firmaOK!

Manuale d’uso

Indice

1. Introduzione

1.1. Scopo del documento

Il presente manuale d'uso descrive le principali funzionalità dell'applicazione di firma digitale **firmaOK!** distribuita da Poste Italiane.

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
- gestione PIN e PUK del dispositivo crittografico (smart card o token USB)

2. firmaOK!: caratteristiche del software

2.1. Distribuzioni disponibili e requisiti software

L'applicazione **firmaOK!** viene distribuita nelle seguenti versioni:

- **firmaOK! Portable**, su token USB, garantisce il supporto con i sistemi operativi:
  - MS Windows 8, 10, 11;
  - macOS (ultime due versioni stabili);
  - Ubuntu (ultima LTS).
- **firmaOK! per Windows**, installazione disponibile per ambienti desktop Windows (8, 10, 11);
- **firmaOK! per macOS**, installazione disponibile per ambienti desktop macOS (ultime due versioni stabili);
- **firmaOK! per Ubuntu**, distribuito come archivio tar.gz per ambienti con ultima LTS;

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

2.2. Requisiti di sistema

Prima di utilizzare **firmaOK!**, 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. firmaOK! Portable

Questa versione dell'applicazione viene distribuita a bordo di token USB. Non richiede alcuna installazione da parte dell'utente. Trattandosi di una versione multipiattaforma, la modalità di avvio dell'applicazione sono conformi al comportamento standard del sistema operativo sul quale **firmaOK!** deve essere utilizzata.

Windows

Se è attiva la funzione di esecuzione automatica (autorun), quando si collega il token USB al computer, verrà avviata automaticamente la splashscreen di Figura 1.

Nel caso in cui la funzione di esecuzione automatica non sia abilitata, per avviare l'applicazione sarà necessario navigare nella cartella principale del token USB e cliccare sul file "autorun.exe".

macOS

In analogia a quanto descritto nel paragrafo precedente, per avviare l'applicazione è necessario visualizzare la cartella principale del token USB ed avviare il file "Firma4NG.app".

Linux

Per avviare **firmaOK!** occorre eseguire l'applicazione "autorun.sh", presente nella cartella principale del token USB.

Figura 1. Splashscreen PosteKey

Una volta avviata la splashscreen, indipendentemente dal sistema operativo su cui ci si trova è sufficiente selezionare l'ultimo pulsante in basso contrassegnato dal logo "firmaOK!" per avviare il programma di firma digitale. A questo punto apparirà sullo schermo il menu principale di firmaOK!:

Figura 2. firmaOK! - menu principale

2.4. firmaOK! per Windows

Per installare l'applicazione su sistemi operativi Windows, 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 firmaOK!.

2.5. firmaOK! per macOS

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

2.6. firmaOK! per Ubuntu

Per installare l'applicazione su sistemi operativi Linux Ubuntu 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.

3. 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 paragrafi che seguono.

Prima di avviare l'operazione è bene controllare di aver inserito la smart card nel lettore o collegato il token USB al PC.

3.1. 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 documenti sul pulsante "Firma" (Figura 2);
- Cliccando sul pulsante "Firma" (Figura 2) e selezionando il/i documenti da firmare dalla finestra di navigazione del PC (Figura 3).

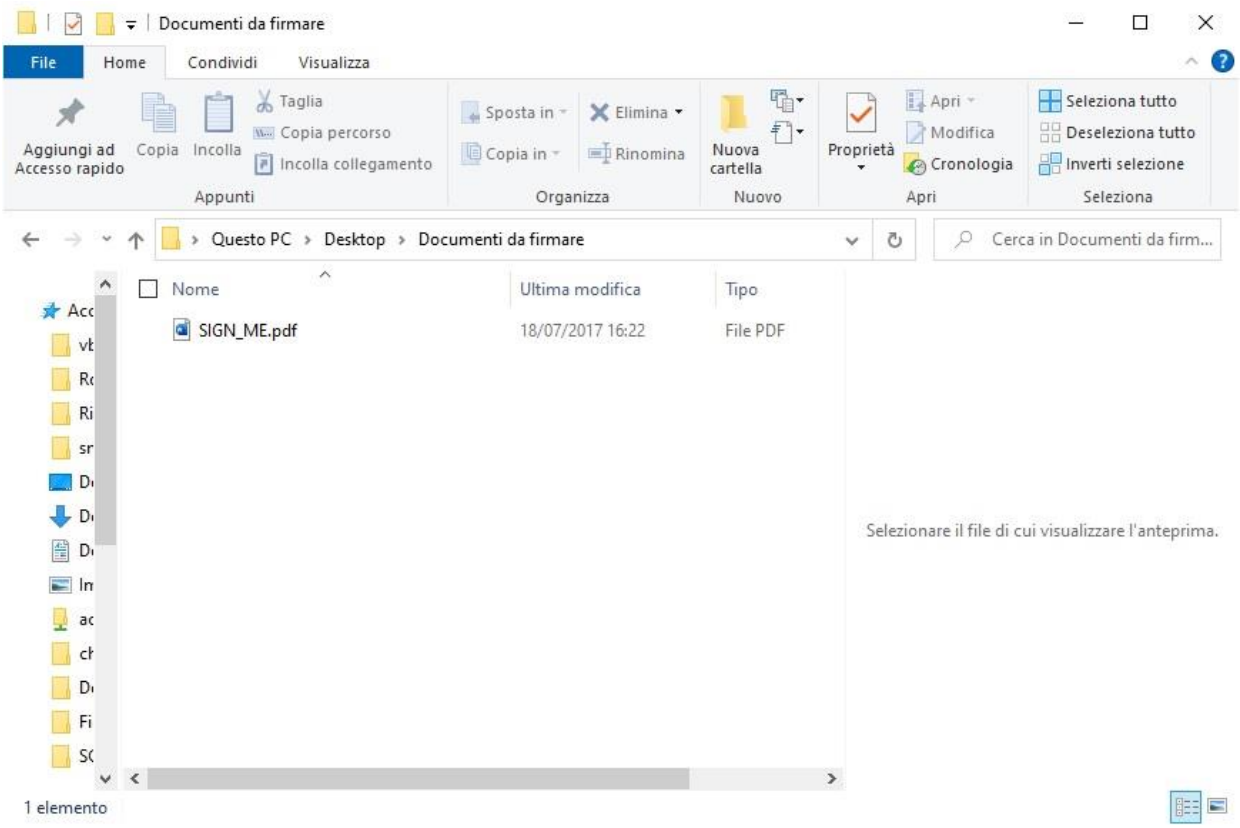


Figura 3. Selezione del file da firmare

Fase 2

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

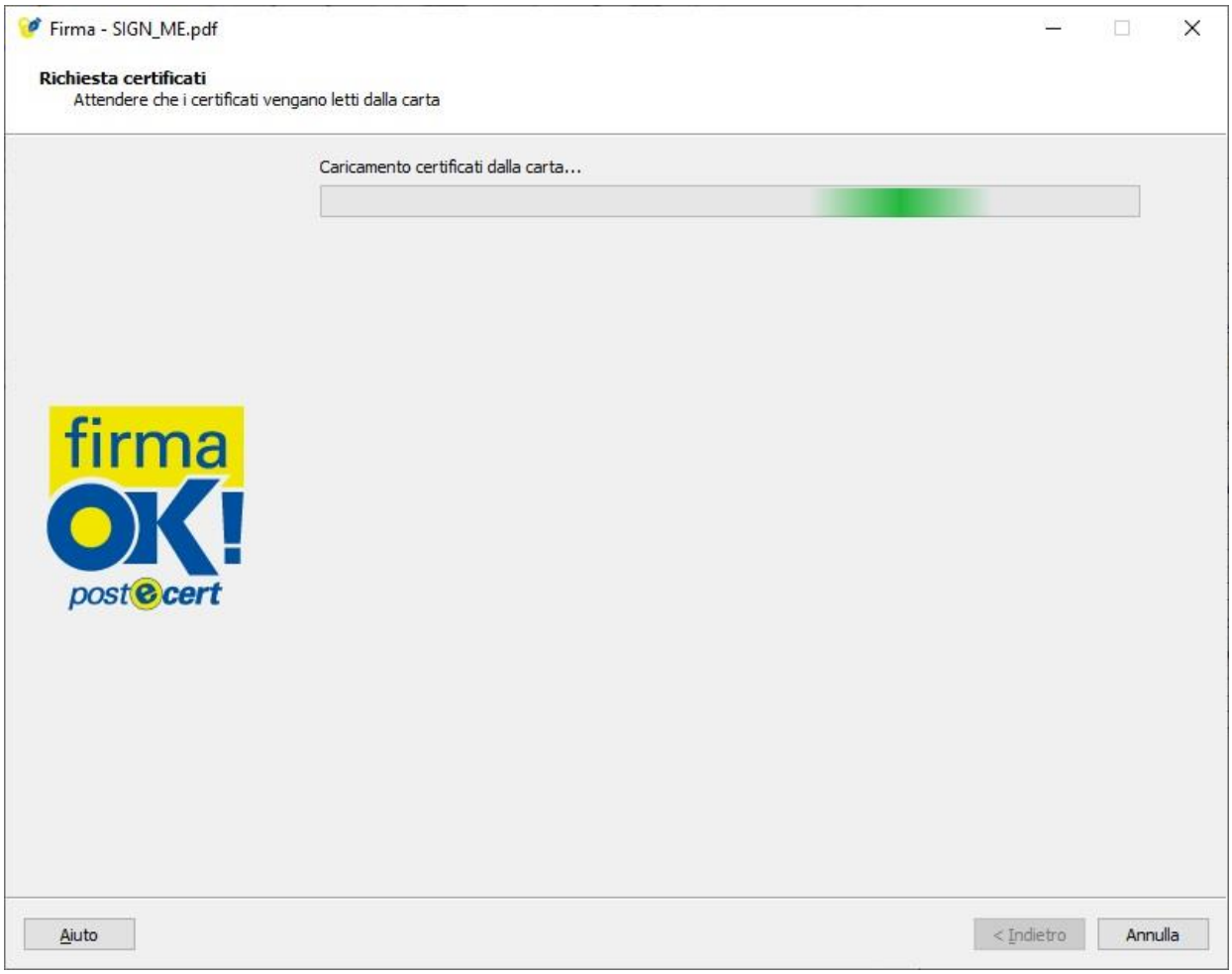


Figura 4. Caricamento certificati dai dispositivi crittografici collegati (smartcard/token)

Fase 3

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

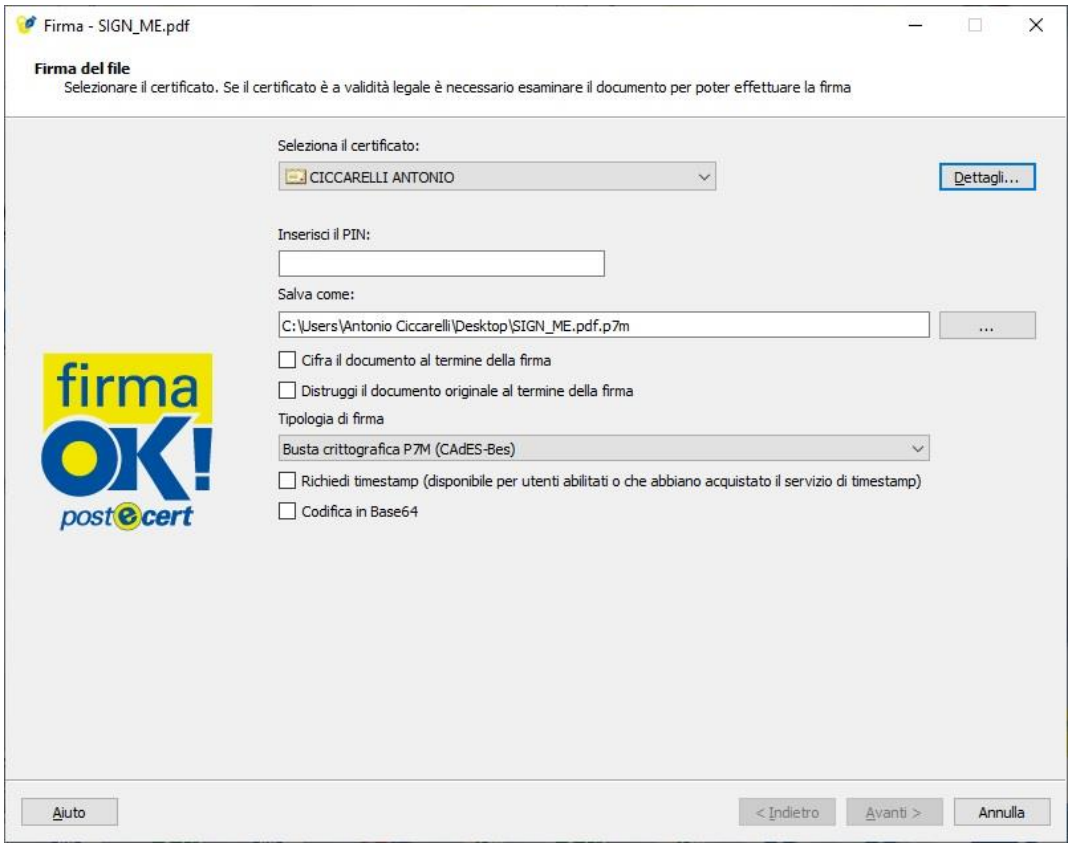


Figura 5. Interfaccia di firma

Viene mostrato come già selezionato il certificato per la firma digitale (o di "non ripudio"), individuato da "COGNOME NOME".

Nota: per controllare che il certificato selezionato è quello di firma digitale, è possibile visualizzarne i dettagli cliccando sul pulsante "Dettagli..." (Figura 5).

Per procedere con l'operazione di firma occorre:

- selezionare nell'apposito menu a tendina il certificato di firma digitale (individuato da "COGNOME NOME");
- inserire il PIN della smart card o del token USB;
- selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "..." della sezione "Salva come:" se si desidera modificare la cartella preimpostata (quella che contiene il documento originale);
- selezionare la tipologia di firma che si vuole apporre al documento dal menu a tendina. I formati di firma a disposizione sono (Figura 6):
    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 un 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 pulsanti "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica";

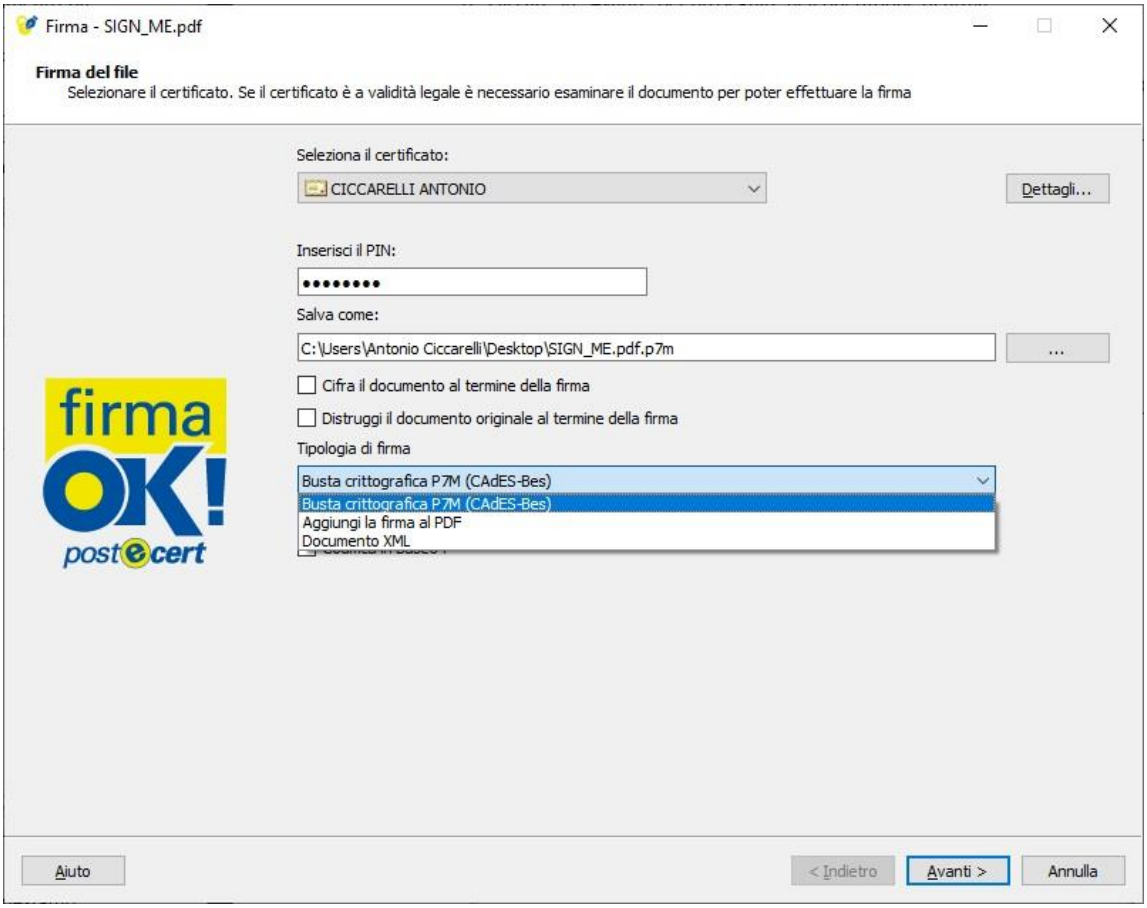


Figura 6. Tipologia di firma

- 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, come descritto al parag. 5, il servizio da utilizzare per richiedere la marca temporale;

- 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.

