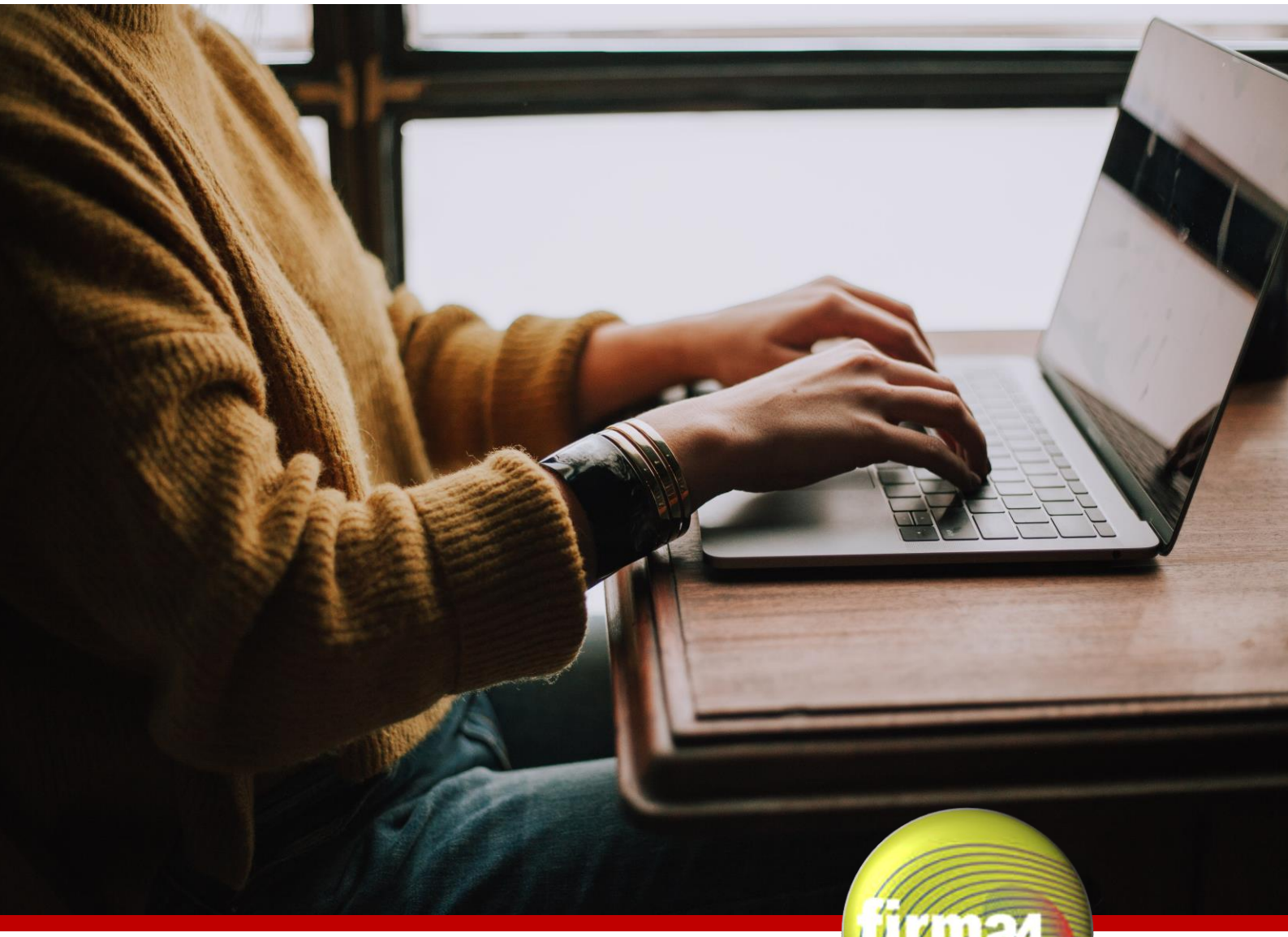

# BIT4ID firma4ng

## Manuale Utente

RELEASE 4.0 – 2022-04-15

# SOMMARIO

# INDICE DELLE FIGURE

# INDICE DELLE TABELLE

# INTRODUZIONE

## CHI SIAMO

Bit4id - Fondata nel 2004 con sede in **Italia**, nasciamo per rendere semplici, sicure e omogenee le tecnologie per l'autenticazione, la firma digitale e la cifratura. Siamo riusciti ad affermarci in molti paesi sia europei sia extra-europei, vantando la presenza diretta in Spagna, Portogallo, Inghilterra, Polonia, Macao e Perù.

Fin dal suo inizio Bit4id ha agito come abilitatore tecnologico. In quanto tale, tutto il software prodotto incentrato sugli utenti, e fa della facilità d'uso il proprio obiettivo. **Universal Middleware** (abbreviato in UMW) è il nostro prodotto di punta, implementato con un'interfaccia intuitiva e tutte le funzionalità sono disponibili a colpo d'occhio.

Grazie al nostro nuovo token DigitalDNA Key, basata sulla tecnologia PKI, ogni azienda o service provider può implementare l'**Identità Digitale** in modo immediato, semplice e soprattutto facilmente scalabile per vincere le nuove sfide.

## SCOPO DEL DOCUMENTO

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

- Apposizione di firme digitali in formato .P7M;
- Apposizione di firme digitali in formato .PDF;
- Apposizione di firme digitali in formato .XML;
- 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;
- Cifrare e decifrare file;
- Creare una cartella cifrata;
- Gestione PIN e PUK del dispositivo crittografico (smart card o token USB).

# FIRMA4NG: CARATTERISTICHE DEL SOFTWARE

## DISTRIBUZIONI DISPONIBILI E REQUISITI SOFTWARE

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

- **firma4ng portable**, su token USB, compatibile con tutti i sistemi operativi:
  - Microsoft Windows 8, 8.1, 10, 11 (in tutte le versioni, sia 32 che 64 bit);
  - Mac OS X (10.9.5 e superiori);
  - Linux (Ubuntu: 14.04 LTS, 16.04 LTS; Fedora 23,24);

- **firma4ng per Windows**, installazione disponibile per ambienti desktop Windows (8, 8.1, 10, 11 in tutte le versioni sia 32 che 64 bit);

- **firma4ng per Mac OS X**, installazione disponibile per ambienti desktop Mac OS X (10.9.5 e superiori, sia 32 che 64 bit);

- **firma4ng per Linux 32**, distribuito come archivio tar.gz per ambienti desktop Linux (Ubuntu: 14.04 LTS, 16.04 LTS; Fedora 23,24);

- **firma4ng per Linux 64**, distribuito come archivio tar.gz per ambienti desktop Linux (Ubuntu: 14.04 LTS, 16.04 LTS; Fedora 23,24).

A seconda della versione di interesse, di seguito sono riportate le diverse modalità di installazione ed avvio dell'applicazione.

## 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.

## FIRMA4NG PER WINDOWS

Per installare l'applicazione su sistemi operativi Windows (a 32 e 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.

## FIRMA4NG PER MAC OS X

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

## FIRMA4NG PER LINUX

Per installare l'applicazione su sistemi operativi Linux (32 e 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.

## AVVIO DEL FIRMA4NG

Una volta installato il software, è sufficiente fare doppio click sull'icona di avvio per aprire il programma di firma digitale. A questo punto apparirà sullo schermo il menu principale, riportato in Figura 1 a partire dal quale è possibile attivare tutte le funzionalità previste:

- Firmare un file, trascinandolo o cliccando sul bottone "Firma" (Figura 1);
- Verificare la firma di file, trascinandolo o cliccando sul bottone di "Verifica" (Figura 1);
- Apporre una marca temporale su un file, trascinandolo o cliccando sul bottone di "Marca Temporale" (Figura 1);
- Cifrare e decifrare un file o una cartella, accedendo al sottomenù visibile dopo aver cliccato sul bottone "Applicazioni" (Figura 2);
- Gestire il proprio token o smartcard, accedendo al sottomenù visibile dopo aver cliccato sul bottone "Gestione Token" (Figura 3).

Per ognuna di queste funzionalità appena menzionate è presente un paragrafo del manuale che ne dettaglia l'uso.


*Figura 1 – firma4ng – menu principale.*


*Figura 2 – firma4ng – sottomenù "Applicazioni".*


*Figura 3 – firma4ng – sottomenù "Gestione token".*

# FIRMA DIGITALE DI UN DOCUMENTO

Questa funzionalità permette di firmare digitalmente uno o più documenti con certificati elettronici.

La procedura da seguire è molto semplice e viene descritta nei sottoparagrafi che seguono. Prima di avviare l'operazione è bene controllare di aver inserito la smart card nel lettore o il token nella porta USB.

## FIRMA DI UNO O PIÙ DOCUMENTI

### Fase 1

È possibile avviare l'operazione di Firma in una delle seguenti modalità:

- Selezionando e trascinando (drag&drop) il/i documento/i o cartella sul bottone "Firma" (Figura 4);


*Figura 4 – firma4ng – drag&drop.*

- Cliccando sul bottone “Firma” (Figura 1) e selezionando il/i documento/i da firmare dalla finestra di navigazione del PC (Figura 5).

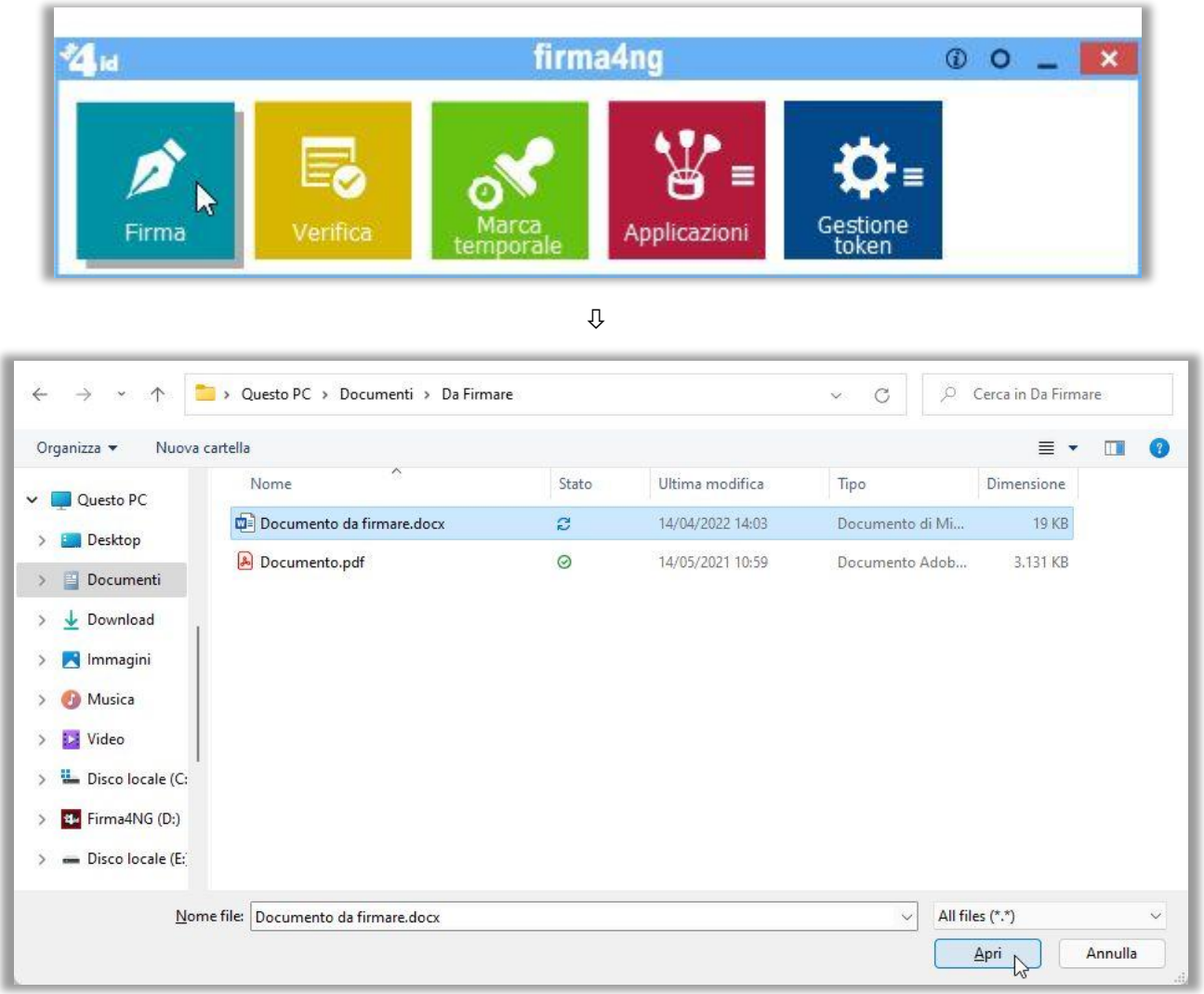


*Figura 5 – Selezione del file da firmare.*

## Fase 2

Attendere il caricamento dei certificati (Figura 6) contenuti nella smart card inserita nel lettore o nel token USB crittografico collegato al PC.

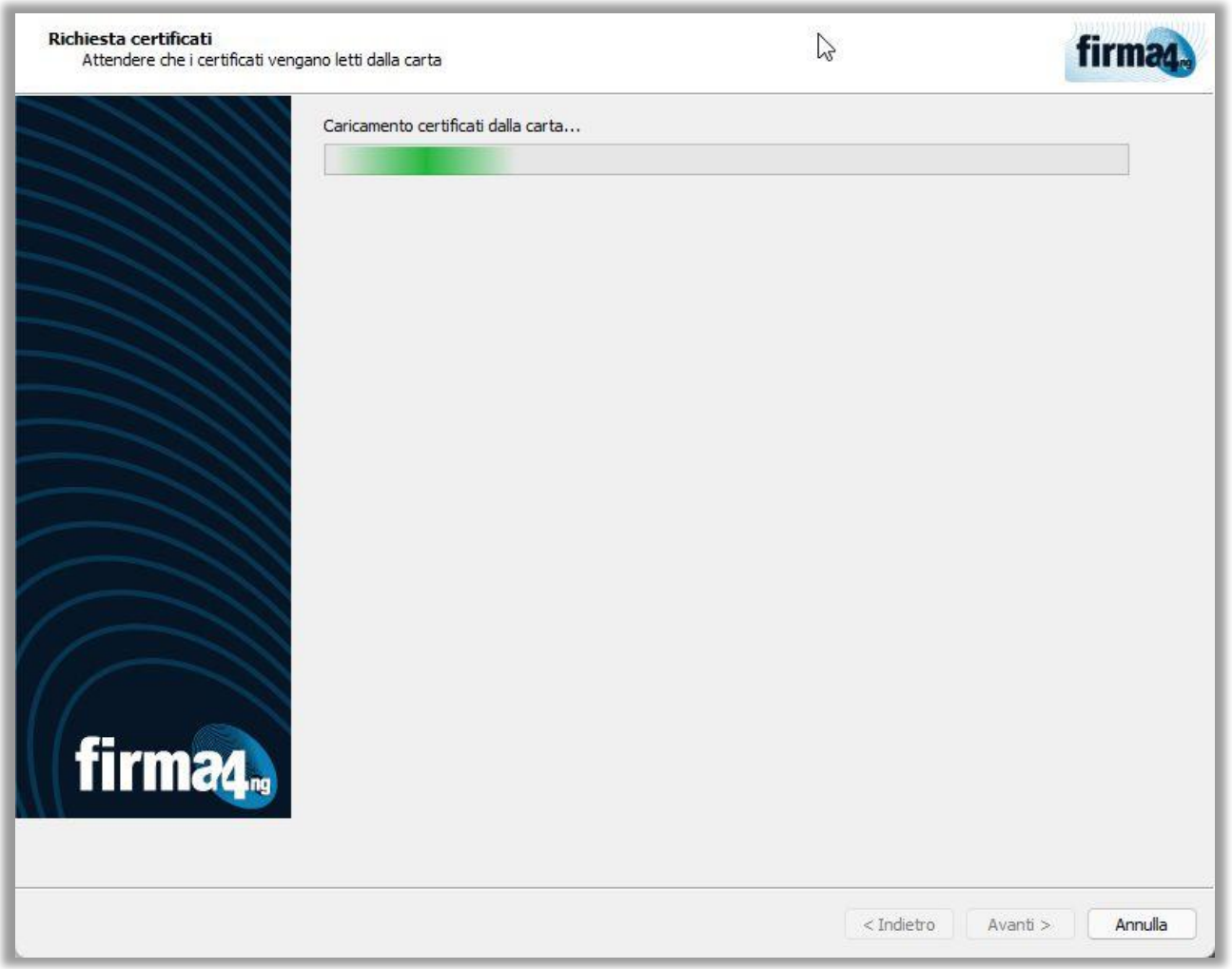


*Figura 6 – Caricamento certificati dai dispositivi crittografici collegati (smartcard/token).*

## Fase 3

Al termine del caricamento dei certificati, si apre la finestra di firma:

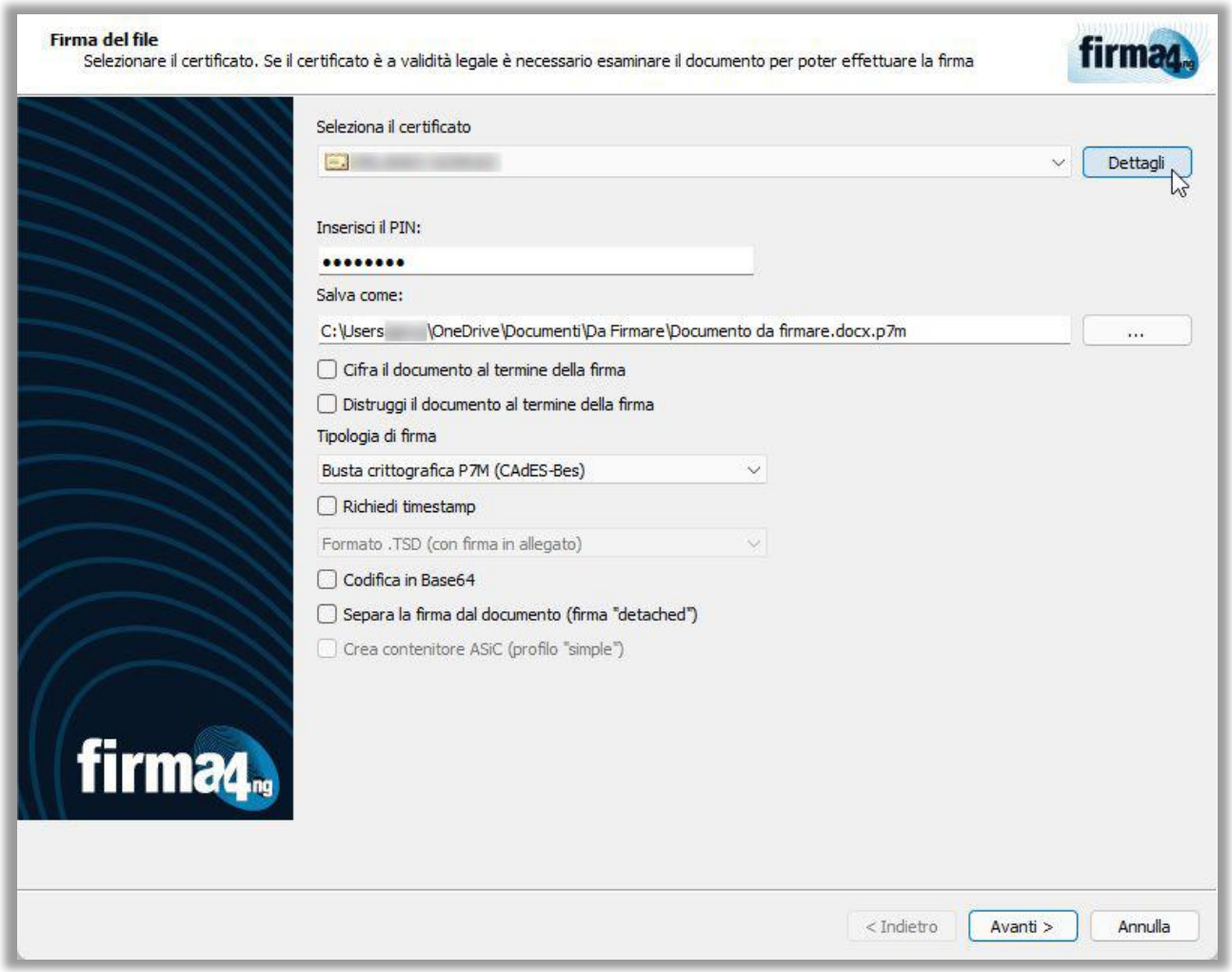


*Figura 7 – Interfaccia di firma.*

Viene mostrato come già selezionato il certificato per la firma digitale (o di "non ripudio").

