

Trust Signer Client



Agosto 2018

Indice degli argomenti

Indice degli argomenti	2
1 Introduzione	4
2 Requisiti di Sistema	4
2.1 Software	4
2.2 Hardware	4
3 Installazione	5
3.1 Aggiornamenti	6
3.2 Note per l'installazione in ambiente Linux	6
4 Lancio dell'Applicazione	6
5 Utilizzo dell'applicazione	7
5.1 Struttura della finestra principale	7
6 Impostazioni di utilizzo	9
6.1 Impostazioni Personalizzate	11
6.1.1 Autenticazione	11
6.1.2 Tipologia di Firma	12
6.1.3 Cartelle di Default	15
7 Selezione del documento	16
7.1 Accesso al Servizio	18
7.2 Operazioni sul file selezionato	18
8 Firma di un documento	22
8.1 Scelta della tipologia di firma p7m	23
8.2 Firmare un documento p7m	24
8.2.1 Firma semplice	25
8.2.2 Controfirma	28
8.2.3 Firma parallela	29
8.3 Firmare un documento PDF	29
8.4 Firma multipla di documenti	35
9 Verifica della firma di un documento	35

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

1 Introduzione

Il Client **di Trust Signer** è un'applicazione per la firma digitale remota che utilizza la tecnologia FSM che prevede l'utilizzo del telefono cellulare come dispositivo sia per l'autenticazione che per la firma digitale in modalità remota.

Con esso è possibile:

- Firmare digitalmente un qualsiasi documento elettronico in modalità P7M-CADES,
- Firmare digitalmente un qualsiasi documento PDF in modalità PAdES o CADES
- Verificare l'autenticità e l'integrità della firma apposta su un documento elettronico,
- Estrarre il documento originale da una busta firmata.

2 Requisiti di Sistema

2.1 Software

Trust Signer è un'applicazione sviluppata interamente in Java pertanto possiede la caratteristica principale comune a tutte le applicazioni sviluppate in tale linguaggio e cioè quella di essere **multiplatforma**, ossia in grado di essere eseguita su qualsiasi sistema operativo che dispone di una Java Virtual Machine (JVM).

L'unico prerequisito software risulta essere quello di avere una JVM installata sul proprio sistema.

L'utente è tuttavia agevolato dalla modalità di installazione dell'applicazione che fa uso della tecnologia Java Web Start (vedi paragrafo Installazione) che tra le altre cose provvede a verificare l'esistenza della JVM nella versione richiesta ed eventualmente all'installazione.

La versione minima richiesta per la JVM è la 6.0 o superiore.

Il download da browser Google Chrome con una versione superiore alla v.42 presenta dei problemi superabili con il downgrade o utilizzando un browser alternativo.

2.2 Hardware

Unico requisito hardware per l'esecuzione del **Trust Signer** Client è una connessione attiva ad Internet.

	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Nel caso si utilizzi un proxy aziendale, il download potrebbe subire rallentamenti o arrestarsi. Verificare ed eventualmente modificare le impostazioni del proxy.

3 Installazione

Come indicato precedentemente per l'installazione dell'applicazione si fa uso della tecnologia Java Web Start. L'utente non deve far altro che connettersi tramite browser all'indirizzo fornito dal gestore della piattaforma FSM.

Alla prima connessione viene automaticamente verificato che l'utente disponga di una JVM nella versione minima richiesta ed in caso negativo procede all'installazione.

Terminata questa fase Java Web Start, procede al download dell'applicazione ed alla sua installazione. Contestualmente viene creato un collegamento sul Desktop dell'utente che consente, per i successivi utilizzi, di aprire l'applicazione direttamente senza doversi collegare all'indirizzo suddetto:



Figura 1



Figura 2

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

3.1 Aggiornamenti

Ad ogni lancio dell'applicazione e prima della sua esecuzione, viene automaticamente verificata la presenza di aggiornamenti ed in caso affermativo si chiede di procedere con il download di quest'ultimi.

L'utente è quindi sicuro di utilizzare sempre l'ultima versione dell'applicazione.

3.2 Note per l'installazione in ambiente Linux

Alcune distribuzioni Linux possono non avere installato nel browser il plugin Java che consente il lancio automatico dell'applicazione come descritto nel paragrafo precedente.

Per una verifica si può andare al seguente link:

<http://www.java.com/it/download/testjava.jsp>

che ne verifica la presenza e consente, in caso, di procedere all'installazione.

Un'alternativa è utilizzare il seguente comando direttamente da una console/shell di sistema:

```
javaws <URL_FILE_JNLP>
```

dove <URL_FILE_JNLP> è l'URL del file JNLP dell'applicazione.

Ad esempio:

```
javaws https://download.ittelecom.it/sw/Trust Signer Client/cryptogui.jnlp
```

In ogni caso è richiesto che sia installata una qualsiasi Java VirtualMachine. Nelle distribuzioni più comuni si può fare direttamente dal package manager specifico (es. in Ubuntu, tramite Ubuntu Software Center è possibile installare IcedTea OpenJDK, ...).

4 Lancio dell'Applicazione

Al momento della prima connessione, dopo il download e l'installazione, l'applicazione si apre senza ulteriori interventi da parte dell'utente.

Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Per i successivi utilizzi invece è sufficiente che l'utente esegua un doppio click sul collegamento all'applicazione creato sul Desktop in fase di installazione (*vedi par. 3*).

5 Utilizzo dell'applicazione

5.1 Struttura della finestra principale

La figura seguente mostra la suddivisione della finestra principale all'apertura dell'applicazione nelle varie aree di interesse:

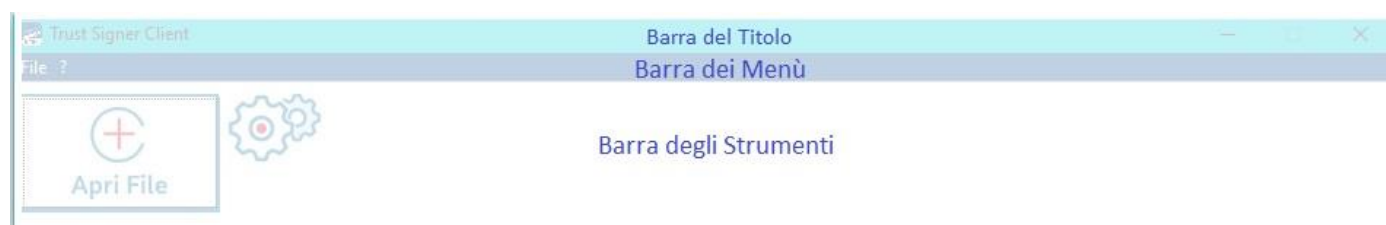


Figura 3

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Finestra del Menù Principale dopo l'aggiunta di un documento da firmare

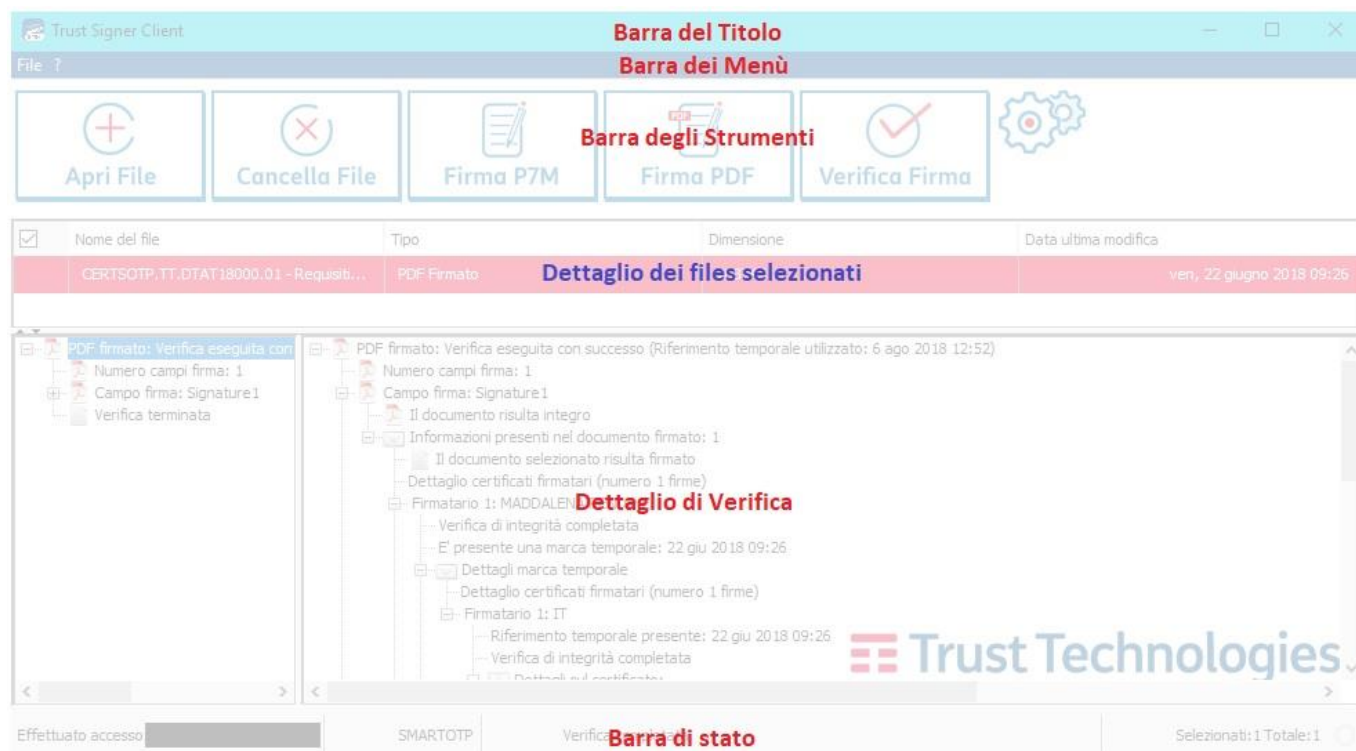


Figura 4



Figura 5

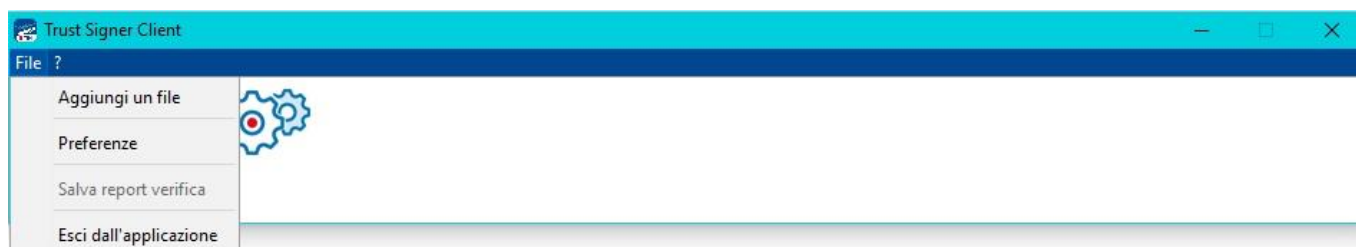


Figura 6

- Nella **Barra del Titolo** è presente il titolo dell'applicazione, **Trust Signer Client**.

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

- Nella **Barra dei Menù**, sono presenti le voci contenenti tutte le azioni che possono essere compiute attraverso l'applicazione e sono racchiuse nelle due voci di menù: *File* ed *Help*.
- Nella **Barra degli strumenti** sono presenti, sotto forma di tasti funzione, le stesse azioni della Barra dei Menù.
- Nei **Dettagli file selezionato** è compresa l'area che riporta i dettagli del documento selezionato (nome, dimensione, data di ultima modifica)
- La **Barra di stato** riporta le informazioni di accesso (nome utente), lo stato di avanzamento delle varie operazioni, il numero di file selezionati.

Aggiungi un file: consente di aggiungere un file che si vuole autenticare (si può accedere o dalla barra dei Menù, o dal tasto "Apri file")

Preferenze: permette di verificare e modificare le impostazioni dell'applicazione attraverso le tre schede **Autenticazione**, **Tipologia di firma** e **Cartelle di default** (accessibile anche attraverso il tasto "Impostazioni")

Esci dall'applicazione: per chiudere l'applicazione.

6 Impostazioni di utilizzo

L'unica impostazione che occorre compiere per poter utilizzare l'applicazione di Firma Digitale, è quella di inserire il proprio Codice Fiscale.

Come rappresentato nella *Figura 7*, dal tasto **Impostazioni**, scheda **Autenticazione** (accessibile anche attraverso il Menù File/Preferenze), c'è la casella in cui inserire il proprio **codice fiscale** e attraverso il tasto "Prova la connessione" (*Figura 8*), si può verificare che la connessione sia in grado di raggiungere la piattaforma del servizio.

