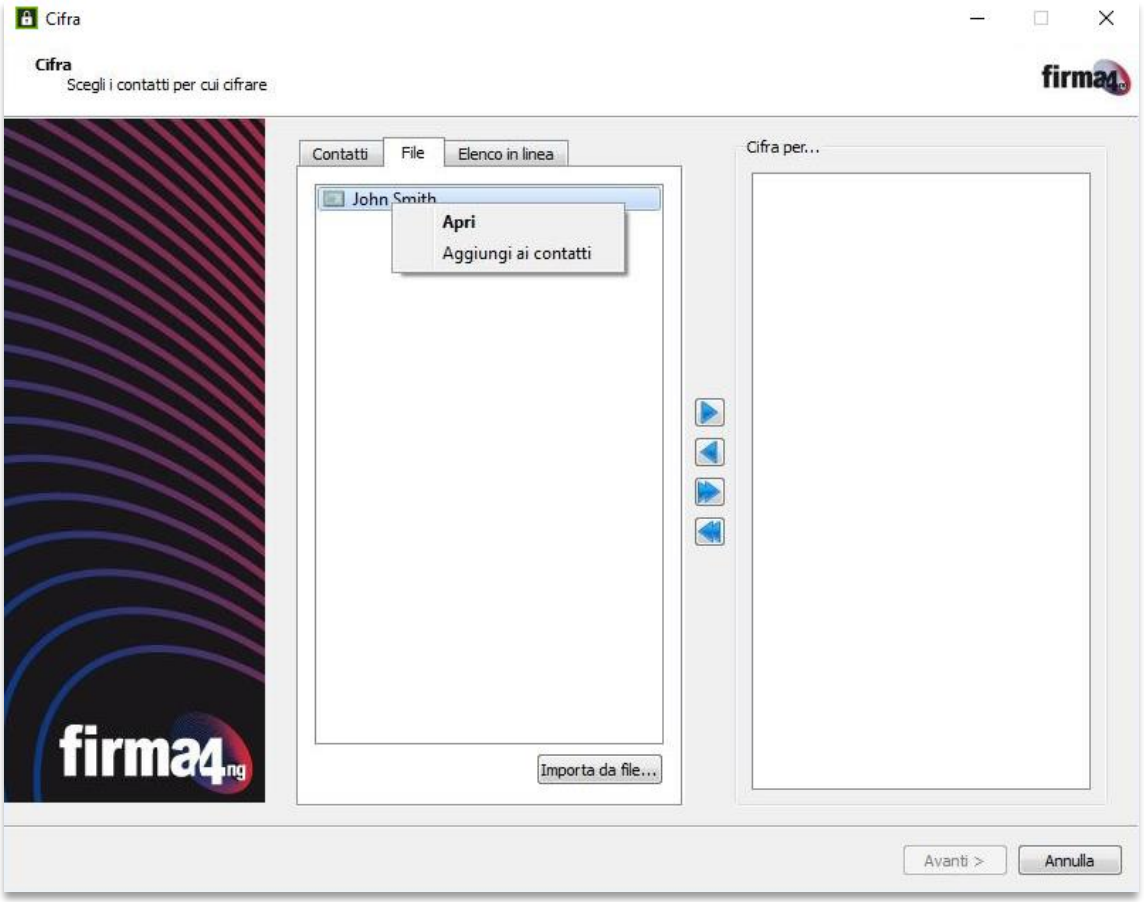


Figura 51

Al temine delle operazioni di caricamento dei certificati, per cifrare un documento selezionare della sezione "Contatti" il certificato da utilizzare presente e cliccare il pulsante con la freccetta rivolta a destra ( ) per spostarlo nella sezione **"Cifra per…"** (Figura 52).

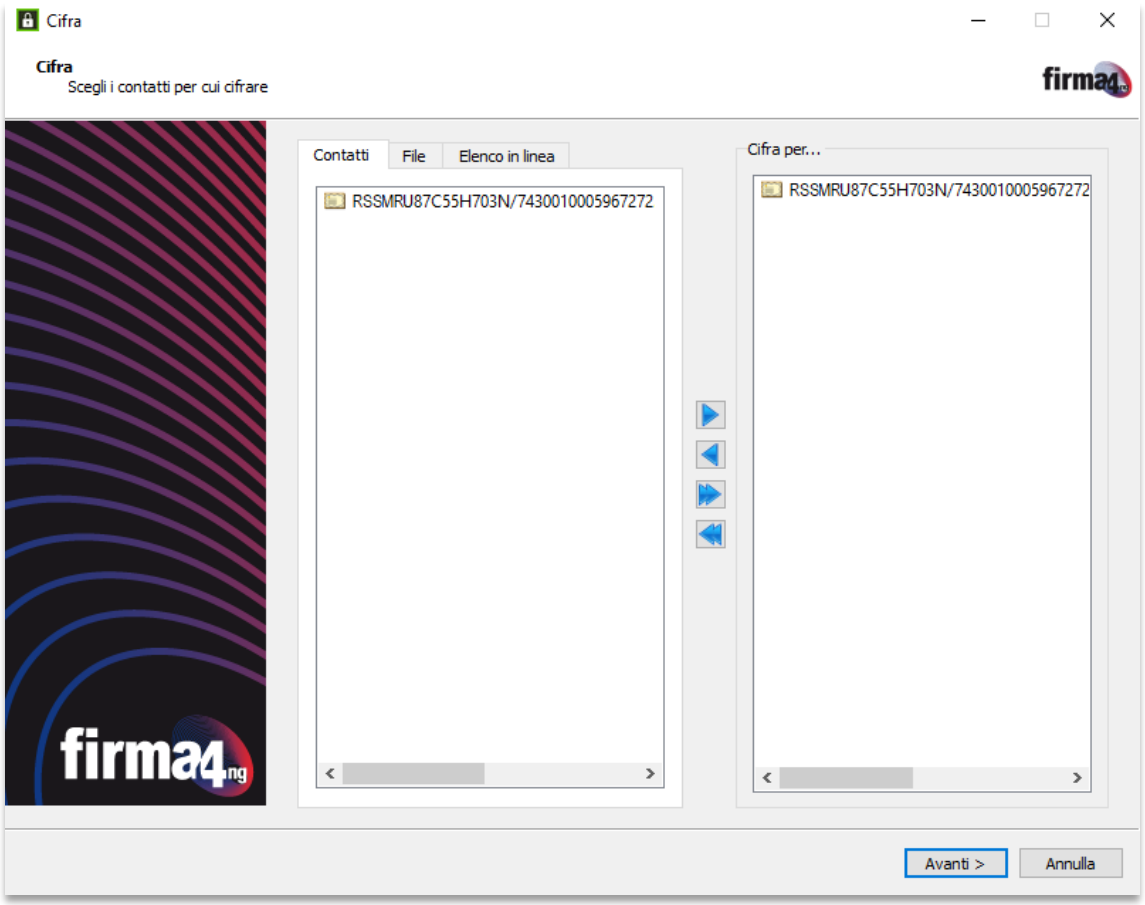


Figura 52

È possibile aggiungere o rimuovere i contatti per cui si intende cifrare il documento utilizzando i pulsanti posti al centro delle due sezioni:

 Per aggiungere il contatto selezionato alla lista dei certificati con cui cifrare il documento;

 Per rimuovere il contatto selezionato dalla lista dei certificati con cui cifrare il documento;

 Per aggiungere tutti i contatti della lista alla lista dei certificati con cui cifrare il documento; il documento verrà cifrato per tutti i destinatari indicati;

 Per rimuovere tutti i contatti dalla lista dei certificati con cui cifrare il documento.