*Nota*: per controllare che il certificato selezionato è quello di firma digitale, è possibile visualizzarne i dettagli cliccando sul bottone "Dettagli" (Figura 7).

Per procedere con l'operazione di firma occorre:

- Selezionare nell'apposito menù a tendina il certificato di firma digitale, facendo bene attenzione a selezionare quello indicato con NOME COGNOME;

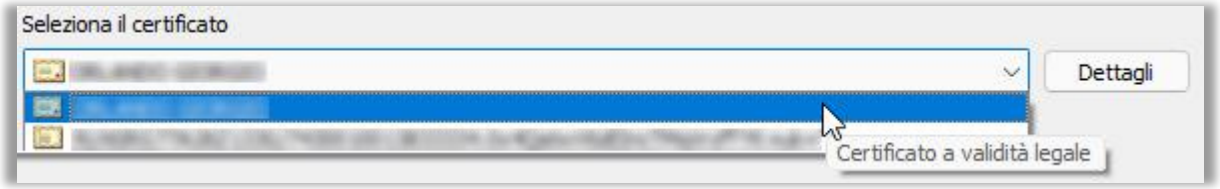


*Figura 8 – Selezione certificato.*

- Inserire il PIN della smart card o del token USB;

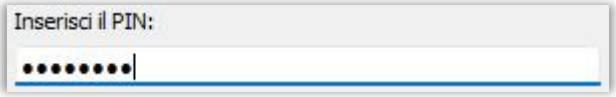


*Figura 9 – Inserisci PIN.*

- Selezionare la cartella in cui salvare il documento firmato cliccando sul bottone "…" della sezione "Salva come:" se si desidera modificare la cartella preimpostata (quella che contiene il documento originale);


*Figura 10 – Selezione Cartella.*

- Selezionare la tipologia di firma che si vuole apporre al documento dal menù a tendina. I formati di firma a disposizione sono (Figura 8):

  a) "Busta crittografica P7M (CAdES)" - formato sempre selezionabile, qualunque sia il tipo di documento da firmare;

  b) "Aggiungi la firma al PDF" - formato selezionabile solo nel caso in cui il documento da firmare sia in formato PDF (anche nella modalità di firma di più documenti, questo formato sarà presente solo se tutti i documenti selezionati sono esclusivamente documenti PDF);

c) “Documento XML” – formato sempre selezionabile, qualunque sia il tipo di documento da firmare (ma non nel caso in cui l’operazione di firma sia stata lanciata dai bottoni “Aggiungi firma” o “Aggiungi controfirma” presenti nella schermata di “Verifica” (Figura 1);

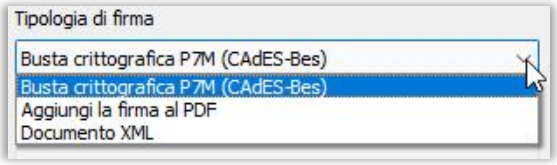


*Figura 11 – Tipologia di firma.*

- Se si vuole aggiungere una marca temporale sulla firma, spuntare la casella “Richiedi timestamp”. Proseguendo con l’operazione di firma sarà poi possibile selezionare o configurare il servizio da utilizzare per richiedere la marca temporale;

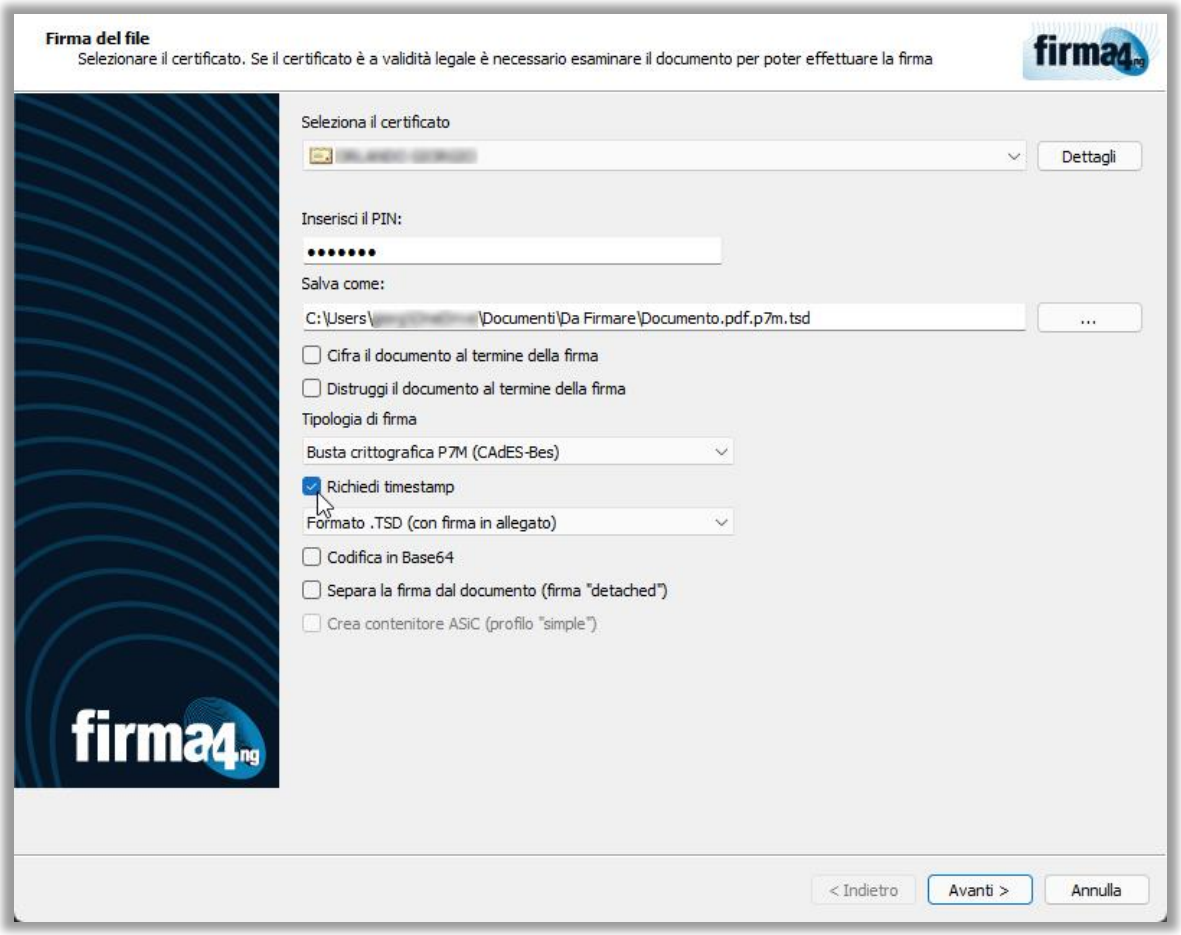


*Figura 12 – Tipologia di firma.*

- Cliccare su “Avanti” per avviare l’operazione di firma.

## Fase 4

- In caso di firma di un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante “Apri documento”.
  a) 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.”;
  b) Cliccare su “Avanti” per proseguire nell’operazione di firma.
- Qualora i documenti da firmare fossero più d’uno, occorre prendere visione del contenuto di ciascun documento che si sta per firmare cliccando sul collegamento ipertestuale rispettivo a ciascun titolo.
  a) Selezionare la checkbox “Dichiaro di aver preso visione dei documenti, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta.”;
  b) Cliccare su “Avanti” per proseguire nell’operazione di firma.

## Fase 5

Attendere che il documento selezionato venga firmato.

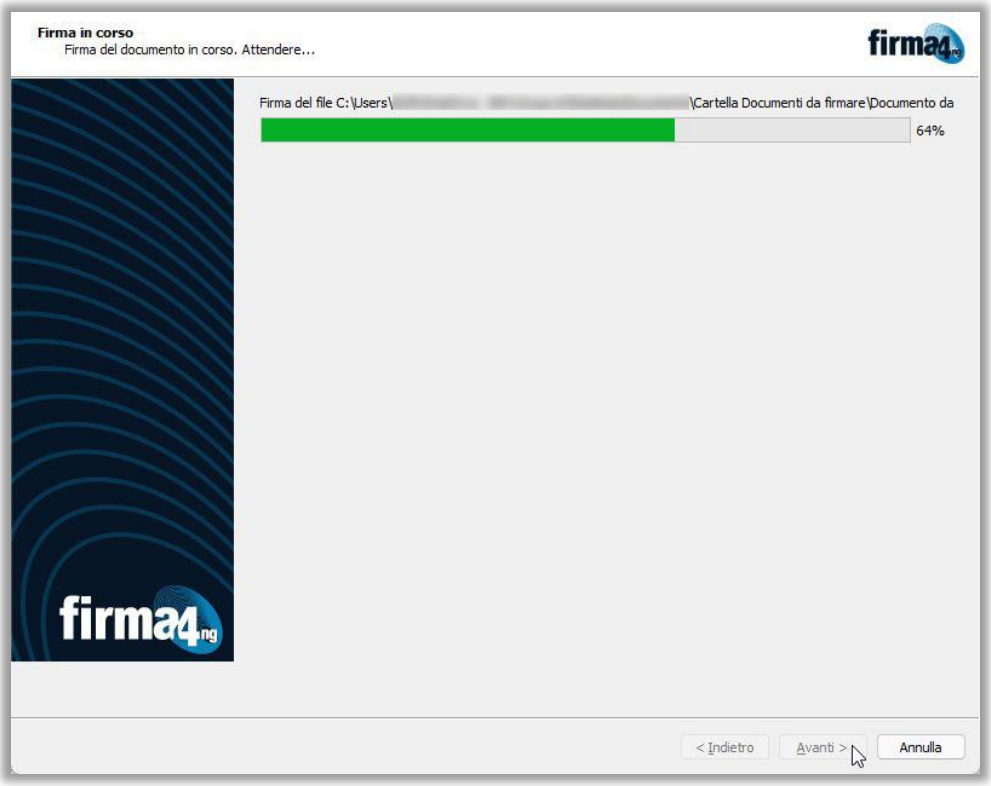


*Figura 13 – Fase di Firma.*

## Fase 6

Al termine dell'operazione di firma, il documento firmato verrà salvato in locale sul PC, all'indirizzo indicato nella schermata di esito della firma. Cliccando sull'indirizzo del documento firmato si avvierà l'operazione di "Verifica" della firma.

Per chiudere la schermata, cliccare sul bottone "Termina".

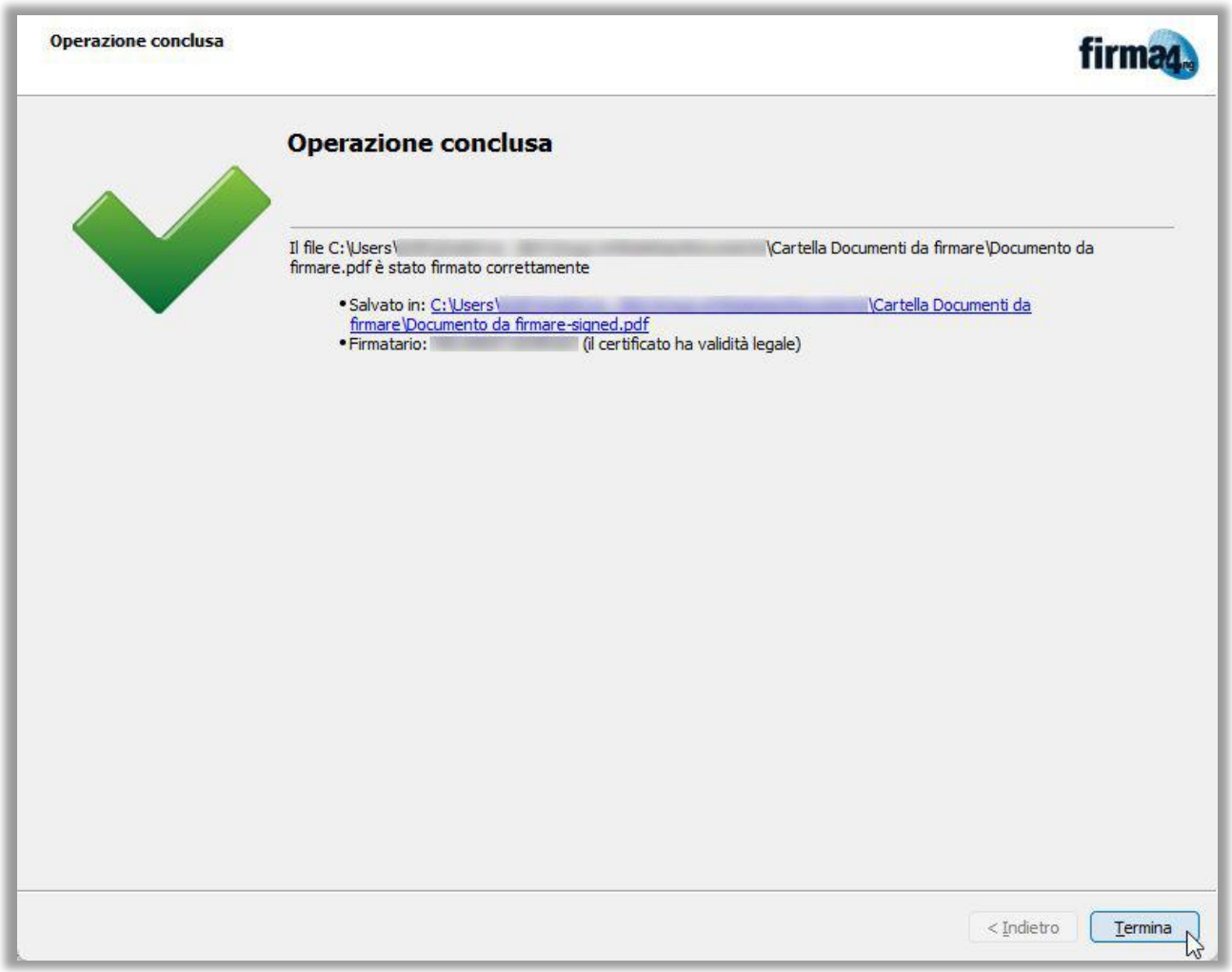


*Figura 14 – Conclusione operazione di firma.*

## FIRMA DI DOCUMENTI PDF

Se si desidera apporre una firma su un documento PDF, occorre selezionare dal menù a tendina la tipologia di firma “Aggiungi la firma al pdf” (Figura 15) e selezionare una delle seguenti opzioni proposte:

- **Firma invisibile**: il PDF verrà firmato senza aggiungere alcun dettaglio di tipo “grafico” al documento;
- **Firma grafica (modalità avanzata)**: sarà possibile selezionare la posizione della firma ed aggiungere eventualmente un'immagine (opzione non disponibile nel caso di 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 “FirmaPDF” del menù “Opzioni”; sarà comunque possibile modificare la configurazione spuntando la casella “Modifica opzioni” e personalizzando le opzioni di firma PDF.

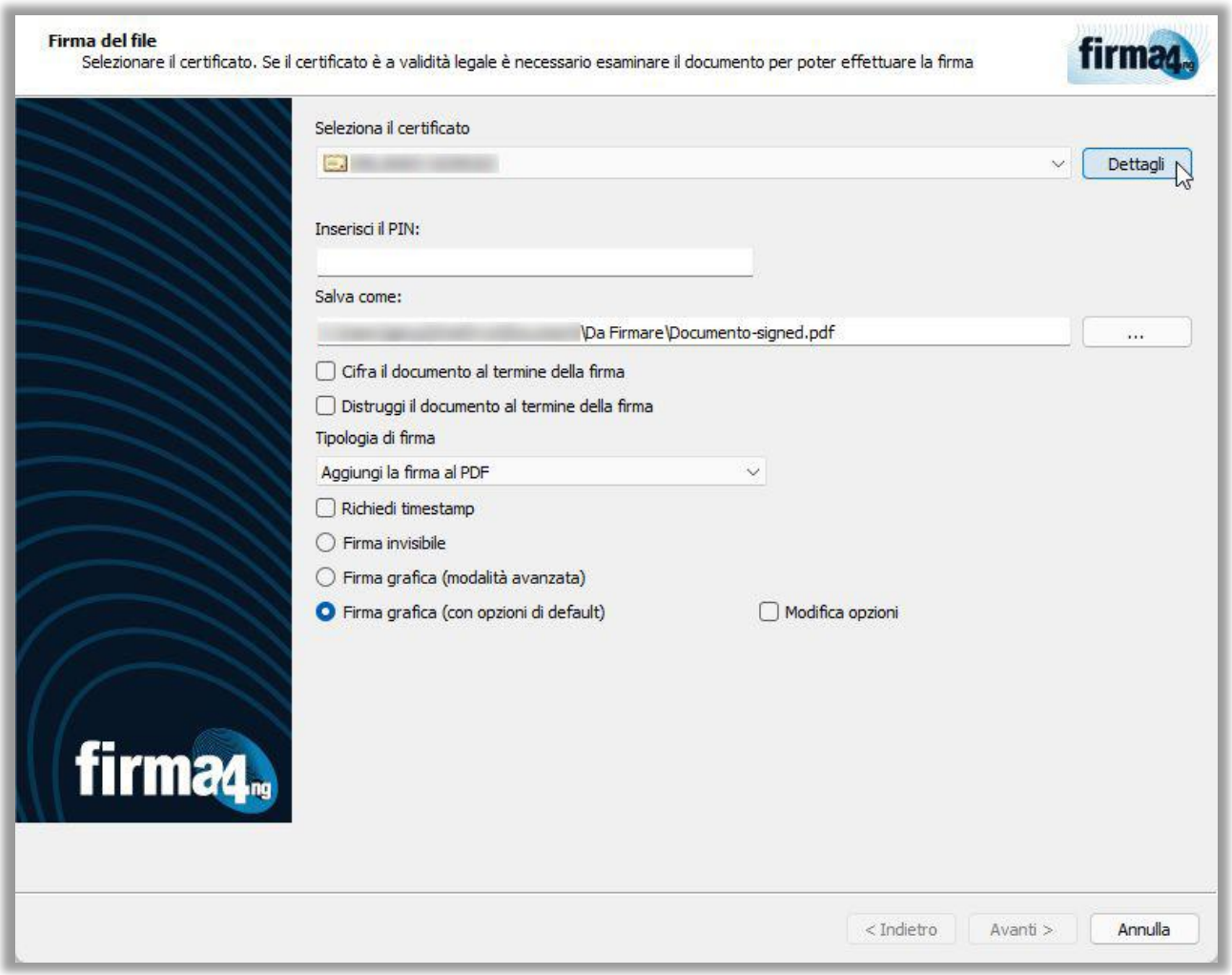


*Figura 15 – Dettaglio delle opzioni di firma PDF.*

Più in dettaglio, nel caso in cui si sia selezionata la "**Firma grafica (modalità avanzata)"** verrà mostrata la seguente schermata (Figura 16) per la selezione e il posizionamento della grafica.