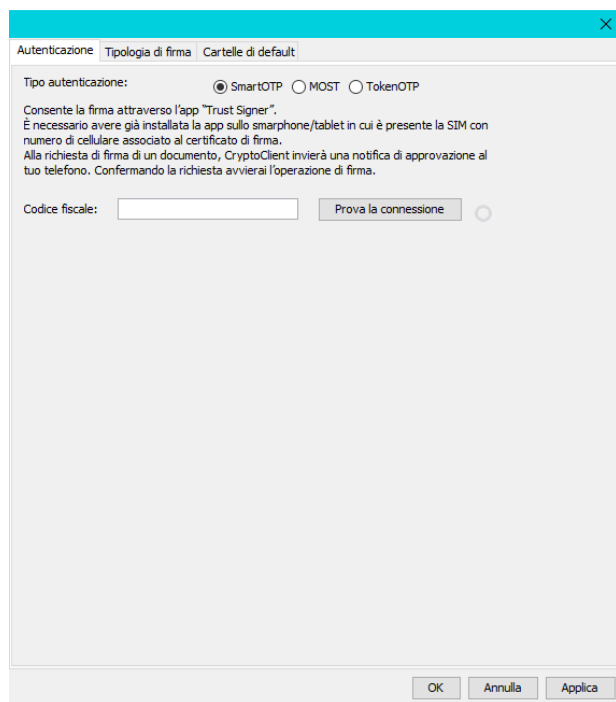


Figura 7

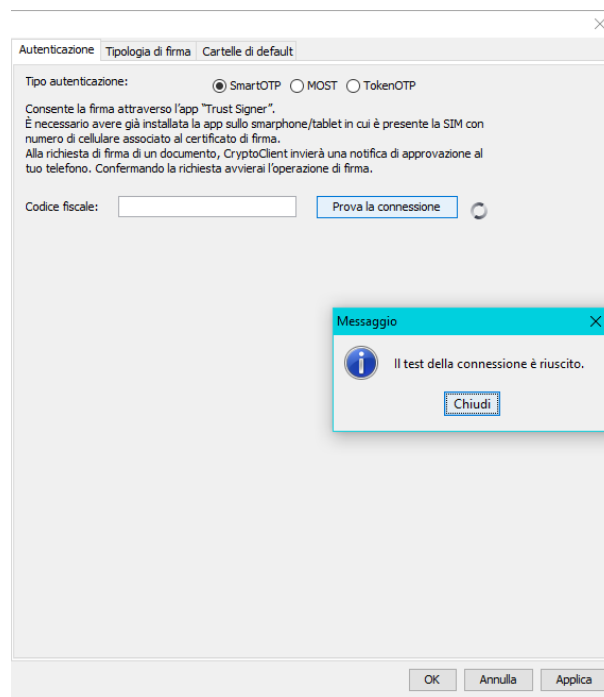


Figura 8

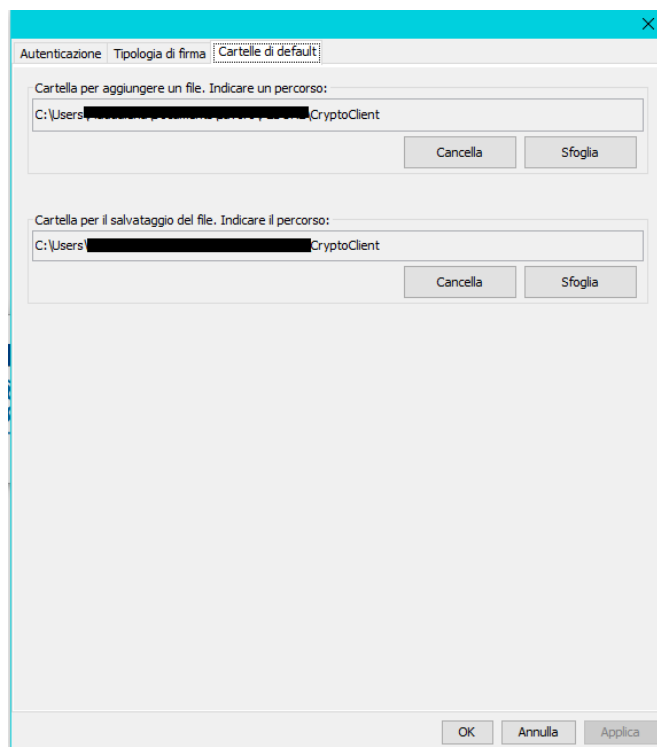


Figura 9

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

6.1 Impostazioni Personalizzate

Dal menu principale, cliccando sul tasto **Impostazioni**, l'utente accede alla finestra per configurare e personalizzare l'applicazione.

La finestra è suddivisa in tre pannelli:

- **Autenticazione**
- **Tipologia di firma** (preimpostata)
- **Cartelle di default**

Nella parte bassa, i pulsanti, comuni a tutti i pannelli, assumono il seguente significato:

OK – Salva le proprietà eventualmente modificate e chiude la finestra

Annulla – Chiude la finestra senza effettuare alcun salvataggio delle proprietà eventualmente modificate

Applica – Salva le proprietà modificate mantenendo aperta la finestra. Il pulsante viene abilitato non appena una proprietà viene modificata.

6.1.1 Autenticazione

Il pannello contiene le informazioni di impostazione del proprio codice fiscale e la verifica di connessione al server FSM (fig. 7 e fig. 8)

♦ Tipi di Autenticazione

- | | | | |
|------|----------|---|--|
| i. | SmartOTP | → | consente l'autenticazione tramite l'app mobile TrustSigner |
| ii. | MOST | → | acronimo di MOBILE Strong Authentication, consente la firma tramite autenticazione con chiamata a un Numero Verde nazionale |
| iii. | TokenOTP | → | riguarda la modalità personalizzata di firma dedicata ai clienti di Banca Sella. |

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

- ♦ **Codice Fiscale** Consente di impostare il codice fiscale utente richiesto al momento della prima selezione documenti in modo che l'utente non sia costretto a digitarlo ad ogni accesso.
- ♦ Il pulsante **Prova la connessione** permette di eseguire un semplice test di connessione all'URL sopra indicato per verificare da subito che non vi siano problemi di connettività tramite la rete Internet.

6.1.1.1 SmartOtp

Consente la firma attraverso Strong Authentication effettuata con l'app "**TrustSigner**".

E' necessario aver già installato l'app su smartphone/tablet in cui è presente la SIM con numero di cellulare associato al certificato di firma.

Alla richiesta di firma di un documento, Trust Signer Client invierà una notifica di approvazione al telefono con tale SIM. Confermando la richiesta, si avvierà il processo di firma.

6.1.1.2 MOST

Consente la firma attraverso Strong Authentication effettuata con chiamata ad un Numero Verde Nazionale (non è quindi utilizzabile dall'estero). E' necessario l'utilizzo del telefono sul quale è inserita la SIM con numero di cellulare associato al certificato di firma.

Tale processo non richiede ulteriori installazioni e può essere eseguito sia da smartphone che da un tradizionale telefono cellulare a tastiera.

6.1.1.3 TokenOTP

E' la tipologia di firma dedicata ai clienti di Banca Sella.

Per informazioni ulteriori su tale tipologia di firma, rivolgersi direttamente ad una filiale di Banca Sella.

6.1.2 Tipologia di Firma

Qui è possibile selezionare le opzioni che si vogliono attribuire alla firma da apporre:

- Tipologia,
- Marcatura Temporale,

	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

- Aspetto firma PDF,
 - Immagine di default,
 - Opzioni di Verifica.
-
- ♦ Firma PDF
 - ☞ Firma Semplice

 - ♦ Firma P7M
 - ☞ Firma Semplice
 - ☞ Controfirma
 - ☞ Firma parallela

6.1.2.1 Seleziona la tipologia di firma P7M

Mentre per la firma PDF, esiste la sola tipologia di Firma Semplice, con delle opzioni selezionabili ad ogni richiesta di firma di un documento PDF, "**Seleziona la tipologia di firma P7M**" (vedi 8.1) permette di scegliere la tipologia di firma da applicare solo in caso di firma P7M.

La scelta, una volta memorizzata, è applicata finché non si interviene nuovamente per modificarla, anche in esecuzioni differenti del Trust Signer Client di Trust Signer.

6.1.2.2 Opzioni Marcatura Temporale

Con l'associazione di un riferimento temporale ai propri documenti elettronici l'utente può dimostrare la loro esistenza ad un determinato istante e dare loro la validità legale corrispondente alla tipologia di firma utilizzata per la sottoscrizione.

In tale sezione è possibile selezionare la modalità di richiesta della Marcatura Temporale:

- ♦ Nessuna marcatura,
- ♦ Esegui sempre marcatura,
- ♦ Chiedi ad ogni operazione.

6.1.2.3 Configura aspetto della firma PDF

Consente di impostare le opzioni sull'uso del *testo predefinito* (vuoi che compaia? Allora apponi il check, altrimenti non lo apporre) e sull'immagine da utilizzare nel caso di spunta della casella **Usa immagine predefinita** nella finestra **Configura aspetto firma** (vedi Firmare un Documento PDF par. 8.3).

	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Si tenga tuttavia presente che si tratta di opzioni che vengono preimpostate ma che l'utente può modificare all'atto della firma PDF.

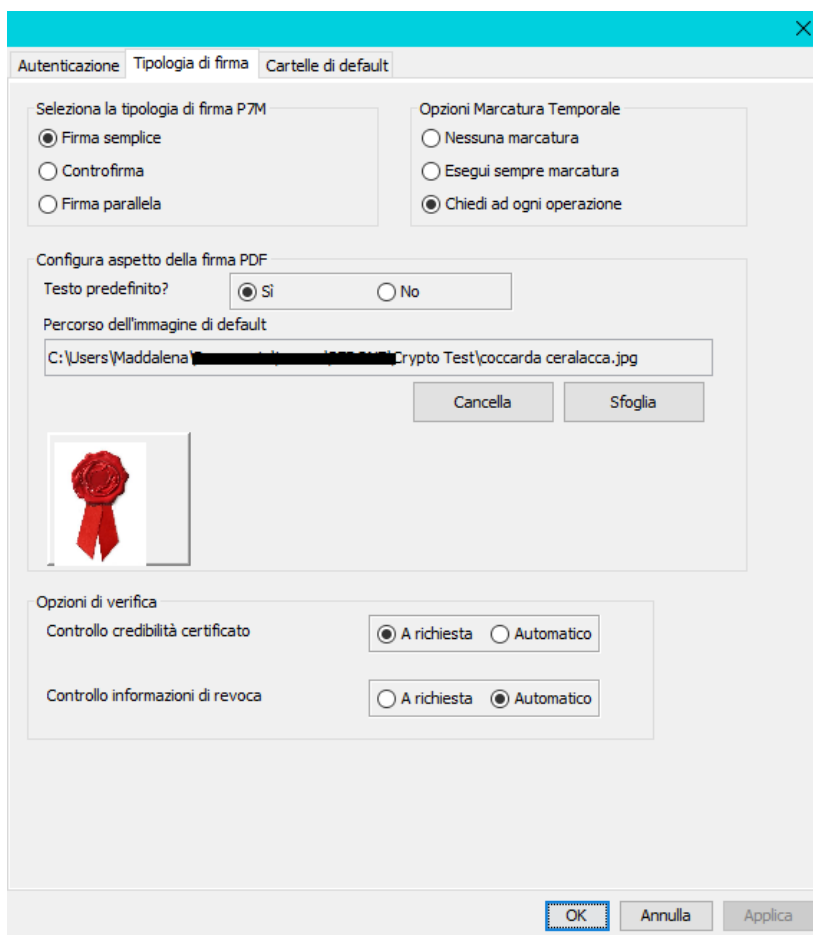


Figura 10

6.1.2.4 Opzioni di verifica

Consente di personalizzare la modalità di verifica di un documento firmato.

- **Controllo credibilità Certificato**
- **Controllo informazioni di revoca**

In entrambi i casi:

- Selezionando **A richiesta**, il relativo controllo non sarà eseguito al momento della selezione di un documento (impostazione predefinita).

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

- Selezionando **Automatico**, il relativo controllo sarà eseguito al momento della selezione del documento.

Si noti che tali impostazioni hanno effetto solo sulla verifica che viene eseguita quando si aggiunge un file in lista e tale file è un documento firmato; premendo il pulsante **Verifica Firma** sulla barra degli strumenti, l'applicazione esegue sempre e comunque la verifica completa.

6.1.3 Cartelle di Default

Consente di impostare le cartelle predefinite per la selezione dei file da processare e il salvataggio dei documenti una volta firmati rispettivamente.

Si tratta come sempre delle cartelle proposte, che l'utente può comunque modificare al momento di aggiungere un nuovo file o salvare un file firmato semplicemente navigando tramite la finestra di dialogo.

Per impostare le cartelle di default, l'utente deve:

- 1) Premere il pulsante **Sfoglia**
- 2) Nella finestra **Modifica posizione** navigare fino alla cartella prestabilita e premere **Scegli**

Il pulsante **Cancella** esegue un reset del valore.

In caso i valori non fossero impostati, per entrambe le posizioni viene considerata come cartella predefinita la cartella utente così come definita sul sistema in uso.