Al termine delle modifiche, cliccare su "Avanti" per continuare.

FASE 3

Dopo aver selezionato un contatto, appare la schermata in cui selezionare le opzioni da utilizzare per la cifratura del documento (Figura 53).

Figura 53

Nella schermata è possibile:

- Scegliere la cartella di destinazione e il nome con cui verrà salvato il documento cifrato, cliccando sul pulsante **"..."**;

- Selezionare l'algoritmo da utilizzare per cifrare fra quelli elencati nel menu a tendina (DES-EDE3-CBC oppure AES-256-CBC);
  Nota: per maggiore sicurezza si consiglia di utilizzare l'algoritmo AES-256-CBC;

- Spuntare la casella **"Salva in formato PEM"** per salvare il documento cifrato in formato PEM;

- Spuntare la casella **"Distruggi il documento originale"** per cancellare definitivamente dal PC il documento originale al termine dell'operazione di cifratura.
- **Nota**: attivando questa funzione il file originale non potrà più essere recuperato.

Cliccare "Avanti" per procedere con la cifratura del documento; al termine dell'operazione appare una schermata con l'esito e la cartella di destinazione in cui è stato salvato il documento cifrato (Figura 54). Cliccare su "Termina" per chiudere la schermata.

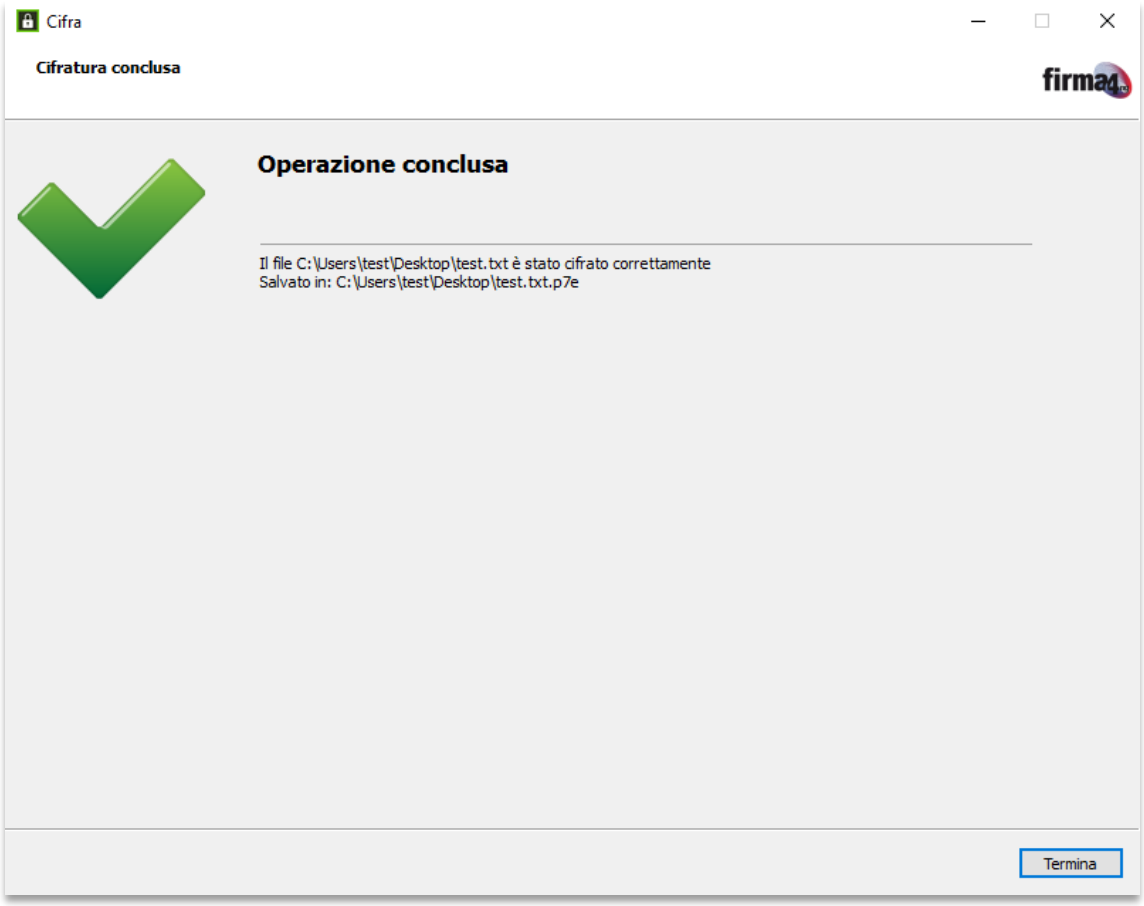


Figura 54

8.2 Decifratura

Al pulsante **"Decifra"** corrisponde la funzione di cifratura di uno o più documenti.

FASE 1

A partire dal menu secondario "Applicazioni" (Figura 46), è possibile avviare l'operazione di decifratura attraverso una delle seguenti modalità:

• Selezionando e trascinando il documento sul pulsante "Decifra" presente nel menu secondario (drag&drop);

• Cliccando sul pulsante "Decifra" presente nel menu secondario e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 55).