- Se i documenti da firmare sono più d'uno, l'applicazione richiederà di inserire il PIN tante volte quanti sono i documenti selezionati. Per disabilitare la richiesta del PIN ad ogni operazione di firma, basterà andare nella sezione "Firma" del menu "Opzioni", deselezionare la casella "Richiedi il PIN della smart card per ogni file in caso di firma massiva" e salvare la nuova configurazione cliccando sul pulsante "Salva".

Fase 5

Attendere che il documento selezionato venga firmato.

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 pulsante "Termina".

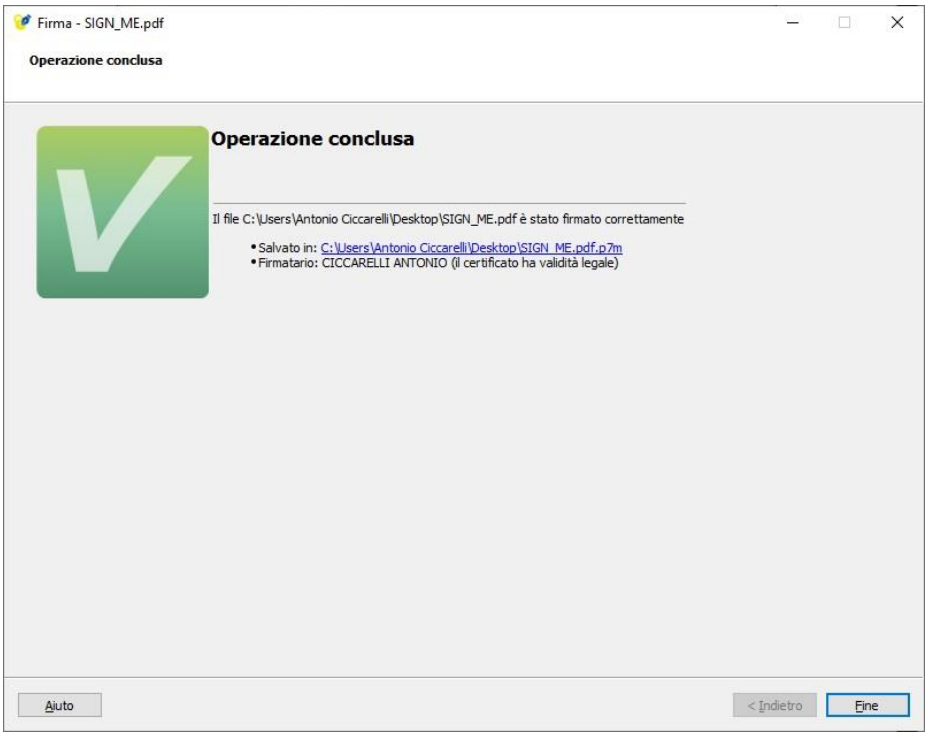


Figura 7. Conclusione operazione di firma

3.2. Funzioni avanzate di firma: Firma multipla e Firma semplice

Selezionando un documento firmato in formato p7m e trascinandolo (funzionalità "drag&drop") sopra il pulsante di "Firma" della schermata principale dell'applicazione, si accederà alle operazioni di Firma multipla o Firma semplice:

Figura 8. Selezione Firma multipla o Firma semplice

Firma multipla

Se si desidera apporre al documento firmato una nuova firma, parallela o controfirma, basterà selezionare il pulsante "Firma multipla".
Al termine dell'operazione di verifica sarà possibile selezionare la tipologia di firma che si vuole apporre: dopo aver selezionato il certificato del firmatario di interesse, per la "Firma parallela" si dovrà selezionare

il primo pulsante dall'alto nella colonna di destra, per la "Controfirma" occorrerà invece selezionare il secondo pulsante dall'alto (Figura 9).

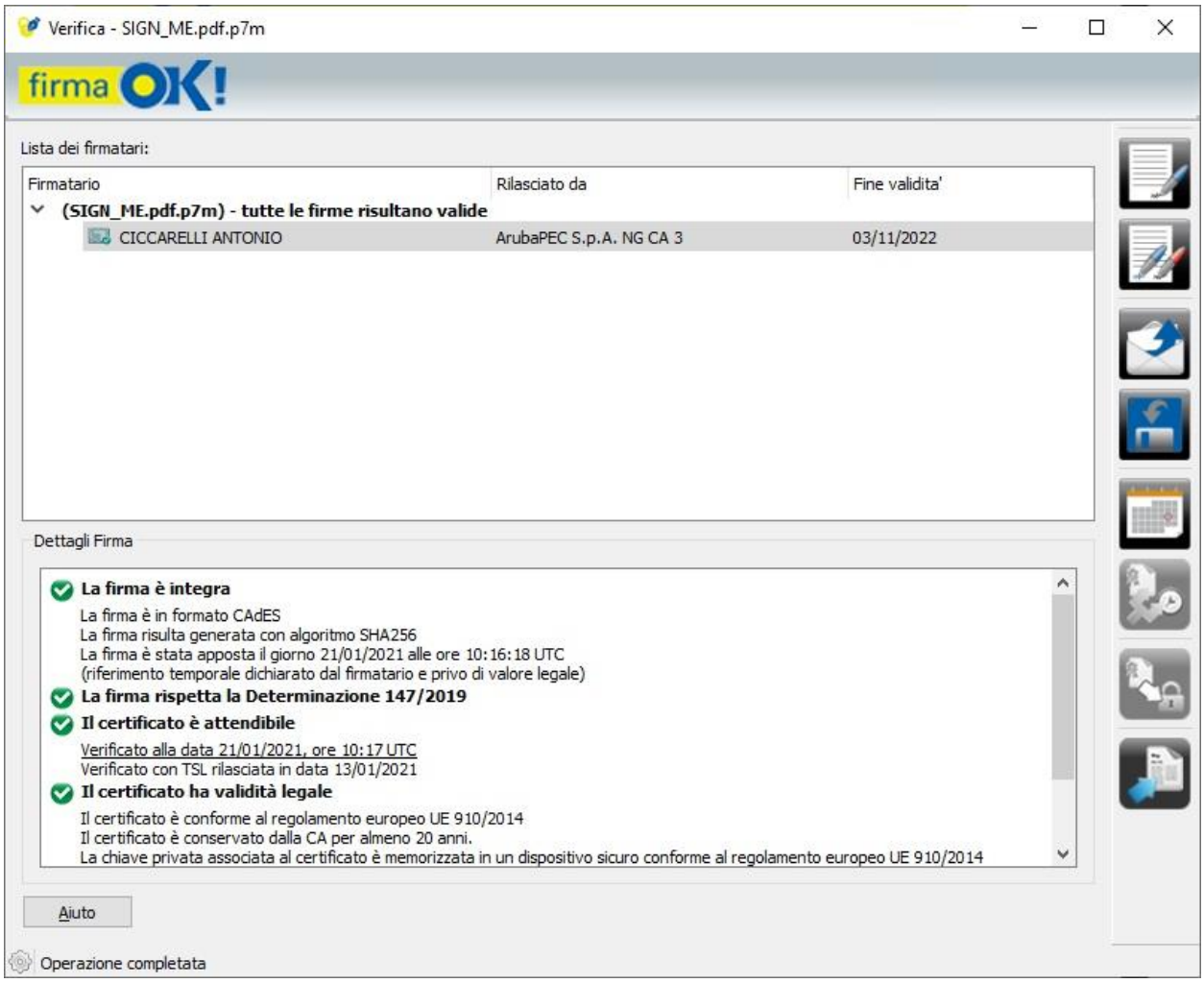


Figura 9. Selezione firma Parallela o Controfirma dal pannello di verifica

Di seguito sono elencate le differenze, sia dal punto di vista dei formati che dal punto di vista formale, delle due tipologie di firma multipla sopra indicate:

- **Firma parallela**: la firma viene aggiunta allo stesso livello di tutte le firme già presenti sul documento. Questa firma è apposta sullo stesso contenuto delle firme precedenti e viene di norma utilizzata per aggiungere firme ad un documento già firmato in quei processi documentali che ne prevedono l'utilizzo.
- **Controfirma**: la firma viene apposta sulla firma selezionata e di fatto sottoscrive quest'ultima. Questo aspetto è messo in evidenza attraverso una rappresentazione indentata (ad albero) delle firme.

Firma semplice (o "matrioska")

Selezionando l'operazione "Firma semplice" il documento verrà nuovamente firmato; il risultato di questa operazione sarà un documento con tante estensioni ".p7m" quante sono le firme semplici ad esso apposte.

3.3. Firma di documenti PDF

Se si desidera apporre una firma su un documento PDF, occorre selezionare dal menu a tendina la tipologia di firma "Aggiungi la firma al PDF" (Figura 10) 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 "Firma PDF" del menu "Opzioni"; sarà comunque possibile modificare la configurazione spuntando la casella "Modifica opzioni" e personalizzando le opzioni di firma PDF.

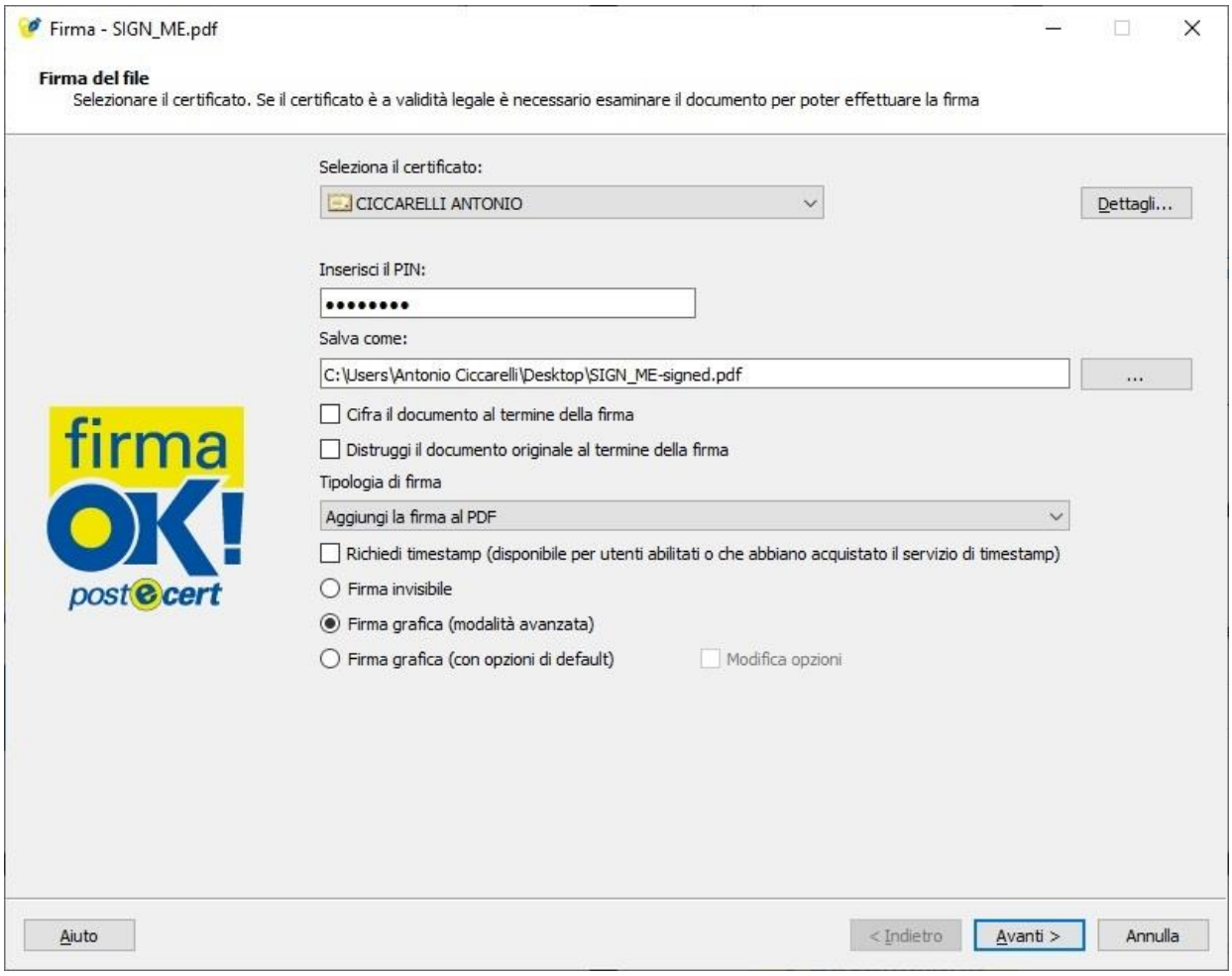


Figura 10. Dettaglio delle opzioni di firma PDF

Più in dettaglio, nel caso in cui si sia selezionata la "**Firma grafica (modalità avanzata)"** verrà mostrata la seguente schermata (Figura 11) per la selezione e il posizionamento della grafica.