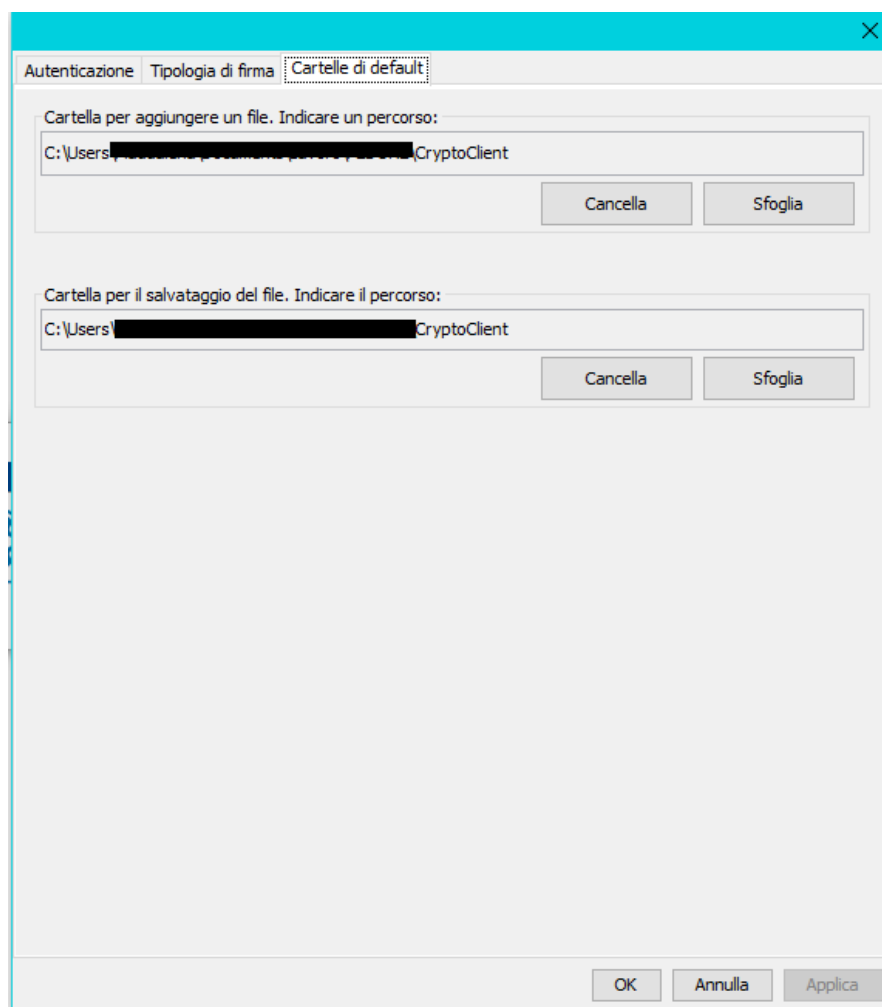


Figura 11

7 Selezione del documento

All'apertura dell'applicazione, e prima di procedere con qualsiasi operazione di firma e verifica, l'utente dovrà selezionare il documento o i documenti sui quali operare. Per effettuare questa operazione l'utente deve:

- 1) Aprire la finestra di selezione tramite il pulsante **Apri file** (unico pulsante attivo in questa fase) o scegliendo dal menu **File** → **Aggiungi un file**
- 2) navigare fino a portarsi nella cartella dove si trovano i file da selezionare
- 3) selezionare i file e premere su **Apri**

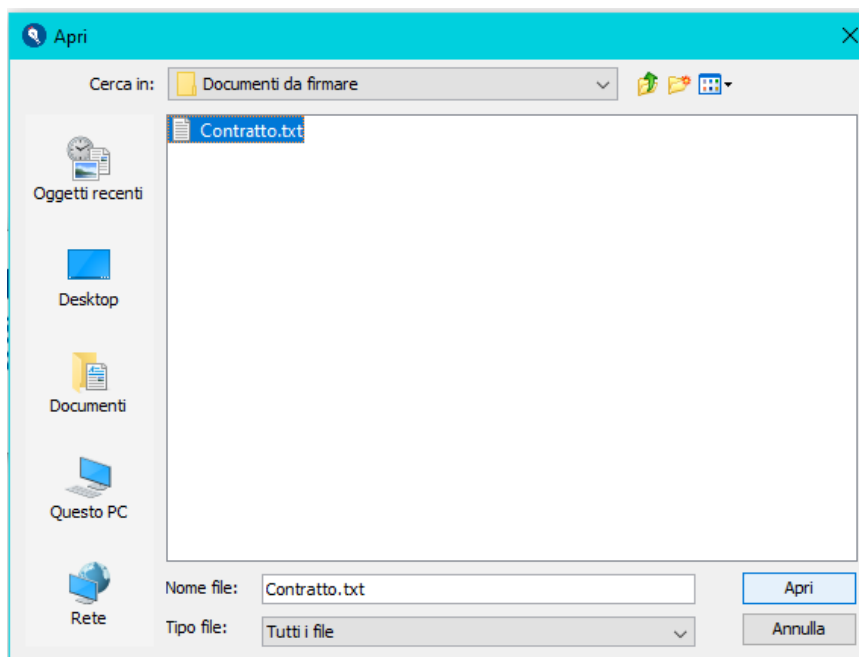


Figura 12

In questa fase l'utente può selezionare:

- *un singolo file*
- *un insieme contiguo di file tramite l'utilizzo del tasto SHIFT*
- *un insieme anche non contiguo tramite l'utilizzo del tasto CTRL*
- *una cartella*
- una combinazione qualsiasi dei punti precedenti
- tutti i files contenuti nel Dettaglio files, mediante un check nella casella in alto a sinistra della finestra di interfaccia dell'applicazione (vedi fig. 13).
- Si noti che la selezione di una cartella equivale alla selezione di tutti i file contenuti in essa.
- A questo punto i documenti selezionati saranno aggiunti in lista e l'utente potrà procedere con le operazioni pianificate.

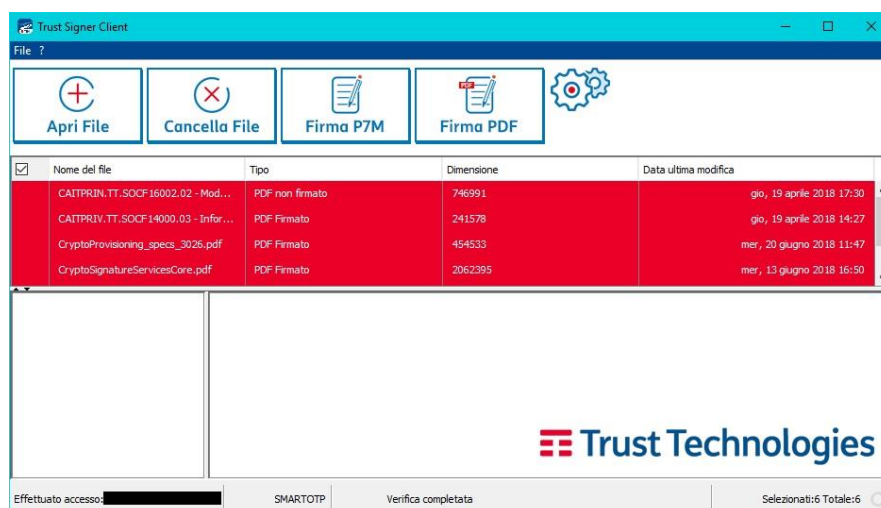


Figura 13

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

7.1 Accesso al Servizio

Ad ogni nuovo lancio dell'applicazione ed una volta selezionato il file, sarà richiesto l'identificativo utente: **Codice Fiscale** associato all'utenza FSM (a meno che non si metta il check sulla casella "Imposta come predefinito").

L'utente dovrà compilare obbligatoriamente il campo e premere sul pulsante **OK** per proseguire.

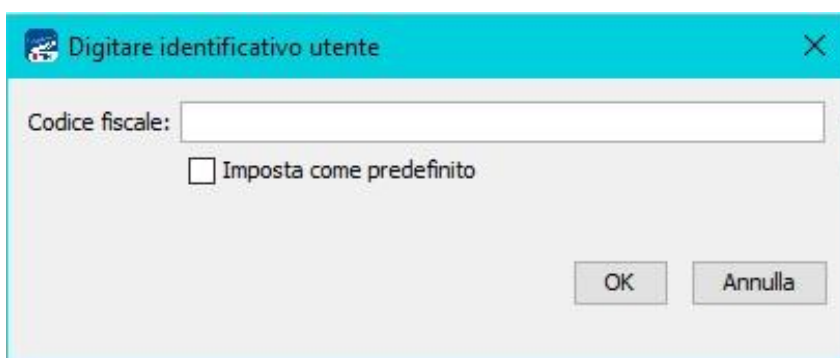


Figura 14

L'identificazione dell'utente sarà valida fino alla chiusura dell'applicazione e verrà richiesta ad un successivo utilizzo.

E' possibile, in alternativa, scegliere l'opzione di salvataggio dell'identificativo (**Imposta come predefinito**): in questo modo l'identificativo è salvato nel file di configurazione dell'applicazione evitando così di doverlo digitare in utilizzi futuri.

Si ricorda che in questa fase non è eseguito alcun controllo di validità dell'identificativo inserito.

La scelta del pulsante **Annulla** o la chiusura della finestra tramite il pulsante della "x" in alto a destra comporta l'annullamento della richiesta d'accesso e il ripristino della schermata iniziale dell'applicazione.

7.2 Operazioni sul file selezionato

All'inserimento del file in lista il **Trust Signer Client** identifica la tipologia del documento ed in base a questa abilita i pulsanti operativi secondo lo schema in tabella:

Tipo documento	Verifica automatica	Operazioni abilitate	Ammessa selezione multipla
PDF firmato	Sì	Firma P7M (± marca temporale) Firma PDF (± marca temporale) Verifica completa	✓ ✓
Busta P7M	Sì	Firma P7M (± marca temporale) Verifica completa Estrazione file originale	✓
Busta TimeStamped Data (TSD)	Sì	Estrazione file originale	
PDF non firmato	Non applicabile	Firma P7M (± marca temporale) Firma PDF (± marca temporale)	✓ ✓
Certificato	Sì	Firma P7M (± marca temporale) Verifica completa	✓
Documento generico (nessuno dei casi prec.)	Non applicabile	Firma P7M (± marca temporale)	✓

Per **Operazioni abilitate** si intende:

Firma P7M – esegue una firma del documento selezionato in modalità *PKCS7 – CaDes*, con o senza Marcatura Temporale

Firma PDF – esegue la firma in modalità *PaDes* del documento PDF selezionato, con o senza Marcatura Temporale

Verifica completa – esegue una verifica completa del documento firmato selezionato includendo cioè il controllo delle informazioni di revoca (CRL) nonché della attendibilità del certificato

Estrazione file originale – esegue l'estrazione e salvataggio di una copia del file originale da una busta firmata.

Alla selezione di un file, se applicabile (documento firmato o certificato), l'applicazione esegue una verifica della o delle firme contenute nel file selezionato (*Verifica automatica*).

Nella finestra di **Selezione della data di verifica** (Figura 15), visualizzata prima di effettuare la verifica del documento firmato, è possibile modificare la data proposta ed eseguire quindi la verifica ad una data particolare scelta dall'utente.

A meno che non siano presenti marche temporali, la verifica del documento viene effettuata a partire da una data proposta, che si riferisce o ad un riferimento temporale presente all'interno del file firmato (il più basso cronologicamente in caso di più riferimenti temporali) oppure alla data del giorno in caso non sia presente alcun riferimento temporale.

Se nel documento firmato sono presenti una o più firme con marca temporale, la loro verifica verrà effettuata automaticamente alla data della marca temporale.

	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Tutte le firme apposte allo stesso documento, e prive di marche temporali, saranno quindi verificate alla data prescelta. La data selezionata è indicata quindi nel dettaglio della verifica.

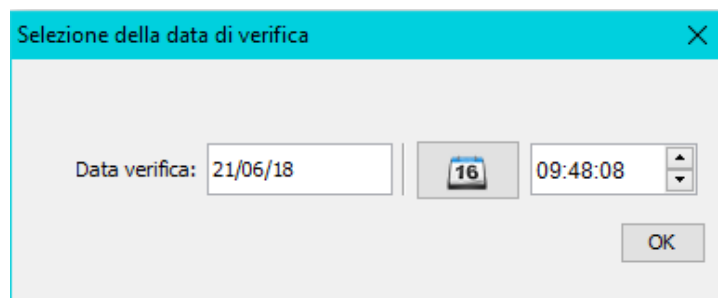


Figura 15

Dopo la selezione della data di verifica, nel caso in cui sia presente un server Proxy, viene richiesta l'autenticazione con le proprie credenziali di accesso:



Figura 16

Selezionando un **PDF firmato**, la finestra principale dell'applicazione si presenta come nella figura seguente (figura 17), presentando la possibilità di scegliere sia la tipologia di firma P7M, che PDF.

Per maggiori dettagli sulle informazioni di verifica si rimanda al capitolo specifico (Verifica della firma di un documento).

