SOMMARIO

Che cos’è la Firma Digitale – concetti

L a *Firma Digitale* o *firma elettronica qualificata* è un particolare tipo di firma elettronica che, nell'ordinamento giuridico italiano, ha lo stesso valore legale di una tradizionale firma autografa apposta su carta.

La firma digitale è disciplinata dal "Codice dell'amministrazione digitale" (*D.lgs 82/2005*)

L'apposizione di firma digitale su un documento è un processo informatico di crittografia a chiave pubblica che consente al sottoscrittore di rendere manifesta l'autenticità del documento e al destinatario di verificarne la provenienza e l'integrità. In particolare la firma digitale garantisce:

- ***Autenticità***: l'identità del sottoscrittore è sicura
- ***Integrità***: certezza che il documento non è stato modificato dopo l'apposizione della firma
- ***Non ripudio***: il documento firmato ha piena validità legale e non può essere ripudiato dal sottoscrittore

Tutto il processo di firma elettronica qualificata si basa su certificati digitali. Per tale motivo è fondamentale garantire l'affidabilità degli Enti autorizzati al rilascio di tali certificati. È stato quindi costituito un elenco di certificatori accreditati. L’elenco pubblico dei certificatori è mantenuto, sottoscritto digitalmente e reso disponibile in rete da *DigitPA*.

Per maggiori dettagli sui certificatori accreditati:

Per maggiori dettagli sui certificatori accreditati:

- https://dss.agid.gov.it/tsl-info/it

[torna all'indice]

Che cos'è la Firma Digitale – tipologie

Esistono due tipi di formato possibili per i documenti firmati digitalmente:

- ***estensione .p7m - CADES***. Il formato di firma digitale CAdES è uno dei più diffusi, poiché il file d'estensione .p7m della cosiddetta busta informatica, da esso prodotta, è riconosciuto dalla normativa vigente come valido per garantire l'interoperabilità tra i sistemi di firma digitale.

- ***estensione .pdf - PADES. PAdES***. è un acronimo che sta per PDF Advanced Electronic Signature. In buona sostanza, si tratta di una firma elettronica che, basando sul formato PDF le modalità e le tecnologie per l'identificazione dell'autore del documento e per le informazioni contenute nel documento originale (secondo la norma ETSI TS 102 778 e lo standard ISO 32000-1), garantisce le qualità necessarie per essere definita "firma elettronica avanzata" (con valore legale) secondo quanto individuato dalla Direttiva 1999/93/EC . Il formato Pades (*.pdf) è ritenuto maggiormente attendibile del *.p7m in quanto il formato pdf oltre che ad essere maggiormente leggibile per l'ampia diffusione dei software compatibili che ne permettono la lettura, è un formato che permette la firma di soli files di documenti. Il formato *.p7m permette in teoria la firma anche di files eseguibili.

Per maggiori dettagli sulla firma digitale ed il suo utilizzo, si rimanda al sito:

- http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

[torna all'indice]

Come dotarsi della Firma Digitale?

Per dotarsi della firma digitale è necessario rivolgersi esclusivamente ai certificatori accreditati.

Bisogna quindi registrarsi presso un ente di certificazione autorizzato (vedi elenco) e ottenere così una smart card con il certificato di firma digitale e relativo PIN.

N.B. Sebbene le procedure per la richiesta di firma digitale siano pressoché tutte identiche, per le modalità operative si rimanda ai singoli Enti. Va precisato comunque che, **in nessun caso**, è possibile ottenere un dispositivo di firma digitale senza incontrarsi personalmente con il certificatore o suo incaricato.

È necessario quindi dotare la propria postazione di un lettore di smart card o token usb e di software per effettuare le operazioni di firma e/o verifica dei documenti. Tra i numerosi software gratuiti che è possibile utilizzare, consigliamo l'applicativo ArubaSign rilasciato da Aruba S.p.a.

Solitamente, chi rilascia il certificato può fornire il kit completo di firma, composto da certificato, lettore e software.

Punti di rilascio capillari nel territorio:

- Camere di commercio (per le Aziende e professionisti)

- Ordini professionali
- CCNS (carta nazionale dei servizi) in molte regioni per singole provincie rilasciano i certificati di firma all'interno delle tessere sanitarie e forniscono gratuitamente i lettori di card.
- Aruba s.p.a. e altri autorizzati

[torna all'indice]

Firmare l'autocertificazione con ArubaSign

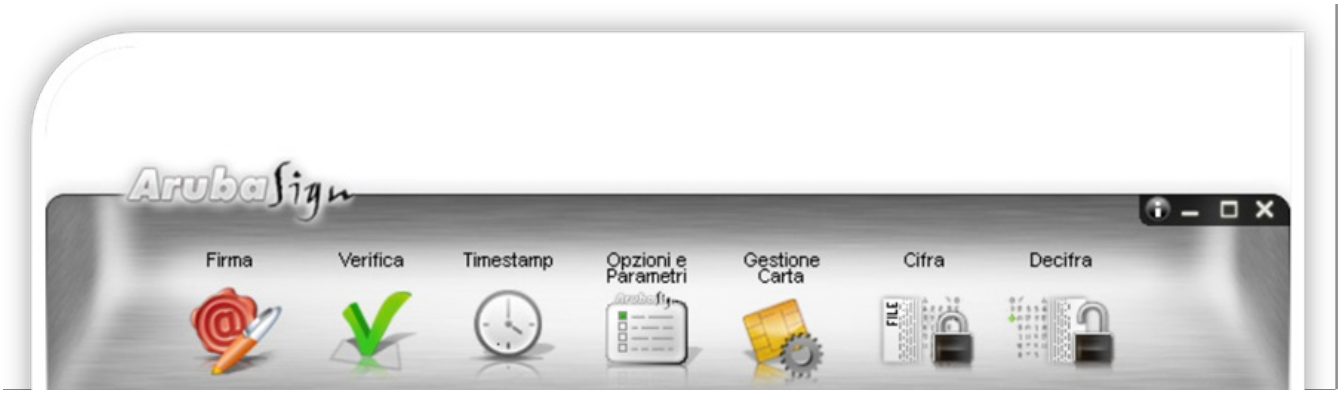
A titolo esemplificativo, di seguito vengono riportate alcune schermate in cui viene simulata la firma digitale dell'autocertificazione generata dal portale dell'Elenco Fornitori Professionisti e Gare telematiche; la firma verrà apposta tramite ArubaSign, software distribuito da Aruba S.p.a., uno dei certificatori più utilizzati in Italia.

È possibile scaricare il software ArubaSign dal seguente indirizzo:

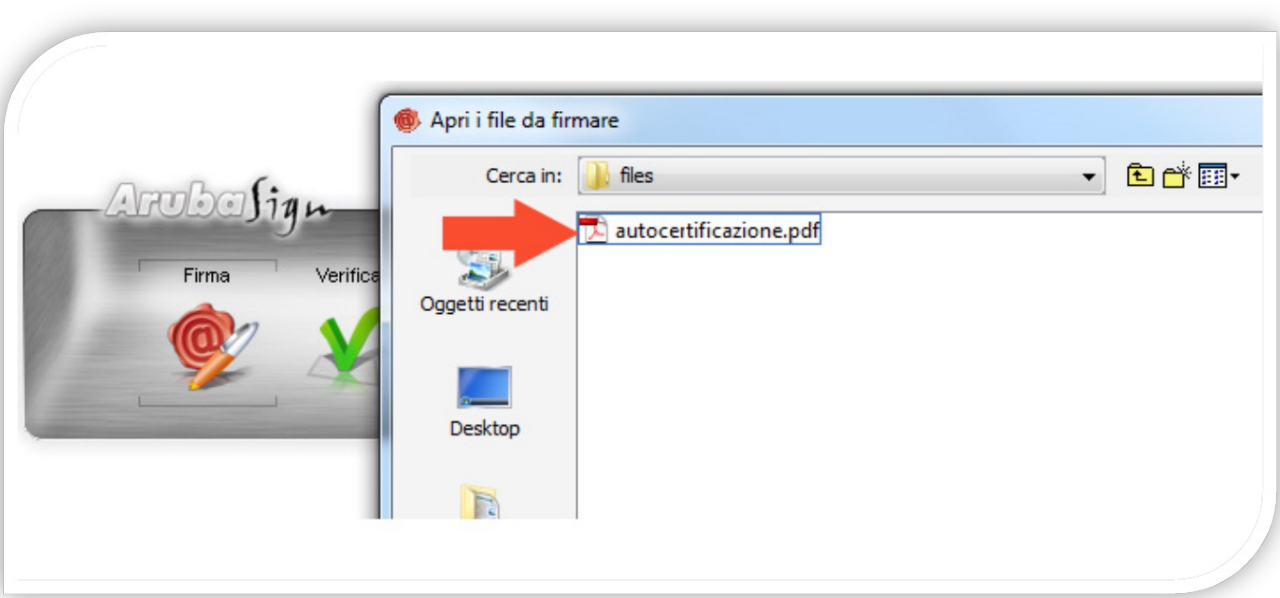
- http://www.pec.it/Download.aspx

Generare l'autocertificazione e salvare il file in una cartella del proprio pc

Installare e avviare il software ArubaSign per la firma digitale

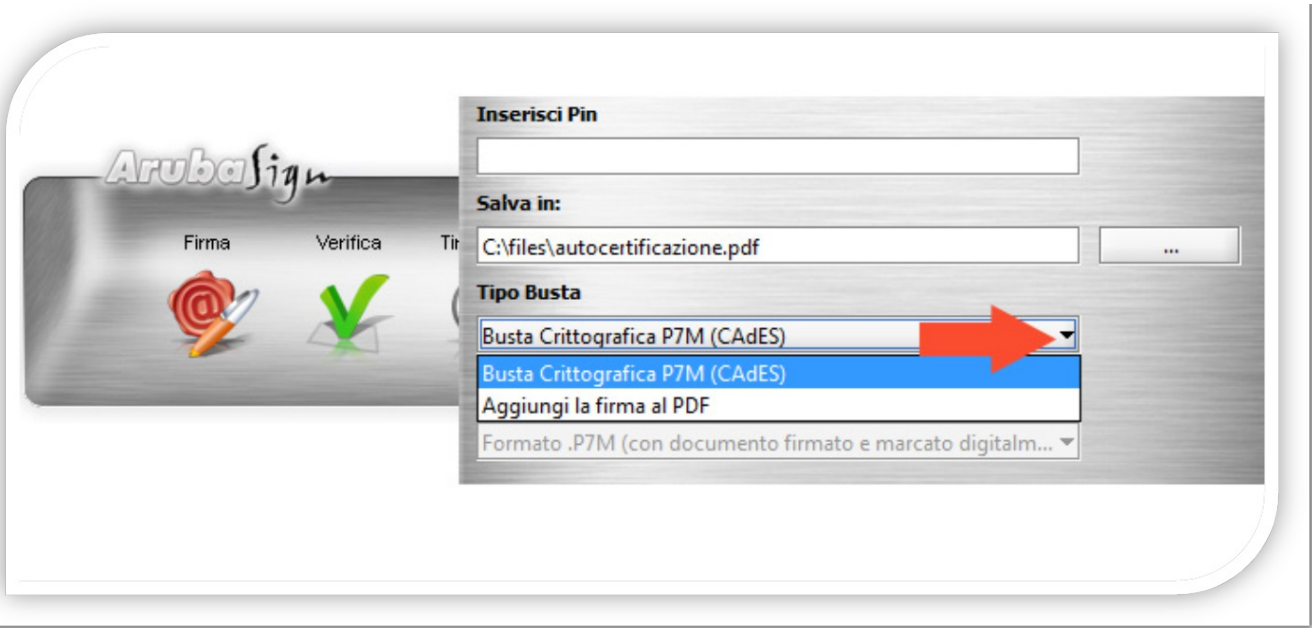


Selezionare il documento da firmare cliccando su “Firma”
(verrà aperta una finestra di navigazione per selezionare il file desiderato)

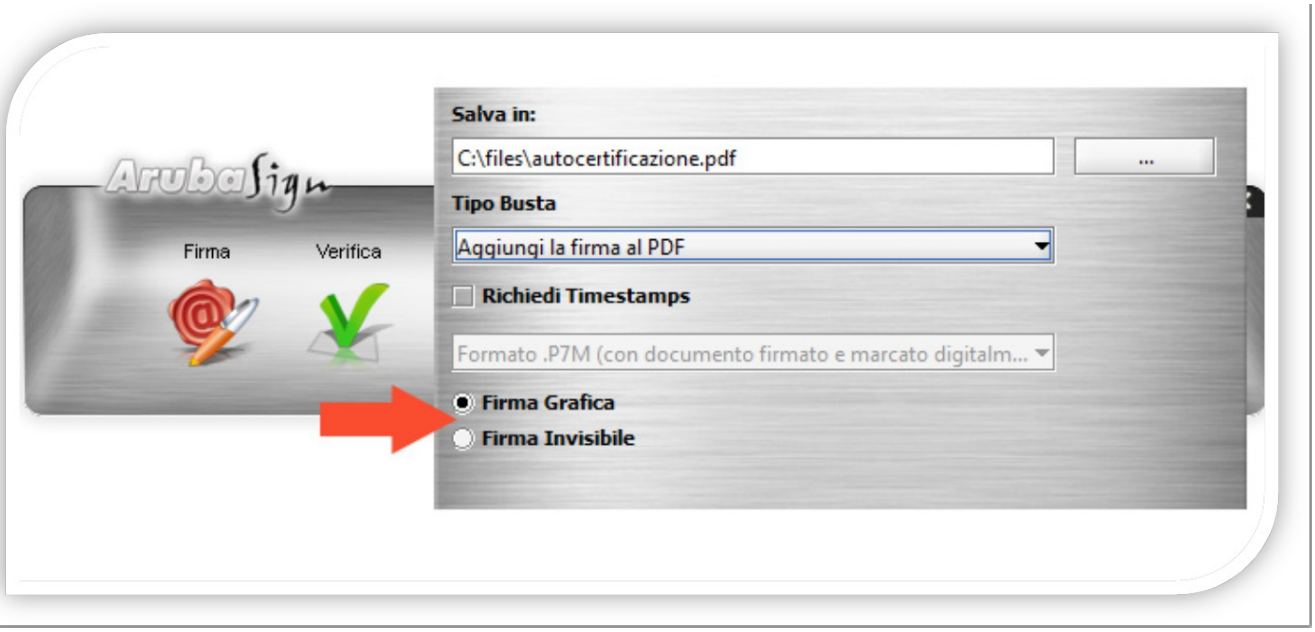


Inserire il PIN, ovvero il codice univoco associato alla propria firma digitale
(nella stessa finestra è possibile scegliere la cartella di destinazione del file dopo la firma)