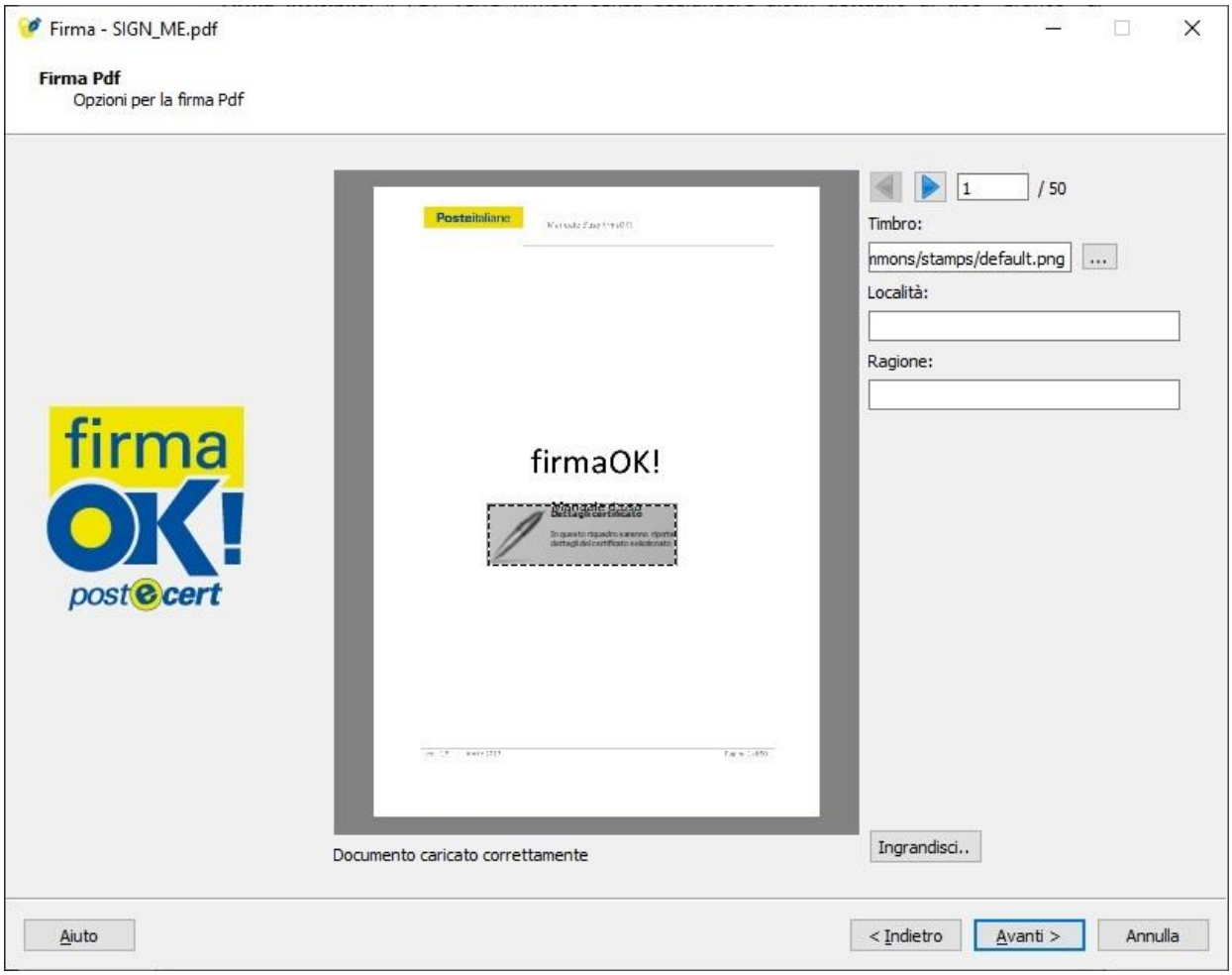
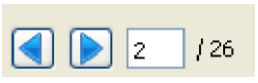


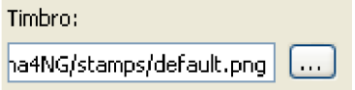
Figura 11. Firma grafica PDF

Dalla schermata è possibile pertanto:

a. selezionare la pagina dove apporre la firma:



b. selezionare l'immagine da associare alla firma:



c. inserire i campi "Località" e "Ragione" da aggiungere (eventualmente) alla firma:

d. ingrandire la schermata di apposizione della firma grafica, mediante un click su "Ingrandisci"

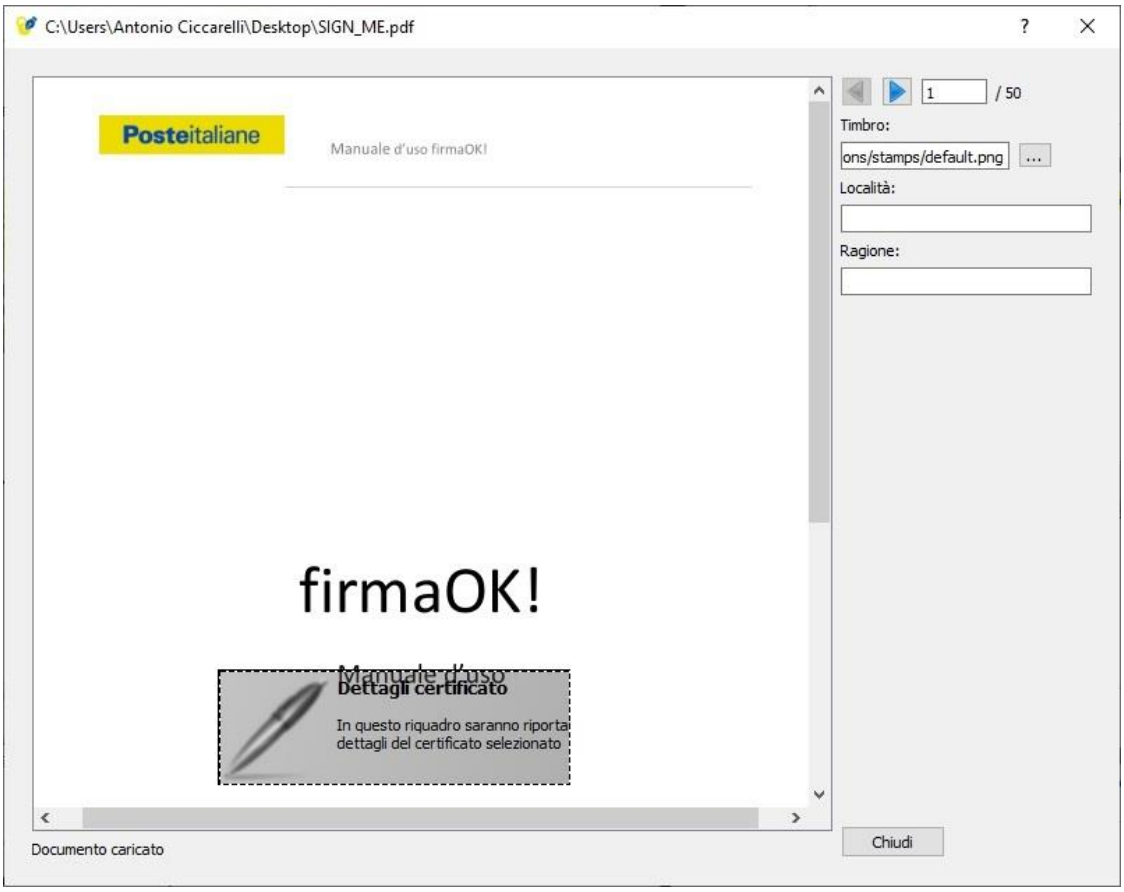


Figura 12. Firma grafica PDF - zoom

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 13):

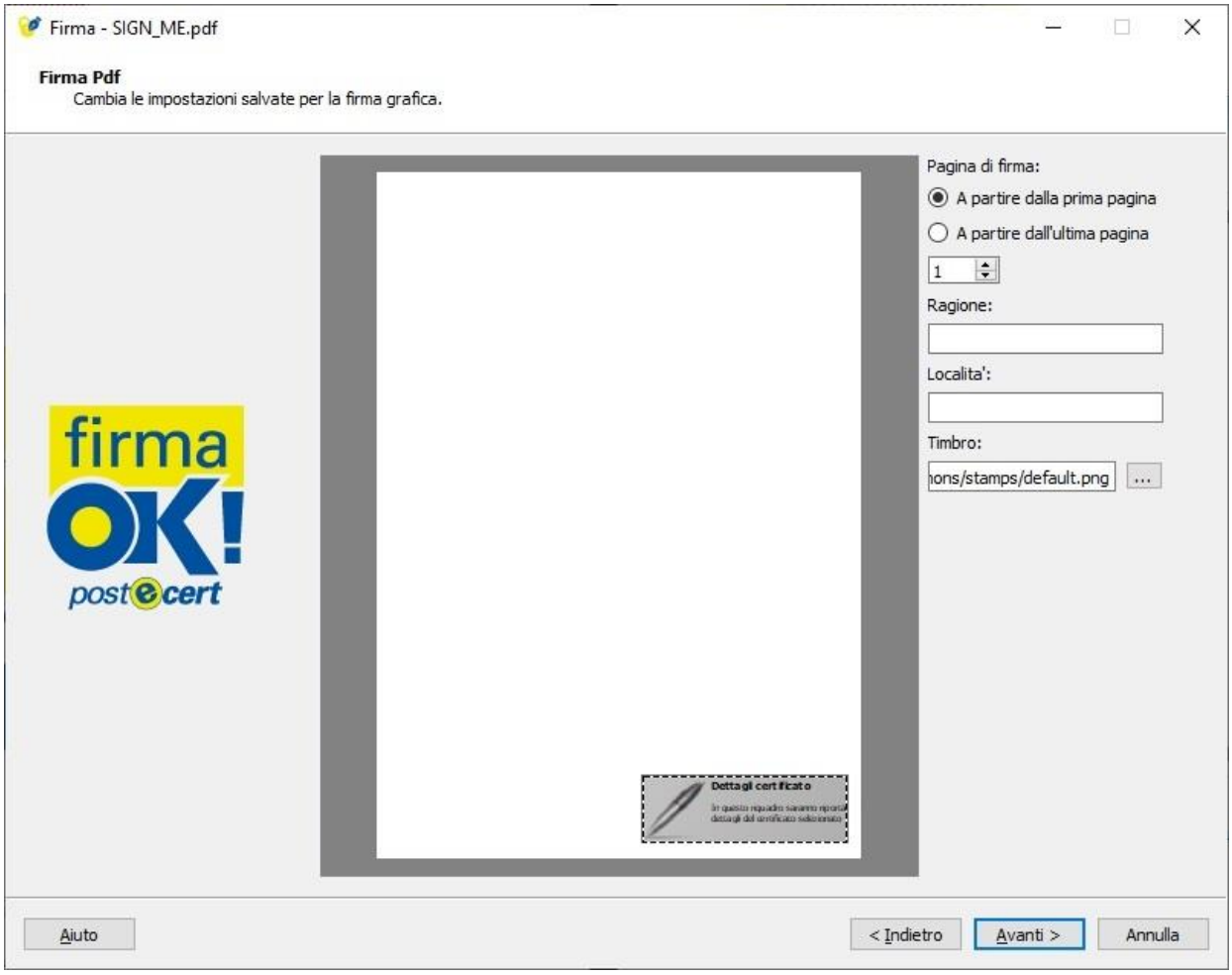


Figura 13. Firma grafica PDF – modifica opzioni

dalla quale 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 del paragrafo 4.1.

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

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

3.3. Firma remota

Questa funzionalità è disponibile soltanto nella versione installabile del firmaOK!, pertanto i token USB, che portano a bordo la versione portable del programmi di firma, ne sono esenti. Se si desidera apporre una firma remota su un documento, occorre selezionare dal menu principale l'opzione Firma.

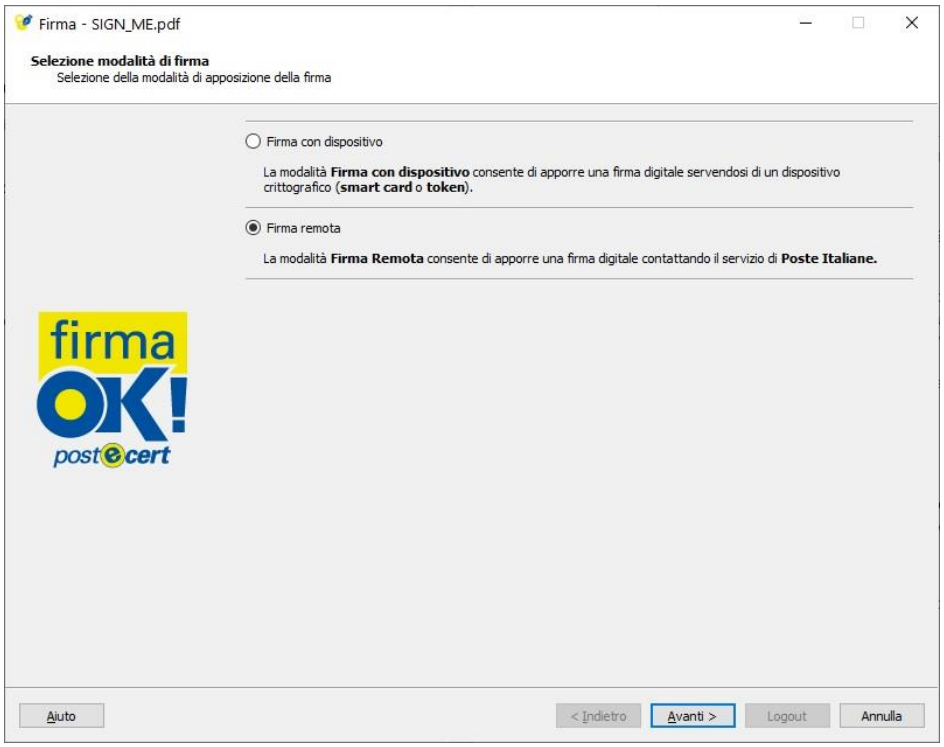


Figura 14. Selezione della tipologia di firma (tramite certificato remoto o locale)

Comparirà la schermata di selezione sulla tipologia di firma che si intende apporre. Selezionare "Firma remota" e attendere che compaia la schermata di autenticazione come nella figura sottostante.

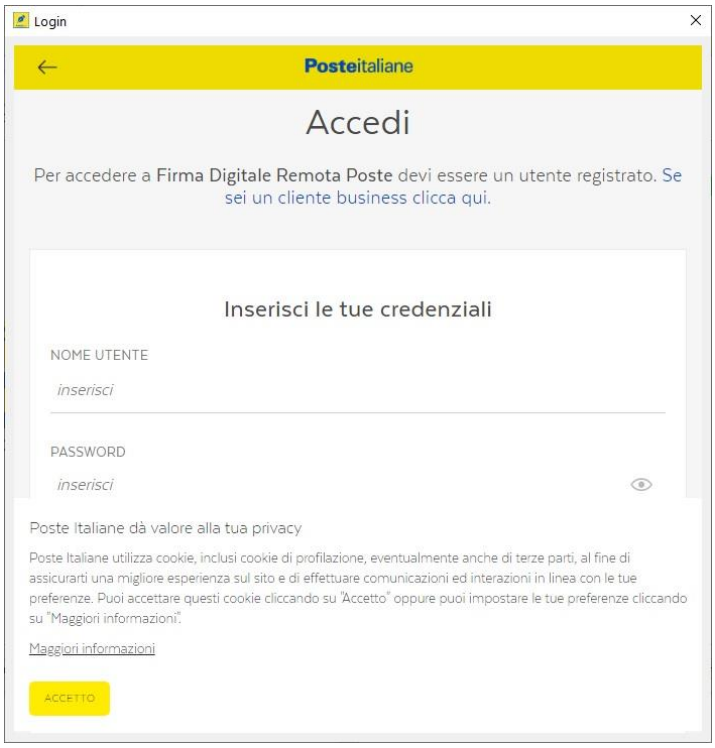


Figura 15. Inserimento credenziali di firma remota

Inserire nelle apposite caselle testuali il nome utente e la password con cui si è registrati sul portale delle Poste Italiane per la firma remota. Se l'autenticazione avrà buon fine, comparirà la consueta schermata del software firmaOK! da cui sarà possibile inserire il PIN e modificare impostazioni sul formato della firma. In caso contrario, comparirà un errore e si verrà invitati a ripetere la procedura di autenticazione.

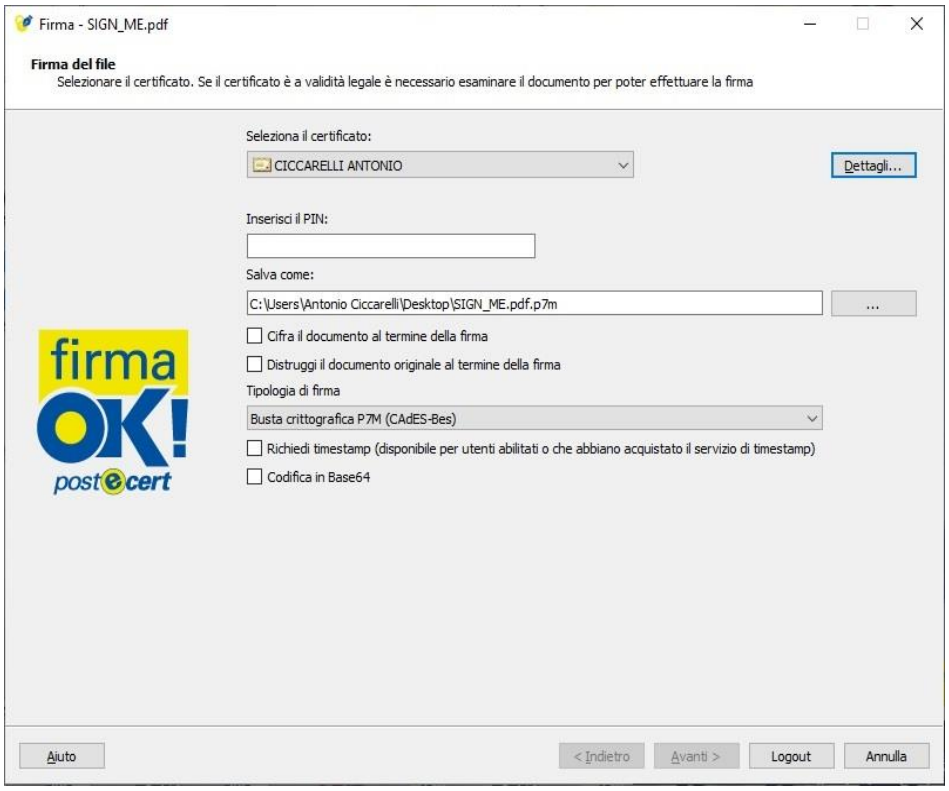


Figura 16. Schermata di selezione certificato di firma remota

Una volta comparsa la schermata in fig. 16, occorrerà procedere come una comune firma, inserendo il PIN e cambiando all'occorrenza le impostazioni presenti a schermo. Cliccando sul pulsante "Logout" sarà possibile scollegare il proprio account contenente i certificati di firma remota, altrimenti cliccare "Avanti" per procedere con la firma e la richiesta della OTP (One Time Password) che verrà inviata sul numero del dispositivo mobile indicato in fase di adesione sulla pagina di registrazione di Poste Italiane.