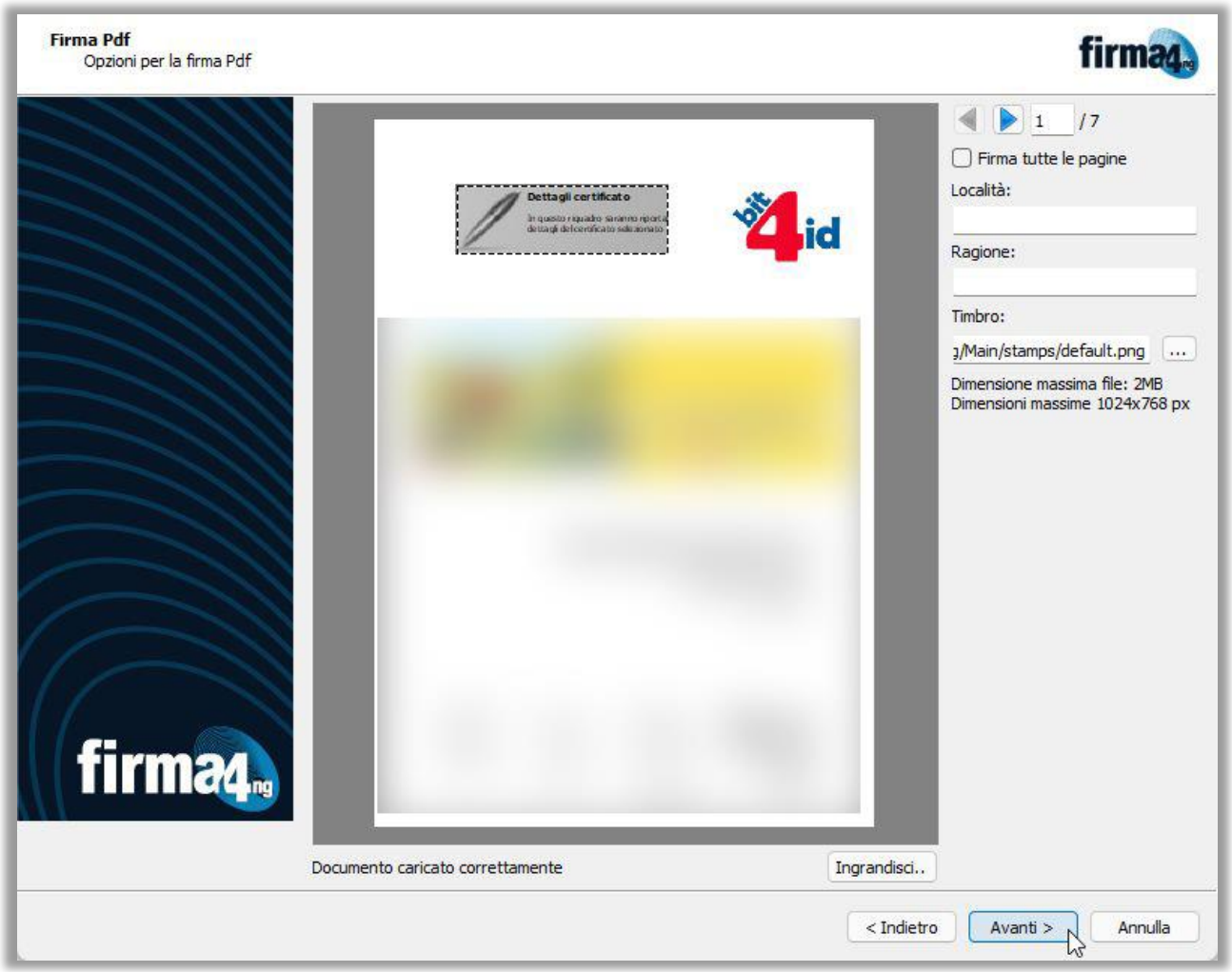


*Figura 16 – Firma grafica PDF.*

Dalla schermata è possibile pertanto:

a. Selezionare la pagina dove apporre la firma (a partire dall'inizio o dalla fine del documento):

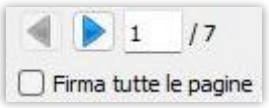


*Figura 17 – Selezione pagina.*

b. Inserire i campi "Località" e "Ragione" da aggiungere (eventualmente) alla firma:


*Figura 18 – Inserimento campi "Località" e "Ragione".*

c. Selezionare l'immagine da associare alla firma:

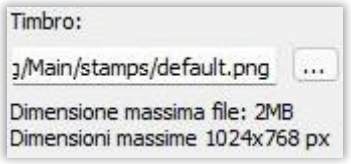


*Figura 19 – Selezione immagine da associare alla firma.*

Se si è scelta l'opzione "**Firma grafica (con opzioni di default)**" è possibile modificare la configurazione impostata come standard, spuntando la casella "Modifica opzioni".
Si aprirà la schermata che segue (Figura 20):

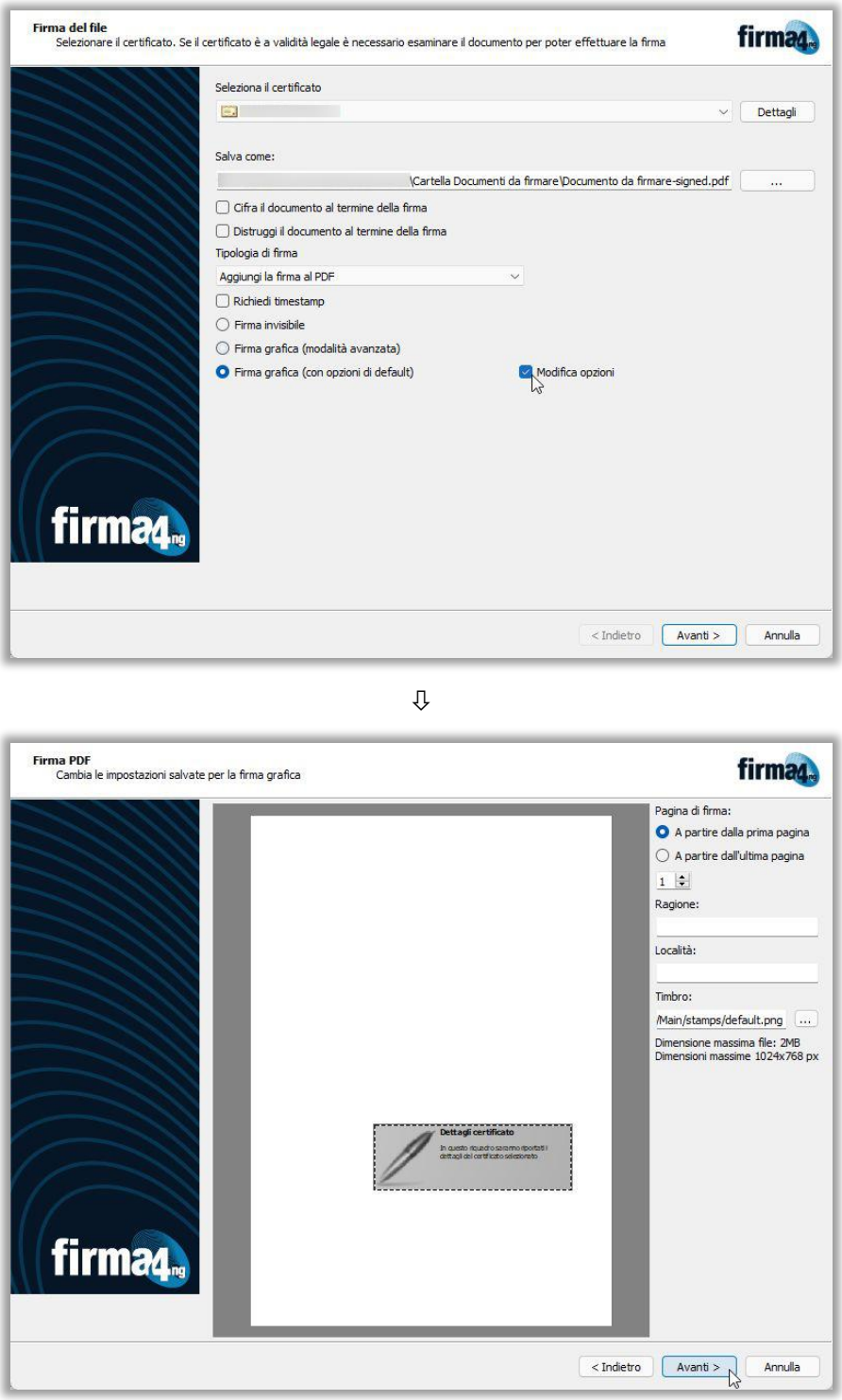


*Figura 20 – Firma grafica PDF – modifica opzioni.*

Dalla schermata in figura 20 è possibile modificare/inserire:

a) La posizione della firma
b) Le dimensioni della firma da apporre
c) Il numero di pagina del documento dove apporre la firma
d) La Ragione e Località
e) L'immagine da includere nella firma.

La procedura di firma riprende dalla Fase 4 precedentemente descritta.

Si ricorda che nel caso di firma PDF è possibile effettuare la verifica sia attraverso il bottone "Verifica" del menu principale, sia utilizzando l'applicazione Acrobat Reader di Adobe.

Al termine dell'operazione di firma, per chiudere la finestra cliccare sul bottone "Termina".

# APPOSIZIONE DI MARCHE TEMPORALI

Per apporre una marca temporale su un documento, firmato o meno, occorre cliccare sul bottone “Marca temporale” presente nel menu principale dell’applicazione.

*Nota:* firma4ng permette l’apposizione di una marca temporale contestualmente all’operazione di firma. In questo caso, si aprirà una finestra attraverso la quale è possibile configurare un servizio di marcatura temporale, se si desidera utilizzare un servizio diverso da quello presentato come già selezionato.

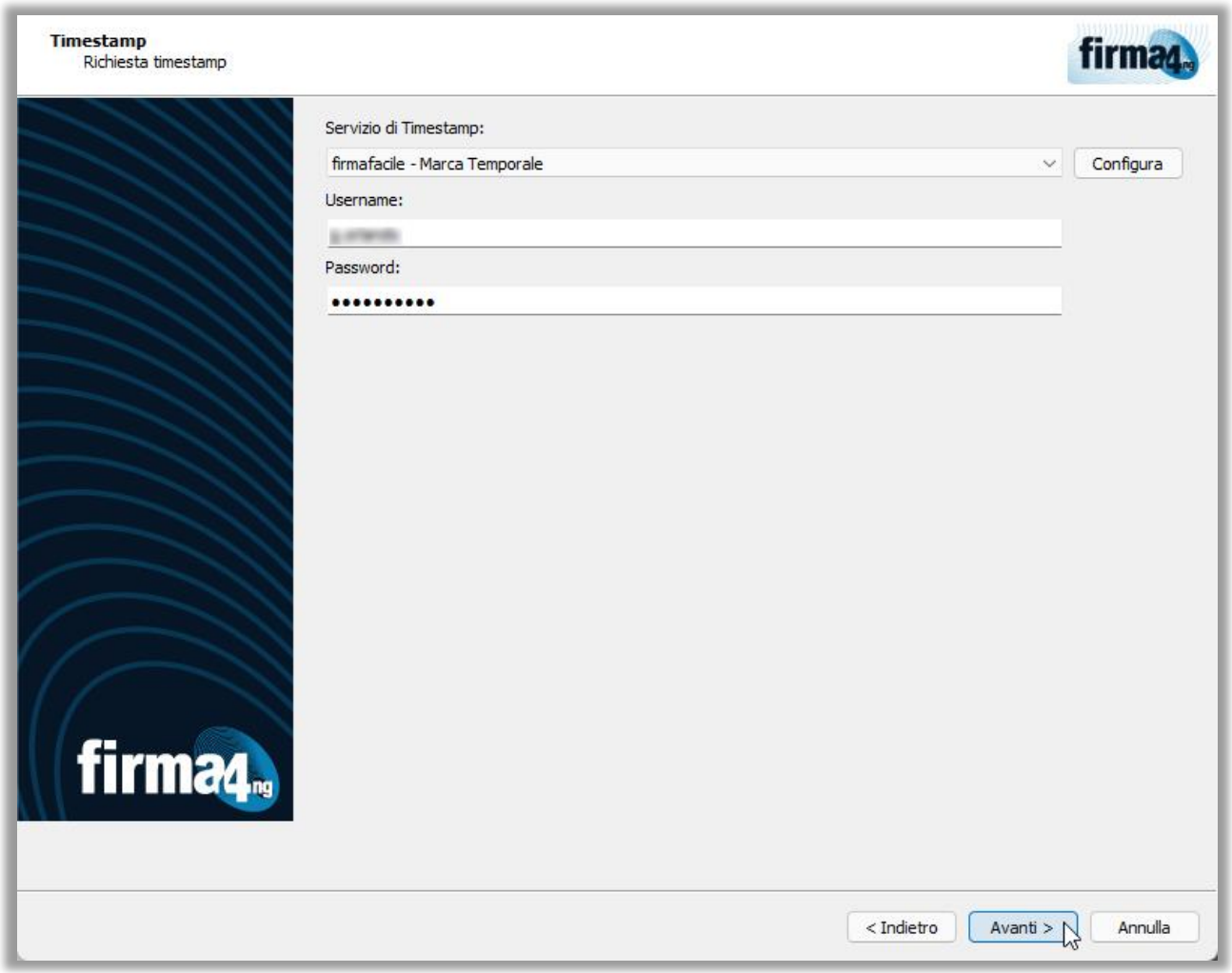


*Figura 21 – Marca temporale (contestualmente a un’operazione di firma).*

### Fase 1

Per avviare l'operazione di marcatura temporale di un documento, si può alternativamente:

- selezionare e trascinare (drag&drop) il documento che si intende marcare temporalmente sul bottone "Marca Temporale" del menu principale;
- cliccare sul bottone "Marca Temporale" del menu principale e selezionare il documento dalla finestra di navigazione del PC.

### Fase 2

Si aprirà una finestra (Figura 22) nella quale, dopo aver selezionato il servizio di marcatura temporale da utilizzare, è possibile indicare il nome e la cartella di destinazione della marca temporale ed il formato in cui salvare la marca temporale fra quelli presenti nella lista del menù a tendina:

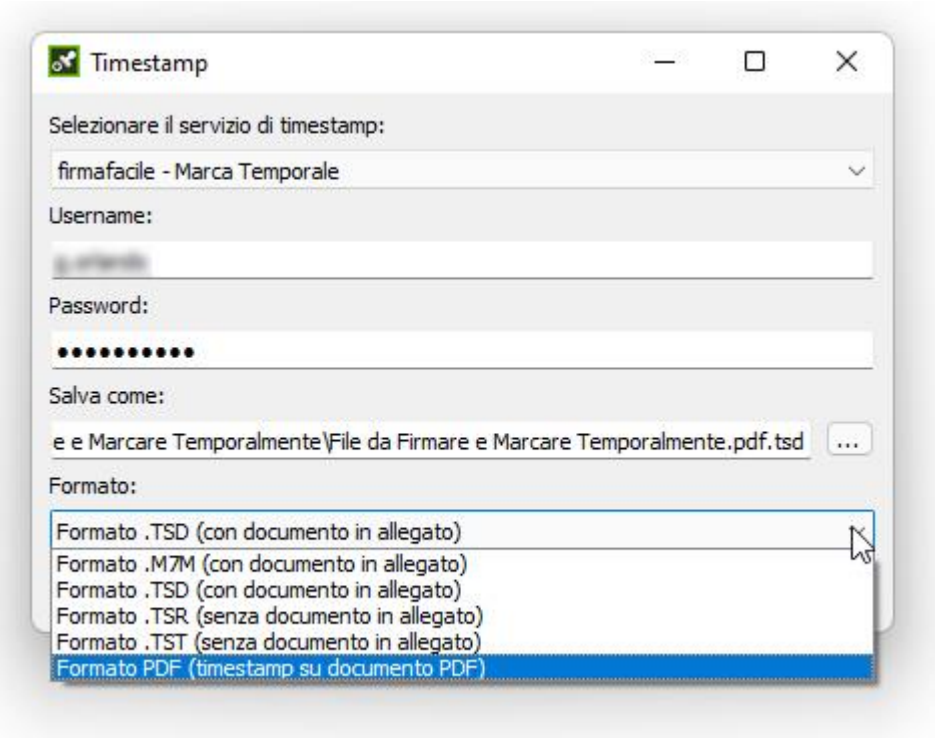


*Figura 22 – Marca temporale (da bottone "Marca temporale" del menu principale).*

Inoltre sarà possibile selezionare il formato di marca temporale da apporre, tra:

- **M7M**: è il primo formato storicamente introdotto per contenere sia l'evidenza della marca temporale (il file con formato tsr) che il file stesso sottoposto a marcatura; quindi, sottoponendo a verifica un file con formato M7M non abbiamo bisogno di altro in quanto nel file stesso è contenuto sia l'originale che l'evidenza informatica della marca temporale. Si tenga presente che non tutti i software riconoscono e sono in grado di verificare il formato M7M;

- **TSD**: è l'ultimo formato in ordine di tempo introdotto per contenere sia l'evidenza della marca temporale (il file con formato tsr), sia il file stesso sottoposto a marcatura; quindi, sottoponendo a verifica un file con formato TSD non abbiamo bisogno di altro in quanto nel file stesso è contenuto sia l'originale che l'evidenza informatica della marca temporale. Diversamente dal formato M7M il formato TSD rispetta una sintassi di composizione che rispetta standard ampiamente riconosciuti dalla comunità informatica;

- **TSR/TST**: è il formato più semplice contiene di fatto solo l'impronta del file, NON tutto il file, e l'evidenza informatica di quella che è l'apposizione della marca temporale. Per fare la verifica di un file con questo formato è indispensabile possedere anche il file originale che si è marcato, altrimenti sarà solo possibile controllare che la marca temporale sia stata realizzata in modo corretto ma non verificare se il file tsr/tst corrisponde al file originale. La dimensione di un file con formato ed estensione tsr/tst è sicuramente inferiore al file originale;

- **PDF**: equivalente al formato M7M, ma applicabile unicamente a file in formato .pdf.

ATTENZIONE: Il formato M7M è stato deprecato e non è conforme alla Deliberazione CNIPA n. 45/2009 (art. 17, comma 4).

1. Quando il firma4ng aprirà il file e otterrà i certificati, presenterà la schermata dove fare bene attenzione a selezionare come Tipologia di **Firma Busta crittografata .P7M (CAdES-Bes)**, a spuntare la casella **Richiedi timestamp**, per infine immettere il PIN e cliccare su Avanti.