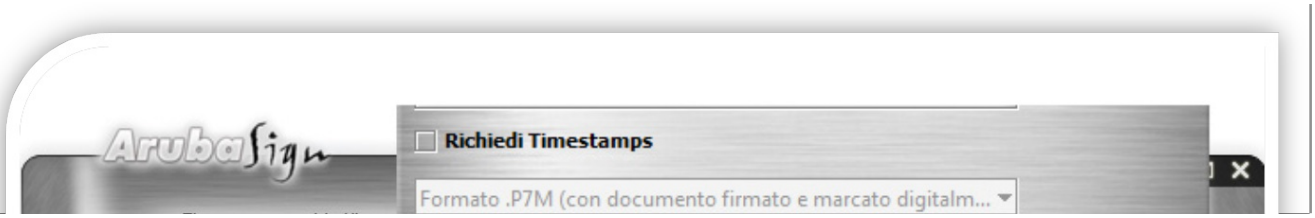
Scegliere la tipologia di firma, se CAdES o PAdES*
(in caso venga scelto il formato PAdES, è necessario scegliere se inserire graficamente la propria firma da file, o invisibile)



Scegliere la tipologia di firma, se grafica o invisibile
(in caso si scelga di inserire graficamente la propria firma da file, il processo di firma avrà un passaggio aggiuntivo*)

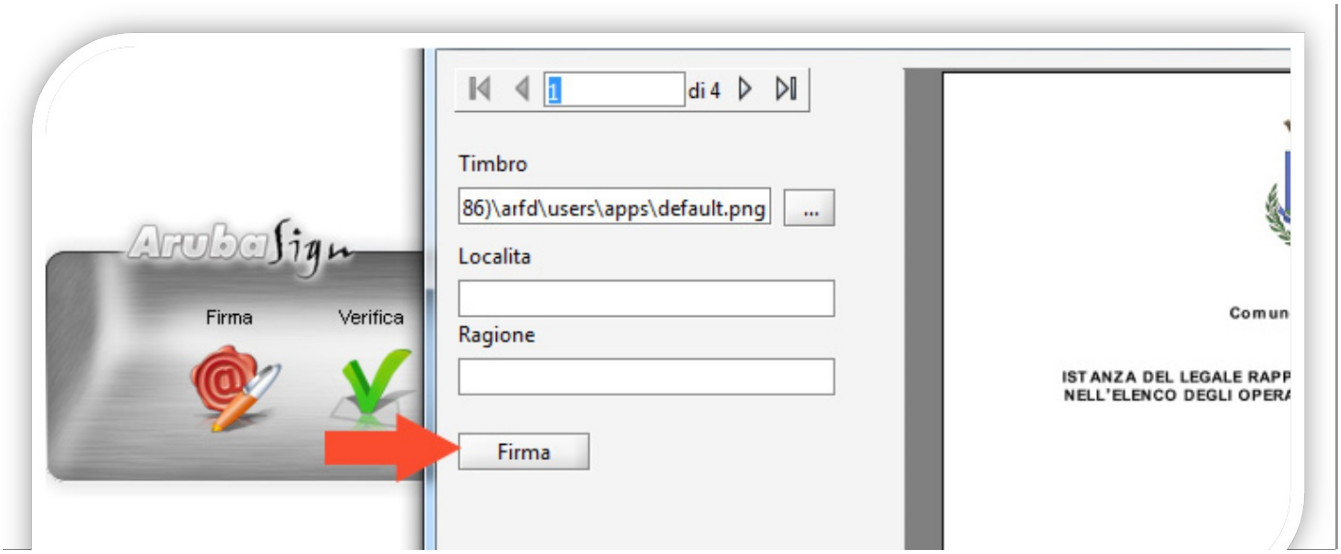


Una volta inserito il pin cliccare sul pulsante “avanti”



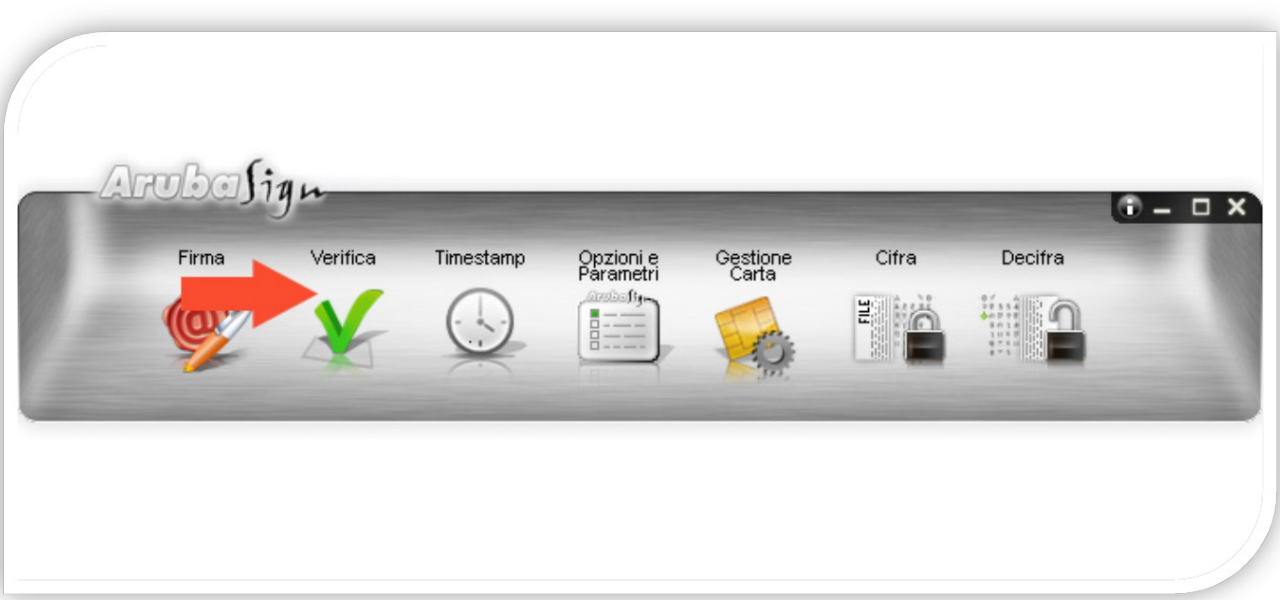
Spuntare la dichiarazione come richiesto e poi cliccare sul pulsante “avanti”
(nella stessa finestra è possibile aprire il file che si sta firmando attraverso il pulsante “Apri Documento”)

* Se è stato scelto di apporre una firma grafica verrà richiesto di selezionare il file della firma

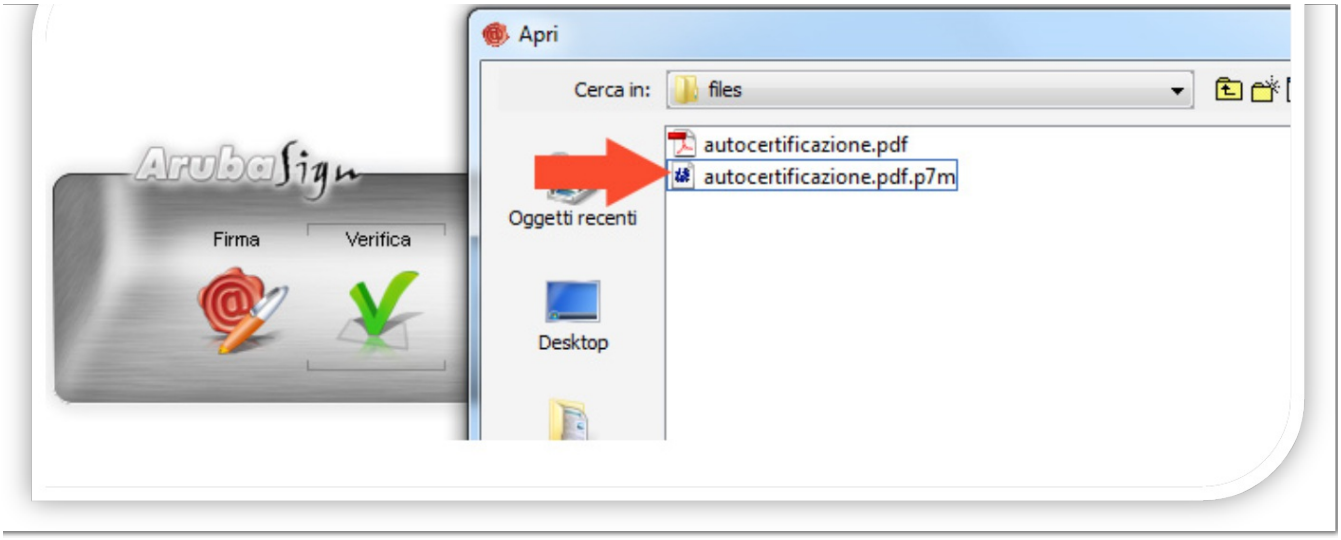


Il documento è stato firmato correttamente e viene data conferma
(nella stessa finestra viene mostrato il percorso in cui viene salvato il file firmato digitalmente)

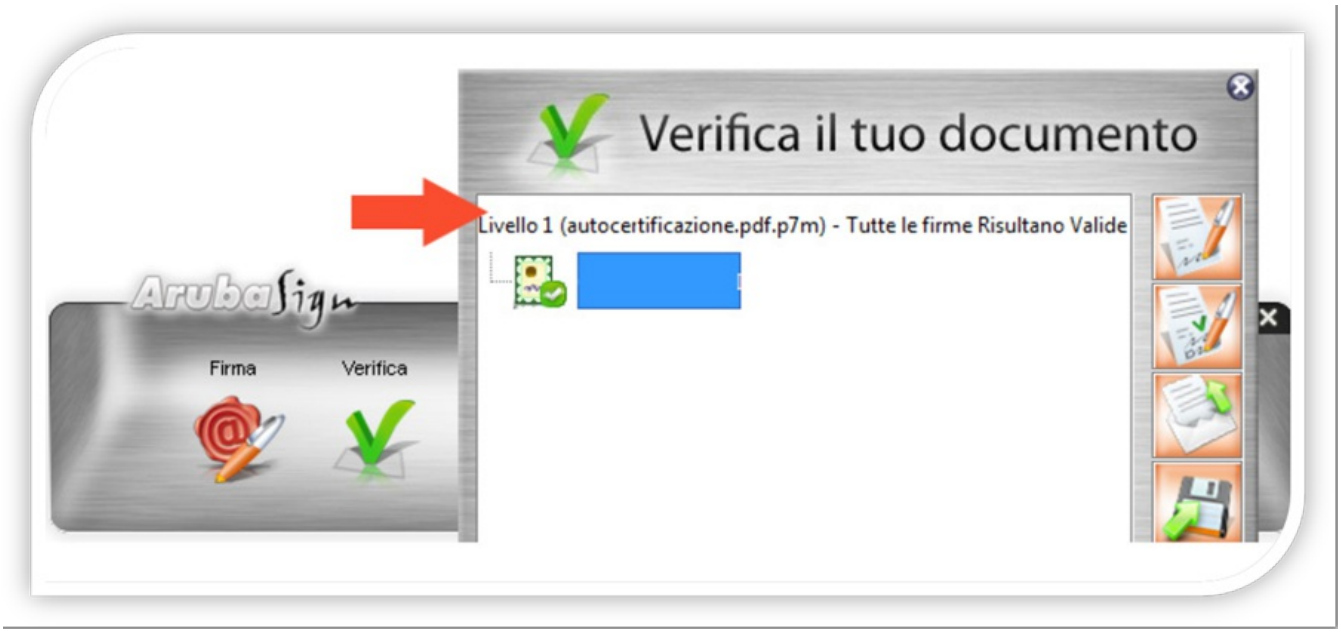
Fase conclusiva. Verifica della firma digitale: cliccare su “verifica”
(è possibile verificare con questi passaggi qualsiasi documento firmato digitalmente)



Selezionare il file firmato digitalmente di cui si vuole verificare la firma e la validità
(il file deve avere come estensione *.pdf o *.p7m)



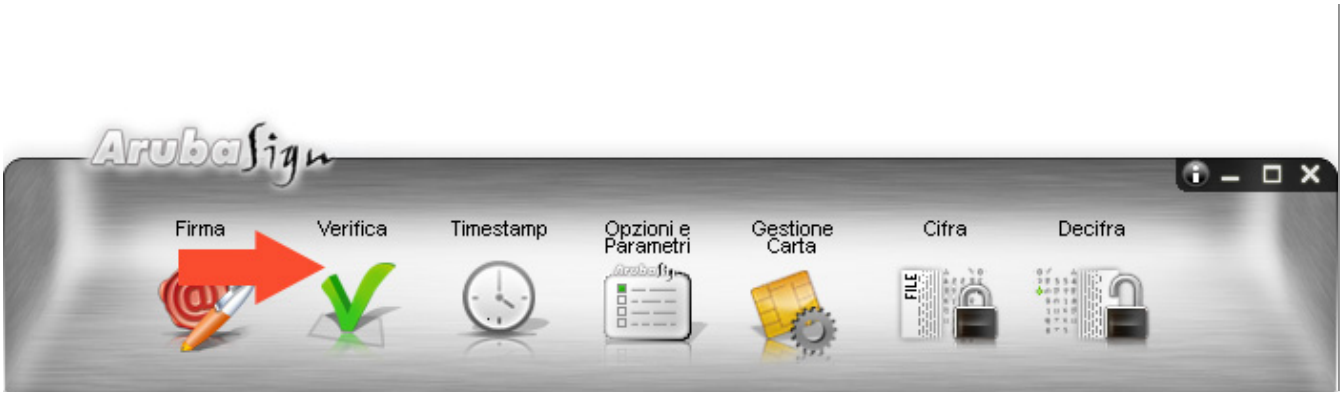
Firma verificata e valida
(vengono mostrati i dettagli sulla firma e sulla sua validità)