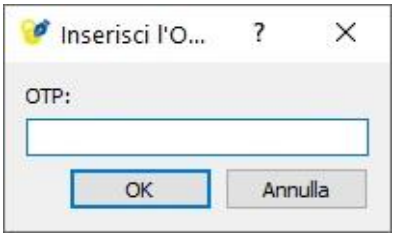


Figura 17. Schermata di inserimento OTP (One Time Password) contestualmente ad una firma

Inserire nell'apposita casella testuale il codice numerico riportato nel messaggio inviato tramite SMS sul numero del dispositivo mobile e cliccare sul pulsante "OK". La One Time Password non ha scadenza temporale, bensì resta valida fino al suo utilizzo. Una volta inseriti i dati correttamente, la firma verrà apposta sul documento nei modi e nei termini configurati inizialmente.

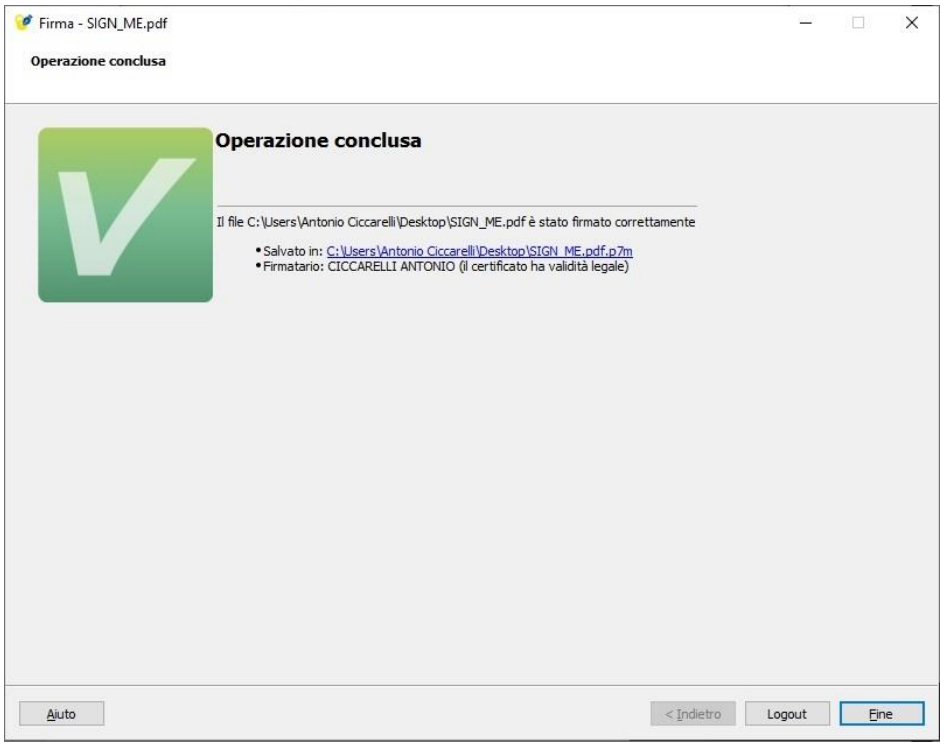


Figura 18. Apposizione della firma digitale con certificato remoto conclusa con successo

Il documento è ora pronto per essere verificato.

4. Apposizione di marche temporali

Per apporre una marca temporale su un documento, firmato o meno, occorre cliccare sul pulsante "Marca temporale" presente nel menu principale dell'applicazione.

Si fa presente che l'operazione di marcatura temporale, interagendo con un servizio in linea, necessità della connessione a Internet.

Nota: firmaOK! permette l'apposizione di una marca temporale contestualmente all'operazione di firma. In questo caso, si aprirà una finestra (Figura 19) attraverso la quale è possibile configurare un servizio di marcatura temporale, se si desidera utilizzare un servizio diverso da quello presentato come già selezionato.

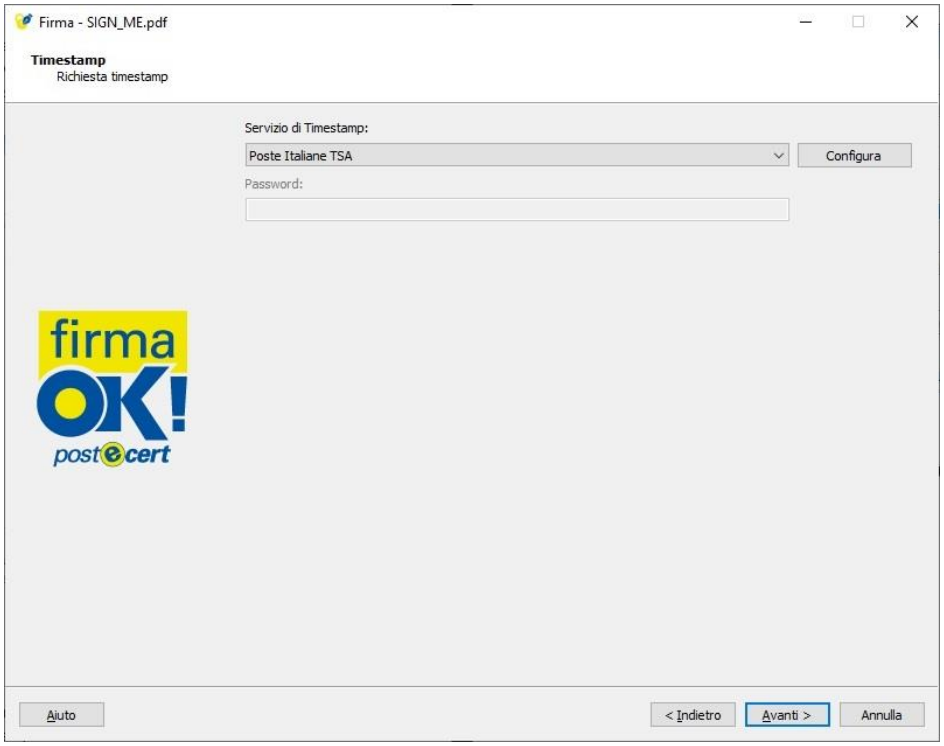


Figura 19. Marca temporale (contestualmente a un'operazione di firma)

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 pulsante "Marca Temporale" del menu principale;
- cliccare sul pulsante "Marca Temporale" del menu principale e selezionare il documento dalla finestra di navigazione del PC.

Fase 2

Si aprirà una finestra (Figura 20) 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 menu a tendina (Figura 21):

- **.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

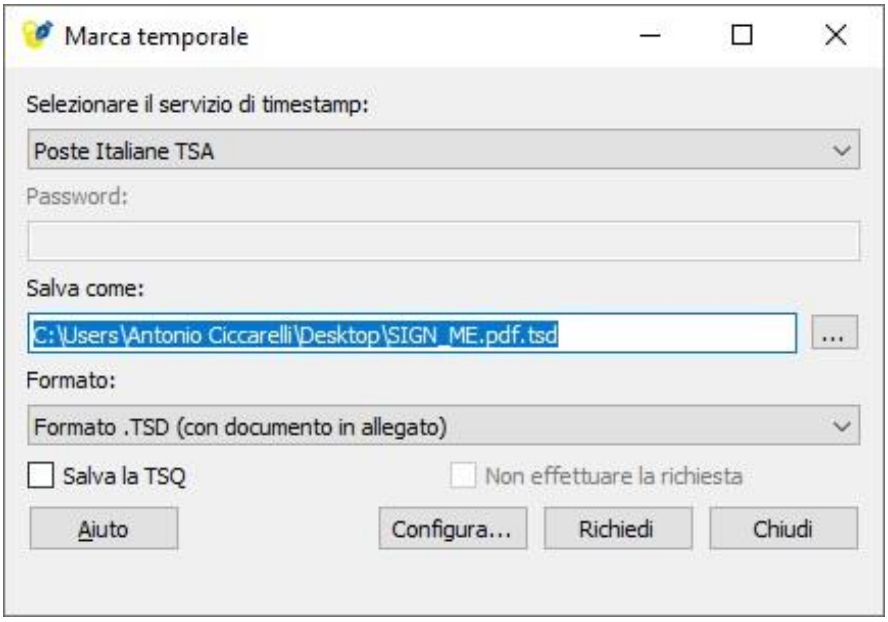


Figura 20. Marca temporale (da pulsante "Marca temporale" del menu principale)

firmaOK! supporta infatti tutti i formati di marche temporali previsti dagli standard e dalla normativa Nazionale.

Fase 3

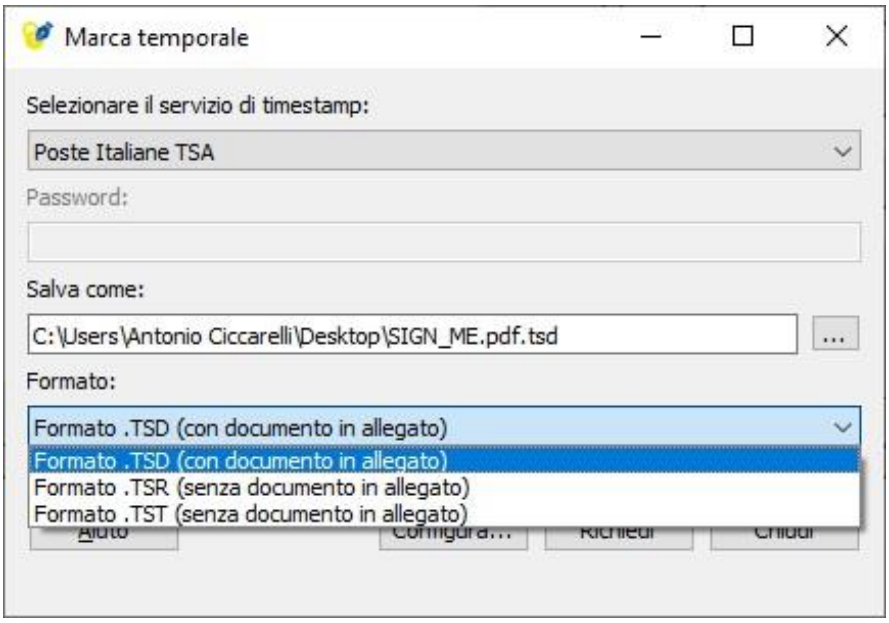


Figura 21. Marca temporale - formati supportati

Si fa presente che l'operazione di marcatura temporale necessita della connessione a Internet in quanto il firmaOK! per completare tale operazione comunica con il servizio di Timestamp selezionato in precedenza. Il software è rilasciato con la configurazione di default necessaria per permettere l'iterazione con il server di Timestamp di Poste Italiane. Nel caso la configurazione dovesse essere cambiata è possibile farlo cliccando sul pulsante Configura accedendo al pannello in Figura 22.

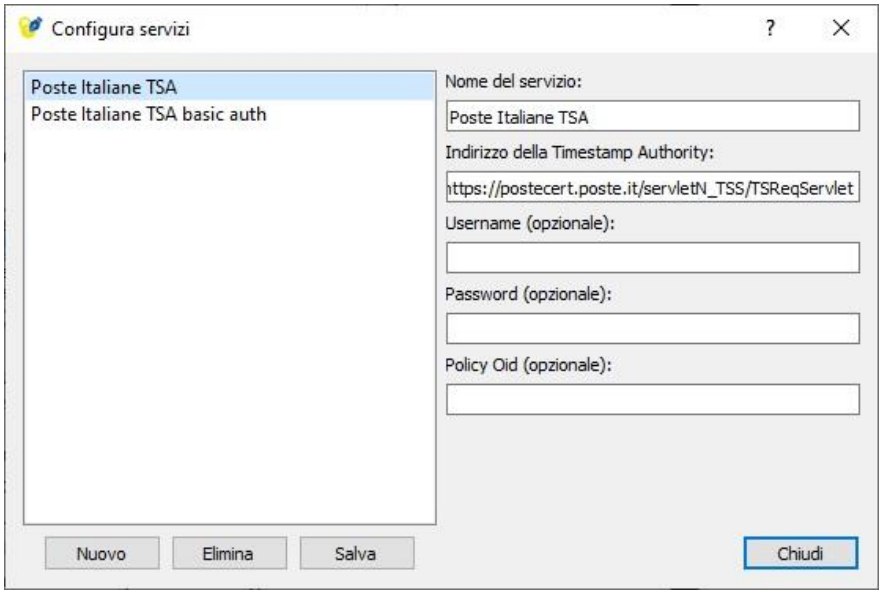


Figura 22. Configurazione Marca temporale di default

La configurazione di default è "Poste Italiane TSA", come si evince dalla Figura 23 è possibile una configurazione alternativa ovvero "Poste Italiane TSA basic auth", questa differisce da quella di default in quanto l'autenticazione presso il servizio richiederà username e password invece del solo PIN.

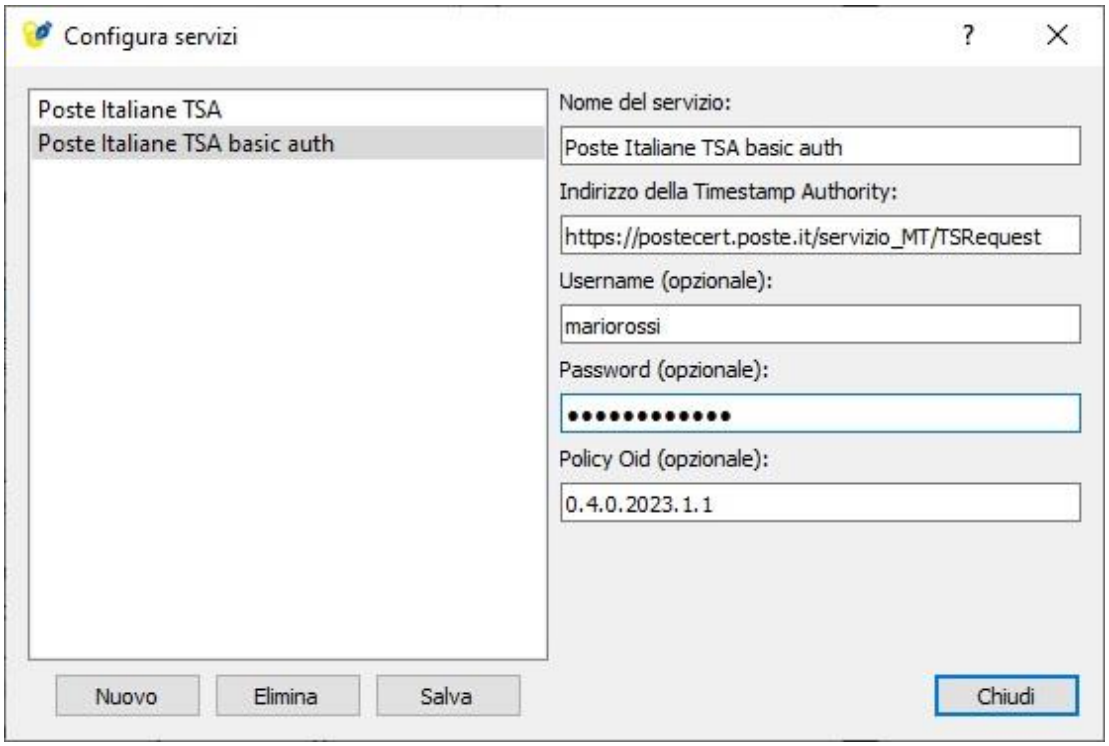


Figura 23. Configurazione Marca temporale alternativa

Fase 4

Per inviare la richiesta di marcatura temporale cliccare sul pulsante "Richiedi" (Figura 20).