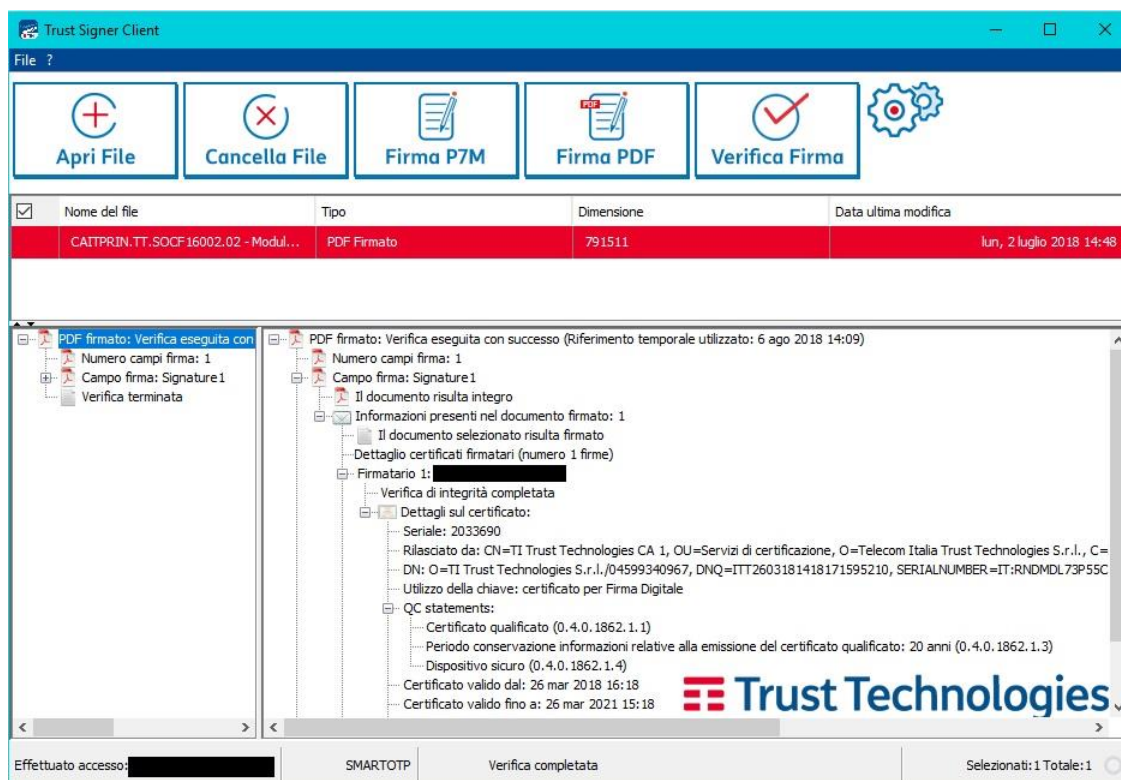


Figura 17

Selezionando invece un file non PDF, non firmato, l'interfaccia si presenterà in questo modo:

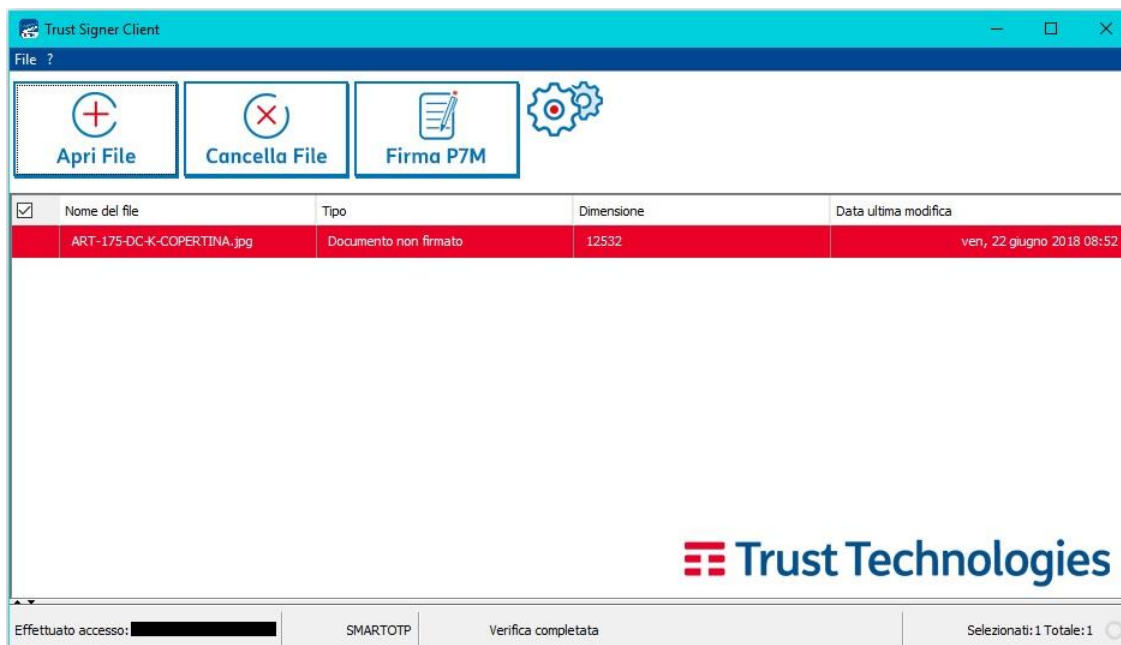


Figura 18

Selezionando un file non PDF , firmato, l'interfaccia dell'applicazione sarà la seguente:

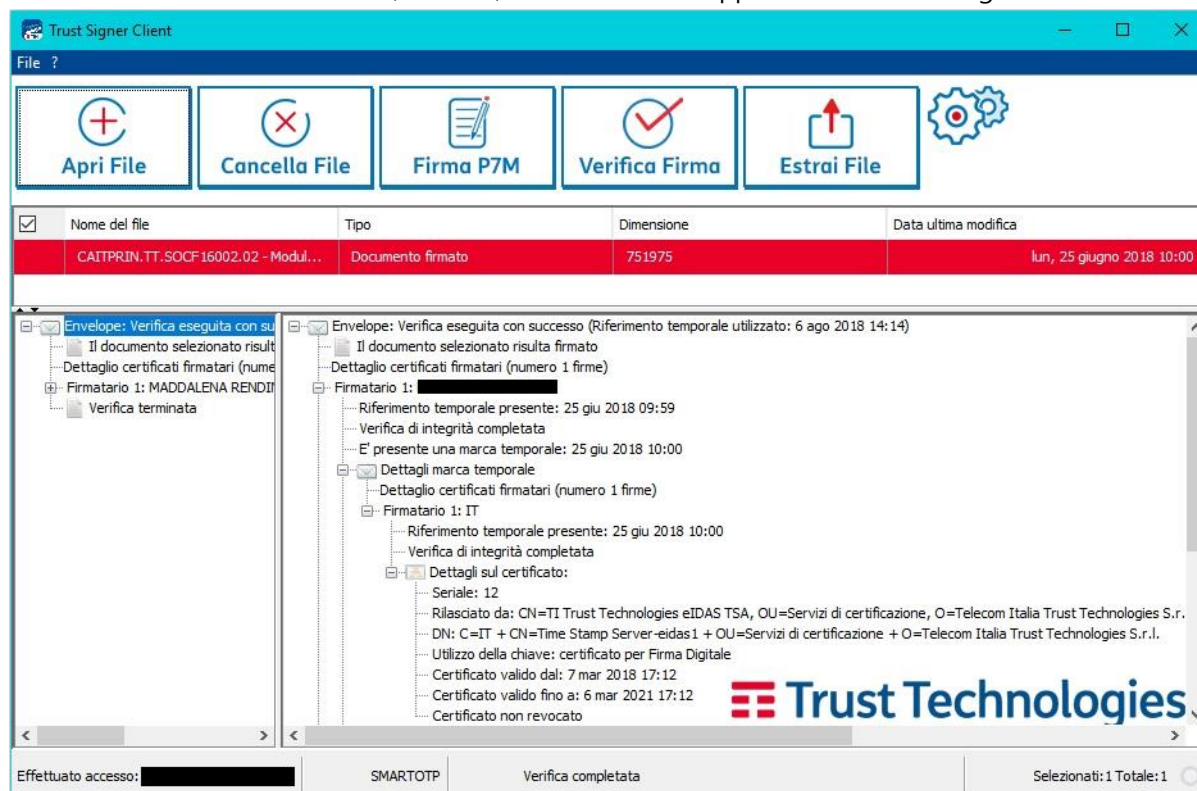


Figura 19

La verifica della firma è normalmente semplice, ossia senza controlli delle liste di revoca e della attendibilità del certificato.

In alternativa a queste operazioni l'utente può anche decidere di rimuovere il documento selezionato dalla lista, poiché inserito per errore o dopo aver terminato le operazioni, tramite click sul pulsante **Rimuovi file**. Si tenga presente che tale operazione non comporta in alcun modo la cancellazione fisica del file dalla cartella di selezione.

Anche in questo caso sono ammesse selezioni multiple.

Attraverso Estrai File, è invece possibile visualizzare il file originale.

8 Firma di un documento

Il **Trust Signer Client** di Trust Signer, permette di applicare due differenti tipi di firma digitale:

1) Firma P7M – CaDes

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

- a. Firma semplice
- b. Controfirma.
- c. Firma parallela

2) Firma PDF – PaDes

- a. Firma semplice

8.1 Scelta della tipologia di firma p7m

L'utente ha la possibilità di scegliere tre differenti tipologie:

- Firma Semplice: firma Cades (p7m) a Matrioska: si considera il precedente interno p7m come documento da firmare (in modalità anche detta annidata).
- Controfirma: firma Cades (p7m) esplicitamente riferita ad altra firma presente sul documento.
- Firma Parallela: firma Cades (p7m) su documento già firmato, dove però la nuova firma si aggiunge a quella già presente nella busta p7m.

La scelta dev'essere effettuata **prima** di iniziare l'operazione di firma attraverso il pannello ***Tipologia di firma*** dalle ***Impostazioni***.

Procedere come segue:

1. Dal menu dell'applicazione scegliere ***Strumenti / Impostazioni*** (per impostazione predefinita la finestra si apre già con il pannello ***Tipologia di firma***)

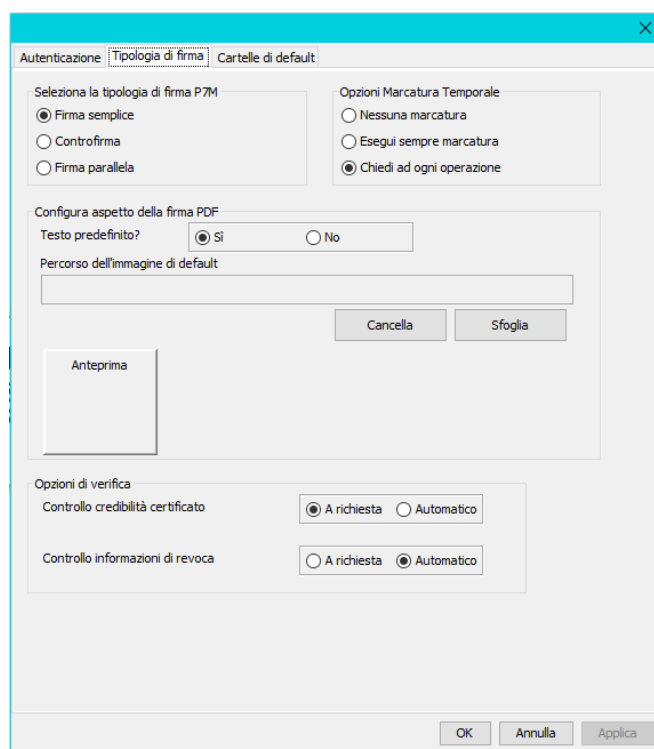


Figura 20

2. Selezionare la tipologia di firma P7M desiderata.
3. Premere sul pulsante OK per salvare l'impostazione e chiudere la finestra.
4. Procedere con la firma.

Non è necessario eseguire tali passaggi ad ogni firma: l'applicazione memorizza l'ultima scelta effettuata e quindi si deve ripetere la procedura solo in caso l'utente voglia cambiare tipologia di firma.

8.2 Firmare un documento p7m

Per applicare una firma P7M ad un file si procede seguendo i seguenti passi:

- 1) Si seleziona il documento da firmare secondo le modalità descritte precedentemente
- 2) Si preme il pulsante **Firma P7M**.

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

8.2.1 Firma semplice

Prima ancora della finestra di messaggio che richiede se si vuole visualizzare il file da firmare, compare la finestra che richiede se si vuole utilizzare la marcatura temporale.