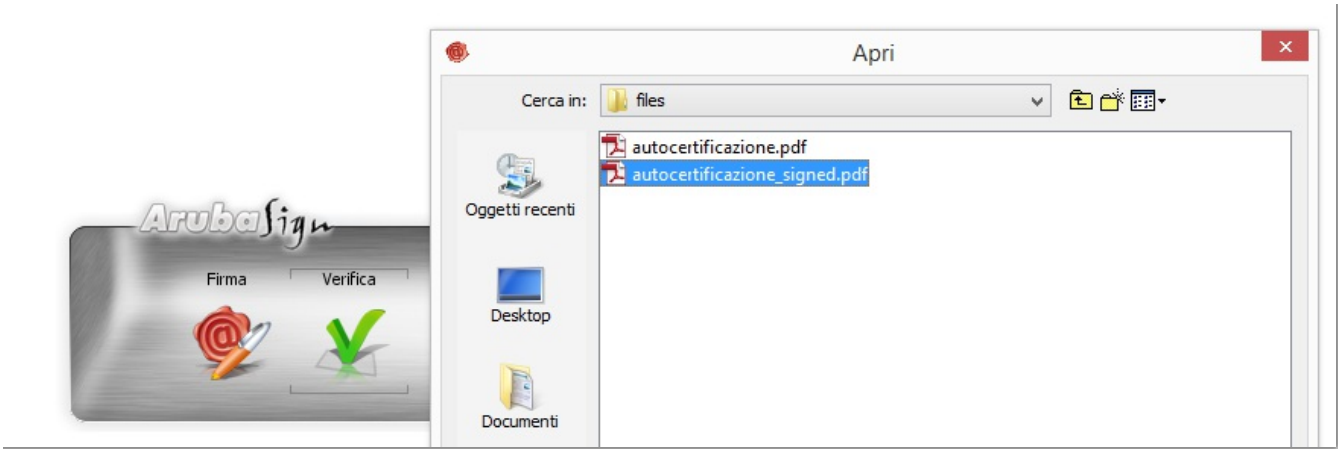
[torna all'indice]

Verificare la validità di una firma su un documento

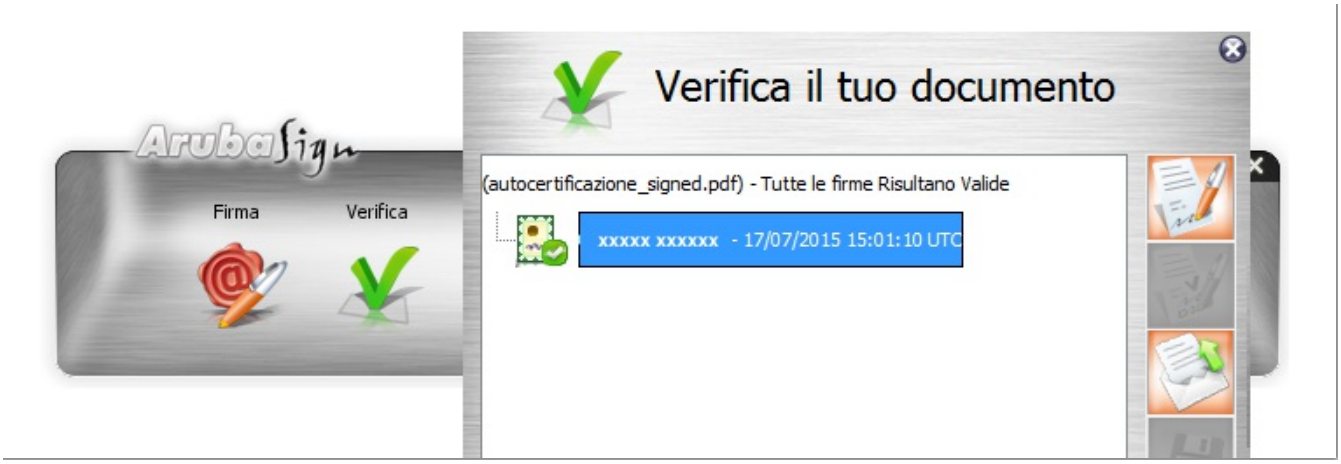
Per verificare la validità di una firma digitale apposta su un documento, aprire il software Aruba Sign e cliccare su *Verifica*.



Selezionare il file firmato digitalmente di cui si vuole verificare la validità.



Verranno così mostrati i dettagli sulla firma e sulla validità del certificato.



[torna all'indice]

Come applicare una marca temporale

Per apporre una marca temporale è sufficiente trascinare il file sopra il pulsante "Timestamp"

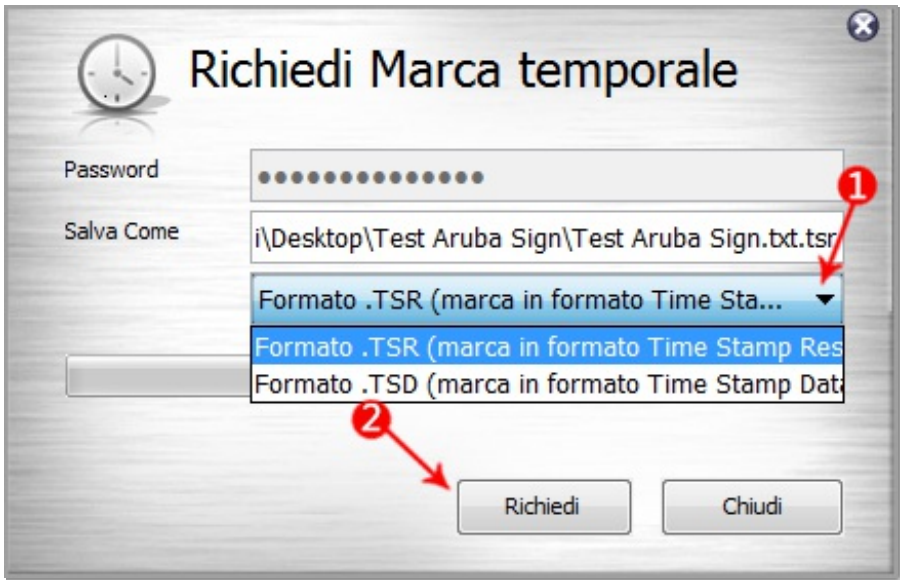
Alla pagina visualizzata:

- Selezionare il formato di salvataggio della marca temporale. E' possibile scegliere tra:
  - **TSR**: Il File creato contiene solo l'impronta del file, non tutto il file, e la marca temporale in formato TSR è separata dal documento. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Se si appone una marca temporale in formato TSR e si desidera inviarla a un destinatario, è necessario inviare anche il documento di origine.
  - **TSD**: Il File creato comprende sia il file sottoposto a marcatura che la marcatura temporale stessa. Se si appone una marca temporale in formato TSD e si desidera inviarla a un destinatario, non è necessario inviare anche il documento di origine.

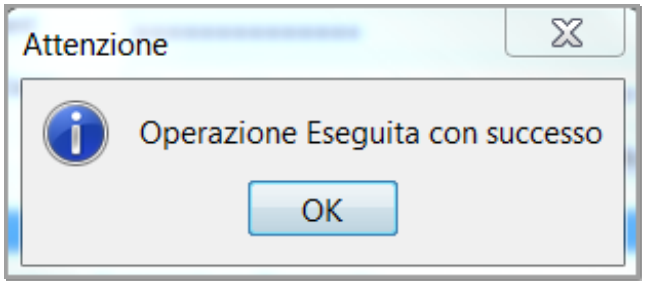
Gli altri dati (password e cartella di destinazione del file) sono indicati automaticamente del sistema

- La password è preimpostata a seguito della configurazione dell'Account di marcatura Temporale
- Il percorso di destinazione del File inserito è la cartella su cui risiede il file originale

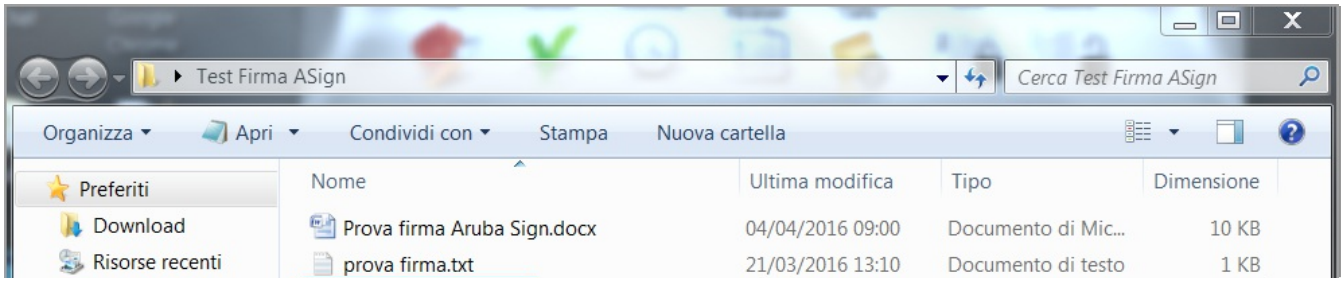
Spuntare su "Richiedi" per completare l'operazione



Cliccare "Ok" al messaggio che notifica la corretta marcatura del file per completare l'operazione



Il file è disponibile nella cartella indicata in fase di apposizione della marcatura stessa



[torna all'indice]

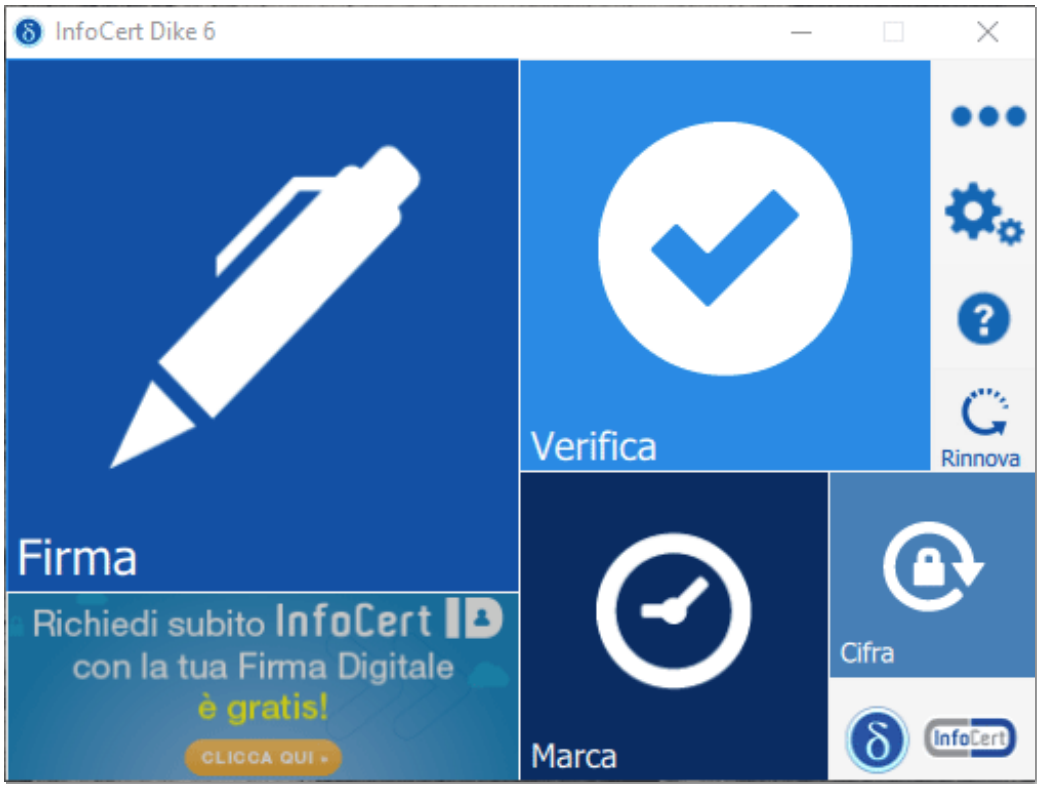
Firmare un documento con Dyke

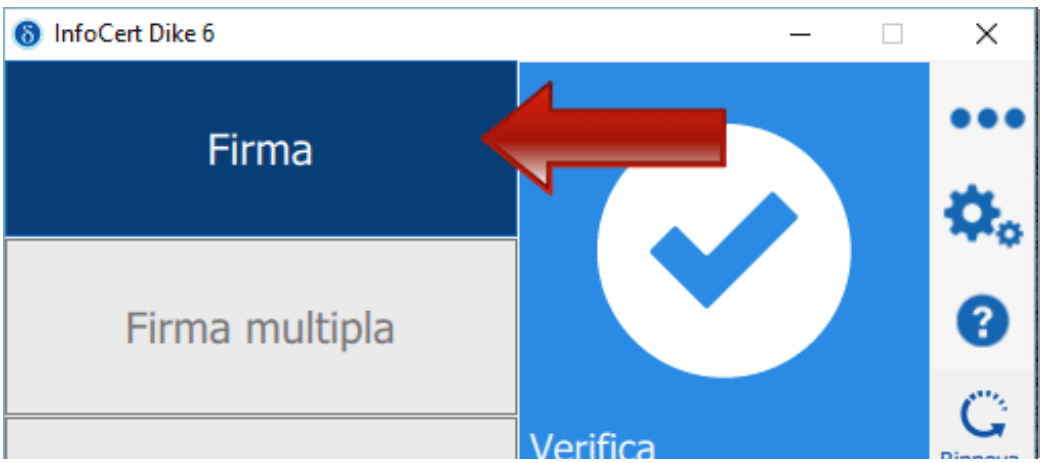
A titolo esemplificativo, di seguito vengono riportate alcune schermate in cui viene simulata la firma digitale di un documento; la firma verrà apposta tramite Dike, software distribuito da Infocert., uno dei certificatori più utilizzati in Italia.