Fase 5

Selezionare il certificato con cui firmare la richiesta di marcatura temporale (individuato da "COGNOME NOME") ed inserire il PIN del dispositivo crittografico (smart card o token USB) collegato al PC. Cliccare quindi su "OK" per proseguire.

Fase 6

Al termine dell'operazione di marcatura temporale, firmaOK! mostra all'utente un messaggio con l'esito dell'operazione. Cliccare su "OK" per chiudere il messaggio; per chiudere la finestra "Timestamp" cliccare sul pulsante "Chiudi".

5. Verifica di file firmati e/o marcati temporalmente

firmaOK! 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 pulsante "Verifica";
- cliccando sul pulsante "Verifica" (Figura 1) e selezionando il/i documenti da verificare dalla finestra di navigazione del PC.

Fase 2

firmaOK! effettua la verifica del documento, il cui esito viene mostrato nella schermata che segue (Figura 24).

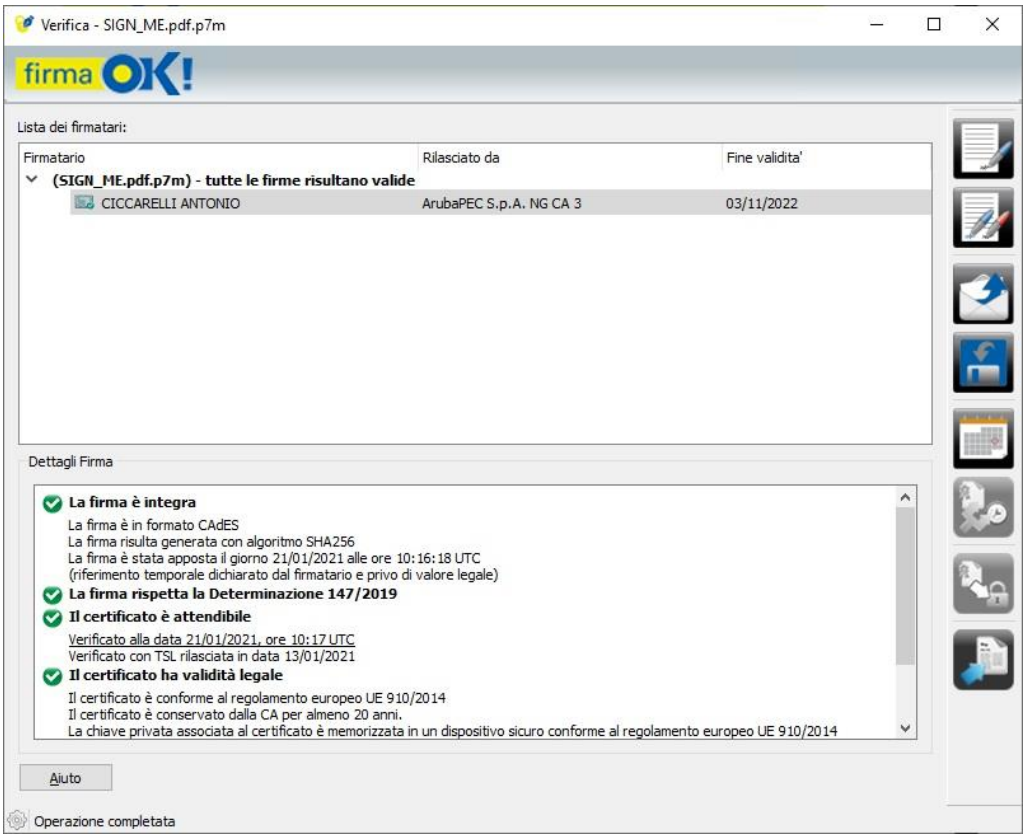


Figura 24. Pannello di Verifica

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 25).
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.

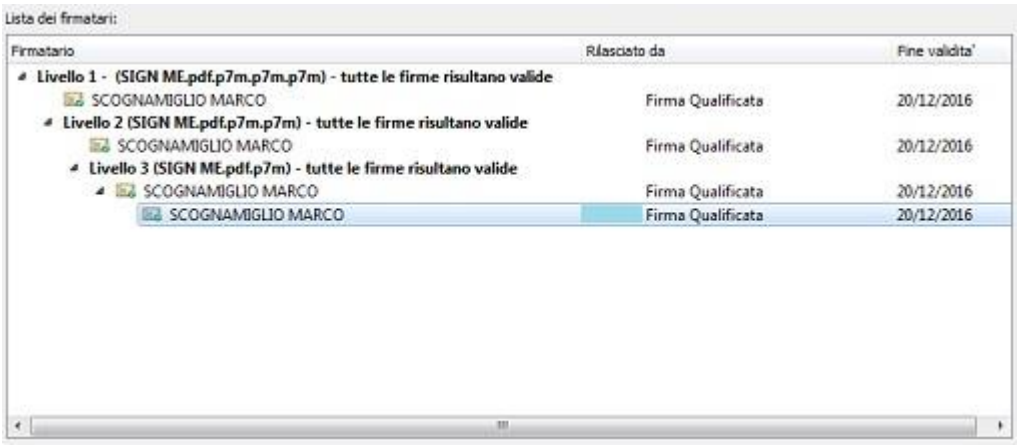


Figura 25. Elenco firme apposte sul documento verificato.

Nella parte bassa della schermata (Figura 26) 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".
- **Aderenza alle Regole Tecniche previste dalla Normativa vigente**: viene mostrato l'esito del controllo relativo all'aderenza e al rispetto della Normativa Vigente.
- **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".
- **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".
- **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 26. Dettagli sulla verifica

In Figura 27 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

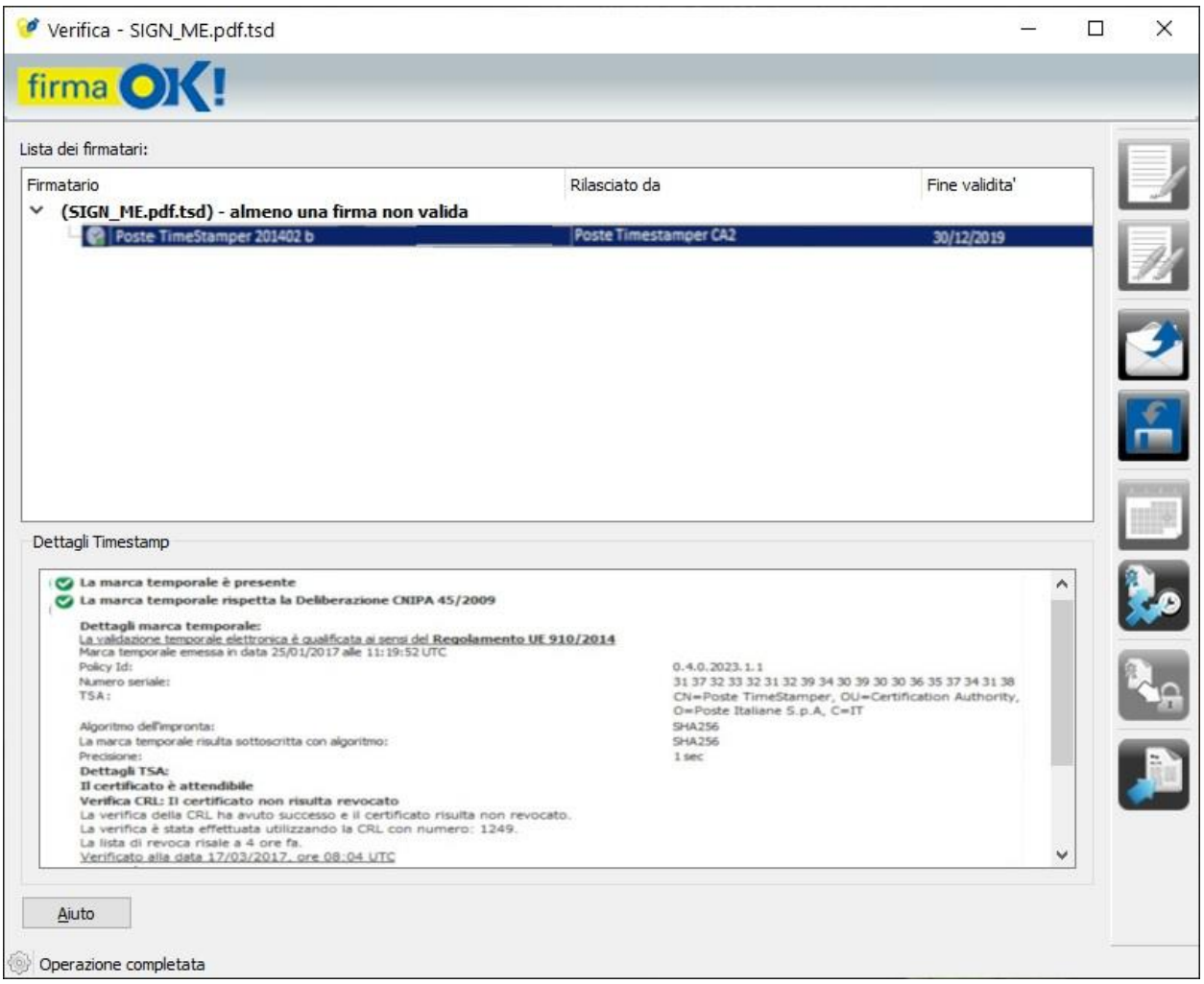


Figura 27. Verifica marca temporale

Dal menu verticale, presente sul bordo destro della schermata di Verifica (Figura 24), è inoltre possibile effettuare le seguenti operazioni (partendo dall'alto):

- 
  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 selezionare una specifica data in cui effettuare la verifica della firma apposta al documento. Cliccando sul pulsante "Verifica alla data" si apre la seguente finestra:

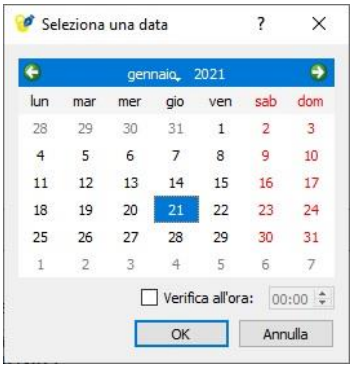


Figura 28. Verifica alla data

- 
  Separa marca temporale: separa il documento originario dalla sua marca temporale salvando quest'ultima su un file con estensione .tsr
- 
  Aggiungi ai destinatari: Se il certificato associato alla firma del documento è valido anche per la cifratura di un file potrà essere salvato nella rubrica contatti (vedi paragrafo 7.1)
- 
  Salva report di verifica: consente la comoda esportazione in formato PDF dell'esito della verifica con dettagli aggiuntivi riguardanti il certificato di firma digitale, la firma e l'apposizione delle marche temporali.

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.

6. Gestione chip (disponibile solo su versione portable - PosteKey)

6.1. HID<>CCID (Conversione della modalità di funzionamento del dispositivo)

Il token PosteKey si contraddistingue come un dispositivo di firma digitale completamente "plug&play": per utilizzarlo basta che venga inserito nella porta USB del proprio pc senza dover effettuare installazioni e configurazioni ulteriori. Tutto il software necessario alle operazioni di firma digitale è infatti ospitato sulla memoria interna del dispositivo, che viene rilevato in maniera automatica dal sistema operativo della postazione utente. Questa modalità di funzionamento, che è quella di default del token PosteKey, è denominata "**modalità HID**" dato che il dispositivo utilizza i driver di sistema *Human interface device*, che consentono l'interazione con il pc in maniera semplice e pressoché immediata, senza richiedere alcuna installazione (utilizza in altre parole lo stesso sistema di connessione di mouse e tastiere).

Tuttavia, qualora si desideri l'interfacciamento del dispositivo PosteKey anche da parte di quelle applicazioni già presenti nel pc host (come ad esempio Mozilla Firefox, Adobe Reader/Professional, Safari, software di Firma Digitale di terze parti, etc…), è necessario convertire la modalità di funzionamento da quella **HID** (descritta in precedenza) a quella **CCID**.
Nella modalità **CCID** il token PosteKey si comporta alla stregua di un normale lettore con smartcard inserita. Questa è la modalità da selezionare qualora si intenda effettuare l'accesso a portali web con il certificato di autenticazione (occorre comunque verificare che la tipologia di certificato di autenticazione presente sulla SIM della Postekey sia quello richiesto dallo specifico portale, ad esempio alcuni portali della Pubblica Amministrazione richiedono specificatamente un certificato di autenticazione della tipologia CNS).

Per effettuare la conversione basta cliccare una sola volta il pulsante "HID<>CCID" nel menu "Gestione chip" come mostrato nella figura seguente:

Figura 29. Conversione HID<>CCID

Qualora l'operazione sia stata condotta sotto Windows, l'avvenuta conversione del dispositivo può essere controllata da "Pannello di controllo/Gestione dispositivi": apparirà nell'elenco "Lettori di smartcard" un dispositivo CCID (come evidenziato dalla freccia rossa nella figura sottostante:

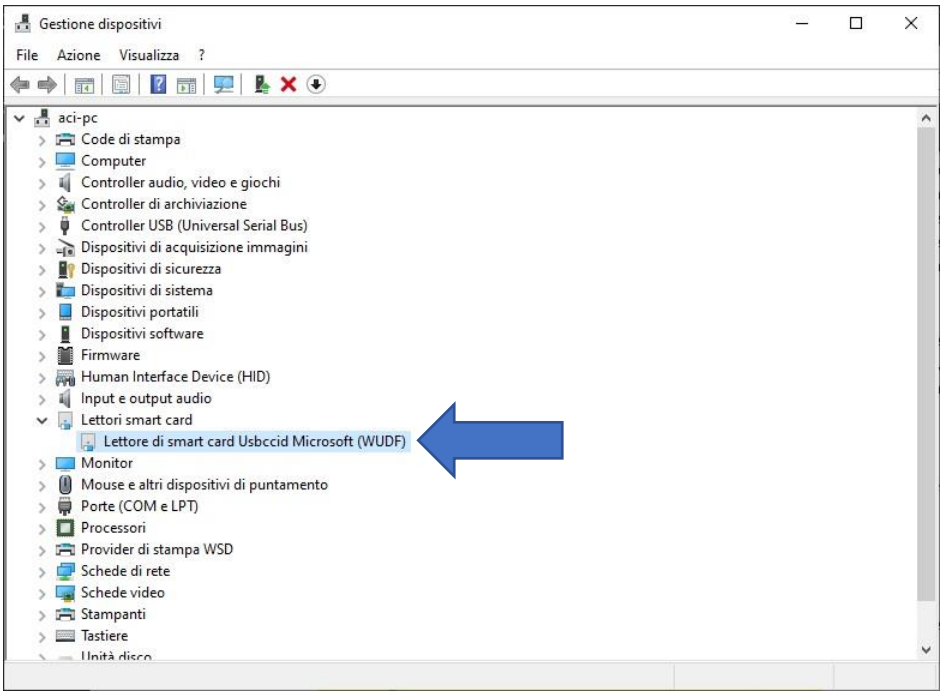


Figura 30. Conversione HID<>CCID effettuata su Windows

Sugli altri sistemi operativi il token PosteKey viene sempre rilevato come un lettore CCID.

Nota 1): per utilizzare il token in modalità CCID come un normale lettore con le applicazioni di terze parti, è necessario dopo la conversione di cui sopra procedere alla configurazione del modulo PKCS#11 all'interno dell'applicazione che si intende utilizzare. Il modulo PKCS#11 è ospitato a bordo della memoria del token. A seconda del sistema operativo utilizzato, lo si può recuperare rispettivamente ai seguenti path:

- Windows: ROOT\System\Firma4NG_Windows\Firma4
- macOS: ROOT\System\Firma4NG.app\Contents\Resources
- Linux: ROOT\System\Firma4NG_Linux\Firma4

A seconda della specifica applicazione di terze parti che si intende utilizzare, si faccia riferimento al relativo manuale nella sezione dedicata interfacciamento con lettori di smartcard.