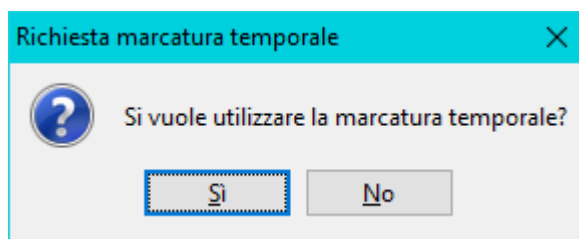


Figura 21

Successivamente, a seconda del tipo di file che si vuole firmare, la finestra di messaggio **Visualizza file** chiede se procedere all'apertura del documento in modo tale che l'utente possa prendere visione di ciò che si appresta a firmare.

Premere **Sì** se si vuole lanciare l'applicazione predefinita per visualizzare il documento o **No** per continuare senza visualizzare il documento.

Caso particolare per documenti con estensione DOC, XLS, PPT e MDB: oltre alla richiesta di visualizzare il documento, il messaggio contiene l'avviso che il documento potrebbe contenere dei campi con valori non statici (macro o campi variabili).

Anche questa opzione di visualizzazione sarà attiva solo in caso di selezione di uno ed un solo documento. In caso di richiesta di visualizzazione, l'utente ha il tempo di prendere visione del documento ed al termine decidere se procedere o meno scegliendo l'opzione desiderata nella finestra di **Conferma firma** rimasta in attesa nel frattempo.

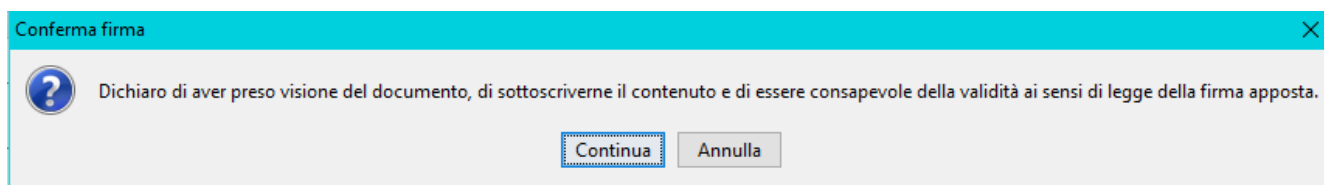


Figura 22

Se si sceglie **Annulla** l'operazione di firma viene annullata e si torna alla finestra principale.

Scegliendo **Sì** si procede al passo seguente.

Se l'utente ha scelto di non visualizzare il documento o l'opzione non è applicabile e quindi non è stato visualizzato alcun messaggio, si passa direttamente al punto seguente.

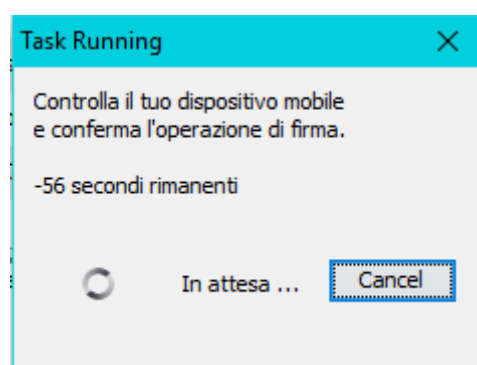
Se all'identificativo utente sono associati più certificati attivi, l'applicazione ne mostrerà la lista in un'apposita finestra in modo tale che l'utente possa scegliere quale utilizzare.

Questo passo è ovviamente saltato nel caso di un solo certificato attivo associato all'utente.

Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Inizia il processo di firma ed una finestra di *progress* informa l'utente che ha 60 secondi di tempo per terminare l'operazione di autenticazione. Se la **modalità di Autenticazione** impostata è **SmartOtp**, quindi attraverso l'app mobile **Trust Signer** dal proprio cellulare, o tablet se munito di SIM, si avrà la seguente situazione:

Da **Client**:



Su **dispositivo con**
SIM di numero di cellulare associato al
Certificato di firma
arriva la notifica:



Figura 23

Figura 24

Dal cellulare, si fa tap sulla notifica, e si aprirà direttamente l'app TrustSigner, a cui seguirà immediatamente dopo una finestra di messaggio **Autorizza Firma digitale** (Fig. 25), e confermando con tap su **"S"**, verrà terminata l'operazione di firma con notifica di conferma (Fig. 26).



Figura 25



Figura 26

Subito dopo, sul Client, comparirà la finestra di autenticazione attraverso il PIN personale di firma (Pin del certificato di firma selezionato precedentemente)

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza



Figura 27

Questa operazione, se il PIN è valido, termina il processo di firma.

Premendo il pulsante **Annulla**, l'operazione viene invece annullata e si torna alla finestra principale.

Completare l'operazione assegnando un nome al file firmato (come impostazione predefinita viene proposto il nome del file originario), scegliendo la posizione in cui salvarlo e confermando con **Salva**.

L'applicativo salva il file aggiungendo all'estensione propria (ad esempio .xlsx) l'ulteriore estensione **p7m**, che identifica il file come firmato.

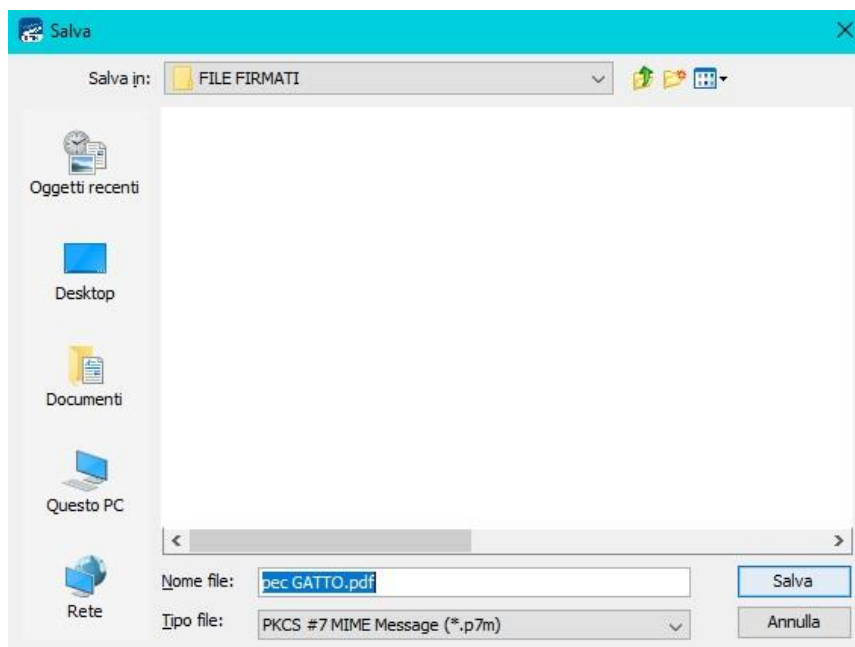


Figura 28

Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

8.2.2 Controfirma

Se la tipologia di firma scelta è **Controfirma**, l'applicazione verificherà la presenza di altre firme e presenterà all'utente l'**Elenco dei firmatari**, come nella Fig. 29:

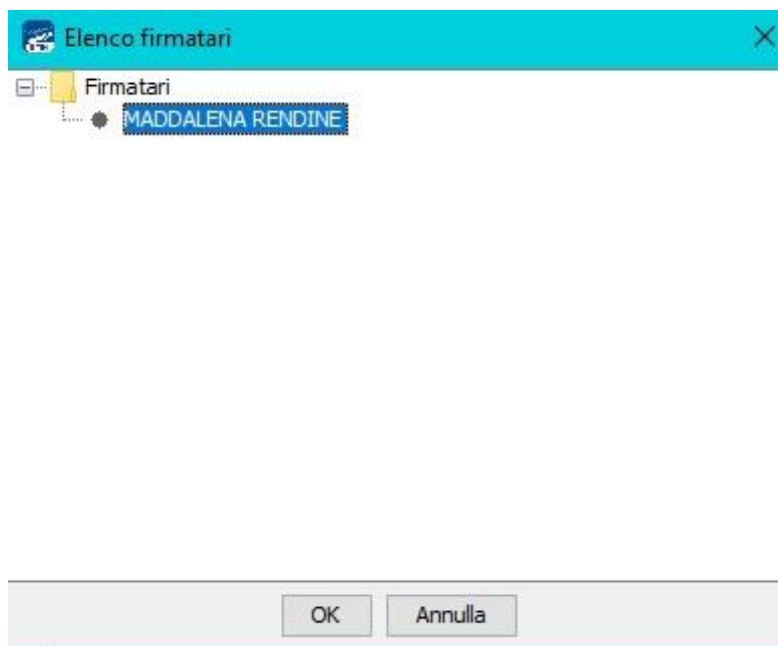


Figura 29

L'utente quindi seleziona il firmatario da controfirmare e procede premendo il pulsante **OK**. Premendo **Annulla** l'operazione viene invece annullata e si torna alla finestra principale.

Si noti che l'opzione **Controfirma** è attivabile solo:

- In caso di selezione di uno ed un solo documento.
- In caso di file pdf con un'apposizione di **firma P7M e non PDF**.

Nel caso in cui il file selezionato non sia stato già firmato, l'applicazione restituirà questa schermata, con le sole azioni visibili dalla Barra degli strumenti (figura 30):

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

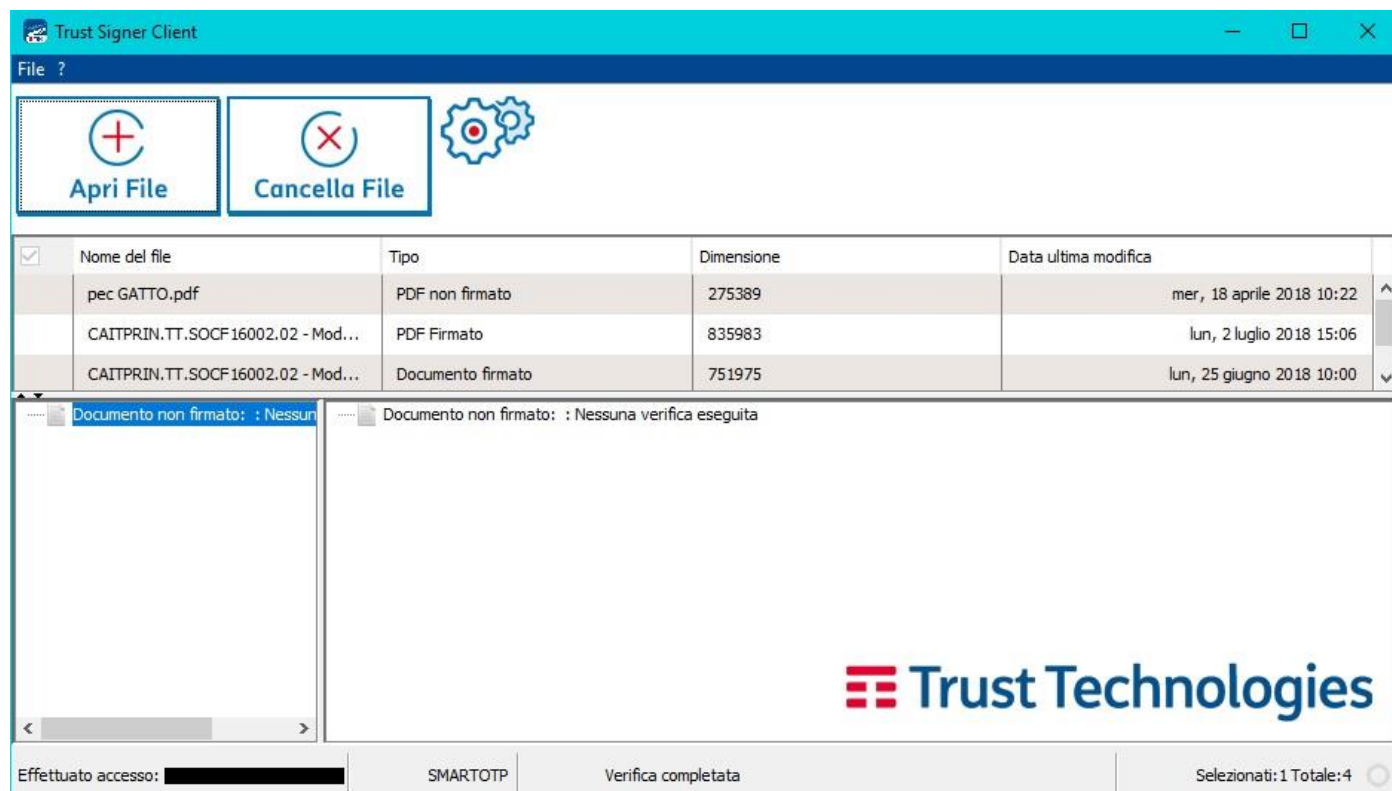


Figura 30

8.2.3 Firma parallela

La firma parallela CADES, viene apposta su un documento già firmato, dove però la nuova firma si aggiunge a quella già presente nella busta p7m.

8.3 Firmare un documento PDF

Per applicare una firma PDF ad un file si procede seguendo i seguenti passi:

- 1) Si seleziona il documento PDF da firmare secondo le modalità descritte precedentemente;
- 2) Premere il pulsante **Firma PDF**
- 3) L'applicazione apre il documento da firmare in un visualizzatore. L'utente dopo aver preso visione del documento dovrà tracciare l'area all'interno della quale voler apporre la firma sul documento

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

trascinando il mouse all'interno della pagina e tenendo premuto il tasto sinistro per rilasciarlo solo al termine del disegno dell'area.