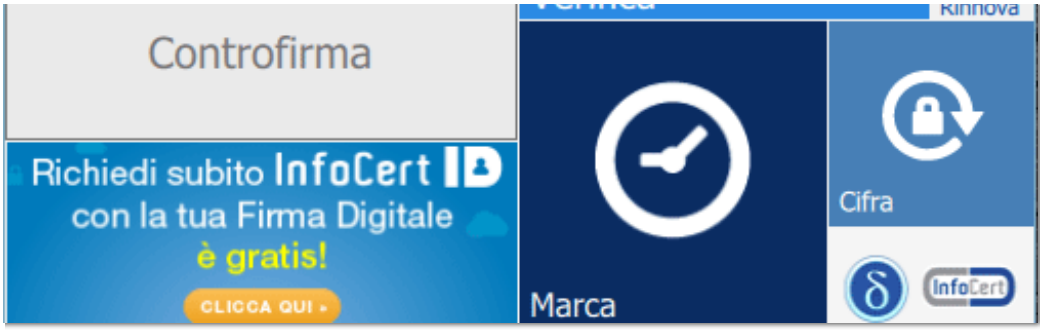
È possibile scaricare il software Dike dal seguente indirizzo:

https://www.firma.infocert.it/prodotti/dike6.php

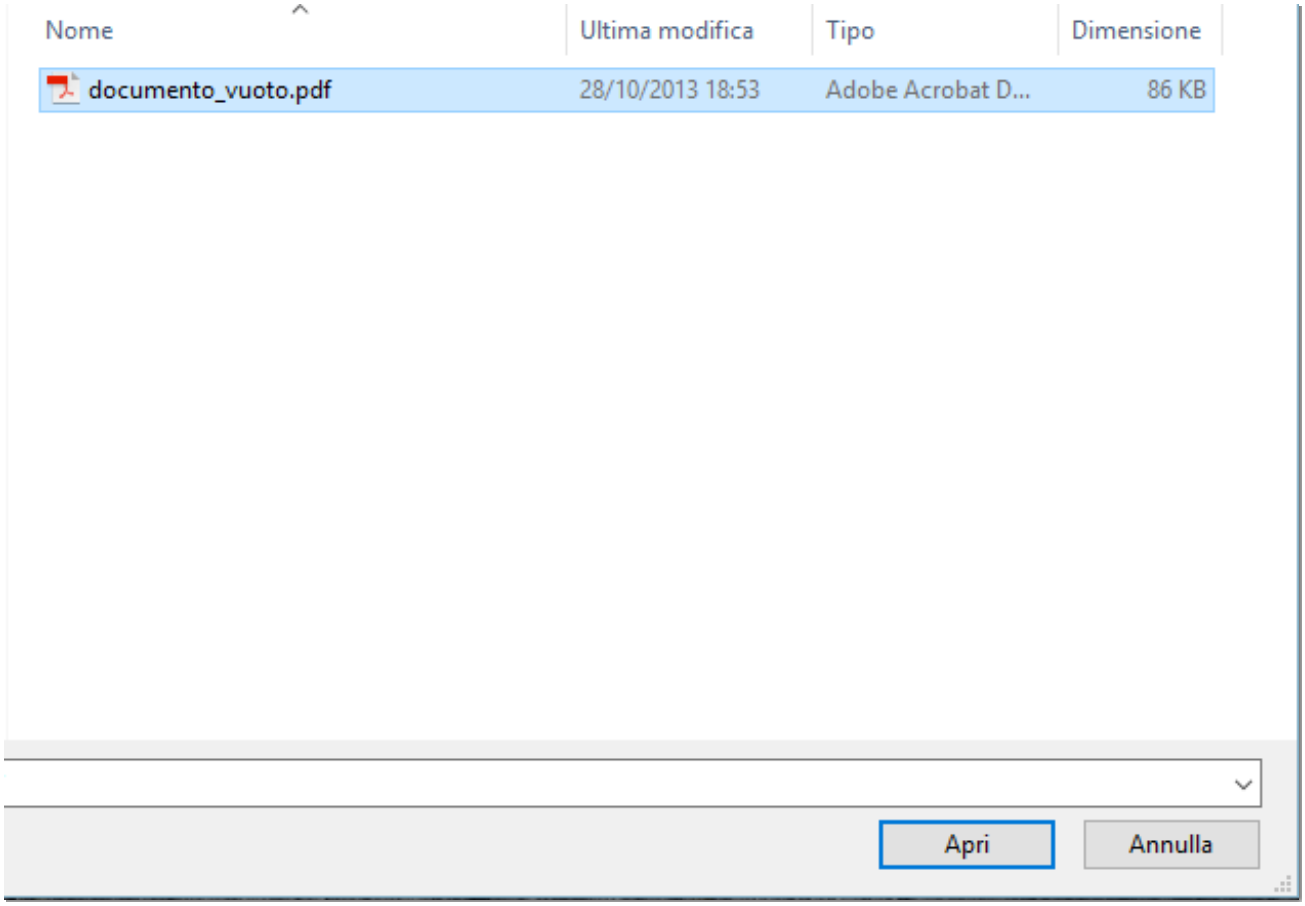
Installare e avviare il software Dike per la firma digitale



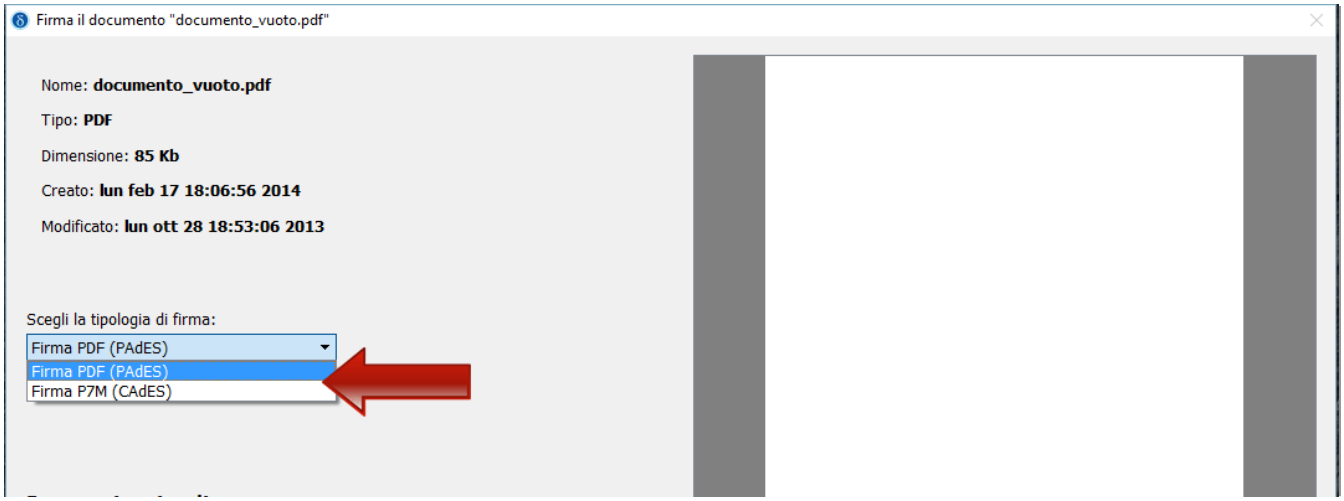


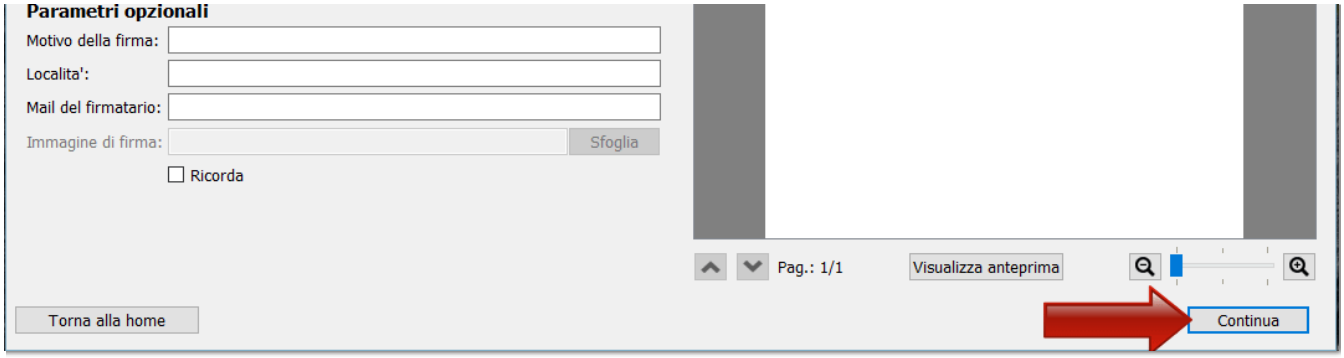


Selezionare il documento da firmare cliccando su *Firma*

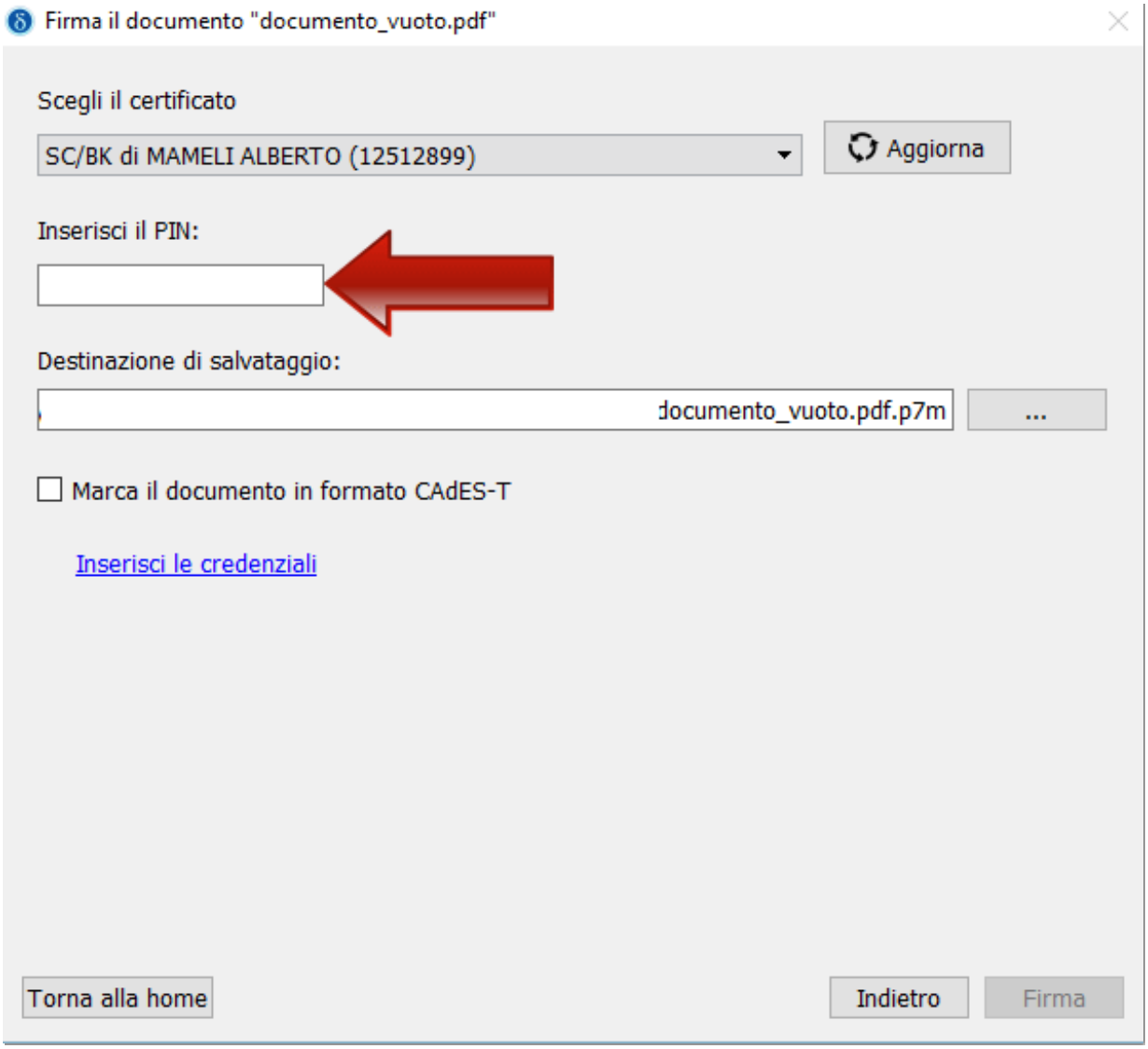


Dal menu a tendina Tipo busta, selezionare la tipologia di firma e cliccare sul pulsante continua.

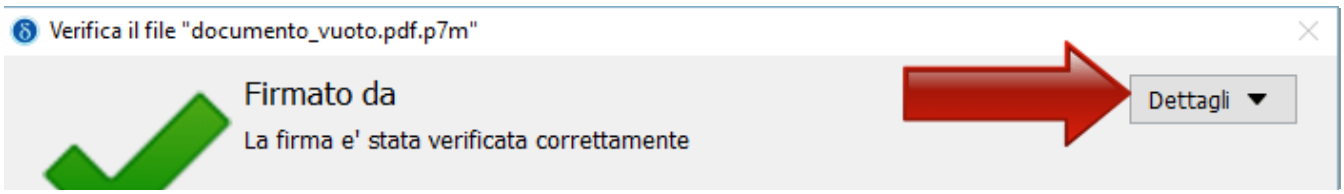




Inserire il PIN, ovvero il codice univoco associato alla propria firma digitale.



Dike darà conferma dell'avvenuta firma.