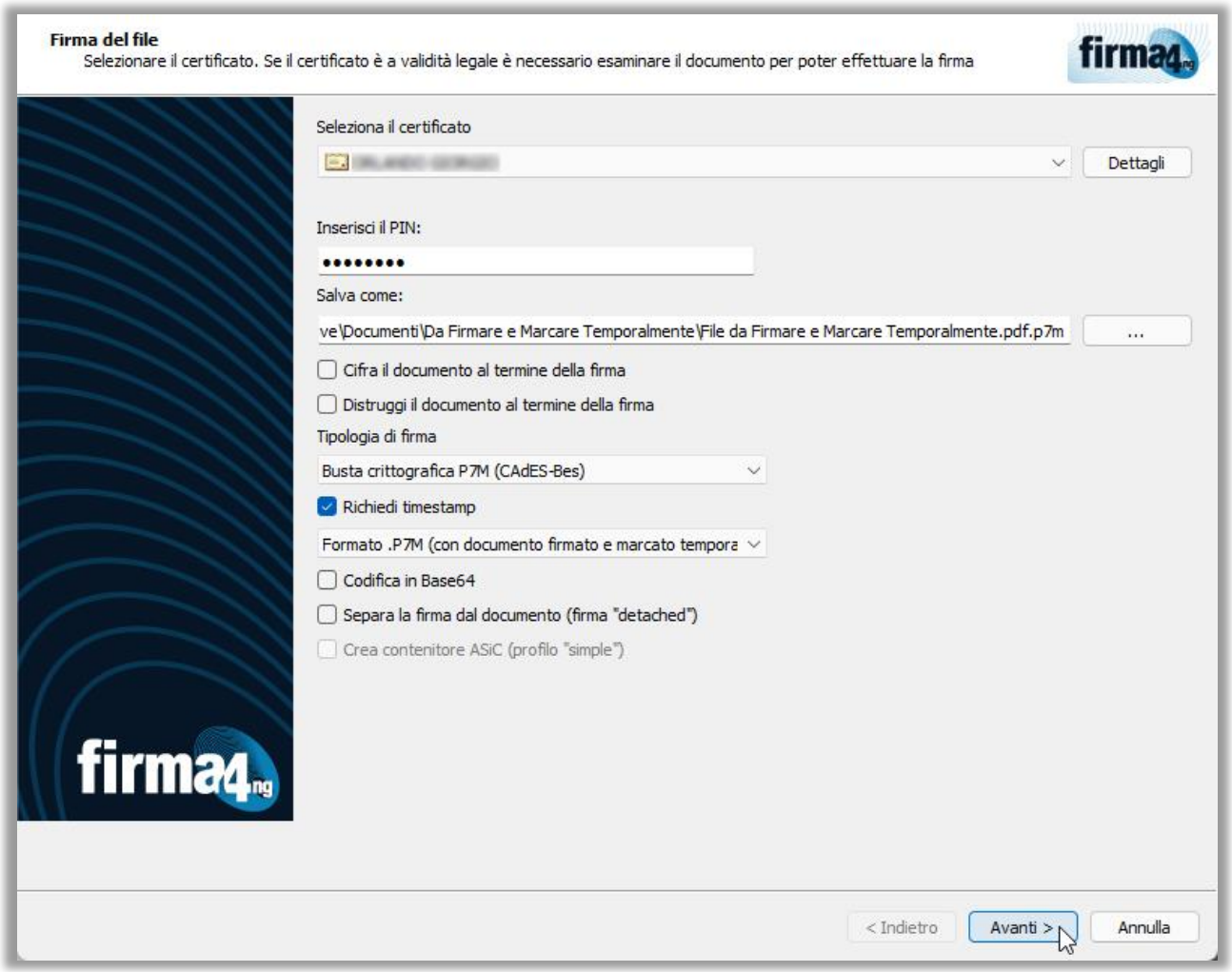


*Figura 23 – Spunta Casella "Richiedi Timestamp"*

2. Verrà quindi presentata una schermata in cui è necessario, dopo aver cliccato sul pulsante "**Apri documento…**" per consultare il contenuto del file selezionato, confermare spuntando la relativa casella, di aver preso visione del documento si voglia firmare digitalmente.

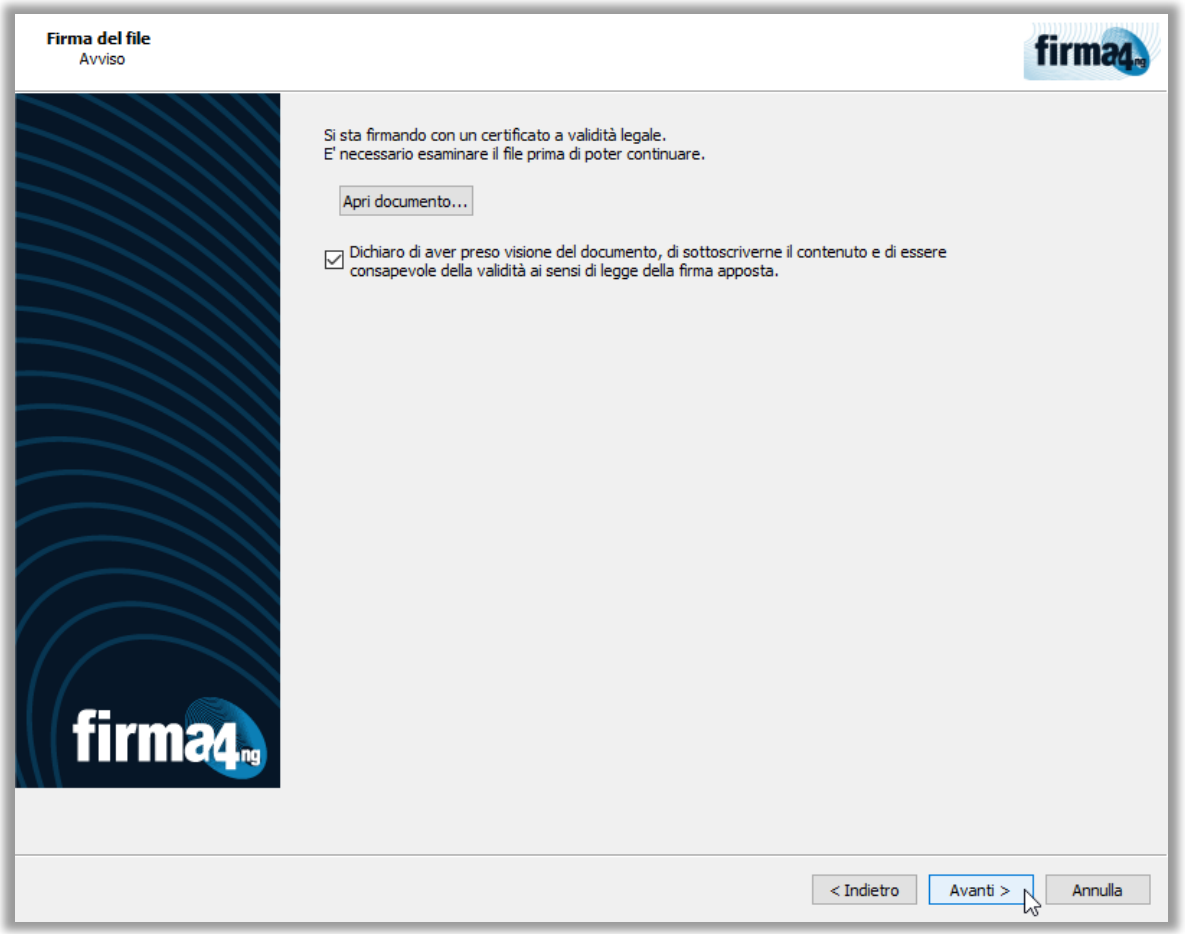


*Figura 24 – Dichiarazione di presa visione*

3. Dopo aver cliccato sul pulsante Avanti, verrà presentata la finestra in cui risulterà necessario in prima istanza selezionare come Servizio di Timestamp: **firmafacile – Marca Temporale** per poi immettere correttamente la propria Username e Password e concludere cliccando su Avanti.

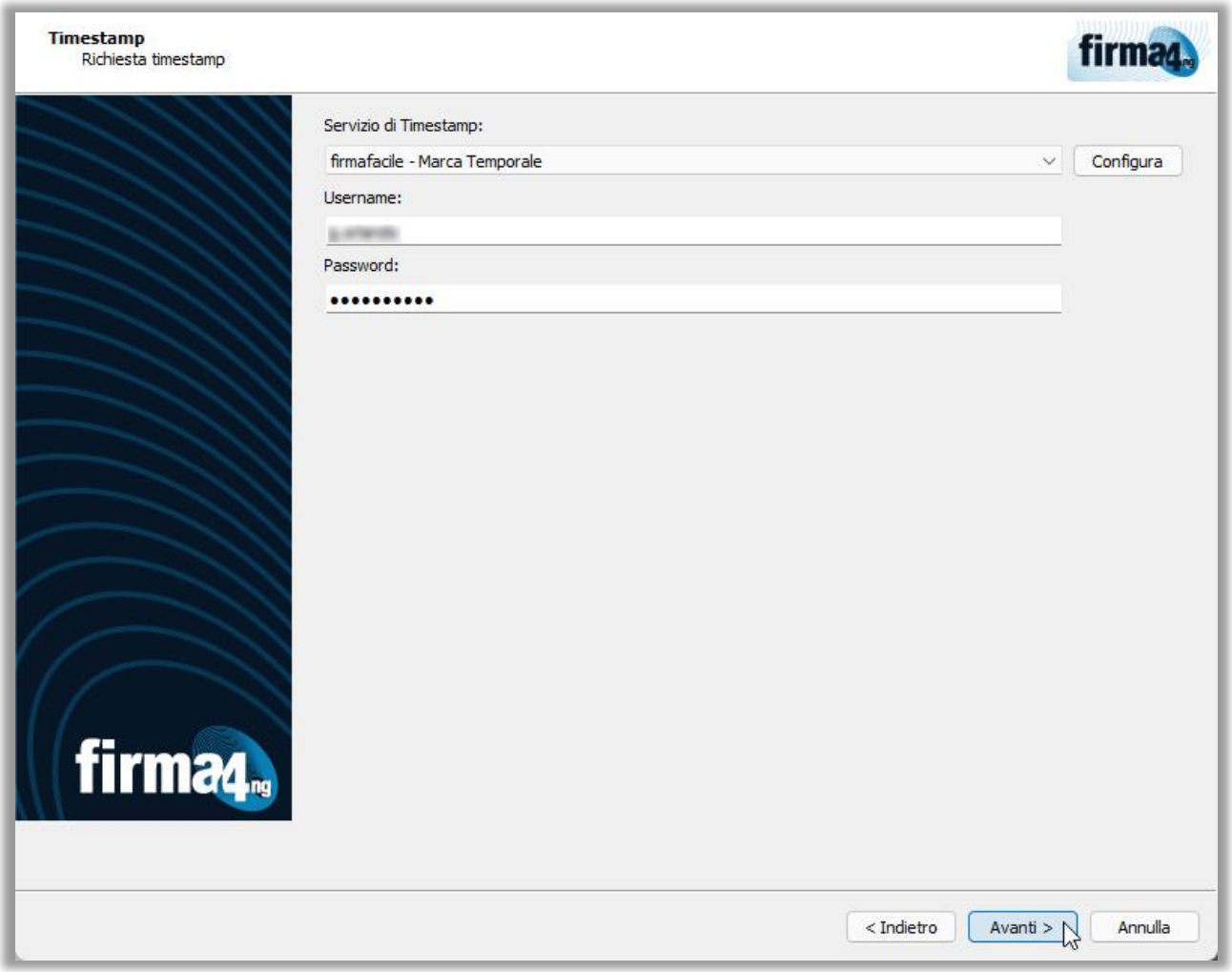


*Figura 25 – Compilazione Username e Password Timestamp*

4. Infine, dopo aver cliccato su Avanti, verranno conclusi dal firma4ng sia il processo di firma digitale che di marcatura temporale per restituire un resoconto, come di seguito riportato.

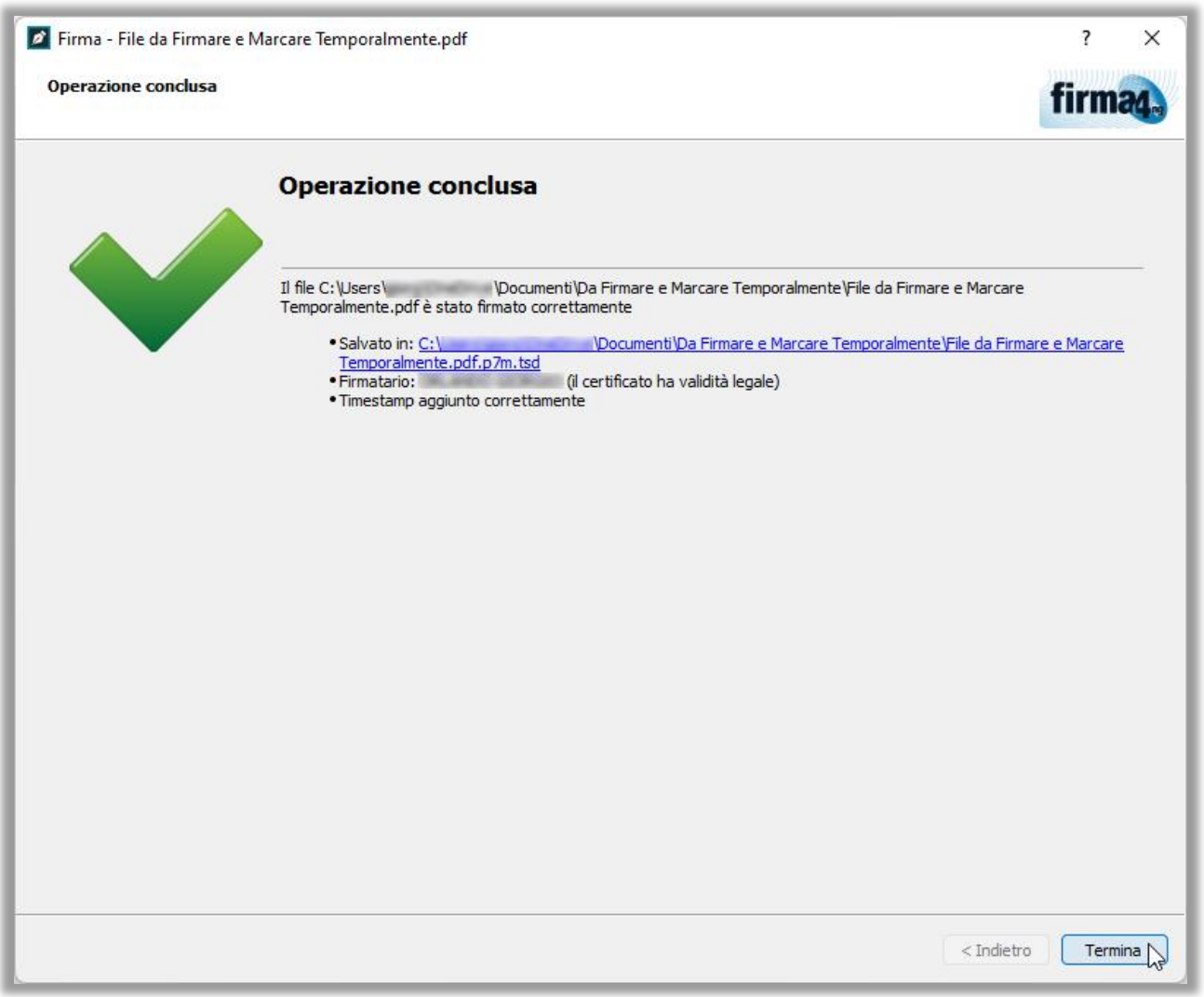


*Figura 26 – Conclusione apposizione marca temporale*

# VERIFICA DI FILE FIRMATI E/O MARCATI TEMPORALMENTE

firma4ng permette di verificare la validità di un file firmato e/o marcato temporalmente.

### Fase 1

È possibile avviare l'operazione di Verifica in una delle seguenti modalità:

- Selezionando e trascinando (drag&drop) il/i documenti sul bottone "Verifica";
- Cliccando sul bottone "Verifica" (Figura 1) e selezionando il/i documenti da verificare dalla finestra di navigazione del PC.

### Fase 2

firma4ng effettua la verifica del documento firmato, il cui esito viene mostrato nella schermata che segue (Figura 27).

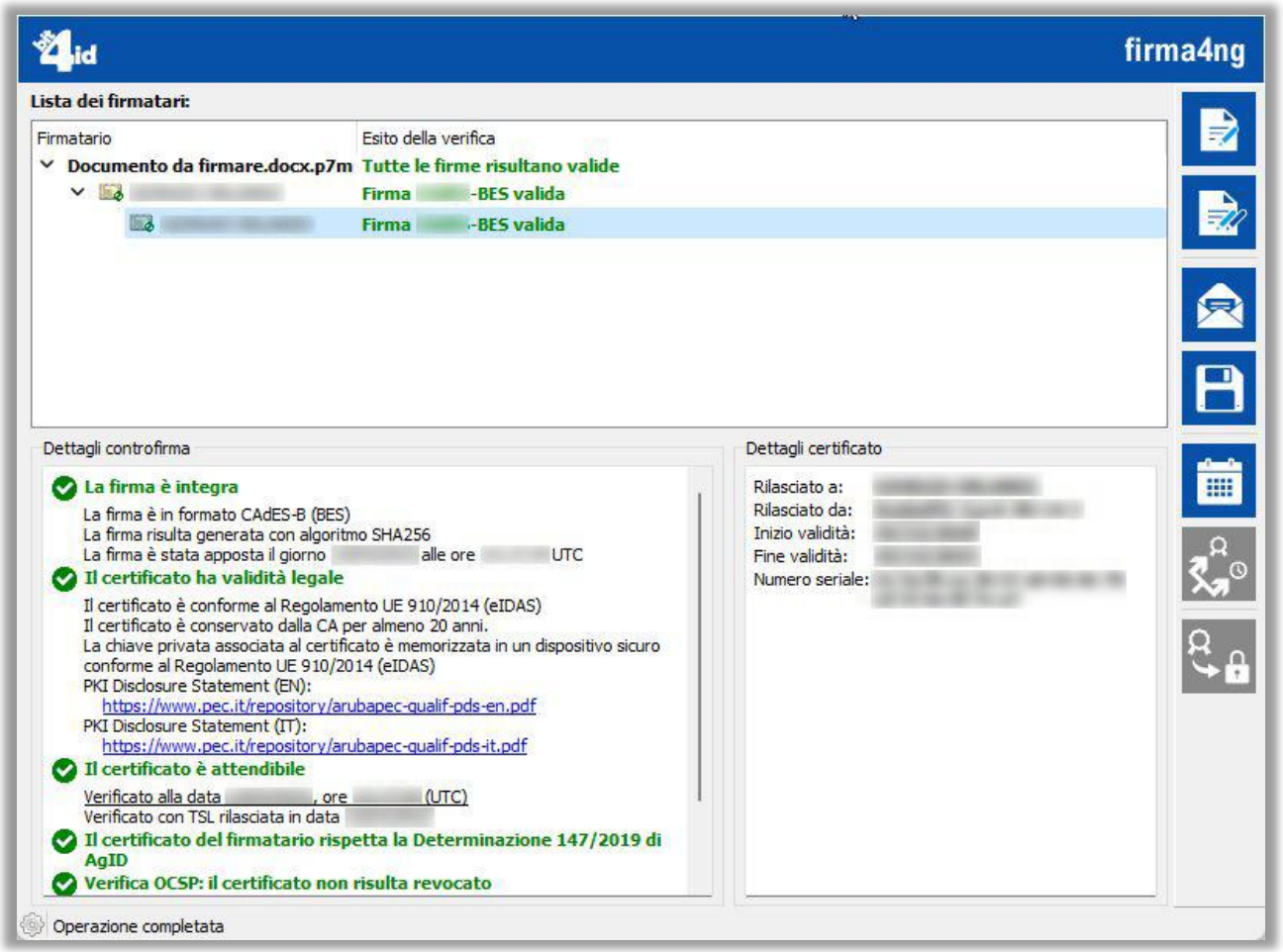


*Figura 27 – Pannello di Verifica.*

La schermata di Verifica è divisa in tre sezioni. Nella parte alta della finestra viene mostrata la lista di tutte le firme (ed eventuali marche temporali) apposte sul documento (Figura 28). Vengono elencati tutti i certificati dei firmatari del documento. È possibile visualizzare i dettagli di un certificato mediante un doppio click su uno di essi.