L'operazione può essere ripetuta finché l'area non sarà ritenuta ottimale: è sufficiente eseguire nuovamente il click e trascinamento per tracciare una nuova area mentre la precedente sarà automaticamente annullata.

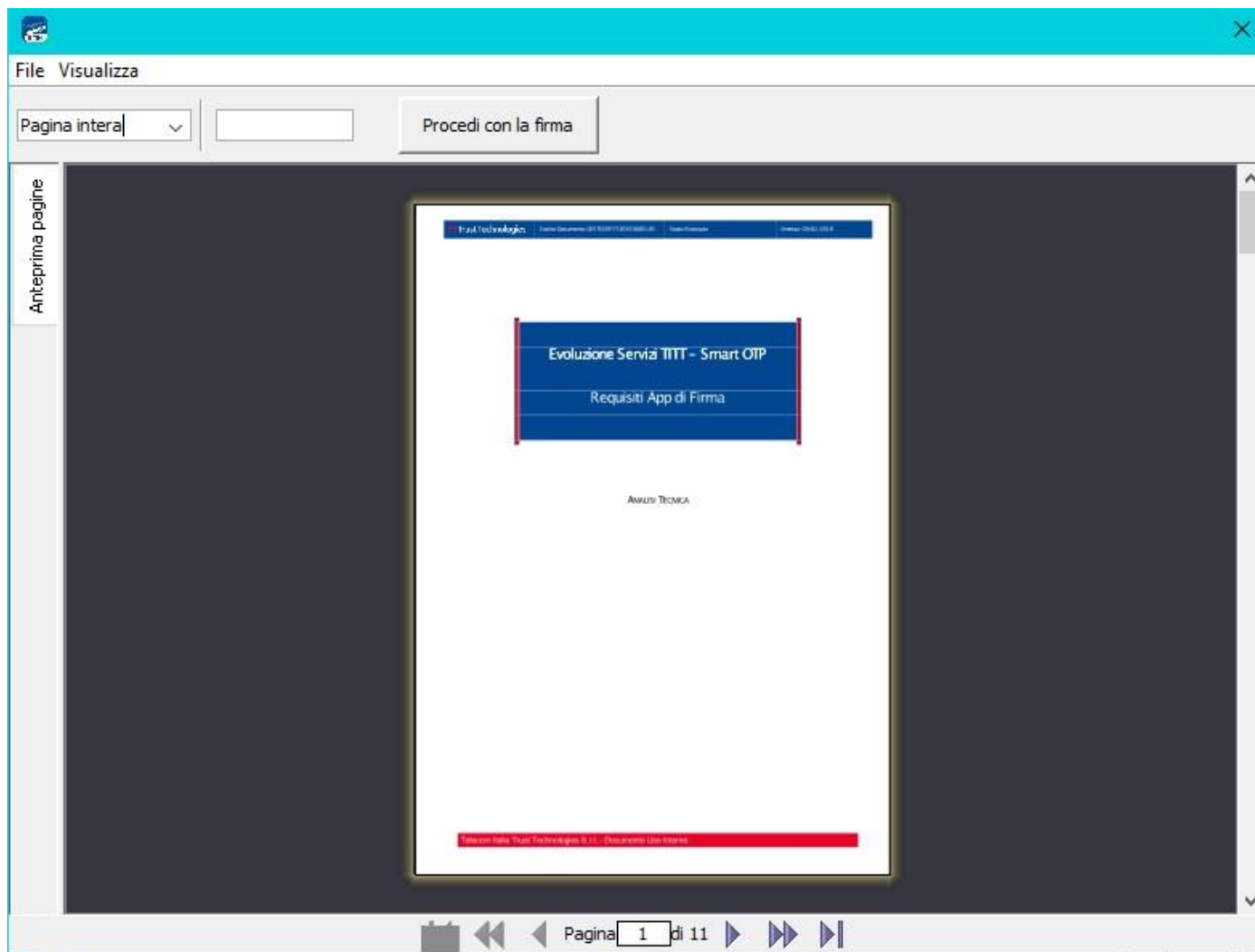


Figura 31

- Definita l'area, l'utente procede premendo il pulsante **Procedi con la firma** posto sulla barra degli strumenti del visualizzatore.

Questo aprirà una nuova finestra, **Configura aspetto della firma**, che consente all'utente di personalizzare la firma inserendo:

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

- un'immagine
- un testo
- il motivo della firma

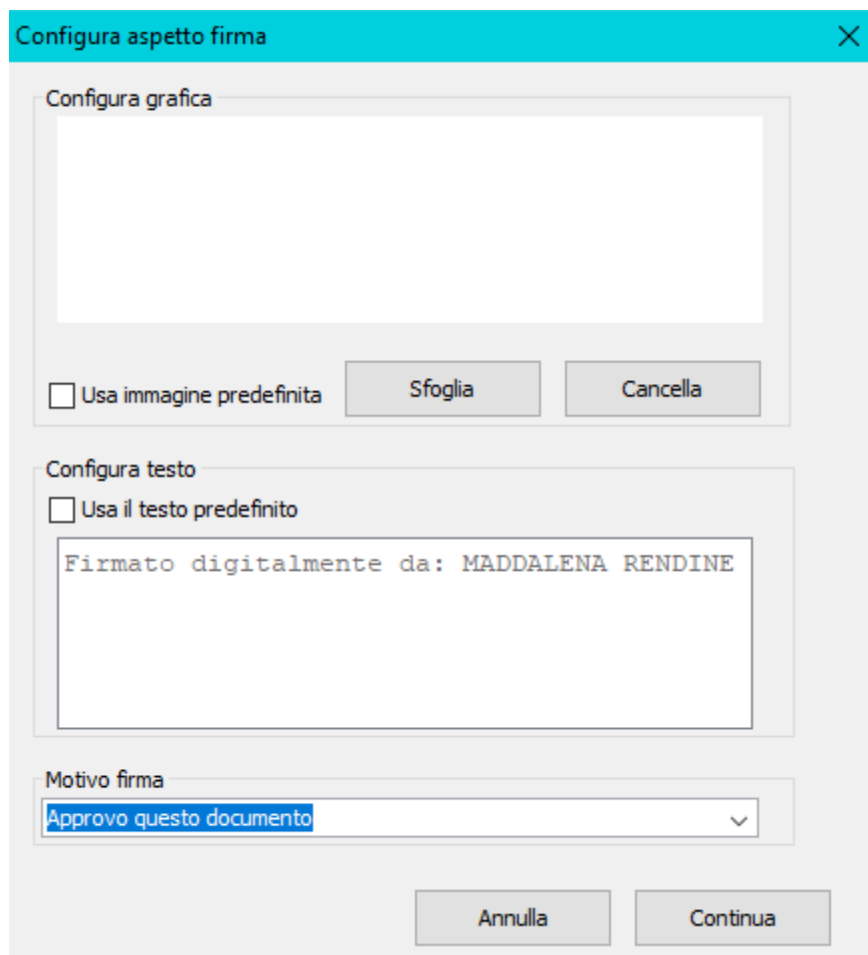


Figura 32

Configura grafica: in questa sezione l'utente può selezionare un'immagine che sarà poi visualizzata nell'area di firma selezionata. La scelta dell'immagine avviene tramite il pulsante **Sfoglia** che permette di aprire una finestra e navigare fino alla cartella contenente l'immagine.

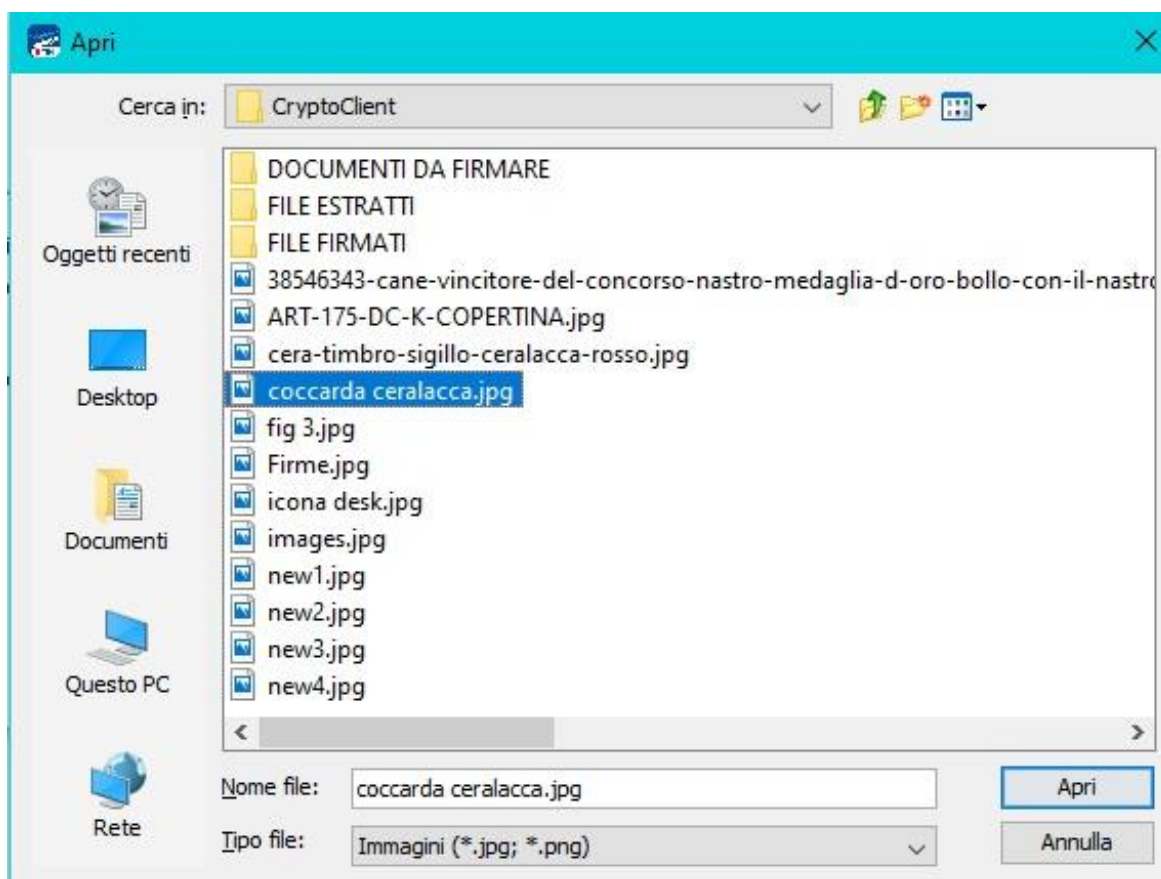


Figura 33

Il pulsante **Apri** seleziona l'immagine.

L'area bianca mostrerà un'anteprima dell'immagine selezionata.

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

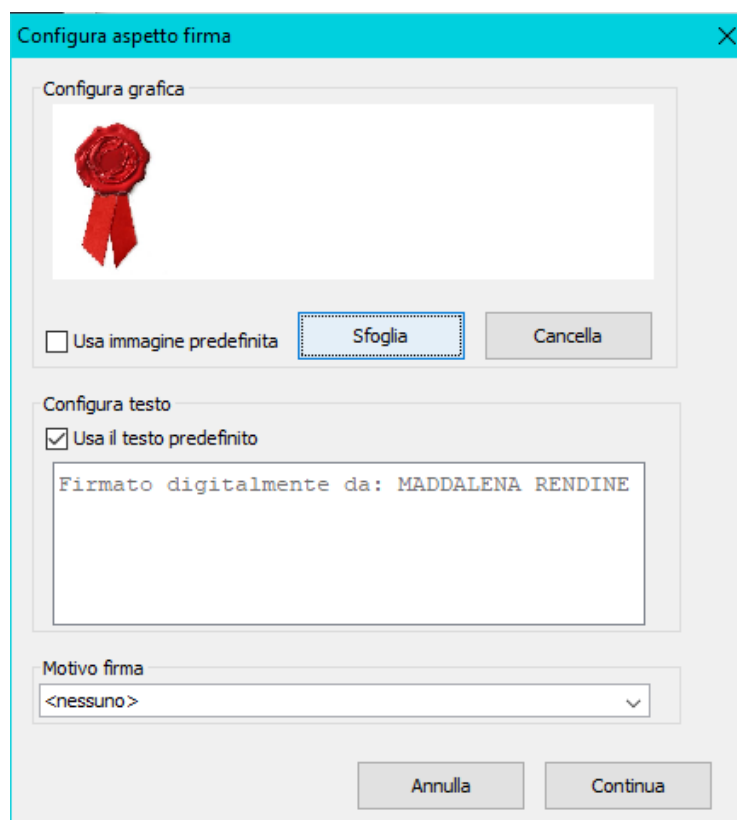


Figura 34

L'utente può altresì selezionare un'immagine precedentemente impostata tramite le impostazioni predefinite dell'applicazione spuntando la casella **Usa immagine predefinita**.