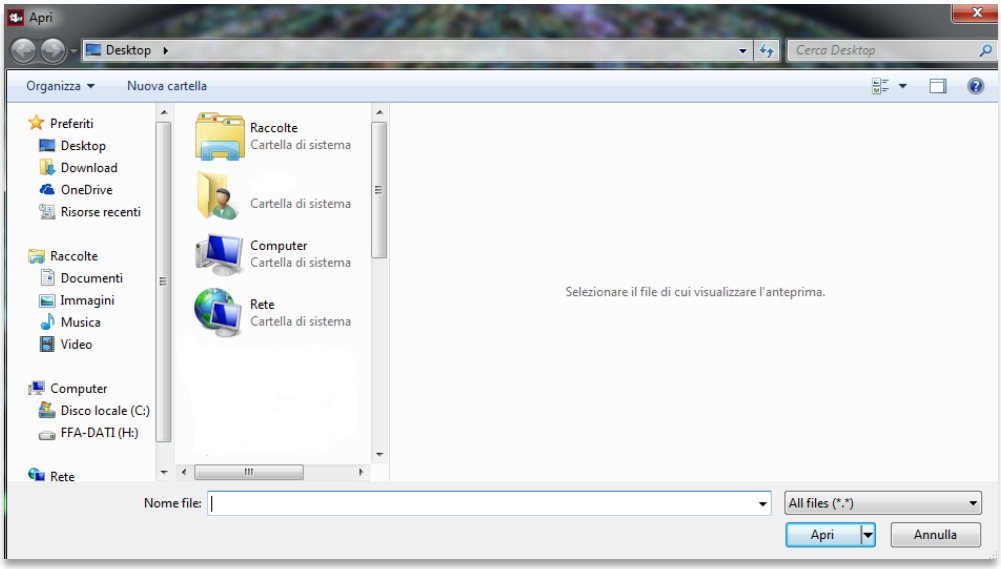


Figura 55

Attendere il caricamento dell'operazione.

FASE 2

Se è presente il certificato con cui è possibile decifrare il documento, si apre la schermata nella quale inserire il PIN del dispositivo (Figura 56). Inserire il PIN, poi cliccare su "Avanti" per procedere alla decifratura del documento.

Figura 56

FASE 3

Attendere l'analisi del file.

Al termine dell'analisi viene riportato l'esito dell'operazione. In caso di esito positivo, è possibile aprire il documento appena decifrato cliccando su "Apri contenuto" oppure salvarlo sul proprio PC cliccando su "Salva contenuto…".

Per chiudere la finestra "Decifra" cliccare su "Termina".

8.3 Storico

Cliccando sul pulsante **"Storico"** è possibile accedere alla cronologia delle attività svolte. Scegliere il tipo di attività da visualizzare selezionando in alto a sinistra una cartella tra "Documenti" e "Operazioni" (Figura 57).

- Nella cartella **"Documenti"** sono elencati i file che sono stati firmati digitalmente. L'utente può scegliere di aprire, eliminare o condividere ciascun file.
- Nella cartella **"Operazioni"** vengono elencate le attività di gestione e configurazione, ad esempio le operazioni di cambio PIN, sblocco PIN o eventuali autenticazioni effettuate sui servizi online (es. accesso al portale INPS). L'utente può visualizzare maggiori informazioni o eliminare ciascuna operazione della lista.

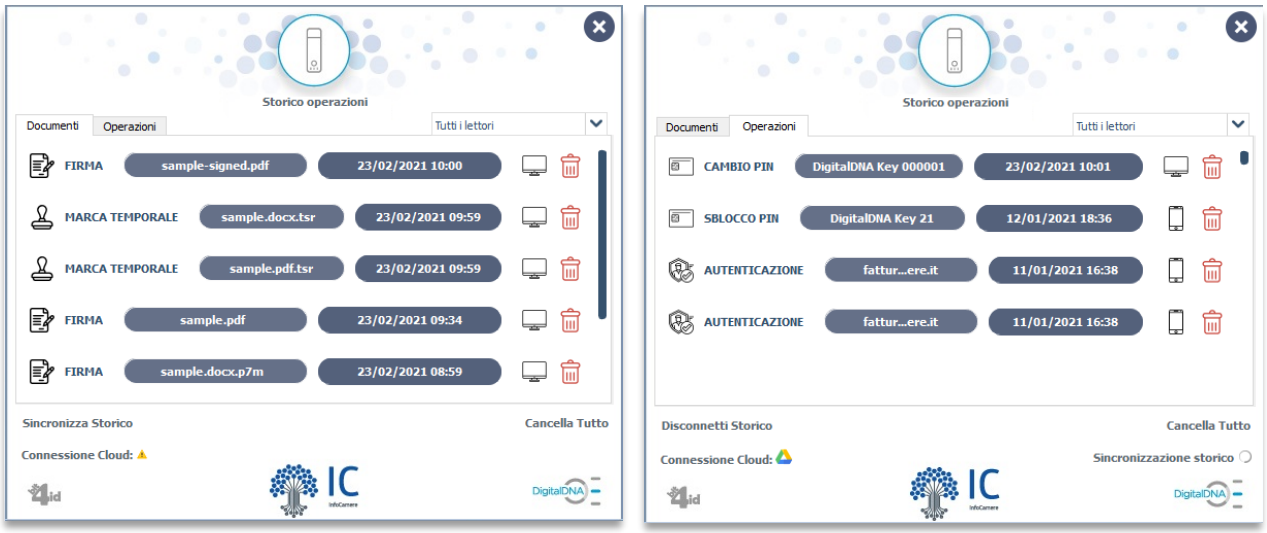


Figura 57

Attraverso la tendina in alto a destra è possibile selezionare per quale dispositivo si vuole visualizzare lo Storico. Per visualizzare le attività di tutti i dispositivi utilizzati, selezionare "Tutti i lettori".

Cliccando sulla voce in basso a sinistra **"Sincronizza Storico"** è possibile sincronizzare lo Storico con un account di archiviazione in cloud Google Drive o Dropbox. Quando lo Storico è sincronizzato a un account, appare l'icona corrispondente accanto alla voce "Configurazione Cloud". La sincronizzazione può essere annullata in qualunque momento cliccando su "Disconnetti Storico" (Figura 58).