Prendendo come esempio l'utilizzo del browser Mozilla Firefox per effettuare l'autenticazione su un portale occorre seguire la procedura indicata in Appendice A).

Nota 2): Su alcune distribuzioni Linux, in circostanze particolari, si può verificare che la conversione HID<>CCID abbia l'effetto di non far rilevare più alcun lettore di smartcard alla postazione host. Questo si verifica qualora sul pc host non sia installato/avviato il servizio di sistema pc/sc. Per installarlo seguire la presente procedura:

- Ubuntu:

  Prima di eseguire il comando, controllare di avere i diritti di amministratore

```
apt-get install pcscd
```

  Dopo l'installazione è sufficiente riavviare.

Per controllare se il servizio è stato installato correttamente basta lanciare il comando `ps -A | grep pcscd`

Nota 3): L'operazione di conversione non è persistente in quanto la rimozione della chiavetta USB riporta il dispositivo in modalità di default: HID. È necessario effettuare nuovamente l'operazione ogni qualvolta si presenti la necessità di operare in modalità CCID.

6.2. Card Manager

Selezionando nel menu il pulsante "Card Manager", si apre una schermata dalla quale è possibile gestire la smart card (Figura 31).

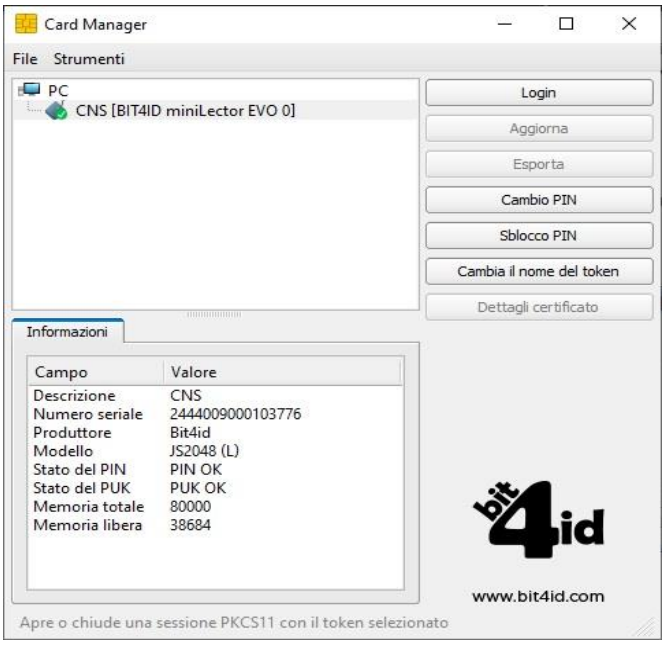


Figura 31. Card Manager

In particolare, grazie all'applicazione **Card Manager** di Bit4ID è possibile gestire i dispositivi crittografici (smart card e token USB), attraverso le operazioni elencate di seguito:

- **Login:** consente di effettuare una lettura dei certificati presenti sulla smart card o token USB, previa immissione del PIN;
- **Aggiorna:** consente di aggiornare la schermata dei certificati;

- **Esporta:** consente all'utente di esportare in formato ".cer" il certificato caricato a bordo della smart card o token USB, la chiave
  privata associata al certificato non verrà esportata per motivi di sicurezza;
- **Cambio PIN:** consente di cambiare il PIN della smart card o token USB;
- **Sblocco PIN:** consente di sbloccare il PIN (in seguito a un blocco della smart card dovuto all'inserimento di un PIN errato per sei volte consecutive) mediante inserimento del PUK;
- **Cambia il nome del token:** modifica l'etichetta con cui viene mostrato a schermo il nome del dispositivo (es. "CNS" può essere modificato in "Smart card lavoro");
- **Dettagli certificato:** disponibile dopo aver effettuato la login e selezionato un certificato. Apre una schermata da cui poter leggere

7. Utilities

Cliccando sul pulsante "Utilities" del menu principale di firmaOK!, viene avviato il menu secondario, che contiene alcune funzionalità per la crittografia ("Cifra" e "Decifra") ed altri strumenti di utilità ("Opzioni", "Manuale utente" e "Info" in Figura 32).

Figura 32. Menu Utilities

7.1. Cifratura di uno o più documenti

firmaOK! 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 pulsante "Utilities" si apre il menu secondario con il pulsante 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 (Figura 33):

- selezionando e trascinando (drag&drop) il/i documenti sul pulsante "Cifra" del menu secondario;
- cliccando sul pulsante "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 se stessi, selezionare il certificato da utilizzare e spostarlo, nella sezione "Cifra per…", utilizzando l'apposito pulsante 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 pulsante "Importa da file…" e selezionare il certificato (".cer") da caricare;
- Dal tab "Elenco in linea": effettuare la ricerca specificando i parametri previsti dal menu 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 pulsante con la freccetta destra:

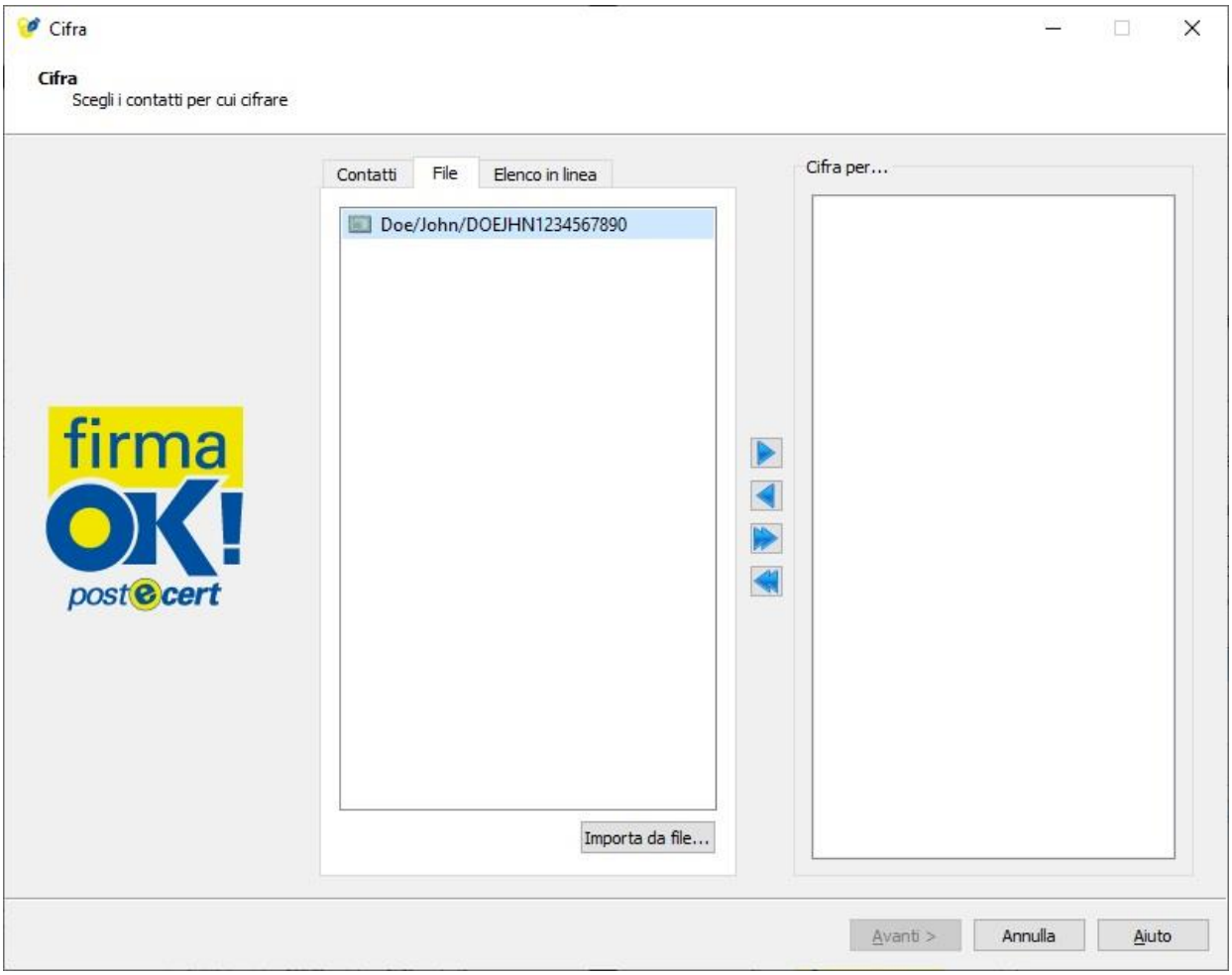


Figura 33. Cifratura di documenti

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

- 
  Per aggiunge il contatto selezionato alla lista dei certificati con cui cifrare il documento;
- 
  Per rimuove il contatto selezionato dalla lista dei certificati con cui cifrare il documento;
- 
  Per aggiunge 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.

La rubrica "Contatti"

In firmaOK! 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".

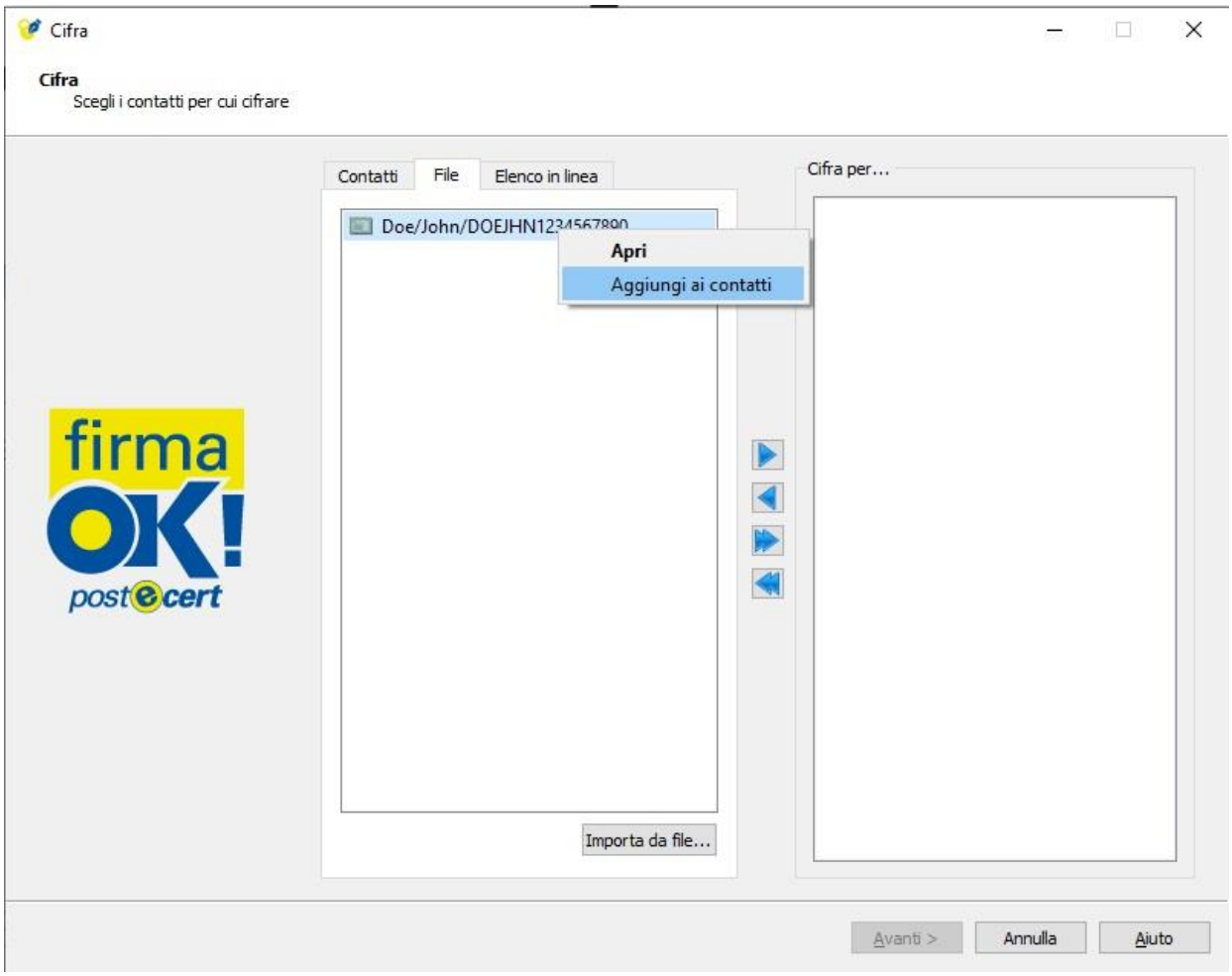


Figura 34. La rubrica Contatti

- **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 pulsante "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 pulsante "Avanti" è possibile selezionare le opzioni da utilizzare per la cifratura del documento.

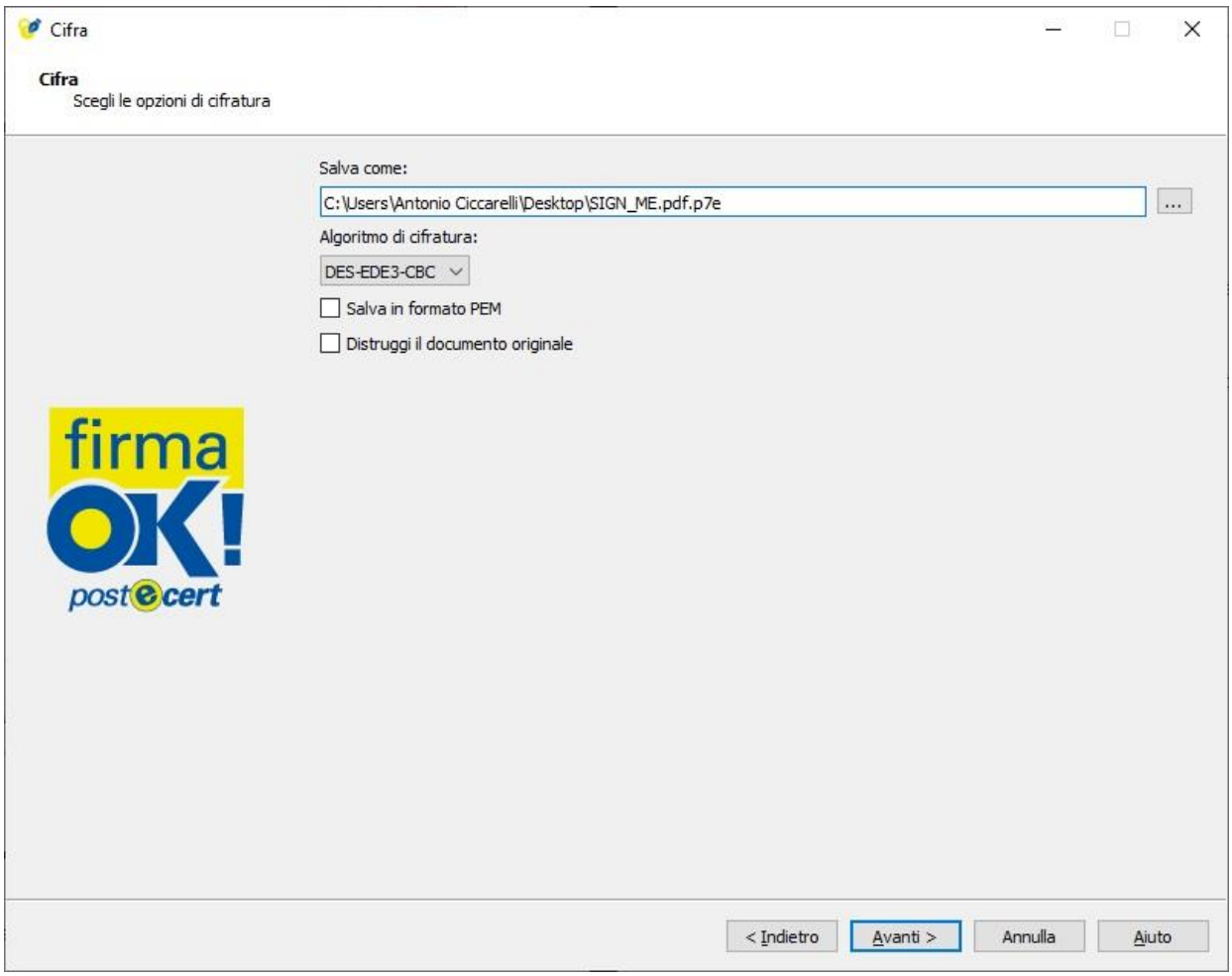


Figura 35. Opzioni cifratura

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 pulsante "...";
- selezionare l'algoritmo da utilizzare per cifrare fra quelli elencati nel menu 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: data la maggiore sicurezza che offre, 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 pulsante "Termina" è possibile chiudere la schermata.