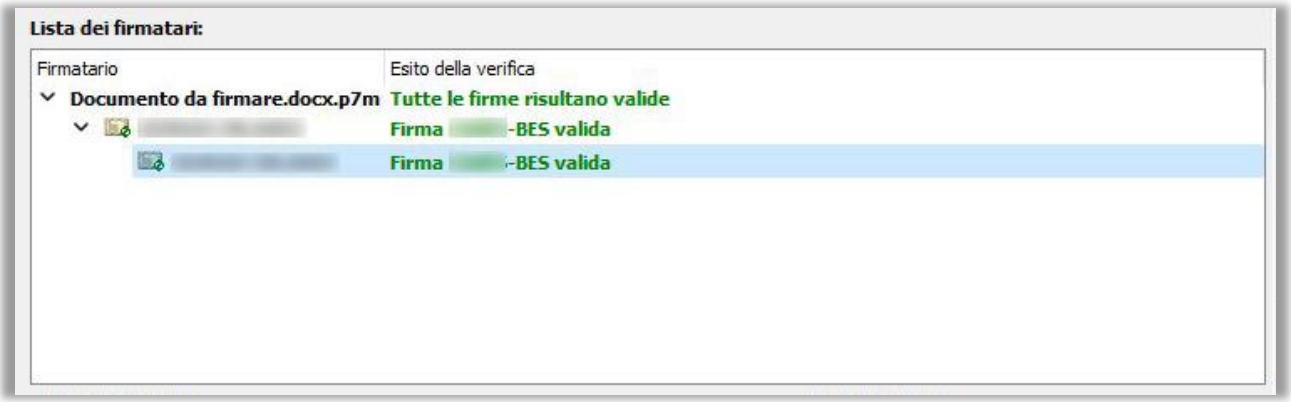


*Figura 28 – Elenco firme apposte sul documento verificato.*

Nella parte bassa della schermata (Figura 29) sono mostrati i dettagli delle verifiche effettuate su una specifica firma/marca temporale, e riguardano:

- **Verifica 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 all'algoritmo utilizzato per la creazione della firma ed il formato del documento firmato/marcato.

  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 Determinazione 147/2019 di AgID".

- **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.
  In caso di esito positivo viene mostrato il messaggio: "Il certificato non risulta revocato".


*Figura 29 – Dettagli sulla verifica.*

In Figura 30 è mostrato il caso di verifica di un documento a cui è stata apportata una marca temporale riportando nella sezione “dettagli Timestamp” i relativi dettagli:

- data e ora della marca temporale della marca temporale
- l’algoritmo di impronta utilizzato
- informazione circa il sistema di TSA utilizzato
- l’attendibilità del certificato utilizzato durante il processo

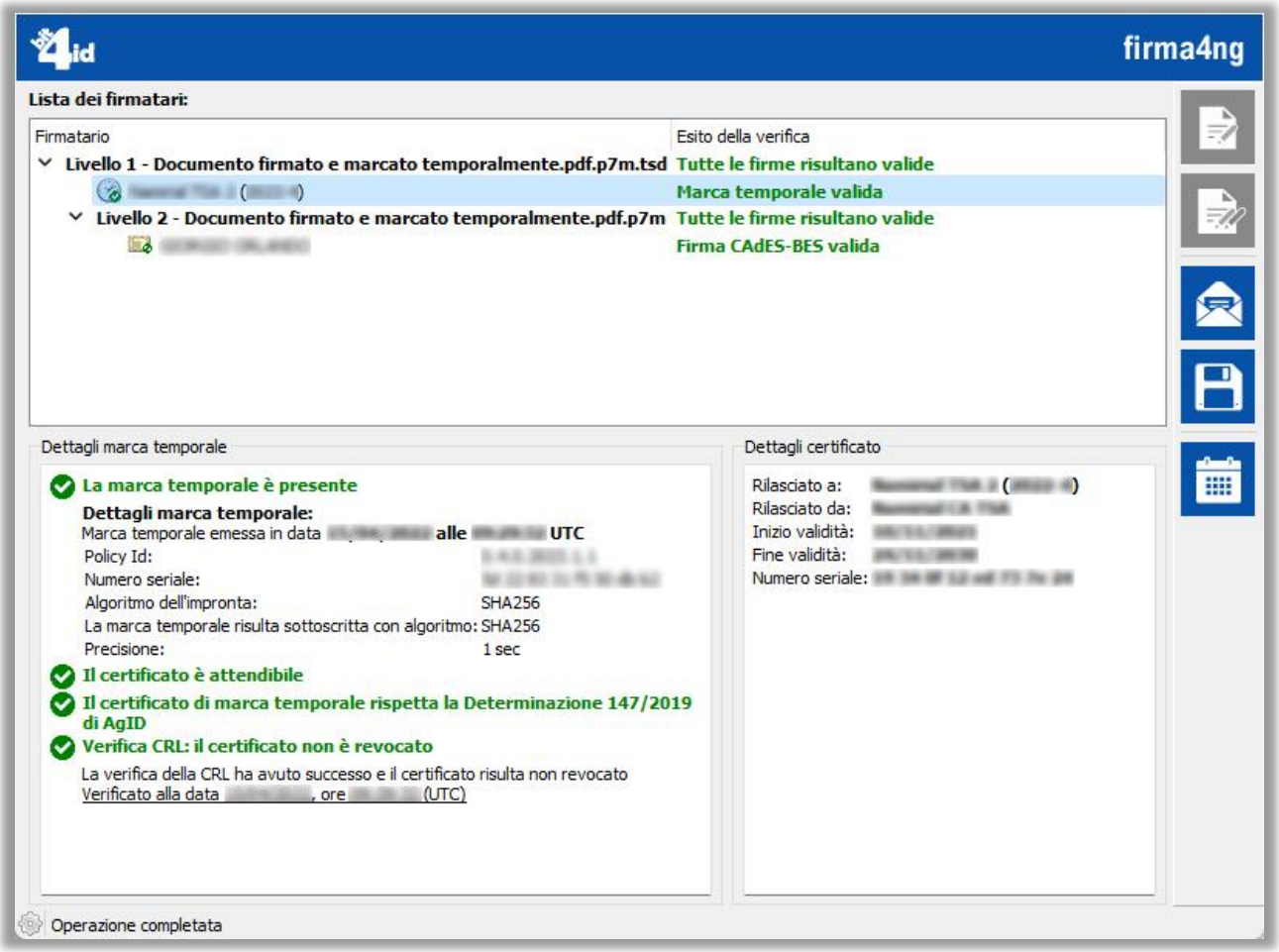


*Figura 30 – Verifica marca temporale.*

Dal menù verticale, presente sul bordo destro della schermata di Verifica è inoltre possibile effettuare le seguenti operazioni (partendo dall'alto):

| Icona | Funzionalità |
|---|---|
|  | **Aggiungi firma**: per aggiungere una ulteriore firma al documento (avviando la procedura di Firma). |
|  | **Aggiungi controfirma**: per aggiungere una controfirma alla firma selezionata (avviando la procedura di Firma). |
|  | **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 verificare se la firma apposta al documento era (o sarà) valida in una specifica data, passata o futura. Cliccando sul bottone "Verifica alla data" si apre la finestra in Figura 31. |

*Tabella 1 – Operazioni di verifica.*

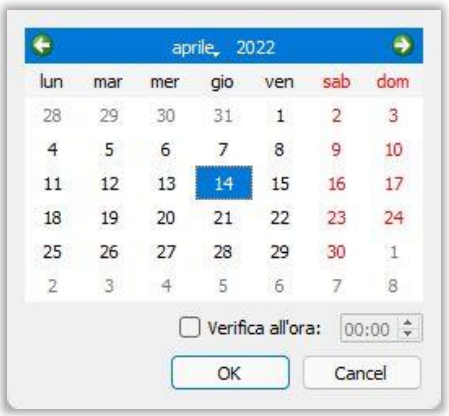


*Figura 31 – Verifica alla data.*

Nel caso in cui il documento firmato contenga delle firme marcate temporalmente, la verifica di tali firme verrà sempre effettuata alla data presente nella marca temporale.

# APPLICAZIONI

Cliccando sul pulsante “Applicazioni” del menu principale di firma4ng (Figura 1), viene avviato il menù secondario (Figura 32), che contiene alcune funzionalità per la crittografia quali la cifratura di un file “Cifra”, la decifratura “Decifra” di un file e la creazione di una cartella cifrata “Cartella cifrata”.


*Figura 32 – Sotto menù "Applicazioni".*

## CIFRATURA DI UNO O PIÙ DOCUMENTI

firma4ng consente la cifratura di uno o più documenti mediante una procedura del tutto analoga all’operazione di firma. A partire dal menu principale, cliccando sul bottone “Applicazioni” si apre il menù secondario con il bottone di “Cifra”.
Se si desidera cifrare dei documenti per se stessi, occorre controllare di aver inserito la smart card nel lettore, o collegato il token USB al PC prima di avviare l’operazione.

### Fase 1

Per lanciare l’applicazione di cifratura si può procedere indifferentemente in uno dei seguenti modi:

- Selezionando e trascinando (drag&drop) il/i documenti sul bottone “Cifra” del menù secondario;
- Cliccando sul bottone “Cifra” e selezionare il/i documento/i da marcare utilizzando la finestra di navigazione del PC.

### Fase 2

A valle dell’inserimento della smart card nel lettore o del collegamento al PC del token USB, l’applicazione legge i certificati presenti sul dispositivo e li carica nella sezione “Contatti”.

Per cifrare un documento per sé stessi, selezionare il certificato da utilizzare e spostarlo, nella sezione “Cifra per…”, utilizzando l’apposito bottone con la freccetta destra.

Se si desidera cifrare un documento per un destinatario, è possibile caricarne il certificato nei seguenti modi:

- Dal tab “File”: cliccare sul bottone “Importa da file…” e selezionare il certificato (“.cer”) da caricare;
- Dal tab “Elenco in linea”: effettuare la ricerca specificando i parametri previsti dal menù a tendina;

in entrambe le modalità, al temine delle operazioni di caricamento dei certificati, occorre selezionare i contatti e spostare i certificati nella sezione “Cifra per…” utilizzando il bottone con la freccetta destra:

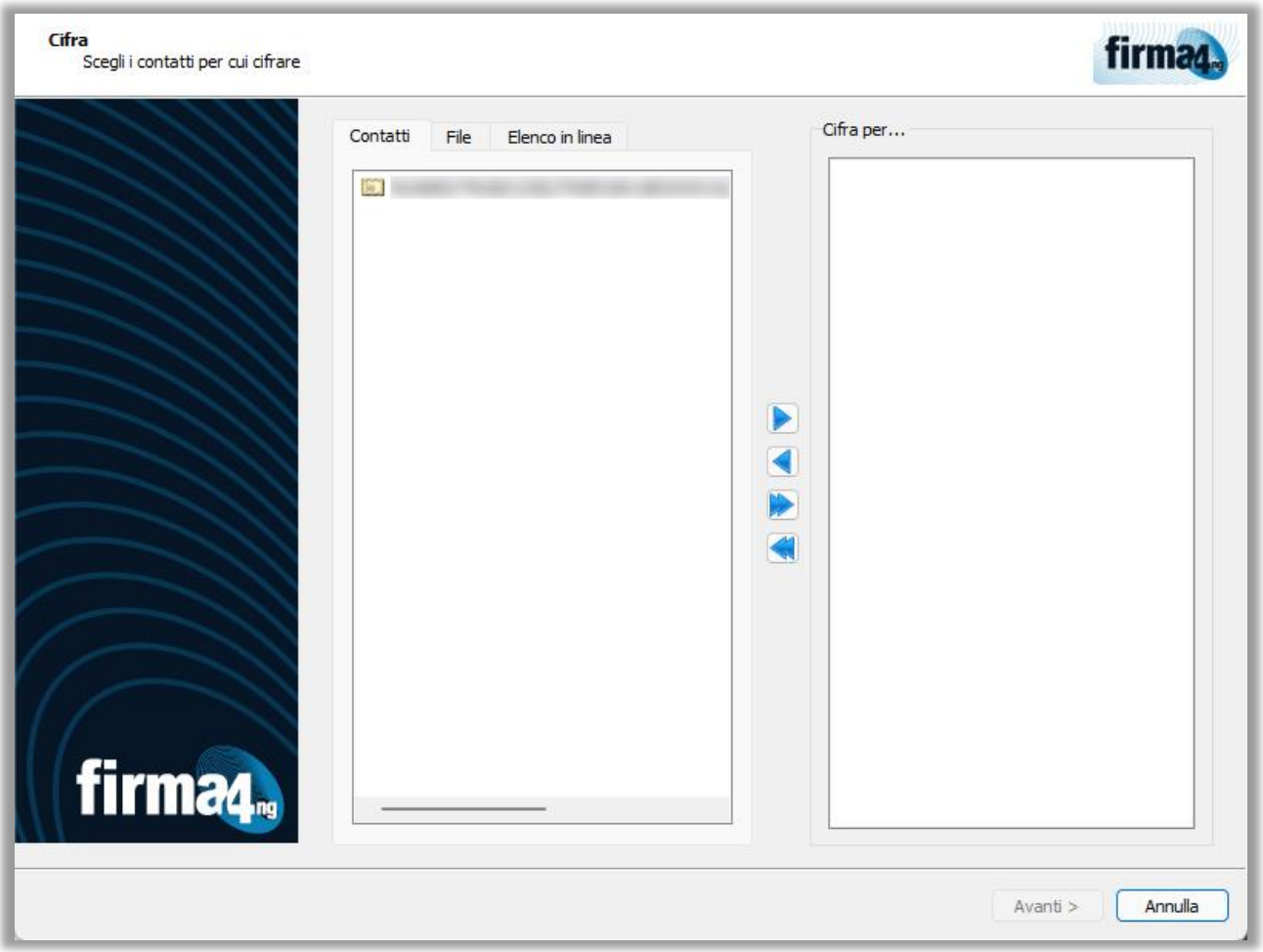


*Figura 33 – Cifratura di documenti.*

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

| Icona | Funzionalità |
|---|---|
|  | 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 rimuove tutti i contatti dalla lista dei certificati con cui cifrare il documento. |

*Tabella 2 – Azioni per cifratura.*

## La rubrica "Contatti"

In firma4ng è disponibile una rubrica personale di contatti, nella quale memorizzare i certificati dei contatti per i quali cifrare un documento.

È possibile importare contatti all'interno della rubrica sia caricandoli da file residenti sul pc (sezione "File"), che ricercandoli sul Registro pubblico dei certificati (sezione "Elenco in linea") gestito dal Certificatore. Di seguito sono dettagliate le due modalità a disposizione:

- **File:** per inserire nella rubrica dei Contatti un destinatario il cui certificato è disponibile su file, dalla sezione "File" occorre cliccare su "Importa da file" e scegliere il certificato (.cer) da importare. 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".

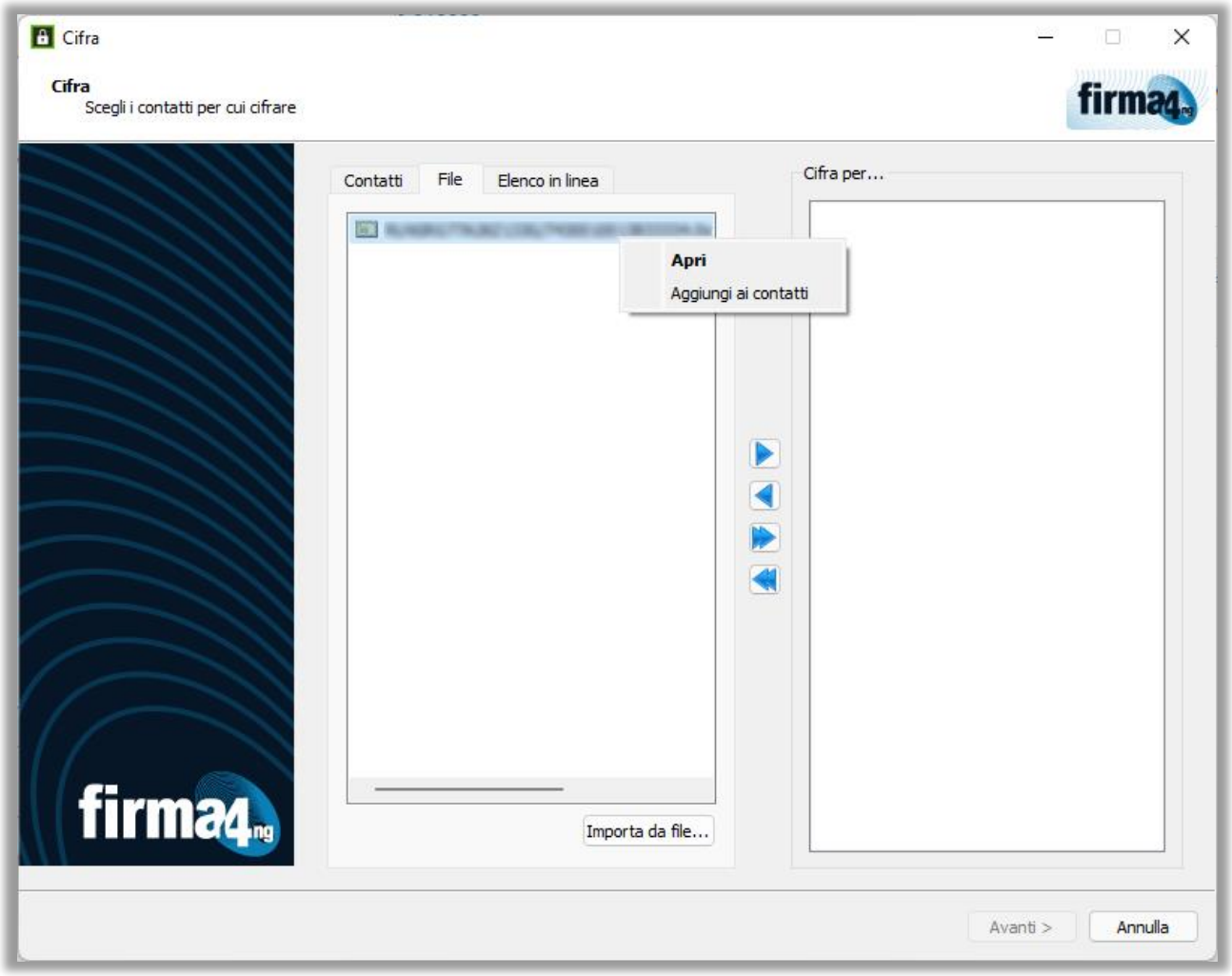


*Figura 34 – La rubrica Contatti.*

- **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 sul bottone "Cerca". 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".

## Le opzioni di cifratura

Dopo aver selezionato almeno un certificato con cui cifrare il documento, cliccando sul bottone “Avanti” è possibile selezionare le opzioni da utilizzare per la cifratura del documento.