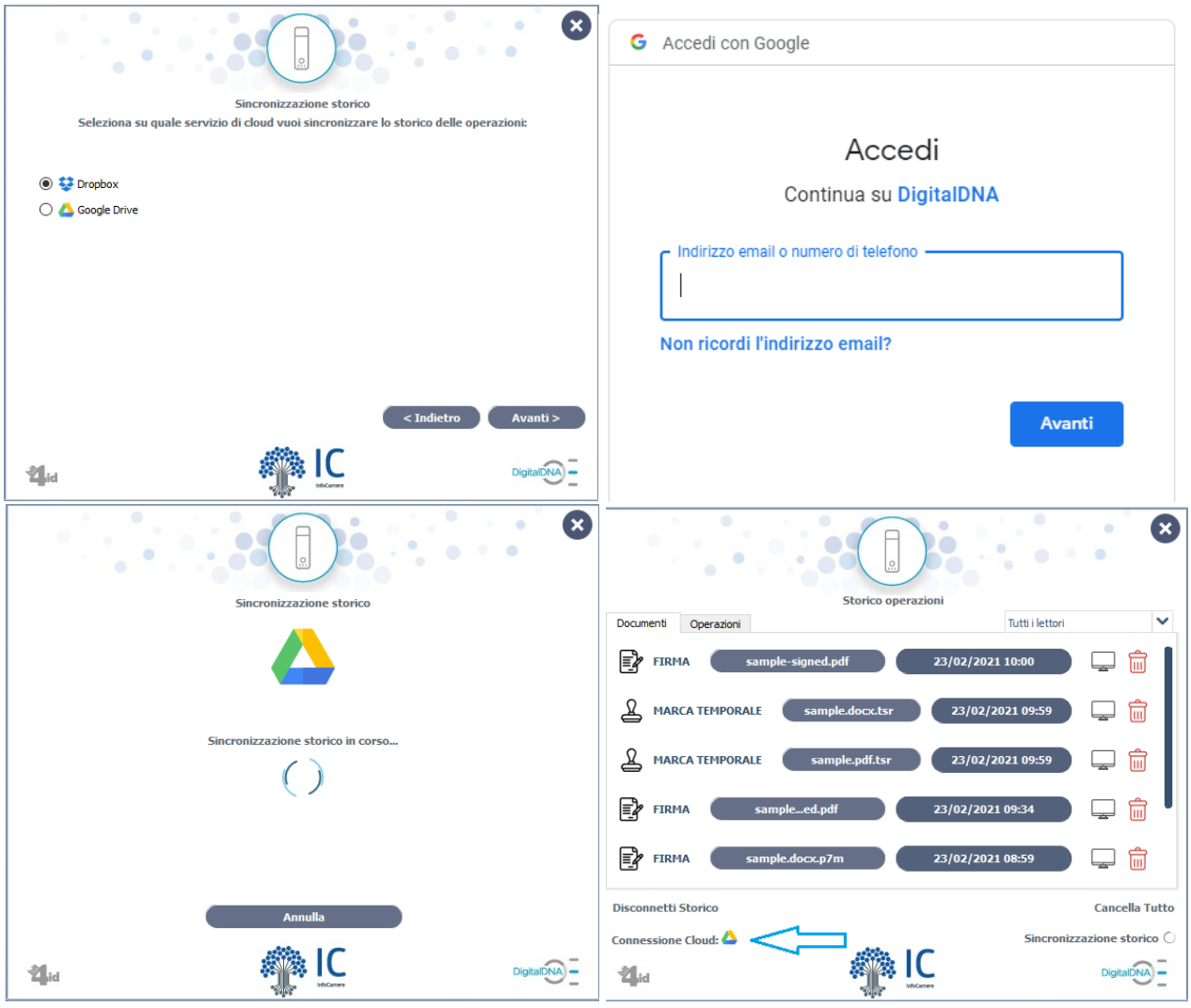


Figura 58

Per eliminare tutte le attività memorizzate nello Storico, cliccare sulla voce in basso a destra "Cancella tutto".

8.4 Impostazioni

Cliccando sul pulsante **"Impostazioni"** presente nel menu secondario "Applicazioni" (Figura 46) si apre la finestra per la configurazione di *firma4ng*.

8.4.1 Generale

Nella sezione "Generale" (Figura 59) è possibile effettuare le seguenti operazioni:

- Cancella cache CRL: permette di cancellare le CRL (Certificate Revocation Lists, contenenti la lista dei certificati revocati e/o sospesi) salvate localmente sul PC. Per le operazioni di verifica successive a tale cancellazione sarà necessario scaricare e salvare in locale le CRL;
- Configurazione di default: ripristina la configurazione iniziale dell'applicazione;
- Avvia aggiornamento del software: avviare manualmente l'aggiornamento del software;
- Avvia aggiornamento TSL: avviare manualmente l'aggiornamento della TSL.

Al termine delle modifiche, cliccare su "Salva".

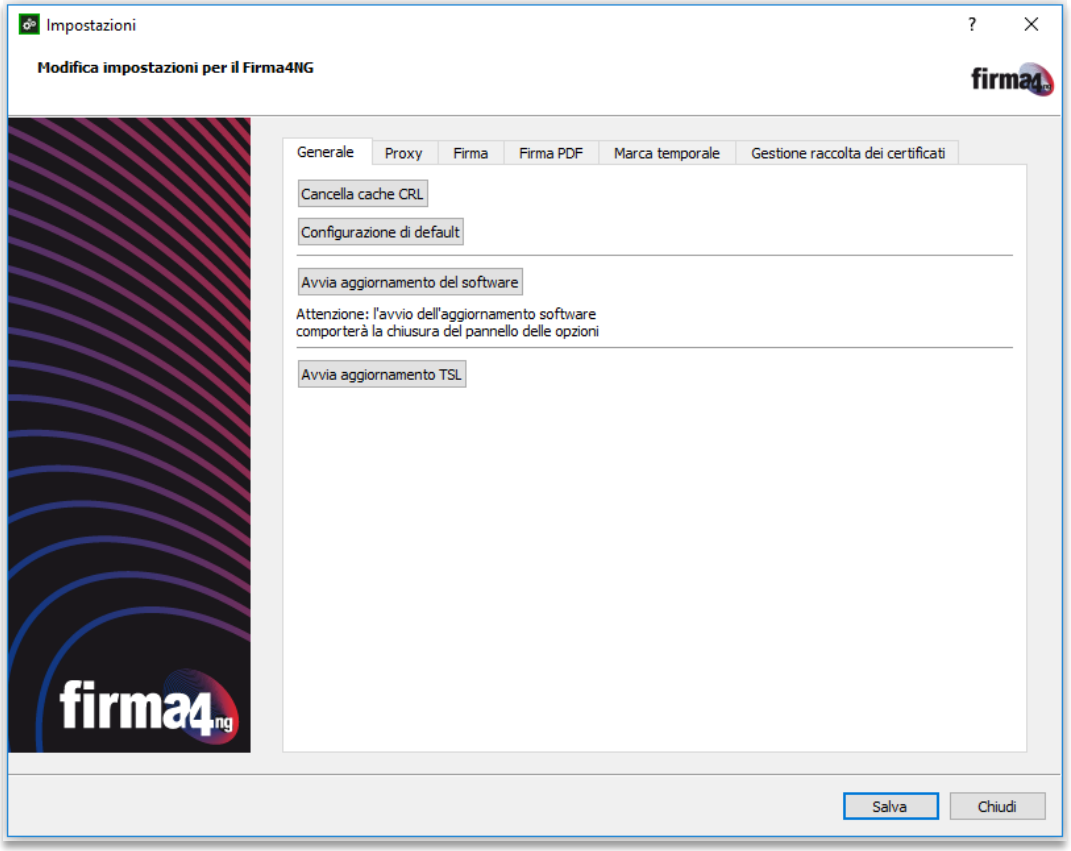


Figura 59

8.4.2 Proxy

Nella sezione "Proxy" (Figura 60) è possibile configurare un Proxy HTTP o LDAP. Per ciascuna delle due configurazioni (Proxy generico e Proxy LDAP) è possibile selezionare le seguenti opzioni:

- Nessun proxy: se selezionato non viene utilizzato nessun proxy;
- Configurazione manuale: se si desidera configurare manualmente i parametri per l'utilizzo del proxy specificando 'Tipo', 'Host' e 'Porta';

Le credenziali di accesso presenti nella sezione si riferiscono ai valori nome utente e password per l'autenticazione al proxy. Se non specificate in fase di configurazione, le credenziali verranno richieste solo se è necessaria l'autenticazione al proxy.