7.2. Decifratura di uno o più documenti

Con firmaOK! 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 pulsante "Decifra" del menu 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:

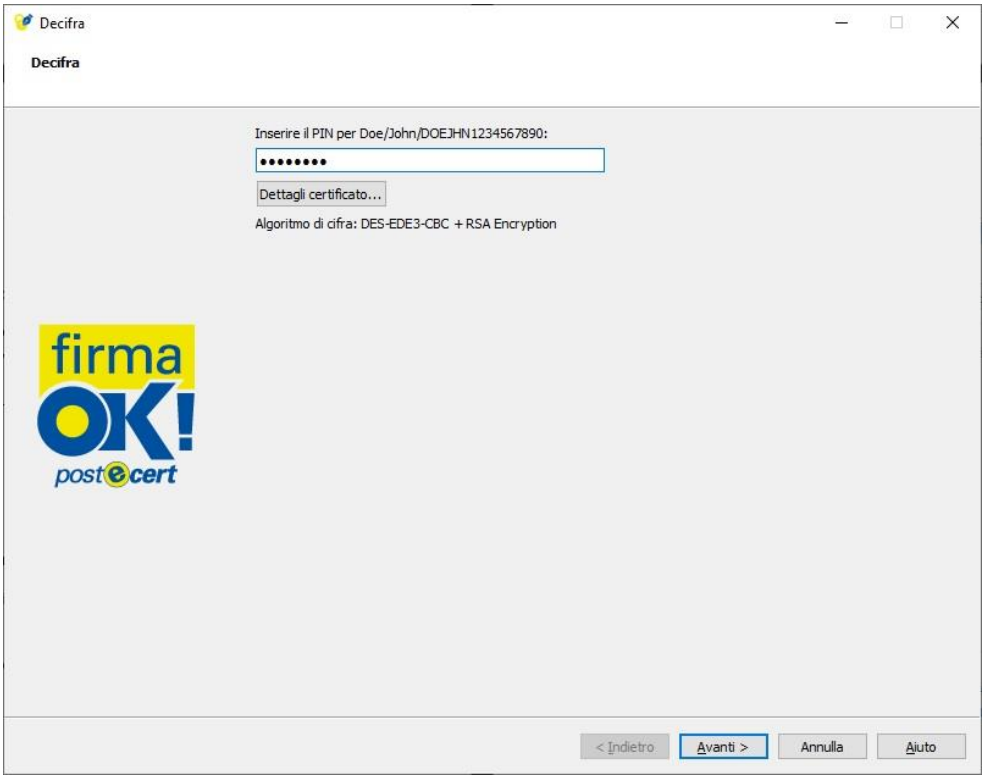


Figura 36. Decifratura

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 pulsante "Apri contenuto" oppure salvarlo in locale sul proprio PC cliccando sul pulsante "Salva contenuto…".

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

7.3. Opzioni

Cliccando sul pulsante "Opzioni" del menu secondario, si apre la finestra che consente la personalizzazione della configurazione di firmaOK! e ne permette il salvataggio (pulsante "Salva").

Se si desidera ripristinare la configurazione iniziale di firmaOK!, basta cliccare sul pulsante "Ripristina".

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

8.3.1. Tab "Generale"

Da questa sezione (Figura 37) è possibile effettuare le seguenti operazioni:

- **Cancella cache CRL**: consente di eliminare la cache locale all'applicazione delle CRL, in questo modo la prossima operazione che richiederà il controllo delle CRL dovrà necessariamente scaricarle dagli appositi punti di distribuzione;
- **Configurazione di default**: ripristina le configurazioni di default di firmaOK!
- **Avvia aggiornamento del software:** avvia manualmente l'aggiornamento software di firmaOK!
- **Avvia aggiornamento TSL:** avvia manualmente l'aggiornamento dell'Elenco Pubblico dei Certificatori contattando il servizio TSL dell'Unione Europea (conformemente a quanto previsto dal Regolamento (UE) 910/2014 "EIDAS")

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

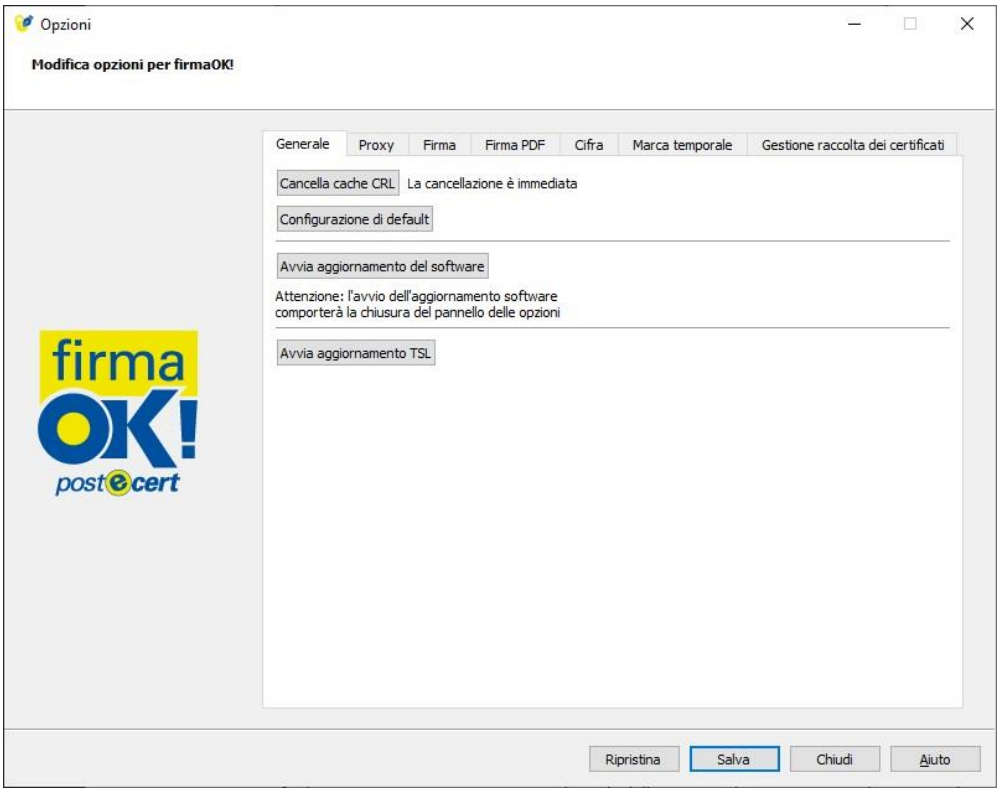


Figura 37. Opzioni – tab "Generale"

8.3.2. Tab "Proxy"

In questa sezione (Figura 38) 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 pulsante "Salva" per salvare la nuova configurazione.

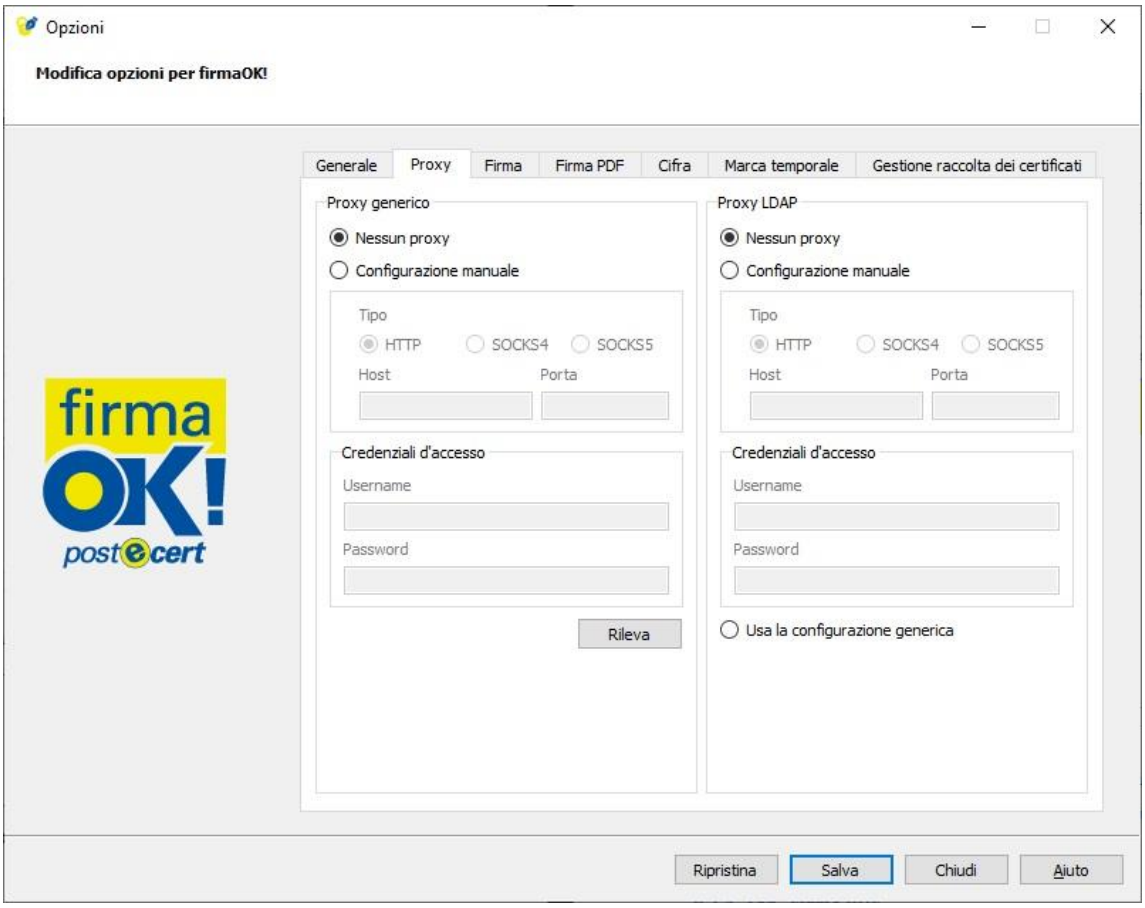


Figura 38. Opzioni – tab "Proxy"

8.3.3. Tab "Firma"

In questa sezione (Figura 39) è possibile configurare il formato in cui verranno salvati automaticamente i documenti firmati oppure selezionare l'opzione secondo la quale firmaOK! seleziona automaticamente il formato di firma da applicare in funzione della tipologia del documento da firmare.
È inoltre possibile:

- impostare una cartella di destinazione dove salvare i documenti firmati con la procedura di firma di più documenti;
- bloccare/sbloccare l'operazione di firma nel caso in cui il certificato selezionato non sia credibile;
- bloccare/sbloccare l'operazione di firma nel caso in cui il certificato selezionato non sia adatto alla firma digitale qualificata;
- bloccare/sbloccare l'operazione di firma nel caso in cui il certificato selezionato sia sospeso/revocato;
- abilitare/disabilitare la richiesta del PIN della smart card o del token USB, nel caso in cui si siano selezionati più documenti da firmare (firma massiva).

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

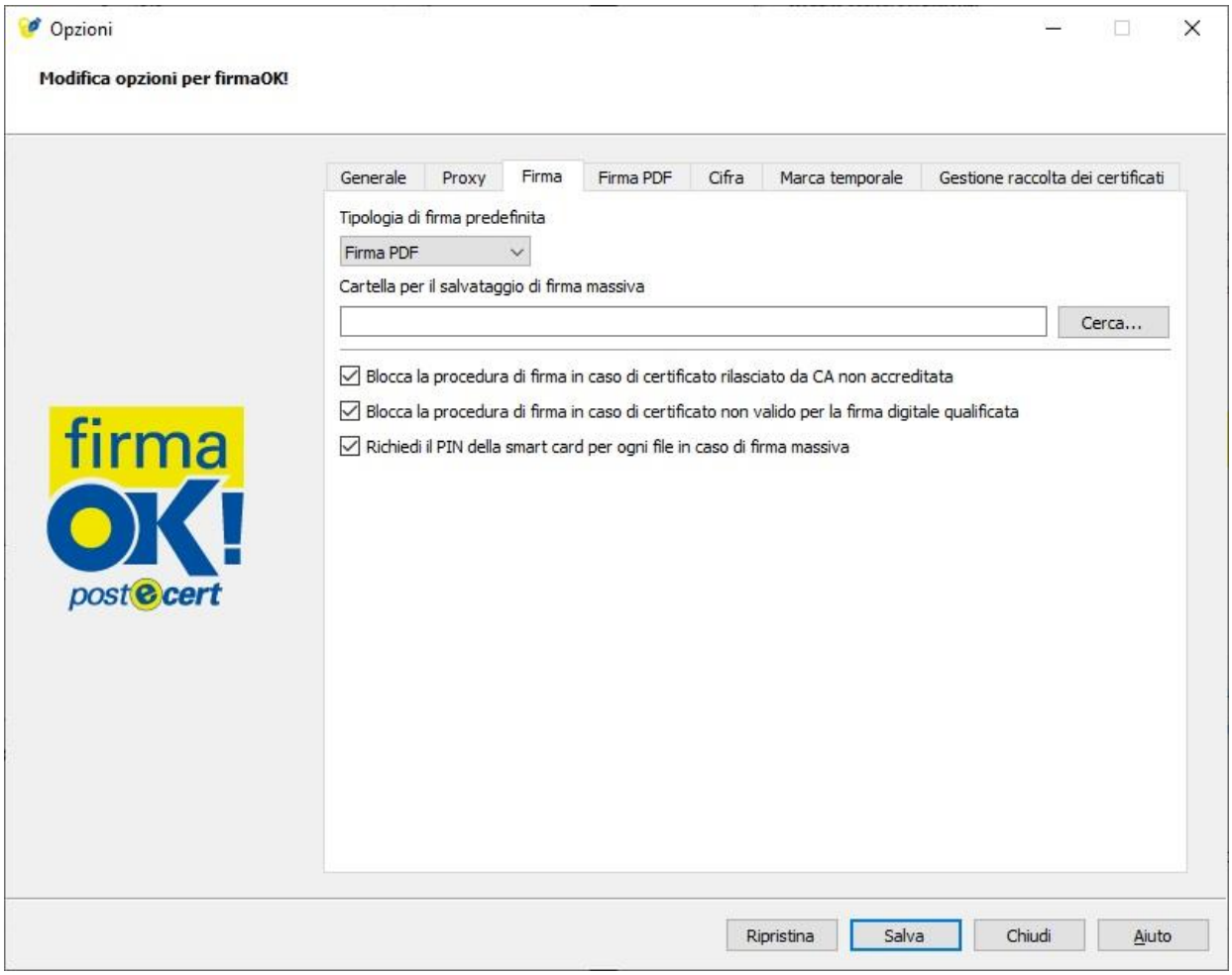


Figura 39. Opzioni – tab "Firma"

8.3.4. Tab "Firma PDF"

In questa sezione (Figura 40) è possibile definire la configurazione standard da utilizzare per apporre la firma grafica in formato PDF, personalizzando i valori dei campi presenti.