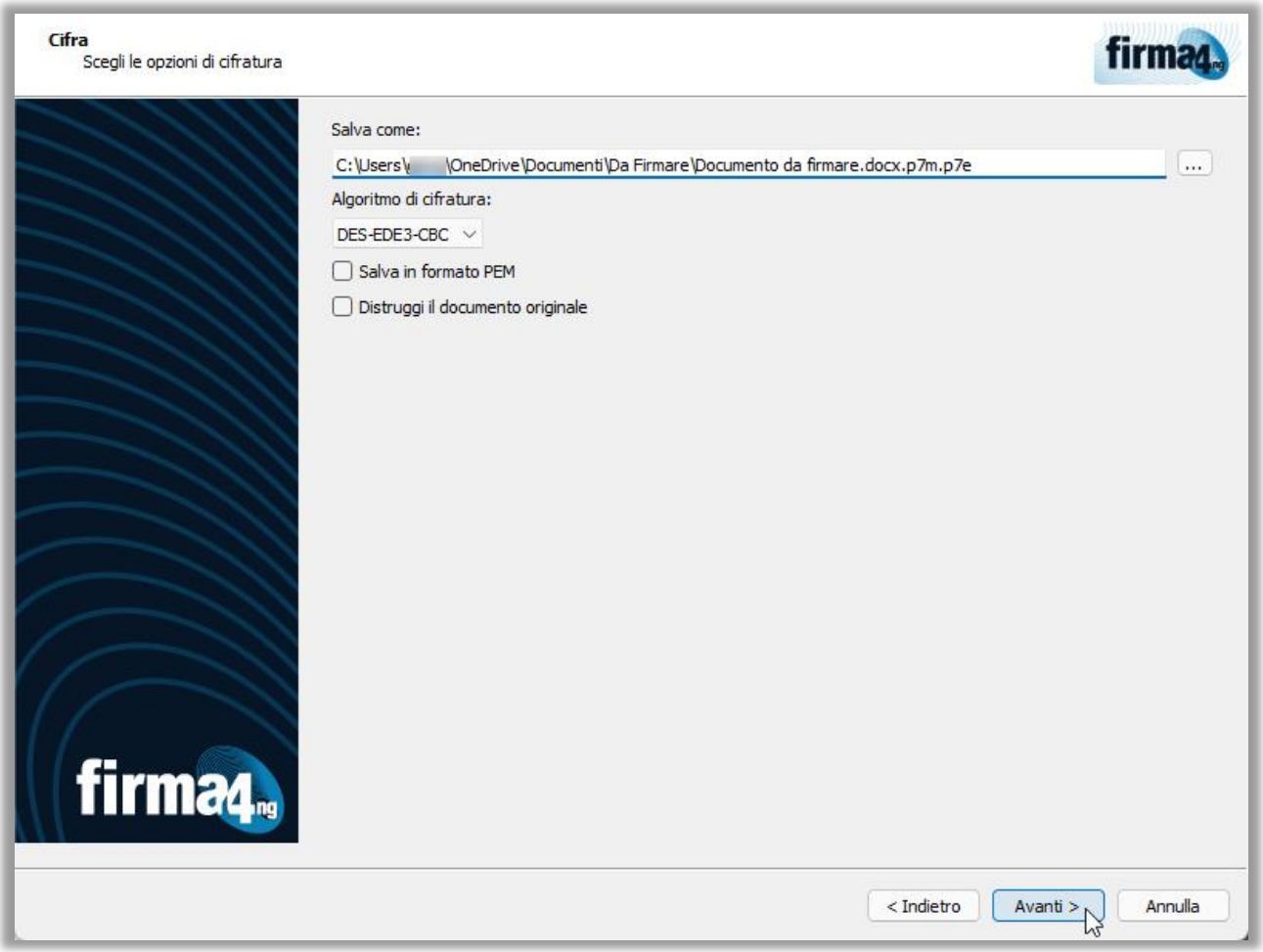


*Figura 35 – Opzioni cifratura.*

Nella schermata di Cifra (Figura 35) è possibile:

- Scegliere la cartella di destinazione e il nome con cui verrà salvato il documento cifrato, cliccando sul bottone “…”;

- Selezionare l'algoritmo da utilizzare per cifrare fra quelli elencati nel menù a tendina (DES-EDE3-CBC oppure AES-256-CBC);

- Scegliere “Salva in formato PEM” se si vuole salvare il documento cifrato in formato PEM, spuntando l’apposita casella.
  *Nota: per maggiore sicurezza, si consiglia di utilizzare l’algoritmo AES-256-CBC.*

- Spuntare la casella “Distruggi il documento originale”: al termine dell’operazione di cifratura il documento originale verrà cancellato ‘definitivamente’ dal PC, e non potrà più essere recuperato.

Cliccando su “Avanti” si procederà con la cifratura del documento, al termine della quale viene mostrata una schermata con l’esito dell’operazione e l’indicazione relativa alla cartella di destinazione in cui è stato salvato il documento cifrato. Con il bottone “Termina” è possibile chiudere la schermata.

## DECIFRATURA DI UNO O PIÙ DOCUMENTI

Con firma4ng è possibile decifrare documenti precedentemente cifrati per se stesso.
In maniera del tutto analoga alla cifratura, è possibile avviare l’operazione di decifratura in uno dei seguenti modi:

- Selezionando e trascinando (drag&drop) il/i documento/i da decifrare sul bottone “Decifra” del menù secondario dell’applicazione.
- Cliccando sull'icona “Decifra”: si aprirà una finestra di navigazione del PC per selezionare i documenti da decifrare.

Se nel dispositivo crittografico è presente il certificato con cui è possibile decifrare il documento, si aprirà la seguente schermata:

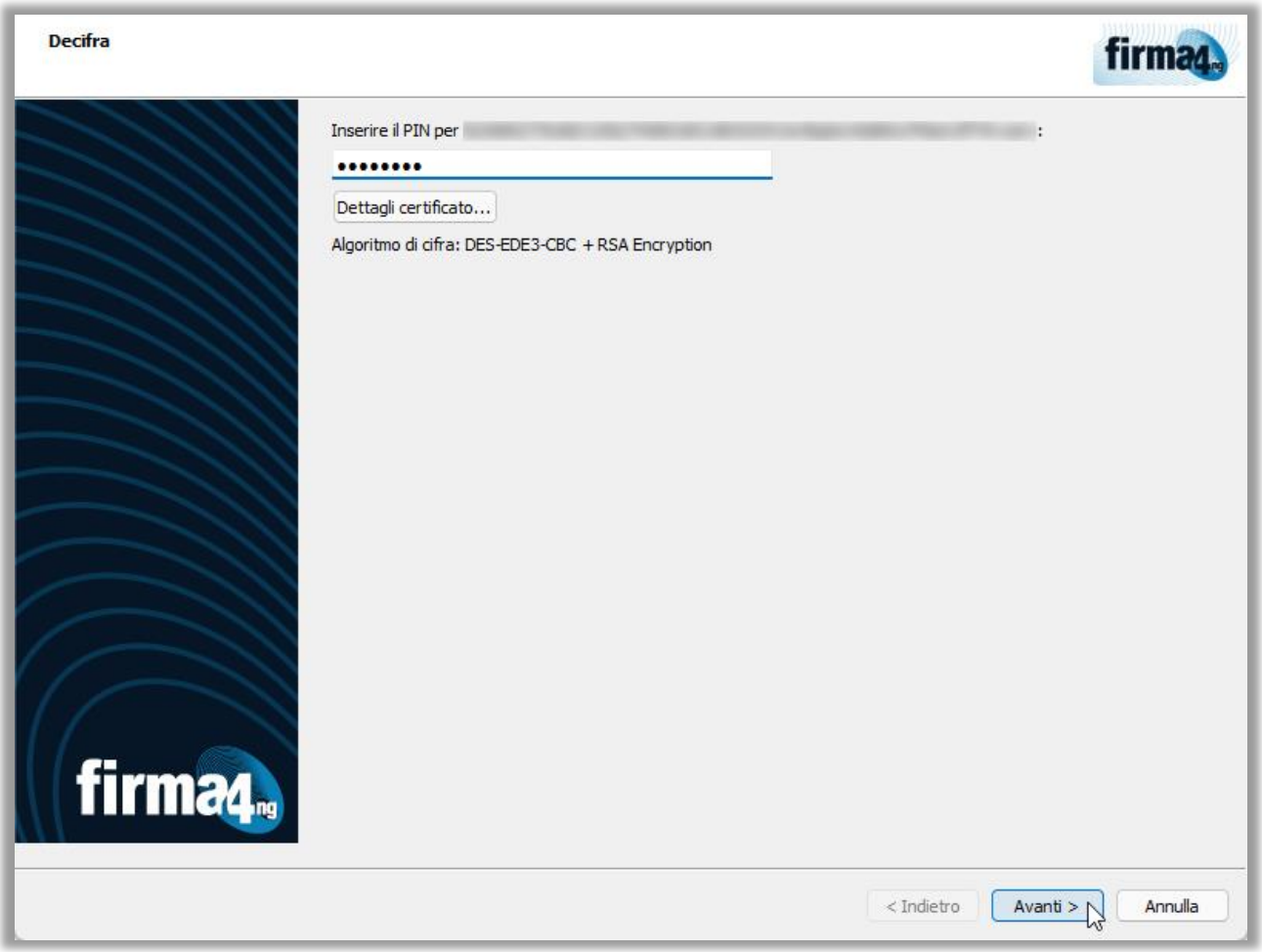


*Figura 36 – Decifratura.*

nella quale si deve inserire il PIN del dispositivo crittografico per procedere alla decifratura del documento (Figura 36).

Nella schermata finale viene riportato l'esito dell'operazione e, in caso di esito positivo, sarà possibile aprire il documento appena decifrato cliccando sul bottone "Apri contenuto" oppure salvarlo in locale sul proprio PC cliccando sul bottone "Salva contenuto...".

Per chiudere la finestra "Decifra" cliccare sul bottone "Termina".

## CARTELLA CIFRATA

La funzionalità “Cartella cifrata” permette di creare una cartella cifrata sul file system del PC accessibile solo attraverso il software firma4ng. Per farlo bisogna cliccare sull'icona “Cartella cifrata” del menù secondario relativo alle “Applicazioni” e inserire il pin della smartcard per decifrarne il contenuto.

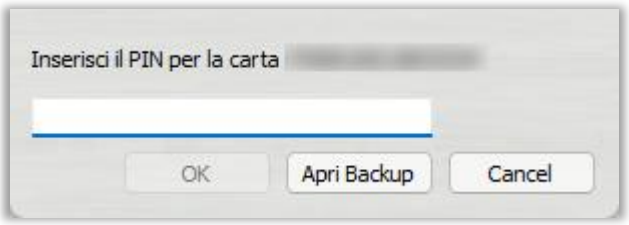


*Figura 37 – Inserimento pin per accesso alla cartella cifrata.*

Una volta inserito il pin corretto l’utente potrà navigare all’interno della cartella cifrata e creare e rimuovere sottocartelle cartelle, importare ed esportare file e creare eventuali copie di backup.

Di seguito il significato delle icone presenti sulla barra della Cartella Cifrata:

| Icona | Funzionalità |
|---|---|
|  | **Crea Nuova Cartella** |
|  | **Aggiungi File:** Trascinando un file su questa icona o cliccandoci sopra, in maniera del tutto automatica il file verrà salvato nella cartella cifrata. |
|  | **Sali di livello**: Quando si è all’interno di una cartella, questo pulsante consente all’utente di salire di un livello fino a tornare nella cartella principale. |
|  | **Aggiorna**: per aggiornare la visualizzazione delle cartelle |

| | |
|---|---|
|  | **Rimuovi Selezionati**: per eliminare file e/o cartelle precedentemente selezionate |
|  | **Esporta Selezionati:** per esportare file presenti all'interno di una cartella, ad esempio, sul desktop del Pc. Quando un file viene esportato, esso potrà essere aperto utilizzando il programma corrispondente alla sua estensione (es. un file .doc verrà aperto con Word) |
|  | **Crea Backup del disco cifrato:** per creare una cartella di backup dell'intero FileSystem cifrato. Per crearne una è necessario specificare il percorso su cui salvarla ed inserire una password, come indicato in Figura 39 |
|  | **Apri Backup:** per aprire una cartella di cui era stata fatta una copia di backup. Per aprire la cartella è necessario richiamare il percorso su cui era stata memorizzata ed inserire la password scelta in fase di backup come indicato in Figura 40 |

*Tabella 3 – Azioni per cifratura.*

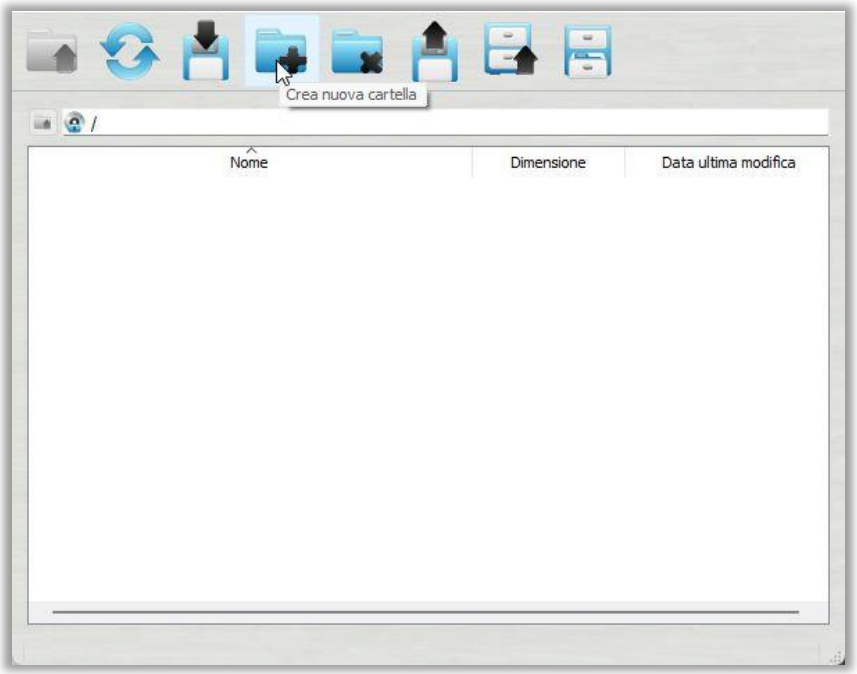


*Figura 38 – Creazione sotto cartella nella cartella cifrata.*

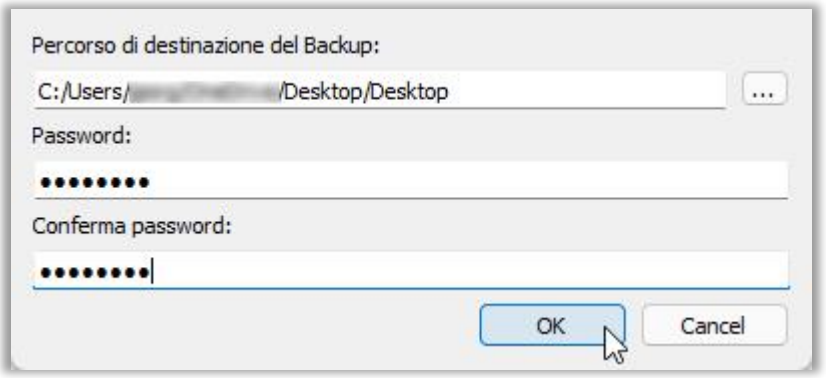


*Figura 39 – Creazione Backup.*

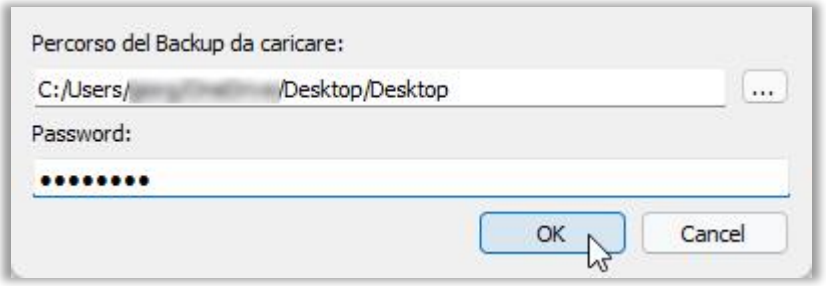


*Figura 40 – Caricamento di un backup.*

# GESTIONE TOKEN/SMARTCARD

Il sottomenù "Gestione Token" (Figura 41) permette all'utente di gestire la propria smartcard/token criptografico e di configurare al meglio il firma4ng.


*Figura 41 – Sottomenù "Gestione Token".*

## OPZIONI

Cliccando sul bottone "Opzioni" del menù secondario "Gestione Token", si apre la finestra che consente la personalizzazione della configurazione di firma4ng e ne permette il salvataggio (bottone "Salva").

Se si desidera ripristinare la configurazione iniziale di firma4ng, basta cliccare sul bottone "Ripristina".

Nei paragrafi che seguono vengono riportati i dettagli delle sezioni che compongono le opzioni di configurazione.

### Tab "Generale"

Da questa sezione (Figura 42) 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.

- **Avviare aggiornamento TSL**: avviare manualmente l'aggiornamento della TSL.

Cliccare sul bottone “Salva” per salvare la nuova configurazione.

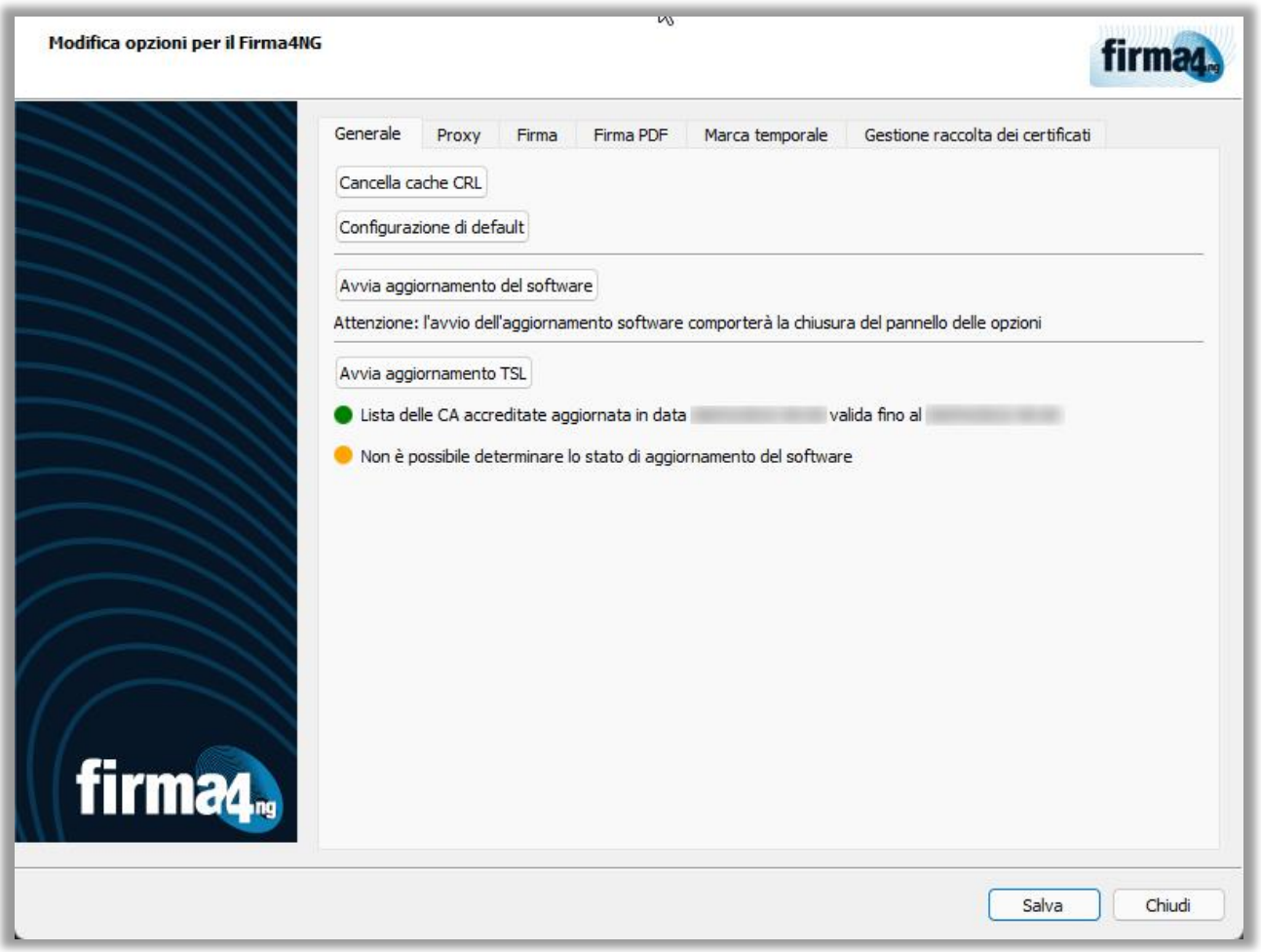


*Figura 42 – Opzioni – tab “Generale”.*

## Tab “Proxy”

In questa sezione (Figura 43) 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'.