Nella sezione di configurazione 'Proxy LDAP' è possibile, inoltre, selezionare l'opzione "Usa la configurazione generica" per utilizzare la stessa configurazione specificata nella sezione 'Proxy generico'.

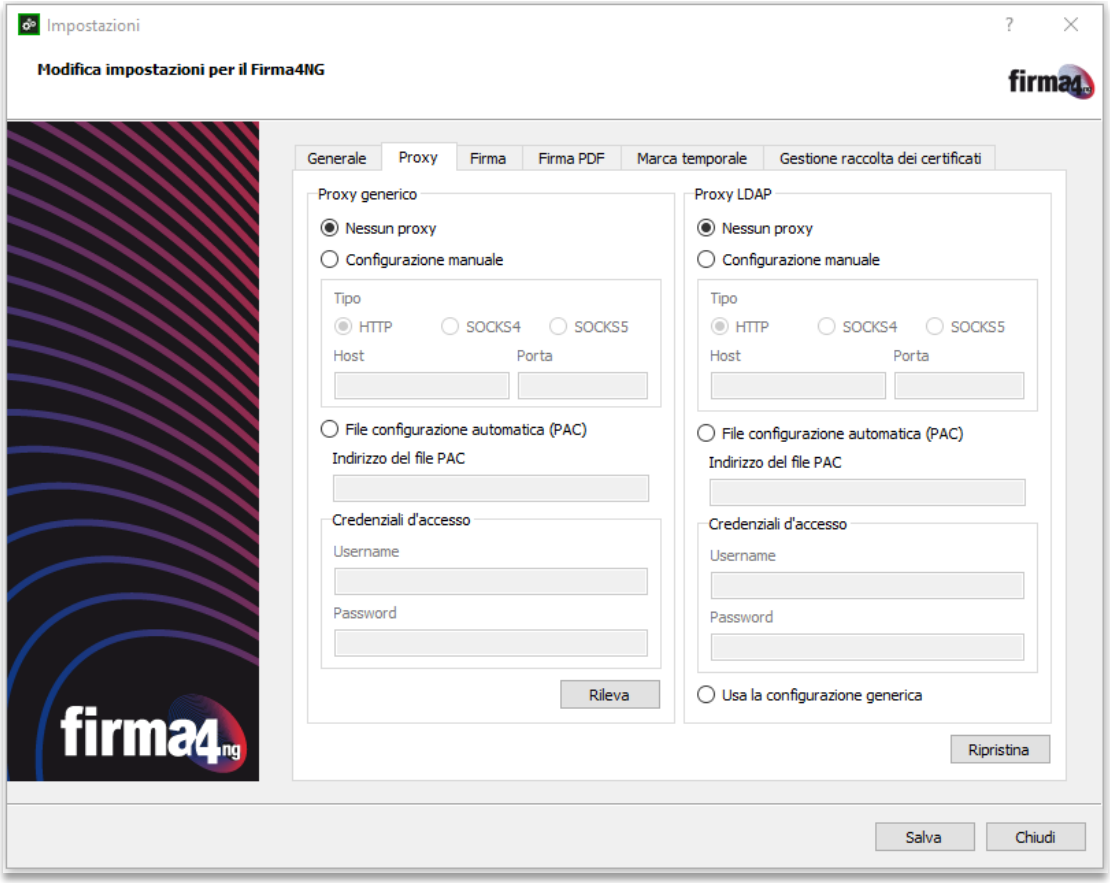


Figura 60

Per ripristinare la configurazione iniziale, cliccare su "Ripristina".

Al termine delle modifiche, cliccare su "Salva".

8.4.3 Firma

Nella sezione "Firma" (Figura 61) è possibile configurare il formato in cui verranno salvati i documenti firmati, scegliendo tra:

- In funzione dell'input: formato stabilito in base alla tipologia di documento da firmare;
- Firma P7M/Cades;
- Firma PDF;
- Firma XML.

È anche possibile scegliere la cartella di destinazione in cui salvare i documenti firmati con la procedura di firma multipla, cliccando su "Cerca…"

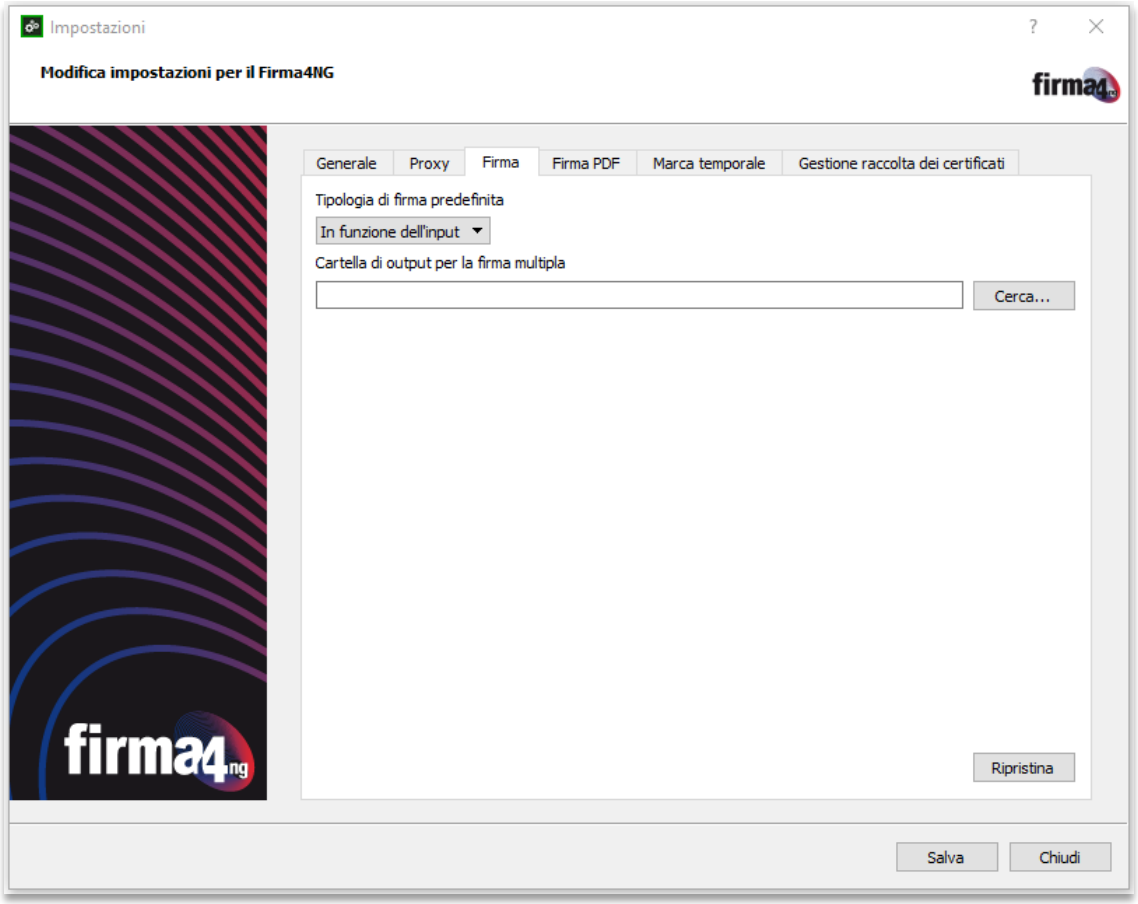


Figura 61

Per ripristinare la configurazione iniziale di *firma4ng*, cliccare su "Ripristina".