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

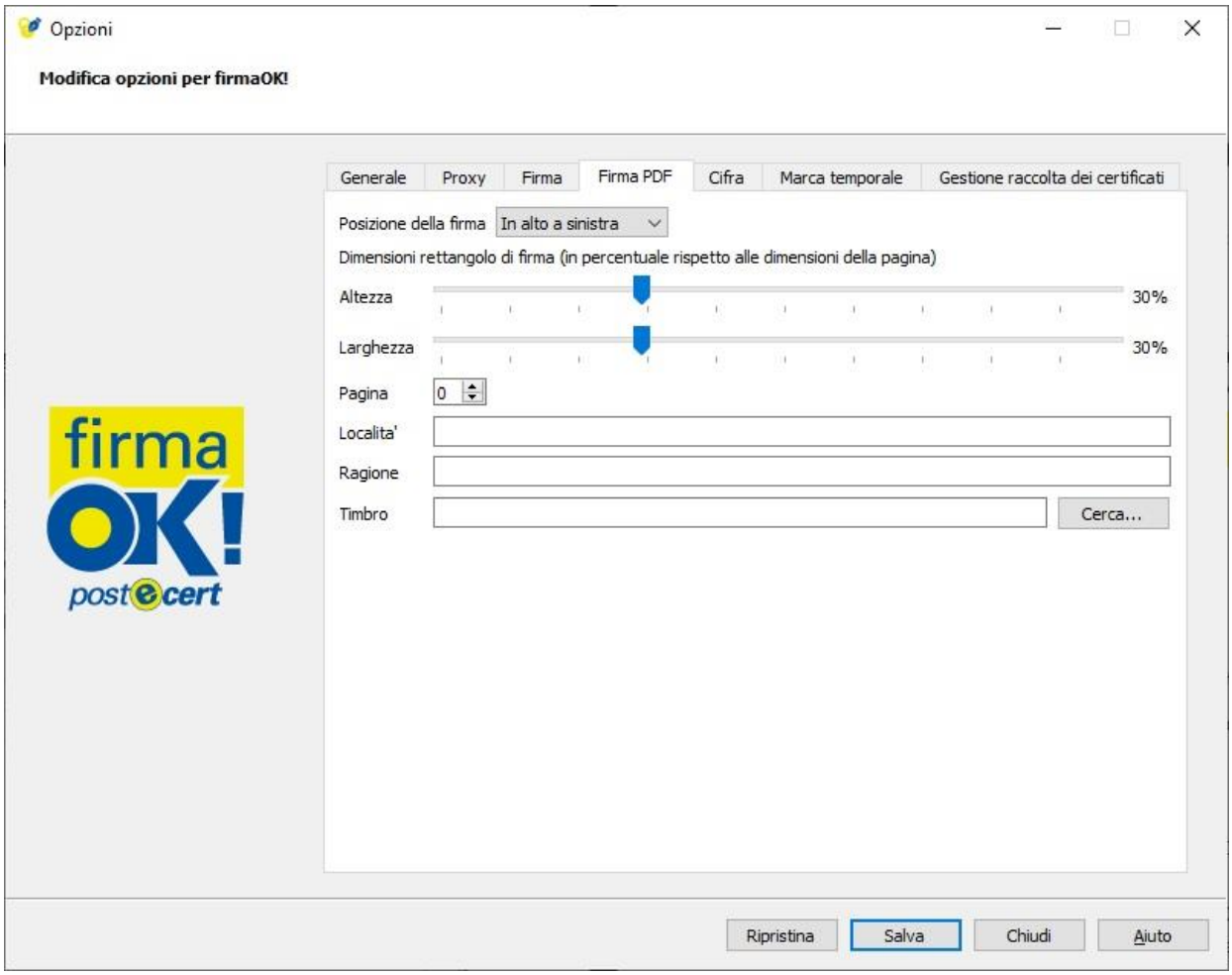


Figura 40. Opzioni – tab "FirmaPDF

8.3.5. Tab "Cifra"

In questa sezione è possibile definire la configurazione standard da utilizzare nelle operazioni di cifratura, scegliendo:

- **algoritmo di cifratura di default**: l'algoritmo standard da utilizzare per la cifratura di documenti;
- **cartella per il salvataggio automatico di file cifrati**: indicare il percorso sul PC dove salvare i documenti cifrati.

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

8.3.6. Tab "Marca Temporale"

In questa sezione 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 Postecert.
È comunque possibile configurare altri servizi di marcatura temporale, utilizzando il pulsante "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 pulsante "Elimina".

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

8.3.7. Tab "Gestione Raccolta Certificati"

In questa sezione è possibile gestire l'archivio dei certificati utilizzato da firmaOK!.

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 pulsante "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 pulsante "Salva" per salvare la nuova configurazione.

7.4. Manuale Utente

La pressione di questo pulsante consente l'apertura del presente manuale.

7.5. Info

Schermata con le informazioni relative al prodotto firmaOK! quali la versione del software ed il riferimento alla società che ha sviluppato l'applicazione.

8. Aggiornamento automatico di firmaOK!

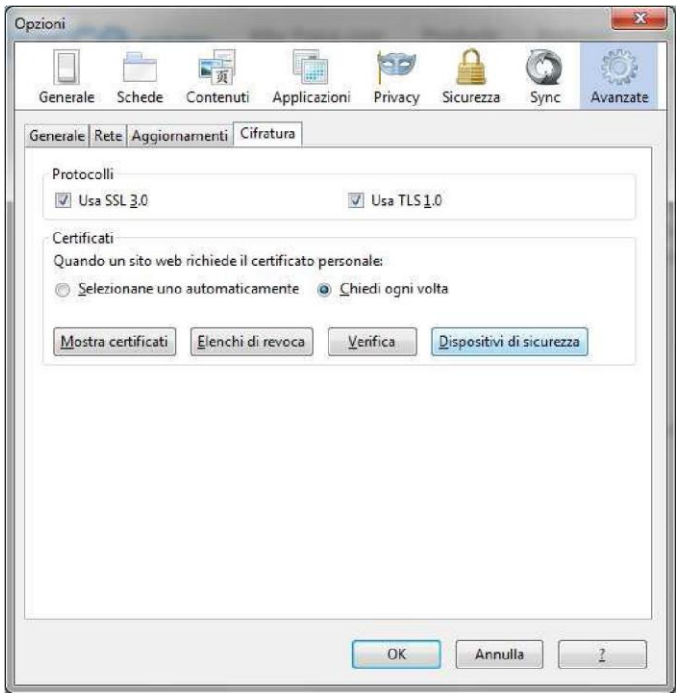
firmaOK! è inoltre dotato di una funzionalità di aggiornamento automatico: ad ogni avvio dell'applicativo viene effettuato un controllo sulla disponibilità di nuove versioni e, a seguito dell'autorizzazione da parte dell'utente, viene effettuato l'aggiornamento.

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

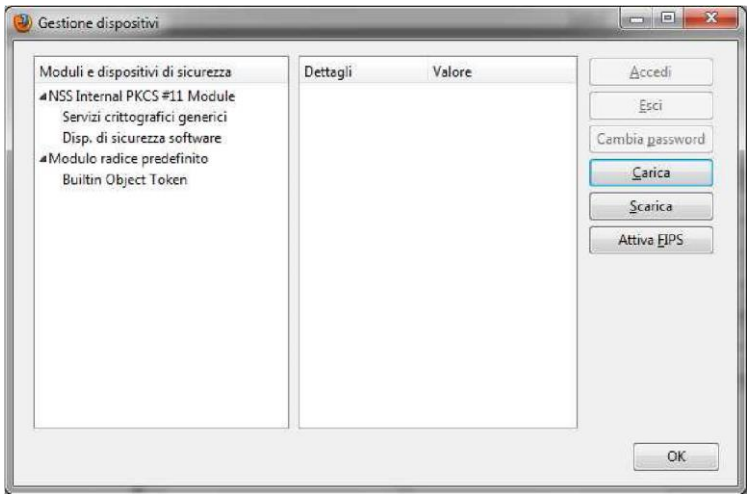
Appendice A) – Interfacciamento Postekey - Firefox

Per utilizzare il token Postekey con il browser Mozilla Firefox è necessario procedere alla seguente configurazione specifica:

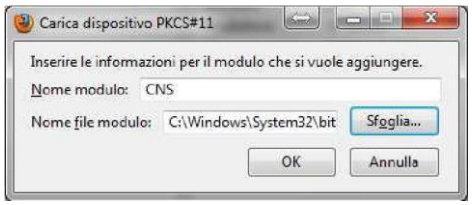
- Dal menu del browser, visibile dopo aver cliccato sui tre puntini disposti verticalmente in alto a destra, selezionare la voce "Strumenti \ Opzioni" del browser, selezionare l'icona "Avanzate" e quindi la scheda "Avanzate"



- Cliccare su "Dispositivi di sicurezza"



- Cliccare su "Carica", assegnare un nome modulo a piacere (es. CNS) quindi cliccare su sfoglia e selezionare il file bit4ipki.dll oppure bit4xpki.dll (solo uno dei due è presente) dal path ROOT\System\Firma4NG_Windows\Firma4 (solo uno dei due è presente, a seconda del dispositivo utilizzato). Al termine dell'operazione cliccare OK.

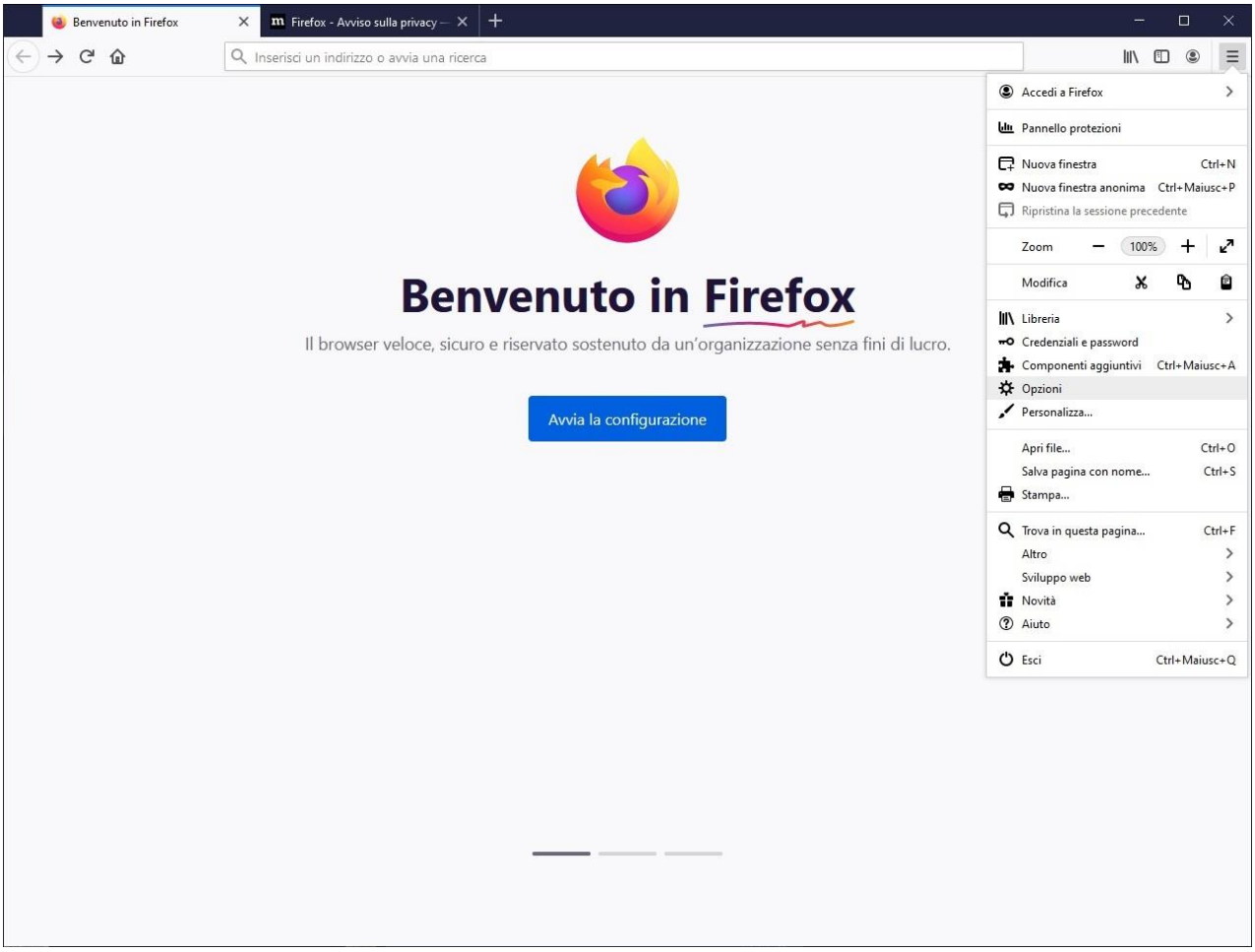


- Si fa presente che tale configurazione non è necessaria se si utilizza il browser presente sulla chiavetta, vedi Figura 1 pulsante "Internet" in quanto già pre-configurato per interagire con il firmaOK!.

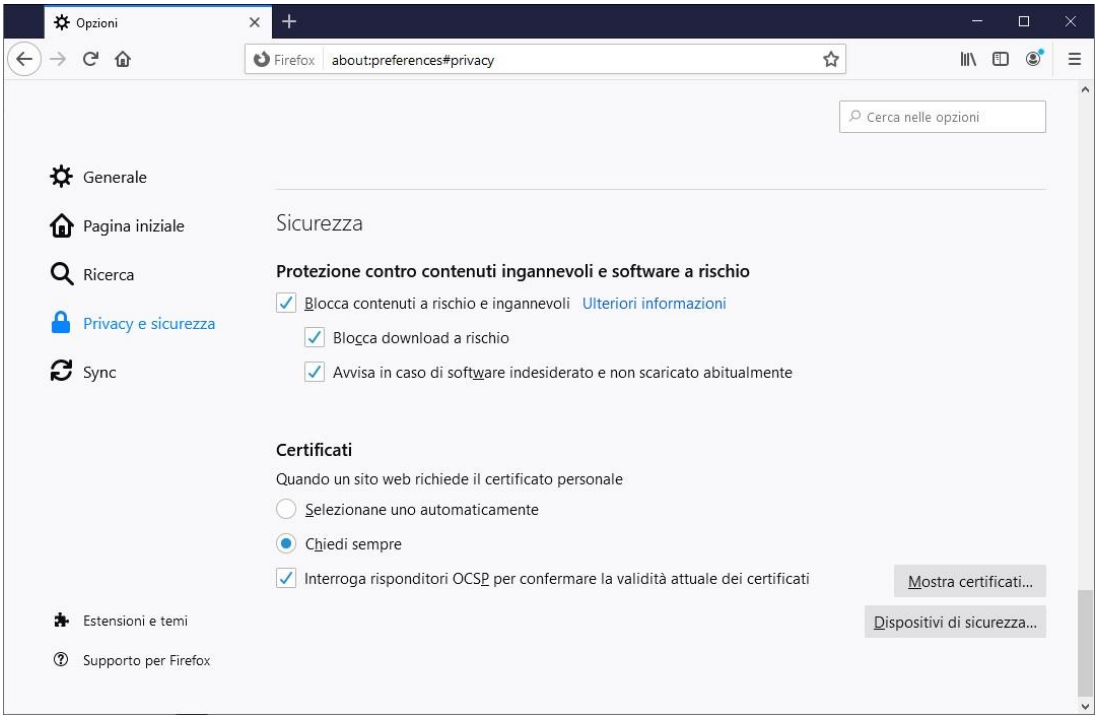
Appendice B) – Interfacciamento firmaOK! - Firefox

Per configurare il browser Mozilla Firefox è necessario procedere nel seguente modo:

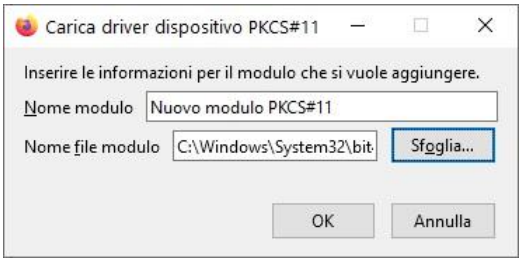
- Dal menu del browser, visibile dopo aver cliccato sui tre trattini disposti parallelamente in alto a destra, selezionare la voce " Opzioni" del browser, selezionare l'icona "Avanzate" e quindi la scheda "Privacy e sicurezza"



- Cliccare su "Dispositivi di sicurezza"



- Cliccare su "Carica", assegnare un nome modulo a piacere (es. CNS) quindi cliccare su sfoglia e selezionare il file bit4xpki.dll dal percorso "C:\Windows\System32"'. Al termine dell'operazione cliccare OK.



- Si fa presente che tale configurazione non è necessaria se si utilizza il browser presente sul token USB, vedi Figura 1 pulsante "Internet" in quanto già pre-configurato per interagire con il firmaOK!


Posteitaliane