Cliccare sul bottone "Salva" per salvare la nuova configurazione.

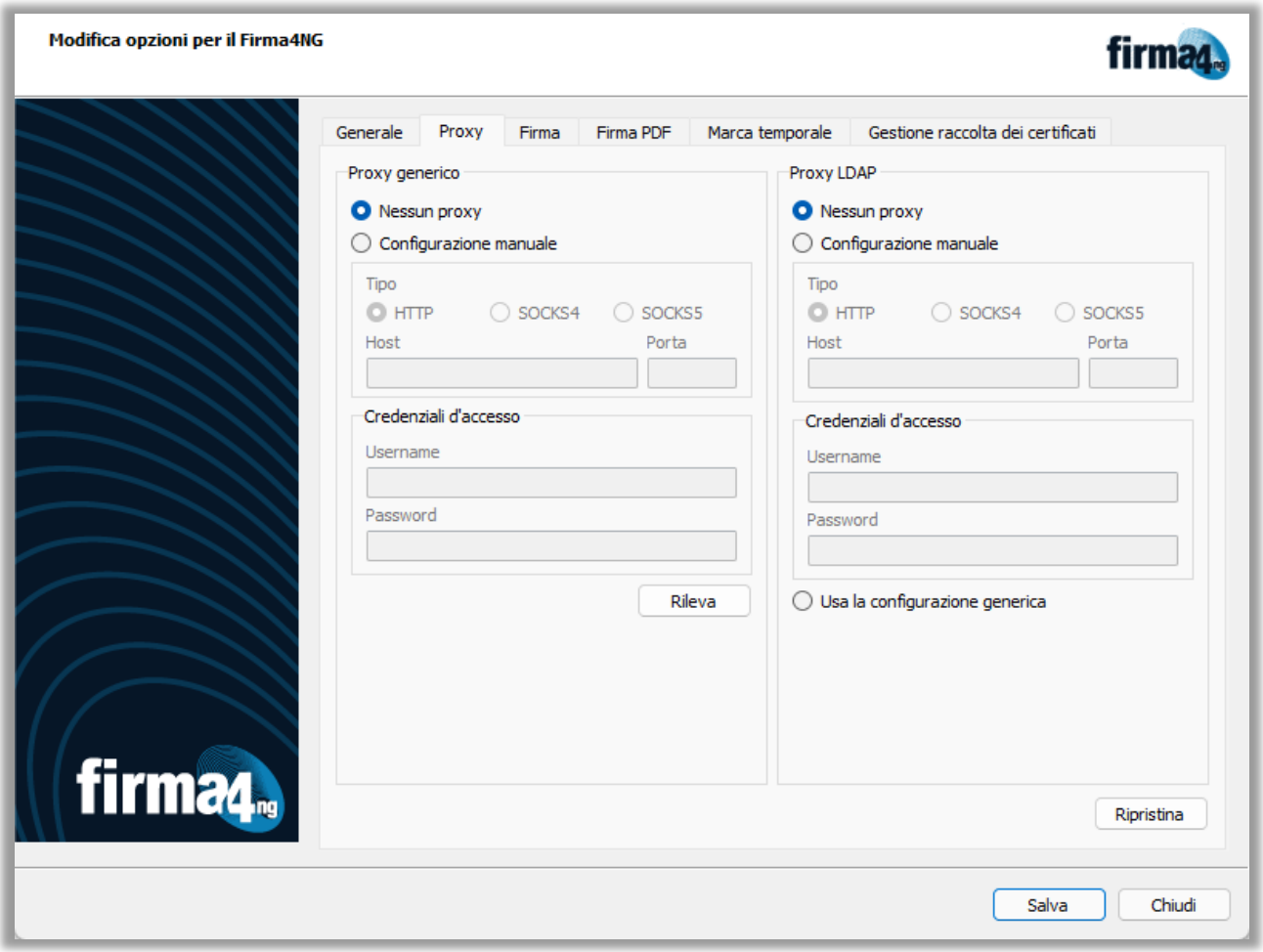


*Figura 43 – Opzioni – tab "Proxy".*

### Tab “Firma”

In questa sezione (Figura 44) è possibile configurare il formato in cui verranno salvati automaticamente i documenti firmati oppure selezionare l’opzione secondo la quale firma4ng seleziona automaticamente il formato di firma da applicare in funzione della tipologia del documento da firmare. È inoltre possibile:

- impostare una cartella di input dove prelevare i documenti firmati con la procedura di firma di più documenti;
- impostare una cartella di destinazione dove salvare i documenti firmati con la procedura di firma di più documenti;
- Selezionare la libreria PKCS 11 da utilizzare.

Cliccare sul bottone “Salva” per salvare la nuova configurazione.

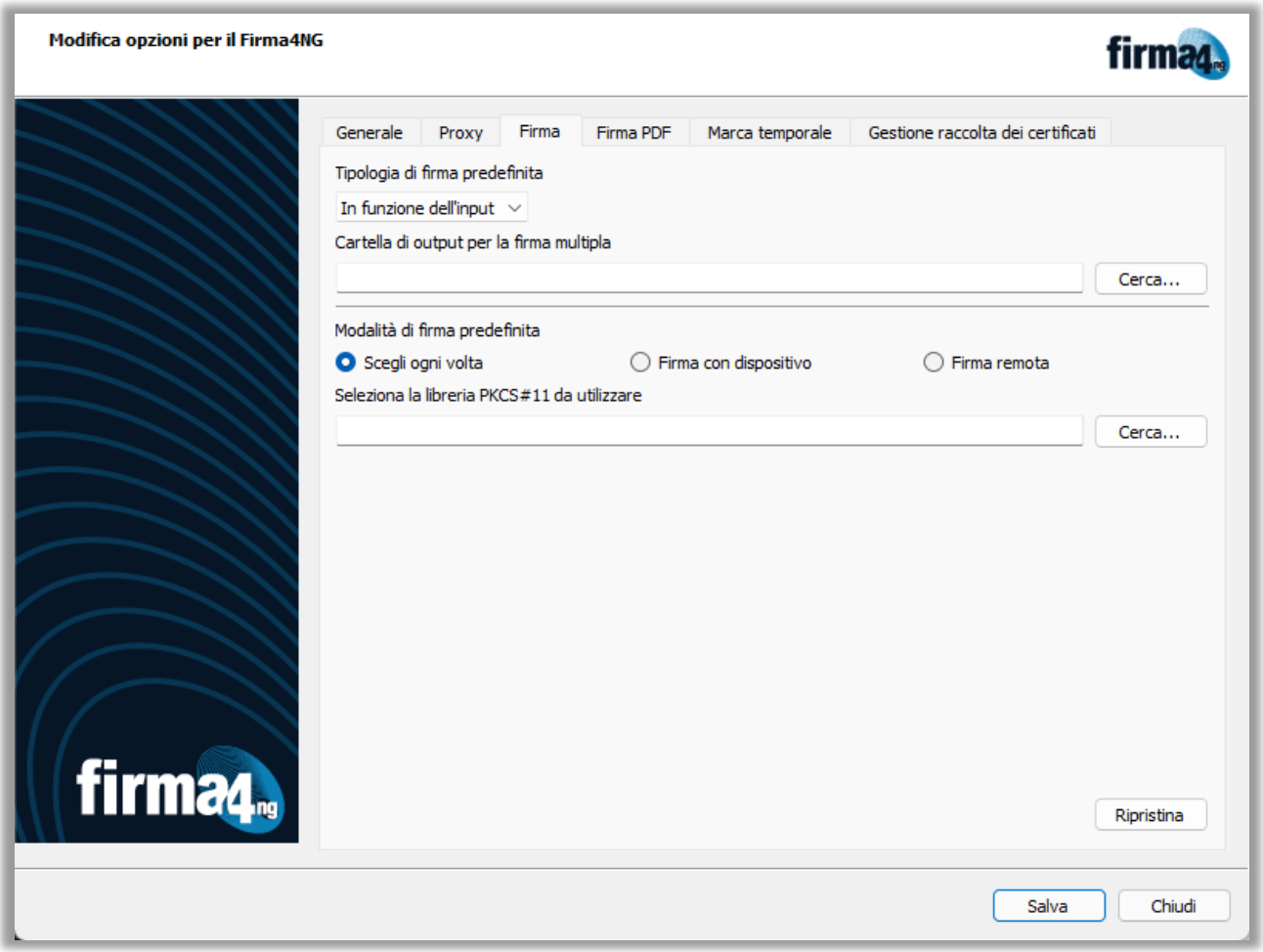


*Figura 44 – Opzioni – tab “Firma”.*

### Tab “Firma PDF”

In questa sezione (Figura 45) è possibile definire la configurazione standard da utilizzare per apporre la firma grafica in formato PDF, personalizzando i valori dei campi presenti.

Cliccare sul bottone “Salva” per salvare la nuova configurazione.

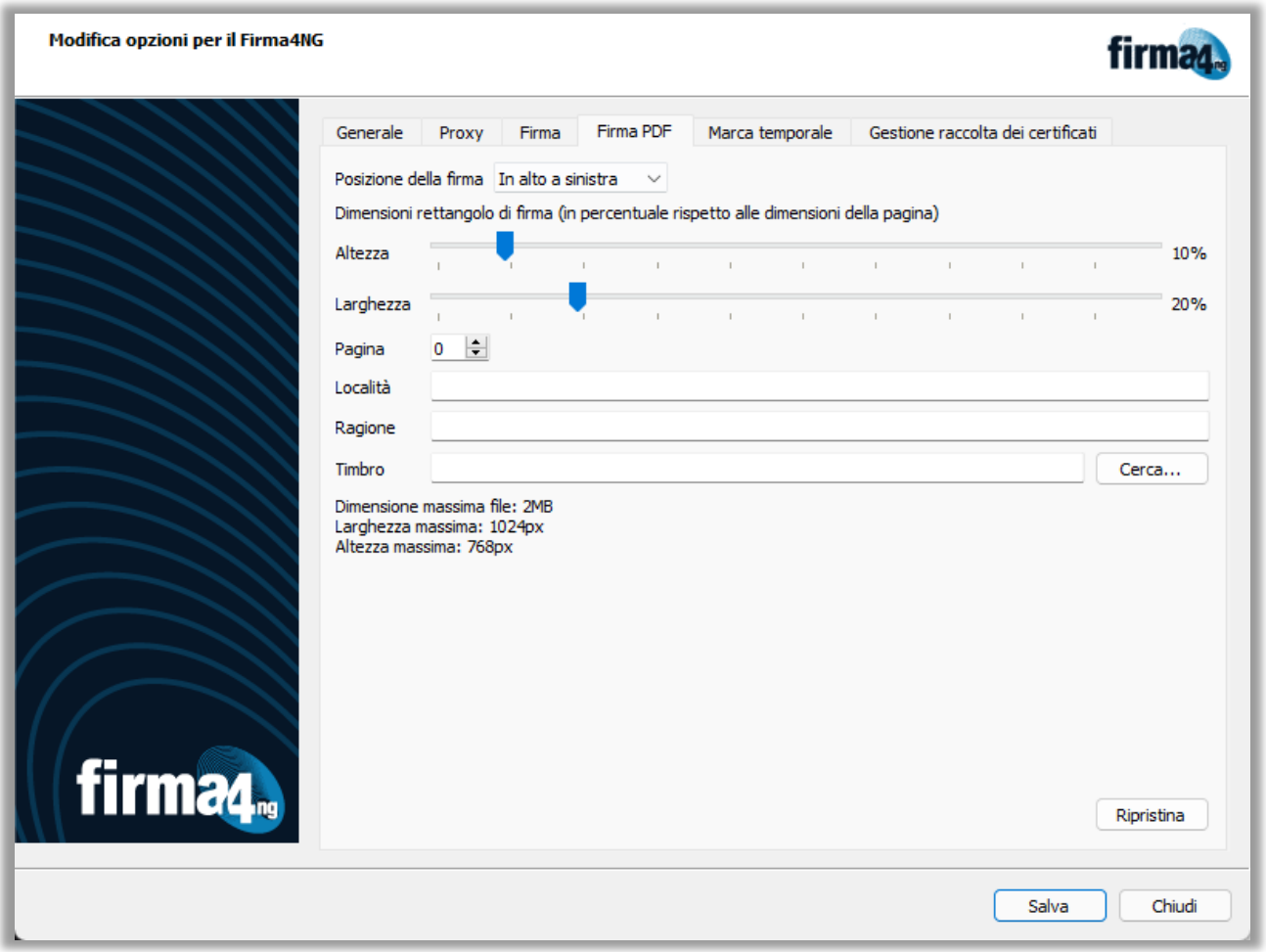


*Figura 45 – Opzioni – tab “FirmaPDF”.*

### Tab “Marca Temporale”

In questa sezione (Figura 46) è possibile configurare il servizio di Marcatura temporale da contattare per le richieste di marche temporali. La configurazione iniziale presenta come standard il servizio offerto da Infocert.

È comunque possibile configurare altri servizi di marcatura temporale, utilizzando il bottone “Nuovo” e valorizzando i parametri richiesti: Nome del servizio; Indirizzo della Time stamping authority ed opzionalmente Username; Password e Policy OID. Analogamente è possibile eliminare un servizio di marcatura temporale selezionandone il nome e cliccando sul bottone “Elimina”.

Cliccare sul bottone “Salva” per salvare la nuova configurazione.

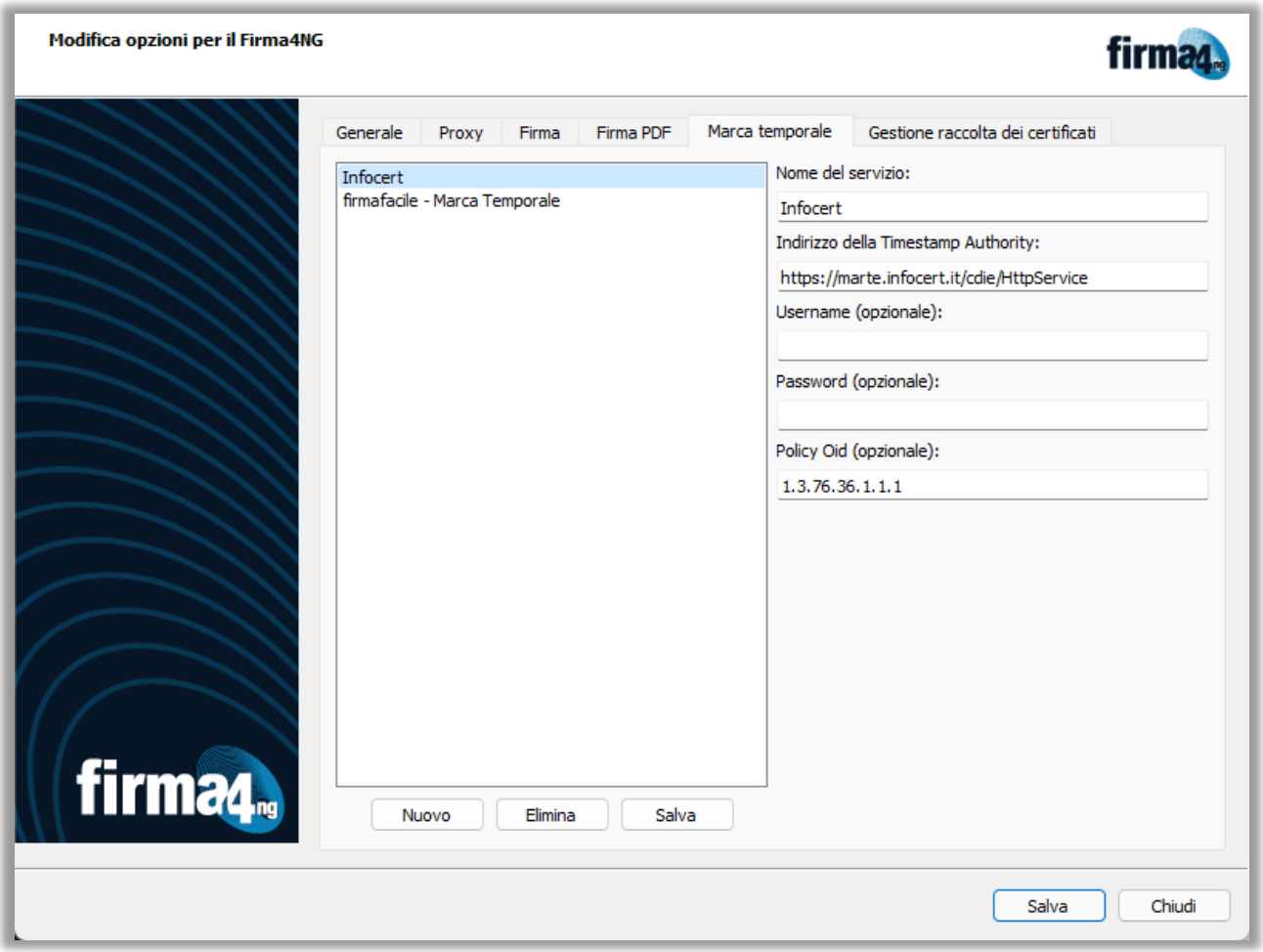


*Figura 46 – Opzioni – tab “Marca Temporale”.*

### Tab “Gestione Raccolta Certificati”

In questa sezione 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 sul bottone “Importa”, oppure ricercare sul registro pubblico dei certificati tenuto da Certificatore, dal tab “Servizio in linea”, selezionando l’indirizzo LDAP e la base di ricerca. Effettuata la ricerca, è possibile inserire i certificati trovati nella cartella “Contatti personali” utilizzando gli appositi bottoni.

Cliccare sul bottone “Salva” per salvare la nuova configurazione.

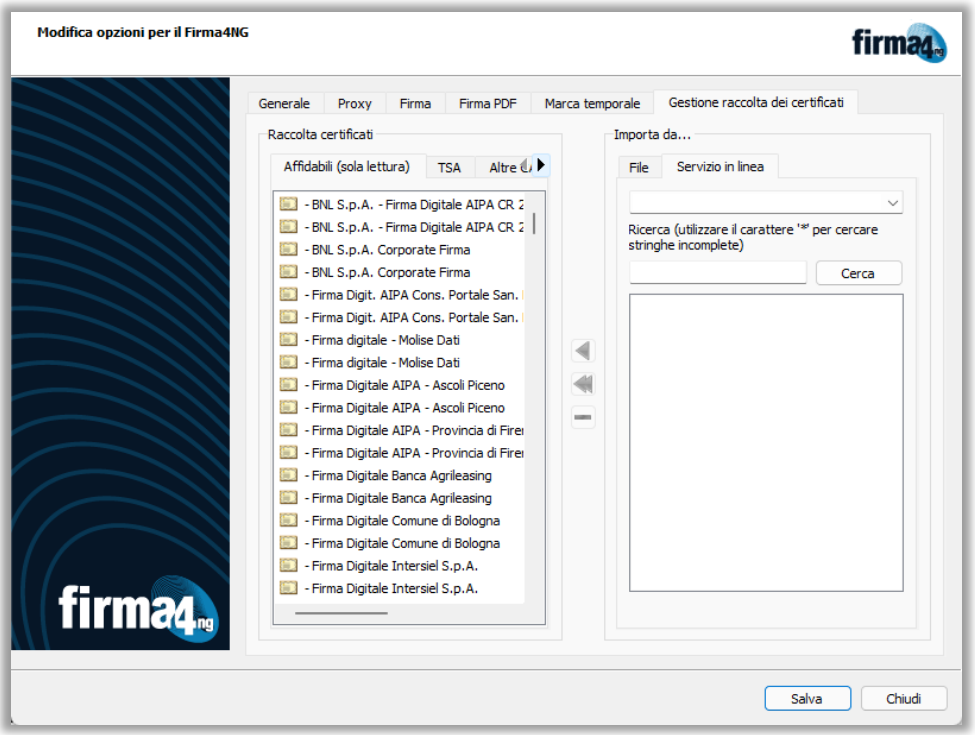


*Figura 47 – Opzioni – tab “Gestione raccolta dei certificati”.*

## CAMBIO PIN

Cliccando sul bottone “Cambio PIN” è possibile cambiare il codice PIN, inserendo nelle apposite caselle di testo il PIN attuale e il nuovo PIN scelto, confermando quest’ultimo una seconda volta.