Al termine delle modifiche, cliccare su "Salva".

8.4.4 Firma PDF

Nella sezione "Firma PDF" (Figura 62) è possibile definire la configurazione standard da utilizzare per apporre la firma grafica in formato PDF, personalizzando i valori dei seguenti campi:

- Posizione
- Altezza
- Larghezza
- Pagina
- Località
- Ragione
- Timbro

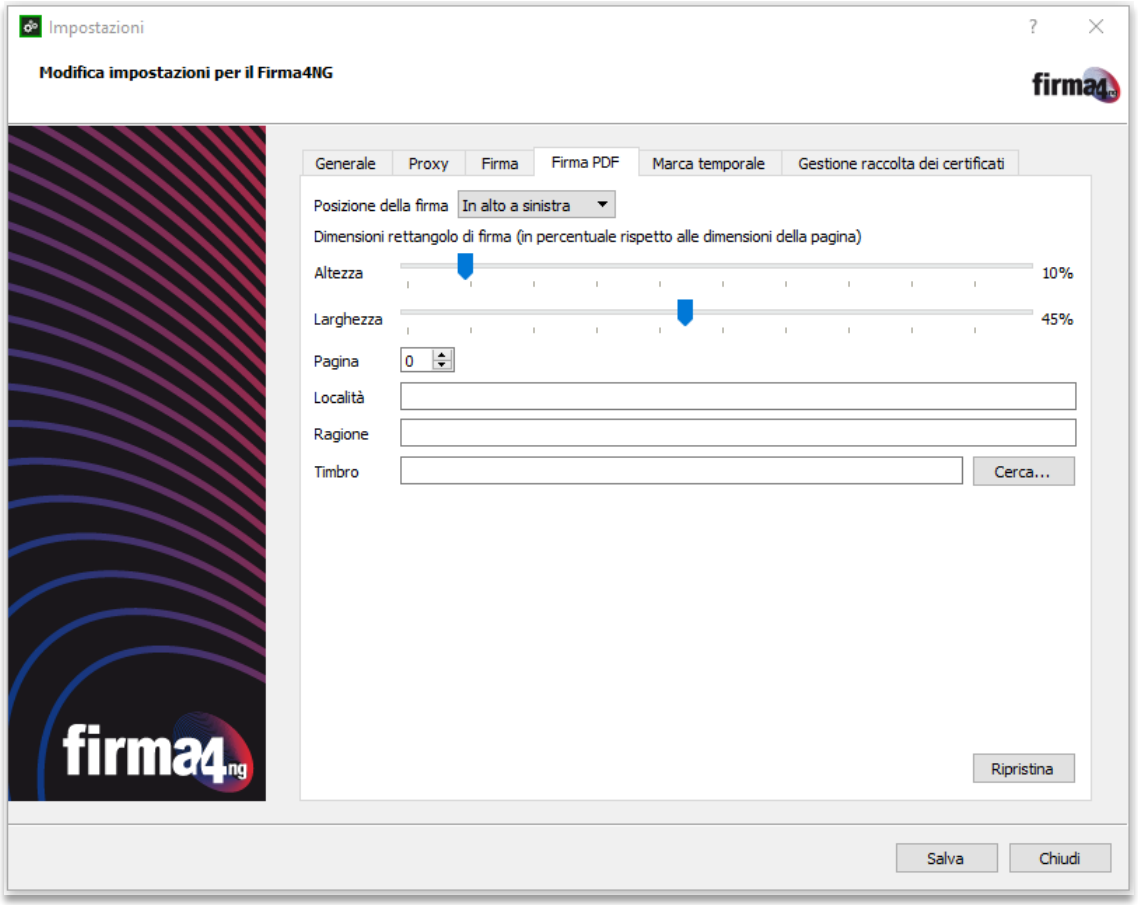


Figura 62

Per ripristinare la configurazione iniziale di *firma4ng*, cliccare su "Ripristina".

Al termine delle modifiche, cliccare su "Salva".

8.4.5 Marca temporale

Nella sezione "Marca temporale" (Figura 63) è possibile configurare il servizio di marcatura temporale da contattare per le richieste di marche temporali.

È possibile configurare nuovi servizi di marcatura temporale cliccando su "Nuovo" e valorizzando i parametri richiesti:

- Nome del servizio;
- Indirizzo della Time stamping authority;
- Username (opzionale);
- Password (opzionale);
- Policy OID (opzionale).

È anche possibile eliminare un servizio di marcatura temporale selezionandone il nome dall'elenco e cliccando su "Elimina".