Un click sul pulsante **Cancella** annulla la selezione (nessuna immagine configurata per la firma).

Configura testo: spuntando la casella **Usa il testo predefinito** l'utente sceglie di utilizzare nella firma un testo prestabilito ed impostato dal gestore della piattaforma FSM, e non modificabile dallo stesso utente, del quale ha comunque un'anteprima nell'area testo subito sotto la casella di spunta.

Motivo firma: permette di selezionare il motivo della firma tra quelli proposti o digitarne uno a piacere. Il pulsante **Annulla** consente di tornare al visualizzatore PDF (e quindi anche di rimodificare l'area di firma selezionata o annullare l'intera operazione), il pulsante **Continua**, invece, di procedere con la firma.

- 5) Selezione del certificato.
- 6) Inizia il processo di firma.
- 7) Completare l'operazione assegnando un nome al file firmato (come impostazione predefinita viene proposto il nome del file originario), scegliendo la posizione in cui salvarlo e confermando con Salva. L'estensione del file sarà comunque .pdf.

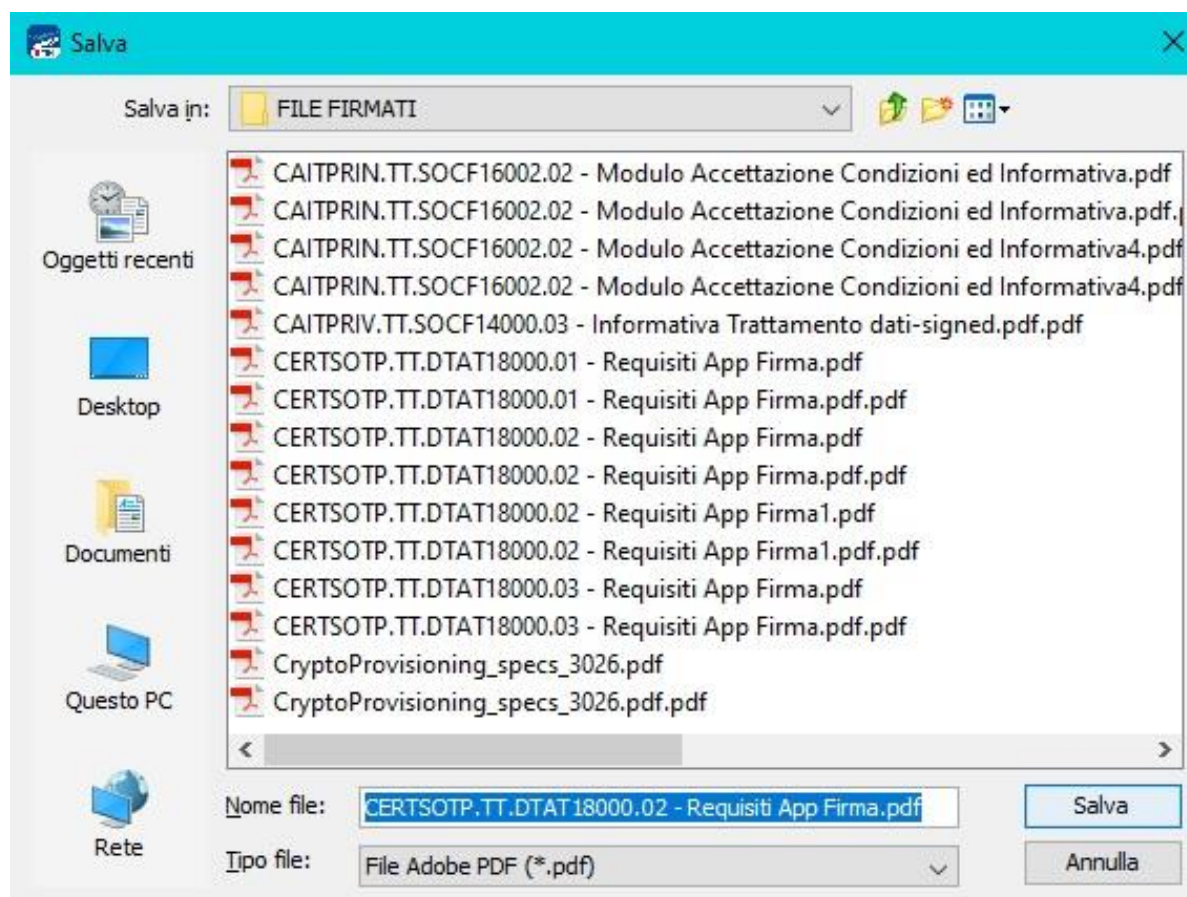


Figura 35

Il risultato, visualizzato nell'esempio con Adobe Acrobat Reader, è quello che si vede nella figura seguente:

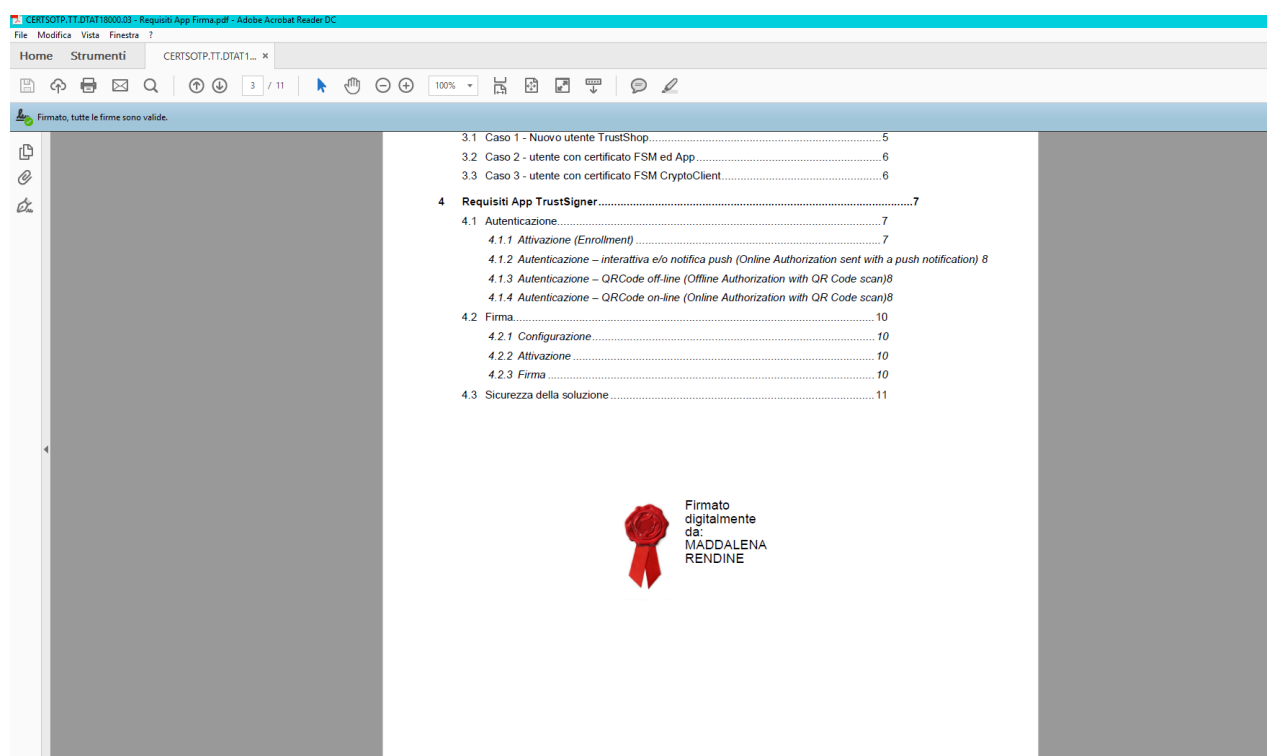


Figura 36

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

8.4 Firma multipla di documenti

Come detto è possibile effettuare una selezione multipla sui documenti inseriti in lista.

In questo caso le sole operazioni possibili sono quelle di firma, oltre alla rimozione di uno o più file dalla lista, mentre sono disabilitate verifica ed estrazione del file originale.

L'autenticazione eseguita tramite chiamata da dispositivo mobile è valida per tutti i documenti selezionati che saranno quindi firmati e salvati nella directory prescelta con nome pari al nome originale con estensione .p7m o .pdf a seconda che si tratti di firma PKCS7/CADES o PDF/PAdES.

In maniera analoga, per quanto concerne la firma PDF, il documento visualizzato è il primo tra quelli in lista. Le impostazioni grafiche nonché la pagina su cui applicare la firma saranno adottate anche per i restanti documenti.

Si noti che la firma PDF è abilitata se tra i documenti selezionati in lista vi è almeno un documento PDF, anche in presenza di altre tipologie di documenti. In questo caso saranno firmati i soli file PDF trascurando gli eventuali file non-PDF.

Analogamente, per la firma P7M, se tra i file selezionati ve ne sono alcuni per i quali questa non è permessa (es. TSD), questi saranno esclusi dalle operazioni di firma.

9 Verifica della firma di un documento

La funzione di verifica dei file consente di verificare che i documenti in possesso dell'utente:

- non siano stati più modificati dopo la firma digitale (**verifica di integrità**)
- siano stati firmati con una coppia di chiavi rilasciata da un certificatore qualificato (**verifica di attendibilità**)
- siano stati firmati con un certificato valido, ossia né sospeso, né revocato (**verifica di validità e controllo CRL**).

Almeno che non siano presenti marche temporali, la verifica dei documenti firmati viene effettuata a partire da una data proposta, che si riferisce o ad un riferimento temporale presente all'interno del file firmato (il più basso cronologicamente in caso di più riferimenti temporali) oppure alla data del giorno in caso non sia presente alcun riferimento temporale. Nella finestra che viene visualizzata prima di effettuare la verifica del documento firmato è poi possibile modificare la data proposta in modo tale, quindi, da eseguire la verifica ad una data particolare scelta dall'utente.

 Trust Technologies	Codice: CERTMOB1.DPMU12005.01
Trust Signer Client – Manuale Utente	Stato: Bozza

Tutte le firme apposte allo stesso documento, e prive di marche temporali, verranno quindi verificate alla data prescelta.

Se nel documento firmato invece sono presenti una o più firme con marca temporale, la loro verifica verrà effettuata automaticamente alla data della marca temporale.

Per verificare un file:

- 1) Selezionare il file firmato che si vuole verificare.
- 2) Premere sul pulsante **Verifica Firma** dalla barra degli strumenti (Fig. 38).
- 3) Se nel documento firmato sono presenti delle firme contenenti dei riferimenti temporali, verrà mostrata la finestra di selezione della data da utilizzare per la verifica (Fig. 37). Per continuare con la verifica alla data proposta premere il bottone **OK**, oppure selezionare una data differente e premere **OK**.

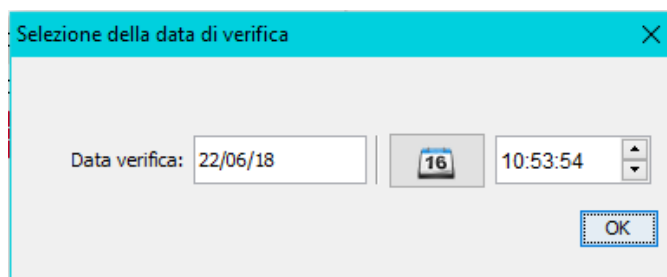


Figura 37

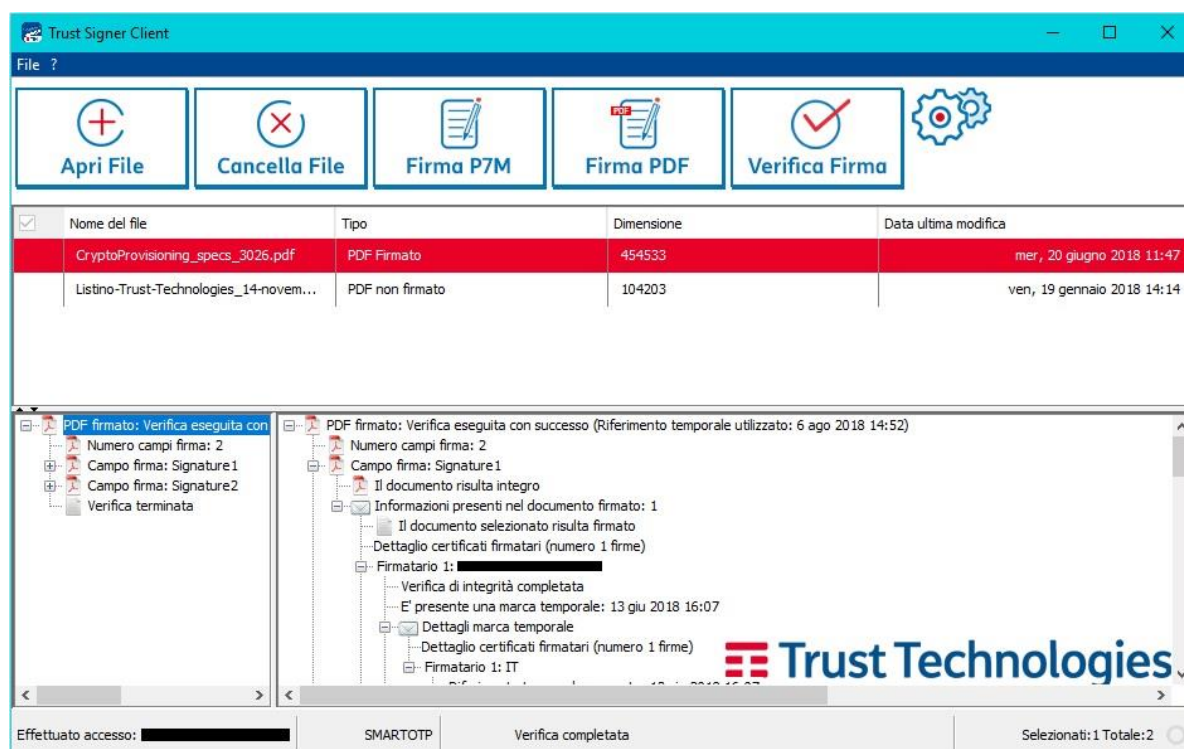


Figura 38

Attenzione: se nel documento sono presenti una o più firme tutte con marca temporale associata, anche se comparirà ugualmente la finestra di selezione della data di verifica, esse verranno tutte verificate alla data della marca temporale.