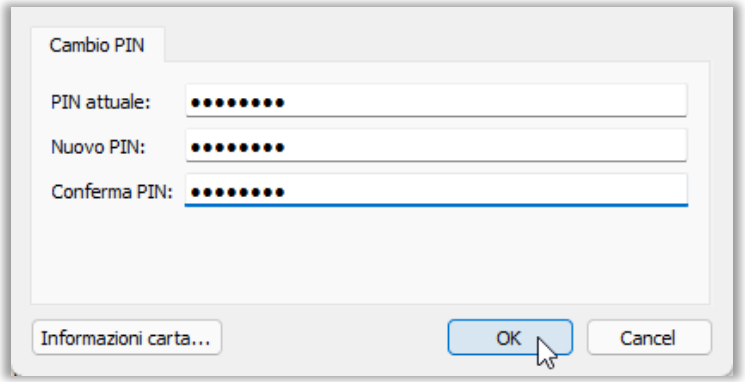


*Figura 48 – Cambio PIN.*

## SBLOCCO PIN

Cliccando sul bottone “Sblocco PIN” è possibile reimpostare il codice PIN nel caso lo si fosse smarrito, o se è stato bloccato dopo un numero eccessivo di tentativi errati di immissione. Ciò avviene inserendo nelle apposite caselle il codice PUK e il nuovo PIN, confermando quest’ultimo una seconda volta.

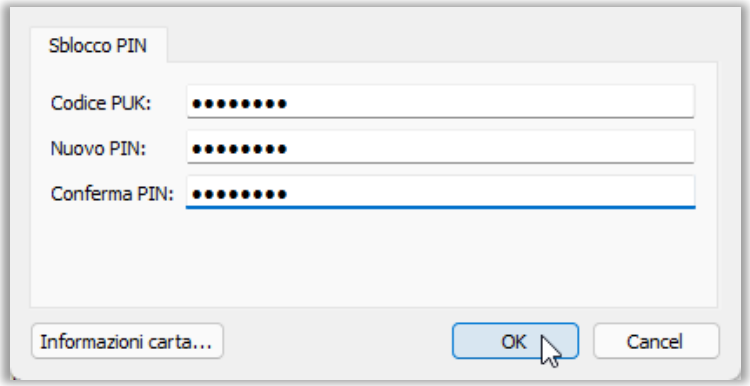


*Figura 49 – Sblocca PIN.*

## CAMBIO PUK

Cliccando sul bottone “Cambio PUK” è possibile cambiare il codice PUK, inserendo nelle apposite caselle di testo il nuovo PUK scelto e il PUK attuale, confermando quest’ultimo una seconda volta.

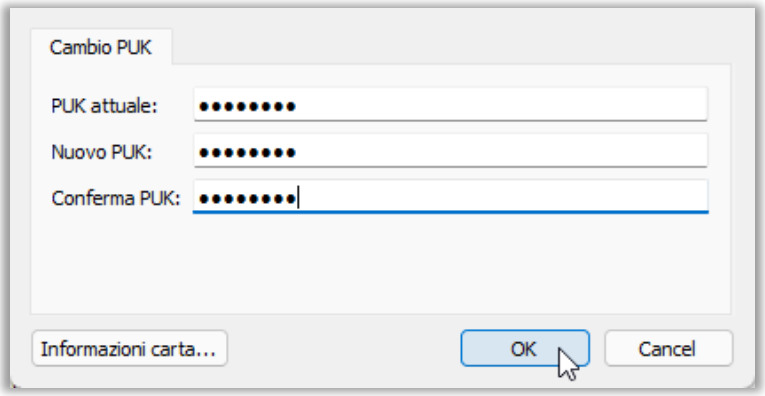


*Figura 50 – Sblocca PUK.*

## INFORMAZIONI CARTA

Una volta cliccato o sul bottone “Cambio PIN”, o sul bottone “Cambio PUK”, o sul bottone “Sblocca PUK” e possibile accedere al bottone “Informazioni carta” per visualizzare informazioni sulla smartcard e conoscere gli oggetti (certificati e chiavi) presenti su quest’ultima.

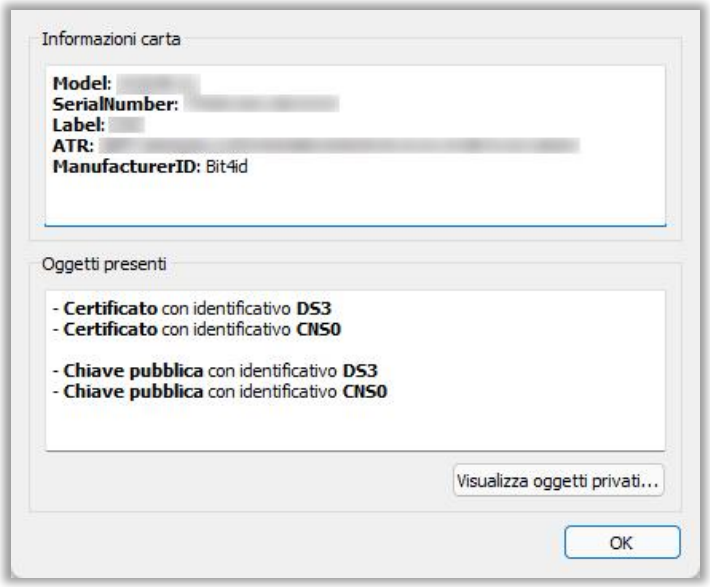


*Figura 51 – Informazioni carta.*

### IMPORTA CERTIFICATO

Il bottone “Importa Certificato” consente l’installazione del middleware che permette la comunicazione tra il lettore e software di terze parti. Questa funzionalità permette al sistema operativo e a programmi di terze parti di riconoscere ed utilizzare (in altre parole "importare") i certificati del dispositivo, e di poter effettuare operazioni come, ad esempio, l'autenticazione sui portali web www.inps.it o www.giustizia.it tramite la smart card o il token USB.

## AUTENTICAZIONE CON MOZILLA FIREFOX

Per autenticarsi con il browser Mozilla Firefox presente sul PC è necessario invece procedere alla seguente configurazione specifica:

- Eseguire il browser Mozilla Firefox;

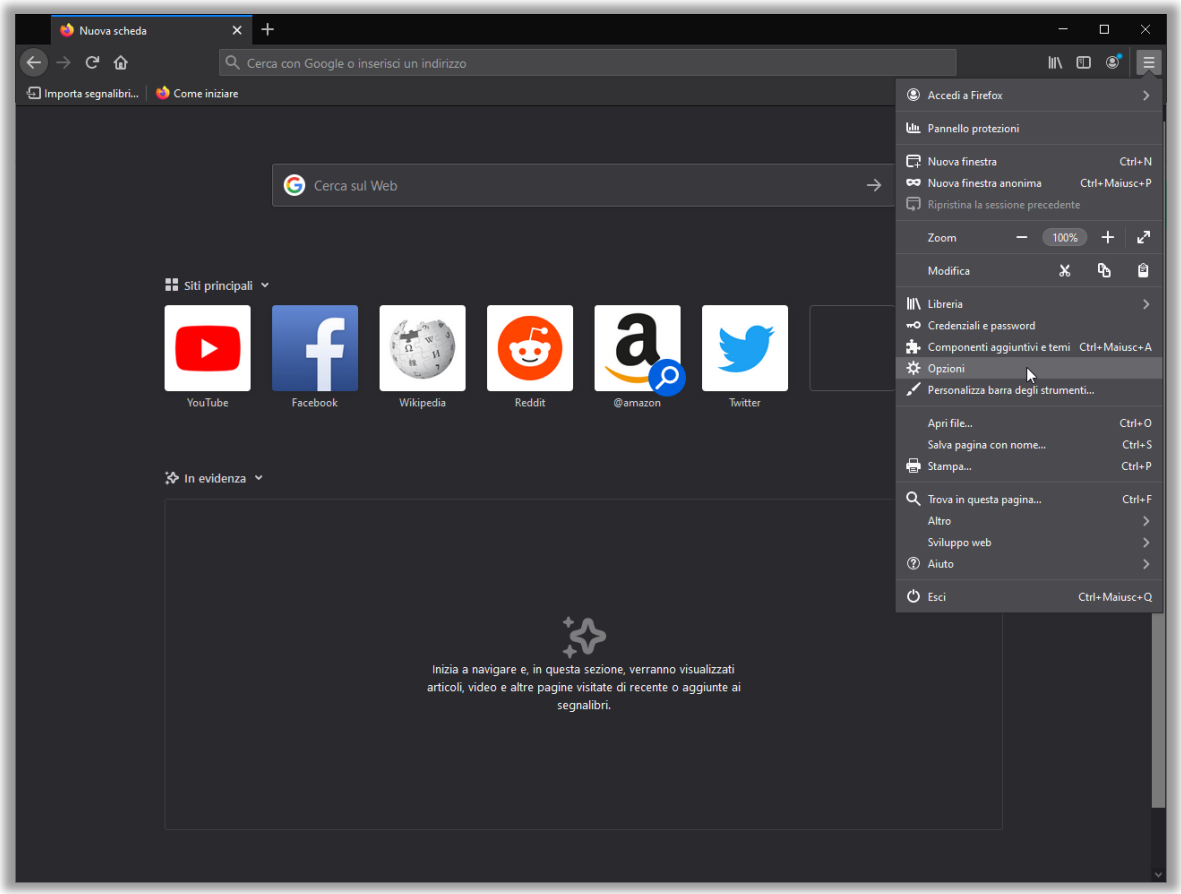


*Figura 52 – Mozilla Firefox.*

- Navigare il seguente percorso: Opzioni --> Privacy e Sicurezza --> Dispositivi di Sicurezza

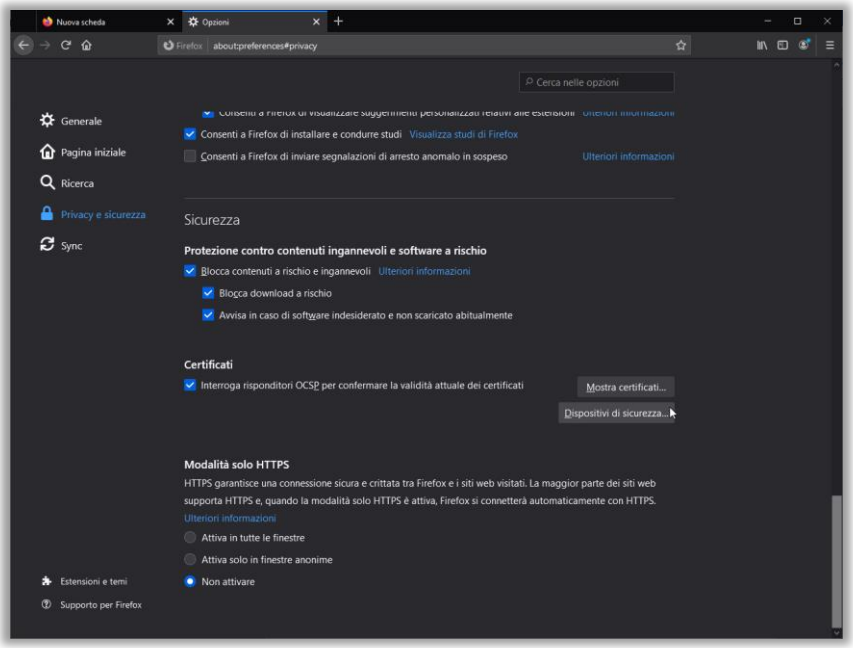


*Figura 53 – Dispositivi di Sicurezza in Mozilla Firefox.*

- Una volta aperta la finestra Gestione dispositivi bisognerà cliccare su Carica;

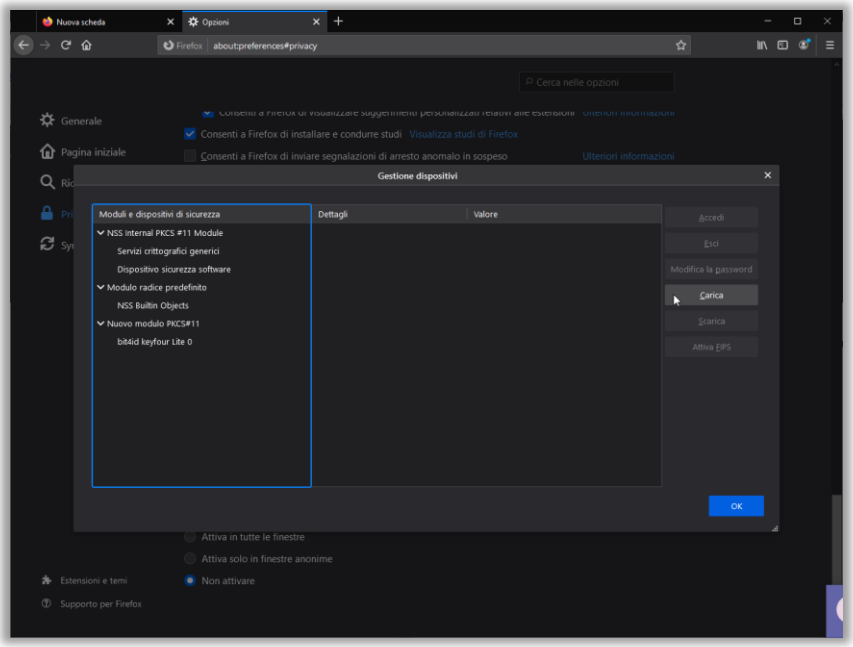


*Figura 54 – Carica.*

- Cliccare il tasto sfoglia;

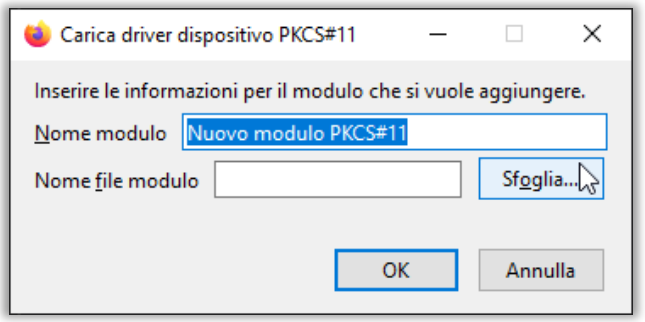


*Figura 55 – Carica driver.*

- Recarsi al percorso *C:/WINDOWS/SYSTEM32* e caricare il file **bit4xpki.dll** e poi premere Apri;

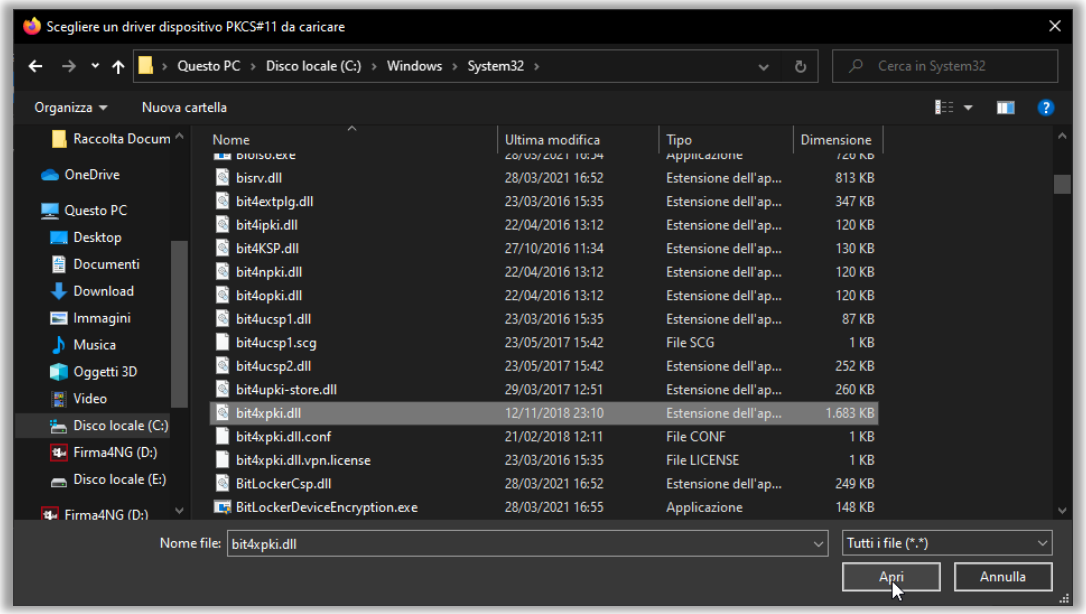


*Figura 56 – Selezione libreria.*

- Infine, cliccare su OK per poter concludere il corretto caricamento della necessaria libreria.

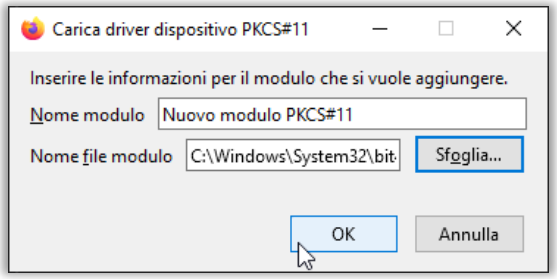


*Figura 57 – Caricamento libbreria.*

## AGGIORNAMENTO AUTOMATICO DI FIRMA4NG

firma4ng è inoltre dotato di una 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 si attiva se il PC è collegato ad Internet.


**ITALY**
NAPLES
Via Diocleziano, 107
80125 - Napoli
+39 081 7625600
+39 081 19731930
info@bit4id.com

**SPAIN**
BARCELONA
Edf. Bcn Advanced Industry Park
C. Marie Curie, 8-14
08042 – Barcelona
+34 935 35 35 18
info.es@bit4id.com

**PERU**
LIMA
Av. Antonio Miroquesada 360
piso 04 Ofic. 112
Magdalena del Mar
15076 – Lima
+51 1 242 9994
info.pe@bit4id.com

**INDIA**
GURGAON
D-201, G block, Sushant Lok 2
Gurgaon, Haryana, 122003
+91 837 583 3588
+91 958 220 3731
bit4idhelpdesk@gmail.com
bit4idindia@gmail.com

**UNITED KINGDOM**
LONDON
99 Cumberland Road
Plaistow
London E13 8LH
United Kingdom
+44 203 608 2566
+44 20 78553780
info@bit4id.com

**MACAU**
MACAU
Avenida da Praia Grande, 409,
China Law Building,
21/F and 23/F A-B, Macau
+853 2833 3332

**ECUADOR**
QUITO
Conocoto Pasaje S9 y García
Moreno
OE1 482 – Quito
Ecuador
+593 99 282 5835
info.ec@bit4id.com

**PORTUGAL**
LISBON
Rua A Gazeta de Oeiras, Nº 2, 2º B
2780-171 Oeiras
Lisboa
+351 214 694 060
info.pt@bit4id.com