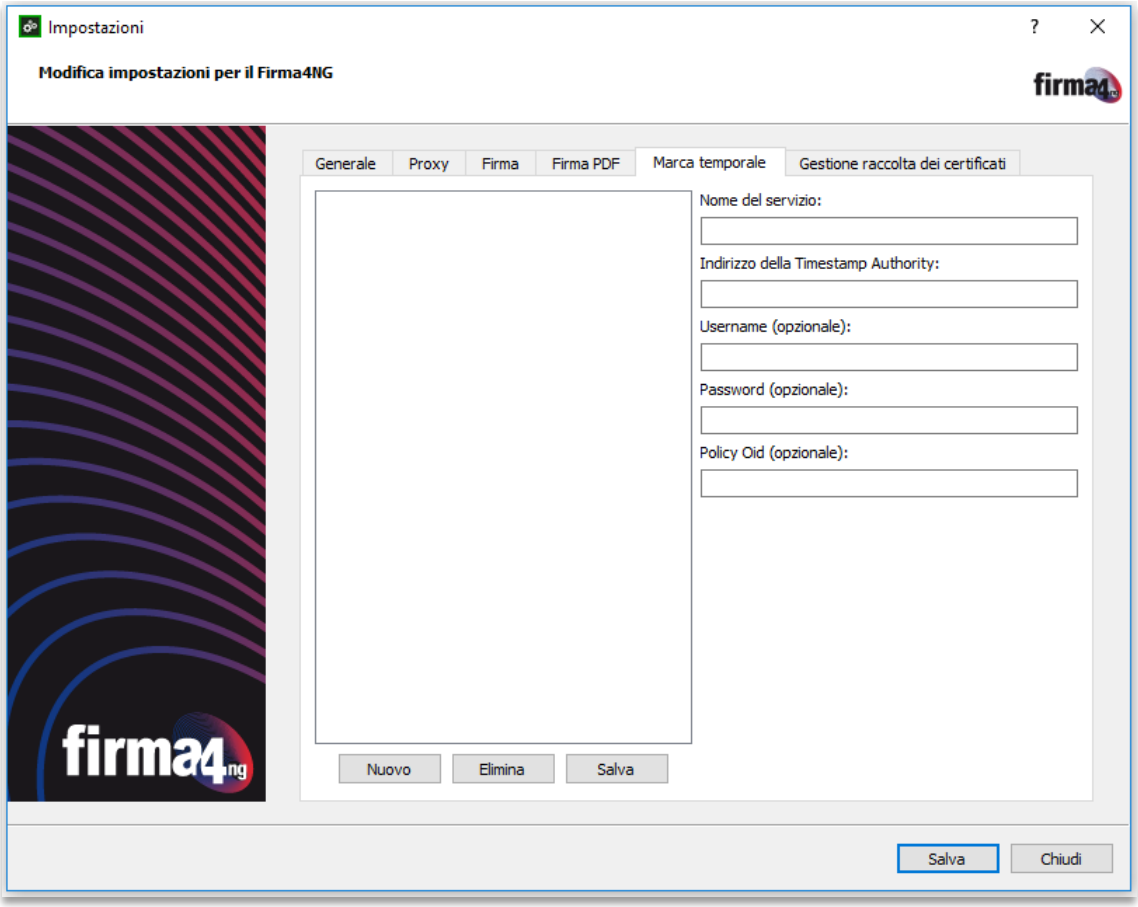


Figura 63

Al termine delle modifiche, cliccare su "Salva".

8.4.6 Gestione raccolta dei certificati

Nella sezione "Gestione raccolta dei certificati" (Figura 64) è possibile gestire l'archivio dei certificati utilizzato da *firma4ng*. In particolare, nell'area *"Raccolta certificati"* questi sono raggruppati nelle seguenti cartelle:

Affidabili: contiene certificati delle Autorità di Certificazione (CA) presenti nell'elenco pubblico tenuto da AgID;

TSA: contiene certificati delle Autorità di Certificazione del servizio di Marcatura temporale erogato dai vari Certificatori Accreditati;

Altre CA: contiene certificati di Autorità di Certificazione che seppure non presenti nell'elenco pubblico delle CA accreditate, sono reputati attendibili;

Contatti personali: contiene la lista dei certificati dei contatti per i quali cifrare i documenti.

Nell'area *"Importa da…"* è invece possibile caricare i certificati da *"File"* cliccando su *"Importa"*, oppure ricercarli sul Registro pubblico dei certificati tenuto dal Certificatore tramite il tab *"Servizio in linea"*, selezionando l'indirizzo LDAP e la base di ricerca. Una volta effettuata la ricerca, è possibile inserire i certificati trovati nella cartella "Contatti personali" utilizzando gli appositi pulsanti nella parte centrale della schermata.

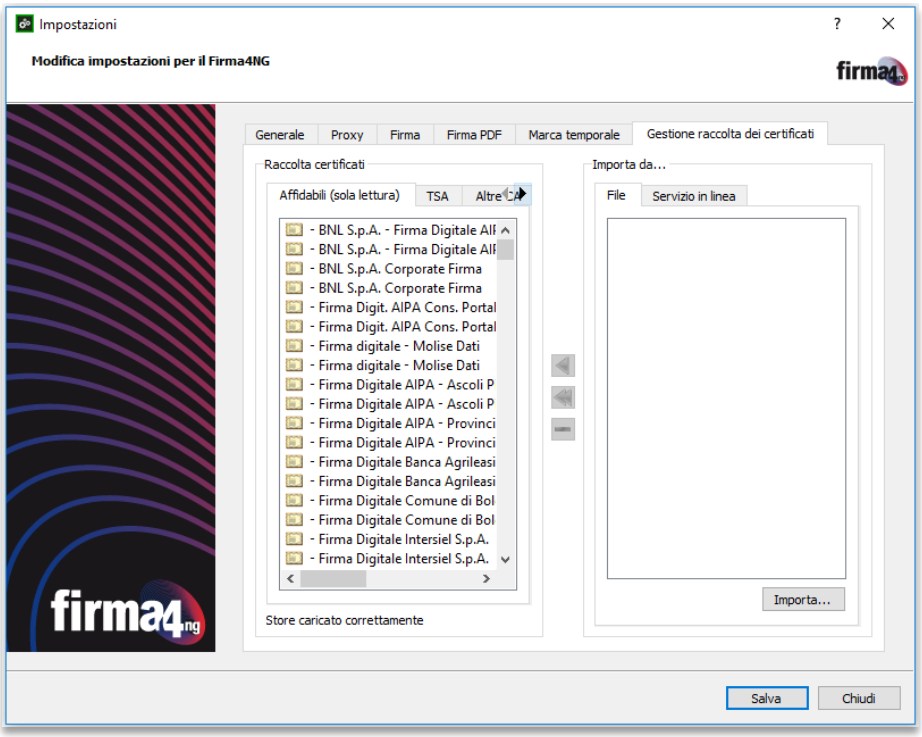


Figura 64

Al termine delle modifiche, cliccare su "Salva".

9. GESTIONE DigitalDNA

Cliccando sul pulsante **"Gestione DigitalDNA"** presente nel menu principale (Figura 1), si apre un menu secondario (Figura 65) che contiene le seguenti voci:

- Associazione
- Diagnostica
- Aggiornamento Firmware

Figura 65

9.1 Associazione via Bluetooth

Cliccando sul pulsante **"Associazione"** si avvia automaticamente la configurazione del token DigitalDNA che si vuole utilizzare via Bluetooth. La procedura guidata illustra in poche schermate i passaggi da seguire per abbinare correttamente il dispositivo al software *firma4ng* (Figura 66).*

1. Accendere il token DigitalDNA
2. Selezionare dall'elenco dei dispositivi rilevati la DigitalDNA Key da associare
3. Tenere premuto il pulsante del token fino a quando il LED inizia a lampeggiare
4. Fatto!

Figura 66

Per associare un nuovo dispositivo cliccare su "Ripeti abbinamento". Una volta conclusa l'associazione, cliccare sulla "X" in alto a destra per chiudere la schermata.

* Funzione disponibile dopo aver abilitato la connessione Bluetooth sul computer in uso.