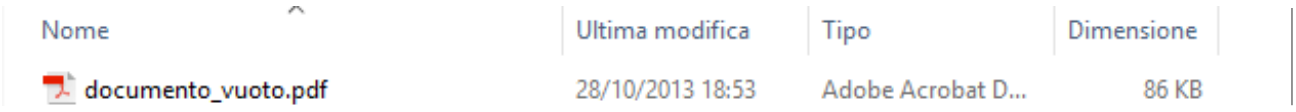


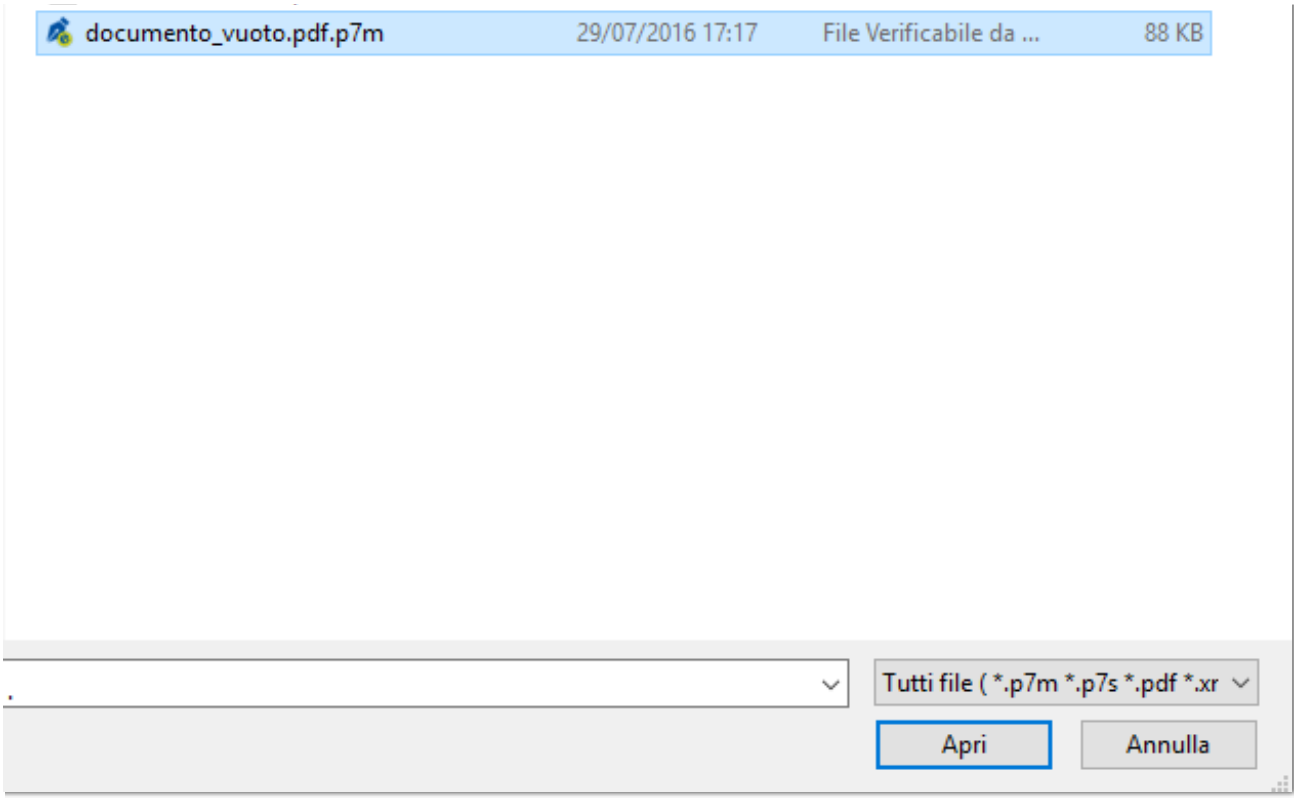
[torna all'indice]

Verificare la validità di una firma su un documento

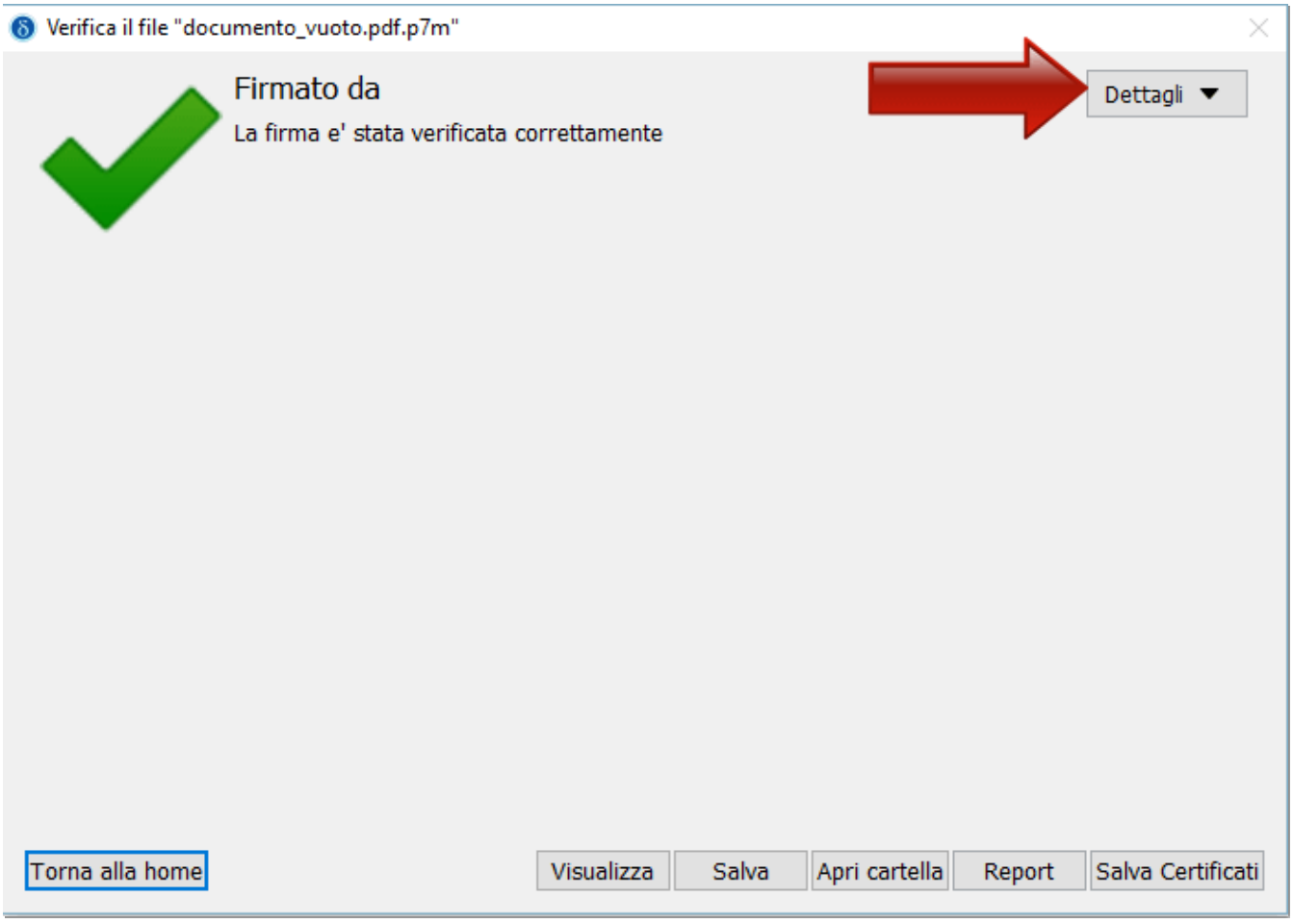
Per verificare la validità di una firma digitale apposta su un documento, aprire il software Dike e cliccare su *Verifica*.

Selezionare il file firmato digitalmente di cui si vuole verificare la validità.





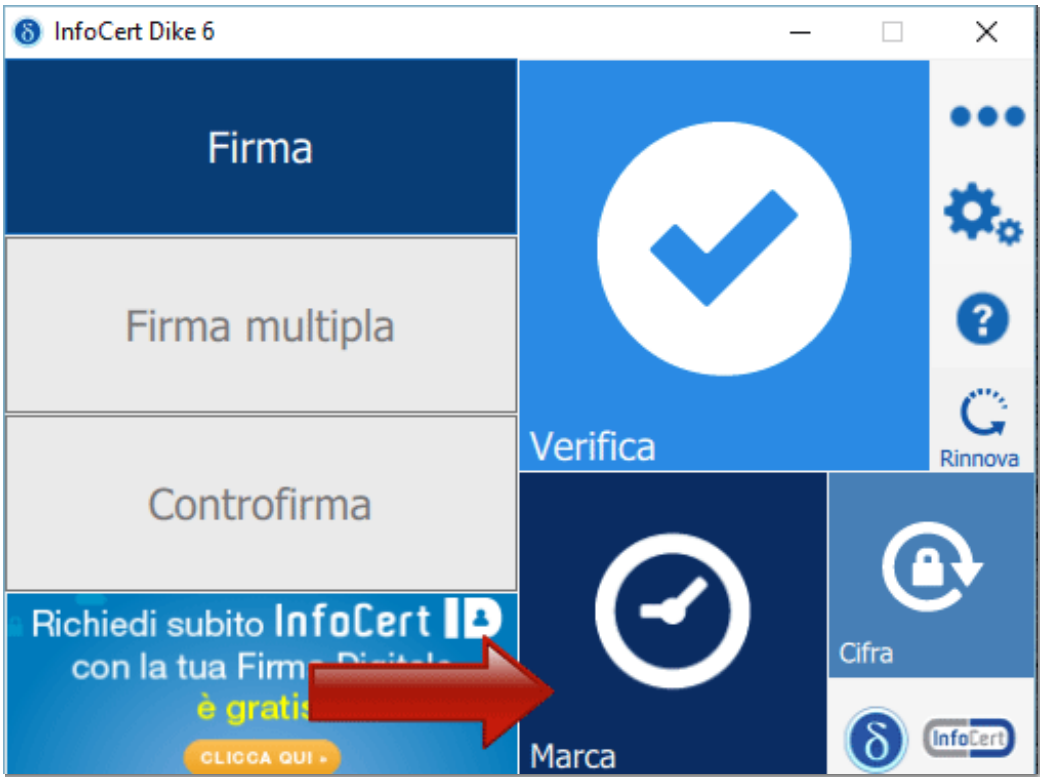
Verranno così mostrati i dettagli sulla firma e sulla validità del certificato.



[torna all'indice]

Come applicare una marca temporale

Per apporre una marca temporale è sufficiente trascinare il file sopra il pulsante "Marca"



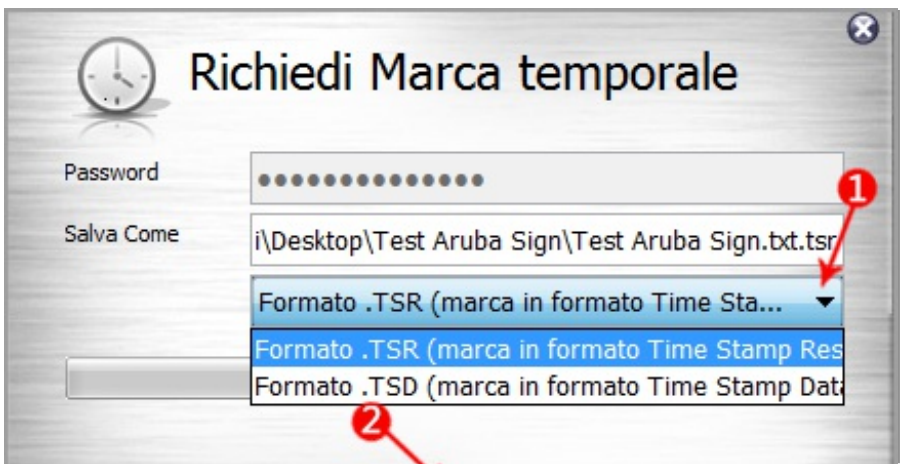
Alla pagina visualizzata:

- Selezionare il formato di salvataggio della marca temporale. E' possibile scegliere tra:
  - **TSR**: Il File creato contiene solo l'impronta del file, non tutto il file, e la marca temporale in formato TSR è separata dal documento. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Se si appone una marca temporale in formato TSR e si desidera inviarla a un destinatario, è necessario inviare anche il documento di origine.
  - **TSD**: Il File creato comprende sia il file sottoposto a marcatura che la marcatura temporale stessa. Se si appone una marca temporale in formato TSD e si desidera inviarla a un destinatario, non è necessario inviare anche il documento di origine.

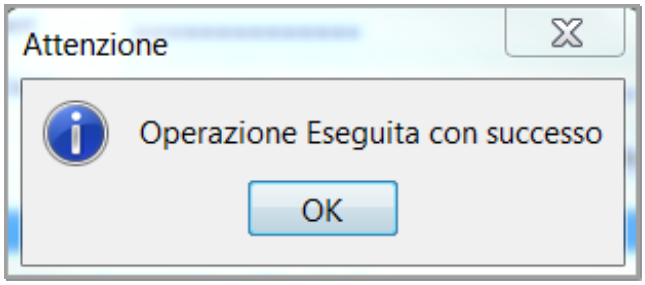
Gli altri dati (password e cartella di destinazione del file) sono indicati automaticamente del sistema

- La password è preimpostata a seguito della configurazione dell'Account di marcatura Temporale
- Il percorso di destinazione del File inserito è la cartella su cui risiede il file originale

Spuntare su "Richiedi" per completare l'operazione



Cliccare "Ok" al messaggio che notifica la corretta marcatura del file per completare l'operazione



[torna all'indice]

Firmare un documento con Firma OK

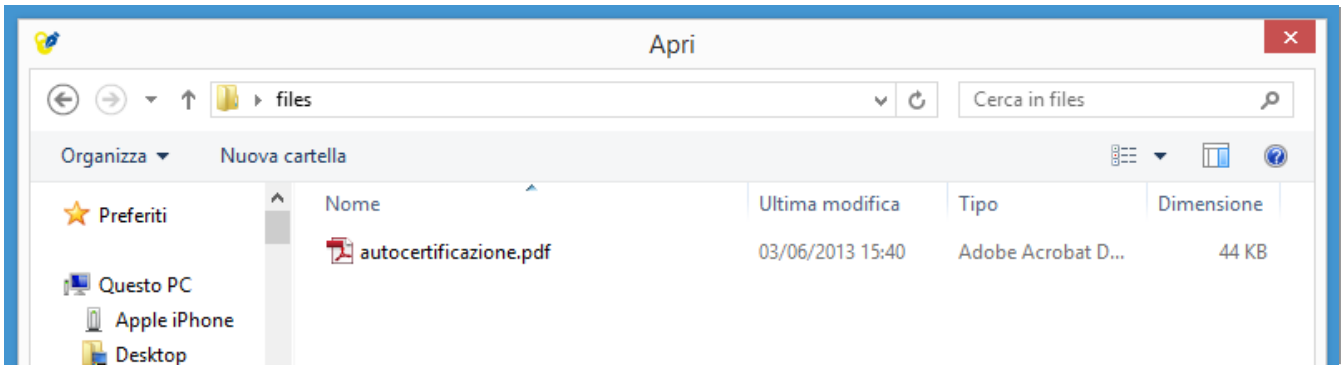
A titolo esemplificativo, di seguito vengono riportate alcune schermate in cui viene simulata la firma digitale di un documento; la firma verrà apposta tramite Firma OK, software distribuito dal Gruppo Poste Italiane.