4) Nell'area di dettaglio verifica verrà visualizzato il risultato:

- nell'area di sinistra, la radice dell'albero riporta la tipologia di documento e l'esito generale della verifica con la data di riferimento. In particolare comparirà il testo **Verifica eseguita con successo** o **Verifica fallita** a seconda che l'esito della verifica sia stato positivo o negativo rispettivamente.

I nodi di primo livello riportano invece le informazioni principali, ossia il numero dei campi firma, la lista dei campi firma ed eventuali riferimenti temporali trovati.

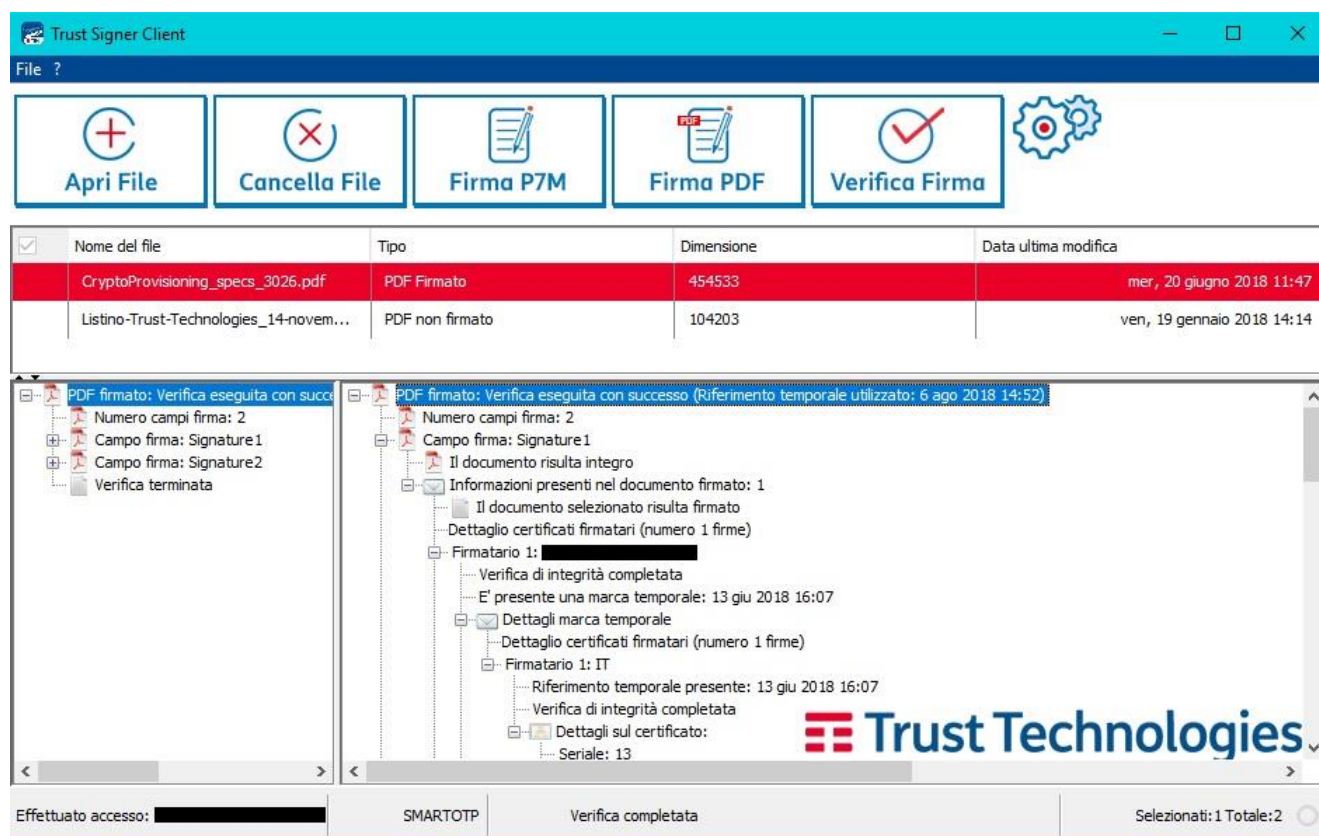
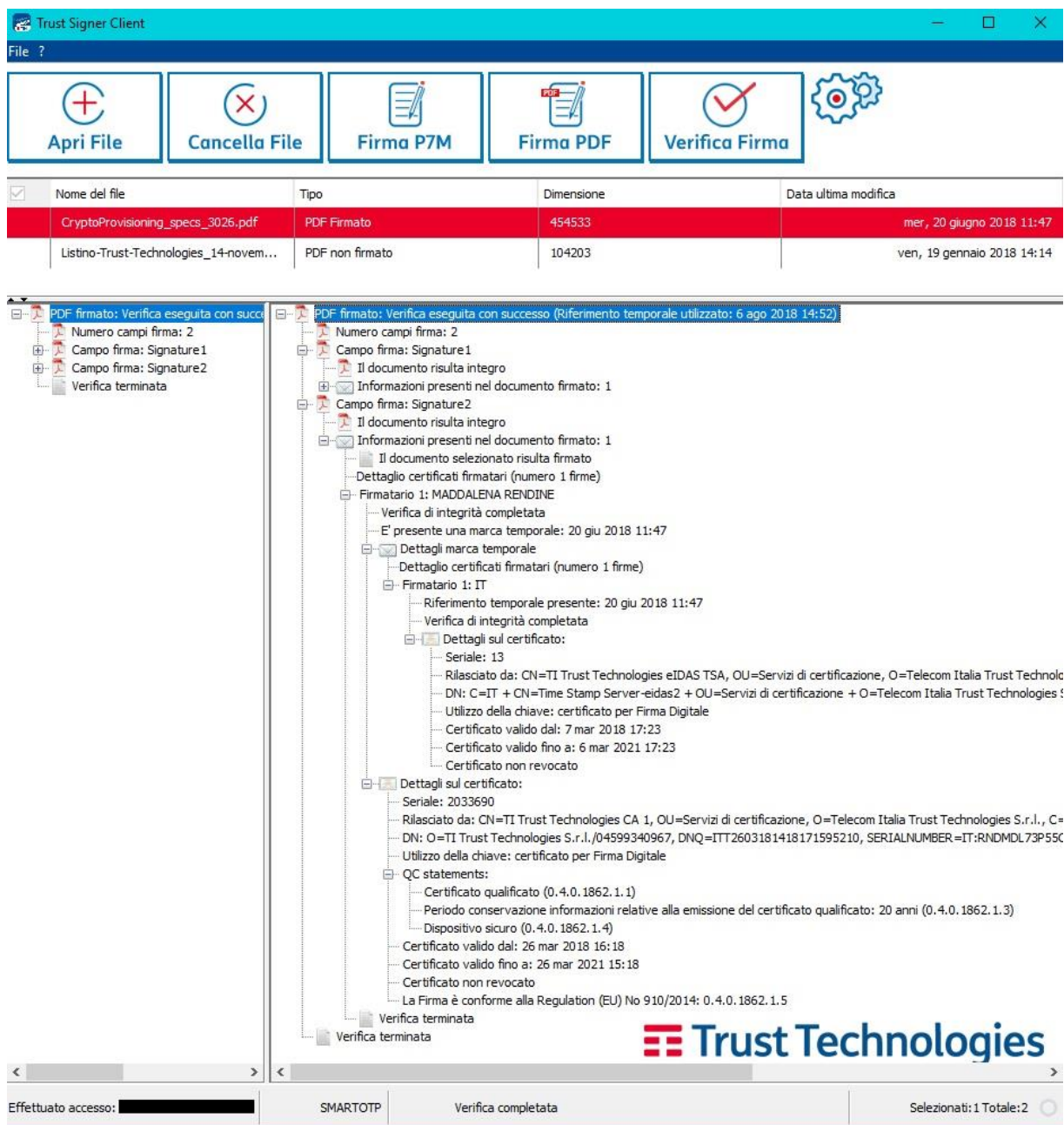


Figura 39

- nell'area di destra, vi è il dettaglio completo dei vari campi firma ed in particolare dei certificati con cui il documento è stato firmato e quindi:
 - i. verificare l'attendibilità del certificato, ossia che il certificato del firmatario sia stato rilasciato da un certificatore accreditato che ne garantisca quindi la validità;
 - ii. controllarne la revoca, per verificare che il certificato con cui è stato firmato il documento sia valido, ovvero né sospeso né revocato.



The screenshot displays the Trust Signer Client application window. At the top, there is a menu bar with 'File ?' and a toolbar with buttons for 'Apri File', 'Cancella File', 'Firma P7M', 'Firma PDF', 'Verifica Firma', and a settings icon. Below the toolbar is a table listing files:

Nome del file	Tipo	Dimensione	Data ultima modifica
CryptoProvisioning_specs_3026.pdf	PDF Firmato	454533	mer, 20 giugno 2018 11:47
Listino-Trust-Technologies_14-novem...	PDF non firmato	104203	ven, 19 gennaio 2018 14:14

The main area shows a detailed verification report for the selected PDF file. The report is structured as follows:

- PDF firmato: Verifica eseguita con successo (Riferimento temporale utilizzato: 6 ago 2018 14:52)
- Numero campi firma: 2
- Campo firma: Signature1
- Campo firma: Signature2
- Verifica terminata
- Il documento risulta integro
- Informazioni presenti nel documento firmato: 1
- Campo firma: Signature2
- Il documento risulta integro
- Informazioni presenti nel documento firmato: 1
- Il documento selezionato risulta firmato
- Dettaglio certificati firmatari (numero 1 firme)
- Firmatario 1: MADDALENA RENDINE
- Verifica di integrità completata
- E' presente una marca temporale: 20 giu 2018 11:47
- Dettagli marca temporale
- Dettaglio certificati firmatari (numero 1 firme)
- Firmatario 1: IT
- Riferimento temporale presente: 20 giu 2018 11:47
- Verifica di integrità completata
- Dettagli sul certificato:
 - Seriale: 13
 - Rilasciato da: CN=TI Trust Technologies eIDAS TSA, OU=Servizi di certificazione, O=Telecom Italia Trust Technolo
 - DN: C=IT + CN=Time Stamp Server-eidas2 + OU=Servizi di certificazione + O=Telecom Italia Trust Technologies
 - Utilizzo della chiave: certificato per Firma Digitale
 - Certificato valido dal: 7 mar 2018 17:23
 - Certificato valido fino a: 6 mar 2021 17:23
 - Certificato non revocato
- Dettagli sul certificato:
 - Seriale: 2033690
 - Rilasciato da: CN=TI Trust Technologies CA 1, OU=Servizi di certificazione, O=Telecom Italia Trust Technologies S.r.l., C=
 - DN: O=TI Trust Technologies S.r.l./04599340967, DNQ=ITT2603181418171595210, SERIALNUMBER=IT:RNDMDL73P55C
 - Utilizzo della chiave: certificato per Firma Digitale
- QC statements:
 - Certificato qualificato (0.4.0.1862.1.1)
 - Periodo conservazione informazioni relative alla emissione del certificato qualificato: 20 anni (0.4.0.1862.1.3)
 - Dispositivo sicuro (0.4.0.1862.1.4)
 - Certificato valido dal: 26 mar 2018 16:18
 - Certificato valido fino a: 26 mar 2021 15:18
 - Certificato non revocato
 - La Firma è conforme alla Regulation (EU) No 910/2014: 0.4.0.1862.1.5
- Verifica terminata

The bottom status bar shows: Effettuato accesso: [redacted], SMARTOTP, Verifica completata, and Selezionati: 1 Totale: 2.

Figura 40