9.1.1 Riconoscimento automatico via Bluetooth

Quando un token DigitalDNA si trova **acceso in prossimità del computer** viene automaticamente riconosciuto dal computer tramite il segnale Bluetooth, anche se il software *firma4ng* è momentaneamente chiuso*.

Il computer mostra una notifica in basso a destra con cui l'utente può scegliere come proseguire: associando il token o ignorando il riconoscimento automatico (Figura 67).

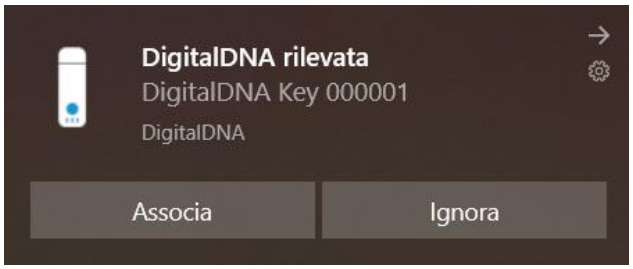


Figura 67

- Cliccando su **Associa** si apre automaticamente la procedura di Associazione del software *firma4ng* descritta nel paragrafo 9.1 e in Figura 66
- Cliccando su **Ignora** l'utente chiude la notifica senza avviare l'associazione del token DigitalDNA.

* Funzione disponibile dopo aver abilitato la connessione Bluetooth sul computer in uso.

9.2 Diagnostica

Cliccando sul pulsante **"Diagnostica"** si avvia automaticamente il tool di diagnostica, ovvero lo strumento che consente di analizzare lo stato dei dispositivi DigitalDNA.

Prima di iniziare la scansione, verificare che il dispositivo sia correttamente collegato alla porta USB del computer e che il tasto della batteria sul dispositivo sia impostato su ON. Quindi cliccare su "*Avvia il tool di diagnostica del dispositivo*" (Figura 68).

Figura 68

Il tool di diagnostica esegue una scansione per verificare il corretto funzionamento del dispositivo e per identificare potenziali problemi. Attendere il completamento della scansione (Figura 69).

Figura 69

Al termine della scansione, vengono mostrati i risultati dell'analisi effettuata sul dispositivo (Figura 70). Attraverso lo strumento di diagnostica è possibile verificare sia le condizioni generali e le prestazioni del token DigitalDNA collegato (es. stato della batteria, funzionamento Bluetooth), sia la corretta configurazione del computer in uso, andando a controllare lo stato di driver, middleware, connessione internet, chiavi di registro, aggiornamenti necessari o antivirus attivi (questi ultimi, infatti, potrebbero interferire con il normale funzionamento del software *firma4ng*). Eventuali anomalie o errori di funzionamento vengono segnalati con la scritta in rosso "*Errore*" e vengono dettagliati nella sezione in basso. Cliccare su "Test del buzzer" per verificare il corretto funzionamento del segnalatore acustico.

Figura 70

A seguito della scansione, il tool di diagnostica genera automaticamente un report con il riepilogo dei risultati. Cliccando sul pulsante "Stampa report" (Figura 70) è possibile salvare e stampare il report della diagnostica effettuata sul dispositivo. Dopo aver cliccato sul pulsante, selezionare la cartella di destinazione sul proprio PC per salvare il file, quindi aprire il PDF e avviare la stampa (Figura 71).

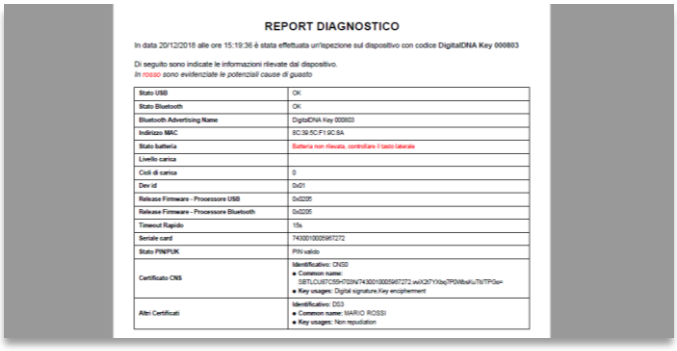


Figura 71

9.3 Aggiornamento Firmware

Cliccando sul pulsante **"Aggiornamento Firmware"** è possibile verificare l'esistenza di una nuova versione del firmware da installare sul PC in uso.

Nel caso in cui risulti disponibile una nuova versione del firmware, sarà possibile avviare manualmente l'installazione dell'aggiornamento. Al contrario, se il firmware risulta già aggiornato all'ultima versione, non sono necessarie ulteriori azioni da parte dell'utente.

10. CASSETTO DIGITALE DELL'IMPRENDITORE

Cliccando sul pulsante **"Cassetto digitale dell'imprenditore"** presente nel menu principale (Figura 1) si apre automaticamente il browser Internet sulla pagina web *impresa.italia.it* dedicata al Cassetto digitale, il servizio per il cittadino imprenditore per accedere tramite CNS o SPID ai documenti (visure, atti, bilanci) e alle pratiche della propria impresa (Figura 72).

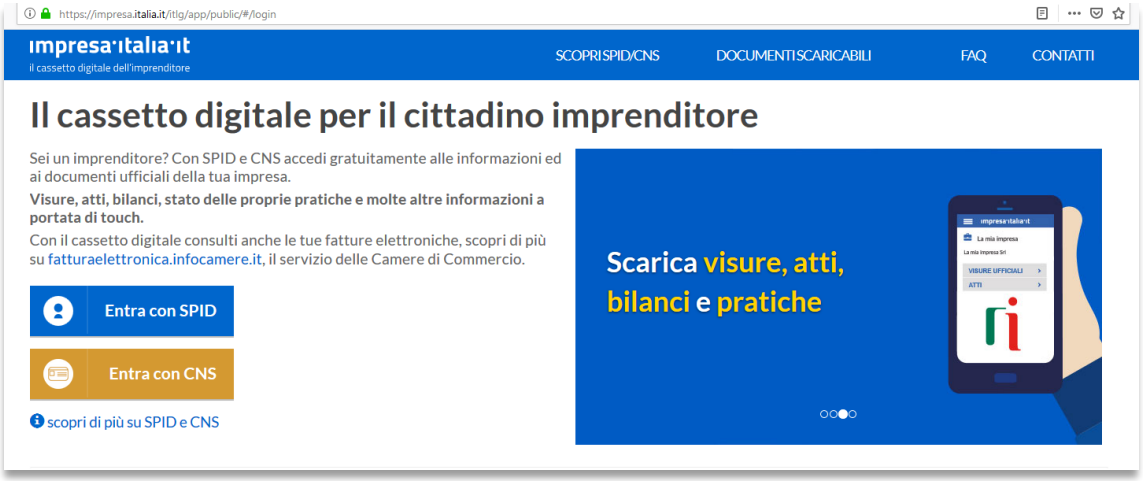


Figura 72