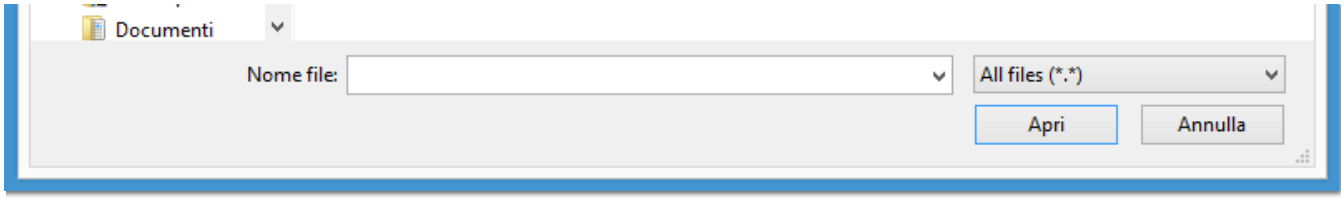
È possibile scaricare il software Firma OK dal seguente indirizzo:

- http://postecert.poste.it/firma/download.shtml

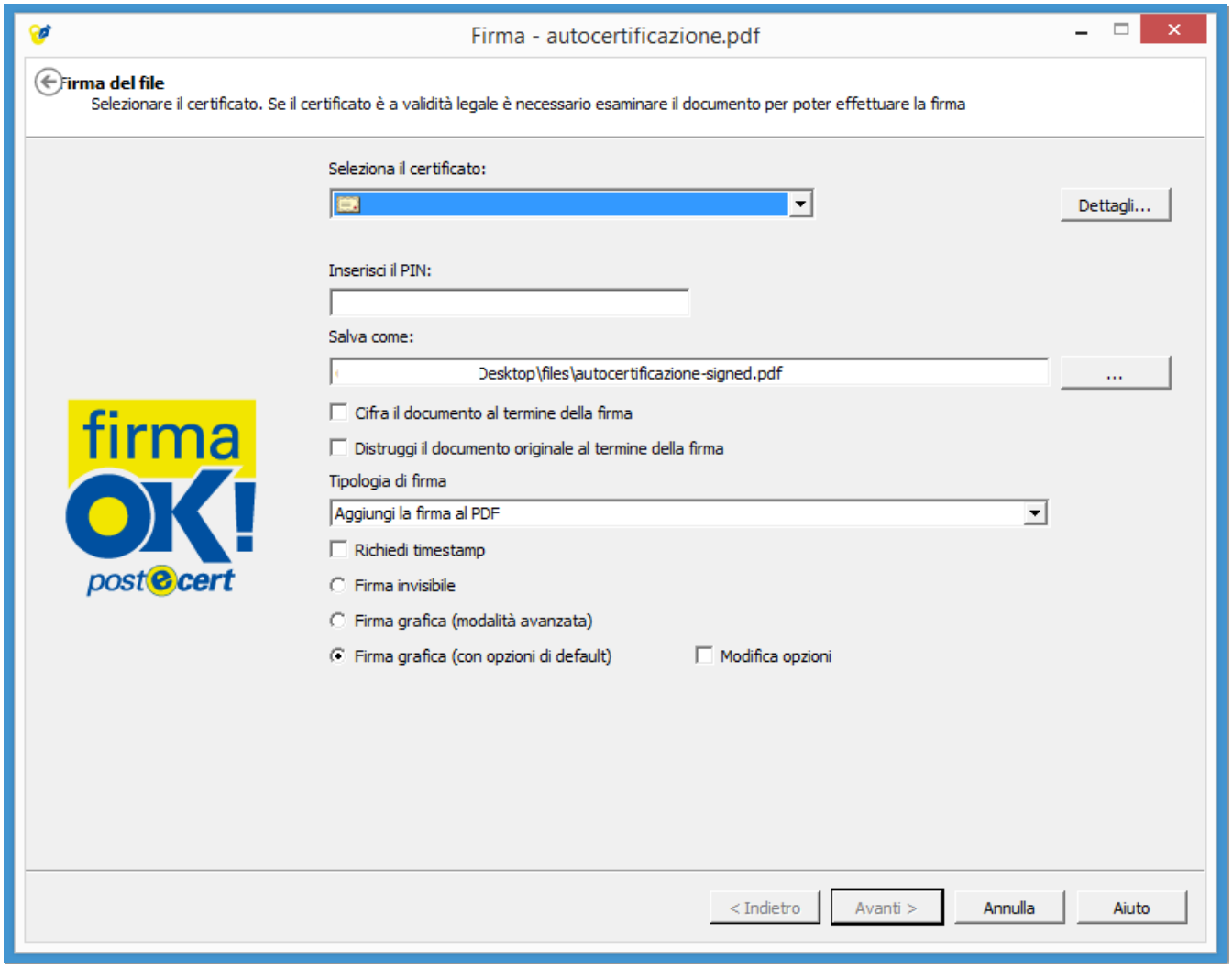
Installare e avviare il software Firma OK per la firma digitale

Selezionare il documento da firmare cliccando su *Firma*

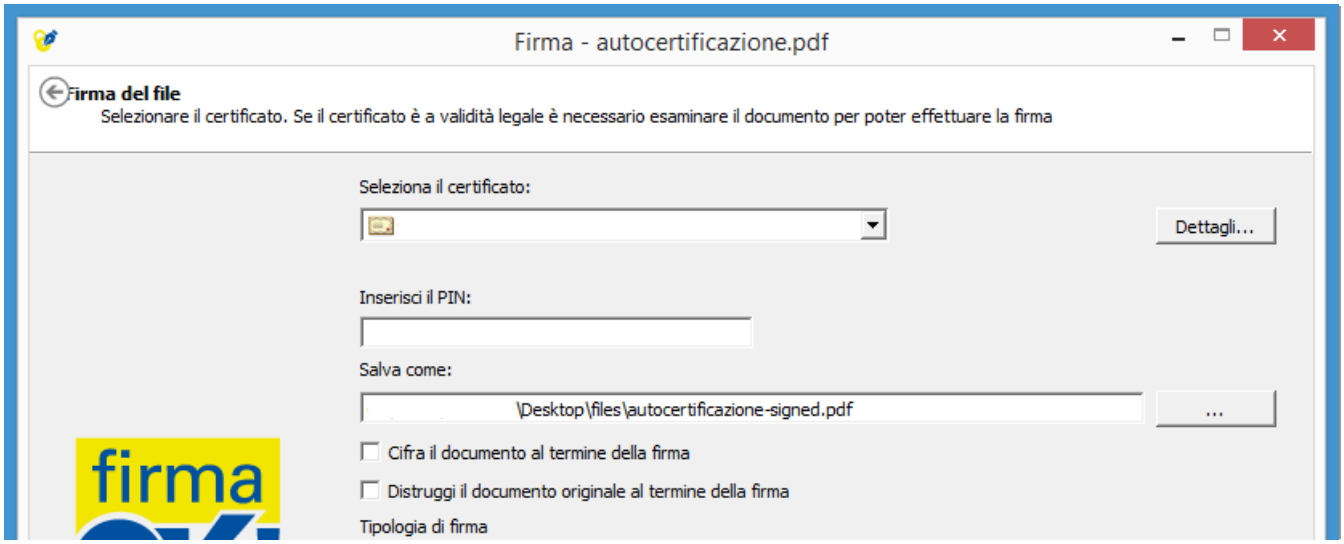


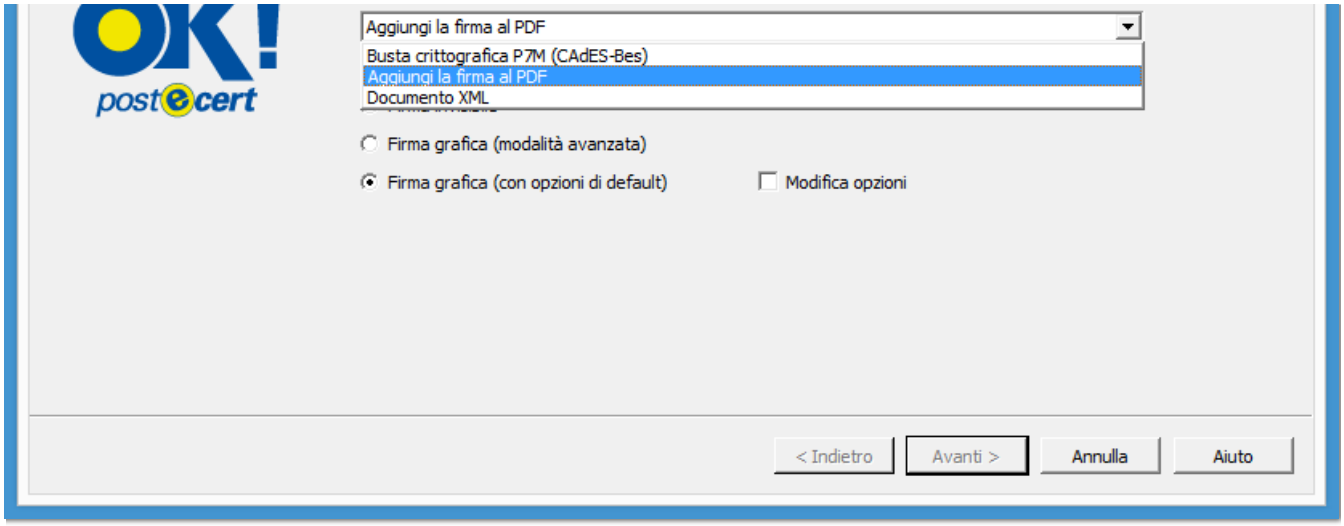


Inserire il PIN, ovvero il codice univoco associato alla propria firma digitale.



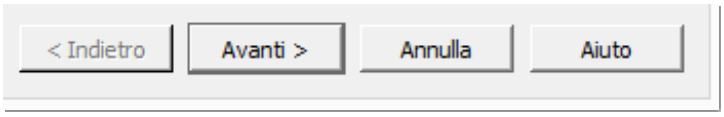
Dal menu a tendina Tipologia di firma busta, selezionare l'opzione *aggiungi firma al PDF* per scegliere PADES come tipologia di firma.



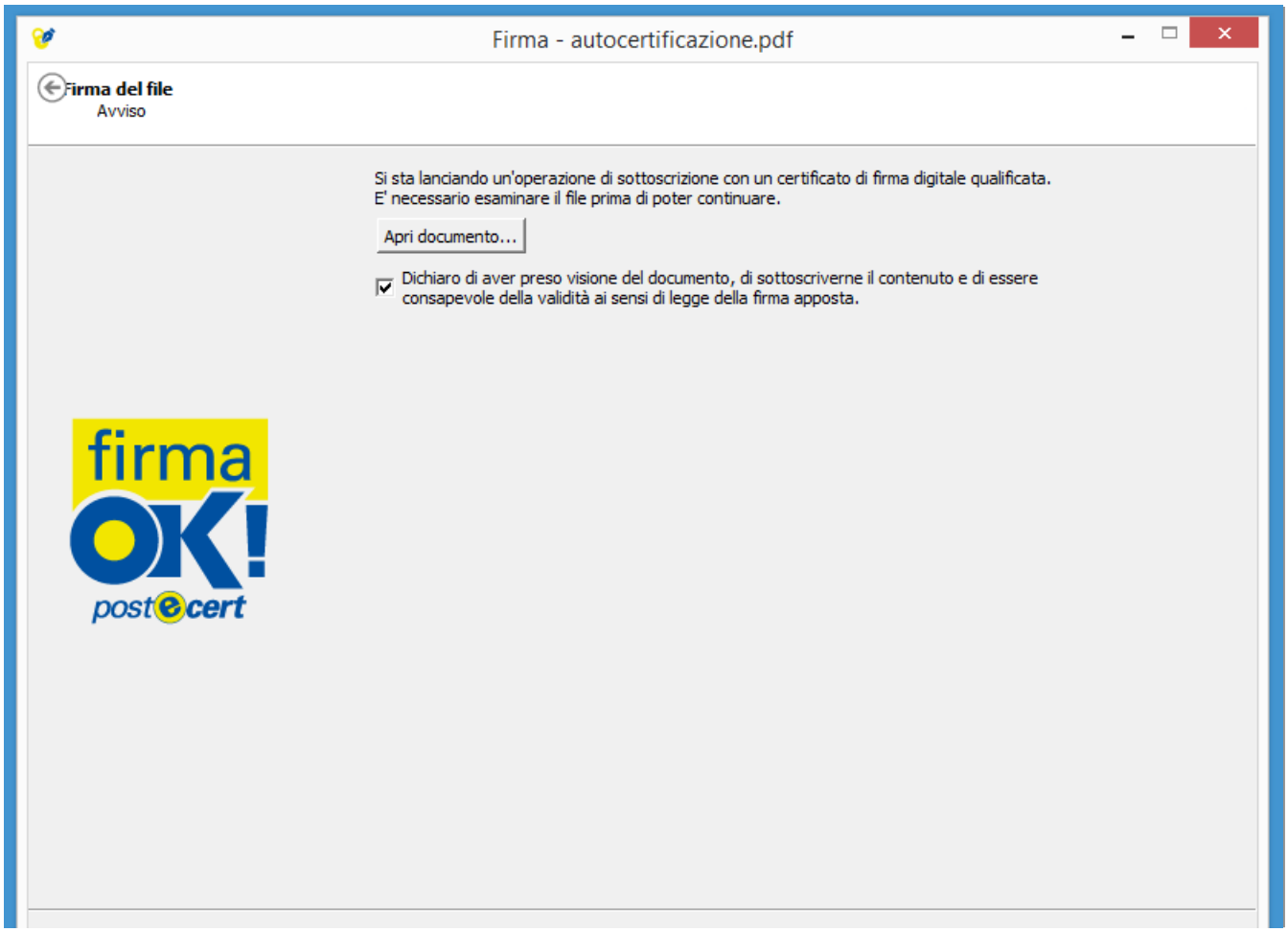


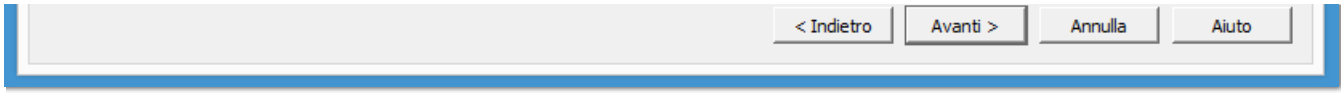
Quando viene scelto il formato PADES, è necessario scegliere se inserire graficamente la propria firma, o se eseguirla invisibile.

Cliccare su *Avanti* dopo aver inserito il PIN

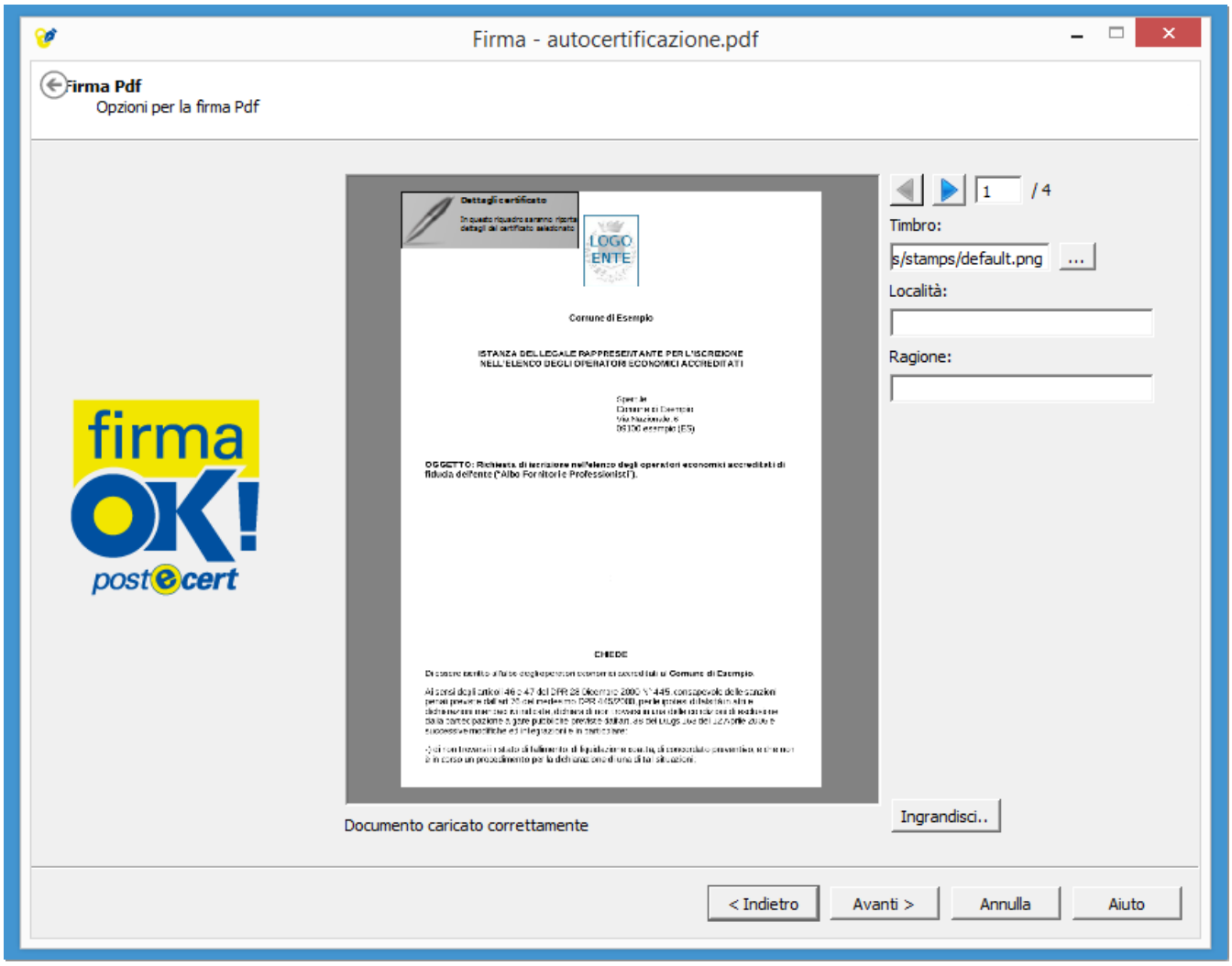


Dichiarare di aver letto il documento prima di apporre la firma. Cliccando su *Apri documento* sarà possibile visualizzare il file che ci si appresta a firmare digitalmente. Dopo aver verificato di aver selezionato il file corretto, spuntare la casella accanto alla dicitura “Dichiaro di aver preso visione del documento…”



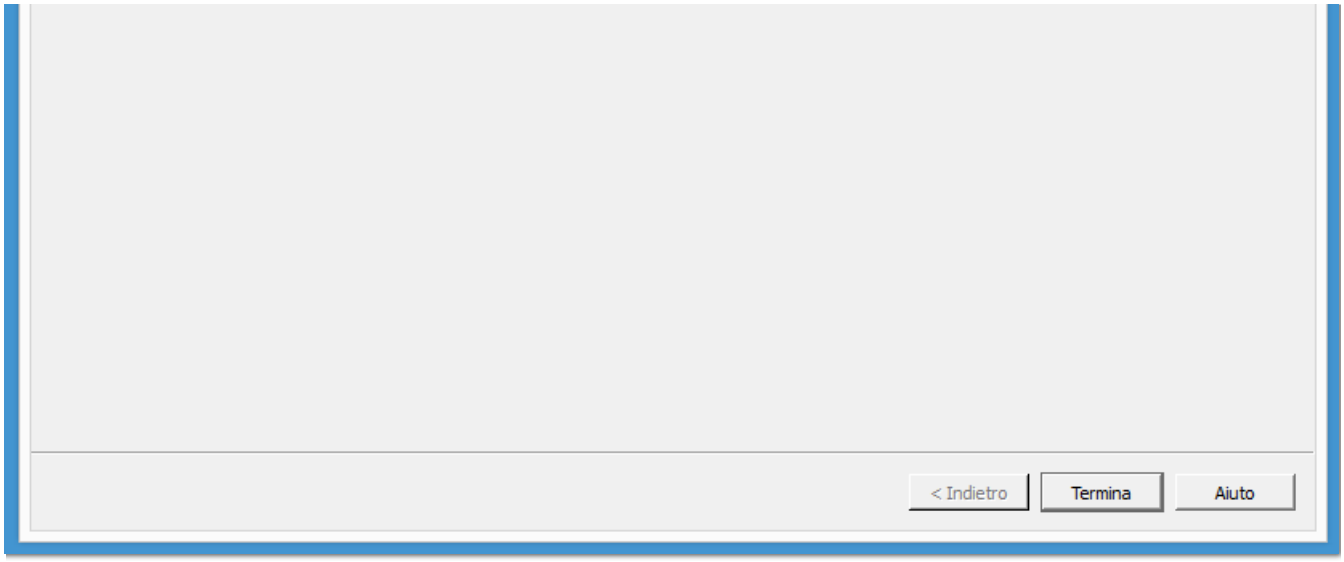


Cliccando ancora su *Avanti*, il documento verrà firmato. Se si sceglie di eseguire una firma grafica, si dovrà selezionare l'area in cui eseguire la firma. Cliccando su *Avanti*, il documento verrà firmato graficamente e salvato.



Firma OK darà conferma dell'avvenuta firma, indicando la cartella in cui si trova il file firmato digitalmente.

Cliccando su *Termina*, la procedura verrà conclusa.

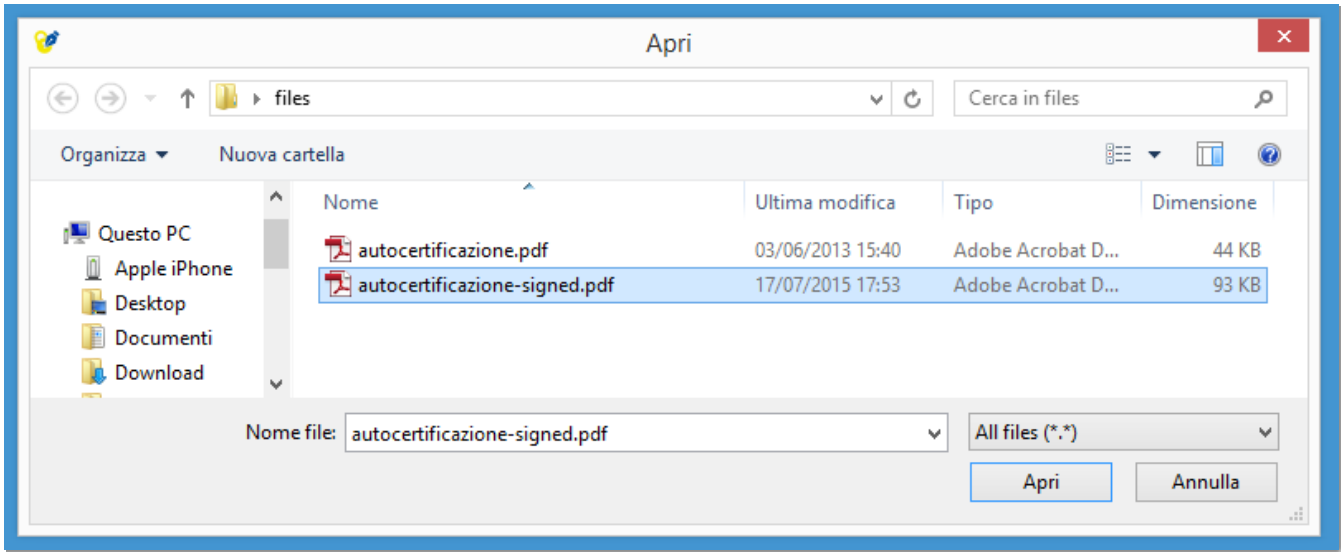


[torna all'indice]

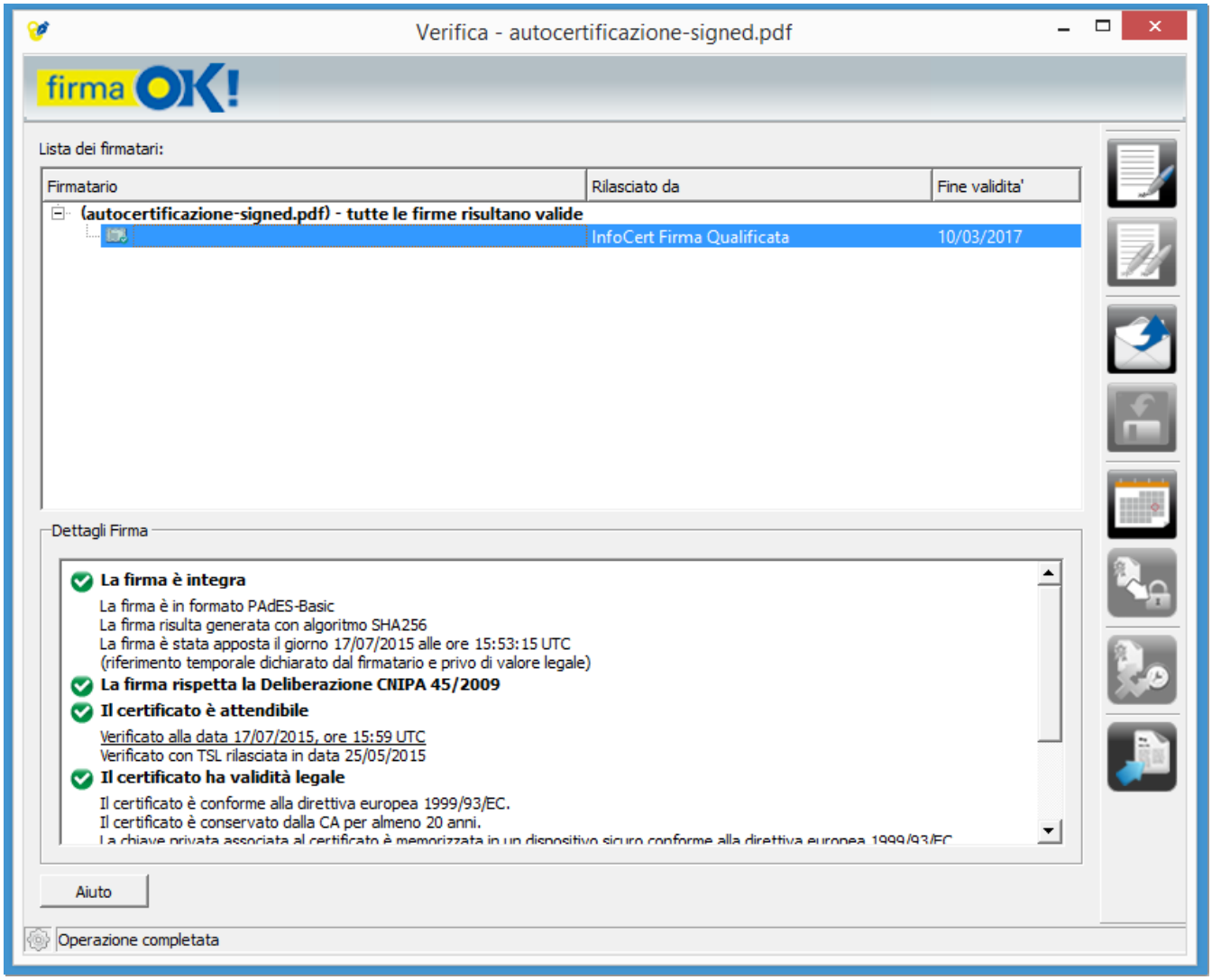
Verificare la validità di una firma su un documento

Per verificare la validità di una firma digitale apposta su un documento, aprire il software Firma OK e cliccare su *Verifica*.

Selezionare il file firmato digitalmente di cui si vuole verificare la validità.



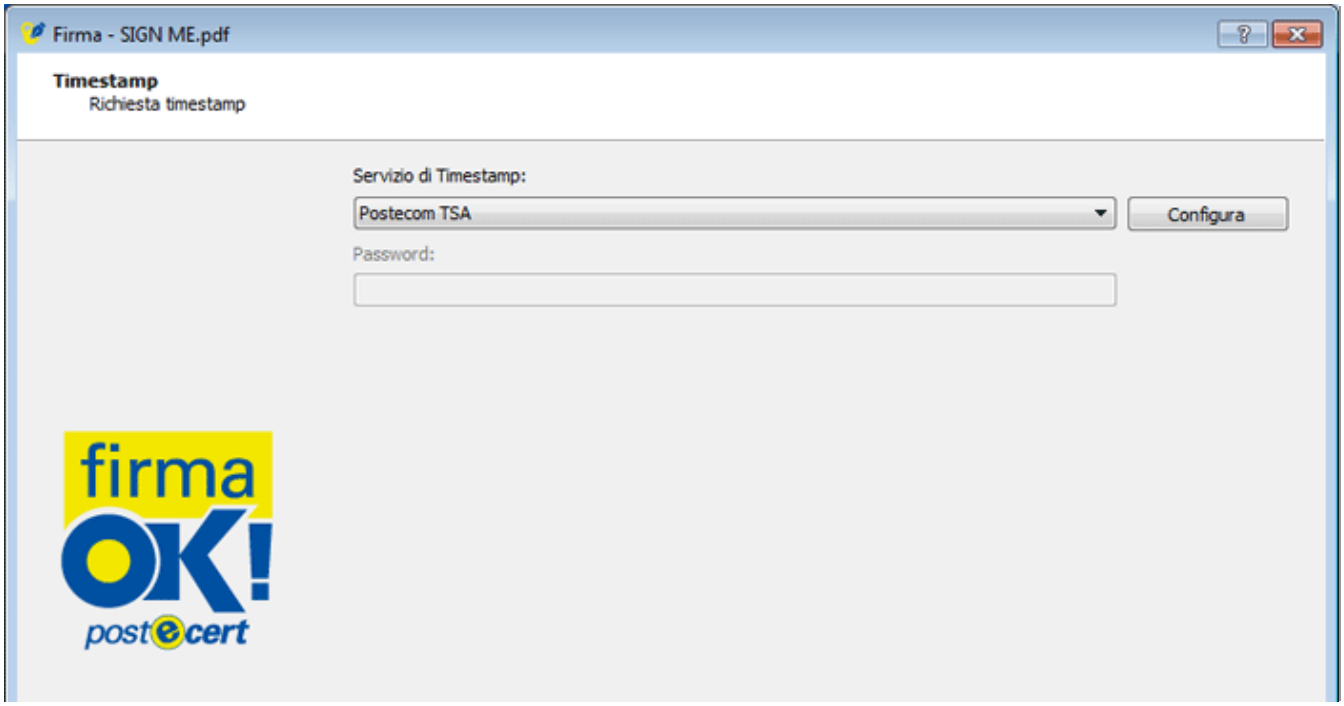
Verranno così mostrati i dettagli sulla firma e sulla validità del certificato.

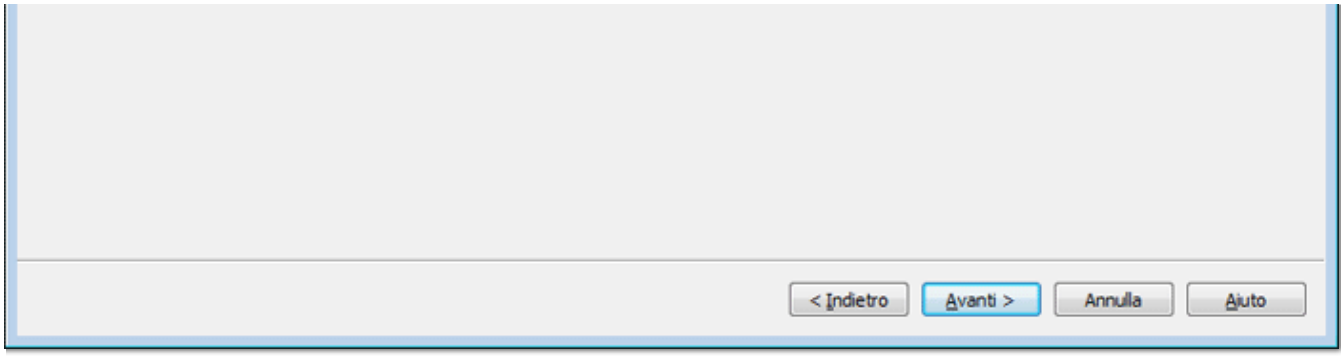


[torna all'indice]

Apposizione di marche temporali

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





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

Fase 1

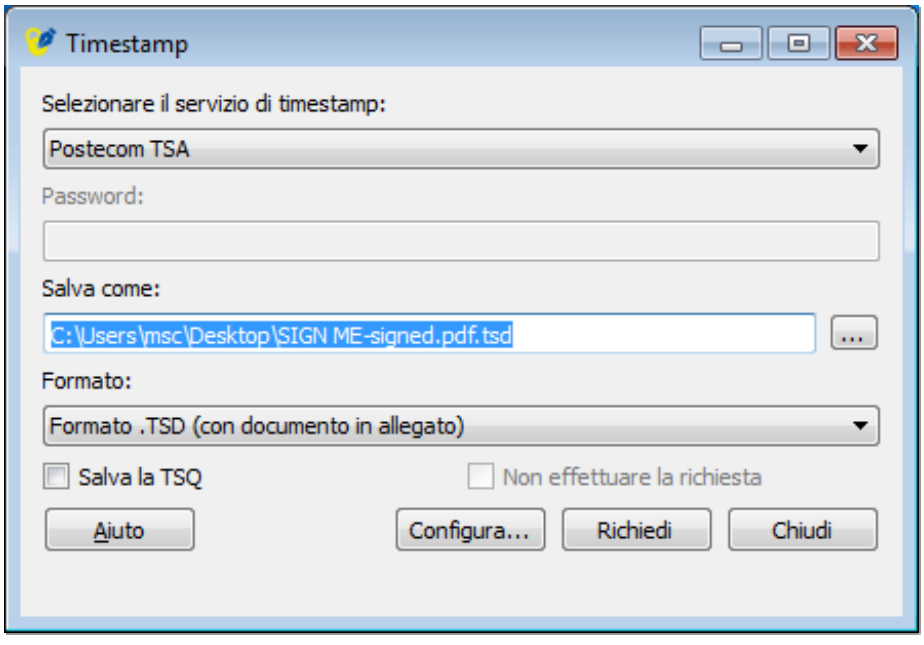
Per avviare l'operazione di marcatura temporale di un documento, si può alternativamente:

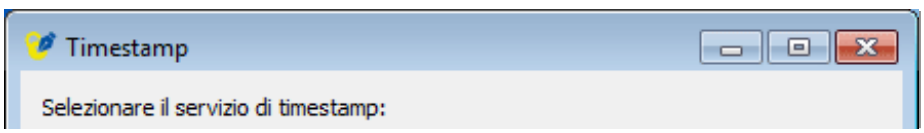
- selezionare e trascinare (drag&drop) il documento che si intende marcare temporalmente sul bottone "Marca Temporale" del menù principale;
- cliccare sul bottone "Marca Temporale" del menù principale e selezionare il documento dalla finestra di navigazione del PC.

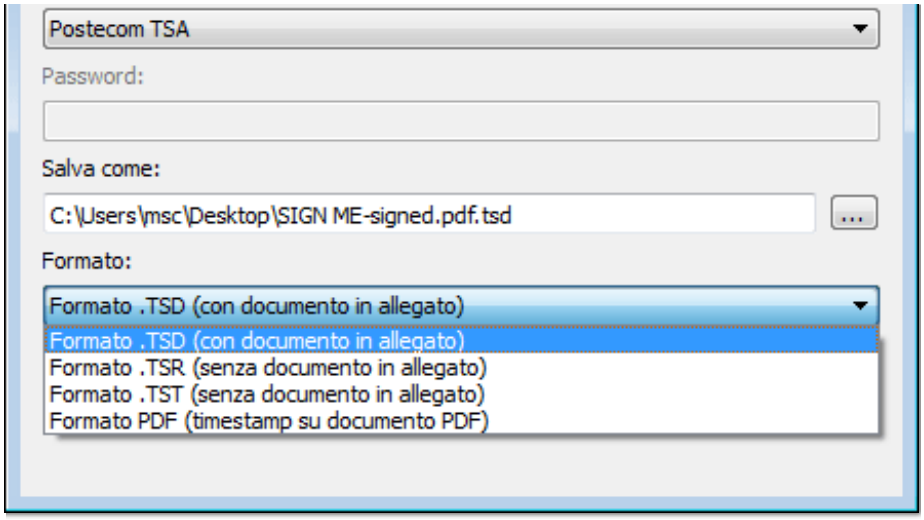
Fase 2

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

- .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







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 bottone Configura accedendo al pannello.

Fase 3
Per inviare la richiesta di marcatura temporale cliccare sul bottone "Richiedi".

Fase4
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 5
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 bottone "Chiudi".

[torna all'indice]

@PEC

La Posta Elettronica Certificata (denominata anche **Posta Certificata** o **PEC**) è il nuovo sistema di posta elettronica che consente di fornire al mittente garanzie sulla trasmissione e la ricezione dei messaggi.

L'invio e la consegna dei messaggi, infatti, vengono attestati tramite specifiche ricevute che il gestore del servizio rilascia al mittente e che conferiscono all'e-mail lo stesso valore di una raccomandata con ricevuta di ritorno (secondo quanto stabilito dal decreto DPR 11 Febbraio 2005 che disciplina l'utilizzo della PEC.)

La **Posta Certificata** diventa così il mezzo di comunicazione più immediato e sicuro per la trasmissione di documenti, agevolando tutti quelli che sono gli iter burocratici tra i cittadini e pubbliche amministrazioni.

In più, oltre ad avere la certezza della ricezione, con il sistema di Posta Certificata è garantita la certezza del contenuto: i protocolli di sicurezza utilizzati fanno sì che non siano possibili modifiche al contenuto del messaggio e agli eventuali allegati

del messaggio e agli eventuali allegati.

N.B.: E' necessario chiarire che, una comunicazione di posta elettronica certificata, ha valore di raccomandata con ricevuta di ritorno solo nel caso in cui sia il mittente che il destinatario utilizzino indirizzi di posta certificata e che i messaggi siano inviati tramite i server di un gestore certificato.
Infatti, nel caso in cui venga inviato un messaggio da un' indirizzo di posta certificata a uno di posta elettronica ordinaria, il destinatario riceverà la Ricevuta di Accettazione (all'interno di un messaggio detto Busta di Trasporto contenente i Dati di Certificazione) ma NON quella di Avvenuta Consegna.

[torna all'indice]

Normativa di riferimento

- Legge 18 giugno 2009, n. 69 recante "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile": Art.34.
- Circolare CNIPA CR/49 recante "Modalità di accreditamento all'elenco pubblico dei gestori di PEC";
- Decreto 2 novembre 2005 recante "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata";
- DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3";
- Codice dell'Amministrazione Digitale: artt. 6, 45 e seguenti;
- "Direttiva per l'utilizzo della posta elettronica nelle pubbliche amministrazioni", emanata il 27 novembre 2003 dal Ministro dell'Innovazione e le Tecnologie di concerto con il Ministro per la Funzione Pubblica;
- DPR 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"

[torna all'indice]

La Marca Temporale

La Marca Temporale è un servizio che permette di datare in modo certo e legalmente valido ad un documento informatico (non necessariamente firmato digitalmente), consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

E' obbligatoria dal 01 gennaio 2013 per i segretari di Enti pubblici, per la stipula dei contratti, ove successivamente alla firma dei Dirigenti di settore, il segretario dovrà verificare l'autenticità delle Firme digitali ed apporre la marca temporale sul contratto.

Quando normalmente si appone la Firma digitale su un documento informatico, l'orario mostrato proviene dal computer del firmatario. Dato che il certificato di firma è valido per tre anni dal momento della sua emissione, questa limitazione tecnica compromette la validità nel tempo della firma stessa, poichè dopo sua la scadenza, sarebbe possibile modificare (portando indietro) la data del sistema operativo e dare a credere che al momento della firma, il certificato fosse ancora valido. Per questo motivo la validità dei file firmati, diventa automaticamente ripudiabile in fase di giudizio, dopo la scadenza del certificato di firma. La validità della firma viene, chiaramente estesa, se si decide di rinnovare il certificato di firma senza cambiare la smart card.

Il servizio di Marca Temporale può essere utilizzato sia su file non firmati digitalmente, garantendone una

collocazione temporale certa e legalmente valida, sia su documenti informatici sui quali è stata apposta Firma Digitale: in tal caso la Marca Temporale attesterà il preciso momento temporale in cui il documento è stato creato, trasmesso o archiviato.

Come sancito dall'articolo 49 del Dpcm del 30/03/2009, le Marche Temporali emesse devono essere conservate in appositi archivi per un periodo non inferiore a 20 anni.

Caratteristiche

Come i file firmati digitalmente diventano .P7M, i file "Marcati Temporalmente" utilizzano come estensione .TSD (TimeStampedData). E' possibile inoltre scindere il file della marca da quello del documento marcato, in quel caso la marcatura generata avrà come estensione .TST ("Time-stamp Token") oppure .TSR ("Time-stamp Response", vecchio formato) in base al setup del software. Sebbene il TSR stia sparendo, entrambi sono validi legalmente ma hanno due codifiche diverse, quindi non è sicuro che i sistemi automatici di destinazione possano accettarli entrambi. Un file firmato e marcato contemporaneamente assume invece estensione .M7M . La marca temporale può essere anche aggiunta al .PDF lasciandone inalterata l'estensione.

Il file originale e la relativa marca temporale possono:

- Essere mantenuti separatamente (es.: file ".TXT" file ".TSR"): ma bisogna ricordarsi che i due file sono correlati, altrimenti la marca temporale da sola non è valida;
- Essere accoppiati in un unico file secondo lo standard RFC 5544: in tal caso viene creato un file con estensione '.TSD', che comprende sia il file originale, ad esempio '.TXT', che la marca temporale ".TSR/.TST";
- Essere accoppiati in un unico file secondo una regola pratica, mediante creazione di un file di tipo S/MIME, con estensione '.M7M', che comprende sia il file originale, ad esempio '.TXT', che la marca temporale ".TSR/.TST";

Riassumendo:

- Un file .TXT firmato digitalmente assume l'estensione .P7M
- Un file .TXT marcato temporalmente assume l'estensione .TSD
- Un file .P7M marcato temporalmente assume l'estensione .M7M
- Un file .PDF (sia firmato che non) marcato temporalmente può essere lasciato con estensione .PDF

[torna all'indice]

Torna su